A·30 Taller tecnológico de ciberseguridad

01

Curso escolar
1º Bachillerato
2º Bachillerato

Fechas
Septiembre 2026 - Mayo 2027

Áreas de aprendizaje
Digitalización
Orientación profesional
Tecnología

Formato
Taller de empresa

Idioma
Castellano

Alcance geográfico
Álava, Bizkaia, Gipuzkoa

Entidad que imparte la actividad
42 Urduliz Bizkaia

El taller tecnológico de ciberseguridad tiene el objetivo de sensibilizar al alumnado de 1º y 2º de Bachillerato de los peligros de navegar en las redes. Mediante la resolución de un desafío propuesto, ofrece la posibilidad de adquirir conocimientos básicos en ciberseguridad y desarrollar competencias transversales como el trabajo en equipo, el aprender a aprender, la resolución de problemas o la gestión de la frustración. A través de un reto, el alumnado tratará de capturar a unos cibercriminales, mientras trabajan conceptos como: la búsqueda de información en fuentes abiertas (OSINT), la exploración de metadatos, la criptografía, comprobar si la información procede de fuentes fiables (checksum MD5), ocultar información dentro de otros mensajes (esteganografía), etc.

Descriptores STEM

STEM 1	STEM 2	STEM 3
STEM 4	STEM 6	

Recursos

Recursos materiales
La empresa facilitará sus instalaciones y equipamiento tecnológico para la realización del taller.

Recursos económicos
Desplazamiento a la empresa (coste subvencionado para centros de Bizkaia por la Diputación Foral).

Más información
42urduliz.com

A·30 Taller tecnológico de ciberseguridad

DESARROLLO

Fase: ejecución de la actividad

La actividad es una experiencia presencial en el campus de 42 Urduliz Bizkaia, que tiene una duración de 3 horas y consta de:

- Primera parte de contexto sobre la ciberseguridad y las diferentes vulnerabilidades.
- La segunda parte es un taller práctico en el que las personas participantes tienen el reto de capturar a unos cibercriminales. A través de una serie de pistas que han ido dejando, será necesario que resuelvan la trama y para ello deberán: buscar información en fuentes abiertas (OSINT), explorar metadatos, descubrir la criptografía, comprobar si la información procede de fuentes fiables (checksum MD5) y descifrar información dentro de otros mensajes (esteganografía).
- Durante el taller pondrán en práctica la metodología 42 (sin profesores, sin libros, de manera colaborativa y gamificada).
- En la última parte se realizará una puesta en común de aprendizajes y conclusiones.

Además, estudiantes del campus 42 Urduliz Bizkaia que trabajan en el ámbito tecnológico ofrecerán una charla sobre sus profesiones con el objetivo de inspirar vocaciones en el sector digital, haciendo hincapié en la importancia de tener en cuenta los sesgos y la perspectiva de género.

Esta experiencia es una iniciativa de 42 Urduliz Bizkaia, el campus de programación impulsado por Fundación Telefónica y Diputación Foral de Bizkaia. La metodología de aprendizaje que se utiliza es la “metodología 42”, que está basada en el aprendizaje entre pares, gamificada y a través de proyectos.

Fase: integración en el aula

42 Urduliz Bizkaia facilitará recursos didácticos de apoyo para seguir trabajando este tipo de contenidos en el aula.

A·30 Taller tecnológico de ciberseguridad

VINCULACIÓN CURRICULAR

Aprendizajes curriculares que se trabajan en la actividad:

Digitalización

- Aportaciones y peligros de las tecnologías: ciberseguridad, la protección de datos, medidas preventivas y herramientas/ mecanismos de defensa.
- Búsqueda y tratamiento de la información: motores de búsqueda, búsqueda avanzada (operadores booleanos, filtros, etc.) y evaluación de la información (fuentes fiables, fake news, etc.).
- Análisis de datos y extracción de información.
- Pensamiento crítico: emprendimiento, resiliencia, perseverancia y creatividad para abordar la resolución de problemas desde una perspectiva interdisciplinar.
- Trabajo en equipo: comunicación efectiva (roles, responsabilidades, etc.) y colaboración (liderazgo, resolución de conflictos, etc.).

Tecnología

- Redes informáticas: conceptos básicos, funcionamiento de Internet y seguridad en redes (firewalls, VPN, ataques comunes, etc.).
- Seguridad en sistemas operativos: antivirus, antimalware, hardening, etc.
- Criptografía: conceptos básicos (algoritmos de cifrado, claves, hashes, etc.), tipos de cifrado (simétrico, asimétrico, hash, etc.) y criptografía en la vida diaria (https, HTTPS, PGP, etc.).
- Esteganografía: conceptos básicos (técnicas de ocultación de información, esteganografía digital, etc), tipos de esteganografía (imágenes, audio, vídeo, etc.) y detección de esteganografía.