TECH FAB LAB

CEEI Comunidad Valenciana

TECH LEADERS

BLOCKCHAIN Y CIBERSEGURIDAD PARA STARTUPS Y SCALEUPS

Blockchain
Adela Erades Pérez
INTK BUSINESS SECURITY

Ciberseguridad
Lucía Bort Lorenzo
INTK BUSINESS SECURITY

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA MINISTERIO DE TRANSFORMACIÓN DIGITAL Y FUNCIÓN PÚBLICA

Plan de Recuperación, Transformación y Resiliencia

GENERALITAT VALENCIANA Conselleria de Innovación, Industria, Comercio y Turismo

GVA NEXT Fondos Next Generation en la Comunitat Valenciana

BLOCKCHAIN

Más allá del Bitcoin

BLOCKCHAIN: La analogía del libro de cuentas

1. **No hay un solo cuaderno.** Cada habitante del pueblo tiene una copia exacta de ese cuaderno en su casa.
2. **Es verificado:** Si Ana intenta pagar otros 10 euros pero ya no tiene saldo, todos los vecinos miran sus cuadernos y dicen: 'Imposible, Ana, según nuestros registros ya gastaste tu dinero'. La transacción se rechaza democráticamente.
3. **Es imborrable:** Lo que se escribe en el cuaderno se hace con 'tinta permanente'. Nadie puede arrancar una página o usar típex sin que los demás se den cuenta de que su copia no coincide.

Esto es Blockchain. Es un libro de registro digital, compartido por miles de ordenadores, donde una vez que se escribe algo, es imposible borrarlo o alterarlo sin que todos se den cuenta.

BLOCKCHAIN: De la analogía a la realidad

Base de datos distribuida

- **Transparencia:** Todos los participantes (dependiendo del tipo de red) tienen acceso a la misma información en tiempo real.
- **Seguridad:** Para hackear la red, tendrías que atacar a miles de ordenadores al mismo tiempo, lo cual es matemáticamente y económicamente casi imposible.
- **Inmutabilidad:** Lo que registráis ahí, se queda ahí para siempre. Es la máquina de la verdad definitiva para vuestros datos.

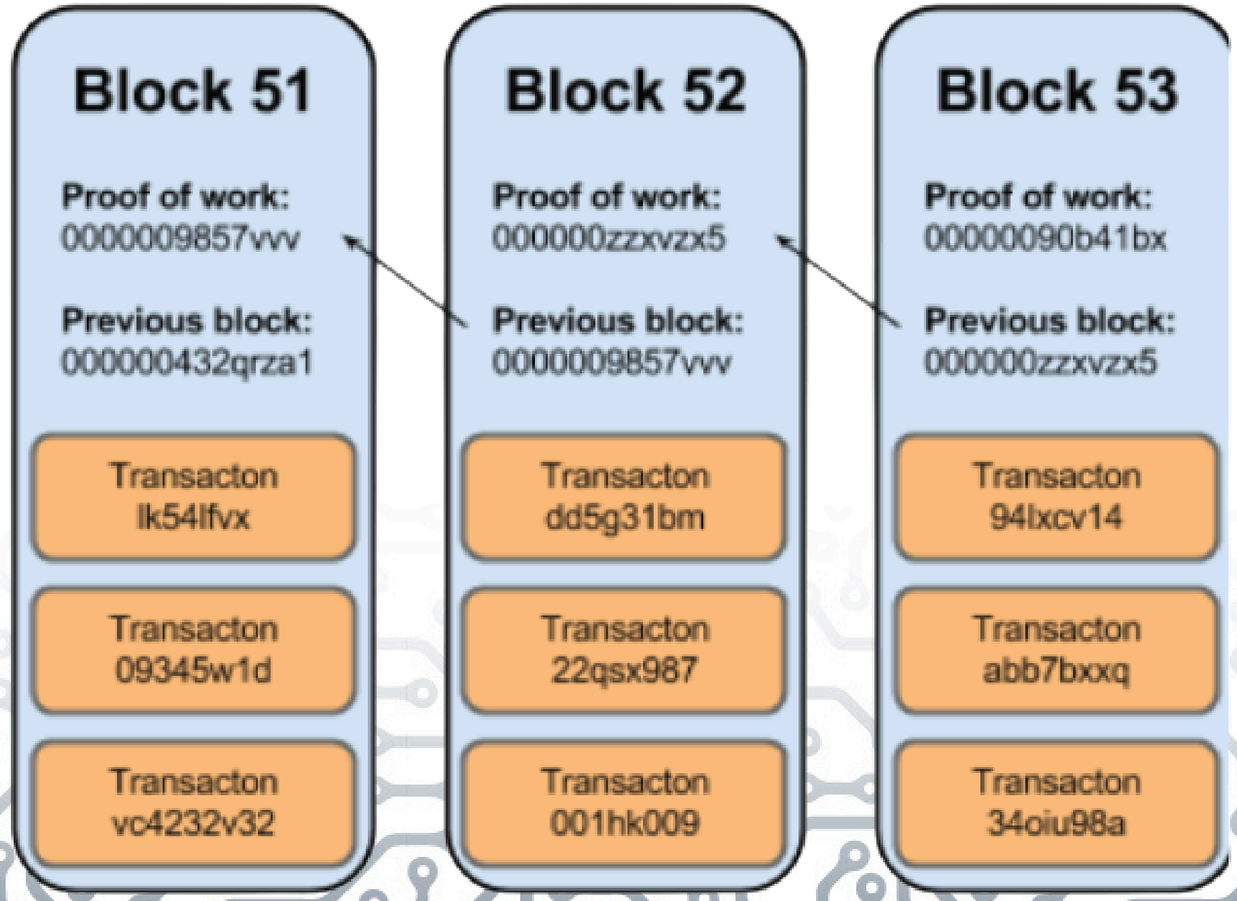
BLOCKCHAIN: Importancia para vuestras empresas

- **Reducción de costes:** Si eliminamos al intermediario (al 'banco' o al 'notario'), las comisiones desaparecen o bajan drásticamente.
- **Trazabilidad y Auditoría:** Para una scaleup que necesita demostrar a inversores o reguladores que sus datos son reales, Blockchain ofrece una auditoría perfecta. Nadie puede acusaros de 'cocinar los libros' porque el libro no lo controláis solo vosotros.
- **Nuevos Modelos de Negocio:** Permite crear economías donde vuestros usuarios pueden intercambiar valor entre ellos sin que vosotros tengáis que custodiar ese valor, reduciendo vuestra responsabilidad legal y riesgos de seguridad.

BLOCKCHAIN: Seguridad y automatización

- **Input:** Cualquier cantidad de datos, desde una palabra, hasta “enciclopedias”
- **Función:** Proceso matemático.
- **Output (Hash):** Un código único de longitud fija.
- **La Regla de Oro:** Si cambias una sola coma en el Input, el Hash cambia totalmente.

BLOCKCHAIN: Seguridad y automatización



BLOCKCHAIN: Diferencias entre CSV y Hash Criptográfico

	CSV (Código Seguro de Verificación)	Blockchain (Hash Criptográfico)
¿Qué es?	Un **localizador**. Es como una "url" o una etiqueta que dice: "Busca este documento en el archivo del Ayuntamiento".	Una **huella matemática**. Es el resultado de comprimir el contenido del documento en sí mismo.
Dependencia	**Centralizada.** Necesitas ir a la web de la entidad (Sede Electrónica) para validarlo.	**Descentralizada.** Puedes verificarlo matemáticamente sin pedir permiso a ninguna entidad.
Punto de Fallo	Si el servidor de la entidad se cae o un admin cambia el archivo en el servidor, el CSV valida algo falso o deja de funcionar.	Si la red está activa, la verificación es infalible. Nadie puede cambiar el archivo original sin romper la cadena.
Confianza	Confías en la **institución**.	Confías en las **matemáticas**.

BLOCKCHAIN: Seguridad y automatización

- **Input:** Cualquier cantidad de datos, desde una palabra, hasta “enciclopedias”
- **Algoritmos de consenso:** Son el corazón de blockchain, permitiendo a nodos independientes llegar a un acuerdo sobre qué transacciones son legítimas y qué nuevo bloque añadir a la cadena, resolviendo el problema de la confianza en un entorno distribuido.
- **Output (Hash):** Un código único de longitud fija.
- **Criptografía (Hashing):** Funciones como SHA-256 crean "huellas digitales" únicas (hashes) para cada bloque y enlazan los bloques, haciendo que cualquier alteración sea detectable inmediatamente, cambiando el hash del archivo.

BLOCKCHAIN: Minería

¿Quién resuelve los algoritmos?
Imagina que tienes un candado de combinación digital con millones de combinaciones posibles. El trabajo del minero no es usar "inteligencia" para abrirlo, sino usar fuerza bruta.

1. El minero coge un grupo de transacciones recientes y las mete en un paquete.
2. El protocolo de red le dice al minero: *"Para que este bloque sea válido, el código digital (hash) resultante debe empezar con diez ceros".*
3. Como el resultado del hash es impredecible, el minero empieza a probar números aleatorios (llamados Nonce) una y otra vez a una velocidad vertiginosa.
4. El minero informa al resto de la red. Si es correcto, se le permite escribir el bloque en la historia y recibe bitcoins + las comisiones de las transacciones.

BLOCKCHAIN: Nodos de consenso

Un nodo es cualquier ordenador conectado a la red de blockchain que ejecuta el software de esa criptomoneda. No todos los nodos (ordenadores) minan, pero todos los mineros deben ser nodos.

Cuando un minero dice "¡Encontré el bloque!", los nodos reciben esa información y la revisan instantáneamente. Verifican cosas como:

- ¿Las transacciones dentro del bloque son legítimas? (¿Tiene fondos la persona que envía?).
- ¿El problema matemático realmente fue resuelto correctamente?
- ¿El bloque tiene el tamaño y formato correcto?

Los nodos "Full" guardan una copia completa de toda la historia de transacciones desde el día uno.

BLOCKCHAIN: Nodos de consenso

Aquí es donde entra la magia del "consenso". Como no hay un banco central, todos los nodos deben ponerse de acuerdo sobre cuál es la verdad.

1. Un minero encuentra una solución y la transmite.
2. Los nodos cercanos la reciben, la validan y, si es correcta, la pasan a sus vecinos (propagación).
3. En segundos, todos los nodos del mundo actualizan sus copias del registro (Ledger) con el nuevo bloque.
4. Consenso alcanzado: Todos están de acuerdo en que ese bloque es el siguiente en la cadena.

BLOCKCHAIN: Aplicación práctica, los Smart Contracts

Programa informático que vive dentro de la blockchain y que se ejecuta automáticamente cuando se cumplen ciertas condiciones, sin que nadie pueda detenerlo o cambiarlo.

Contrato tradicional: Le pagas al abogado, él hace el papel, tú firmas, la otra parte firma. Si la otra parte no cumple (no te entrega el producto), tienes que llamar al abogado, ir a juicio y esperar meses.

- Depende de: La buena fe y los intermediarios.

Smart Contract (máquina expendedora): Tú metes la moneda y seleccionas el producto "A1". La máquina (el código) detecta el dinero y automáticamente deja caer el producto.

- No necesitas un cajero que te vigile.
- No necesitas confiar en el dueño de la máquina.
- Si no pones el dinero, no sale el producto. El código es la ley.
- Si el producto no sale, automáticamente se te devuelve el importe pagado.

BLOCKCHAIN: Aplicación práctica, los Smart Contracts

Los smart contracts siguen instrucciones simples pero estrictas programadas en ellos:

"SI (usuario envía 5 ETH al contrato) Y (la fecha es después del 01/01/2026), ENTONCES (transferir propiedad del Token X al usuario)."

Una vez que este código se sube a la blockchain, nadie puede modificarlo. Ni siquiera el creador del contrato. Si envías los 5 ETH, el contrato te dará el token. No puede "arrepentirse" ni robarte.

BLOCKCHAIN: Aplicación práctica, los Smart Contracts

Ejemplos:

Apuestas deportivas sin casa de apuestas:

- Tú y yo apostamos al resultado del Real Madrid vs Barça. Enviamos el dinero al Smart Contract. El contrato consulta una fuente de datos fiable (Oráculo) tras el partido y envía automáticamente todo el dinero al ganador. Sin intermediarios que cobren comisión.

Seguros de vuelo:

- El contrato sabe si tu vuelo se retrasó más de 2 horas (conectado a bases de datos de aeropuertos). Si pasa, te deposita el dinero de la indemnización al instante, sin que tengas que llenar formularios ni pelear con la aseguradora.

BLOCKCHAIN: Conclusiones

El Blockchain no sirve para todo.

Es una tecnología lenta y cara comparada con una base de datos tradicional. No la uséis para guardar fotos o datos que no importan mucho.

Usad Blockchain solo cuando necesitéis:

1. Que varias partes que no confían entre sí compartan datos (Consorcios).
2. Que nadie pueda censurar o borrar la información (Inmutabilidad).
3. Que el valor se mueva automáticamente (Smart Contracts).

Si vuestra startup cumple estos requisitos, esta tecnología os dará una ventaja competitiva brutal. Si no, usad una base de datos normal, que funciona de maravilla.

Ciberseguridad

Protegiendo la innovación y el crecimiento en entornos digitales modernos.

Ciberseguridad: La realidad del entorno digital

- **El mito:** "Somos demasiado pequeños para ser un objetivo".

- **La realidad:** Las startups son objetivos atractivos (datos valiosos, pasarelas a empresas más grandes, menores defensas iniciales).

Características del entorno actual:

- Trabajo híbrido/remoto (perímetro difuso).
- Dependencia crítica de terceros (SaaS, APIs).
- Desarrollo rápido (CI/CD) vs. Deuda de seguridad.
- **Dato clave:** El coste medio de una brecha de datos puede suponer el cierre de una startup en fase temprana.

Ciberseguridad: Principios básicos. La triada CIA

Confidencialidad:

- Solo las personas autorizadas pueden acceder a la información.
- **Ejemplo:** Proteger la IP (Propiedad Intelectual), datos financieros y listas de clientes.

Integridad:

- La información es precisa, completa y no ha sido alterada sin autorización.
- **Ejemplo:** Asegurar que el código fuente no tiene inyecciones maliciosas o que los saldos de los usuarios son correctos.

Disponibilidad:

- La información y los sistemas están accesibles cuando se necesitan.
- **Ejemplo:** Evitar caídas por ataques DDoS que detengan el servicio (SaaS down = Churn).

Ciberseguridad: Amenazas habituales

Phishing e ingeniería social

El eslabón humano: El 90% de los ciberataques comienzan con un correo electrónico.

Tipologías comunes:

- Spear Phishing: Ataques dirigidos a empleados específicos (RRHH, Finanzas).
- CEO Fraud (Whaling): Suplantación de fundadores para solicitar transferencias urgentes.

Señales de alerta: Urgencia injustificada, remitentes desconocidos, enlaces acortados sospechosos.

Ciberseguridad: Amenazas habituales

Ciberseguridad: Amenazas habituales

Ransomware y extorsión

Mecanismo: Software malicioso que cifra los datos y exige un rescate.

La doble extorsión:

a. Cifrado de datos (parada operativa).
b. Amenaza de publicación de datos exfiltrados (daño reputacional/GDPR).

Vectores de entrada: RDP (Escritorio remoto) expuesto, correos maliciosos, vulnerabilidades no parcheadas.

Ciberseguridad: Amenazas habituales

Ciberseguridad: Amenazas habituales

Fugas de datos y Shadow IT

Fugas por configuración:

- Buckets de S3 públicos.
- Bases de datos sin contraseña expuestas a internet.

Amenaza interna: Empleados descontentos o negligentes.

Shadow IT: Uso de herramientas no aprobadas (ej. subir datos sensibles a herramientas de IA públicas o WeTransfer personal).

Ciberseguridad: Buenas prácticas desde el día 0

Higiene de identidad y accesos

MFA (Autenticación Multifactor):

- Obligatorio para todo (Google Workspace, AWS, GitHub, Slack).
- Preferencia por App o Llave física (YubiKey) sobre SMS.

Gestores de Contraseñas:

- Prohibido reutilizar passwords.
- Uso corporativo de herramientas como 1Password o LastPass.

Principio de Mínimo Privilegio (PoLP): Dar solo los permisos necesarios para realizar el trabajo, por tiempo limitado.

Ciberseguridad: Buenas prácticas desde el día 0

Seguridad en dispositivos (Endpoints)

- **Cifrado de disco:** BitLocker (Windows) o FileVault (Mac) activados por defecto.
- **EDR (Endpoint Detection and Response):** Más allá del antivirus tradicional; detección de comportamiento anómalo.
- **Política de actualizaciones:**
  - Sistemas operativos y navegadores siempre en la última versión ("Patch Tuesday").
  - Automatización de parches (MDM - Mobile Device Management).

Ciberseguridad: Buenas prácticas desde el día 0

Cultura de seguridad

- **Onboarding:** La seguridad es parte del kit de bienvenida.
- **Transparencia:** Crear un canal donde reportar errores (ej. "Hice clic en un enlace raro") no sea motivo de castigo, sino de solución rápida.
- **Formación continua** a empleados y directivos para estar al día de las últimas amenazas.
- **Simulacros:** Pruebas de phishing ético para entrenar el ojo del empleado.

Ciberseguridad: Seguridad en la nube y activos

Modelo de responsabilidad compartida

- **Proveedor (AWS/Azure/GCP):** Responsable de la seguridad de la nube (hardware, red global, centros de datos).

- **Cliente (Tu):** Responsable de la seguridad en la nube.
  - Datos de clientes.
  - Gestión de identidades (IAM).
  - Configuración de Firewall/Puertos.
  - Cifrado de datos.

Ciberseguridad: Seguridad en la nube y activos

Protección de Activos Digitales y Desarrollo

- DevSecOps: Integrar seguridad en el ciclo de desarrollo (Shift Left).
  - Escaneo de código estático (SAST).
  - Escaneo de dependencias (evitar librerías vulnerables).
- Gestión de Secretos: Nunca hardcodear claves API o credenciales en el código (GitHub). Usar Vaults.
- Backups: La regla 3-2-1. Asegurar que los backups son inmutables (protección contra ransomware).

Ciberseguridad: Próximos pasos

Hoja de ruta para Startups

1. **Activar MFA en el 100% de las cuentas hoy.**
2. **Realizar un inventario de activos (¿Qué tenemos y quién tiene acceso?).**
3. **Implementar una solución de EDR en portátiles.**
4. **Establecer una política de Backups automatizada.**
5. **Programar una formación básica de concienciación.**

Ciberseguridad: Próximos pasos

- La seguridad no es un destino, es un proceso continuo.
- La seguridad habilita las ventas (genera confianza en clientes B2B y Enterprise).

TECH FAB LAB

CEEI Comunidad Valenciana

PRÁCTICAS EN CIBERSEGURIDAD

INYECCIÓN 1: Algo huele mal

Es viernes a las 16:30 PM. El equipo se prepara para el fin de semana.

- **Soporte al cliente:** Reporta que varios usuarios se quejan de que la plataforma va muy lenta y da "Error 500" al intentar loguearse.
- **Slack de la empresa:** Un desarrollador Junior comenta: "Oye, no puedo acceder al repositorio de código, dice que mis credenciales han cambiado. ¿Alguien tocó algo?"
- **Finanzas:** El CFO recibe un correo del CEO pidiendo una transferencia urgente, pero el CEO está en una reunión y dice que él no ha enviado nada.

INYECCIÓN 1: Algo huele mal

Preguntas:

- ¿Quién toma el mando en este momento? ¿Tenéis un plan de respuesta a incidentes definido?
- ¿Cómo clasificáis esto? ¿Es un fallo técnico, un bug o un incidente de seguridad?
- ¿A quién se avisa primero? ¿Se despierta al CTO?
- ¿Qué herramientas usáis para verificar qué está pasando (Logs, AWS CloudTrail, etc.)?

INYECCIÓN 2 : La doble extorsión

Son las 17:15 PM. La situación ha escalado drásticamente.

- **Pantallas bloqueadas:** Varios portátiles de empleados (incluido el de un administrador de sistemas) muestran un fondo de pantalla rojo con un mensaje: "Sus archivos han sido cifrados por el grupo LockBit. Tienen 24 horas."
- **La prueba:** El mensaje incluye un enlace a la Dark Web donde muestran una muestra de vuestra base de datos de clientes (emails, teléfonos y contraseñas hasheadas).
- **La demanda:** Piden 10 Bitcoins (aprox. $500k USD) para dar la clave de descifrado y no publicar toda la base de datos.
- **Redes Sociales:** Un usuario en Twitter (X) publica una captura de pantalla de vuestra base de datos preguntando: "¿Es cierto que os han hackeado? Mis datos están ahí."

INYECCIÓN 2 : La doble extorsión

Preguntas para la discusión:

1. **Técnica:** ¿Cortáis el acceso a internet de toda la empresa? ¿Apagáis los servidores (afectando la disponibilidad) para contener el ataque?
2. **Negocio:** ¿Pagáis el rescate? (Debatir pros y contras: es ilegal en algunos sitios, no garantiza recuperación vs. coste de cerrar la empresa).
3. **Legal:** ¿Tenéis ciberseguro? ¿A quién hay que notificar legalmente (Agencia de Protección de Datos) y en qué plazo (72h GDPR)?
4. **Comms:** El tweet se está viralizando. ¿Qué respondéis? ¿"Estamos investigando" o "Confirmamos brecha"? (El silencio destruye la confianza).

INYECCIÓN 3: Recuperación y realidad

Son las 20:00 PM. Se ha decidido no pagar.

- **Estado de los Backups**: El equipo técnico informa que los backups on-premise están cifrados también. Sin embargo, los backups en la nube (AWS S3) parecen intactos, pero la última copia es de hace 48 horas.
- **Impacto:** Se perderán 2 días de datos de clientes y transacciones.
- **Prensa:** Un periodista tecnológico llama al CEO al móvil personal pidiendo declaraciones.

INYECCIÓN 3: Recuperación y realidad

Preguntas para la discusión:

1. ¿Cómo gestionáis la pérdida de datos de 48h con los clientes afectados?
2. ¿Cuánto tiempo tardaréis en restaurar el servicio desde S3 ("RTO - Recovery Time Objective")? ¿1 hora? ¿2 días?
3. ¿Cómo garantizáis que al restaurar el backup no volvéis a meter al atacante en el sistema (persistencia)?
4. ¿Cuál es el mensaje oficial final a la prensa y empleados?

Conclusiones

- ¿Qué falló? (Ej. Faltaba MFA, backup conectado a la red principal, nadie sabía quién tenía la contraseña del Twitter corporativo).

- ¿Qué funcionó bien? (Ej. La detección fue rápida, el equipo mantuvo la calma).

La lista de tareas inmediata:

- ¿Necesitamos contratar un seguro?
- ¿Necesitamos mejorar la política de backups inmutables?
- ¿Necesitamos redactar plantillas de comunicación de crisis hoy mismo?

Práctica 2: El gran contrato, due diligence

Vuestra startup está a punto de cerrar el contrato más grande de su historia con un banco internacional ("BigCorp"). Este contrato asegura la ronda de inversión Serie B.

El obstáculo: Antes de firmar, el equipo de seguridad de BigCorp debe auditaros.

Práctica 2: El gran contrato, due diligence

EL CUESTIONARIO DE LA VERDAD
Lunes, 9:00 AM. El contrato está listo, pero llega un correo del CISO (Chief Information Security Officer) del banco.

- **El adjunto:** Un Excel con 250 preguntas de seguridad.
- **El plazo:** "Necesitamos esto respondido para mañana si queréis firmar el viernes".
- **Las preguntas difíciles:**
  a. "¿Realizan pruebas de penetración externas cada 6 meses?" (Nunca habéis hecho una).
  b. "¿Están los datos cifrados en reposo y en tránsito con gestión de llaves centralizada?" (No estáis seguros).
  c. "¿Tienen un plan de continuidad de negocio (BCP) probado anualmente?" (No tenéis ni el documento).

Práctica 2: El gran contrato, due diligence

Preguntas para la discusión:

1. Ventas dice: "Pon que SÍ a todo, luego lo arreglamos. Si decimos que no, perdemos el contrato". ¿Qué hacéis?
2. ¿Cómo respondéis a lo que no tenéis? ¿Mentís? ¿Decís "En Roadmap"? ¿Decís "No, pero tenemos este control compensatorio"?
3. Consecuencias: Legal debe opinar: ¿Qué pasa si mentimos en este Excel y luego hay un incidente? (Spoiler: Es fraude contractual).

Práctica 2: El gran contrato, due diligence

El pentest sorpresa
Miércoles, 10:00 AM. Habéis enviado el cuestionario con algunas respuestas "optimistas".

- **El banco responde:** "Gracias. Para verificar vuestras respuestas, nuestro equipo 'Red Team' va a realizar un escaneo y ataque controlado a vuestra API de staging hoy mismo".
- **El hallazgo (14:00 PM):** El auditor del banco llama. Han encontrado una vulnerabilidad crítica:
  - Es posible ver los datos de otros clientes cambiando un número en la URL (IDOR - Insecure Direct Object Reference).
  - También han encontrado una clave de API de AWS "hardcodeada" en el código visible en el navegador.

Práctica 2: El gran contrato, due diligence

Preguntas para la discusión:

1. **Priorización:** El equipo de desarrollo está trabajando en una característica vital para el lanzamiento del producto la semana que viene. ¿Paráis todo el desarrollo para arreglar esto hoy?
2. **Comunicación:** ¿Cómo explicáis esto al banco? ¿Admitís la culpa total o intentáis minimizarlo? ("Era un entorno de pruebas...").
3. **Remediación:** ¿Tenéis logs para demostrar que nadie más ha explotado ese fallo antes que el auditor? (Si no tenéis logs, no podéis demostrar inocencia).

Práctica 2: El gran contrato, due diligence

El ultimátum contractual

Jueves, 16:00 PM. El fallo técnico se ha parcheado, pero el banco ha perdido la confianza.

- **La exigencia:** Envían un anexo al contrato ("Rider de seguridad").
- **Las cláusulas:**
  a. "La startup permitirá auditorías físicas sorpresa en sus oficinas".
  b. "En caso de brecha de seguridad, la multa será de 1 millón de euros o la rescisión inmediata".
  c. "Deben obtener la certificación ISO 27001 en menos de 6 meses".

Práctica 2: El gran contrato, due diligence

Conclusiones

Preguntas

1. **Documentación:** ¿Nos hemos dado cuenta de que nos faltan políticas escritas? (A veces hacemos las cosas bien, pero no están escritas, y para un auditor, "si no está escrito, no existe").
2. **Deuda de seguridad:** ¿Cuánto tiempo dedicamos a limpiar código vs. crear nuevas características de nuestro producto?
3. **Ventas vs seguridad:** ¿Cómo podemos alinear a Ventas para que no prometa seguridad que no tenemos?

BLOCKCHAIN

Impulsar la capacitación y el acompañamiento de personas emprendedoras, profesionales y empresas en el ámbito de las tecnologías habilitadoras digitales, fomentando el emprendimiento innovador, facilitando la transformación digital del tejido empresarial valenciano y promoviendo la creación, consolidación y escalado de iniciativas empresariales tecnológicas de alto valor añadido.

TECH FAB LAB

CEEI Comunidad Valenciana

TECH LEADERS

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO DE TRANSFORMACIÓN DIGITAL Y FUNCIÓN PÚBLICA

Plan de Recuperación, Transformación y Resiliencia

GENERALITAT VALENCIANA
Conselleria de Innovación, Industria, Comercio y Turismo

GVA NEXT
Fondos Next Generation en la Comunitat Valenciana