GUÍA DE ESTUDIO DE LA UNIDAD 7

El factor humano en la ciberseguridad

Tiempo estimado de estudio fuera del aula: 4 horas

Material obligatorio de estudio para esta semana

1. Diapositivas de la Unidad 7.
2. Vídeo de concienciación (MOOC, Premio al mejor vídeo educativo en el Día de Internet) https://www.youtube.com/watch?v=kvbYbsGoofo&t=4s
3. Material para el Caso 1.

Material complementario/optativo

Lectura sobre ingeniería social
https://www.sba-research.org/wp-content/uploads/publications/jisa_revised.pdf
Lectura sobre cibercrimen (Internet Organised Crime Threat Assessment, IOCTA)
https://www.europol.europa.eu/publications-events/main-reports/iocta-report

Autoevaluación (conceptos que deberían quedar claros tras esta semana de estudio)

1. ¿Por qué solemos decir que las personas somos el eslabón más débil en ciberseguridad? ¿A qué nos referimos cuando decimos que la seguridad por oscuridad no funciona?
2. ¿Qué es un Insider Threat? ¿Cómo pretende lidiar con esta amenaza un ITP?
3. ¿En qué consiste la ingeniería social? ¿Cuáles suelen ser sus objetivos? Menciona las técnicas de ingeniería social que conozcas.
4. ¿Cómo combatirías este tipo de técnicas?
5. ¿Qué es el phishing y qué pretende? ¿Qué tipos específicos de phishing conoces?
6. ¿Qué es un CIO o CISO y cuáles son sus principales responsabilidades?
7. ¿Qué es un Plan Director de Seguridad y cómo se define?
8. ¿Qué es una política de seguridad y para qué sirve? Explica qué partes la componen y menciona alguna típica que suelan tener definida casi todas las organizaciones.
9. ¿Qué tipo de cibercriminales conoces según la tarea que realizan? ¿Qué tipos de modelos de negocio?
10. ¿En qué consiste el cibercrimen como servicio y por qué está de actualidad?
11. ¿Qué es un delito informático?
12. ¿Cuál es el marco regulatorio de la ciberseguridad en España? Menciona las principales leyes o normas que aplican en la actualidad y su ámbito.