Concienciación en Ciberseguridad
en Centros Educativos de la Comunidad Valenciana

Para dar respuesta a las ciberamenazas que acechan a la sociedad valenciana, **CSIRT-CV** ha diseñado el **Plan Valenciano de Capacitación (PVC)**, el cual persigue aumentar tanto el nivel de madurez en ciberseguridad, como la confianza en el uso de la tecnología de ciudadanos, empresas y el propio personal de **GVA**.

Este plan centra gran parte de sus acciones en la formación y concienciación a los colectivos con mayor probabilidad de ser víctimas de amenazas online, como es el caso de los adolescentes.

1. **El objetivo** que se persigue es convertir a los menores valencianos en Human Firewalls, es decir, personas capaces de identificar las amenazas a las que están expuestos y poder responder de forma adecuada ante las mismas.

2. **No olvidemos** que nuestros adolescentes son ***nativos digitales*** y eso hace que ignoren o infravaloren los peligros a los que están expuestos, creyéndose auténticos ***expertos*** en materia de ciberseguridad.

   Esta falta de concienciación sumada a la falsa sensación de seguridad que conlleva el hecho de que en la red no se ven los riesgos tanto como en el mundo físico, sumado al anonimato que brinda Internet, nos lleva a ver la necesidad de poner en marcha acciones específicas para ellos.

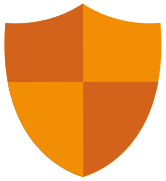
3. **Como parte de esta capacitación** hemos puesto en marcha en todos los centros educativos públicos, concertados y privados de la Comunidad Valenciana, unas jornadas sobre ciberseguridad para todos los alumnos de 2º de la E.S.O, sus profesores y sus padres y madres.

El objetivo fundamental es que estas jornadas se conviertan en una herramienta para introducir la ciberseguridad como un aspecto clave a tratar en el resto del curso.

Las sesiones podrán ejecutarse de forma presencial u online, aunque siempre es aconsejable que se realicen presencialmente debido a su calado entre los alumnos. Estas acciones se enfocan principalmente en los alumnos que cursen 2º de la ESO, pudiendo, siempre que las circunstancias lo permitan, ampliar a 1º de la ESO. **La planificación de estas jornadas de ciberseguridad está dividida en 4 actividades distintas a ejecutar durante 2 días seguidos.**

Sesión de concienciación a alumnos que se llevará a cabo en la mañana de la primera jornada, con una duración de 75 minutos. Dependiendo del número total de alumnos a formar, se puede repetir la actividad hasta un máximo de 2 veces en la misma mañana. En ella, se realizarán unas píldoras formativas con dispositivos que ellos están acostumbrados a utilizar habitualmente y en las que se representarán los principales peligros a los que se enfrentan los jóvenes, exponiéndoles a “ataques reales” por parte de personal especializado.

Sesión de concienciación a madres y padres que se llevará a cabo la tarde de la primera jornada, con una duración de 90 minutos. En ella se tratarán temas como: principales herramientas y aplicaciones utilizadas, comportamientos típicos de menores, amenazas más importantes en las que se ven envueltos sus hijos y recursos de ayuda.



Taller de Seguridad a alumnos que se llevará a cabo durante la mañana de la segunda jornada, con una hora de duración. Este taller tiene un enfoque eminentemente práctico en el que se enseñará a los alumnos a con igurar los dispositivos y sus identidades digitales de forma correcta, además de cómo usar gestores de contraseñas y otras técnicas que les resultarán muy útiles en su día a día. Dependiendo del número total de alumnos a formar, se puede repetir el taller hasta un máximo de 3 veces de manera consecutiva durante la misma mañana.

Sesión de formación a los docentes que se llevará a cabo la tarde de la segunda jornada, con una duración de 120 minutos. El objetivo es proveer a los profesores de los conocimientos necesarios en ciberseguridad para afrontar las situaciones del día a día en las que se ven envueltos con sus alumnos. Dicha sesión tiene un enfoque totalmente pedagógico y en ella se tratarán temas como: proteger la identidad digital, sus dispositivos móviles, sus conexiones…