CSIRT-CV
Centre de Seguretat TIC de la Comunitat Valenciana

C/ Cardenal Benlloch, 69 Entlo – 46010 VALÈNCIA
Tel. 963985300 – Fax. 961961781

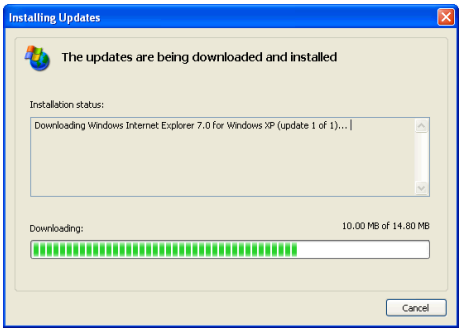
12 medidas básicas para la seguridad Informática

1. Antivirus: Un antivirus es un programa informático específicamente diseñado para detectar y eliminar virus. Instale uno en su ordenador y prográmelo para que revise todo su PC de forma periódica. Verifique también periódicamente que está activo (muchos virus detienen los programas antivirus y dejan a su ordenador indefenso frente a otros ataques). Además, cada día aparecen virus nuevos y para poder protegerse de ellos, su antivirus necesita conocer la "firma", es decir, las características de esos virus. Actualice su antivirus, bien manualmente bien de forma programada, frecuentemente y si fuera posible, a diario. http://www.csirtcv.gva.es/es/paginas/antivirus.html

2. Cortafuegos: Un cortafuegos o "firewall" es un software destinado a garantizar la seguridad en sus comunicaciones vía Internet al bloquear las entradas sin autorización a su ordenador y restringir la salida de información. Instale un software de este tipo si dispone de conexión permanente a Internet, por ejemplo mediante ADSL, y sobretodo si su dirección IP es fija.

3. Actualice frecuentemente sus aplicaciones con los "parches de seguridad": Las vulnerabilidades que se detectan en los programas informáticos más utilizados (navegadores de Internet, procesadores de texto, programas de correo, etc.) suelen ser, precisamente por su gran difusión, un blanco habitual de los creadores de virus. Para evitarlo, una vez detectada una vulnerabilidad, las compañías fabricantes de software

ponen rápidamente a disposición de sus clientes actualizaciones, llamadas “parches de seguridad”,en Internet.
http://www.csirtcv.gva.es/es/paginas/actualizadores-de-programas.html



4. Software Legal: Asegúrese que todo el software instalado en su ordenador proviene de una fuente conocida y segura. No instale copias de software pirata. Además de transgredir la Ley, pueden contener virus, *spyware* o archivos de sistema incompatibles con los de su ordenador, lo cual provocará inestabilidad en su equipo. Tampoco debe confiar en los archivos gratuitos que se descargan de sitios Web desconocidos, ya que son una potencial vía de propagación de virus. En cualquier caso, debe analizar con el antivirus cualquier fichero que se descargue de una página Web.

5. Precaución con el correo electrónico: Analice, antes de abrir, todos los correos electrónicos recibidos y sospeche de los mensajes no esperados, incluso si provienen de algún conocido. En caso de duda, llame por teléfono al remitente para asegurarse. Los virus utilizan la libreta de direcciones de la máquina infectada para enviar sus réplicas y tratar de infectar a otros usuarios haciéndoles creer que están recibiendo un mensaje de un conocido. En estos artículos se exponen los indicios para detectar si un correo es fraudulento: https://recursos.csirtcv.es/index.php?topic=102.0 y http://www.facebook.com/note.php?note_id=146070748776981

Todos aquellos correos que resulten sospechosos, si no conoce al remitente o presentan un “Asunto” clasificado como spam o suplantación, deben ir a la papelera disponible en su correo. De la misma forma, los archivos adjuntos provenientes de correos no confiables deben analizarse con el antivirus y tratarse con especial cuidado como se indica en los puntos 1 y 6. Cuando utilice la papelera, no olvide vaciarla a continuación.

6. Prudencia con los archivos: No descargue de Internet ni de adjuntos de correos electrónicos, ni distribuya o abra ficheros ejecutables, documentos, etc, no solicitados. Revise con su aplicación antivirus cada nuevo elemento que se trate de incorporar a su ordenador. No abra ningún archivo con doble extensión (como archivo.txt.vbs). En condiciones normales usted no tendría que necesitar nunca este tipo de archivos. Configure su sistema para que muestre las extensiones de todos los archivos. Utilice un usuario sin permisos de administrador para las tareas habituales de navegación y edición.

7. Administrador y usuario estándar: Normalmente los sistemas operativos diferencian entre usuarios Administradores y usuarios estándar con permisos limitados. Disponga de un usuario Administrador y uno estándar (ambos con contraseña) y utilice un usuario sin permisos de administrador para las tareas habituales de navegación y edición. Si necesita los privilegios de administrador para realizar alguna tarea como instalar o desinstalar aplicaciones, el propio sistema pedirá la contraseña del administrador. Muchos de los problemas de seguridad son debidos al uso de usuarios administradores. https://recursos.csirtcv.es/index.php?topic=133.

8. Contraseñas seguras: Utilice contraseñas diferente para cada acceso importante (cuenta del banco online, correo electrónico, redes sociales, administrador del sistema, etc). Puede usar una misma contraseña para los accesos menos críticos. Para una buena creación y memorización de las contraseñas consulte los artículos publicados en https://recursos.csirtcv.es/index.php?topic=97.0.

8. Navegación segura: Realice una navegación segura. Tenga en cuenta que, igual que en la vida real, no todo es lo que parece ser. Internet se ha convertido en una herramienta muy potente de información y comunicación, pero al mismo tiempo sirve como terreno para una nueva forma de delincuencia que se ampara en la confianza y el desconocimiento de los usuarios. Deben seguirse unas normas básicas, entre las que se encuentran la mayoría de las medidas ya expuestas: Aplicaciones actualizadas, control en la cesión de datos personales, prudencia con la publicidad, realizar compras online solo a través de medios seguros, etc.

Puede aprender de una forma sencilla todas estas normas y otros conceptos fundamentales de seguridad en la Web en nuestro curso “Navegación Segura” (http://www.csirtcv.gva.es/es/formacion/navegaci%C3%B3n-segura.html) impartido por **CSIRT-cv**.

9. Copias de Seguridad: Realice de forma periódica copias de seguridad de su información más valiosa. En caso de sufrir un ataque de un virus o una intrusión, las secuelas serán mucho menores si puede restaurar fácilmente sus datos.

10. Ayude a los demás: No distribuya indiscriminadamente bromas de virus, alarmas, o cartas en cadena. Infórmese de la veracidad de los mensajes recibidos y ayude a los demás colaborando en la detención de su distribución. No conteste a los mensajes SPAM (publicidad no deseada) ya que al hacerlo confirmará su dirección. Una serie de consejos para combatir el SPAM y demás “correos cadena” pueden encontrarse en https://recursos.csirtcv.es/index.php?topic=117.0

10. Manténgase Informado: Manténgase periódicamente informado de las novedades de seguridad informática a través de los boletines de las compañías fabricantes de software así como de los servicios de información y boletines del **Centro de Seguridad TIC de la Comunitat Valenciana** sobre diversa temática de seguridad. Si usted sabe cómo actuar ante una situación de riesgo, podrá minimizar al máximo las posibles pérdidas. Suscríbase a nuestros servicios gratuitos de información periódica mediante correo electrónico y visite regularmente nuestro sitio Web. Cualquier consulta nos la puede hacer llegar a través de los foros:, a través de las redes sociales Facebook y Twitter o a través de nuestro formulario de contacto en el portal.

Recordar que **CSIRT-cv** ofrece cursos gratuitos online especializados en materia de seguridad y le invitamos también a seguir nuestras campañas de concienciación que desarrollamos en las redes sociales y a participar activamente en las mismas.

Web de CSIRT-cv : http://www.csirtcv.gva.es
Foros de CSIRT-cv: https://recursos.csirtcv.es
Subscripción a boletines: http://www.csirtcv.gva.es/es/paginas/suscribirse-la-lista-boletines-csirt-cv.html
Formulario de contacto: http://www.csirtcv.gva.es/es/formulario/contacto-y-suscripciones.html
Página de CSIRT-cv en Facebook: http://www.facebook.com/Csirtcv
Perfil de CSIRT-cv en Twitter: @csirtcv
Oferta formativa: http://www.csirtcv.gva.es/es/paginas/formaci%C3%B3n.html
Campañas de concienciación: http://www.csirtcv.gva.es/es/paginas/campa%C3%B1-de-concienciaci%C3%B3n.html