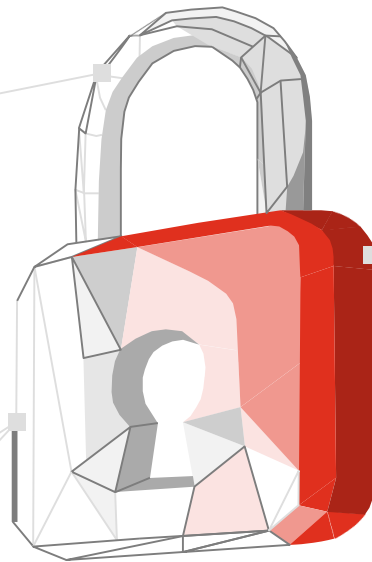


Los CISOs ante la prueba extrema de resiliencia. Plan para emerger más fuerte

Digital Trust Insights Pulse Survey Findings 2020



Resumen

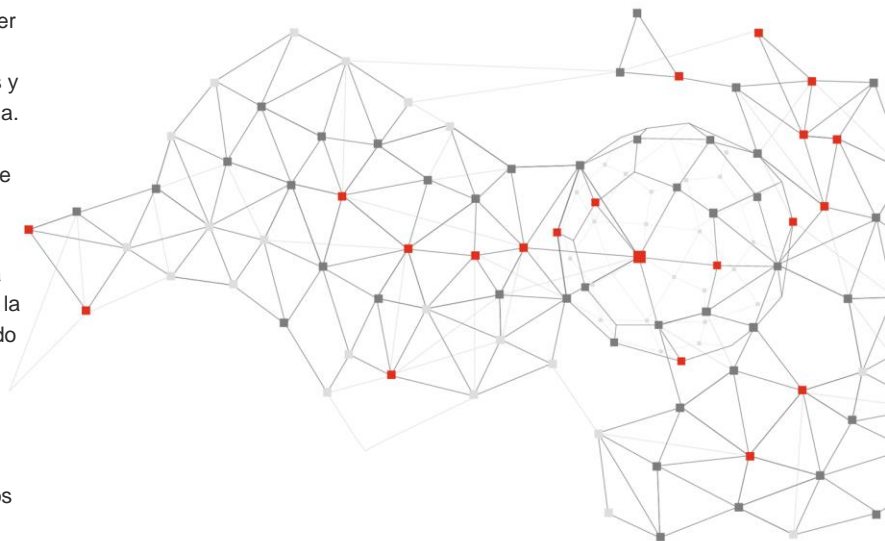
La encuesta de confianza de Digital Trust Insights de PwC a 114 líderes de seguridad e información es similar a un informe posterior a la acción sobre las primeras respuestas a la pandemia de COVID-19. ¿Cómo resistieron esta prueba extrema de resistencia? ¿Cómo están repensando su estrategia e inversiones en el futuro?

La economía digital apoyó a toda la economía cuando las empresas cerraron sus lugares de trabajo durante el brote de coronavirus. Las empresas tecnológicas y las empresas nativas digitales proporcionaron la columna vertebral, mientras que otras empresas aceleraron la digitalización, incluida la automatización, la adopción de la nube, el teletrabajo, entre otros.

Los ejecutivos que en el pasado pudieran haber preguntado sobre el retorno de la inversión a todo el personal de ciberseguridad, soluciones y arquitecturas, ya no lo harán de la misma forma. El valor de sus gastos en ciberseguridad a lo largo de los años, y del liderazgo del CISO - Se volvió claro como el cristal durante esta crisis.

Hoy, los CISO y los CIO se están adaptando a un futuro diferente. Todos planean cambios en la estrategia de ciberseguridad y están priorizando las inversiones.

Los CISO y CIO deben desempeñar un papel importante a medida que las empresas persiguen los mismos objetivos en los próximos meses: aceleran los modelos digitales y se restaura la salud financiera de las organizaciones.



Sobre la encuesta

Digital Trust Insights Pulse Survey 2020



114

ejecutivos de
seguridad y
tecnología (CISO,
CIO y títulos
similares).



Recolección de resultados
28 de julio y el 18 de agosto
de 2020.



Centroamérica y
República Dominicana.

Participaron empresas
pequeñas, medianas y
grandes.



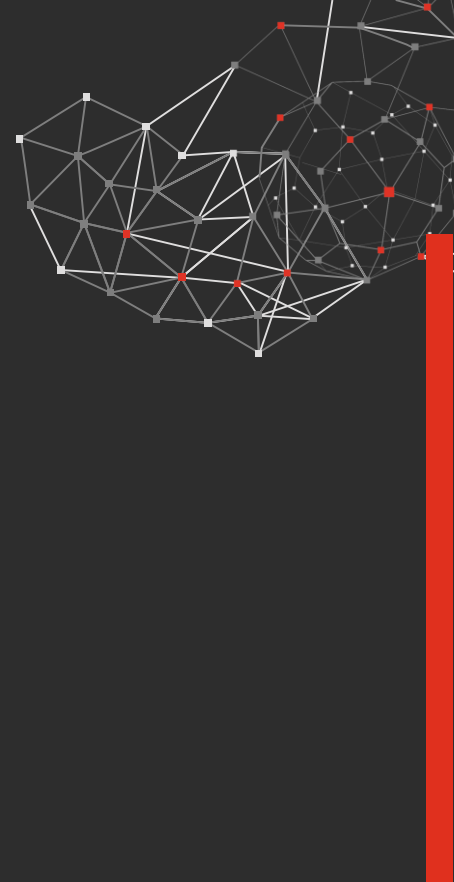
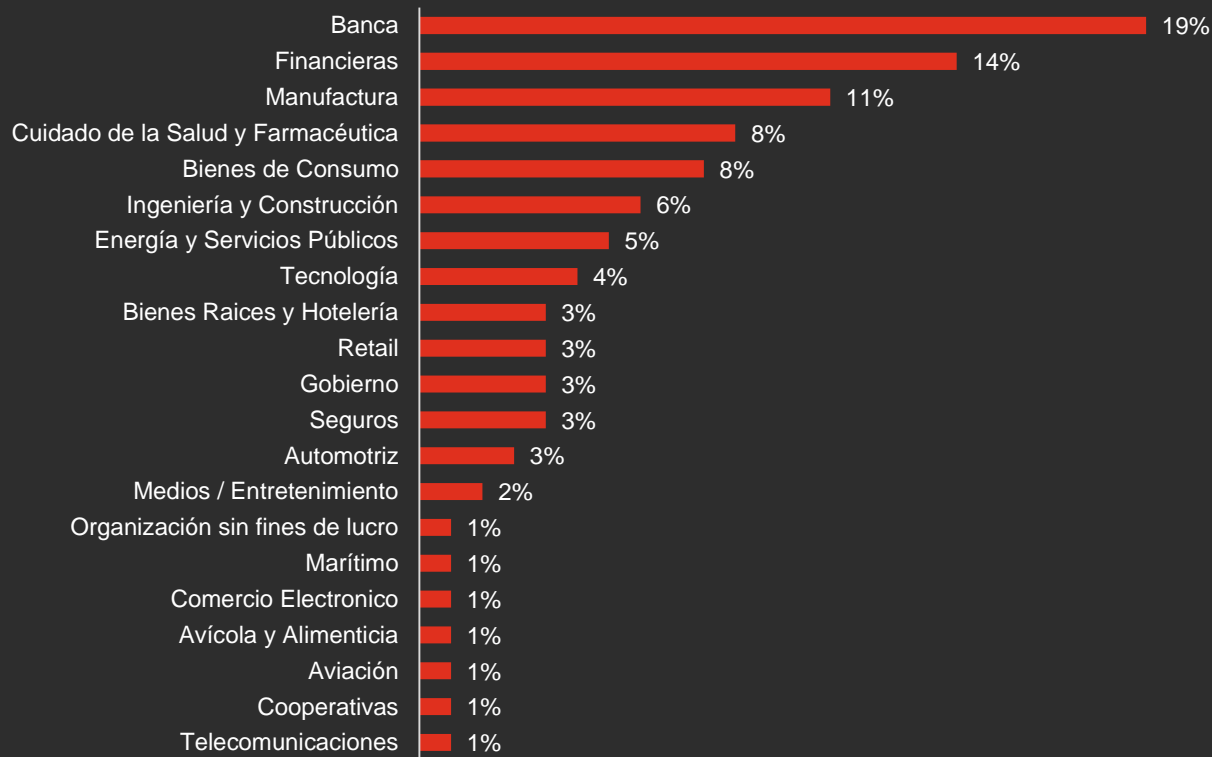
114 líderes de **tecnología y TI** de Centroamérica y República Dominicana fueron encuestados para obtener sus puntos de vista sobre cómo las estrategias de ciberseguridad y privacidad pueden cambiar como resultado de COVID-19



Source: PwC Digital Insights Pulse Survey, agosto 2020



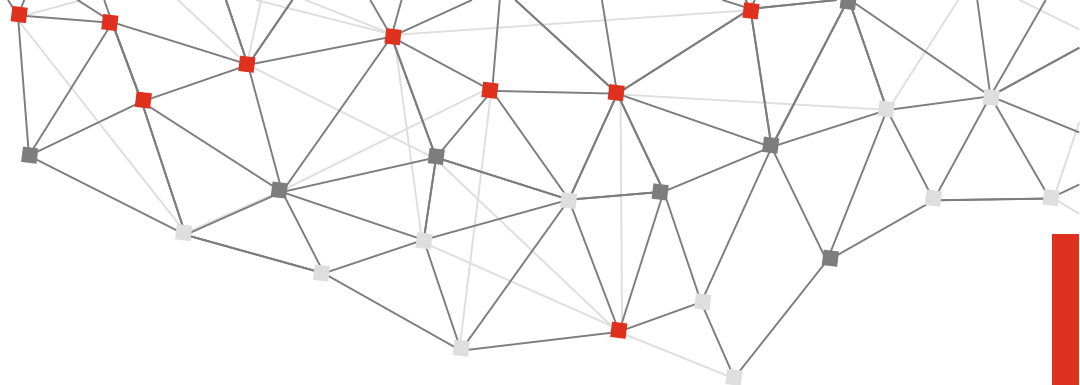
Se obtuvieron respuestas de una variedad de industrias



Las inversiones en los últimos dos o tres años que dieron más resultados durante la crisis no fueron soluciones de seguridad únicas



¿En cuál de las siguientes áreas su empresa ha realizado inversiones en los últimos 2-3 años (por ejemplo, actualizaciones, modernización o integración en toda la empresa)?



Top 3 inversiones realizadas:

78%

Entrenamiento y concientización
de seguridad

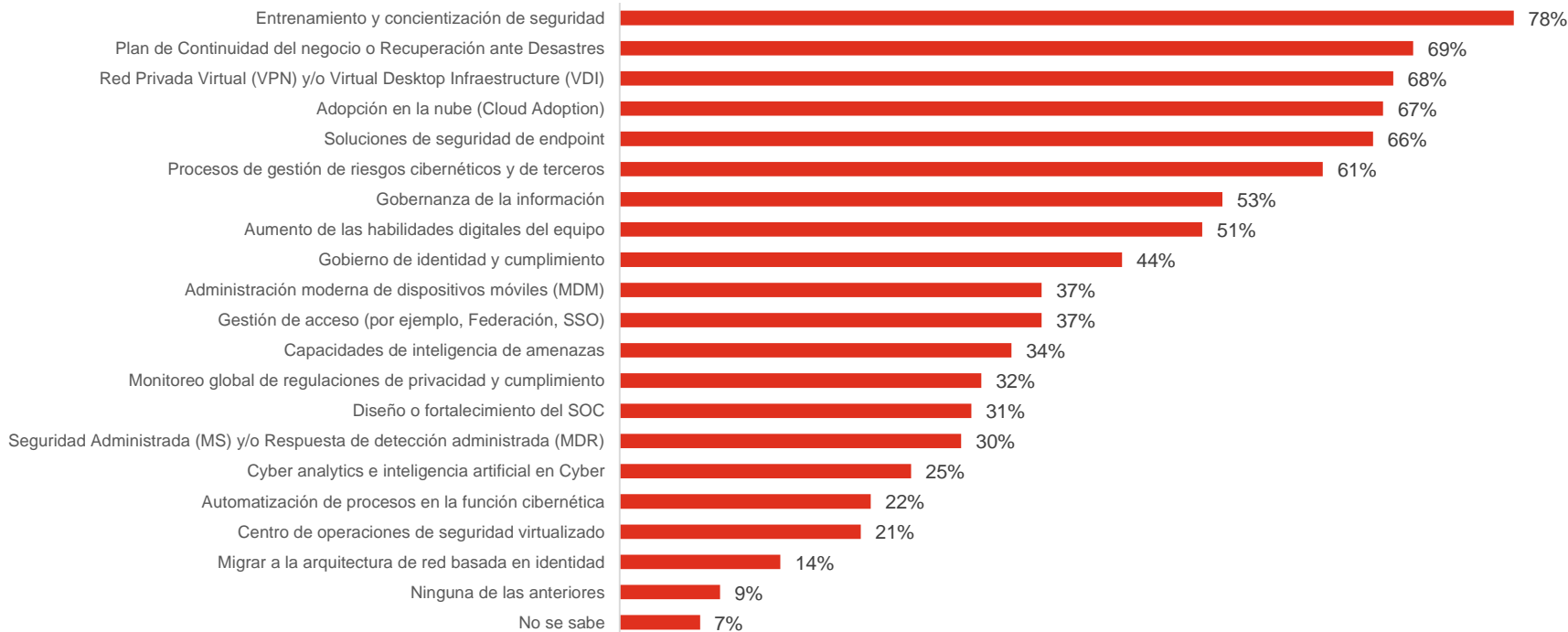
69%

Planes de continuidad del negocio
o recuperación ante desastres

68%

Red Privada Virtual (VPN) y/o Virtual
Desktop Infraestructure (VDI)

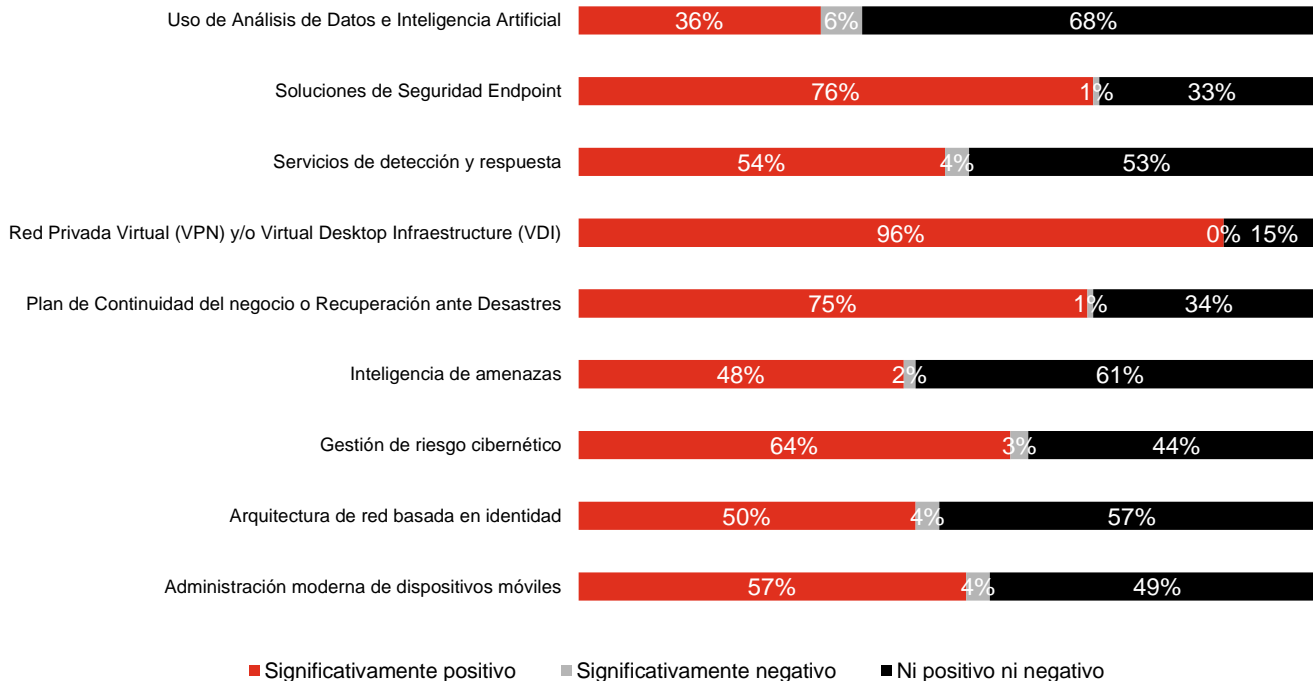
¿En cuál de las siguientes áreas su empresa ha realizado inversiones en los últimos 2-3 años (por ejemplo, actualizaciones, modernización o integración en toda la empresa)?



¿Cuál ha sido el impacto de las inversiones tecnológicas realizadas en años anteriores, durante la crisis de COVID-19?

86%

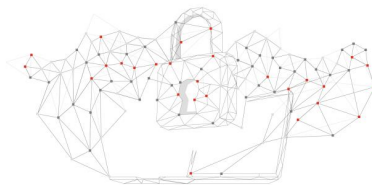
De los encuestados indica que el impacto de las inversiones realizadas en los últimos 2 o 3 años fue significativamente positivo



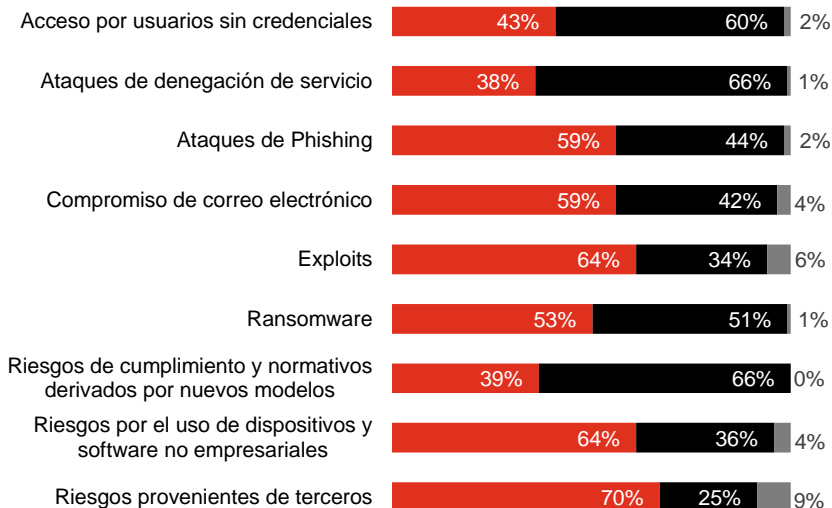
Los CISO vieron cómo los ataques cibernéticos se dispararon desde febrero de 2020 y esperan que las amenazas sigan siendo elevadas en los próximos seis meses



Un aumento en los riesgos o ataques relacionados con COVID-19



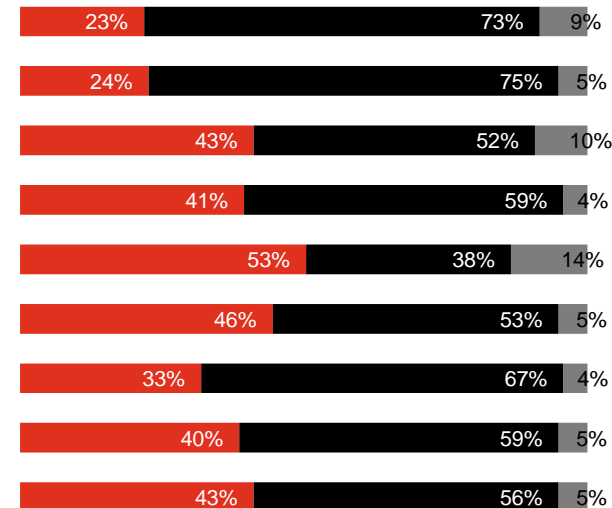
Dentro de su empresa, ¿ha visto un cambio en alguno de los siguientes riesgos o ataques relacionados con COVID-19 desde febrero de 2020?



■ Sin Cambio ■ Incrementó ■ Disminuyó

Source: PwC Digital Insights Pulse Survey, agosto 2020

Y ahora mirando hacia el futuro, ¿de qué manera espera que cambie la incidencia de los riesgos o ataques relacionados con COVID-19 en los próximos 6 meses?

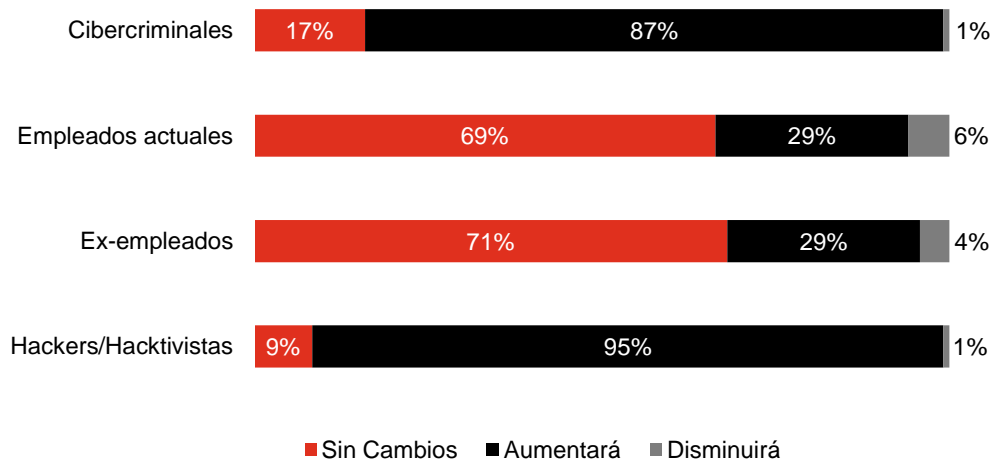


■ Sin Cambio ■ Incrementará ■ Disminuirá

PwC's Digital Trust Insights Pulse Survey Findings

Se espera que la actividad del atacante aumente en los próximos 6 meses.

¿De qué manera espera que la actividad de los actores de amenazas de las siguientes fuentes cambie en los próximos 6 meses?



La pandemia exigió a los CISO que
tomaran acciones inmediatas,
trayendo consigo nuevas necesidades



La pandemia trajo consigo una mayor necesidad de capacitación y conciencia.



61%

De los encuestados insisten en que una mayor capacitación y conciencia en la fuerza laboral es la acción más importante que se debe realizar.

Esto permitirá defenderse ante ataques de phishing y los riesgos relacionados con el trabajo remoto

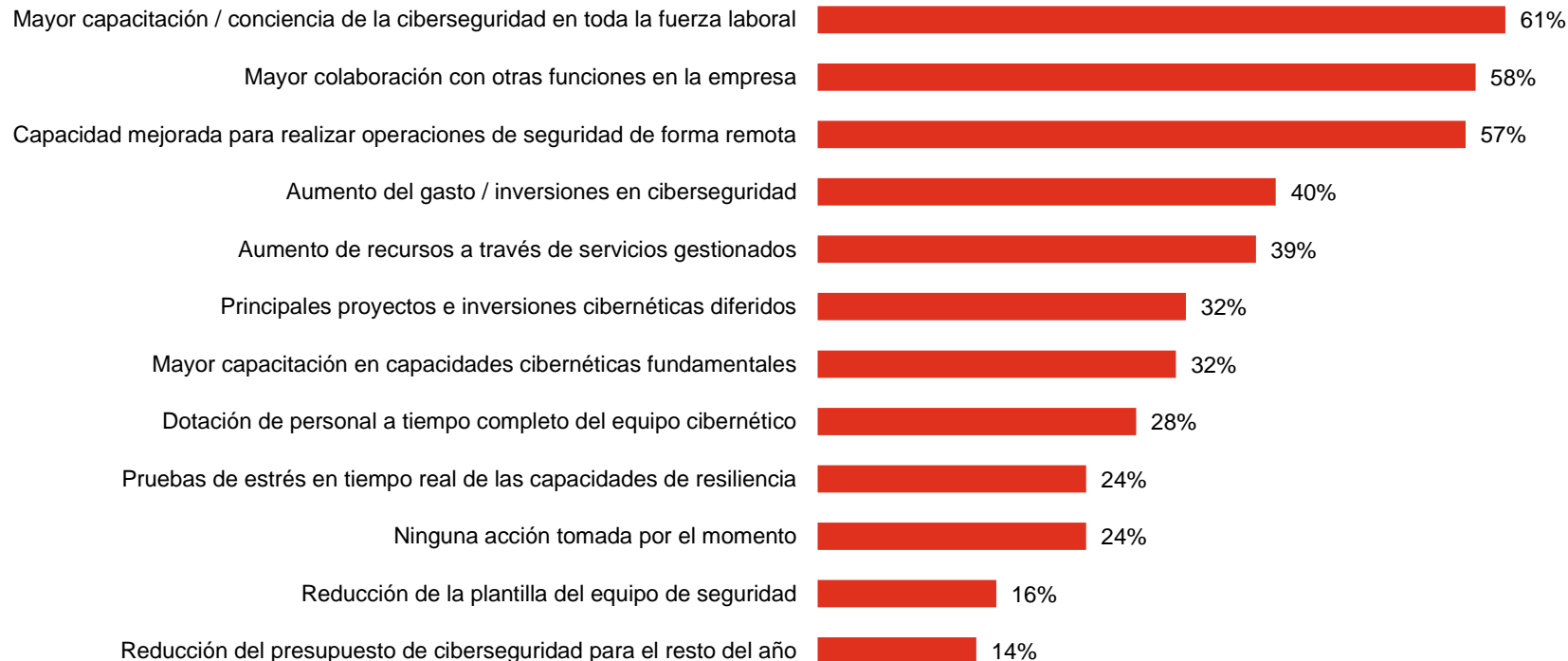


14%

Solo el 14% de los encuestados reducirán el presupuesto de ciberseguridad para el resto del año

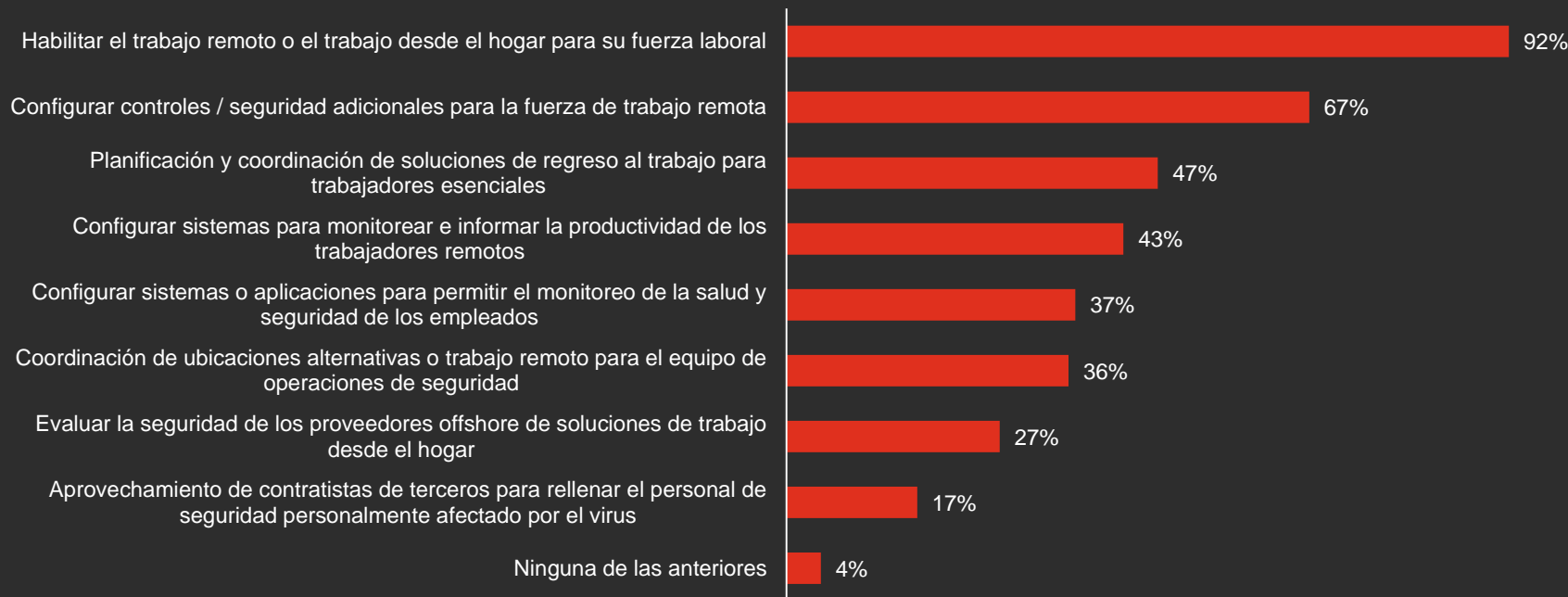


Los CISO tomaron las siguientes acciones durante la crisis

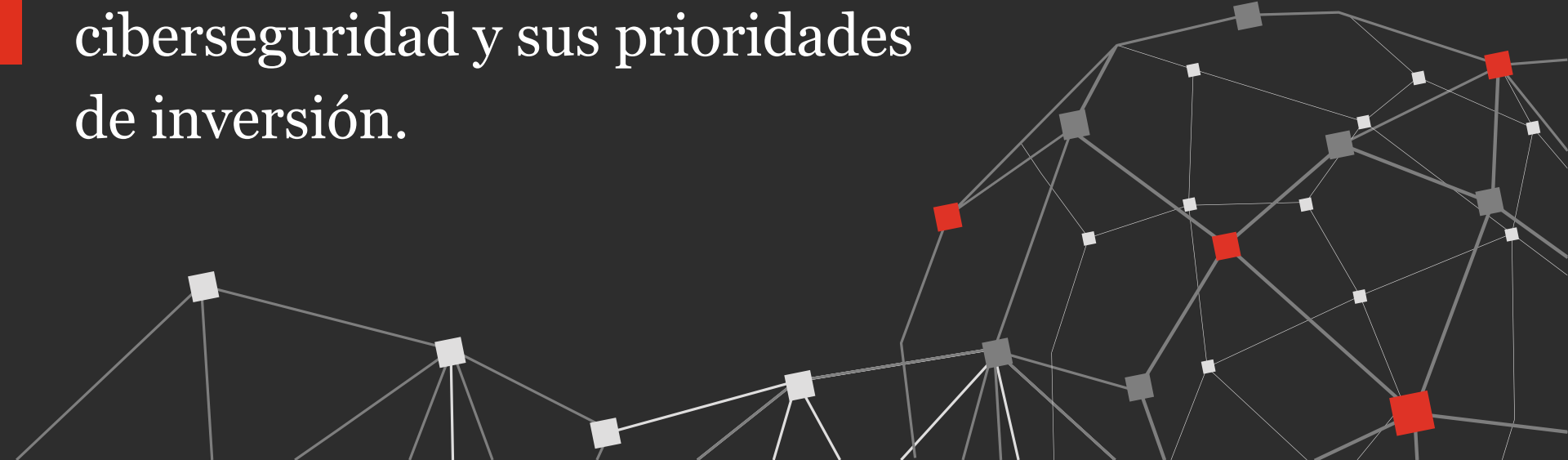


Las crisis precipitan nuevos enfoques; así es como las organizaciones líderes emergen más fuertes de ellas

Con respecto a la crisis de COVID-19, ¿en qué medida ha estado involucrado en cada una de las siguientes categorías?



La pandemia está obligando a los CISO a repensar su estrategia de ciberseguridad y sus prioridades de inversión.



Cambios planificados en la estrategia de ciberseguridad

Dado lo que aprendió durante la crisis, ¿cuál de los siguientes está priorizando para que las futuras inversiones cibernéticas salgan fortalecidas de la crisis?



Las prioridades de inversión en ciberseguridad están cambiando en el futuro debido a la experiencia pandémica

Ganando importancia

- Entrenamiento y concientización de seguridad
- Plan de Continuidad del negocio o Recuperación ante Desastres
- Adopción en la nube (Cloud Adoption)
- Aumento de las habilidades digitales del equipo
- Red privada virtual (VPN) y/o Virtual Desktop Infrastructure (VDI)

No es alto en la lista de prioridades

- Procesos de gestión de riesgos cibernéticos y de terceros
- Automatización de procesos en la función cibernética
- Gestión de acceso (por ejemplo, Federación, SSO)
- Diseño o fortalecimiento del SOC

Sigue siendo importante

- Administración moderna de dispositivos móviles (MDM)
- Capacidades de inteligencia de amenazas
- Gobierno de identidad y cumplimiento
- Gobernanza de la información
- Soluciones de seguridad de endpoint
- Cyber analytics e inteligencia artificial en Cyber

Consigue menos énfasis

- Centro de operaciones de seguridad virtualizado
- Monitoreo global de regulaciones de privacidad y cumplimiento
- Migrar a la arquitectura de red basada en identidad (por ejemplo, segmentación, Zero Trust)

Source: PwC Digital Insights Pulse Survey, agosto 2020

57%

Es hora de intensificar la
imaginación e influencia de los
CISO para avanzar



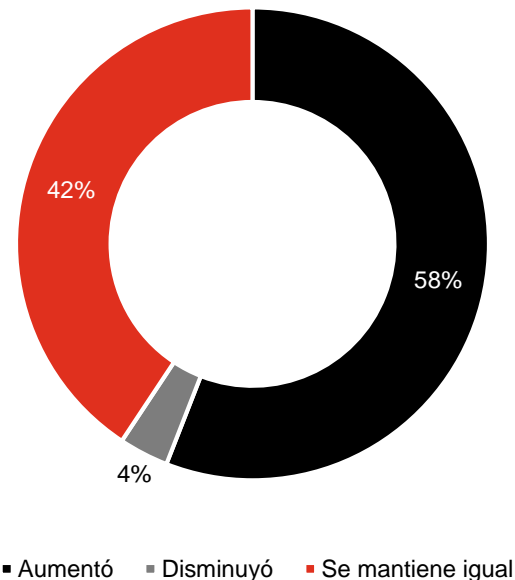
Es hora de intensificar la imaginación e influencia de los CISO para avanzar

58% de los CISO dicen que sus interacciones con el CEO y/o la Junta Directiva se han vuelto más frecuentes durante la crisis.

La comunicación efectiva con la junta y los CEO requiere muchas habilidades de liderazgo que serán invaluableles en los próximos meses.

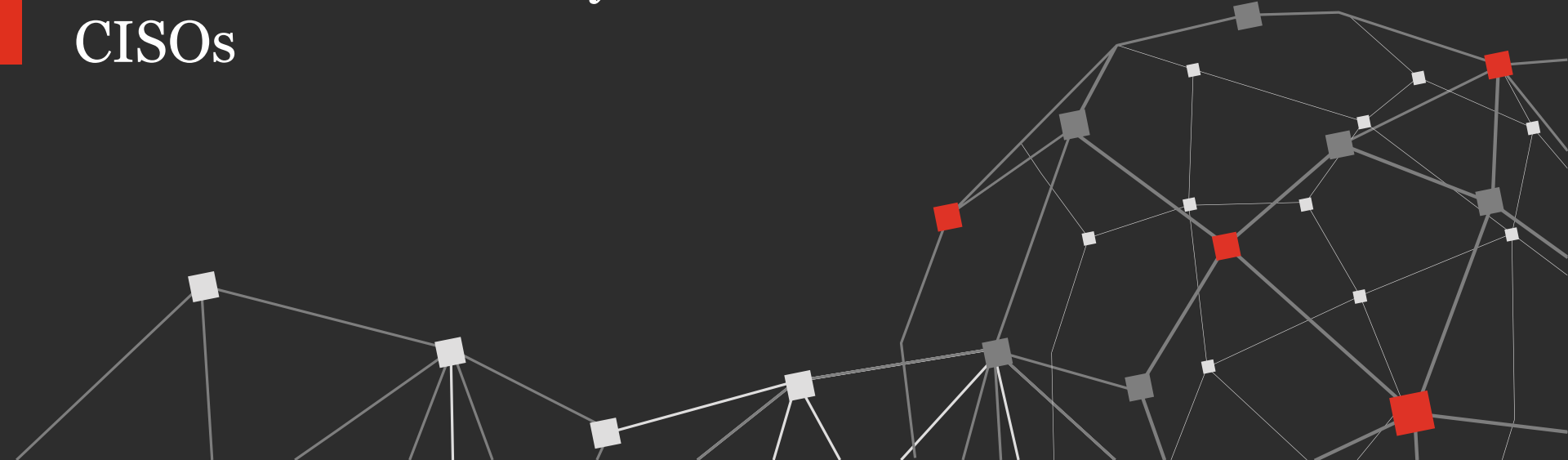
La reapertura de los lugares de trabajo significa hitos nuevos y diferentes para que las organizaciones logren. Los CEO están liderando con atención tanto en lo pragmático y urgente (cómo contengo los costos) como en lo nuevo y a largo plazo (cómo aplico la tecnología para brindar una mejor experiencia al cliente y hacer las cosas de manera más inteligente y eficiente).

A raíz de la crisis de COVID-19, ¿cómo se ha afectado la frecuencia de su interacción con el CEO y/o Junta Directiva?



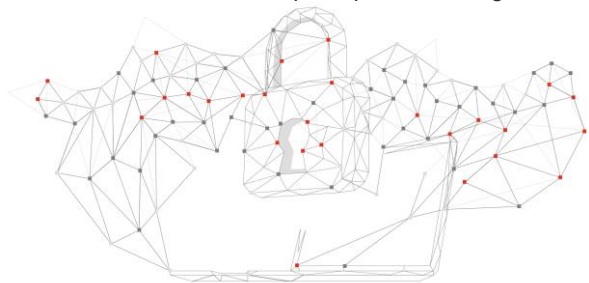
Source: PwC, Digital Trust Insights Pulse Survey, agosto 2020

Plan de acción para los Chief Information Security Officers CISOs



Plan de acción para el CISO

- Mantener mejor colaboración con los líderes empresariales y de riesgo siempre; es decir, más allá de esta crisis.
- Priorizar la identificación y reparación de cualquier brecha o vulnerabilidad que pueda haber resultado de la crisis. Aprovechar la oportunidad para modernizar y simplificar.
- Trabajar en conjunto a la tomadores de decisiones del negocio para anticipar y administrar los riesgos que surgen de la digitalización acelerada, la adopción de la nube y los cambios a los modelos de negocios digitales.
- Continuar comunicándose frecuentemente con el CEO y la Junta.
- Ofrecer a estos líderes formas imaginativas de mejorar la seguridad, la resiliencia y la confianza, al tiempo que ayuda a contener los costos al ser un buen administrador del presupuesto de seguridad cibernética.



¿Cómo emerger más fuerte?



Nuestros contactos

Ignacio Perez

ignacio.perez@pwc.com

Regional Advisory Leader Partner
PwC Central America and Dominican
Republic

Valentina Morales

morales.valentina@pwc.com

Cybersecurity & Privacy Leader
PwC Central America and
Dominican Republic

Ivan Vergara

ivan.vergara@pwc.com

Financial Services & Cyber driver
PwC Central America and
Dominican Republic



Gracias



© 2020 PwC InterAméricas. Todos los derechos reservados. PwC se refiere a la red de PwC y/o a una o más de sus firmas miembro, cada una de las cuales es una entidad legal separada. Ver www.pwc.com/structure para más detalles.

www.pwc.com/interamericas