UAX Universidad Alfonso X el Sabio

ÍNDICE MOOCS PROYECTO PECIEE

CASTRO ALONSO

1. Protección de datos y confidencialidad: ciberseguridad desde la PYME

Cómo proteger los proyectos, evitar filtraciones accidentales y cumplir con el RGPD en el trabajo diario. Casos reales de brechas en la organización y qué enseñanzas dejan:

- Diferencia entre dato personal y dato especialmente protegido en cada sector.
- Qué dice el RGPD sobre accesos no autorizados.
- Riesgos comunes: pantallas visibles, documentos impresos, accesos compartidos.
- Buenas prácticas de seguridad en entornos compartidos.
- Qué hacer (y qué no hacer) ante un incidente

2. Ingeniería social: cuando el eslabón débil es la persona

Correos falsos, llamadas manipuladoras o visitas sospechosas: cómo detectar intentos de engaño dirigidos al personal directivo o administrativo, etc., y qué hacer ante ellos.

- Qué es la ingeniería social y por qué apunta a personas, no sistemas.
- Tipos de ataques más frecuentes en las empresas: *phishing, vishing, smishing*. Ejemplos reales.
- Señales de alerta: cómo reconocer un intento de manipulación.
- Pautas para protegerse y notificar incidentes de forma correcta.

3. Dispositivos conectados, correo y redes: más allá del ordenador de mi organización

Cada vez más aparatos y máquinas profesionales están conectados a la red. Qué implica esto en términos de ciberseguridad, y cómo evitar riesgos también en móviles, correo y WiFi.

- Qué riesgos plantean hoy los aparatos profesionales conectados (IoMT).
- Situaciones reales: accesos remotos no controlados, configuraciones por defecto, contraseñas débiles.
- Uso seguro del correo corporativo y navegación en la red de la organizacíon.
- Buenas prácticas en redes WiFi, móviles y dispositivos USB.
- El papel del profesional en la cadena de seguridad.

4. Ransomware y continuidad asistencial: ¿qué hacer si todo se bloquea?

Qué es un ciberataque de secuestro digital, cómo puede afectar al trabajo y a los distintos departamentos y cómo actuar desde el rol de usuario no técnico.

- Qué es el ransomware y cómo afecta a la actividad de mi empresa.
- Ciclo de un ataque: desde el clic hasta el bloqueo total.
- Ejemplos reales y sus consecuencias.
- Cómo actuar ante una sospecha: qué hacer, qué no hacer y a quién avisar.
- Medidas preventivas desde el día a día: copias, actualizaciones y prudencia.

5. Inteligencia artificial y privacidad: oportunidades y riesgos en la empresa

Cómo se empieza a usar IA en la PYME y por qué debe hacerse con precaución: sesgos, decisiones automatizadas y protección de datos sensibles.

- Cómo se está usando ya la IA , chatbots, organización.
- Dónde están los riesgos: decisiones automatizadas, falta de control humano, sesgos.
- Protección de datos y consentimiento informado en herramientas basadas en IA.
- ¿Se puede usar ChatGPT con los datos de mi empresa?
- Criterios básicos para un uso responsable y seguro de IA en la PYME.

6. Ciberseguridad en el futuro

- Evolución de las amenazas y tecnologías emergentes (blockchain, criptografia, i. cuántica, etc)
- Impacto de la ciberseguridad en la vida cotidiana y en sectores como la salud, entidades financieras, infraestructuras críticas
- Debate sobre cómo imaginan losa alumnos el futuro de la cigberseguridad