Diploma

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

PABLO BARTOLOMÉ GALLARDO
DNI 44247202D

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

IFCT89 SEGURIDAD EN INTERNET Y DISPOSITIVOS MÓVILES

con formación online tutorizada desde el 02/06/2023 hasta el 15/06/2023, con una duración total de 36 horas, en el marco del expediente F211494AA, código de acción formativa 29, código de grupo 5. Formación impartida al amparo del Sistema de Formación Profesional para el Empleo en el marco de la "Resolución 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, para la adquisición y mejora de competencias profesionales relacionadas con los cambios tecnológicos y la transformación digital, dirigidos prioritariamente a las personas ocupadas, en el marco del Plan de Recuperación, Transformación y Resiliencia".

Y para que así conste, se expide este certificado en MADRID, a 15 de junio de 2023.

Contenidos de la acción formativa

MÓDULO 1. INTRODUCCIÓN.
1. Comprensión de la ciberseguridad.
2. Los riesgos, tipos y alcance.
3. Vectores de ataque tipos e impacto.
4. Medidas de prevención y actuación ante posibles ataques.
5. Revisión del contexto futuro de la ciberseguridad.
6. Actividades de autoevaluación para fortalecer los conocimientos adquiridos por el alumno.
MÓDULO 2. CIBERSEGURIDAD. CONCEPTOS BÁSICOS.
1. ¿Qué es la Ciberseguridad?
2. ¿Por qué aplicar la ciberseguridad?
3. ¿Cómo impacta la ciberseguridad en Internet y los dispositivos móviles?
3.1. Aplicaciones y herramientas.
3.2. Detección previa.
3.3. Seguridad.
4. Actividades de autoevaluación para fortalecer los conocimientos adquiridos por el alumno.
MÓDULO 3. RIESGOS, TIPOS Y VECTORES DE ATAQUE.
1. Qué es un riesgo y los elementos de un sistema susceptibles de ser protegidos.
2. Tipos de riesgos.
3. Conceptos básicos de vectores de ataque.
4. Tipos de vectores de ataque (Phishing, malware, social engineering y medidas de actuación).
5. Vectores de ataque: medidas de prevención y actuación generales.
6. Vectores de ataque: medidas de prevención y generales en la gestión de redes conectadas o no a la Red: Cortafuegos, segmentación, monitorización, detección, registro y encriptación.
6.1. Cortafuegos (Firewall).
6.2. Segmentación.
6.3. Monitorización y detección.
6.4. Registro.
6.5. Encriptación.
7. Vectores de ataque: medidas de actuación específicas para los dispositivos móviles.
8. Actividades de autoevaluación para fortalecer los conocimientos adquiridos por el alumno.
MÓDULO 4. MPLICACIONES EN LA CIBERSEGURIDAD DE LA EVOLUCIÓN DE LAS AMENAZAS ACTUALES Y DE LA ADOPCIÓN DE NUEVAS TECNOLOGÍAS
1. Gestión de ingentes cantidades de datos en sistemas cada vez más complejos.
2. La Inteligencia Artificial (IA) será un componente central de todos los sistemas de ciberseguridad.
3. La industria de la ciberseguridad se centrará en las amenazas de la guerra cibernética.
4. Habrá más crackers con los que lidiar.
5. Desarrollo del talento en ciberseguridad se vuelve esencial.
6. La tecnología heredada seguirá siendo un problema.
7. Internet de las cosas (IoT).
8. Supercomputación (Computación cuántica).
9. Mayor uso de las redes autoadaptables.
10. Generalización del uso de los Gestores de Seguridad para el Acceso a la Nube (Cloud Access Security Broker - CASB).
11. Análisis de amenazas internas mediante sistemas UEBA (User and Entity Behavior Analytics).
12. Implantación generalizada de autenticación multifactor física en entornos críticos.
13. El Coronavirus (COVID-19) lo ha cambiado todo (Teletrabajo y la ciberresiliencia).
14. Actividades de autoevaluación para fortalecer los conocimientos adquiridos por el alumno.