



## **POLITICAS DE SEGURIDAD UNIVERSIDAD DE CELAYA**

**Última actualización (25 de mayo de 2006)**

**Una de las líneas institucionales es el aprovechamiento de la tecnología en nuestra práctica educativa**

Con los avances de la tecnología gran parte de la información que generamos se encuentra en los equipos de cómputo, esto nos ha permitido compartir de forma más fácil la información y tener nuestros documentos importantes en un medio electrónico evitando de esta manera el desperdicio de hojas.

Para que esta información no se ponga en riesgo, es necesario establecer conductas de seguridad. La seguridad son los procedimientos y actividades que hacemos para que nuestra información se encuentre a salvo. No existen sistemas 100% seguros por lo que es importante que tomemos las medidas necesarias para evitarlo al máximo.

### **Reglamento para el uso de los recursos informáticos de la Universidad de Celaya.**

Para que cada usuario de la Universidad de Celaya tenga acceso a los recursos e infraestructura dentro del campus deberá cumplir con las siguientes normativas:

- Tener instalado el software antivirus y antispymware institucional.
- Por ningún motivo se permitirá ver pornografía en el campus, no importa que el usuario que la vea sea propietario de la computadora (el ver páginas pornográficas es causa de despido).
- No se deben descargar archivos con títulos atractivos pero sospechosos, desde canales de Chat, redes compartidas como KaZaa, Morpheus, BearShare, etc.



- Es responsabilidad del usuario permitir que su computadora actualice los parches de seguridad (en el anexo se explica el procedimiento).
- No instalar copias de software que no tenga su respectiva licencia (incluye juegos, utilerías, protectores de pantalla o cualquier software que no provenga de una fuente confiable).
- En computadoras que son propiedad de la Universidad de Celaya, queda estrictamente prohibido instalar cualquier software que no ha sido aprobado por la dirección de Informática, en caso de encontrar software que pueda comprometer la seguridad el departamento de Informática se reserva el derecho de eliminarlo en cualquier momento y aplicar la sanción administrativa correspondiente.
- En computadoras de uso personal, el empleado (administrativo, docente, etc.) deberá hacerse responsable del software instalado en su computadora y el comportamiento que genere al conectarla a la red del campus, debiendo responder por cualquier daño o mal funcionamiento que su equipo produzca en los servicios o recursos tecnológicos de la Universidad.

### **Recomendaciones de Políticas de Seguridad:**

- Cuando el sistema le notifique que hay actualizaciones listas para descargarse, instálelas en cuanto le sea posible.
- No ejecutar ningún archivo contenido en un mensaje de correo no solicitado o enviado por un remitente desconocido, así ofrezca atractivos premios o temas provocativos.
- Tener al menos Windows XP Professional actualizado
- No se debe confiar en los archivos gratuitos que se descargan de sitios web desconocidos, ya que son una potencial vía de propagación de virus.
- Siempre que aparezca una ventana nueva lea primero la información antes de continuar.
- Configurar el sistema para que muestre las extensiones de todos los archivos.
- De ninguna manera se debe ejecutar ningún archivo con doble extensión. Ya que puede ser un virus



- No contestar los correos no deseados o de remitentes desconocidos por que pueden dañar tu información.
- La aparición y desaparición de archivos, incluso temporales injustificadamente, lentitud del sistema, bloqueos o re-inicios continuos, desconexiones, inicialización o finalización de programas o procesos sin justificación, el teclado, mouse u otro periférico dejan de funcionar, puede ser evidencias de que nuestro equipo está siendo controlado por un hacker que ha ingresado a nuestro sistema con un **troyano/backdoor**.
- Borre constantemente las cookies, archivos temporales e historial.
- Últimamente se ha puesto de moda el llamado PHISHING, que consiste en que una supuesta entidad “seria” como un banco, le solicita al usuario que de clic en una liga para cambiar o actualizar datos personales o con el fin de enviar un supuesto regalo, esta práctica es sumamente peligrosa ya que al realizar la acción deseada, el usuario se expone a descargar un virus o programa malicioso o compartir sus datos personales a un hacker.

### **Sobre respaldos**

- Si tiene información importante en su computadora mantenga un respaldo fuera de la máquina como una unidad de CD y si es posible **LEJOS** del lugar donde usted trabaja.
- Haga al menos 3 respaldos por semana de sus datos más importantes, o hágase la siguiente pregunta: ¿en caso de un desastre a mi equipo o al servidor, con cuanto tiempo de retraso de información puedo trabajar?, si su respuesta es más de 1 mes, entonces no tiene mucho problema y puede realizar sus respaldos unas pocas veces por año.



## **Sobre claves de Acceso**

- El usuario acepta que cualquier recurso (correo electrónico, documentos en su computadora, sistemas de la Universidad) protegidos por contraseña, son responsabilidad directa del usuario, por lo que dicha contraseña de acceso queda bajo su resguardo.
- Por ningún motivo divulgue su contraseña de la red, a ninguna persona aunque sea empleado de la Universidad.
- Usar Claves de Acceso que no estén asociadas a datos comunes del usuario, tales como la fecha de nacimiento, apellidos, nombres de familiares, mascotas, etc.
- Cambiar la Clave de Acceso por lo menos 2 veces por año y que ésta contenga números y letras y al menos 6 caracteres.
- Las carpetas compartidas de la computadora, dentro de la Red, deberán estar debidamente protegidas mediante controles de acceso.
- No lleve registros ESCRITOS de las claves de acceso (como pequeñas notas o claves escritas en libretas, libros, etc.).

## **Sobre el correo electrónico**

- El medio oficial de comunicación de la Universidad de Celaya es el Correo electrónico, por favor cuide que su cuenta no se use para fines ajenos a la Universidad.
- No proporcione su dirección como parte de un cuestionario para registrarse en alguna página que no tenga que ver con su trabajo, ya que esto puede atraer propaganda indeseable.
- Queda estrictamente prohibido usar el correo electrónico de la Universidad para enviar “cadenas”, chistes, bromas o alertas de supuestos virus, ya que el enviar mensajes innecesarios a la gente, provoca una mala imagen a la Institución, si



tiene duda de alguna supuesta alerta, consulte a la Dirección de Informática donde le orientarán con gusto.

### **Sobre el control de Acceso**

El equipo de la Universidad de Celaya será utilizado para fines académicos y por la persona a la cual fue asignada, esto significa que ninguna persona ajena a la Institución podrá utilizar el equipo.

Si su computadora contiene datos confidenciales sobre la Universidad o sus alumnos, por favor evite que personal ajeno a su área maneje su computadora, (incluyendo familiares o amigos que no sean de la Institución).

Si su área maneja dinero, documentos oficiales o datos confidenciales, por favor cuide el acceso constantemente, y cuando abandone su computadora aunque sea por unos instantes, use la combinación de teclas CTRL-ALT –SUPR y Enter, (solo en Windows XP y Windows 2000) para bloquear su equipo temporalmente.

Si va a prestar su equipo a un alumno para hacer un trabajo académico o está realizando su servicio con usted, asegúrese de que no visite sitios prohibidos como páginas pornográficas (en el caso de los hombres) y páginas de “test “ de cualquier tipo (en el caso de las mujeres)

Si tiene una computadora portátil y va usted a salir de su lugar, es altamente recomendable que la asegure físicamente con un candado que use llave o combinación, ya que el robo de laptops es muy simple y difícil de detectar.

Si desea mayor orientación o desconoce algún término, por favor no dude en comunicarse al Centro de Cómputo, donde le atenderemos con mucho gusto.



## **Sanciones administrativas**

En caso de incurrir en la omisión de algún punto del reglamento de recursos informáticos o de realizar alguna práctica que exponga innecesariamente la información a su cargo o los recursos informáticos de la institución, se procederá a aplicar un acta administrativa o la separación de la universidad.

## ANEXO

### Conceptos.

**Recursos Informáticos:** Son todos los servicios proporcionados por una institución para las actividades diarias como por ejemplo el servicio de almacenamiento de archivos, archivos compartidos, servicio de impresión, servicios de red para programas residentes en un servidor, servicio de Internet e Intranet, etc.

**Virus:** Un virus informático es un programa de computadora que tiene la capacidad de causar daño y su característica más relevante es que puede replicarse a sí mismo y propagarse a otras computadoras.<sup>1</sup>

**Spyware:** Los programas espía o spyware son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas. Además pueden servir para enviar a los usuarios a sitios de internet que tienen la imagen corporativa de otros, con el objetivo de obtener información importante.<sup>2</sup>

**Troyano/backdoor:** Se denomina troyano (o caballo de Troya, traducción más fiel del inglés Trojan horse aunque no tan utilizada) a un programa malicioso capaz de alojarse en computadoras y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de recabar información y/o controlar remotamente la máquina.<sup>3</sup>

**Phishing:** Es un término utilizado en informática, se caracteriza por intentar adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria. El estafador, mejor conocido como phisher se hace pasar por una persona o empresa

---

<sup>1</sup> <http://www.monografias.com/trabajos13/virin/virin.shtml#intro>

<sup>2</sup> <http://es.wikipedia.org/wiki/Spyware>

<sup>3</sup> [http://es.wikipedia.org/wiki/Troyano\\_\(inform%C3%A1tica\)](http://es.wikipedia.org/wiki/Troyano_(inform%C3%A1tica))



de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico o algún sistema de mensajería instantánea.<sup>4</sup>

**Hacker:** (del inglés hack, recortar) es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con las Tecnologías de la Información y las Telecomunicaciones: programación, redes de comunicaciones, sistemas operativos, hardware de red/voz, etc.

**Antivirus:** Son programas cuya función es detectar y eliminar virus informáticos y otros programas maliciosos (a veces denominados malware).<sup>5</sup>

**Antispyware:** Son programas cuya función es detectar y eliminar spywares y otros programas maliciosos (a veces denominados malware).


**Parche de seguridad:** Es una actualización que se hace al sistema operativo, se encarga de corregir fallos del sistema que permiten a los virus entrar a la computadora.

**Cookie:** (en castellano, galleta) es un fragmento de información que se almacena en el disco duro del visitante de una página web a través de Internet, a petición del servidor de la página. Esta información puede ser luego recuperada por el servidor en posteriores visitas.<sup>6</sup>

## **Procedimientos.**

### *Descargar actualizaciones de Windows.*

Para instalar las actualizaciones del sistema operativo (Windows) cada vez que se requiera deberá seguir estos sencillos pasos:

1. En la parte inferior derecha de su pantalla junto al reloj de Windows usted verá este pequeño icono , deberá dar dos clicks sobre él.

---

<sup>4</sup> <http://es.wikipedia.org/wiki/Phishing>

<sup>5</sup> <http://es.wikipedia.org/wiki/Antivirus>

<sup>6</sup> <http://es.wikipedia.org/wiki/Cookie>



2. Posteriormente le aparecerá una ventana donde le indicará que actualizaciones se encuentran listas para instalar en su equipo, no debe preocuparse por escoger las actualizaciones, de un clic en el botón instalar.
3. Momentáneamente la ventana desaparecerá, pero las actualizaciones se estarán instalando mientras usted sigue trabajando.
4. Cuando terminen de instalarse las actualizaciones aparecerá la ventana nuevamente indicándole que se encuentran listas y posiblemente le pida reiniciar la computadora.

#### *Mostrar extensiones de los archivos.*

Para poder ver las extensiones verdaderas de los archivos siga estos sencillos pasos:

Windows Me, 2000 y XP

1. Abra "Mi PC" o el "Explorador de Windows"
2. Seleccione el menú "Herramientas" y de un click en "Opciones de carpetas".
3. Seleccione la pestaña "Ver".
4. DESMARQUE la opción "Ocultar las extensiones para tipos de archivo conocidos" o similar.
5. Para terminar de click en "Aplicar" y en "Aceptar".

#### *Eliminar las cookies y los archivos temporales de Internet.*

Para eliminar las cookies y los archivos temporales de Internet deberá seguir los siguientes pasos:

1. Primero entraremos al panel de control dando un clic en "Inicio" y posteriormente en "Panel de control".
2. Localice "Opciones de Internet" y de doble clic.
3. Estando en la ventana de "Opciones de Internet" localice el botón "Eliminar cookies...".



4. Por último para eliminar los archivos temporales de Internet de un clic en el botón “Eliminar archivos...” (este proceso puede tarda dependiendo de la cantidad de archivos temporales que tenga)