

OTRS Spotlight: Seguridad Corporativa 2024

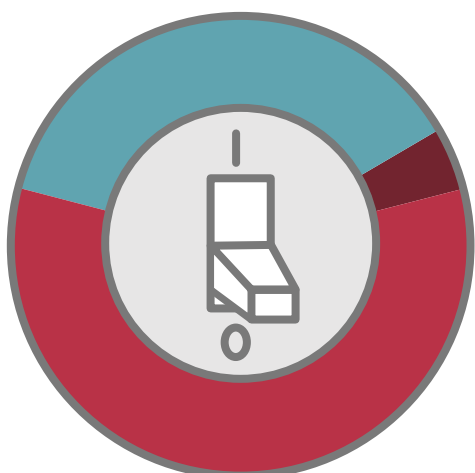
Parte 1: Las Consecuencias de CrowdStrike

93%

Después del incidente de CrowdStrike, el 93 % de las empresas aumentaron sus precauciones de seguridad.

- 45 % Diversificamos nuestro panorama de TI y software para depender menos de un único proveedor de software.
- 40 % Implementamos sistemas avanzados de monitoreo y alerta en tiempo real.
- 39 % Introdujimos pruebas adicionales para nuevos parches y actualizaciones.
- 39 % Implementamos o actualizamos nuestro plan de respuesta a incidentes.
- 36 % Implementamos o actualizamos nuestros planes de recuperación ante desastres y de respaldo.
- 26 % Pasamos a implementaciones por etapas para parches y actualizaciones.
- 24 % Implementamos la gestión unificada de terminales (UEM, por sus siglas en inglés).
- 17 % Desactivamos las actualizaciones automáticas de todo nuestro software.
- 4 % No tomamos ninguna medida y 3 % No sé.

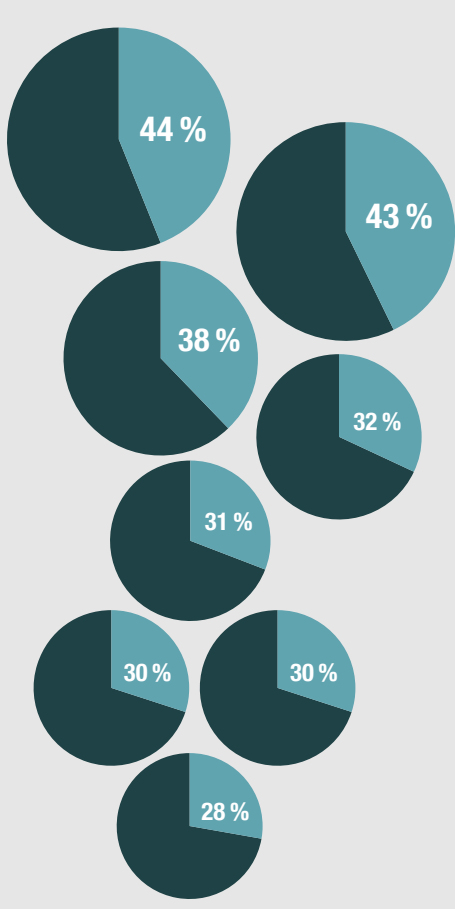
Si bien no todas las organizaciones se vieron directamente afectadas por el incidente de CrowdStrike, fue una llamada de atención para la mayoría para intensificar su seguridad informática.



¿Alguno de los sistemas de su organización se vio afectado por la interrupción de TI causada por la actualización defectuosa implementada por CrowdStrike en julio de 2024?

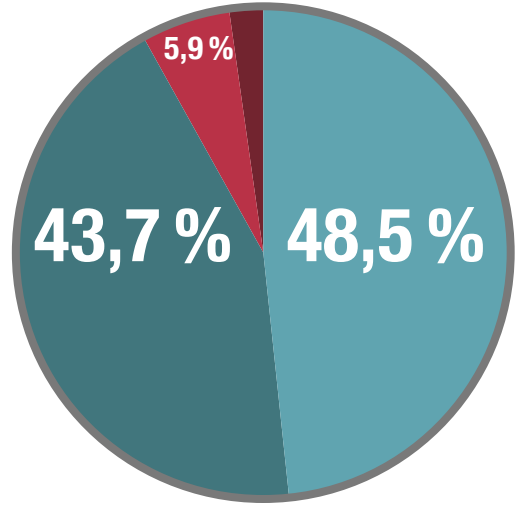
- 58,2 % Sí.
- 37,4 % No.
- 4,4 % No sé.

Sólo algunas de las directamente afectadas estaban preparadas para mitigar el impacto del incidente de CrowdStrike utilizando sus propios recursos.



- 44 % Seguimos los **pasos de remediación** descritos por CrowdStrike tan pronto como estuvieron disponibles.
- 43 % Instalamos la **solución implementada por CrowdStrike** tan pronto como estuvo disponible.
- 38 % Usamos **sistemas avanzados de monitoreo y alerta en tiempo real**, que nos permitieron intervenir rápidamente.
- 32 % Contamos con sólidos **mecanismos de reversión, recuperación ante desastres y copias de seguridad** que nos permitieron revertir rápidamente nuestros sistemas a una versión estable.
- 31 % Usamos **gestión unificada de terminales (UEM)**, que nos permitió identificar rápidamente los sistemas afectados e iniciar las medidas adecuadas para mitigar el impacto (de forma remota).
- 30 % Contamos con un **sólido plan de respuesta a incidentes** que nos ayudó a identificar, aislar y resolver rápidamente el problema.
- 30 % Generalmente realizamos **pruebas previas a la implementación para parches y actualizaciones nuevos**, lo que nos permitió detectar el defecto e intervenir rápidamente.
- 28 % Generalmente realizamos **implementaciones por etapas**, lo que significó que sólo unos pocos sistemas se vieron afectados por el incidente.

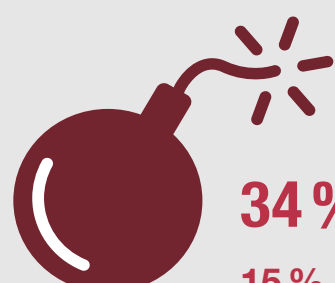
Un festín para los atacantes: la mitad de todos los equipos de seguridad no consideran que su organización esté óptimamente preparada para los incidentes de seguridad.



¿Qué tan preparada está su compañía en caso de un incidente de seguridad?

- 48,5 % Óptimamente.
- 43,7 % Aceptablemente.
- 5,9 % No lo suficiente.
- 1,9 % No sé.

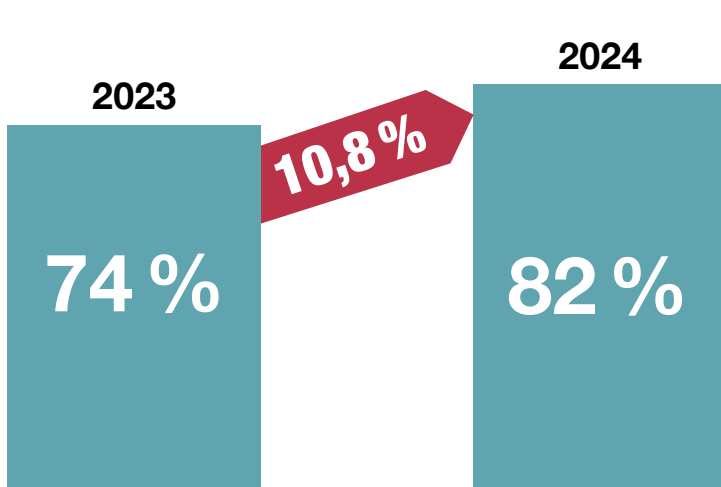
Los 5 principales desafíos que enfrentan los equipos de seguridad durante la respuesta a incidentes:



34 % Rápida evolución de las amenazas

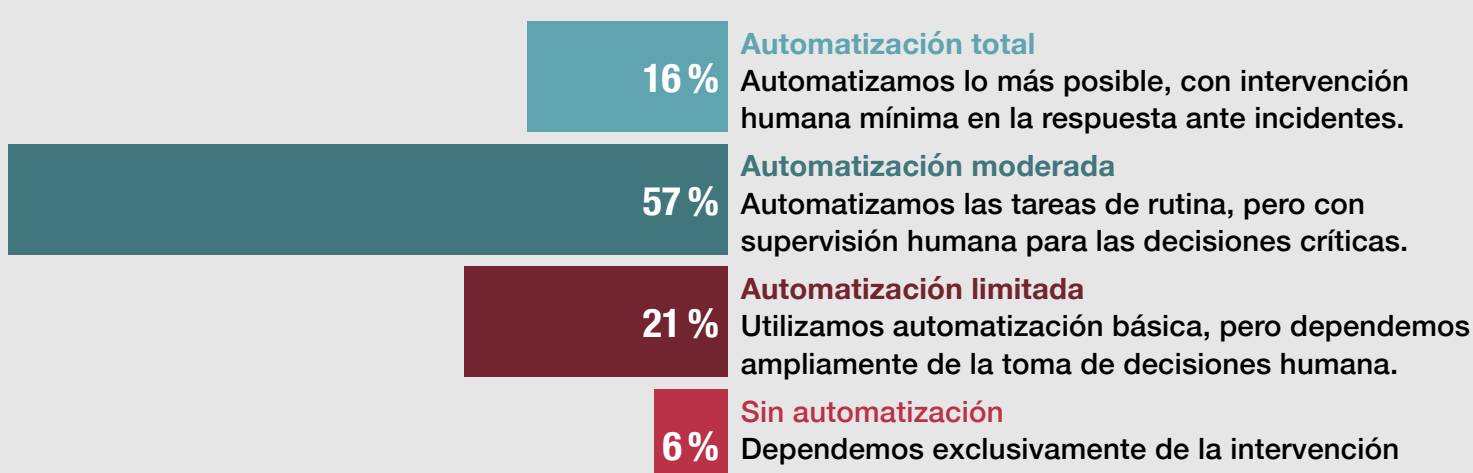
- 15 % Realizar revisiones exhaustivas posteriores a los incidentes
- 12 % Falta de personal capacitado
- 12 % Comunicación oportuna y apropiada con el público
- 12 % Déficit de integración entre las herramientas

La cantidad de incidentes de seguridad aumenta cada año, lo que dificulta que los equipos de seguridad sigan el ritmo de los atacantes.



”Sí. Hemos observado un aumento en incidentes de seguridad.”

Al automatizar sus procesos de respuesta a incidentes, los equipos de seguridad tienen una mejor oportunidad de seguir el ritmo de las amenazas que evolucionan rápidamente.



Los datos utilizados para el estudio se basaron en una encuesta en línea conducida por Pollfish Inc. en nombre de OTRS AG, en la cual 476 profesionales de TI y ciberseguridad de EUA, Alemania, Brasil, México, Australia y Malasia participaron entre el 22 de agosto y el 17 de septiembre de 2024. A menos que se indique lo contrario, todas las cifras se refieren al promedio de todos los países encuestados.

