

Actividad formativa	Seguridad informática, Equipos, Internet y Redes Sociales
----------------------------	--

Fechas de Ejecución	Del 12 al 27 de marzo de 2020
Lugar de Impartición	Online
Destinatarios	PAS
Duración en Horas	15 horas (0,5 ECTS)
Total Participantes	---
Nº de Ediciones	1
Objetivos	<ul style="list-style-type: none"> ✓ Saber en qué consiste la seguridad en red y su papel fundamental en las TIC. ✓ Identificar los peligros que puede encerrar la red, especialmente a las personas más vulnerables. ✓ Conocer los términos más relacionados con la seguridad en red. ✓ Conocer la importancia de mantener protegido nuestras redes y equipos a través de herramientas de gestión de virus. ✓ Conocer las principales herramientas de control de virus y ataques informáticos en la red. ✓ Tomar conciencia de la necesidad de tomar precauciones a la hora de navegar por Internet. ✓ Saber lo que implica la intrusión de malware en los equipos y conocer la terminología asociada. ✓ Identificar los recursos que nos pueden ayudar a contrarrestar los ataques de malwares. ✓ Saber qué son las cookies y en qué consiste su uso adecuado e inadecuado.
Contenidos	<p>MOD. 1 “¿QUÉ ES LA SEGURIDAD EN LA RED?”</p> <p>1. ¿Qué es la seguridad en la red?</p> <p>1.1. Introducción: Seguridad en la red</p> <p>1.2. La importancia de una red segura</p> <p>1.3. Seguridad informática y seguridad de la información: suena parecido, pero no es lo mismo</p> <p>1.4. Los términos más usados en seguridad informática</p> <p>1.5. Control parental y el/la menor en la red</p>



	<p>1.6. Contraseñas eficaces. Transacciones seguras</p> <p>MOD. 2 " VIRUS Y ANTIVIRUS INFORMÁTICOS"</p> <p>1. ¿Qué es un virus informático? Los más peligrosos y sus efectos</p> <p>1.1. La importancia de actualizar la base de datos de virus</p> <p>2. ¿Qué es un antivirus? Antivirus online y residentes. Otros tipos de antivirus</p> <p>2.1. Opciones "online"</p> <p>3. Cortafuegos o firewalls</p> <p>3.1. Clases de cortafuegos</p> <p>3.2. Arquitecturas de cortafuegos</p> <p>4. Precauciones a la hora de navegar por internet</p> <p>5. Precauciones en la descarga de archivos</p> <p>MOD. 3 " MALWARE Y COOKIES"</p> <p>1. ¿Qué son los malwares? Tipos de malwares</p> <p>2. Infección y su propagación</p> <p>2.1. Vías de propagación de la infección</p> <p>3. Daños que pueden provocar</p> <p>4. Prevención de los malwares. Protección activa y pasiva</p> <p>4.1. MalwareBytes Anti-Malware.</p> <p>4.2. Microsoft Malicious Software Removal Tool.</p> <p>4.3. CCleaner</p> <p>4.4. Anti-malware on-line</p> <p>5. ¿Qué son las cookies? Ventajas e inconvenientes</p> <p>5.1. Robo de cookies</p> <p>5.2. Falsificación de cookies</p> <p>5.3. Cookies entre sitios (cross-site cooking)</p> <p>6. Mitos sobre las cookies</p>
Directora	Pilar Rubio López
Organización	Avancc-e

