

Una brecha cuesta de media **4,44 millones de euros.**

Y hay cuatro factores que la encarecen. ¿Cuántos se dan en su empresa?

Consultoría Tecnológica y Ciberseguridad

forvis mazars



Donde se va el dinero

El coste de una brecha no es la multa

Casi dos tercios del coste se van en detectar y escalar el incidente y en el negocio que se pierde por el camino.

Detección y escalado

Investigar qué ha pasado, hasta dónde ha llegado y quién debe decidir.

Negocio perdido

Paradas, clientes que se van y daño a la reputación.

Notificación

Avisar a supervisores, autoridades y afectados en plazo.

Respuesta posterior

Recuperar sistemas, asesoría legal, atención a clientes y sanciones.

En azul oscuro, las dos partidas que suman casi dos tercios del coste.

Fuente: IBM y Ponemon Institute, Cost of a Data Breach Report 2026. Importes en dólares.

Factor 1 de 4

El tiempo

247 días de media para detectar y contener una brecha.

+1,18 M€ cuesta de más una brecha que supera los 200 días: 5,03 M€ frente a 3,85 M€.

LA PREGUNTA INCÓMODA

¿Sabe cuánto tardaría su empresa en detectar una intrusión?

Fuente: IBM y Ponemon Institute, Cost of a Data Breach Report 2026. Importes en dólares.

Factor 2 de 4

N.º 1

de los 30 factores analizados por IBM, el compromiso de un socio o proveedor es el que más encarece una brecha.

258 días

para detectar y contener una brecha que entra por la cadena de suministro.

LA PREGUNTA INCÓMODA

¿Cuándo comprobó por última vez la seguridad real de sus proveedores críticos?

Fuente: IBM y Ponemon Institute, Cost of a Data Breach Report 2026. Importes en dólares.

Factor 3 de 4

1 de 4 brechas maliciosas ya utiliza la IA: suplantaciones con deepfakes y malware.

+900 K€ de coste medio adicional en los ataques impulsados por IA.

LA PREGUNTA INCÓMODA

¿Reconocería su equipo una videollamada falsa de su CEO?

Fuente: IBM y Ponemon Institute, Cost of a Data Breach Report 2026. Importes en dólares.

Factor 4 de 4

El incumplimiento normativo

4 horas

para la notificación inicial con DORA desde que el incidente se clasifica como grave.

72 horas

para notificar a la autoridad de protección de datos con el RGPD. Incumplir los plazos está entre los factores que más encarecen una brecha.

LA PREGUNTA INCÓMODA

¿Sabe quién firma la notificación al supervisor en las primeras horas?

Fuente: IBM y Ponemon Institute, Cost of a Data Breach Report 2026. Importes en dólares.



Como lo reducimos

Cada uno de estos factores se puede reducir antes de la brecha

El tiempo	Ejercicios de crisis (tabletop) y planes de respuesta probados.
Los proveedores	Auditoría técnica de proveedores (TPRM) y pentesting.
Los ataques con IA	Simulaciones de ingeniería social con deepfakes y AI Red Teaming.
La normativa	Circuito de decisión y notificación para DORA, NIS2 y RGPD.

Contactos

Luis Reinoso

Director de Consultoría Tecnológica y Ciberseguridad

luis.reinoso@forvismazars.com

Forvis Mazars es la marca de la red Forvis Mazars Global (Forvis Mazars Global Limited), una red mundial de servicios profesionales. La red opera bajo una única marca en todo el mundo, con sólo dos miembros: Forvis Mazars, LLP en Estados Unidos y Forvis Mazars Group SC, una asociación internacional integrada que opera en más de 100 países y territorios.

Las entidades de la red Forvis Mazars en España prestan servicios de auditoría & assurance, asesoramiento fiscal, legal, financiero, consultoría, outsourcing y sostenibilidad a través de más de 900 profesionales en 8 oficinas.

Visita forvismazars.com/es para conocer más.

© Forvis Mazars 2026. Todos los derechos reservados.