Ciberataque a Inditex a través de un proveedor: radiografía del riesgo en la cadena de suministro

Qué nos dice el incidente del 16 de abril de 2026 y por qué ningún comité de dirección puede seguir tratando a sus proveedores como zona neutral.

El 16 de abril de 2026, Inditex confirmó que un tercero accedió sin autorización a bases de datos alojadas en un proveedor tecnológico externo. No hubo intrusión en sus sistemas propios. No hizo falta. La puerta estaba abierta en otro punto de la cadena. Ese matiz, aparentemente menor, es hoy el problema de ciberseguridad más relevante para cualquier empresa española con proveedores críticos.

Qué ha pasado: los hechos, sin especulación

Inditex —matriz de Zara, Massimo Dutti y otras siete marcas globales, con una facturación de 35.947 millones de euros y presencia en 93 mercados— comunicó la detección de un acceso no autorizado a bases de datos gestionadas por un antiguo proveedor tecnológico. Según su comunicado oficial, la información afectada se limitaba a la relación comercial con clientes en distintos mercados, no a nombres, teléfonos, domicilios, contraseñas ni datos de pago.

La compañía activó sus protocolos internos, notificó a las autoridades competentes y subrayó que sus sistemas y operaciones centrales no se vieron comprometidos. A fecha de cierre de este artículo, **no hay cifras públicas sobre el número de registros afectados ni sobre la identidad del proveedor implicado**. Todo lo que vaya más allá del comunicado corporativo es, por ahora, especulación.

El patrón: grandes marcas españolas atacadas por la puerta de al lado

El caso Inditex no llega en el vacío. Forma parte de una secuencia que debería quitar el sueño a cualquier responsable de seguridad en España.

En las últimas semanas, **Booking** ha lidiado con un incidente de naturaleza similar. **Telefónica** ha gestionado filtraciones asociadas a su ecosistema de proveedores. **Endesa** sufrió una exfiltración que, según lo trascendido, habría comprometido alrededor de 1 TB de datos con impacto estimado en unos 20 millones de personas. **Mango**, en octubre de 2025, notificó un acceso no autorizado a través de uno de los servicios externos que utilizaba para campañas de marketing.

El denominador común es demoledor: **los atacantes ya no asaltan las murallas principales; entran por el proveedor más débil con acceso autorizado**. Gestorías, plataformas de CRM, herramientas de marketing, sistemas de soporte, consultoras de datos. Son eslabones funcionales que a menudo no figuran en los mapas de riesgo del comité de dirección, pero sí en la superficie real de exposición.

Los datos agregados confirman la tendencia. El *Security Report Iberia 2026* de Check Point sitúa a España en el 2% de los ataques globales de ransomware publicados en 2025, con una media de 1.968 ciberataques semanales por organización en la región (un 70% más que en 2023). La AEPD recibió 2.765 notificaciones de brechas de datos personales en 2025, máximo histórico desde la entrada en vigor del RGPD; el 80% provino del sector privado. La propia Agencia advierte que las brechas con mayor impacto en número de afectados se originan con frecuencia en ciberataques a encargados del tratamiento —es decir, proveedores.

El marco regulatorio: ya no es una recomendación, es una exigencia

Cualquier organización española con proveedores que traten datos o gestionen sistemas críticos opera hoy bajo un triángulo normativo muy concreto.

RGPD

El artículo 33 obliga a notificar a la AEPD cualquier brecha con probable riesgo para los derechos de las personas en un plazo máximo de **72 horas** desde que se tiene conocimiento. La obligación no desaparece porque la brecha se produzca en un proveedor: si eres el responsable del tratamiento, respondes tú ante la Agencia y ante los afectados.

NIS2

La ley española de transposición, en tramitación parlamentaria durante 2026, refuerza explícitamente la gestión del riesgo en la cadena de suministro. Exige evaluación formal de proveedores críticos antes de contratar, cláusulas de seguridad en contratos, auditorías periódicas y plazos estrictos de notificación (alerta temprana en 24 h, notificación detallada en 72 h e informe final a los 30 días). La alta dirección responde personalmente del cumplimiento.

DORA

Para entidades financieras y sus proveedores TIC críticos, el reglamento europeo está plenamente vigente y establece requisitos específicos de gestión del riesgo de terceros, incluidas pruebas de resiliencia operativa.

ENS

El Esquema Nacional de Seguridad sigue siendo el referente para administraciones y sus proveedores, y cada vez más pliegos lo exigen como solvencia técnica mínima. Un proveedor sin ENS acreditado tiene hoy menos mercado público.

El efecto combinado es una cascada contractual: si trabajas con grandes empresas o con el sector público, te exigirán evidencias aunque tu organización no esté formalmente designada como esencial o importante.

Checklist operativa: seis medidas no negociables para 2026

Ningún plan defensivo se improvisa después de un incidente. Este es el mínimo razonable para cualquier CISO o responsable de riesgo:

1. Inventario y clasificación de proveedores

Mapea todos los terceros con acceso a datos o sistemas. Clasifícalos por criticidad funcional (qué ocurre si ellos caen o son comprometidos). Sin este inventario actualizado, cualquier política de terceros es ficción.

2. Due diligence previa a la contratación

Antes de firmar, evalúa la postura de seguridad real del proveedor: certificaciones vigentes (ISO 27001, ENS), historial de incidentes, arquitectura, subencargados. Documenta la decisión y revisa el expediente al renovar el contrato.

3. Cláusulas contractuales específicas

Obligación de notificación de incidentes en plazos alineados con los tuyos (no los suyos), derecho de auditoría, requisitos técnicos mínimos, control de subcontratación y penalizaciones. Sin esto, estás ciego ante lo que pase en su infraestructura.

4. Zero Trust aplicado a terceros

Accesos mínimos imprescindibles, autenticación multifactor obligatoria, segmentación de red para aislar el entorno del proveedor, revocación inmediata al terminar el servicio. La AEPD lleva años señalando que las credenciales comprometidas son el vector dominante; el segundo factor es la barrera más eficaz.

5. Auditorías y pruebas periódicas

El cuestionario de alta no basta. Revisión anual como mínimo, pruebas técnicas cuando proceda, seguimiento continuo de alertas e indicadores. Un proveedor que pasó el filtro hace tres años puede no pasarlo hoy.

6. Plan de respuesta coordinado

Protocolo conjunto con proveedores críticos: quién llama a quién, qué se comunica, cómo se preservan evidencias, qué canales se activan con la AEPD, el CCN-CERT y el INCIBE-CERT. Simulacros anuales. Lo que no se ensaya, no funciona el día que hace falta.

Reflexión estratégica: la superficie ya no termina en tu perímetro

Durante años, la ciberseguridad corporativa se dibujó como una muralla alrededor de lo propio. Ese mapa mental ya no sirve. La superficie de ataque real de cualquier organización incluye a sus proveedores, a los proveedores de sus proveedores y a cada integración técnica entre ellos.

El caso Inditex no es una anomalía. Es la normalización de una táctica que los atacantes llevan años refinando: buscar el eslabón más barato con el mejor acceso. La respuesta, por tanto, no es puramente técnica. Es de gobernanza. Implica contratos, procesos, responsabilidades, presupuesto y formación en el comité de dirección.

La pregunta útil ya no es si tu empresa está preparada para defenderse. Es **si está preparada para responder cuando el incidente ocurra —en tu casa o en la de alguien que trabaja para ti—** dentro de los plazos que impone la ley.

Siguiente paso

Si diriges seguridad, riesgo o cumplimiento en una empresa española, tienes esta semana una ventana razonable para auditar dos cosas: los contratos vigentes con tus proveedores críticos y tu capacidad real de notificación en 72 horas. No esperes a la próxima portada.

¿Quieres profundizar? Suscríbete al blog para recibir cada semana análisis de incidentes reales y marcos prácticos de cumplimiento NIS2, DORA y RGPD aplicados a la cadena de suministro.

Isaac Ruiz Romero.