ivanti PULSE

El estado del acceso seguro en Europa

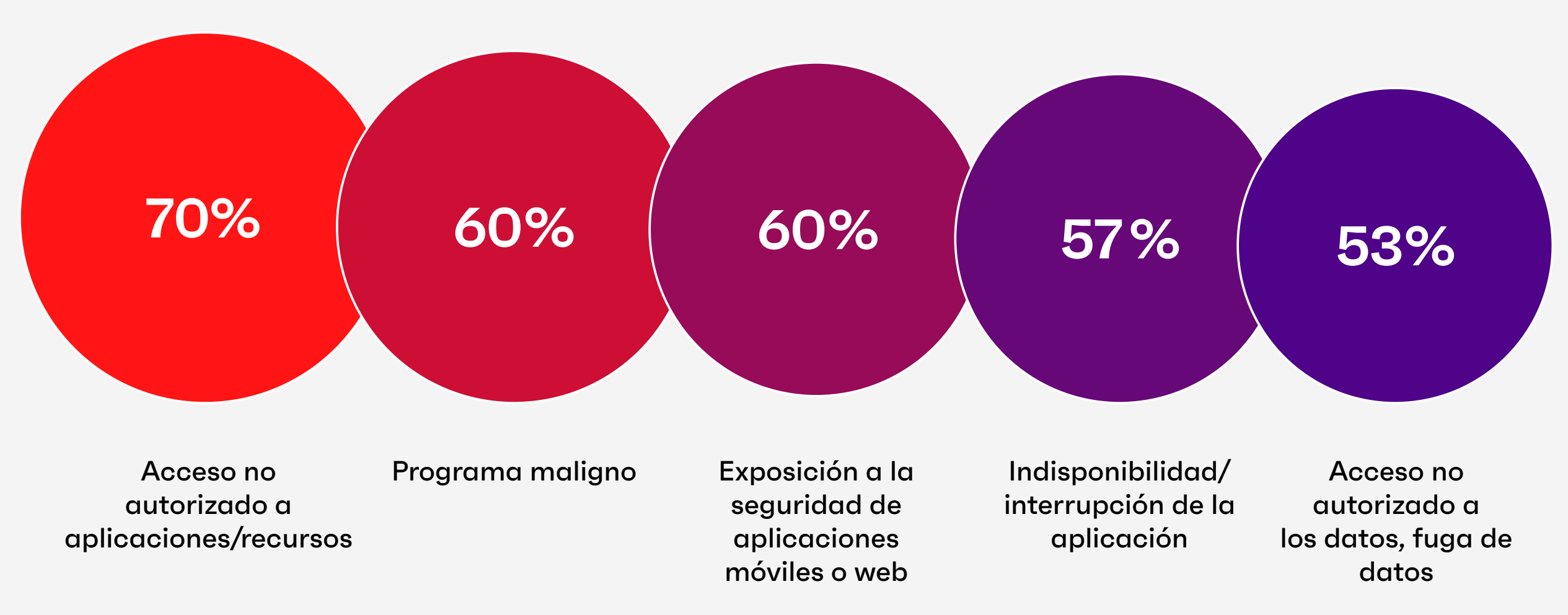
En los últimos 12 meses, los responsables de seguridad y de TI en Europa han experimentado una serie de amenazas a la seguridad. Para combatir estos crecientes desafíos, están dando prioridad a una serie de iniciativas de acceso seguro y están planeando alinearlas con un protocolo de confianza cero. Sin embargo, entre los distintos sectores -en concreto, el de los programas informáticos, el de los servicios financieros y el de la fabricación- esas prioridades difieren.

Ivanti y Pulse encuestaron a 275 líderes de TI y seguridad en Europa para descubrir sus prioridades de acceso seguro para los próximos 12 meses y averiguar cómo se utilizarán para reducir la frecuencia de los desafíos de seguridad.

Las empresas deben definir políticas de acceso para combatir las amenazas a la seguridad

En el último año, más de la mitad de las empresas europeas han sido víctimas de un ataque de seguridad. Lo más habitual es que las organizaciones de los responsables de TI y seguridad se hayan visto afectadas por el acceso no autorizado a aplicaciones y recursos (70%), por el malware (60%) y por la exposición a la seguridad de las aplicaciones móviles o web (60%).

¿Cuál de las siguientes 5 amenazas a la seguridad han afectado más a su organización en los últimos 12 meses?

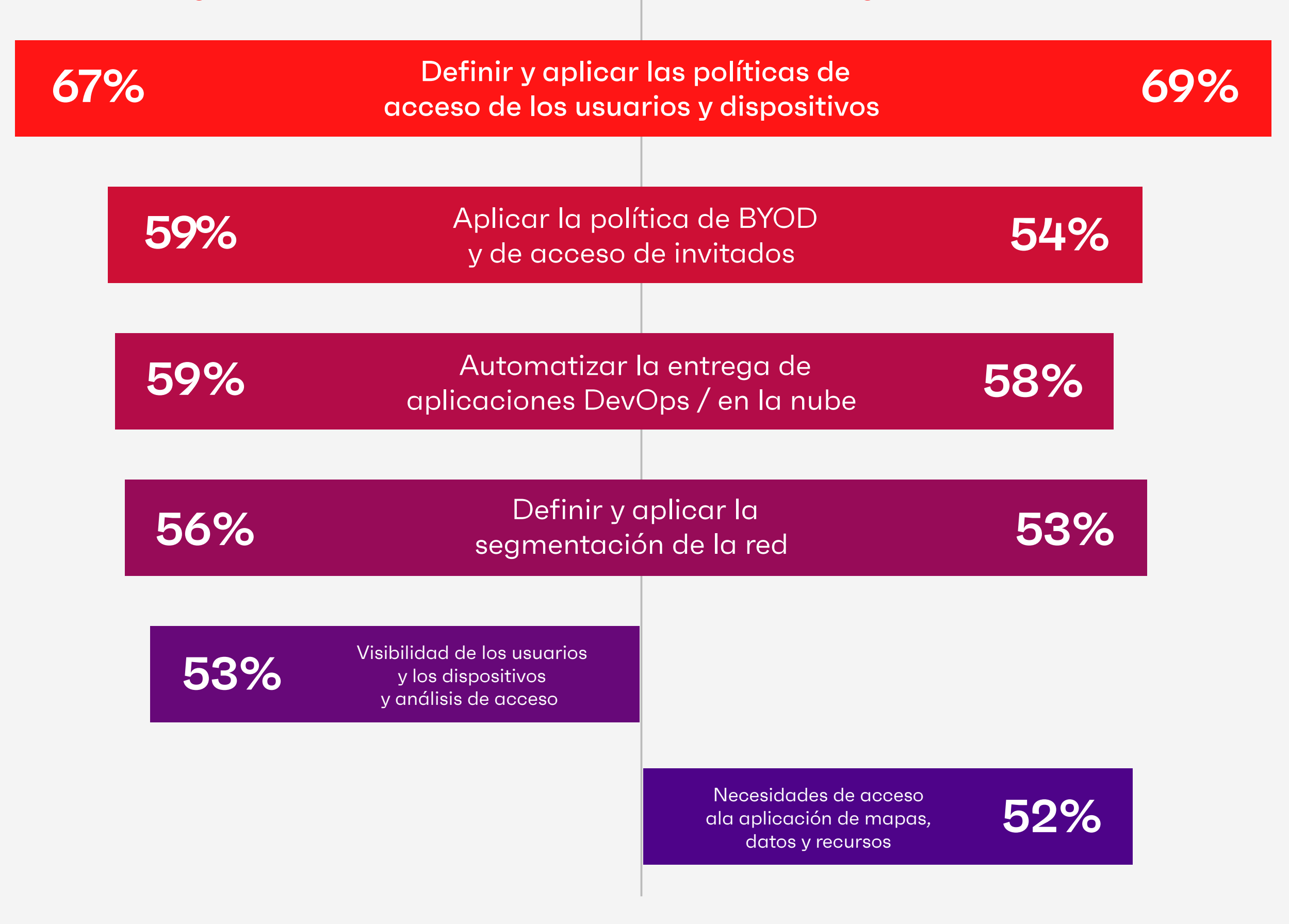


Por el contrario, en América del Norte, la principal amenaza a la seguridad que se ha denunciado es el programa maligno (51%), y en la región de Asia-Pacífico y Japón (APJ) es la exposición a la seguridad de las aplicaciones móviles o web (79%).

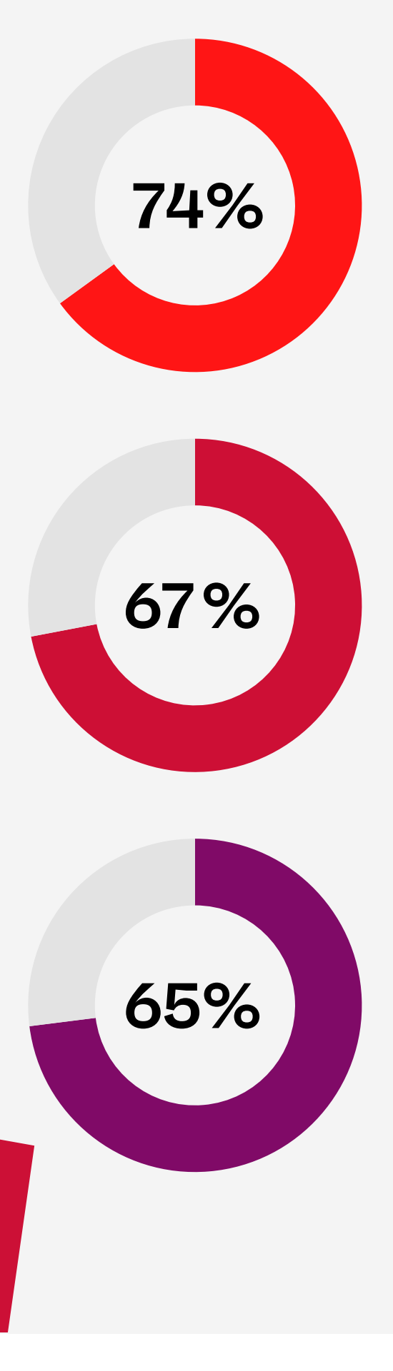
Para reducir el impacto de estas crecientes amenazas a la seguridad, el 67% de los responsables de TI y seguridad afirman que lo más importante para su organización es definir y aplicar políticas de acceso de usuarios y dispositivos. Sin embargo, las tres iniciativas más vitales son también las tres más difíciles de aplicar.

¿Cuáles de las siguientes capacidades de seguridad son más importantes para que su empresa las ejecute con el fin de mitigar las amenazas a la seguridad de acceso?

¿De las siguientes capacidades de seguridad, cuáles son las 5 más difíciles de ejecutar para su organización con el fin de mitigar las amenazas/riesgos de seguridad de acceso?



¿Cuál es la capacidad de mitigación de amenazas más importante según cada industria?



Software
Definir y aplicar las políticas de acceso de los usuarios y dispositivos

Servicios financieros
Automatizar la entrega de aplicaciones DevOps/en la nube

Fabricación
Definir y aplicar las políticas de acceso de los usuarios y dispositivos

Para prevenir aún más las amenazas a la seguridad, los líderes tecnológicos están dando prioridad a la confianza cero y a la seguridad de la TI híbrida

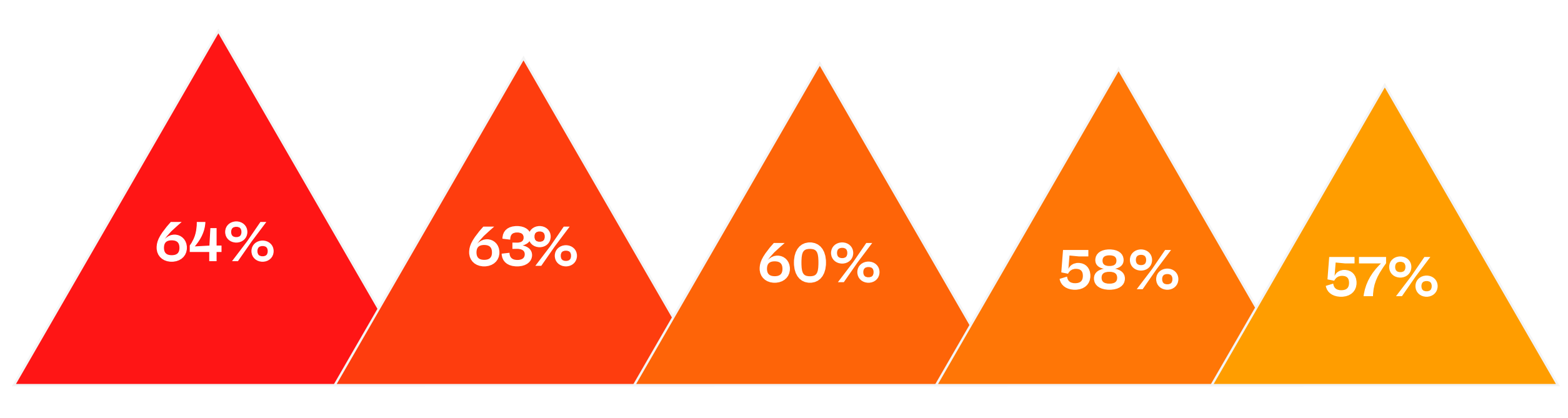
El 99 % de los profesionales de la informática y la seguridad en Europa afirman que sus prácticas de seguridad se alinearán más con una estrategia de confianza cero en los próximos 12 meses.

En los próximos 12 meses, ¿en qué medida los controles de seguridad existentes en su organización se alinearán más con la Confianza Cero?

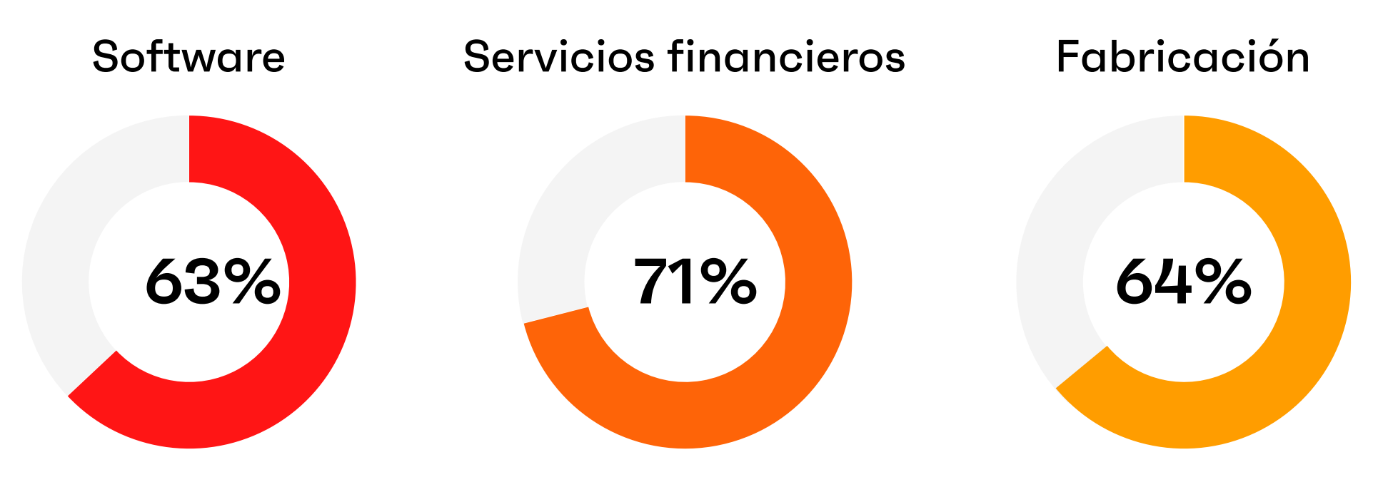
América del Norte está priorizando la alineación de Confianza Cero más que Europa. En el mundo occidental, el 21% de los responsables de TI y seguridad afirman que se alinearán de forma significativa o completa con los principios de Confianza Cero en el próximo año.

Los responsables de TI y seguridad afirman que sus organizaciones están dando prioridad a las iniciativas de seguridad de acceso para permitir la coherencia del control de acceso en los entornos híbridos (64%) y aumentar la entrega y protección de la carga de trabajo de las aplicaciones (63%) en los próximos 12 meses.

En los próximos 12 meses, ¿qué iniciativas de seguridad de acceso son de máxima prioridad para su organización?



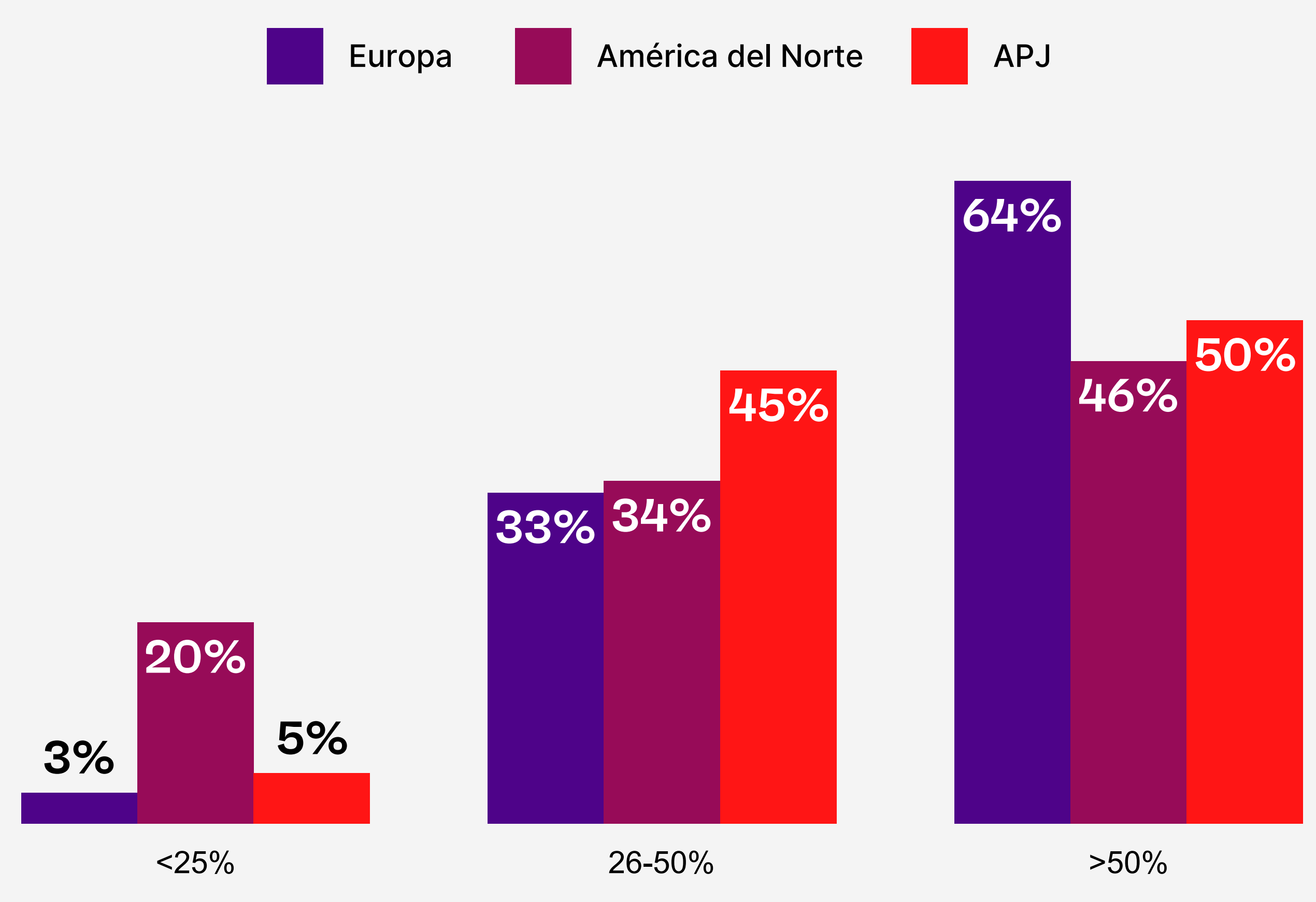
Principales prioridades de las iniciativas de seguridad por sector:



Los líderes de TI y de seguridad se están mudando a los servicios de seguridad proporcionados por la nube y planean consolidar los proveedores

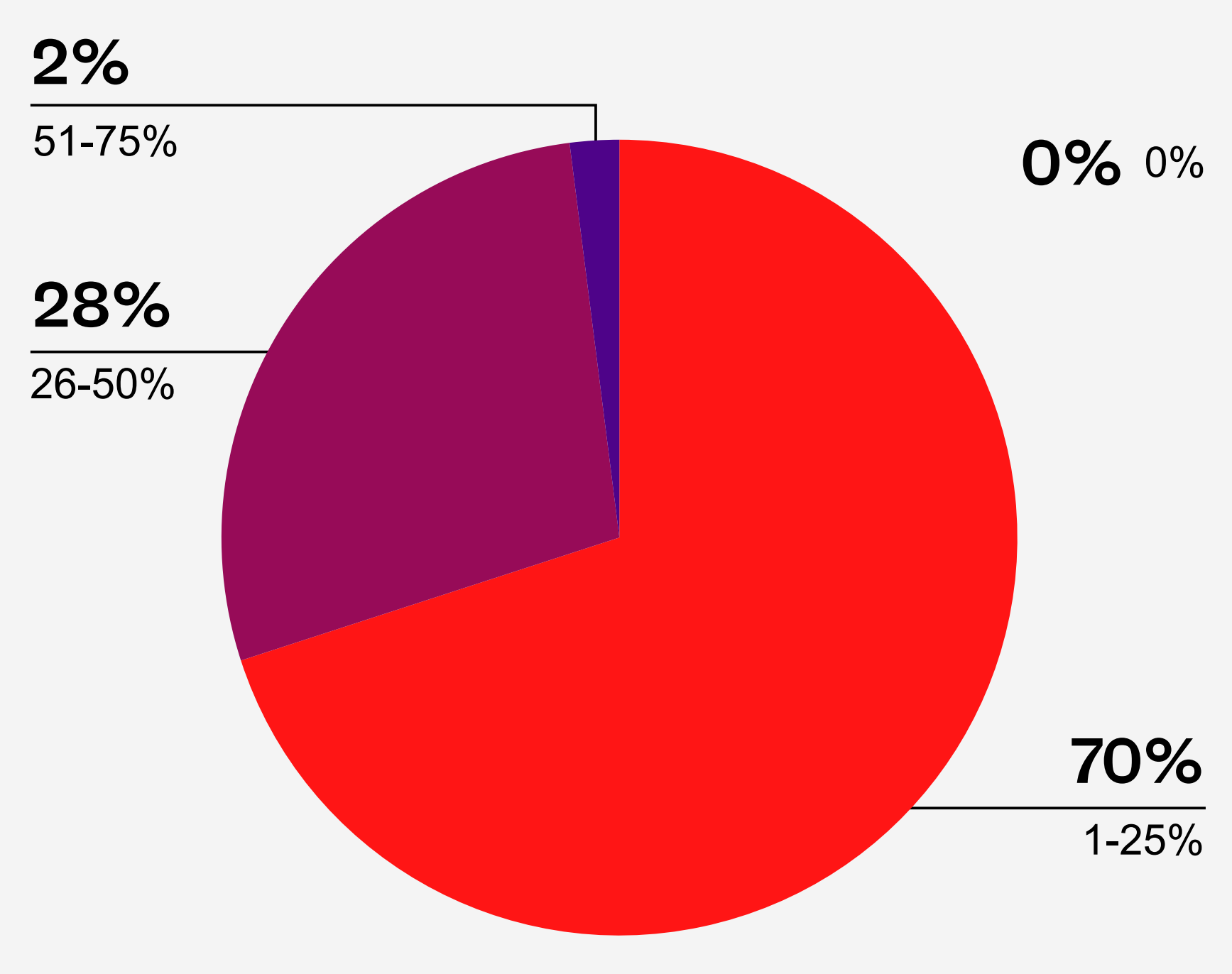
Casi dos tercios (64%) de los responsables europeos de TI y seguridad afirman que sus empresas han pasado la mayoría de sus servicios de seguridad a la entrega en la nube, lo que supone una tasa de adopción mayor que en cualquier otra parte del mundo.

¿Cuántos servicios de seguridad ha cambiado su empresa a la entrega en la nube desde las herramientas de seguridad tradicionales en las instalaciones?



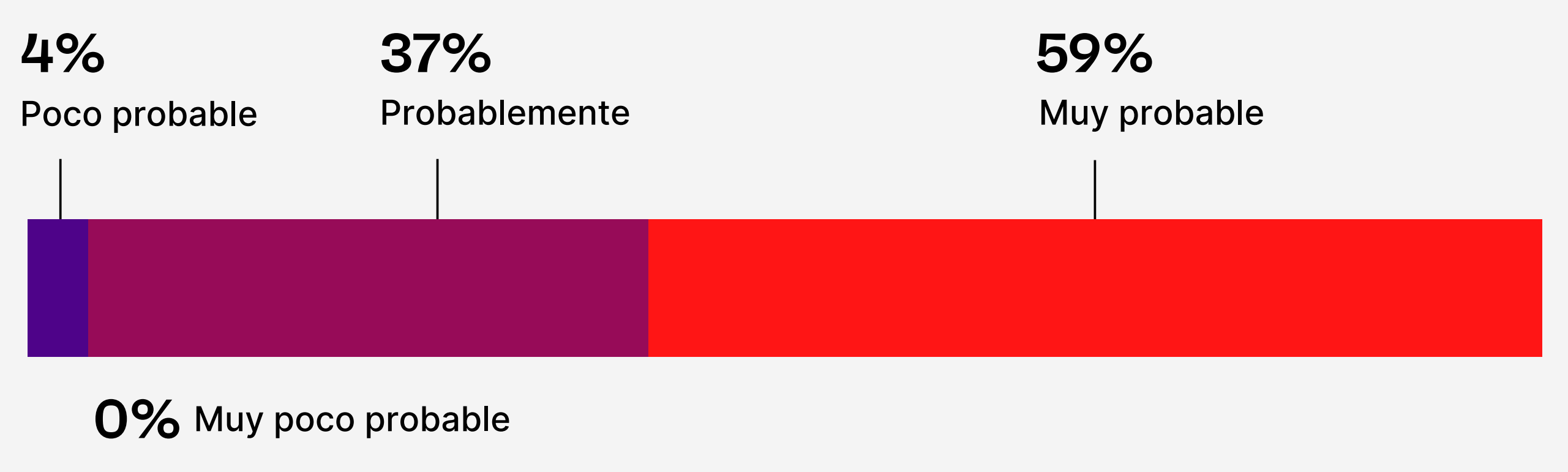
Y el 30% espera que sus empresas aumenten su gasto en servicios de seguridad en la nube en más de un 25% en el próximo año.

En los próximos 18 meses, ¿en qué medida espera que su empresa aumente la inversión en servicios de seguridad en la nube?



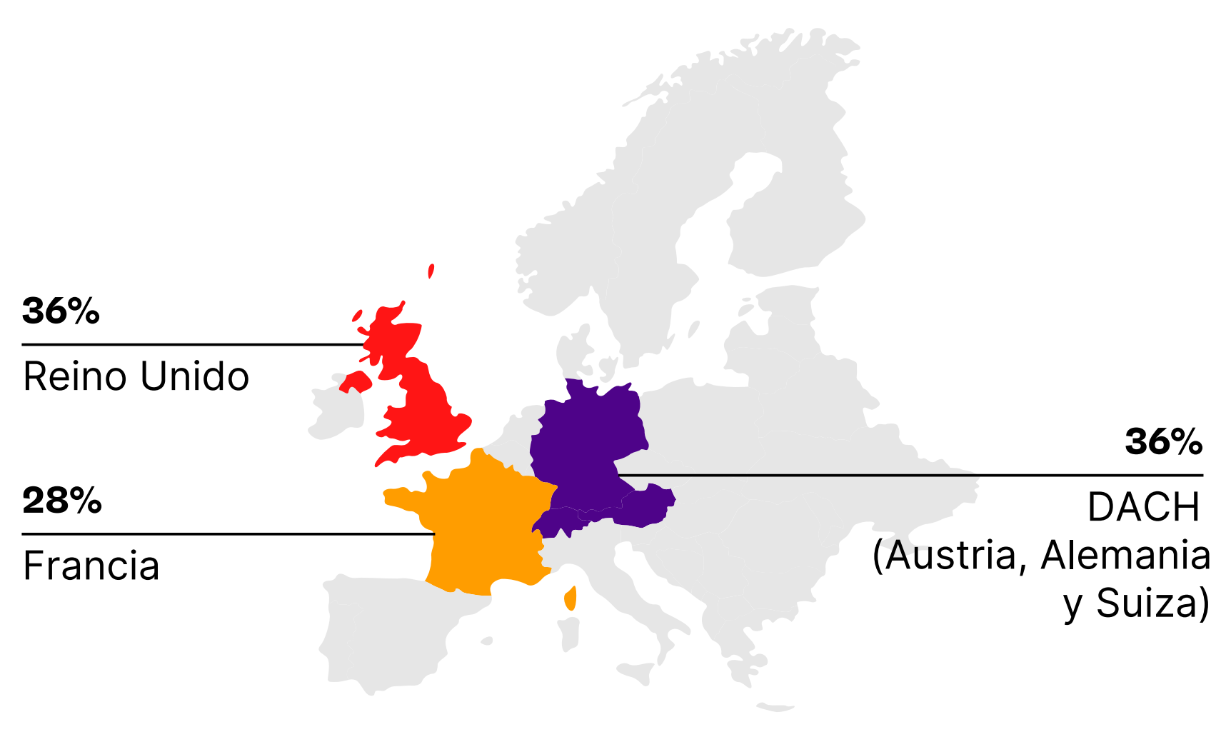
Por último, la gran mayoría (96%) de los encuestados está consolidando actualmente a los proveedores de seguridad en una plataforma unificada, o tiene previsto hacerlo en los próximos meses. Más de la mitad (59%) dijo que este esfuerzo es muy probable.

¿Qué probabilidad hay de que su organización consolide las herramientas de acceso seguro separadas en una plataforma más unificada con menos proveedores en los próximos 12 meses?

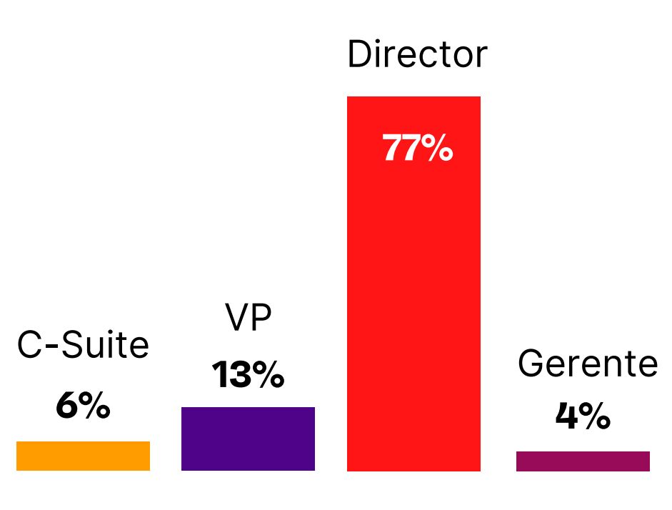


Respdesglose de los componentes

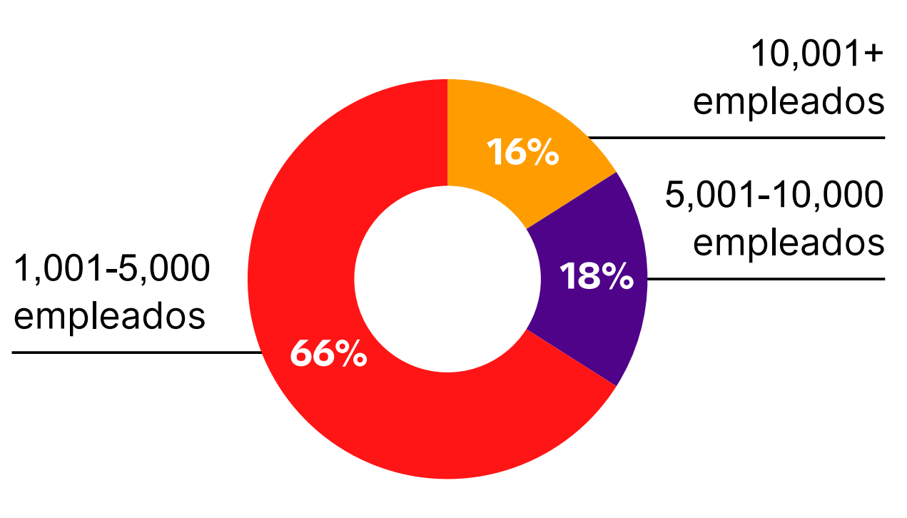
País



Título



Tamaño de la compañía



Datos recogidos del
1 de Octubre al 23 de Noviembre de 2020

Encuestados:
275 líderes de TI y seguridad

Insights impulsados por PULSE