

ssFORMACIO: Seguridad informática

Curso que permite conocer los conceptos básicos sobre la seguridad y privacidad informática, centrándose en los aspectos esenciales que debe conocer todo usuario de un sistema informático para protegerse de las distintas amenazas y peligros que se puede encontrar. A lo largo del curso se analizan diferentes áreas (contraseñas, seguridad en el acceso a redes, virus, cortafuegos, navegación segura por Internet, correo electrónico, redes sociales, uso de ordenadores por menores, etc.), describiendo las amenazas y posibles riesgos en cada una de ellas y ofreciendo consejos y recomendaciones para mantener la seguridad en el trabajo diario con ordenadores.

Seguridad informática

Describe conceptos básicos sobre la seguridad y privacidad informática, centrándose en los aspectos esenciales que debe conocer todo usuario de un sistema informático para protegerse de las distintas amenazas y peligros que se puede encontrar. Está estructurado en diferentes áreas principales (seguridad en el PC, virus y cortafuegos, navegación por Internet, correo electrónico y redes sociales), además de otros aspectos también importantes, describiendo las amenazas y posibles riesgos en cada una de ellas y ofreciendo consejos y recomendaciones para mantener la seguridad en el trabajo diario con ordenadores.

Seguridad en el PC

Se explican distintos conceptos básicos de seguridad en el uso cotidiano de un ordenador o PC: utilización de usuarios estándar y administradores para aumentar la seguridad, uso de ordenadores compartidos o públicos, utilización de contraseñas seguras para los programas y servicios de Internet, acceso a redes o a Internet, uso de redes P2P y descarga de programas. Contenido: 1. Introducción. 2. Usuarios. 3. Ordenadores compartidos. 4. Contraseñas. 5. Acceso a redes. 6. Redes P2P y descarga de programas.

Virus, cortafuegos y actualizaciones

Se explica lo que son los virus informáticos y otro tipo de malware, sus vías de contagio y cómo evitarlos, describiendo la utilización de programas antivirus y cortafuegos para proteger el sistema informático. También se explica la importancia de las actualizaciones del software para mantener la seguridad del sistema informático. Contenido: 1. ¿Qué son los virus? 2. Vías de contagio. 3. Antivirus. 4. Cortafuegos. 5. Actualizaciones.

Navegación por Internet

Se describen aspectos a tener en cuenta por parte de los usuarios para navegar por Internet de una forma segura: ventanas emergentes, cookies, navegación privada o modo incógnito para proteger la privacidad, protocolo seguro (https) y certificados digitales para una navegación segura, acceso a bancos online o realización de compras a través de Internet. Se analiza el uso de los ordenadores e Internet por parte de menores y adolescentes, viendo distintos peligros o amenazas que podemos encontrar, como el ciberacoso, el sexting o el grooming, explicando cómo evitarlos y saber reaccionar ante ellos. Contenido: 1. Introducción. 2. Navegación privada. 3. Páginas seguras. 4. Operaciones bancarias. 5. Compras. 6. Menores en Internet. 7. Ciberacoso y sexting.

El correo electrónico

Uso correcto y con seguridad del servicio de correo electrónico o e-mail, para evitar los principales problemas o peligros que nos podemos encontrar en este aspecto, como el spam, phishing, hoax, timos o fraudes. También se describen características de la mensajería instantánea y de los chats para utilizarlos de manera segura. Contenido: 1. Introducción. 2. Seguridad y confidencialidad. 3. Phishing. 4. Spam y timos. 5. Mensajería instantánea y chats.

Redes sociales

Descripción de cómo podemos utilizar de forma segura de las redes sociales que existen en Internet, para evitar posibles problemas de seguridad y privacidad. También se explican aspectos específicos relacionados con el uso de los móviles y smartphones (teléfonos inteligentes). Finalmente, se ve la necesidad de la realización de copias de seguridad y se indican consejos y recomendaciones a modo de resumen. Contenido: 1. Introducción. 2. Privacidad y confidencialidad. 3. Fotografías y videos. 4. Móviles. 5. Consideraciones finales.