Competencias digitales. Nivel avanzado.

Sku: PA1367

Horas: 5

Formato: HTML

OBJETIVOS

- Valorar la necesidad de la gestión de la seguridad personal y en las organizaciones.
- Conocer las principales amenazas a los sistemas de información.
- Identificar las principales herramientas de seguridad y su aplicación en cada caso.

CONTENIDOS

- **Unidad 1. Introducción a la ciberseguridad (conceptos y términos avanzados)**
- **Unidad 2. La información: confidencialidad, integridad y disponibilidad**
- **Unidad 3. Tipos de actores: estados, hacktivismo, ciberdelincuencia, ciberterrorismo**
- **Unidad 4. Organizaciones públicas con competencias en materia de ciberseguridad**
- **Unidad 5. Tipos de amenazas: Ransomware, Phishing, Smishing, Vishing, entre otras**
- **Unidad 6. Desinformación (fake news)**
- **Unidad 7. Amenazas específicas en el entorno del teletrabajo**
- **Unidad 8. Qué impacto puede tener un ciberincidente**
- **Unidad 9. Buenas prácticas para los empleados: uso seguro de un PC y un móvil en el entorno personal. Uso seguro de un puesto de trabajo y un móvil corporativo**
- **Unidad 10. Copias de seguridad**
- **Unidad 11. Gestión de contraseñas**
- **Unidad 12. Teletrabajo de forma segura**
- **Unidad 13. Navegación responsable, uso seguro del correo electrónico y de las redes sociales**
  - Funcionamiento
- **Unidad 14. Uso seguro de plataformas de colaboración en la nube (en el caso del Ayuntamiento, Office 365)**

- **Unidad 15. Qué hacer en caso de un ciberincidente**