CIBERSEGURIDAD EN AULAS CONECTADAS: PROTECCIÓN DE IOT EN CENTROS EDUCATIVOS.

B.1.1- Características de la actuación.

La aplicación de la tecnología con IoT proporciona a los profesionales de la educación nuevas herramientas para optimizar el trabajo en clase, mejorar la eficiencia del proceso de aprendizaje, conectar.

Al principio, los sensores y actuadores no tenían conexión a redes, con la aparición del IoT a medida que ha ido creciendo e incorporando las tecnologías y la automatización, ha ido evolucionado y hoy se encuentran hiperconectadas en muchos casos a IT, es por ello que también se ha incrementado el riesgo de que estas redes puedan ser atacadas. La conectividad de los dispositivos IoT ha incrementado la exposición de los dispositivos en Internet, lo que los ha vuelto más vulnerables y fáciles de explotar.

Además, tampoco tienen soluciones triviales de parcheado o aislamiento por las características especiales del entorno, La ciberseguridad en estos entornos aúna diferentes principios de seguridad de los entornos OT y principios de seguridad de los entornos IT, con el fin de proteger los distintos activos de un centro educativo, así como las redes, los procesos existentes, los datos y la información.

Este proyecto pretende dar soluciones seguras a las futuras instalaciones de IoT en los centros educativos de todo el territorio nacional en caso que se quiera realizar una instalación de cualquier dispositivo que ayude en el día a día a mejorar el entorno educativo de docentes y alumnos.

Características Principales:

Este proyecto nace con el objetivo de fortalecer la seguridad digital en entornos educativos mediante la implementación de soluciones de ciberseguridad aplicadas a dispositivos IoT. A continuación, se detallan sus principales características:

1. **Colaboraciones intercentros a nivel nacional**
   El proyecto ha sido desarrollado de forma conjunta por tres centros educativos ubicados en diferentes puntos del territorio español: CIPFP Mislata de Valencia (Comunidad Valenciana), CIFP Rodolfo Ucha Piñeiro de Ferrol - La Coruña (Galicia) y el Institut Montsià de Amposta – Tarragona (Cataluña). Esta colaboración ha permitido enriquecer el enfoque del proyecto, compartir buenas prácticas y adaptar las soluciones a contextos educativos diversos, fomentando así una visión más amplia y representativa del panorama educativo nacional.

2. **Enfoque práctico y orientado a la acción**
   Una de las señas de identidad del proyecto es su carácter eminentemente práctico. Los alumnos han trabajado con dispositivos IoT reales (sensores, cámaras, actuadores, etc.) en entornos simulados y reales, aplicando medidas de ciberseguridad para proteger redes y datos. Esta metodología activa ha favorecido un aprendizaje significativo y ha potenciado el desarrollo de competencias técnicas y transversales.

3. **Producción de materiales didácticos y retos formativos**
   Como resultado del trabajo realizado, se ha generado un conjunto de materiales de prácticas, guías técnicas y retos de ciberseguridad diseñados específicamente para el entorno educativo. Estos recursos están orientados a facilitar la replicabilidad del

proyecto en otros centros y a fomentar el autoaprendizaje y la experimentación entre el alumnado.

4. **Difusión abierta y accesible**
   Con el fin de maximizar el impacto del proyecto, todos los materiales generados estarán disponibles en una plataforma web de acceso público. Esta decisión responde a un compromiso con la educación abierta y colaborativa, permitiendo que otros docentes, centros y estudiantes puedan beneficiarse de los contenidos y adaptarlos a sus propias necesidades.

5. **Relevancia social y tecnológica**
   El proyecto responde a una necesidad creciente en el ámbito educativo: proteger los entornos conectados frente a amenazas cibernéticas. En un contexto donde cada vez más centros incorporan tecnologías IoT para mejorar la gestión y la enseñanza, resulta fundamental garantizar la seguridad de estos sistemas. Además, el proyecto contribuye a formar a los futuros profesionales que deberán afrontar estos desafíos en el mundo laboral.

6. **Fomento de la innovación educativa**
   La iniciativa se enmarca dentro de una apuesta por la innovación pedagógica, integrando tecnologías emergentes, metodologías activas y trabajo colaborativo. Esto no solo mejora la calidad de la enseñanza, sino que también posiciona a los centros participantes como referentes en la transformación digital educativa.

B.1.1.1 Desarrollo y cronología de la actuación

Fases	Sep	Oct	Nov	Dic	Ene	Feb	Mar	Abr	May	Jun
1. Definición del Proyecto y Retos a alcanzar	X									
2. Análisis de las diferentes tecnologías y dispositivos a utilizar		X	X	X						
3. Diseño de la Infraestructura					X	X				
4. Implementación y Pruebas de la Infraestructura						X	X	X		
5. simulaciones de Ataques y Defensas								X	X	X

Fases del Proyecto y Temporalización

Fase I: DEFINICIÓN DEL RETO (septiembre 2024)

Objetivos:

- Identificación de las necesidades y problemáticas del centro educativo
- Análisis de la situación actual y tendencias en ciberseguridad en IoT.
- Identificación de las oportunidades de negocio en el campo de la ciberseguridad.
- Establecimiento de objetivos y metas del proyecto mediante la coordinación y planificación del equipo docente participante.
- Estrategias de formación para el personal docente y no docente, y métodos de evaluación.
- Establecer un plan de acción

Fase II: ANÁLISIS DE LAS DIFERENTES TECNOLOGIAS Y DISPOSITIVOS A UTILIZAR (octubre–diciembre 2024)

Objetivos:

- Identificación de las principales tecnologías utilizadas en redes IoT.
- Identificación de los principales dispositivos IoT a utilizar en un centro educativo.
- Análisis de las necesidades y requisitos de seguridad en centros educativos con tecnologías IoT.
- Identificación de posibles obstáculos y limitaciones para la implementación de soluciones IoT en materia de ciberseguridad.

Fase III: DISEÑO DE LA INFRAESTRUCTURA IoT (enero-febrero 2025)

Objetivos:

- Creación de diseño técnico de la infraestructura de IoT
- Diseño de arquitectura de red y segmentación.
- Elección y compatibilidad de dispositivos
- Selección de las herramientas software de control y seguridad para monitorización y telemetría de red.
- Establecimiento de las políticas y normas de seguridad.
- Integración de infraestructura con una solución SIEM (Gestión de información de seguridad y gestión de eventos).

Fase IV: IMPLEMENTACIÓN Y PRUEBAS EN INFRAESTRUCTURA IoT (febrero-junio 2025)

Objetivos:

- Implementación de la infraestructura de IoT
- Instalación de dispositivos
- Configuración de equipos de interconexión de redes
- Formación a nivel administradores de utilización y mantenimiento de los sistemas.
- Puesta en marcha del proyecto
- Supervisión del correcto funcionamiento e integración de las tecnologías IoT
- Cumplimiento de las medidas de seguridad.

Fase V: SIMULACIONES DE ATAQUES Y DEFENSAS (febrero–junio 2025)

Objetivos:

- Simulación en el entorno de aprendizaje real creado de situaciones de ataque y defensa de ciberseguridad.

- Comprobación de la eficacia de las medidas de seguridad implementadas y la adopción de la tecnología por parte de los administradores (alumnos).
- Evaluación del impacto del proyecto en el proceso educativo
- Recolección de feedback de todos los participantes y utilizar esta información para mejorar y ajustar el proyecto según sea necesario.

B.1.1.2. Objetivos previstos

- **Mejora de la formación:** Los alumnos que participen en el proyecto tendrán la oportunidad de adquirir conocimientos en el campo de la ciberseguridad con dispositivos IoT y de aplicarlos en la práctica. Esto mejorará su formación y les permitirá tener una visión más amplia del mundo empresarial y de las tecnologías.

- **Conciencia sobre la seguridad de IoT:** Los estudiantes pueden desarrollar una sólida comprensión de los desafíos y las mejores prácticas en torno a la seguridad de IoT.

- **Habilidades prácticas en seguridad de IoT:** Los alumnos también podrán desarrollar habilidades prácticas en la implementación de medidas de seguridad en dispositivos y redes de IoT. Estas habilidades pueden ser muy valiosas en el mercado laboral actual. Los estudiantes pueden adquirir.

- **Pensamiento crítico y resolución de problemas:** Los estudiantes pueden aprender a identificar vulnerabilidades de seguridad y a desarrollar soluciones efectivas.

- **Preparación para ciberseguridad en entornos industriales:** Este tipo de proyecto puede preparar a los estudiantes para carreras en el creciente campo de la ciberseguridad en entornos OT, particularmente en roles relacionados con IoT.

- **Investigación y reflexión:** Los estudiantes pueden investigar y reflexionar sobre los diferentes elementos facilitadores de aprendizajes

B.1.1.3 Objetivos alcanzados

El proyecto ha cumplido con creces todos los objetivos inicialmente planteados. Los alumnos han demostrado un alto nivel de implicación y han adquirido conocimientos sólidos en ciberseguridad aplicada a dispositivos IoT. La experiencia ha sido enriquecedora tanto a nivel técnico como formativo, permitiendo a los participantes desarrollar competencias clave para su futuro profesional en un entorno tecnológico en constante evolución.

B.1.1.4 Resultados alcanzados

A lo largo del desarrollo del proyecto, los estudiantes han logrado avances significativos en múltiples áreas relacionadas con la ciberseguridad en el ámbito del Internet de las Cosas (IoT). A continuación, se detallan los principales resultados alcanzados:

- **Formación especializada y aplicada:** Los alumnos han recibido formación teórica y práctica en ciberseguridad, centrándose en los riesgos específicos del entorno IoT. Han trabajado con dispositivos reales, simulando escenarios de ataque y defensa, lo que ha reforzado su comprensión de los conceptos y su capacidad para aplicarlos en contextos reales.

- **Concienciación sobre la seguridad en IoT:** A través de talleres, análisis de casos y prácticas guiadas, los estudiantes han desarrollado una conciencia crítica sobre los desafíos que plantea la seguridad en dispositivos conectados. Han aprendido a identificar amenazas comunes, como accesos no autorizados, vulnerabilidades en el firmware o problemas de configuración.

- **Desarrollo de habilidades técnicas:** Los participantes han adquirido competencias prácticas en la implementación de medidas de protección, como el cifrado de comunicaciones, la autenticación segura, la segmentación de redes y el uso de herramientas de análisis de tráfico y detección de intrusiones. Estas habilidades son altamente valoradas en el mercado laboral actual.

- **Fomento del pensamiento crítico y la resolución de problemas:** El enfoque del proyecto ha promovido la autonomía y el pensamiento analítico. Los estudiantes han sido capaces de identificar vulnerabilidades en entornos simulados y proponer soluciones eficaces, desarrollando así su capacidad para enfrentar problemas complejos de forma estructurada.

- **Preparación para entornos industriales (OT):** El proyecto ha introducido a los alumnos en los principios de la ciberseguridad en entornos operacionales (OT), donde la protección de infraestructuras críticas y sistemas industriales es esencial. Esto les ha permitido comprender las diferencias entre los entornos IT y OT, y prepararse para roles profesionales en sectores como la industria, la energía o la automatización.

- **Investigación y reflexión pedagógica:** Finalmente, los estudiantes han participado en actividades de investigación y reflexión sobre su propio proceso de aprendizaje. Han documentado sus avances, compartido experiencias y evaluado críticamente las herramientas y metodologías utilizadas, lo que ha contribuido a una formación más profunda y significativa.

En conjunto, los resultados obtenidos no solo evidencian el cumplimiento de los objetivos, sino que también reflejan un impacto positivo en la formación integral de los alumnos, preparándolos para afrontar los retos de la ciberseguridad en un mundo cada vez más conectado.

B.1.1.5 Impacto en el colectivo de actuación y en el territorio

La implementación de este proyecto ha generado un impacto positivo y tangible en varios niveles:

1. Impacto en el colectivo educativo participante

- **Mejora de la seguridad digital:** La instalación y configuración de sensores IoT con medidas de ciberseguridad ha contribuido a crear entornos escolares más seguros, protegiendo tanto la infraestructura tecnológica como los datos personales de alumnos y docentes.
- **Concienciación y cultura de la ciberseguridad:** El proyecto ha fomentado una mayor conciencia sobre la importancia de la seguridad digital entre todos los miembros de la

comunidad educativa, promoviendo buenas prácticas y hábitos responsables en el uso de la tecnología.

- **Participación activa del alumnado:** Al involucrar a los estudiantes en un proyecto real con impacto directo en su entorno, se ha potenciado su motivación, sentido de pertenencia y compromiso con la mejora de su centro educativo.
- **Transferencia de conocimiento:** Los conocimientos adquiridos por los alumnos pueden ser compartidos con otros compañeros, docentes y familias, ampliando el alcance del proyecto más allá del grupo inicial.

2. Impacto en el territorio

- **Modelo replicable para otros centros:** Este proyecto puede servir como modelo para otros centros educativos en España, demostrando que es posible mejorar la ciberseguridad mediante soluciones IoT accesibles y con participación estudiantil.
- **Contribución a la estrategia nacional de ciberseguridad:** Iniciativas como esta se alinean con los objetivos de la Estrategia Nacional de Ciberseguridad, que promueve la protección de infraestructuras críticas, la formación de talento y la concienciación ciudadana.
- **Fomento de vocaciones tecnológicas:** Al exponer a los jóvenes a tecnologías emergentes y desafíos reales, se estimula el interés por carreras STEM (Ciencia, Tecnología, Ingeniería y Matemáticas), contribuyendo al desarrollo de talento local en un sector estratégico.
- **Reducción de la brecha digital:** Al integrar tecnologías avanzadas en centros educativos, especialmente si se trata de zonas rurales o con menos recursos, se contribuye a reducir desigualdades en el acceso y uso seguro de la tecnología.

Este proyecto no solo ha fortalecido la seguridad digital de los centros participantes, sino que también ha generado un efecto multiplicador en la comunidad educativa y ha sentado las bases para futuras iniciativas de ciberseguridad educativa a nivel nacional.