MARSH

Redefining cybersecurity strategy for frontier risks

La aceleración tecnológica amplía la exposición a riesgos frontera como IA, OT/IoT, la cadena de sumnistro y computación cuántica. Para la Alta Dirección, la prioridad es pasar de una postura reactiva a una estrategia integrada que cuantifique el riesgo, fortalezca la resiliencia y asegure el ecosistema tecnológico.

1

Los riesgos frontera ya impactan el negocio

30% de incidentes analizados por Verizon se vinculó con terceros o cadena de suministro. 60% de profesionales TI indica no estar preparado ante amenazas generadas por IA.

2

La exposición es dinámica y sistémica

IA, OT/IoT, cadena de sumnistro y computación cuántica cambian rápido, tienen alta incertidumbre y pueden multiplicar impactos entre proveedores, clientes y operaciones.

3

Gobernanza cuantificada para decidir mejor

FAIR, comités RACI, MITRE/CTEM y marcos NIST/ISO/ATT&CK ayudan a traducir incertidumbre en inversión priorizada, responsables y criterios de aceptación.

4

Resiliencia operativa, no respuesta aislada

Informes, backups inmutables, RTO/RPO, equipo rojo, búsqueda de amenazase integración SOC-proveedores 24x7 reducen tiempo de detección, contención y recuperación.

5

Arquitectura segura y ecosistema controlado

Identidad como perímetro, Zero Trust, microsegmentación, CSPM/CNAPP, DevSecOps, SBOM, VRM/TPRM y cifrado post-cuántico reducen el riesgo operativo y de terceros.