

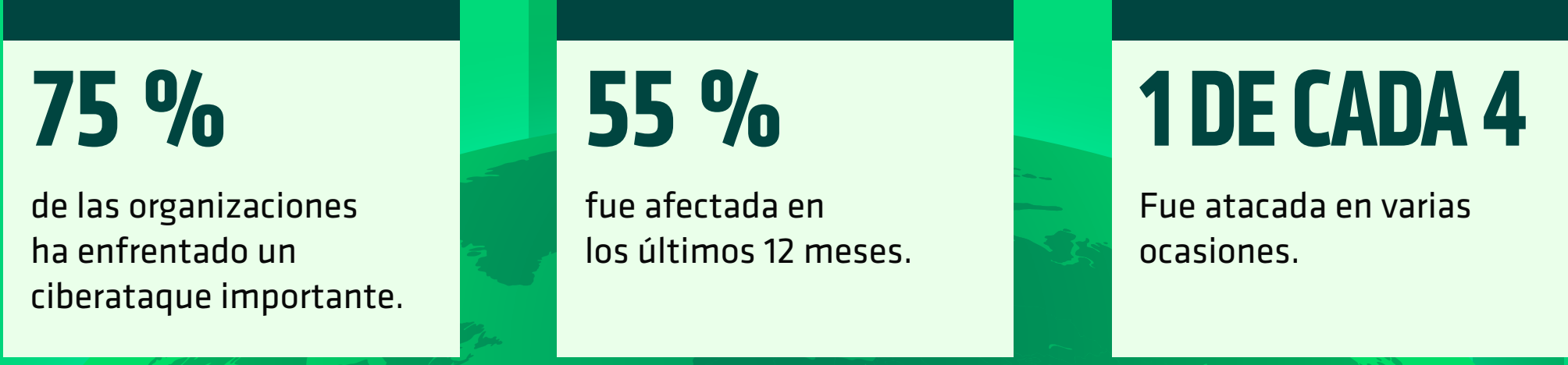
PREPARADAS PARA EL RIESGO O EXPUESTAS AL RIESGO

La brecha de resiliencia cibernética en organizaciones medianas

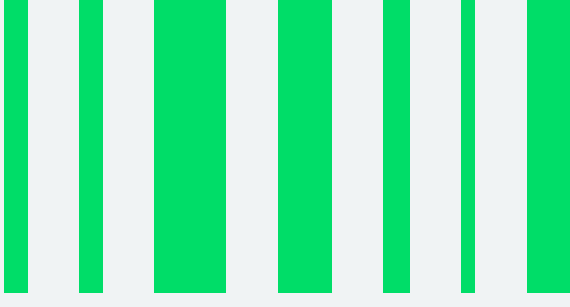


Los ciberataques ya no son eventos aislados, sino una característica duradera de nuestro mundo digital. Cada día trae un nuevo recordatorio, ya que las organizaciones medianas de todo el mundo son el objetivo de ataques con mayor frecuencia. Ningún negocio es inmune, y la creciente frecuencia y sofisticación de las amenazas ha provocado un aumento en los ciberataques materiales que causan daños financieros, operativos y de reputación medibles.

UNA ENCUESTA GLOBAL REALIZADA A CASI 1000 RESPONSABLES DE LA TOMA DE DECISIONES DE TI Y OPERACIONES DE SEGURIDAD DE ORGANIZACIONES DE ENTRE 1000 A 1999 EMPLEADOS REVELA LA REALIDAD.



EL DAÑO ES PROFUNDO Y LOS COSTOS SE ACUMULAN RÁPIDAMENTE.



INCLUSO CON LA EVIDENCIA A SIMPLE VISTA, MUCHAS ORGANIZACIONES SOBRESTIMAN SU RESILIENCIA.



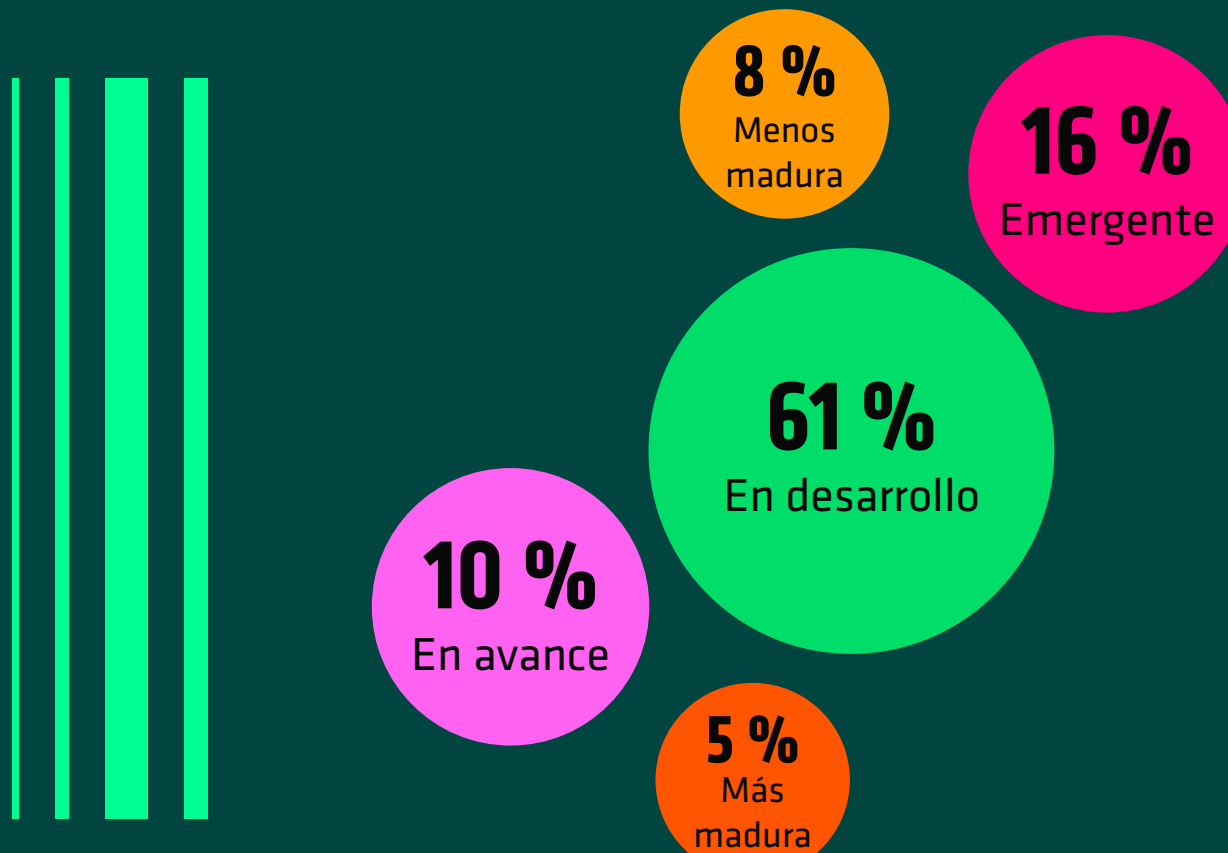
LA MAYORÍA AÚN PRIORIZA LA PREVENCIÓN Y LA DETECCIÓN SOBRE LAS FUNCIONES IGUALMENTE CRÍTICAS DE RESPUESTA Y RECUPERACIÓN.

Ordenado según el marco de ciberseguridad del NIST. El tamaño del cuadro muestra la proporción de inversiones en resiliencia cibernética, de mayor a menor.



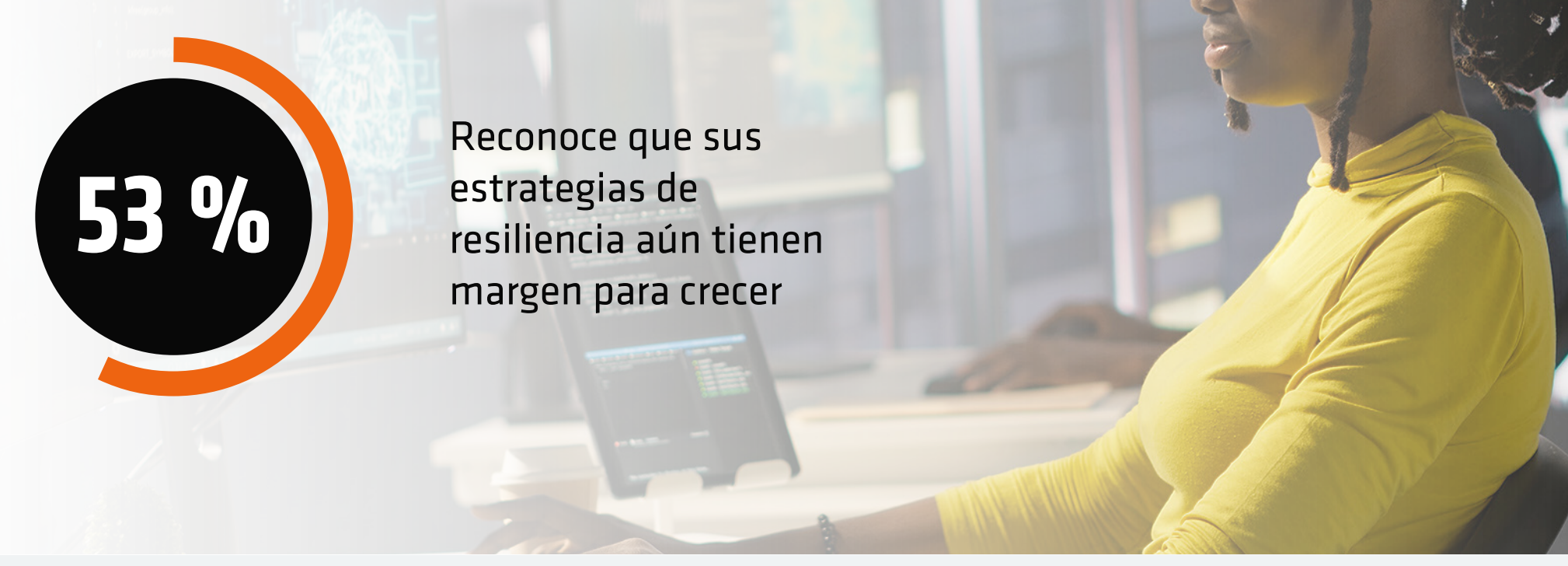
LA CONFIANZA Y LOS PATRONES DE GASTO SOLO CUENTAN PARTE DE LA HISTORIA

La verdadera resiliencia depende de las prácticas y capacidades que las respaldan. Cuando se evalúan en función de criterios de desempeño del mundo real, solo el 5 % de las organizaciones demuestra madurez en cinco áreas esenciales: **protección de datos, recuperación de datos, detección e investigación de amenazas, resiliencia de aplicaciones y optimización del riesgo de datos.**



Para las organizaciones más resilientes cibernéticamente, la resiliencia es sistemática e integral. Entre otras mejores prácticas, se aseguran de que los datos confidenciales se respalden globalmente, se apliquen la autenticación multifactor y los controles administrativos, se maximice la inteligencia de amenazas, se asegure la recuperación a través de la corrección y se cumplan sistemáticamente las medidas de seguridad de cumplimiento.

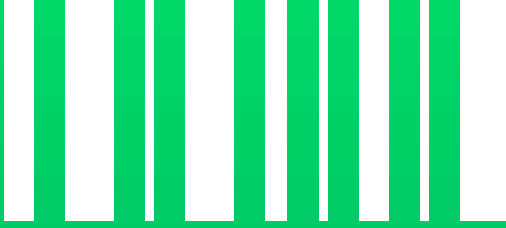
PERO LA MADUREZ NO ES ESTÁTICA.



Tomar conciencia sobre la necesidad de mejorar la resiliencia está impulsando la próxima evolución, fomentada por la automatización y la IA. 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.



¿ESTÁ PREPARADO PARA EL RIESGO?



- Obtenga información sobre **las soluciones de resiliencia cibernética de Cohesity** para **organizaciones medianas**.
- Evalúe la **madurez de su resiliencia cibernética** con esta **tarjeta de puntuación de resiliencia**
- Suba de nivel con un **plan de acción de resiliencia cibernética de cinco pasos**

Vanson Bourne encuestó a 3200 líderes de TI y seguridad de América del Norte, Asia-Pacífico, Europa y América Latina, que representan a organizaciones con 1000 empleados o más en 2025. Los encuestados incluyeron a 977 participantes de organizaciones medianas de entre 1000 y 1999 empleados.