Sugerencias para integrar la CIBERSEGURIDAD en el reto planteado en las IV Teleco Games.

Durante la realización del proyecto se llevará a cabo una **promoción de la cultura de la ciberseguridad**, fomentando la **concienciación** en esta materia e incorporando **medidas que favorezcan un uso responsable y seguro de la tecnología**.

Atendiendo a las **metas seleccionadas** por cada equipo participante para dar respuesta al reto planteado en estas Teleco Games vinculadas a uno o varios **Objetivos de Desarrollo Sostenible (ODS)**, se podrán:

- Desarrollar acciones de **divulgación y concienciación** en materia de ciberseguridad aplicadas a diferentes ámbitos: transporte, TIC, salud, enseñanza, banca, entre otros.

Para ello , los equipos participantes podrán trabajar en propuestas de concienciación relacionadas con:

- Uso seguro de contraseñas.
- Privacidad y protección de la información y los datos personales.
- Uso responsable de redes sociales y videojuegos.
- Prevención del **ciberacoso** y estrategias de actuación.
- Identificación de **engaños y fraudes online** (phishing).
- Gestión de la **huella digital**.
- Promoción de un **uso equilibrado de la tecnología**.

Estas pueden ir desde acciones más simples como “buenas prácticas”, hasta implementaciones en el código vinculadas a una o varias de las **siguientes fases:**

1. Durante el desarrollo del proyecto (trabajo en grupo), por ejemplo:
    - Fomentando el uso de repositorios privados o compartidos con control de acceso (por ejemplo, en GitHub Classroom, Google Drive, o repositorios que faciliten los centros educativos a sus estudiantes).
    - Recomendando el uso de librerías oficiales o bien documentadas para funciones de comunicación y cifrado.
    - Manteniendo rutinas de seguridad como bloquear y cerrar sesiones en dispositivos después de utilizarlos, mantener los equipos con el software actualizado, utilizar contraseñas seguras y hacer copias de seguridad.

2. Durante la ejecución del proyecto (cuando el sistema está funcionando), por ejemplo:
    - Controlando el acceso a los dispositivos conectados, para que únicamente aquellos previamente autorizados puedan establecer comunicación con el sistema.
    - Cifrando los datos transmitidos a través de tecnologías inalámbricas como WiFi o Bluetooth, con el fin de evitar que puedan ser interceptados o leídos por terceros no autorizados.

3. Durante la difusión del proyecto (en RRSS, presentaciones), por ejemplo:
    - Evitando compartir públicamente información privada de las personas que hayan participado en el proyecto sin tener su autorización (nombre completo, edad, centro educativo, ubicación, etc.)..
    - No mostrando en público información sensible como direcciones IP, claves de red o credenciales.

Para la integración de forma sencilla, de una reflexión o acción concreta que evidencie cómo la **ciberseguridad** contribuye o beneficia activamente al cumplimiento de las metas abordadas en el reto, y/o en el proceso de elaboración del proyecto presentado, aconsejamos que se explore la web del Instituto Nacional de Ciberseguridad **(INCIBE)**, en su apartado de jóvenes:

https://www.incibe.es/menores/jovenes

En la web de INCIBE se pueden encontrar consejos para el uso de internet en la búsqueda de información, uso seguro de las redes sociales a nivel personal y para la difusión del proyecto, así como rutinas de seguridad como bloquear y cerrar sesiones en dispositivos después de utilizarlos, mantener los equipos con el software actualizado, utilizar contraseñas seguras y hacer copias de seguridad.

Los docentes pueden utilizar el material didáctico de INCIBE para incluir de manera transversal al proyecto, nociones de ciberseguridad, como la disponible en:

https://www.incibe.es/menores/materiales/presentacion-para-mayores-de-14-anos