Seguridad, datos e integración

El 19 de julio de 2024, miles de pasajeros del aeropuerto de Palma hicieron horas de cola en los mostradores de facturación. No hubo ningún ataque. Una actualización defectuosa de CrowdStrike Falcon, un programa de seguridad, había bloqueado unos **8,5 millones de ordenadores Windows** en todo el mundo, según Microsoft. Aena pasó a procedimientos manuales. Cayó una pieza de la que dependía todo, y todo lo que estaba conectado a ella se paró.

Cada tecnología que añadiste a tu plan en la lección anterior trae dos regalos: **datos nuevos**, que tienes que gestionar, y **puertas nuevas**, que alguien tiene que cerrar. Y todo tiene que estar conectado, así que también tienes que saber qué pasa cuando falla una pieza.

Qué aprenderás

- Encontrar las posibles **brechas de seguridad** de cada área de tu plan, partiendo de tu auditoría pasiva de D5, y dar a cada una una medida
- Definir cómo se **trata** cada tipo nuevo de datos a lo largo de su ciclo de vida
- Dar a cada objetivo estratégico un **indicador** con una fórmula y una fuente de datos
- Dibujar el **diagrama de integración** de datos, aplicaciones y plataformas en diagrams.net, con la **fuente de verdad** de cada dato
- Evitar la trampa de las medidas genéricas («instalar un antivirus») que no responden a ninguna brecha concreta

Cerraduras para cada barrio

En el juego de ciudades, la ciberseguridad es la policía, las murallas y las cerraduras. Un barrio nuevo sin ellas es una invitación.

> Una **brecha de seguridad**, en esta unidad, es un punto débil de un área: algo que podría ir mal con sus datos o sistemas, por un ataque, por un error o por accidente.

No la confundas con una **violación de la seguridad de los datos personales**: eso es un incidente que ya ha ocurrido, y el RGPD (Reglamento (UE) 2016/679, artículo 33) dice que se debe notificar a la autoridad «sin dilación indebida y, de ser posible, a más tardar 72 horas» después de que la empresa tenga constancia. Tu plan analiza las brechas para que las violaciones no lleguen a ocurrir.

Para cada área: **qué activo o dato hay, qué podría ir mal, qué medida pones y qué ley se aplica.**

Área	Activo o dato	Posible brecha	Medida	Ley
Pedidos	Portal B2B con cuentas de hoteles	El personal de recepción de un hotel comparte una sola contraseña	Una cuenta por persona, MFA, registro de accesos	RGPD (datos de contacto)

Área	Activo o dato	Posible brecha	Medida	Ley
Hornos	Medidores IoT en la red del obrador	Dispositivos con contraseñas de fábrica en la misma red que la oficina	Red separada para la OT, cambiar las credenciales	—
Calidad	Registros de temperatura	Un sensor falla y nadie se da cuenta de que los registros se han parado	Alarma cuando dejan de llegar datos, copia diaria	Normativa de seguridad alimentaria
Todas	Servicios en la nube de terceros	Dependencia del proveedor	Copias de seguridad propias, contrato y ubicación de los datos comprobados	RGPD, NIS2 si se aplica

El punto de partida para tu empresa es la **auditoría pasiva** de D5: las cabeceras de seguridad, las cookies y la política de privacidad de su web pública.

> **Solo pasiva**
> Todo lo que digas sobre la seguridad de la empresa real sale de lo que su web muestra a cualquier visitante: securityheaders.com, Mozilla HTTP Observatory, las DevTools del navegador, el banner de cookies, la política de privacidad. Nunca la escanees, nunca sondees puertos, nunca pruebes un inicio de sesión.

> **Cuidado: «instalar un antivirus»**
> Una medida que no responde a una brecha concreta es decoración. Si no puedes decir qué brecha cierra una medida, bórrala.

Datos que entran, decisiones que salen

Cada tecnología nueva produce datos nuevos: pedidos del portal, consumo de los hornos, temperaturas de las cámaras. Para cada uno se tienen que definir dos cosas.

Tratamiento. El ciclo de vida que usaste en D5: cómo se recoge, dónde se guarda, quién puede acceder, cuánto tiempo se conserva y cómo se elimina. Si son datos personales, se aplican el RGPD y la LOPDGDD (Ley Orgánica 3/2018).

Análisis. Los datos te tienen que decir si se están cumpliendo los objetivos.

> Un **indicador** (o **KPI**, key performance indicator) es un número, calculado con una fórmula fija a partir de datos que tienes, que muestra si se está alcanzando un objetivo.

En el juego de ciudades, los indicadores son las capas de la vista de información: tráfico, contaminación, felicidad. Cada objetivo de la sección 1 necesita al menos uno.

Objetivo	Indicador y fórmula	De dónde salen los datos	Cada cuánto
Desperdicio	kg rechazados o no vendidos ÷ kg producidos	ERP (producción) y registro de devoluciones	Semanal
Pedidos en línea	Pedidos de hoteles por el portal ÷ todos los pedidos de hoteles	Portal y ERP	Mensual
Energía	kWh de los hornos ÷ kg producidos	Medidores IoT y ERP	Mensual

Las tuberías entre edificios

> La **integración** es cómo viajan los datos entre aplicaciones, y sobre qué plataformas funcionan esas aplicaciones.

Piensa en tres capas:

Capa	Qué contiene	En el obrador de ejemplo
Datos	Clientes, pedidos, consumos, temperaturas	Cada dato tiene **una fuente de verdad**: el cliente «vive» en el ERP
Aplicaciones	Los programas que usan los datos	Portal, ERP, cuadro de mando, modelo de previsión. Se comunican mediante **API**; las exportaciones manuales son el último recurso
Plataformas	Dónde funcionan las aplicaciones	Servicios en la nube de D3, un dispositivo edge en el obrador para los sensores

> La **fuente de verdad** de un dato es el único sistema donde se crea y se corrige; todos los demás sistemas lo copian de allí.

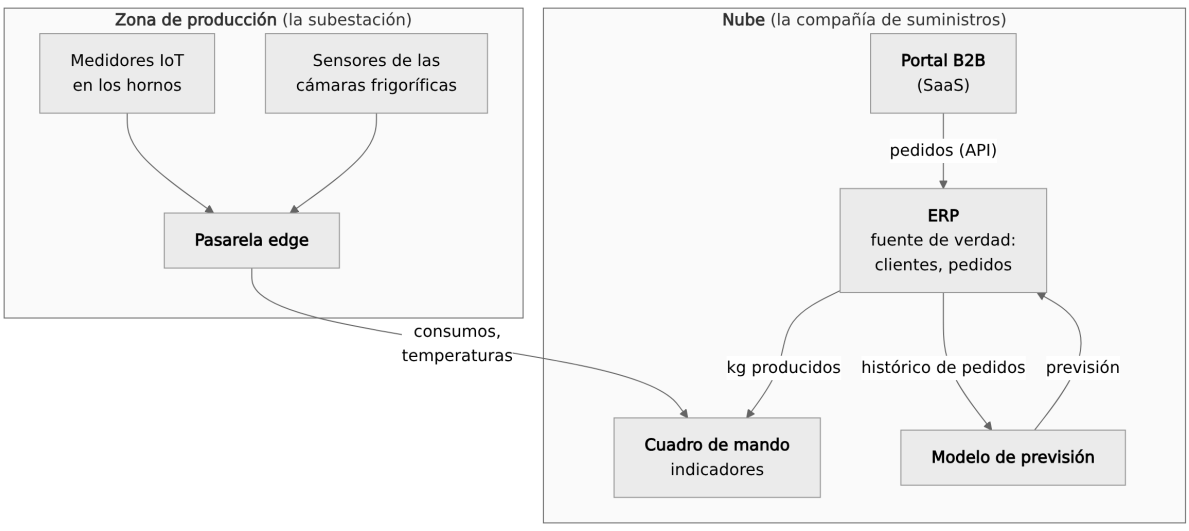
> Una **API** (interfaz de programación de aplicaciones) es una puerta que un programa abre para que otro programa le pueda pedir datos o enviárselos, sin una persona en medio.

Aquí tienes el diagrama de integración del obrador de ejemplo, del mismo tipo que dibujarás:

Comprueba cada diagrama con tres preguntas: **¿dónde está la fuente de verdad? ¿cómo viaja el dato? ¿qué pasa si cae una pieza?** La historia del aeropuerto de Palma es la respuesta a la tercera pregunta cuando nadie se la hizo.

En clase: diagrama, brechas e indicadores

Paso	Haz esto	Deberías ver
1 · grupo	El/la Técnico/a abre app.diagrams.net, elige **Device** (guardar en este ordenador) y crea un diagrama en blanco. Los demás dictan a partir de D3 y la sección 2	Un lienzo vacío



Paso	Haz esto	Deberías ver
2 · grupo	Una caja por aplicación, agrupadas por plataforma (nube, edge, local); flechas etiquetadas con **qué** viaja y **cómo** (API, fichero, a mano); la fuente de verdad de cada dato marcada	Un diagrama que alguien de fuera del grupo podría leer
3 · grupo	**File › Export as › PNG**, y guardad también el fichero `.drawio`	Dos ficheros: la imagen y el diagrama editable
4 · solo	Toma **un área** del plan y escribe dos posibles brechas, el activo afectado, una medida para cada una y la ley implicada. Al menos una debe salir de tu auditoría pasiva de D5	Dos filas en la tabla compartida de brechas
5 · solo	Escribe el indicador de **un** objetivo: nombre, fórmula, de dónde salen los datos en el diagrama, cada cuánto	Un indicador que podrías calcular de verdad

Entrega en Classroom (actividad de clase individual): tus dos filas de brechas y tu indicador, con el diagrama del grupo en PNG adjunto. Solo pasiva, y sin IA generativa.

Para tu proyecto

Esta lección construye la **sección 3 · Seguridad y datos** del D6 · Plan de transformación (criterios g y h) y el diagrama de integración de la **sección 4** (criterio i). Las brechas parten de tu auditoría de D5; las plataformas salen de tu arquitectura de D3. Si D3 ya no encaja con las tecnologías de la sección 2, actualízala y escribe el cambio en el registro de cambios.

Ideas clave

- Una **brecha de seguridad** es un punto débil de un área; una **violación de la seguridad de los datos personales** es un incidente que ya ha ocurrido, que se debe notificar en 72 horas según el RGPD. Los planes analizan las brechas para prevenir las violaciones.
- Para cada área: activo, posible brecha, una medida concreta, la ley implicada. Parte de tu auditoría **pasiva** de D5.
- Cada tipo nuevo de datos necesita su **tratamiento** definido a lo largo de su ciclo de vida.
- Cada objetivo necesita un **indicador** (KPI) con una fórmula y una fuente de datos que tengas de verdad.
- La **integración** tiene tres capas: datos, aplicaciones, plataformas. Cada dato tiene una **fuente de verdad**, y las aplicaciones se comunican mediante **API**.
- Pregúntate siempre qué pasa si cae una pieza: el 19 de julio de 2024, una sola actualización defectuosa paró la facturación del aeropuerto de Palma.

Comprobación rápida

1 ¿Qué diferencia hay entre una brecha de seguridad y una violación de la seguridad de los datos personales?

- **A** Ninguna: son dos nombres para lo mismo
- **B** Una brecha es un punto débil que se podría aprovechar; una violación es un incidente que ya ha ocurrido
- **C** Una brecha solo afecta a la OT y una violación solo a la IT
- **D** Una violación siempre la provoca un atacante externo

2 ¿Cuál de estas medidas está bien emparejada con una brecha concreta?

- **A** «Instalar un antivirus en cada ordenador», para todas las áreas
- **B** «Una cuenta por persona y MFA», para un portal donde el personal del hotel comparte una sola contraseña
- **C** «Comprar un router más rápido», para los registros de temperatura en papel
- **D** «Contratar a un abogado», para dispositivos IoT con contraseñas de fábrica

3 Con la web real de tu empresa, ¿cuál de estas acciones está permitida en el proyecto del curso?

- **A** Escanear sus puertos abiertos para encontrar servicios vulnerables
- **B** Probar contraseñas habituales en su página de inicio de sesión
- **C** Leer sus cabeceras de seguridad en securityheaders.com y su banner de cookies
- **D** Enviarle un correo de phishing de prueba

4 ¿Qué hace que un indicador sea útil en el plan?

- **A** Que suene impresionante en la presentación
- **B** Que mida algo que no tenga relación con los objetivos, así es objetivo
- **C** Que tenga una fórmula fija y se pueda calcular con datos que el plan recoge de verdad
- **D** Que se calcule solo una vez, al final del proyecto

5 ¿Qué es la fuente de verdad de un dato?

- **A** La aplicación más cara de la empresa
- **B** El único sistema donde ese dato se crea y se corrige; los demás lo copian de allí
- **C** La copia de seguridad en la nube
- **D** Cualquier hoja de cálculo donde aparezca el dato

6 En un diagrama de integración, ¿qué debe decir cada flecha?

- **A** Nada: las flechas solo muestran que dos cajas están relacionadas
- **B** Qué viaja y cómo: por ejemplo «pedidos, por API»
- **C** El precio de cada aplicación
- **D** El nombre de la persona que la instaló

7 Un hotel usa un sistema de reservas en la nube conectado a su sistema de llaves de las habitaciones. ¿Qué dos preguntas debería ayudar a responder su diagrama de integración?

- **A** Si el sistema de reservas cae, ¿los huéspedes pueden seguir abriendo sus habitaciones?
- **B** ¿De qué color deberían ser las cajas del diagrama?
- **C** ¿Qué sistema tiene la lista correcta de huéspedes, y cómo la recibe el sistema de llaves?
- **D** ¿Cuántas plantas tiene el hotel?

Datos, puertas y tuberías ya están en su sitio. Las últimas piezas son las personas que gestionarán la nueva ciudad, y el plan escrito de qué cambia y cuándo: Personas y documentación.

Soluciones

1. B · El plan analiza las **brechas** para prevenir las **violaciones**. Y una violación también la puede provocar un error, como un correo enviado a la persona equivocada.

2. B · Una medida debe **cerrar una brecha concreta**. Las contraseñas compartidas se cierran con cuentas personales y autenticación multifactor.

3. C · Solo observación **pasiva**: lo que la web ya muestra a cualquier visitante. Nunca escanees, sondees ni pruebes inicios de sesión en una empresa real.

4. C · Un **indicador** convierte datos en una comprobación de un objetivo. Si los datos no están en tu diagrama, no lo puedes calcular.

5. B · Con una sola **fuente de verdad**, la dirección del cliente se corrige en un solo sitio y todos los demás sistemas reciben la correcta. Con varias, se contradicen.

6. B · Una flecha sin contenido esconde la parte importante. Etiqueta **qué** viaja y **cómo** (API, fichero, a mano), para que se vean las fricciones.

7. A, C · Las preguntas de control de todo diagrama: **qué pasa si cae una pieza**, y **dónde está la fuente de verdad y cómo viaja el dato**.