PREPARADOS PARA EL RIESGO O EXPUESTOS AL RIESGO:

COHESITY

La Brecha de Ciberresiliencia en la Atención Médica

Los ciberataques ya no son sucesos aislados, sino una característica constante de nuestro mundo digital. Cada día trae un nuevo recordatorio, ya que las organizaciones sanitarias de todo el mundo son cada vez más blanco de ataques. Ninguna organización es inmune, y la creciente frecuencia y sofisticación de las amenazas han provocado un aumento de los ciberataques que causan daños cuantificables a nivel financiero, operativo y de reputación.

UNA ENCUESTA GLOBAL REALIZADA A CASI 400 RESPONSABLES DE LA TOMA DE DECISIONES EN MATERIA DE TI Y SEGURIDAD EN ORGANIZACIONES SANITARIAS REVELA ESTA REALIDAD:

85 %
de las organizaciones sanitarias han sufrido un ciberataque importante

66 %
se vieron afectados en los últimos 12 meses

1 de cada 3
ha sido atacado multiples veces

LOS DAÑOS SON PROFUNDOS Y LOS COSTOS SE ACUMULAN RÁPIDAMENTE

92 % perdió ingresos

59 % perdió pacientes o clientes

80 % de las organizaciones sanitarias que cotizan en bolsa tuvieron que revisar sus directrices financieras

97 % se enfrentó a consecuencias regulatorias o legales

94 % pagó un rescate en los últimos 12 meses

AUN CON LAS PRUEBAS A LA VISTA, MUCHAS ORGANIZACIONES SANITARIAS SOBREESTIMAN SU CAPACIDAD DE RESILIENCIA.

49 %
tiene plena confianza en su estrategia de ciberresiliencia

LA MAYORÍA SIGUE DANDO PRIORIDAD A LA PREVENCIÓN Y LA DETECCIÓN POR ENCIMA DE LAS FUNCIONES IGUALMENTE CRUCIALES DE RESPUESTA Y RECUPERACIÓN.

Pedido basado en el marco de ciberseguridad del NIST.
El tamaño de los recuadros muestra la proporción de inversiones en ciberresiliencia de mayor a menor.

#2	#1	#3	#4	#5
Identificar	Proteger	Detectar	Responder	Recuperar

LA CONFIANZA Y LOS PATRONES DE GASTO SOLO CUENTAN UNA PARTE DE LA HISTORIA

La verdadera resiliencia depende de las prácticas y capacidades que la respaldan. Al evaluarlas según criterios de rendimiento reales, solo el 2 % de las organizaciones sanitarias demuestran madurez en cinco áreas esenciales: **protección de datos, recuperación de datos, detección e investigación de amenazas, resiliencia de las aplicaciones y optimización del riesgo de los datos.**

La creciente conciencia sobre la necesidad de mejorar la resiliencia está impulsando la próxima evolución, impulsada por la automatización y la inteligencia artificial. A medida que las amenazas se vuelven más rápidas y complejas, la automatización es clave para acelerar la detección, optimizar la respuesta y fortalecer la recuperación.

61 %

afirma que una mejor automatización en la detección, respuesta y recuperación es una de las principales lecciones aprendidas tras el ciberataque

37 %

cree que la IA desempeñará un papel central en la forma en que detectan y responden a las amenazas, incluyendo la toma de algunas decisiones autónomas

99 %

planea utilizar IA para respaldar las operaciones de seguridad de datos para 2026

¿ESTÁ PREPARADO PARA ASUMIR RIESGOS?

- **Descargue el informe sobre la ciberresiliencia del sector sanitario para obtener conclusiones detalladas.**
- **Reserve un Taller sobre Resiliencia ante el Ransomware.**
- Obtenga nuestro eBook "**Cinco Pasos para la Ciberresiliencia**" y comience a desarrollar su madurez digital hoy mismo.

Vanson Bourne encuestó a 3200 líderes de TI y seguridad de las regiones de Norteamérica, Asia-Pacífico, Europa y Latinoamérica, que representan a organizaciones con 1000 o más empleados en 2025. Entre los encuestados se encontraban 371 participantes de organizaciones sanitarias.

COHESITY VansonBourne

COHESITY
cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054
6200029-001-ES 4-2026