La hora de la ciberseguridad

La actividad propuesta tiene como objetivo evaluar y fortalecer el nivel de madurez en ciberseguridad de los alumnos de 13 a 18 años a través de dinámicas interactivas y educativas. Utilizando herramientas como Kahoot e Interland, se busca fomentar el aprendizaje de conceptos clave en un entorno lúdico y participativo. Antes de la actividad, se garantizará el cumplimiento de los aspectos éticos mediante la obtención del consentimiento informado de padres y alumnos. Durante la sesión, se llevarán a cabo juegos y cuestionarios diseñados para identificar riesgos comunes, como el phishing, y promover buenas prácticas, como la creación de contraseñas seguras. Finalmente, se recopilarán datos y opiniones a través de una encuesta para analizar los resultados y mejorar futuras actividades relacionadas con la ciberseguridad.

Previo a la actividad

1. **Obtención de Consentimiento:**
    a. Una semana antes de la actividad, enviar a los padres y alumnos los documentos requeridos para solicitar su consentimiento. Estos documentos incluyen:
        i. **Certificado de ética**: Validar que la actividad que se realizará está cumpliendo con la normativa del comité de ética de la Universidad Adolfo Ibáñez.
        ii. **Carta de consentimiento informado**: Notificar tanto a los padres como apoderados de la realización de la actividad, su propósito, la información recaudada y la duración en la base de datos de la universidad.
        iii. **Consentimiento informado:** Notificar a los participantes sobre la actividad a realizar, explicarles claramente sus objetivos y alcances, y obtener su consentimiento para llevarla a cabo. Este paso es fundamental para garantizar el respeto a su privacidad y asegurar que la recolección de datos se realice de manera ética y protegida.

    - *Es crucial solicitar las firmas con antelación para tener todo listo antes de la actividad.*

2. **Revisión de Documentación:**
    a. Confirmar que todos los participantes han enviado sus consentimientos.

b. Guardar las copias firmadas en un formato seguro, preferentemente digital (PDF), para facilitar su consulta posterior, dentro de un repositorio de la universidad.

Durante la actividad

1. **Introducción a la Actividad (5 minutos):**
    a. Comenzar con una breve presentación que explique el propósito de la actividad. Incluir:
        1. Objetivo general: Medir y fortalecer el nivel de madurez en ciberseguridad de los alumnos.
        2. Estructura de la actividad: Un resumen de las dinámicas y herramientas que se utilizarán (Kahoot e Interland).

2. **Fases de la Actividad:**
    a. Fase 1: Kahoot inicial (5-10 minutos):

    Realizar un quiz interactivo a través de Kahoot para medir los conocimientos previos en ciberseguridad de los participantes.

        1. Preguntas orientadas a conceptos básicos de ciberseguridad.
        2. Revisión de las respuestas en tiempo real para fomentar la participación y aclarar dudas generales.

    b. Fase 2: Actividad "Phishing" en Kahoot (5-10 minutos):

    Realizar un segundo Kahoot enfocado exclusivamente en temas de phishing.

        1. Mostrar ejemplos prácticos de intentos de phishing.
        2. Analizar cómo identificarlos y las mejores prácticas para evitarlos.

    c. Fase 3: Juegos Interland (2 dinámicas, máximo 15 minutos cada una):

        1. Reino: Río de la Realidad

        Un juego interactivo que ayuda a los alumnos a distinguir entre lo real y lo falso en el entorno digital.

            1.1 Explicar las reglas brevemente antes de empezar.

1.2 Supervisar el progreso y aclarar dudas durante el juego.

2. **Reino: Torre del Tesoro**

Este juego fomenta la creación de contraseñas seguras.

2.1 Orientar a los participantes sobre los objetivos del nivel antes de comenzar.
2.2 Resaltar la importancia de proteger información personal.

d. Fase 4: Kahoot de cierre (5-10 minutos):

Realizar un último Kahoot como actividad de cierre para consolidar lo aprendido, y para hacer una comparativa con lo que sabían de antes y con lo aprendido ahora en el corto plazo.

1. Preguntas diseñadas para reforzar los conceptos clave vistos durante la actividad.
2. Al final, se puede felicitar a los alumnos y mostrar los resultados destacados.

Después de la actividad

1. **Encuesta de Retroalimentación:**
   a. Compartir un formulario en línea, basado en el modelo MEEGA (Modelo de Evaluación de Experiencia de Gamificación en el Aula), para recoger las opiniones de los alumnos sobre la actividad.

2. **Análisis de Resultados:**
   a. Recopilar y analizar los datos obtenidos en las actividades y la encuesta.
   b. Generar un informe que resuma el nivel de madurez en ciberseguridad de los alumnos y las áreas de mejora detectadas.
   c. Compartir los resultados, si es pertinente, con los participantes o sus padres, siempre respetando las normas éticas y de privacidad.