

Transformación Digital y Ciberseguridad en la Operación

Panel de responsables de áreas operativas de UTE

Participan:

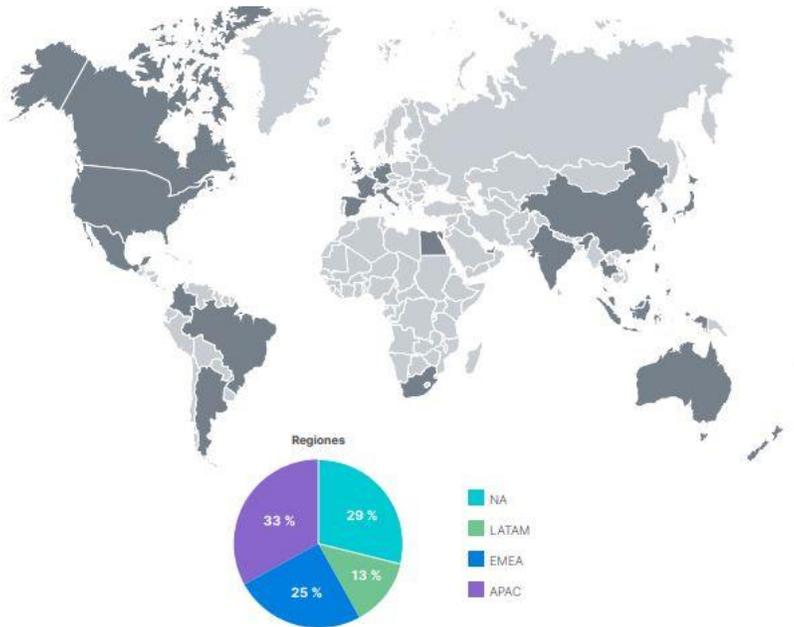
Ing. Michel Levinsky
Ing. Jorge Costa

SETIEMBRE 2022

FORTINET

INFORME

Informe sobre el estado de la tecnología operativa y la ciberseguridad en 2022



El Informe sobre el estado de la tecnología operativa y la ciberseguridad en 2022, en su cuarta edición anual, está basado en una encuesta mundial realizada a más de 500 profesionales de seguridad de TO y revela que las organizaciones siguen avanzando con demasiada lentitud hacia la plena protección de sus activos de tecnología operativa (TO).

Esto llega en un momento en el que los sistemas de TO son cada vez más importantes para el bienestar de muchas organizaciones, los acontecimientos geopolíticos hacen que los ataques sean más probables, se conectan más sistemas de TO a Internet y las amenazas basadas en IP son cada vez más avanzadas y causan más daño. Esta combinación de factores hace que la seguridad de TO aumente en la cartera de riesgos de muchas organizaciones.

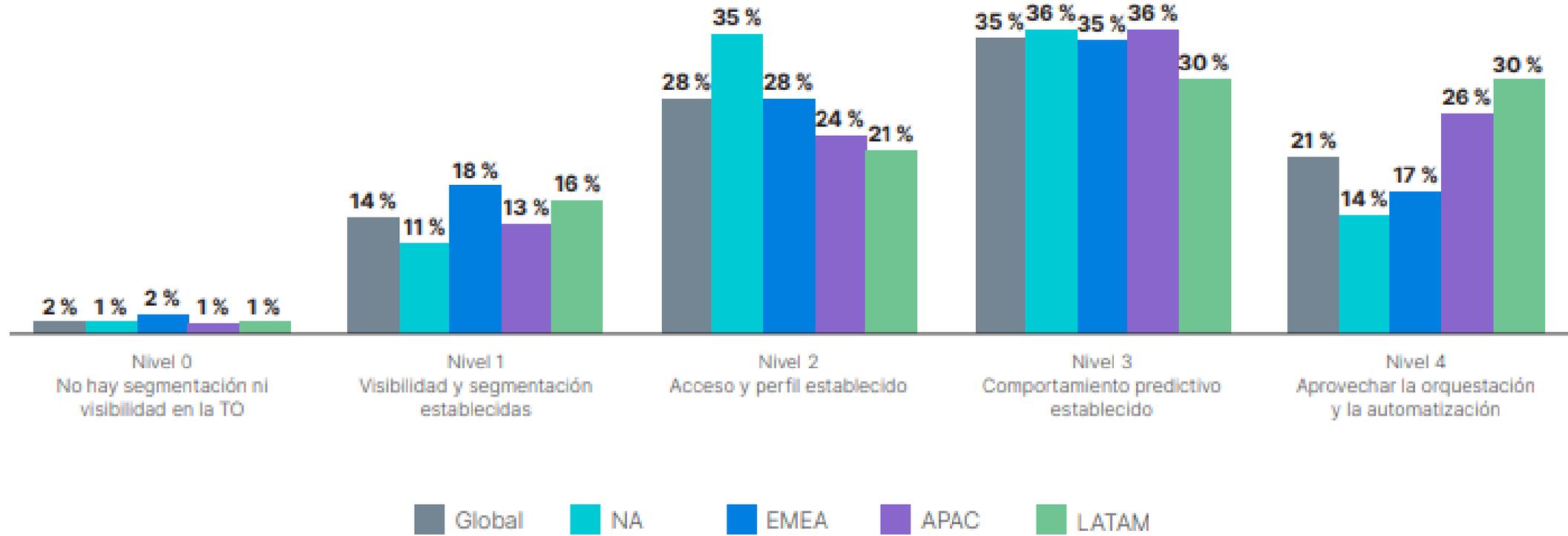


Figura 13: Nivel de madurez de la postura de ciberseguridad de TO.

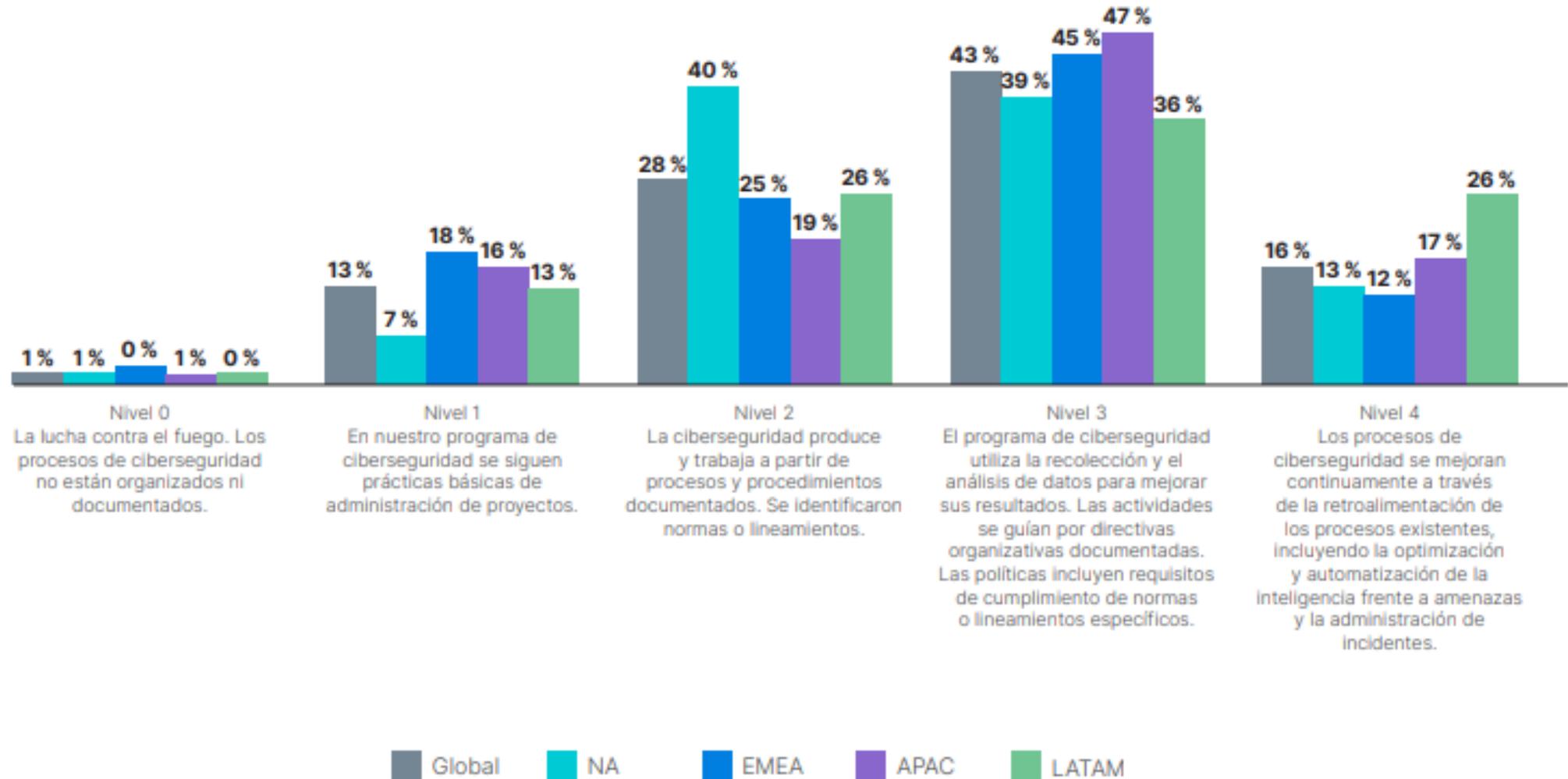


Figura 15: Nivel de madurez del programa general de ciberseguridad.

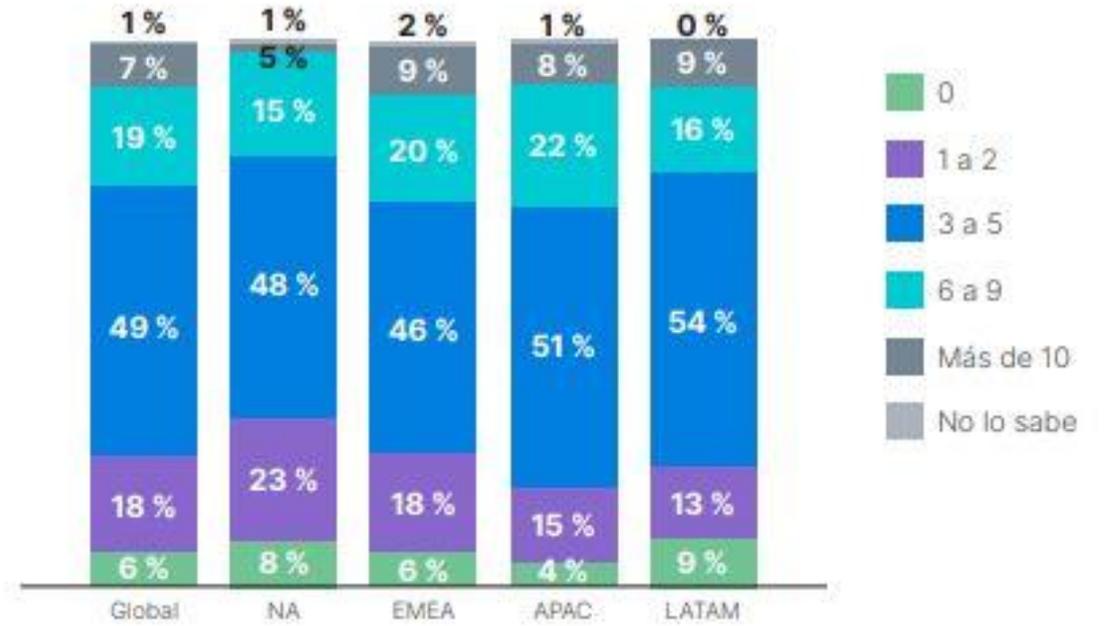
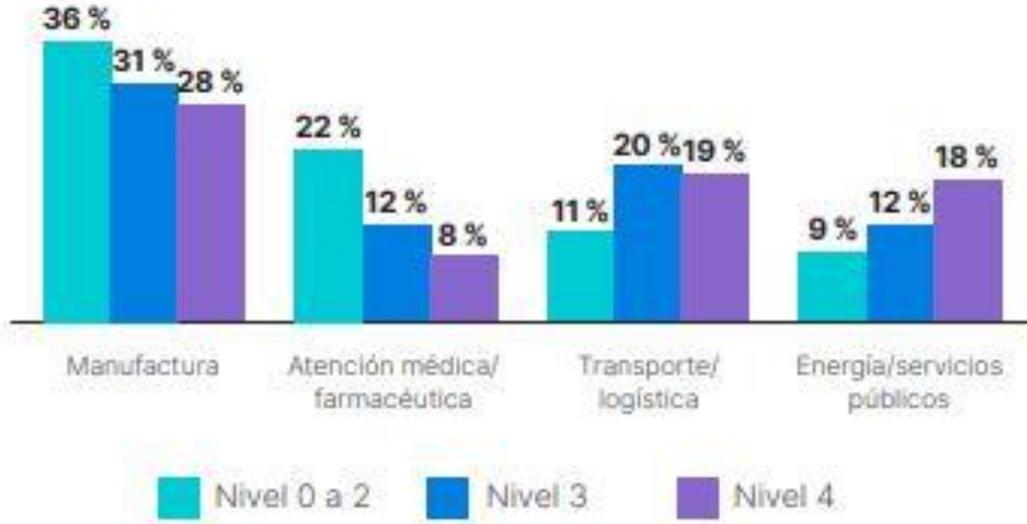


Figura 26: Cantidad de intrusiones durante el último año.

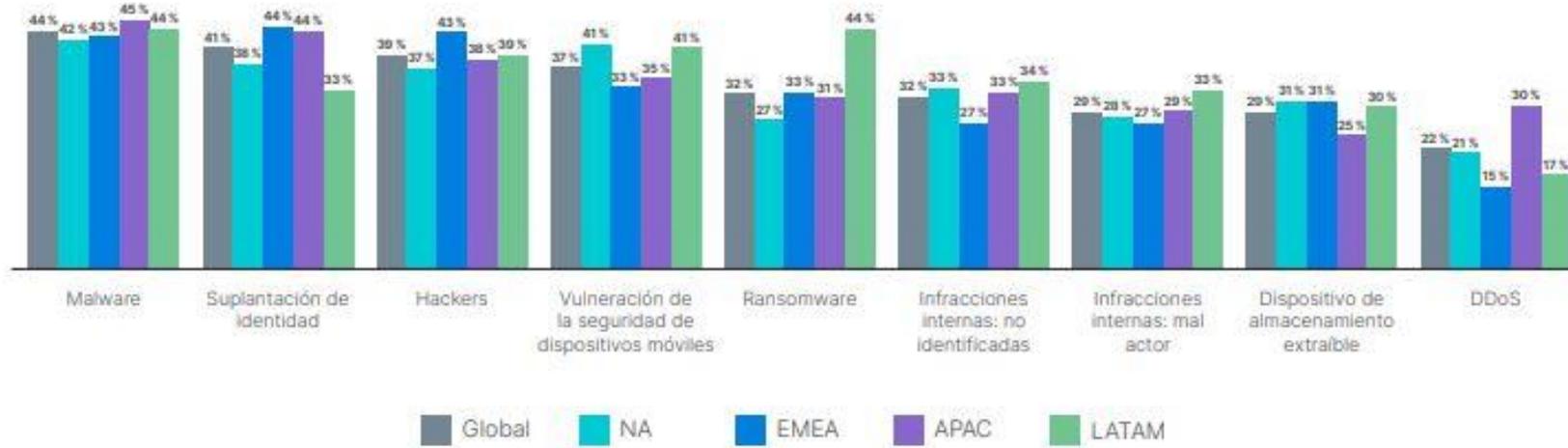


Figura 28: Tipos de intrusiones experimentadas.

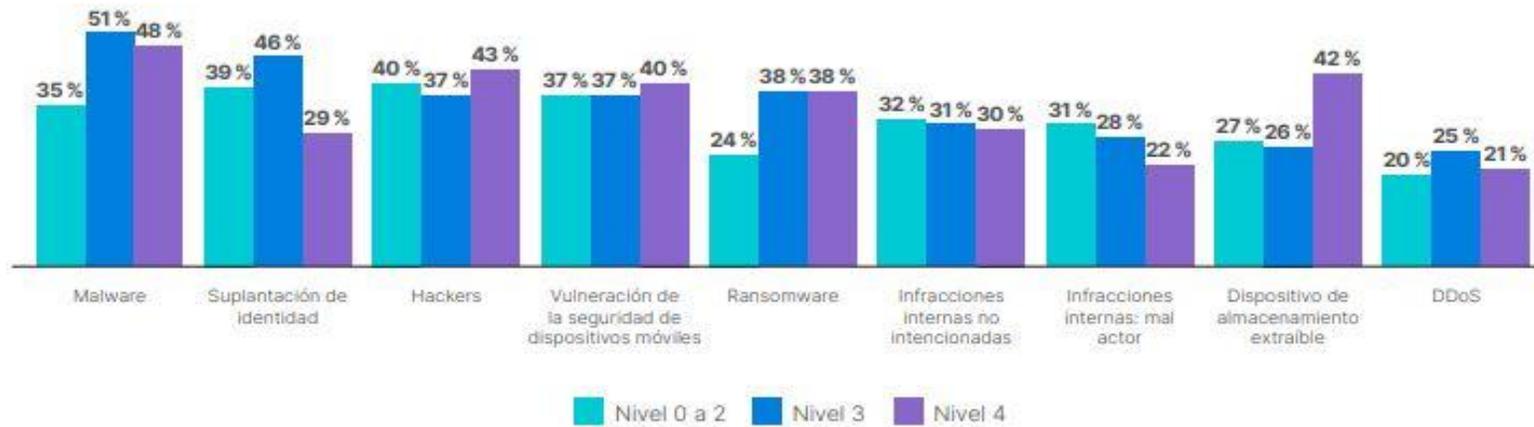


Figura 30: Tipos de intrusiones experimentadas por el nivel de madurez de seguridad informada.

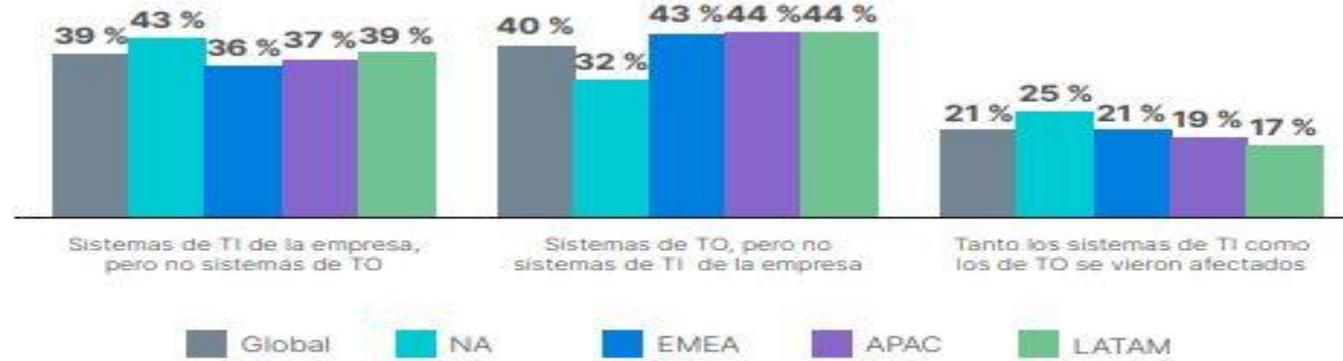


Figura 31: Entornos afectados por las intrusiones.

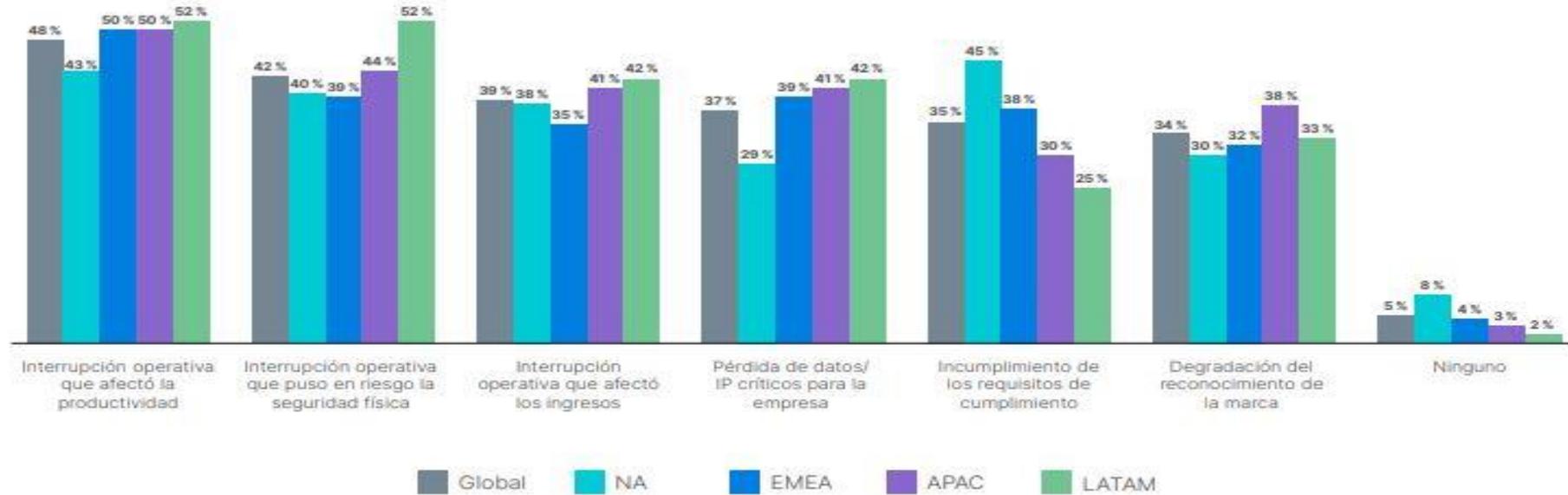


Figura 32: Impactos organizacionales de las intrusiones.

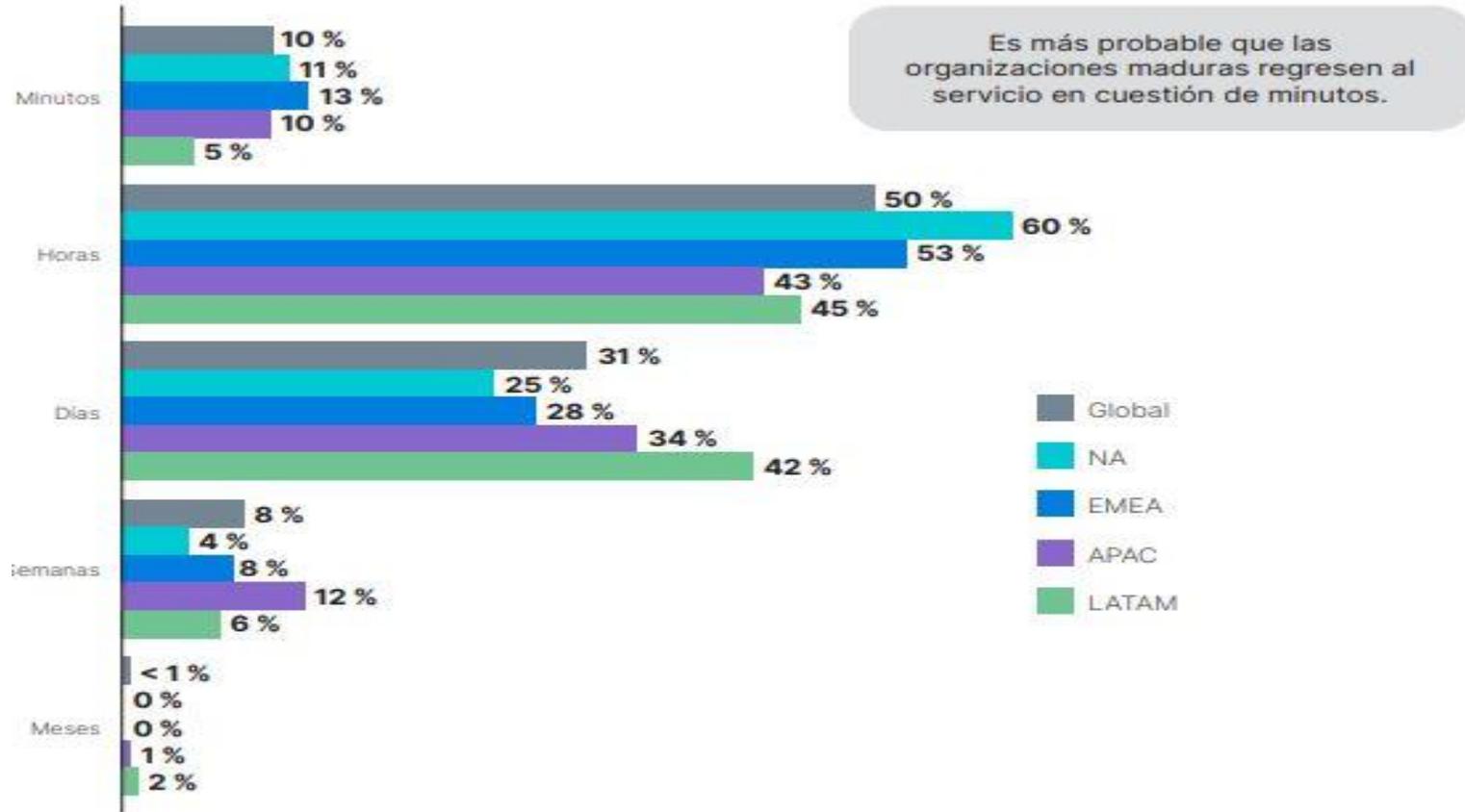


Figura 33: El tiempo de regreso al servicio más largo después de una intrusión.

Personas



33 % de las organizaciones confían la seguridad de TO al vicepresidente/director de ingeniería/operaciones de redes



67 % de los líderes de seguridad de TO tienen experiencia en ingeniería de TO



43 % de los encuestados considera que el tiempo de respuesta a incidentes de seguridad es una de las tres principales medidas de éxito

Postura de seguridad



56 % de las organizaciones reportan que se encuentran en el nivel 3 o 4 de madurez de seguridad de TO



50 % dice que la postura de seguridad de TO es un factor significativo en la puntuación de riesgo general



13 % de las organizaciones tiene visibilidad centralizada de todas las actividades de TO

Prácticas de seguridad



48 % informa a la dirección ejecutiva de las vulneraciones de seguridad



32 % implementó un control de acceso a la red basado en funciones



52 % afirma que el SOC monitorea y les da seguimiento a las actividades de TO

Resultados de seguridad



93 % de las organizaciones tuvo más de 1 intrusión el año pasado;
78 % tuvo más de 3



61 % de las intrusiones afectaron a los sistemas de TO



90 % de las intrusiones tardaron horas o más para restablecer el servicio

Mejores prácticas

Es más factible que las organizaciones top-tier:

- Tengan una visibilidad centralizada
- Se midan por el tiempo de respuesta a la vulnerabilidad
- Implementen NAC basado en funciones
- Reporten compromisos a la seguridad
- Tengan un único proveedor de dispositivos TO

No nos consultaron, pero... qué hubiera respondido UTE?

