



# Diploma

**CENTRO CULTURAL Y DEPORTIVO TAJAMAR SA**, como entidad beneficiaria, otorga a

**GONZALO CABEZAS NUÑEZ**

DNI [REDACTED]

el presente diploma por haber superado con evaluación positiva la acción formativa

## **IFCT0024 CIBERSEGURIDAD PARA USUARIOS**

con formación presencial impartida desde el 28/10/2025 hasta el 06/11/2025, con una duración total de 10 horas, en el marco del expediente F241778AA, código de acción formativa 28, código de grupo 1. Formación impartida al amparo del Sistema de Formación Profesional para el Empleo en el marco de la Resolución de 6 de agosto de 2024, del Servicio Público de Empleo Estatal, por la que se aprueba la convocatoria para la concesión de subvenciones públicas para la ejecución de programas de formación de ámbito estatal, dirigidos prioritariamente a las personas ocupadas.

Y para que así conste, se expide este certificado en MADRID, a 06 de noviembre de 2025.

*XAVIER MUNDET*

## Contenidos de la acción formativa

### MÓDULO DE FORMACIÓN 1: CIBERSEGURIDAD PARA USUARIOS

#### 1. APROXIMACIÓN A LA SEGURIDAD EN SISTEMAS DE INFORMACIÓN

#### 2. ASIMILACIÓN DE CONCEPTOS DE SEGURIDAD EN LOS SISTEMAS

##### 2.1. Clasificación de las medidas de seguridad

##### 2.2. Conocimiento acerca de los requerimientos de seguridad en los sistemas de información

##### 2.3. Identificación de principales características

##### 2.4. Confidencialidad

##### 2.5. Gestión de la integridad

##### 2.6. Comprensión de la disponibilidad

##### 2.7. Identificación de otras características

##### 2.8. Identificación de tipos de ataques

#### 3. CONOCIMIENTO DEL ÁMBITO DE LA CIBERSEGURIDAD PARA LOS

#### USUARIOS

##### 3.1. Comprensión del concepto de ciberseguridad

##### 3.2. Identificación de amenazas más frecuentes a los sistemas de información

##### 3.3. Utilización de tecnologías de seguridad más habituales

##### 3.4. Gestión de la seguridad informática

#### 4. IDENTIFICACIÓN DE SOFTWARES DAÑINOS

##### 4.1. Asimilación de conceptos sobre software dañino

##### 4.2. Clasificación del software dañino

##### 4.3. Identificación de amenazas persistentes y avanzadas

##### 4.4. Prevención sobre la ingeniería social y redes sociales

#### 5. GESTIÓN DE SEGURIDAD EN REDES INALÁMBRICAS

#### 6. APLICACIÓN DE HERRAMIENTAS DE SEGURIDAD

##### 6.1. Aplicación de medidas de protección

##### 6.2. Control de acceso de los usuarios al sistema operativo

##### 6.3. Gestión del permiso de los usuarios

##### 6.4. Gestión del registro de usuarios

##### 6.5. Autenticación de usuarios

##### 6.6. Gestión segura de comunicaciones, carpetas y otros recursos compartidos

##### 6.7. Gestión de carpetas compartidas en la red

##### 6.8. Identificación de tipos de accesos a carpetas compartidas

##### 6.9. Procedimiento para compartir impresoras

##### 6.10. Protección frente a código malicioso

##### 6.11. Configuración del antivirus

##### 6.12. Configuración del cortafuegos (firewall)

##### 6.13. Aplicación del antimalware