A·16 Desafío de ciberseguridad, ¿quieres convertirte en un guardián digital?

01

Curso escolar
3º ESO
4º ESO

Fechas
Febrero - Mayo 2027

Áreas de aprendizaje
Orientación profesional
Tecnología

Formato
Taller de empresa

Idioma
Castellano

Alcance geográfico
Álava, Bizkaia, Gipuzkoa

Entidad que imparte la actividad
Centro de Estudios Mikeldi

A través de un software de máquina virtual, se ofrece la oportunidad al alumnado de asistir en sus instalaciones a un taller tecnológico.

El centro les planteará un reto en el que deberán afrontar y frenar un ciberataque sufrido en sus equipos informáticos y hackeo de las contraseñas del inicio de sesión de dichos dispositivos.

Descriptores STEM

STEM 1 | STEM 4 | STEM 6

Recursos

Recursos materiales
El Centro de Estudios Mikeldi pone a la disposición del alumnado aulas dotadas con el equipamiento informático y el software necesarios.

Recursos económicos
Desplazamiento a la empresa.

Más información
mikeldi.com

A·16 Desafío de ciberseguridad, ¿quieres convertirte en un guardián digital?

DESARROLLO

Fase: ejecución de la actividad

El Centro de Estudios Mikeldi inicia esta actividad, lanzando un reto que deberán solucionar en 2 horas y media, con la ayuda de una persona experta del centro de formación profesional.

Con el objetivo de trabajar pautas de seguridad activa y pasiva, a través de un software de máquina virtual simularán un ciberataque en los equipos informáticos de la sala donde tiene lugar la actividad, donde además han hackeado las contraseñas del inicio de sesión de dichos ordenadores.

A lo largo de esta actividad, el alumnado tendrá la posibilidad de saber cómo dar solución real al problema, gracias a las explicaciones que recibirán como guía. Así mismo, en una segunda parte conocerán mecanismos y herramientas específicas para detectar y prevenir algunas de las amenazas más comunes en medios digitales. Para concluir el taller, desde la perspectiva de la orientación profesional y teniendo muy presente la perspectiva de género, el centro realizará una presentación de media hora sobre los estudios que en este se ofrecen, haciendo hincapié en las vocaciones científico-tecnológicas, la demanda de este tipo de personas profesionales y la necesidad de fomentar la presencia de mujeres en este tipo de ciclos.

Fase: integración en el aula

Con el objetivo de seguir trabajando en el aula el uso seguro y responsable de las tecnologías, dicha actividad será integrada en la programación de aula a través del área de aprendizaje de tecnología y sesiones de tutoría

El alumnado deberá reflexionar sobre los contenidos aprendidos en el taller y crear una infografía conjunta sobre buenas prácticas a tener en cuenta para proteger sus datos digitalmente.

A·16 Desafío de ciberseguridad, ¿quieres convertirte en un guardián digital?

VINCULACIÓN CURRICULAR

Aprendizajes curriculares que se trabajan en la actividad:

Tecnología

- **Seguridad activa:** medidas que previenen e intentan evitar los daños en los sistemas informáticos (cómo mejorar el acceso al ordenador mediante contraseñas seguras y recursos útiles, uso y funcionamiento de una base de datos con Keepass, cifrar una partición de Windows usando un programa gratuito de código abierto DiskCryptor para proteger la confidencialidad de los datos almacenados en un volumen del equipo, etc.).
- **Seguridad pasiva:** copias de seguridad de los datos en un lugar diferente al original, cuya finalidad es recuperar los datos en caso de desastre (incendios, inundaciones, robos, etc). Usaremos el software gratuito Uranium Backup (copias totales, incrementales y diferenciales).
- **Cómo proteger los dispositivos** de uso habitual configurando y actualizando, contraseñas, sistemas operativos y antivirus de forma periódica (actualizaciones, antivirus online gratuitos). Usaremos un software gratuito como CCleaner para mantener el sistema operativo optimizado para un funcionamiento más rápido.
- **Tipos de software y licencias existentes.** El software utilizado será software gratuito (licencia freeware) o de uso de tiempo limitado (el caso de Windows) licencia Shareware.
- **Seguridad y privacidad:** medidas preventivas y correctivas para hacer frente a riesgos, amenazas y ataques a dispositivos de uso común. Se usará el programa Malwarebytes en su versión gratuita para saber si estamos infectados de software malicioso y configuraremos alguna regla de entrada y salida en el cortafuegos de Windows para evitar ser atacados. A modo de ejemplo, haremos una prueba con un programa Keylogger para capturar las pulsaciones de un usuario sin que lo sepa y cómo prevenir esto.