FORTRA

Estudio sobre pentesting 2024

Introducción

Las prácticas ofensivas de Ciberseguridad, como el pentesting, se distinguen de otros métodos de Seguridad. A diferencia de las medidas defensivas tradicionales, que a menudo se ven obligadas a reaccionar ante las amenazas cuando surgen, la Seguridad ofensiva puede aprovechar la calma y la concentración que aporta la planificación y la adopción de medidas antes de que se haya lanzado un ataque. Sin embargo, determinar las estrategias más eficaces mientras se navega por la estática de las amenazas emergentes, las nuevas medidas de Seguridad y las innumerables técnicas puede ser una tarea desalentadora.

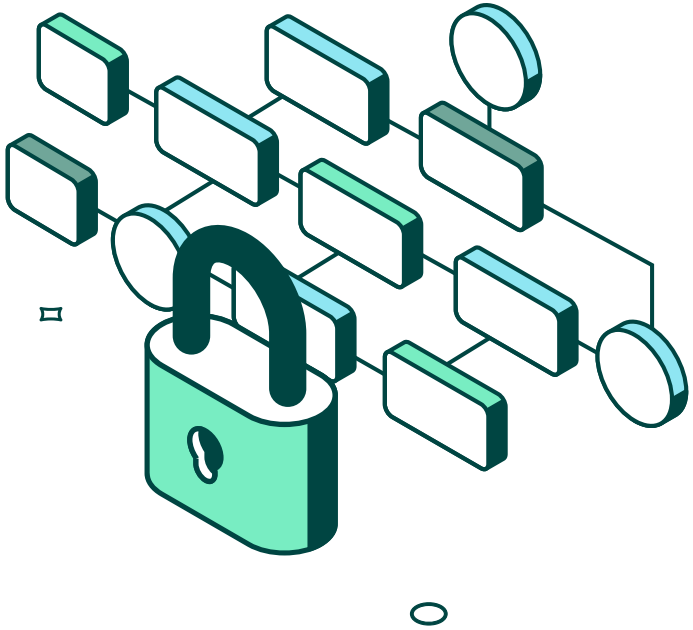
Al conocer cómo otras organizaciones utilizan el pentesting, obtenemos valiosas perspectivas sobre la eficacia de los distintos enfoques, los desafíos encontrados y las lecciones aprendidas. Compartir conocimientos capacita a los profesionales de la Ciberseguridad para tomar decisiones informadas que se ajusten a las necesidades específicas de su organización.

Con esto en mente, Core Security de Fortra desarrolló una encuesta sobre pentesting para recopilar, analizar y distribuir información sobre cómo los profesionales de la Ciberseguridad utilizan el pentesting y otras soluciones proactivas.

Ahora, en su quinto año, esta encuesta continúa haciendo un seguimiento de los cambios, las tendencias, los desafíos y las áreas de desarrollo año tras año. La información recopilada constituye un valioso recurso para los profesionales de la Ciberseguridad comprometidos con el crecimiento y el mantenimiento de una postura de Seguridad proactiva y resistente. En este informe se pretende aportar información sobre el estado actual de las prácticas de pentesting, proporcionando datos actuales y útiles sobre las siguientes cuestiones clave relacionadas con el pentesting:

- Eficacia del pentesting en la prevención de brechas
- Principales problemas de Seguridad, como phishing, ransomware y falta de parches
- Desafíos del pentesting, como la escasez de personal y la falta de recursos para la remediación
- Normativa pertinente y cuestiones de cumplimiento
- Utilización de equipos internos de pentesting
- Selección de equipos de terceros
- Evaluación de herramientas de pentesting
- Otras herramientas de evaluación de la Seguridad, como el escaneo de vulnerabilidades y *red teaming*
- Consolidación del proveedor
- Pentesting en distintos entornos

Además de examinar los resultados de este año, ofreceremos una comparación con los de 2023 para comprender mejor la progresión del campo del pentesting.



Valor del Pentesting

¿Qué valor aporta el pentesting?

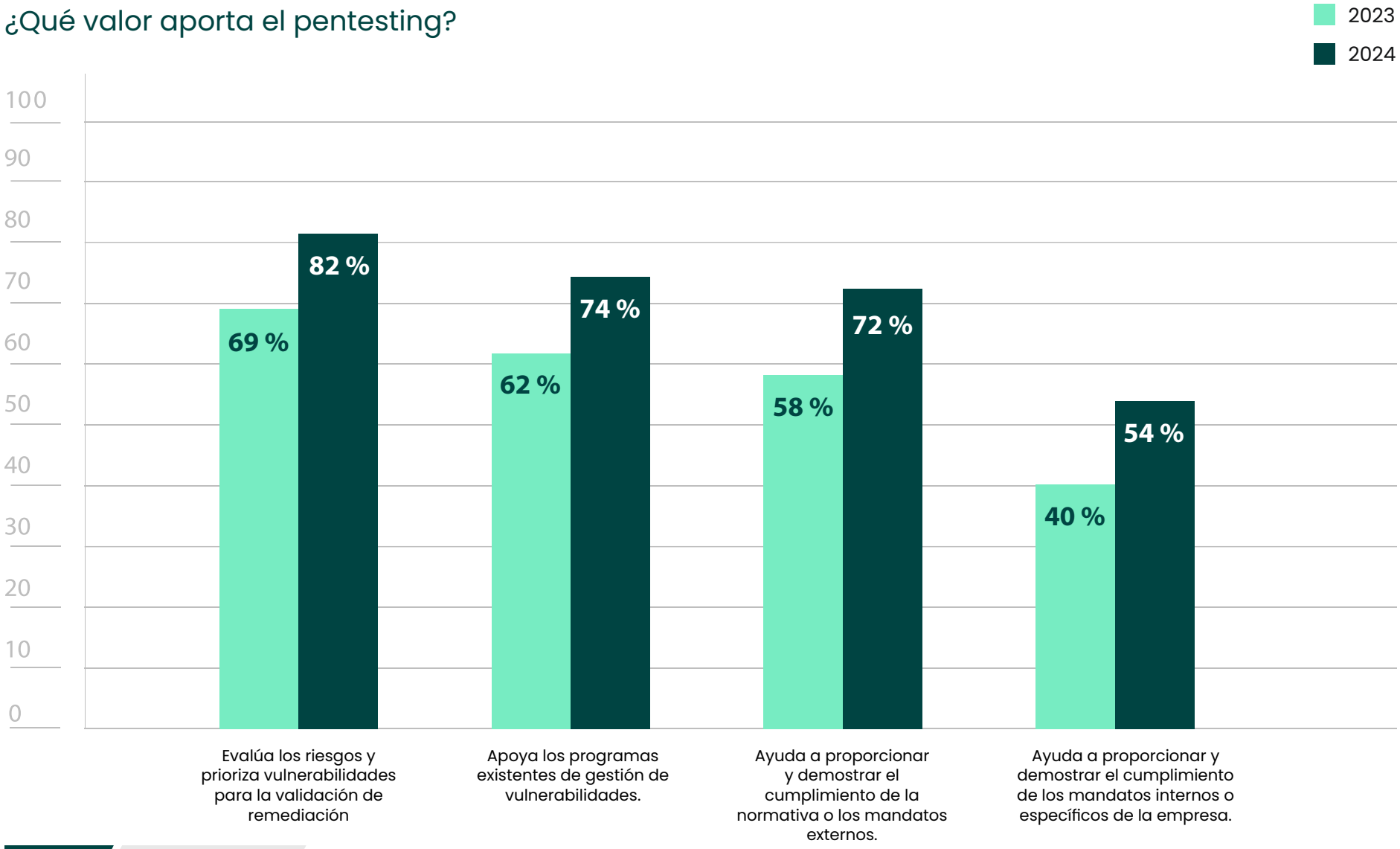


Figura 1: Valor del pentesting

Valor del Pentesting

Los resultados de la encuesta de este año muestran el valor que las organizaciones siguen encontrando en el pentesting. Con todas las categorías con un aumento considerable con respecto al año pasado, las organizaciones también pueden estar descubriendo una cantidad cada vez mayor de casos de uso para el pentesting.

Evaluar el riesgo y priorizar las vulnerabilidades para su remediación es el objetivo principal del pentesting y una práctica de Seguridad ofensiva fundamental. Por lo tanto, no es de extrañar que haya seguido siendo la respuesta más común (82 %) (Figura 1). El aumento del 12 % con respecto al año pasado puede estar vinculado a los aumentos de tamaño similar reflejados en los que utilizan pentesting para el cumplimiento externo (72 %) y los mandatos internos (54 %). Las organizaciones que comenzaron a utilizar pentesting como una forma de mantener y demostrar la adherencia pueden haberse dado cuenta rápidamente de que el pentesting es mucho más que una casilla que hay que marcar. El pentesting proporciona un análisis en profundidad único sobre el impacto potencial de las vulnerabilidades explotadas. De este modo, se puede saber qué puntos débiles son los que causan más riesgos, lo que proporciona el camino más estratégico para cerrar las brechas de Seguridad.

Quizás la mayor prueba del valor del pentesting es que el 72 % de los encuestados considera que el pentesting ha evitado una brecha en su organización (Figura 2). Esto subraya la importancia de los esfuerzos proactivos que identifican y abordan las vulnerabilidades antes de que puedan ser explotadas.

Cabe destacar que el segundo valor más común que los encuestados encontraron en el pentesting fue su función de apoyo a los programas de gestión de vulnerabilidades existentes (74 %) (Figura 1). Aunque algunas organizaciones pueden confiar únicamente en una solución proactiva, como el pentesting, es vital reconocer el valor de la Seguridad ofensiva por capas. La incorporación del pentesting en un programa táctico unificado con soluciones complementarias como la escaneo de vulnerabilidades y de *red teaming* permite a las organizaciones mejorar la cobertura y la eficacia.

¿Cree que el pentesting ha evitado una brecha en su organización?

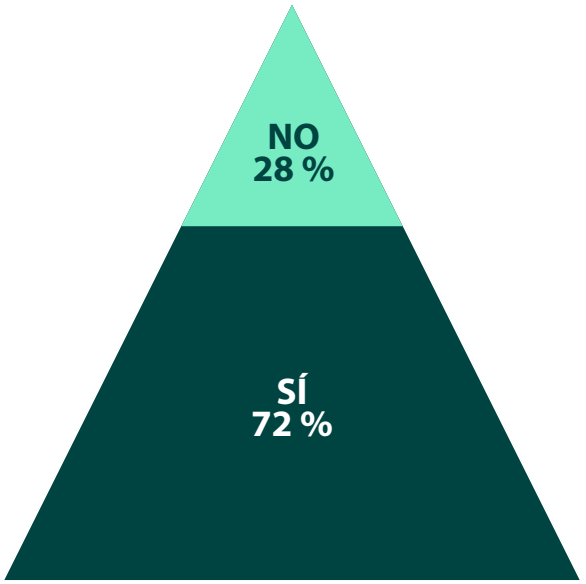


Figura 2: Eficacia del pentesting para la prevención de brechas

Preocupaciones comunes sobre la Seguridad

¿Qué riesgos comunes de Seguridad o puntos de entrada le preocupan más?

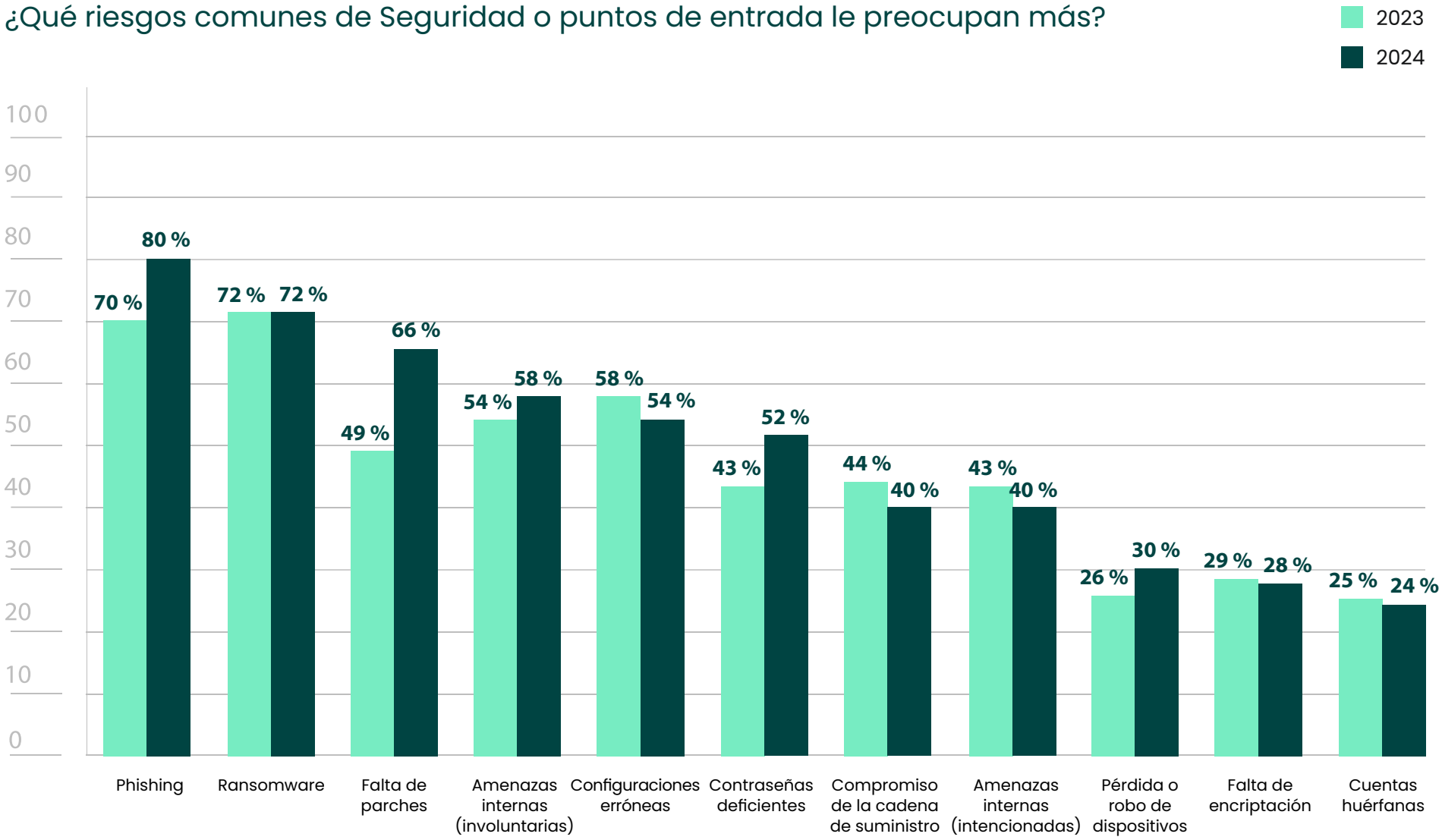


Figura 3: Preocupaciones comunes sobre la Seguridad

Preocupaciones comunes sobre la Seguridad

El phishing (80 %) y el ransomware (72 %) volvieron a ser las principales preocupaciones en materia de Seguridad (Figura 3) para los participantes en la encuesta. El phishing y el ransomware han seguido siendo las dos principales preocupaciones en los últimos tres años, y por buenas razones. El grupo de trabajo antiphishing informó que 2023 fue el peor año registrado para el phishing, con más de cinco millones de ataques de phishing observados.

El ransomware también ha ido en aumento en el último año, ya que SANS ha informado de un incremento del 73 % en los ataques de ransomware. El phishing es el método de entrega más común para el ransomware, por lo que se espera que estas dos amenazas estrechamente vinculadas sigan dominando las preocupaciones de los profesionales de la Seguridad.

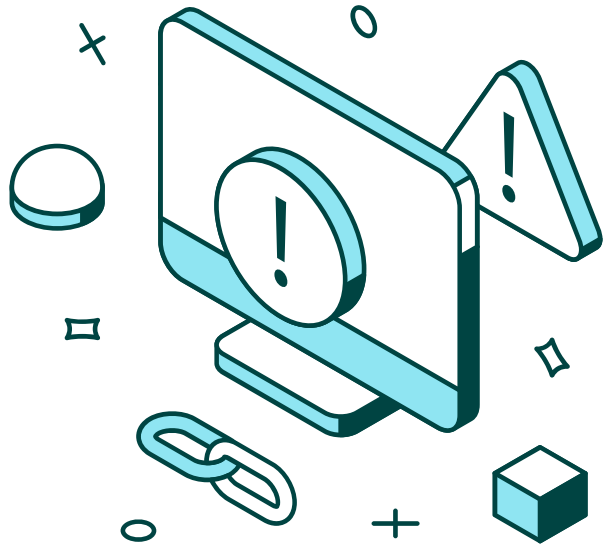
¿Qué hace que el phishing y el ransomware sean amenazas tan omnipresentes? Algunas razones:

- Los kits y servicios que se ofrecen en la dark Web tienen una barrera de entrada baja que permite utilizarlos incluso a atacantes con conocimientos limitados.
- Las operaciones descentralizadas y la complejidad de perseguir la delincuencia internacional hacen que el ransomware y el phishing tengan un riesgo bastante bajo y una recompensa potencialmente muy alta.
- El phishing y el ransomware aprovechan el error humano, que es difícil de prevenir y los convierte en métodos universales que pueden dirigirse a cualquier sector.

Como estas amenazas siguen dando sus frutos año tras año, es poco probable que los atacantes abandonen estas técnicas a corto plazo. En consecuencia, las organizaciones deben comprometerse igualmente con prácticas de Seguridad proactivas, como el pentesting, para reducir el riesgo en la medida de lo posible.

Y hablando de la necesidad de una Seguridad proactiva, la falta de parches (66 %) es la tercera preocupación más común, un 17 % más que el año pasado (Figura 3). Cuando se descubren vulnerabilidades, la única forma de garantizar que un atacante no pueda aprovecharse de ellas es aplicar un parche en cuanto esté disponible. Y con más de 1000 vulnerabilidades en el Catálogo de Vulnerabilidades Explotadas Conocidas de CISA, la necesidad de aplicar actualizaciones oportunas es más crítica que nunca. Aunque parece una práctica bastante sencilla, existen múltiples desafíos que pueden impedir la aplicación rutinaria de parches en una organización. La falta de personal puede hacer que la aplicación de parches pierda prioridad. Los problemas de compatibilidad y los periodos de inactividad o interrupción de la actividad también pueden causar retrasos. Y la creciente complejidad de los entornos informáticos hace que los profesionales de IT y Seguridad se enfrenten a cientos de parches. Las organizaciones deben recurrir a la ayuda de herramientas de gestión de vulnerabilidades y pentesting, que pueden automatizar el escaneado, priorizar los parches en función del riesgo y garantizar que se han aplicado correctamente.

Con los atacantes adaptando continuamente sus técnicas para eludir los controles de Seguridad y explotar las vulnerabilidades emergentes, la preocupación por el phishing, el ransomware, la falta de parches y otras amenazas a la Seguridad no es, desde luego, injustificada. Sin embargo, los expertos en Seguridad no se quedan de brazos cruzados: también perfeccionan sus estrategias, participan regularmente en iniciativas de colaboración y aprovechan las nuevas investigaciones. Y al disponer de herramientas ofensivas y defensivas, participar en la capacitación periódica del *blue team* y fomentar una cultura de vigilancia, las organizaciones pueden poner de su parte para adelantarse a los atacantes.



Desafíos generales del pentesting

¿A qué desafíos se enfrenta su organización con su programa de pentesting?

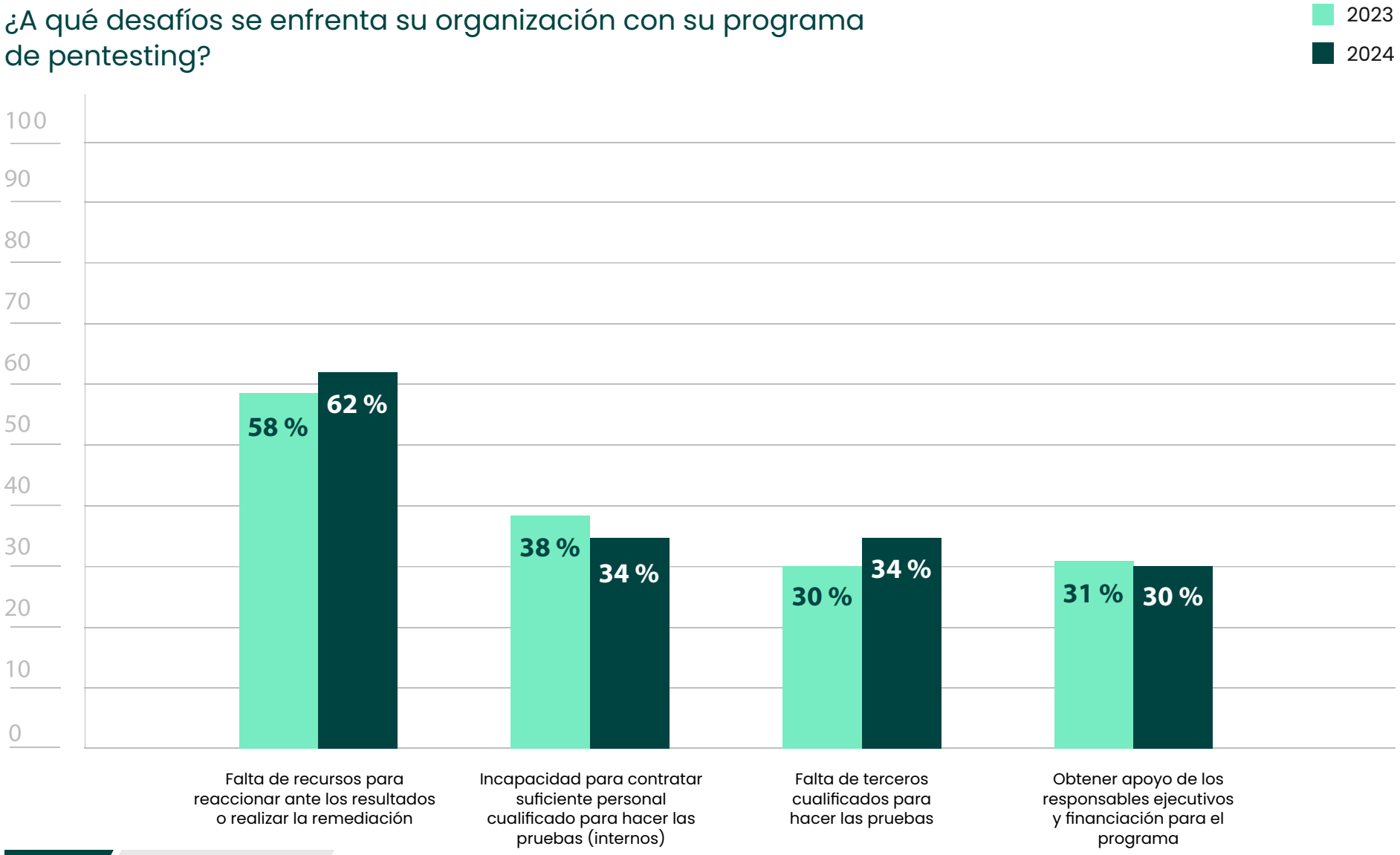


Figura 4: Desafíos del pentesting

Desafíos generales del pentesting

Aunque el pentesting es claramente una práctica de Seguridad ofensiva valiosa, el despliegue y la gestión de iniciativas de pentesting conllevan desafíos. La falta de recursos para actuar en función de los resultados y aplicar medidas de remediación sigue siendo el problema más común (62 %), un 6 % más que el año pasado (Figura 4). Esto puede ocurrir por varias razones. En algunos casos, es posible que los responsables de la toma de decisiones no comprendan del todo la urgencia o la gravedad de los resultados del pentesting. Especialmente cuando se realiza el pentesting para cumplir con la normativa, puede haber una percepción errónea de que cumplir con los mandatos de cumplimiento significa que la organización es totalmente segura. Si los cambios son sustanciales y pueden perturbar el funcionamiento normal de la empresa, también puede haber reticencias por parte de los responsables de la toma de decisiones a la hora de aprobar los cambios necesarios. Pero la razón más común es simplemente que los presupuestos y el personal limitados crean prioridades que compiten entre sí y las medidas de remediación quedan relegadas a un segundo plano.

Además de abogar por un mayor apoyo a los esfuerzos de las medidas de corrección, los equipos de Seguridad deben asegurarse de que sus planes de corrección estén tan claramente delineados como sus planes de pentesting. Si bien los buenos informes de pentesting incluyen recomendaciones de seguimiento, un plan de remediación debe ser más detallado. Esto incluye esbozar los pasos específicos necesarios para abordar los riesgos de mayor prioridad, los recursos necesarios, los plazos y las dependencias.

Tanto la incapacidad para contratar personal cualificado (34 %) como la falta de terceros cualificados (34 %) son pruebas probables y continuas del déficit de competencias en Ciberseguridad (Figura 4). El pentesting parece especialmente afectado por esta escasez continua. Según el estudio 2023 Cybersecurity Workforce Study de (ISC)², el pentesting era la cuarta habilidad más común que faltaba en los equipos SOC. La falta de terceros cualificados indica sin duda que la demanda supera a la oferta.

Aunque existan servicios de pentesting, esto no significa necesariamente que estén "cualificados". Por desgracia, hay equipos de pentesting cuyos servicios consisten en poco más que unos pocos escaneos automatizados. Pueden utilizar tácticas de marketing engañosas, como ofrecer precios irrealmente bajos o testimonios falsos. Además, los actores de amenazas han empezado a crear empresas falsas y a hacerse pasar por empresas legítimas de pentesting para obtener acceso a información sensible o credenciales. Esto destaca la necesidad de que las organizaciones investiguen cuidadosamente a los posibles proveedores para asegurarse de que eligen a un equipo respetable con la experiencia adecuada. Unirse a la creciente lista de espera puede ser frustrante, pero sin duda es mejor que ser estafado.

Cumplimiento normativo y pentesting

Como era de esperar, PCI DSS es la normativa más común para la que los encuestados declararon haber utilizado pentesting (43 %) (Figura 5). Aunque la mayoría de las normativas exigen evaluaciones de Seguridad, PCI DSS exige explícitamente el pentesting. El requisito 11.3 exige que las organizaciones realicen pentesting externo e interno al menos una vez al año y después de cualquier cambio significativo en la infraestructura o las aplicaciones.

Incluso cuando no se requiere explícitamente, el pentesting se utiliza comúnmente para cumplir con los requisitos de evaluación de Seguridad y ayudar a verificar el cumplimiento de otras regulaciones, demostrando a los auditores u otras autoridades que las medidas de Seguridad obligatorias están en su lugar o funcionan correctamente. Con un aumento del 11 % con respecto al año pasado (gráfico 6), cada vez son más las organizaciones que tienen que aumentar la cantidad de pentesting que realizan, probablemente debido a las actualizaciones y adiciones de la legislación y la normativa en materia de Ciberseguridad.

Las iniciativas de cumplimiento se han convertido en una prioridad mundial, y se esperan más cambios en los próximos años. La Directiva actualizada sobre seguridad de las redes y de la información (NIS2) amplió sus requisitos para la gestión de riesgos y debe incorporarse a la legislación nacional de todos los países miembros de la UE antes de octubre de 2024. La Ley de Resiliencia Operativa Digital (DORA) agregará requisitos de gestión de riesgos a las entidades financieras a partir de 2025. Según Gartner, el 75 % de la población mundial tendrá sus datos personales bajo normas de privacidad a finales de 2024.

Curiosamente, hubo un aumento del 23 % en los encuestados que necesitaban ampliar el alcance de su pentesting (Figura 6). Esto puede deberse a varias razones. Por ejemplo, los ataques a la cadena de suministro han dado lugar a un mayor escrutinio sobre la gestión de riesgos de terceros, por lo que las organizaciones pueden sentirse más presionadas para incluir los sistemas y redes de terceros en los compromisos. Además, si las normativas nuevas o actualizadas exigen que las organizaciones evalúen más sistemas, las limitaciones presupuestarias pueden llevarles a ampliar el alcance en lugar de aumentar la cantidad de pruebas que realizan.

Otras alteraciones comunes en las estrategias de pentesting incluyeron un énfasis adicional en las pruebas de Seguridad de red (36 %) y campañas de phishing/ingeniería social (30 %). Solo el 9 % de los participantes, un 7 % menos que el año pasado, declararon que sus estrategias de pentesting no se habían visto afectadas por las necesidades de cumplimiento, lo que ilustra la influencia que el cumplimiento sigue teniendo en los enfoques de pentesting.

¿Utiliza el pentesting para alguna de estas normativas de cumplimiento?

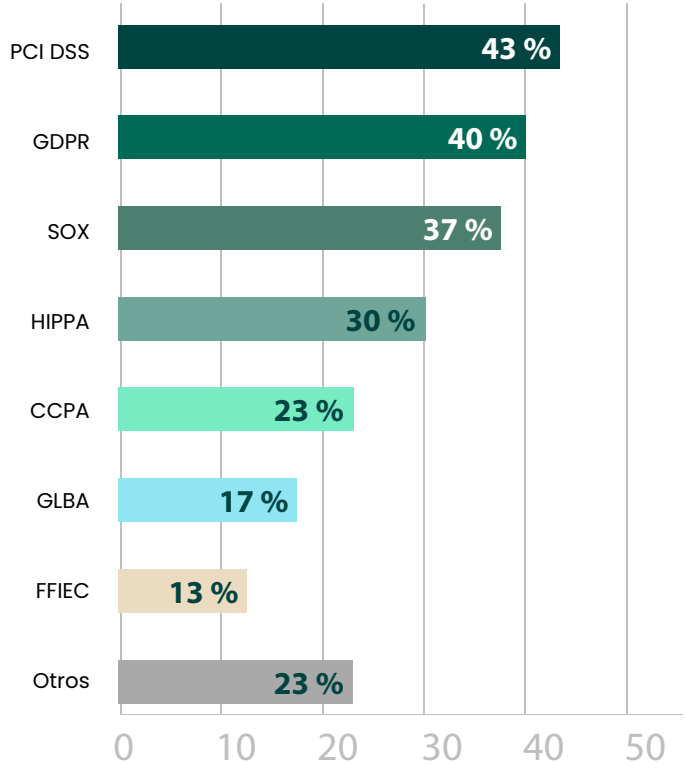


Figura 5: Normativa de cumplimiento para la que se utiliza pentesting

Cumplimiento normativo y pentesting

¿Cómo ha afectado el aumento de las regulaciones o mandatos de cumplimiento a su estrategia o a sus prioridades de pentesting?

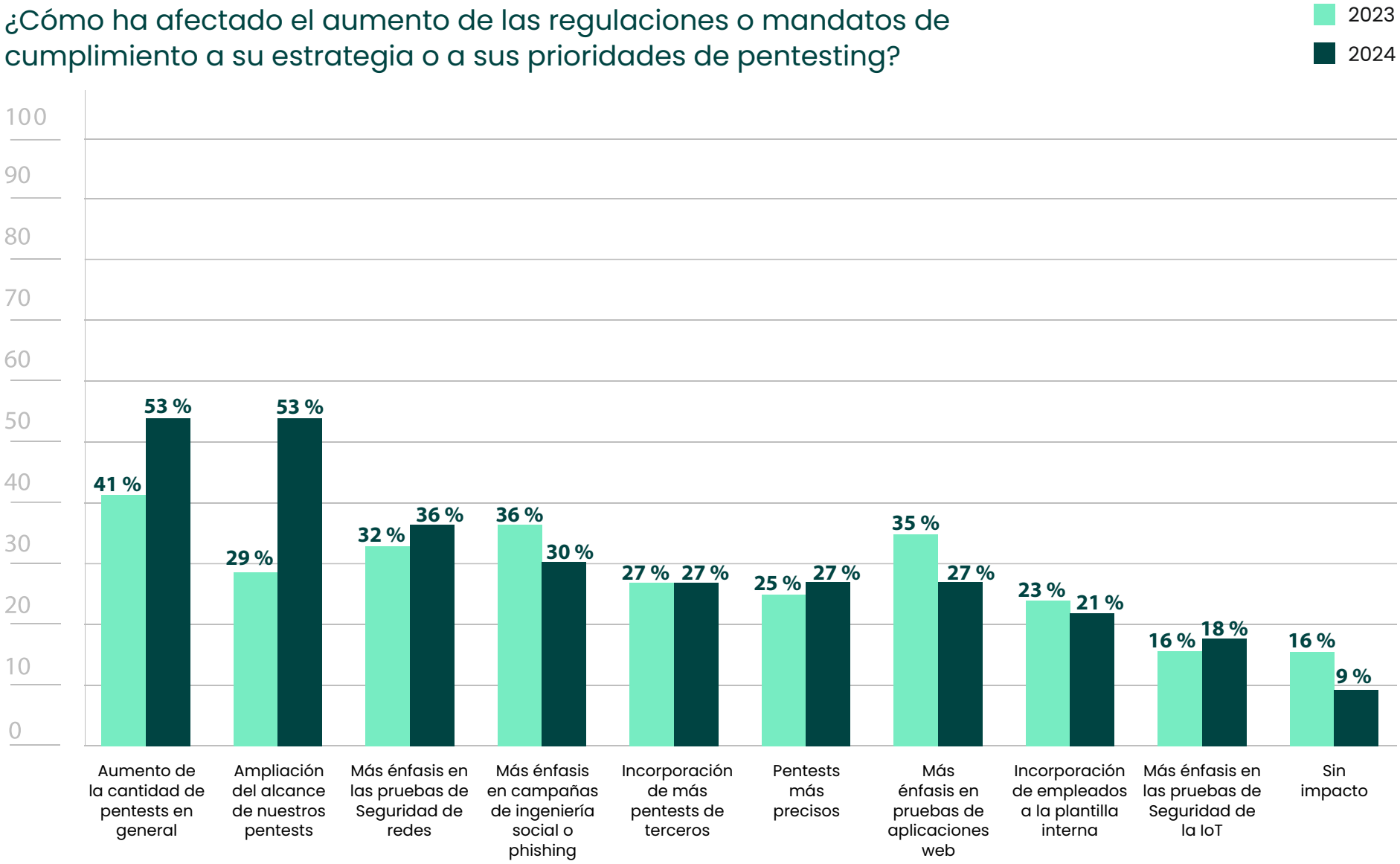


Figura 6: Impacto de los mandatos de cumplimiento en las estrategias de pentesting

Phishing

Con estimaciones de más de tres mil millones de emails de phishing enviados al día, no es de extrañar que el phishing fuera la preocupación de Seguridad más común de los encuestados (80 %) (Figura 3).

Aunque los ataques de phishing no son nada nuevo, los atacantes siempre encuentran formas de cambiar sus tácticas. Por ejemplo, la IA generativa ha provocado una explosión de emails de phishing, con un aumento del 1.265 % de correos maliciosos desde 2022. Los ataques de Business Email Compromise (BEC) también se han vuelto cada vez más comunes, y el FBI recibió 21.489 denuncias solo en 2023. Y la principal amenaza de ingeniería social el año pasado fue el vishing híbrido. Esta estrategia de ataque en varias fases suele utilizar un email falsificado que solicita a la víctima que realice un seguimiento por teléfono. Esto permite al atacante saltarse los filtros de Seguridad básicos, ya que la carga útil es solo un número de teléfono.

Dado que el phishing está más extendido que nunca, fue decepcionante ver una tendencia a la baja en la frecuencia de los ejercicios de ingeniería social. Los ejercicios trimestrales disminuyeron un 7 %, mientras que aumentaron un 6 % los participantes que nunca realizan estos ejercicios (Figura 7). Aunque no se trata de grandes cambios, dada la prevalencia de estos ataques, los ejercicios de ingeniería social deberían ir en aumento.

Los ejercicios de simulación son una de las únicas formas de reducir el riesgo de ataques de ingeniería social. Existe la percepción errónea de que estos ejercicios se limitan a concienciar a los empleados sobre las tácticas utilizadas por los atacantes. Sin embargo, las simulaciones de phishing ayudan a validar las prácticas de Seguridad, proporcionando datos sobre la eficacia con que los filtros de email detectan los mensajes de phishing y midiendo la eficacia de los programas de capacitación. También pueden ayudar a mejorar la respuesta ante incidentes, garantizando que los equipos de Seguridad puedan responder eficazmente a ataques reales de phishing.

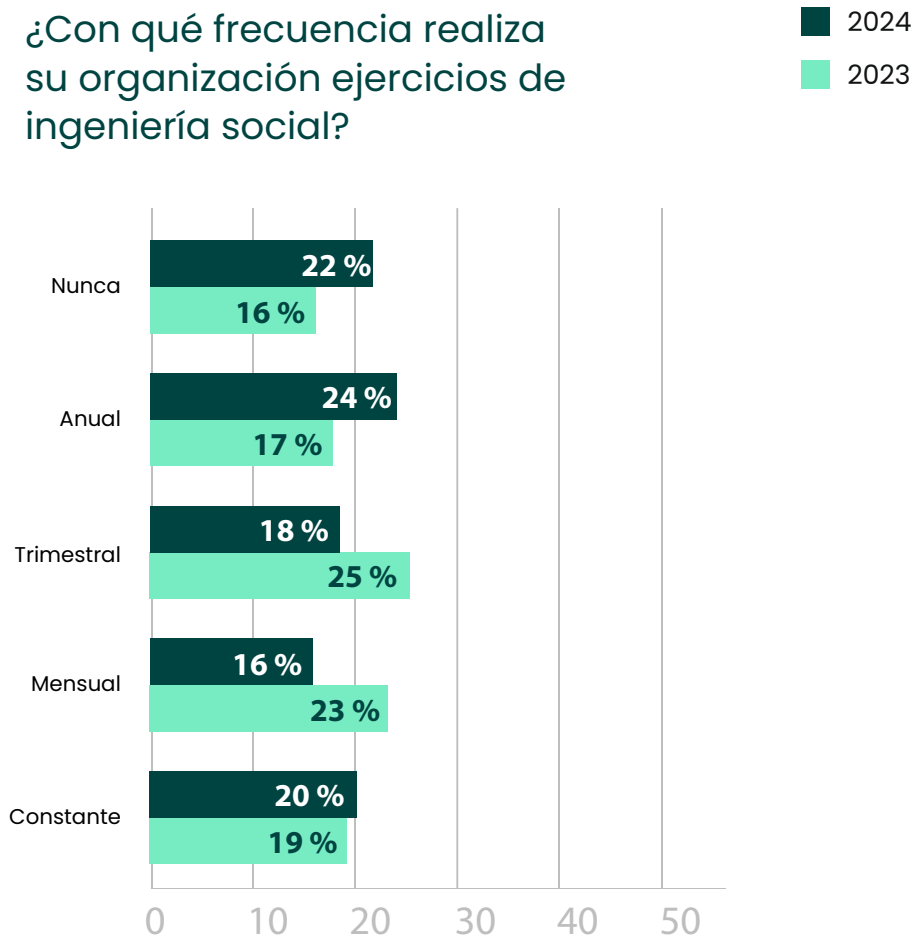


Figura 7: Frecuencia de los ejercicios de ingeniería social

Frecuencia de pentesting

Al igual que con las campañas de phishing, se produjo un ligero descenso en la frecuencia general del pentesting, con una disminución del 9 % en las pruebas trimestrales, un aumento del 5 % en las organizaciones que realizan pruebas un par de veces al año (43 %) y un aumento del 3 % en las organizaciones que nunca realizan pentests (17 %) (Figura 8).

No existe un número mágico cuando se trata de la frecuencia del pentesting. En cambio, depende del tamaño de la organización, la complejidad de su infraestructura técnica, el tipo de datos que maneja y la normativa de cumplimiento aplicable. La mayoría de las organizaciones deberían realizarlo al menos una vez al año, pero deberían realizarse pruebas adicionales si se introducen cambios sustanciales en el entorno informático, si se descubren vulnerabilidades o si se ha producido un incidente de Seguridad.

Otra razón para considerar más de una prueba al año es obtener garantías de que las vulnerabilidades identificadas durante el pentesting inicial se han abordado y remediado adecuadamente. Esto incluye confirmar la correcta aplicación de parches y la eficacia de nuevos controles de Seguridad como firewall, sistemas de detección/prevención de intrusiones y controles de acceso.

Volver a probar a tiempo garantiza que las correcciones no se conviertan en nuevos fallos. Sin embargo, sigue siendo difícil conseguir que se aprueben, como demuestran los encuestados que encuentran dificultades en la falta de seguimiento tras el pentesting (62 %) (Figura 4). La repetición de las pruebas puede considerarse a menudo menos urgente, ya que muchas partes interesadas consideran que los esfuerzos iniciales son suficientes o se muestran reticentes a la necesidad de introducir cambios adicionales.

En última instancia, aunque tanto las pruebas como las repeticiones de pruebas deberían realizarse más a menudo, las mejores prácticas suelen chocar con los aspectos prácticos del mundo real en cuanto a recursos y presupuestos. En estos casos, adoptar un enfoque estratificado de la Seguridad proactiva puede resultar eficaz, ya que las soluciones de gestión de vulnerabilidades pueden ayudar a cerrar las brechas entre las instancias de pentesting. Estas soluciones suelen estar muy automatizadas y pueden programarse fácilmente para que se ejecuten diaria o semanalmente. Esto garantiza que la organización pueda mantenerse al día con algún tipo de evaluación.

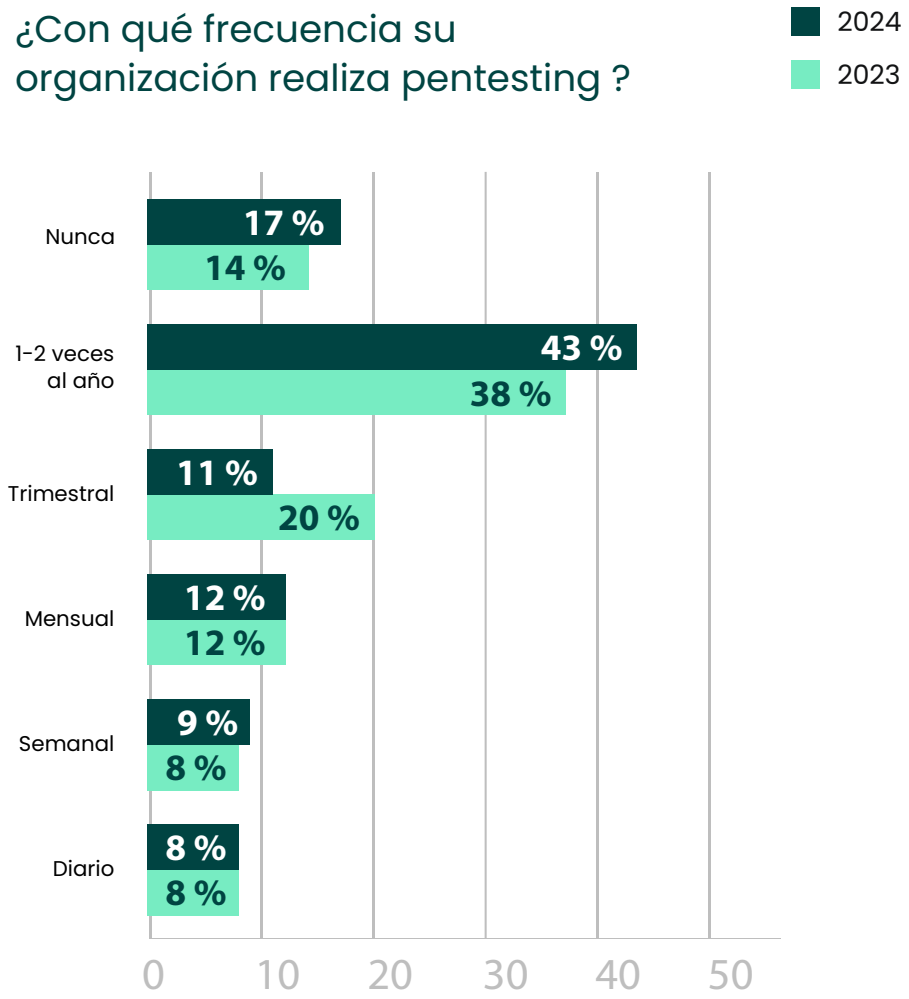


Figura 8: Frecuencia de pentesting

Esfuerzos internos de pentesting

Las organizaciones pueden decidir agregar capacidades internas de pentesting por varias razones. Un equipo interno de pentesting está más familiarizado con las operaciones empresariales y la infraestructura de IT, lo que facilita la adaptación de las metodologías y los enfoques de las pruebas a las necesidades de Seguridad específicas de la organización. También pueden realizar pruebas con más frecuencia, lo que les permite llamar la atención sobre las amenazas emergentes a tiempo, participar potencialmente en el proceso de remediación y volver a realizar pruebas para asegurarse de que las correcciones se han aplicado correctamente.

Este año se observa un descenso del 15 % en el número de encuestados que disponen de equipos internos de pentesting (Figura 9). Sin embargo, el porcentaje de participantes que ya no tienen equipos se mantuvo estable en el 14 %, por lo que no parece indicar que las organizaciones estén encontrando menos útil el pentesting interno. En cambio, este descenso puede explicarse por el aumento del 16 % de los encuestados que recurren exclusivamente a terceros (Figura 10).

La razón más común por la que las organizaciones no realizan pentesting interno es la falta de necesidad de un equipo/pentester a tiempo completo (55 %) (Figura 10). Las organizaciones más pequeñas pueden tener entornos informáticos relativamente sencillos o una superficie de ataque pequeña, lo que hace menos evidente la necesidad de realizar pentesting frecuente o exhaustivo. También es posible que no dispongan de los controles de Seguridad básicos, los conocimientos sobre Seguridad o los recursos necesarios para alcanzar el nivel de madurez de Seguridad que se requiere para empezar a realizar pentesting. Alternativamente, las organizaciones pueden encontrar sus necesidades lo suficientemente satisfechas haciendo que el pentesting sea un aspecto de una función de Ciberseguridad más amplia.

Contar con funciones de Ciberseguridad más generales ha sido una forma habitual para que las organizaciones hagan frente al déficit de competencias en Ciberseguridad. La falta de competencias es también la segunda razón más común para no contar con un equipo interno de pentesting (39 %) (Figura 10). Según el estudio 2023 Cybersecurity Workforce Study de (ISC)², la brecha de cualificación sigue aumentando, un 12,6 % desde el año pasado, con una escasez récord de casi cuatro millones.

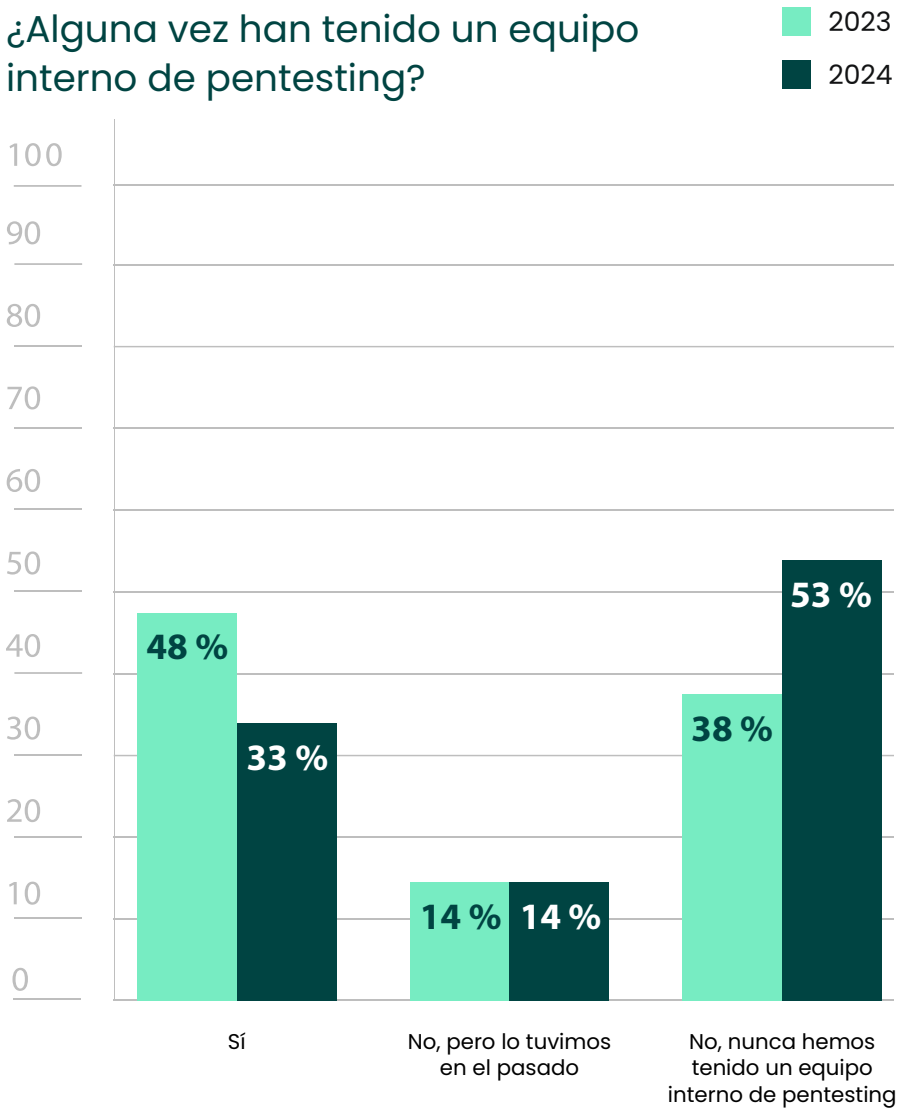


Figura 9: Pentesting interno

Esfuerzos internos de pentesting

¿Por qué su organización no tiene un equipo interno de pentesting?

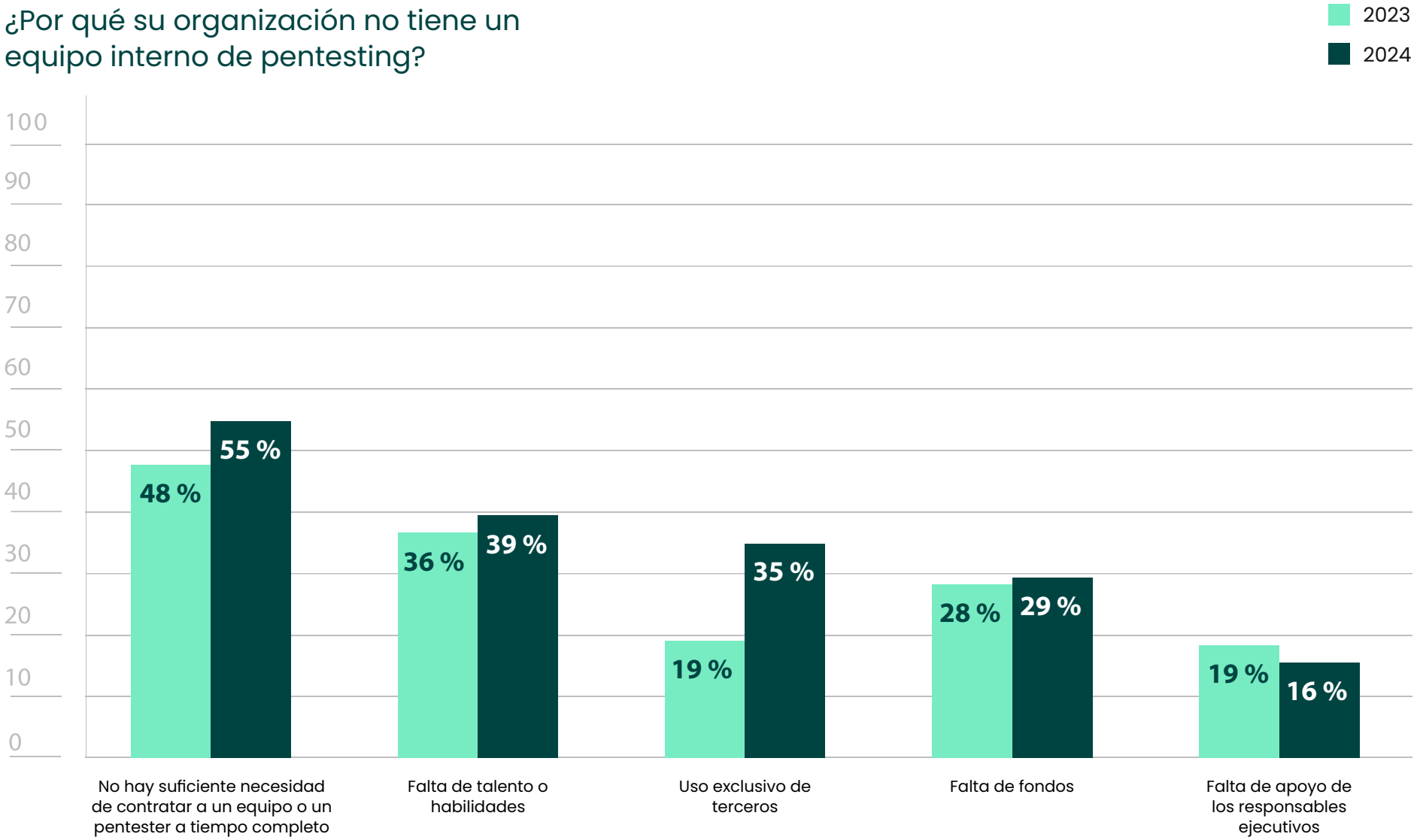


Figura 10: Razones para no tener un equipo interno de pentesting

Servicios de terceros

¿Cuál es la división actual entre el uso de recursos de pentesting internos y externos?

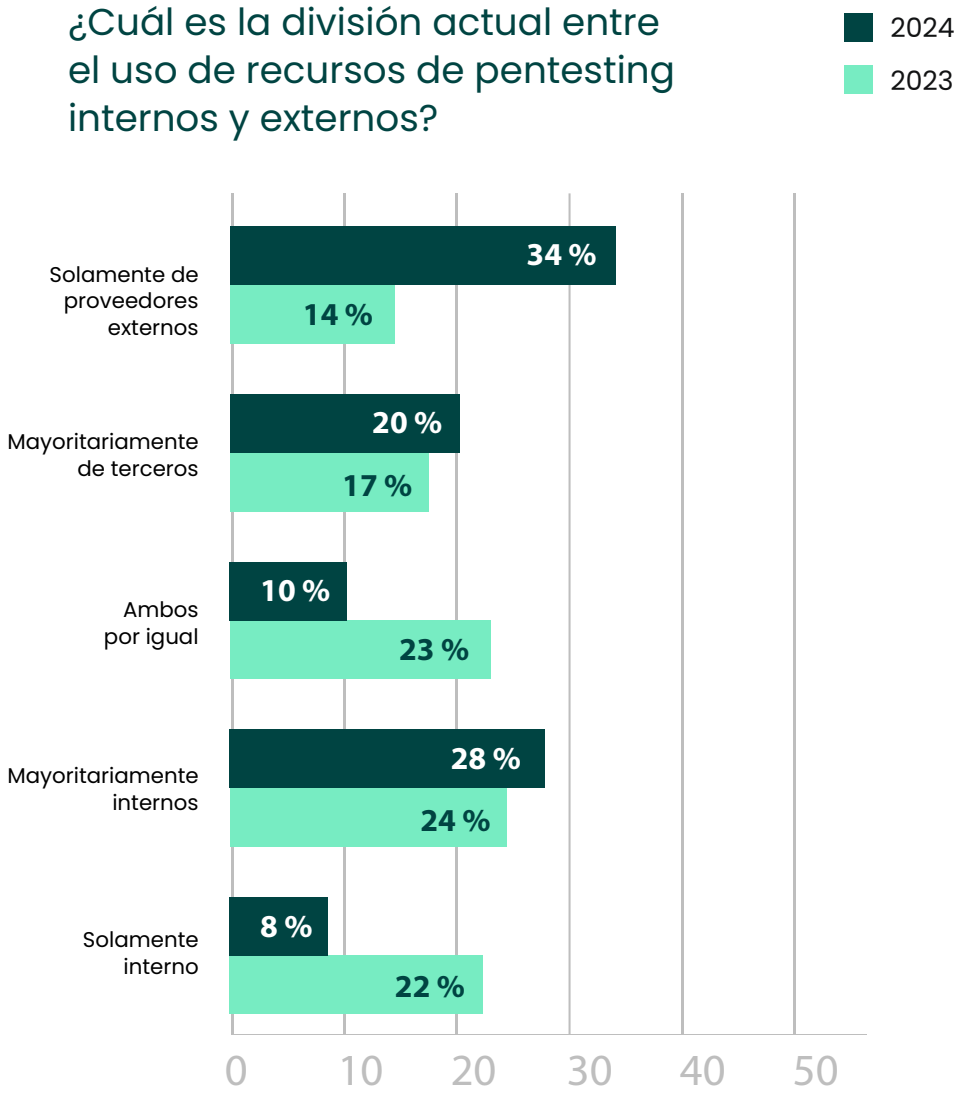


Figura 11: ¿Cuál es la división actual entre el uso de servicios de pentesting internos y externos?

¿Con qué frecuencia cambia el servicio de pentesting externo con el que trabaja?

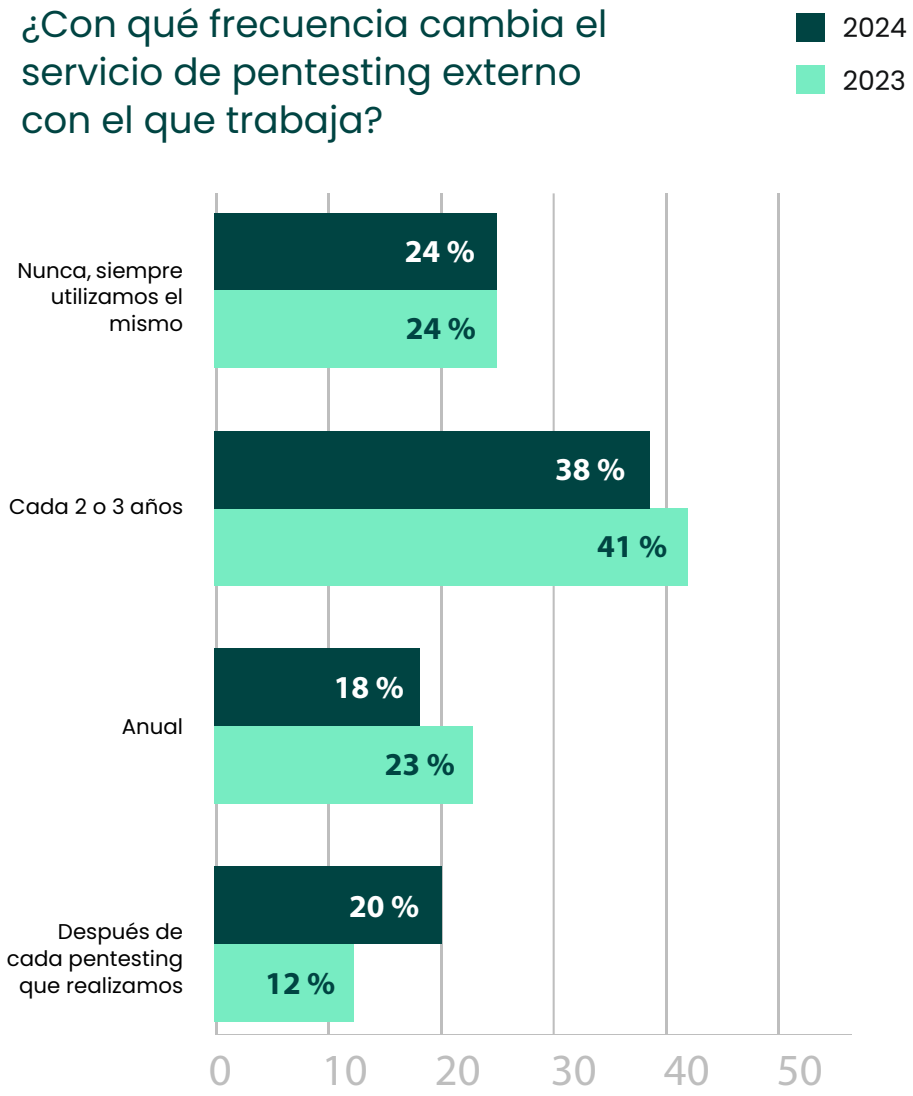


Figura 12: Frecuencia de rotación de los servicios de pentesting de terceros

Servicios de terceros

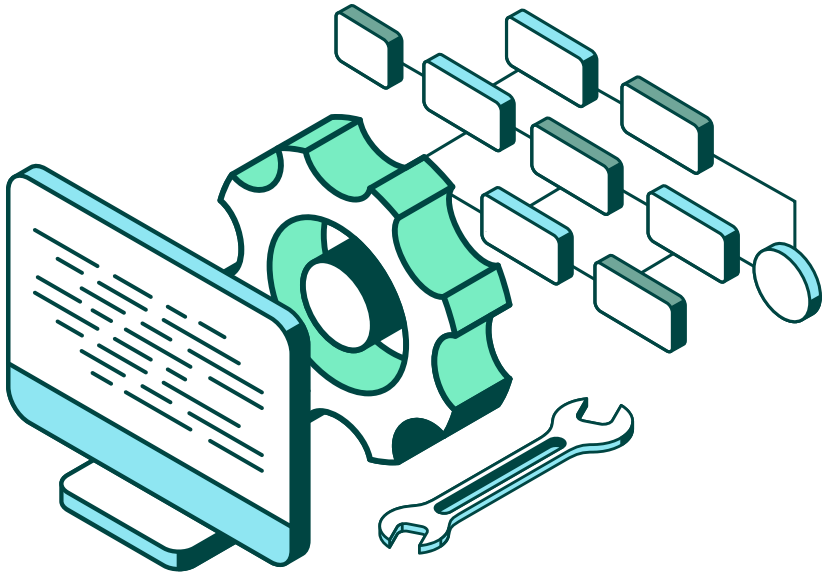
El pentesting realizado por terceros aumentó drásticamente este año, ya que un 92 % de los encuestados recurrió a equipos de terceros de alguna manera (Figura 11). Como ya se ha dicho, esto coincide con el aumento del 16 % de encuestados que recurren exclusivamente a terceros (gráfico 10).

La razón principal por la que se solicitan los servicios de terceros es aún por su punto de vista externo y objetivo (62 %) (Figura 13). Dado que los equipos de Seguridad están tan familiarizados con sus propias infraestructuras, los servicios de terceros pueden ayudar a descubrir puntos ciegos, sesgos y suposiciones que el personal interno puede pasar por alto. Además, como los servicios de terceros se centran exclusivamente en las pruebas, suelen estar más al día con las amenazas emergentes, las tendencias de ataque y las mejores prácticas. Aunque las diferentes competencias parecen ir de la mano de un punto de vista externo, se produjo un descenso del 17 % en la cantidad de participantes que utilizaron servicios de terceros para sus diferentes competencias (33 %). Quizás los participantes asumieron que esta opción solo era relevante para las organizaciones con evaluadores internos, ya que "diferentes" puede interpretarse como "diferentes de las habilidades del equipo interno de pentesting". Si este es el caso, la reducción del uso de equipos internos explicaría esta caída.

Se produjo un aumento del 11 % en el uso de servicios de terceros para el cumplimiento (56 %) (Figura 13). Esto coincide con el aumento de la cantidad de pentests realizado para garantizar el cumplimiento (Figura 6). El cumplimiento también se cita con frecuencia como la razón por la que las organizaciones cambian de proveedor. Sin embargo, no está claro con qué frecuencia las organizaciones deberían cambiar de proveedor. Esto puede explicar por qué hay tanta variación: el 24 % no cambia nunca, el 38 % cambia cada 2 a 3 años, el 18 % cambia cada año y el 20 % cambia después de cada prueba (gráfico 12). La verdad es que ninguna normativa exige explícitamente que las organizaciones cambien de proveedor, solo es una práctica generalmente recomendada.

Dicho esto, con las dificultades para encontrar equipos de terceros cualificados (figura 4) y el deseo de consolidar proveedores (figura 22), a las organizaciones puede resultarles beneficioso encontrar proveedores con equipos grandes. Las organizaciones pueden aprovechar la rotación interna para asegurarse de que se asigna a distintos miembros del equipo la realización de las pruebas, lo que permite obtener nuevas perspectivas, conocimientos variados y evaluaciones independientes, todo ello con un único proveedor de confianza.

Las organizaciones también pueden seguir beneficiándose de agregar algún componente de pentesting interno. Las pruebas internas pueden ser especialmente útiles para repetirlas. Puede resultar difícil justificar ante las partes interesadas la necesidad de contratar un servicio externo que vuelva tan pronto para validar los esfuerzos de remediación. Hacer que un profesional de la Ciberseguridad general asuma las tareas de pentesting puede ser un caso más fácil. Además, contar con alguien que sepa utilizar herramientas de pentesting puede ser especialmente útil si las organizaciones siguen enfrentándose al desafío de encontrar terceros cualificados (Figura 4). Si la espera para la disponibilidad resulta más larga de lo previsto, un evaluador interno puede ayudar a cerrar la brecha.



Servicios de terceros

¿Por qué su organización utiliza expertos en pentesting externos?

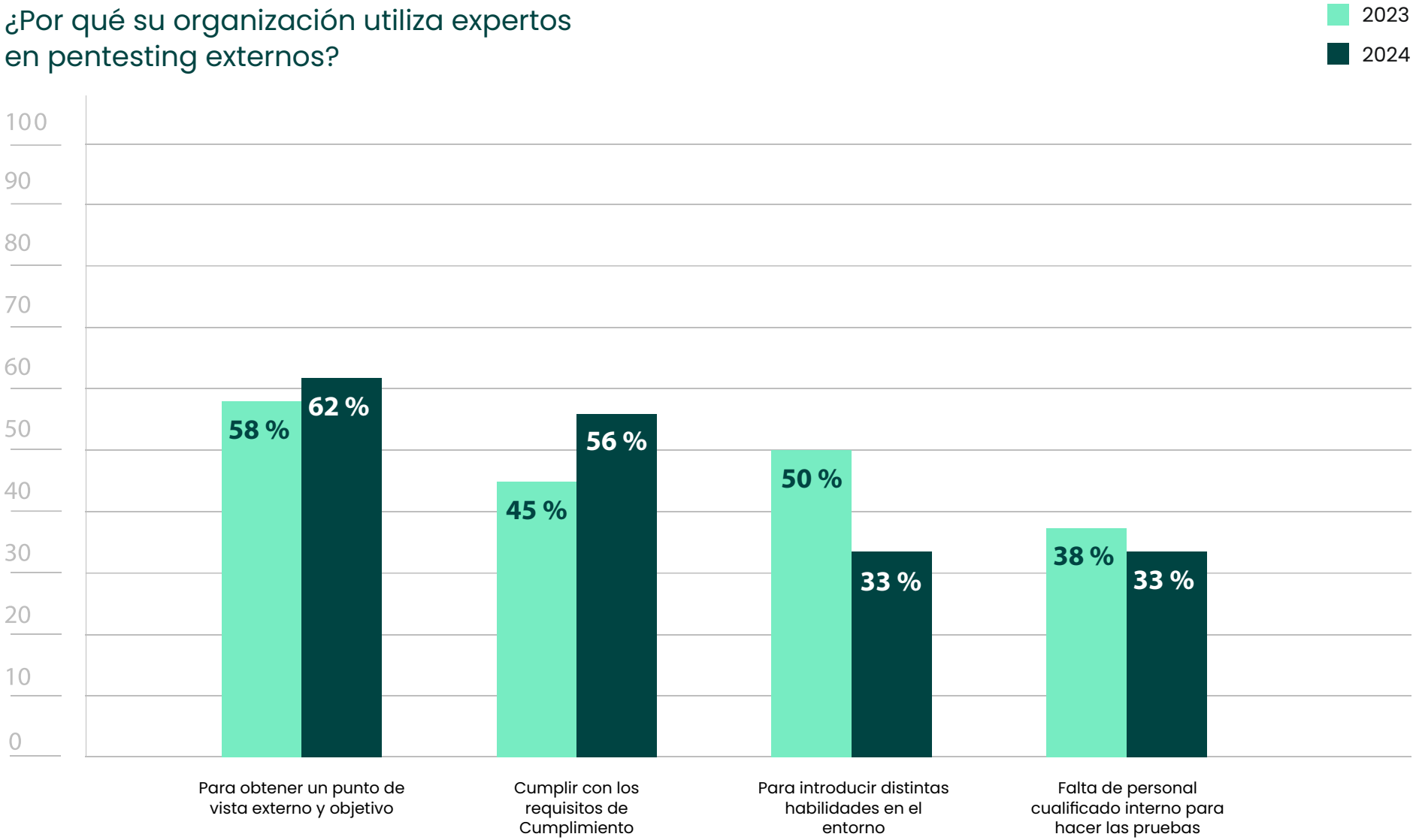


Figura 13: Razones para utilizar los servicios de pentesting de terceros

Herramientas de pentesting

Las herramientas de pentesting son una categoría amplia que puede incluir herramientas especializadas (escáners de puertos, descifradores de contraseñas o herramientas de inyección de SQL) y herramientas más completas que ofrecen diversas funciones para centralizar el proceso de pruebas. Las herramientas de pentesting suelen dividirse en dos categorías: de código abierto (open source) y empresariales. Las herramientas de código abierto suelen ser desarrolladas y mantenidas por la comunidad de Ciberseguridad. Las herramientas empresariales son soluciones comerciales ofrecidas por proveedores de Ciberseguridad. Aunque las herramientas de código abierto son gratuitas, a menudo carecen de funciones avanzadas y no pueden ofrecer un soporte amplio. Las herramientas para empresas tienen un precio, pero suelen ofrecer funciones diseñadas para cumplir con la normativa y satisfacer las necesidades de entornos informáticos complejos.

Este año, el 28 % de los encuestados no utiliza herramientas de pentesting en absoluto, lo que supone un notable aumento del 27 % (Figura 14). Esto se debe, al menos en parte, a la disminución de la cantidad de encuestados con equipos internos de pentesting (Figura 9). Sin embargo, este aumento, sumado al incremento del uso exclusivo de herramientas de código abierto (33 %) (Figura 14) y al aumento del porcentaje de encuestados que consideran el costo como criterio principal (75 %) (Figura 16), también refleja probablemente la inflación y la volatilidad económica mundial. Con el crecimiento del presupuesto de Ciberseguridad un 65 % menor el año pasado, muchas organizaciones pueden estar confiando más en el código abierto cuando es posible.

Sin embargo, sigue habiendo un gran interés por las herramientas comerciales de pentesting, sobre todo por las características/funcionalidades que pueden ofrecer (73 %) (Figura 16). Los informes (65 %), las plantillas/capacidades de automatización (65 %) y disponer de una amplia biblioteca de amenazas (65 %) son las tres capacidades más buscadas en las herramientas de pentesting de pago (Figura 15). La elaboración de informes es esencial tanto para verificar como para demostrar el cumplimiento de las normas de Seguridad. Las capacidades de automatización no solo automatizan por completo las pruebas básicas, sino que también pueden permitir un modelo híbrido de pentesting. La automatización se encarga de las tareas rutinarias, lo que permite al evaluador centrarse en cuestiones más complejas. Esto acelera el proceso de pruebas sin aumentar la cantidad de empleados ni sacrificar la precisión. Por último, una biblioteca de amenazas amplia ofrece acceso a *exploits* escritos por expertos que se actualizan periódicamente, lo que hace que el proceso de pentesting sea más eficaz y seguro.

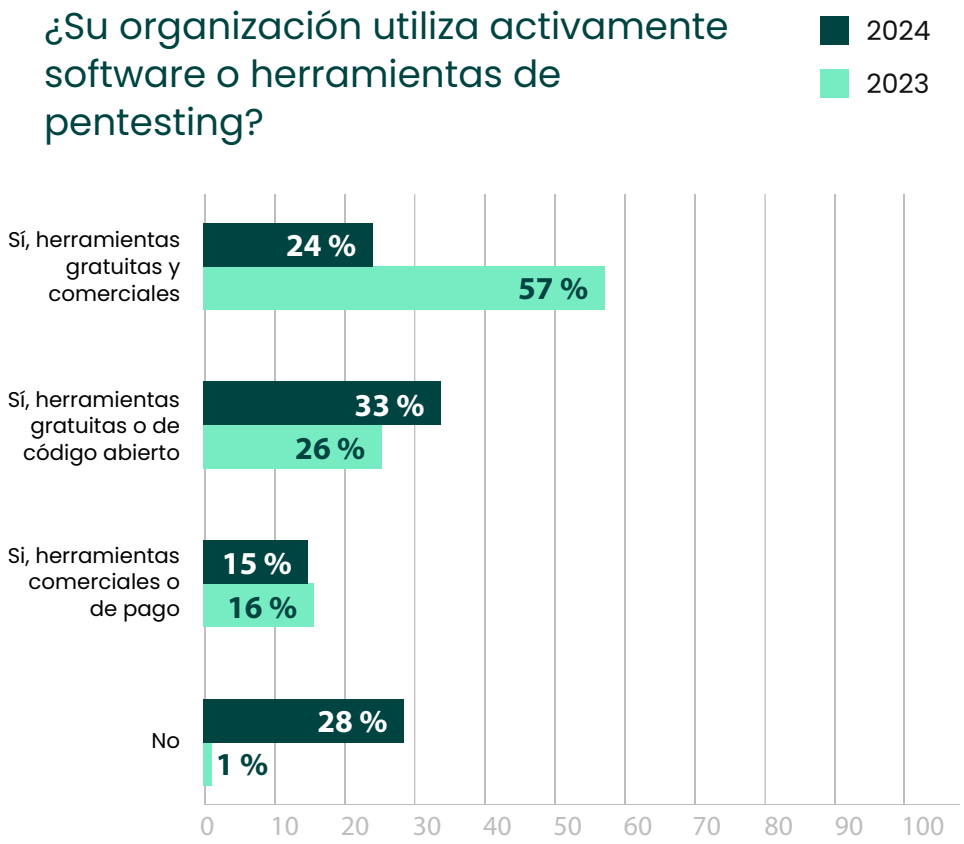


Figura 14: Uso activo de software de pentesting

Herramientas de pentesting

¿Cuáles son las funcionalidades más importantes del software o las herramientas de pentesting comerciales o de pago?

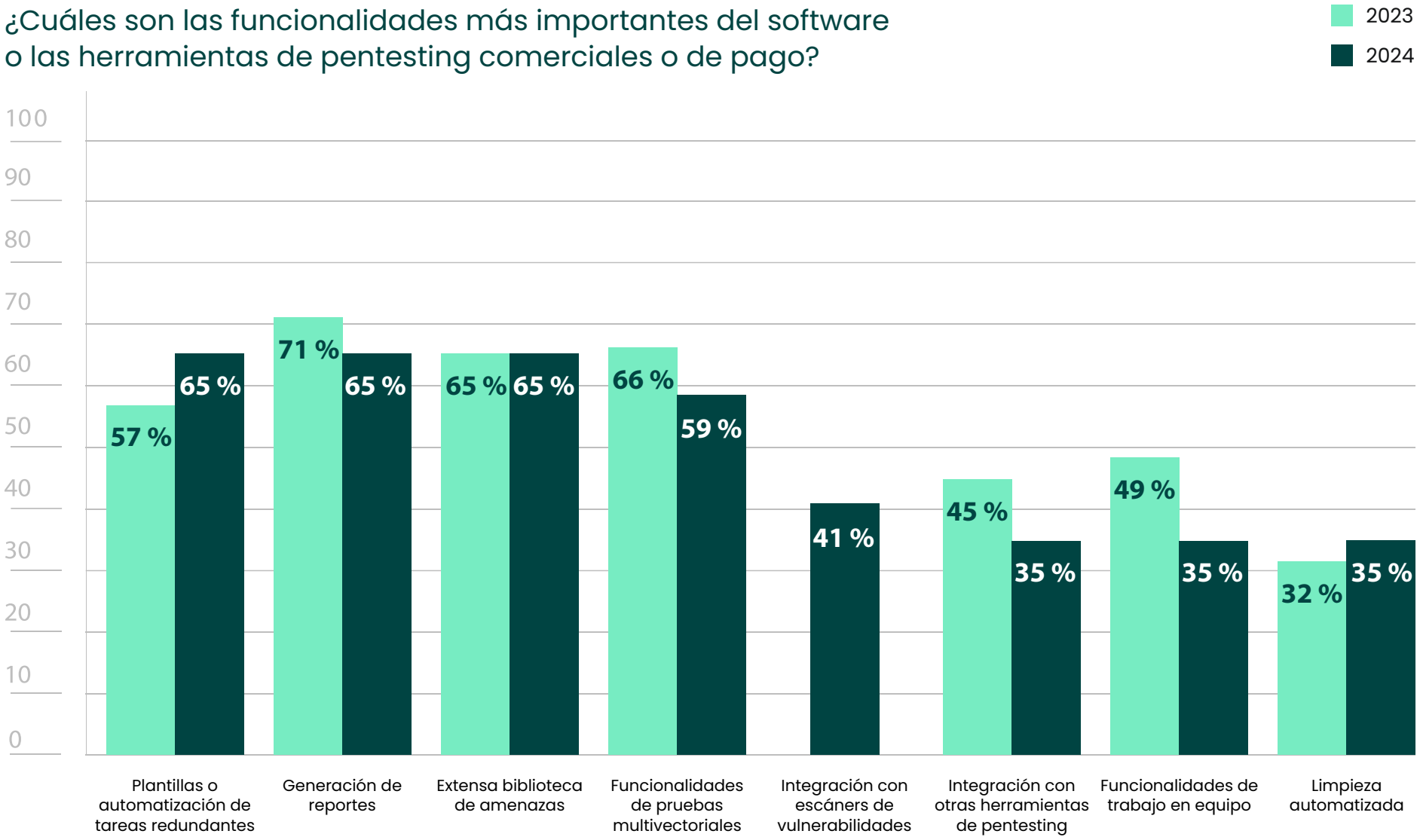


Figura 15: Funcionalidades clave del software de pentesting

Herramientas de pentesting

¿Qué criterios considera más importantes al evaluar el software de pentesting?

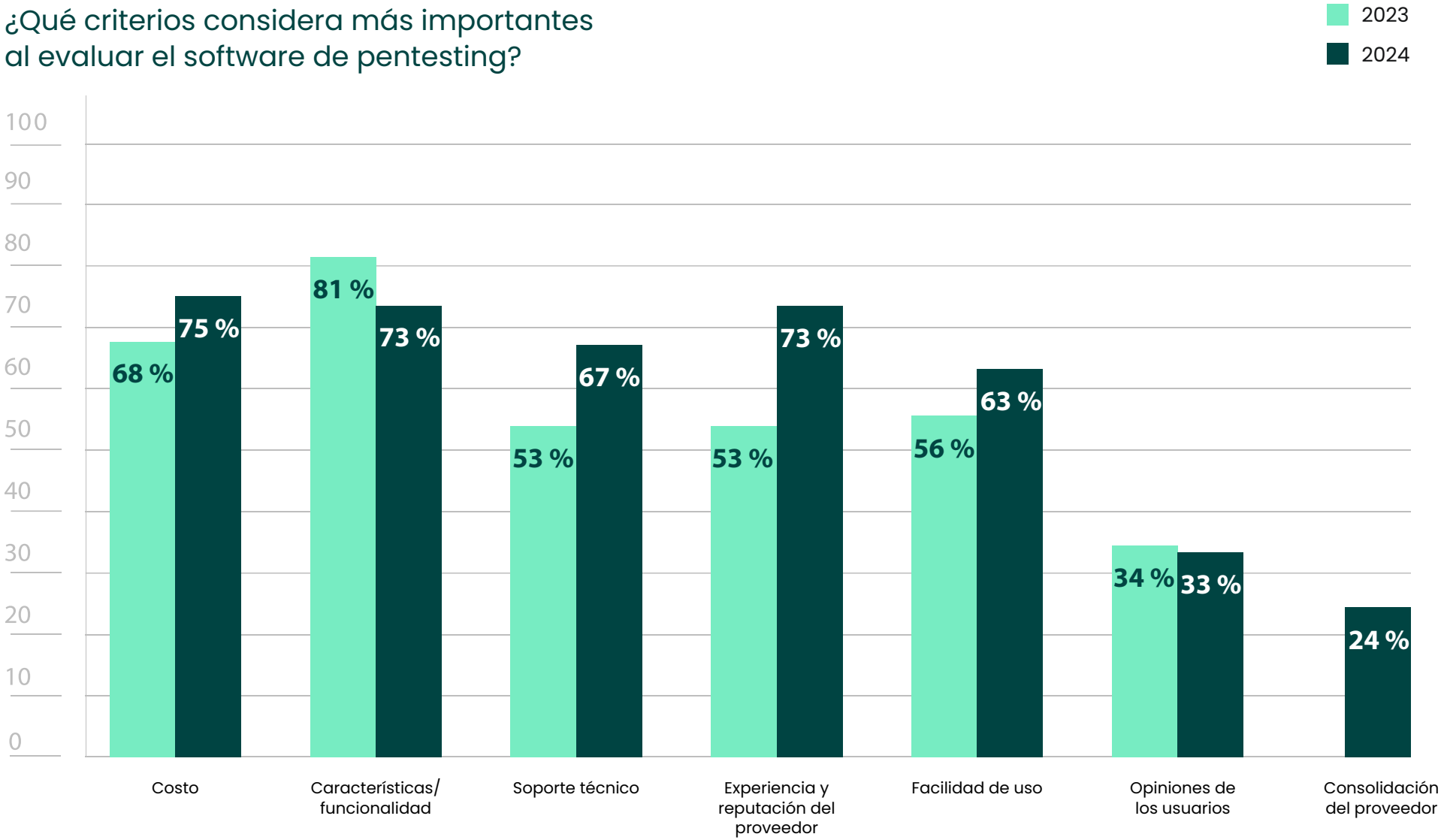


Figura 16: Criterios más importantes al evaluar un software de pentesting

Otras soluciones de evaluación de la Seguridad

El pentesting es solo una parte de la Seguridad ofensiva y debe formar parte de una sólida cartera de soluciones centradas en la prevención y la mejora continua de la postura de Seguridad de una organización. La herramienta más fundamental de la Seguridad ofensiva son los escaneos de vulnerabilidades, que identifican, evalúan y notifican las vulnerabilidades de Seguridad de la red o las aplicaciones de una infraestructura informática. Al estar automatizados, los escaneos de vulnerabilidades suelen proporcionar la imagen más actualizada de la postura de Seguridad de una organización. Agregar pentesting es la siguiente fase lógica, ya que los datos que proporcionan los escaneos de vulnerabilidades pueden utilizarse para informar el pentesting, proporcionando información sobre qué debilidades deben explorarse más a fondo. El 77 % de los participantes en la encuesta que han utilizado el pentesting también disponen de escáners de vulnerabilidades (Figura 18). Curiosamente, el 85 % de los encuestados que no utilizan el pentesting sí disponen de escáners de vulnerabilidades (Figura 17). Su interés por realizar una encuesta sobre el pentesting indica que están empezando a considerar la ampliación de su cartera de Seguridad ofensiva.

La capacitación para promover el conocimiento en materia de Seguridad (66 %) es otra herramienta de Seguridad ofensiva fundamental. Estas sesiones de capacitación suelen ser obligatorias para todo el personal de una organización, por lo que contribuyen a fomentar una cultura de la Seguridad y garantizan que todo el mundo esté familiarizado con las mejores prácticas de Seguridad. Dado que la capacitación es una de las únicas formas de reducir el riesgo de ataques de ingeniería social, se investiga periódicamente sobre la mejor manera de transmitir estas lecciones críticas de forma eficaz y memorable. La gamificación, el diseño adaptable y la variedad de formatos multimedia son solo algunas de las formas en que la capacitación sigue evolucionando.

SAST (32 %) y DAST (27 %), ambos utilizados para probar aplicaciones, demuestran cómo la Seguridad proactiva puede integrarse en el proceso de desarrollo. La postexplotación (20 %), el red teaming (27 %) y la simulación de adversarios (23 %) solo se utilizan en programas más perfeccionados, por lo que es posible que los participantes aún no se encuentren en esta fase de su viaje por la Seguridad. Incluso aquellos que han alcanzado niveles de madurez avanzados pueden utilizar exclusivamente servicios de *red teaming*.

Para el 75 % de los encuestados, el costo es el criterio más importante a la hora de considerar soluciones proactivas (Figura 19). Aunque el costo es siempre una preocupación primordial, 2023 era especialmente difícil. Como ya se ha señalado, la inflación y otros problemas económicos han afectado a los presupuestos de Ciberseguridad. Es probable que esta tendencia continúe con un recorte previsto del 41 % en el gasto en Ciberseguridad este año. Como resultado, las organizaciones tienen que examinar cuidadosamente cada compra, una tarea difícil cuando ningún aspecto de la Ciberseguridad puede considerarse opcional.

¿Qué tipos de soluciones de gestión de vulnerabilidades o amenazas utiliza su organización?

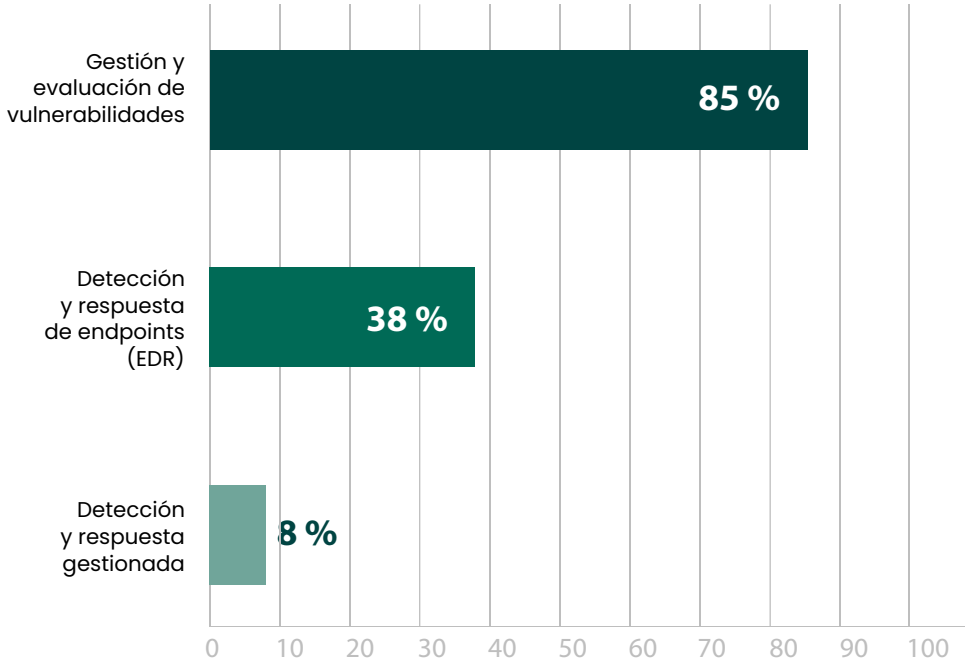


Figura 17: Otras soluciones de evaluación de la Seguridad utilizadas por los encuestados que no realizan pentesting

Otras soluciones de evaluación de la Seguridad

¿Usa alguna de estas otras soluciones tecnológicas de evaluación de la Seguridad?

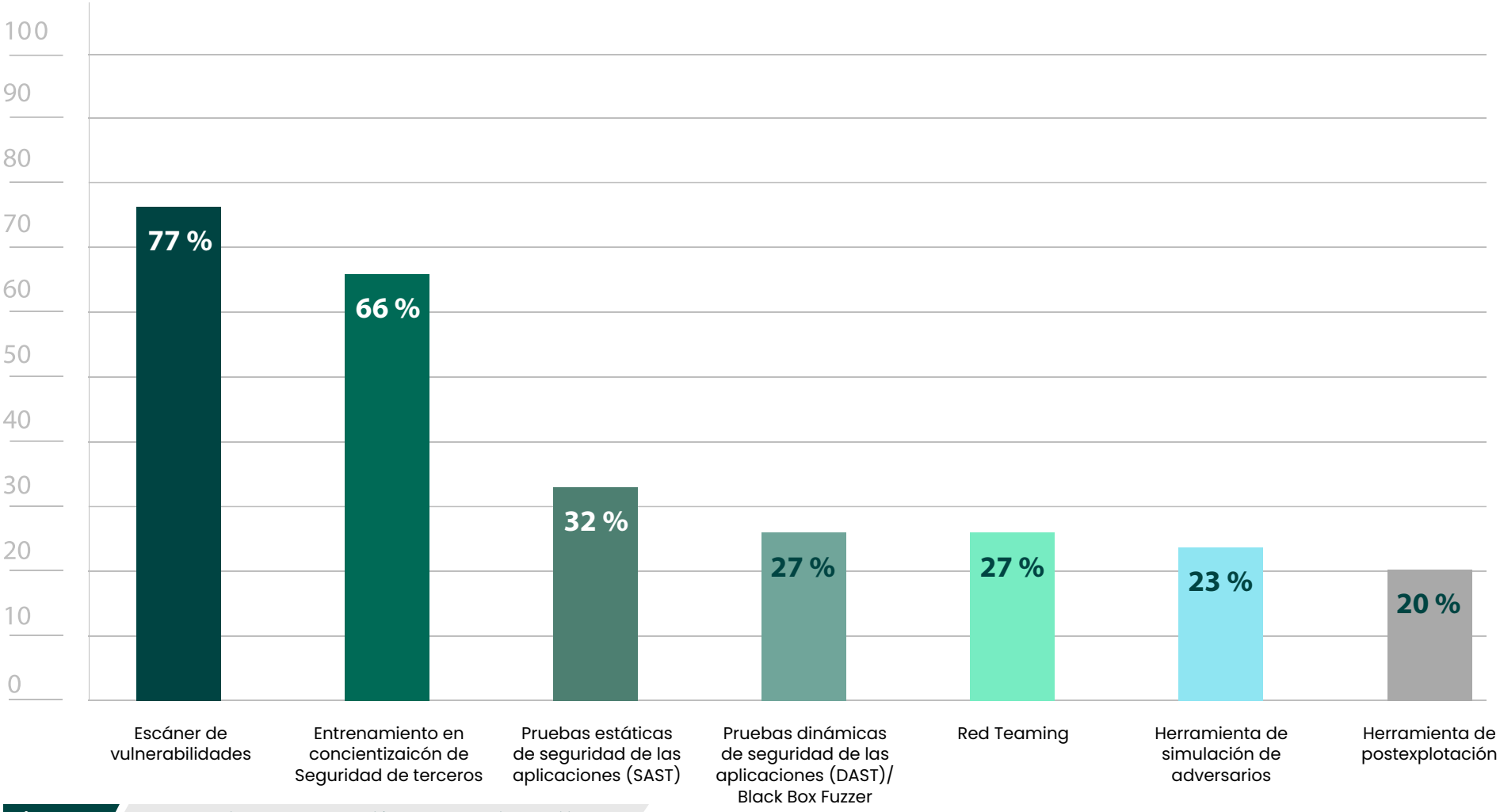


Figura 18: Otras soluciones de evaluación de la Seguridad utilizadas

Otras soluciones de evaluación de la Seguridad

¿Qué criterios considera más importantes a la hora de evaluar estas soluciones de Seguridad proactiva?

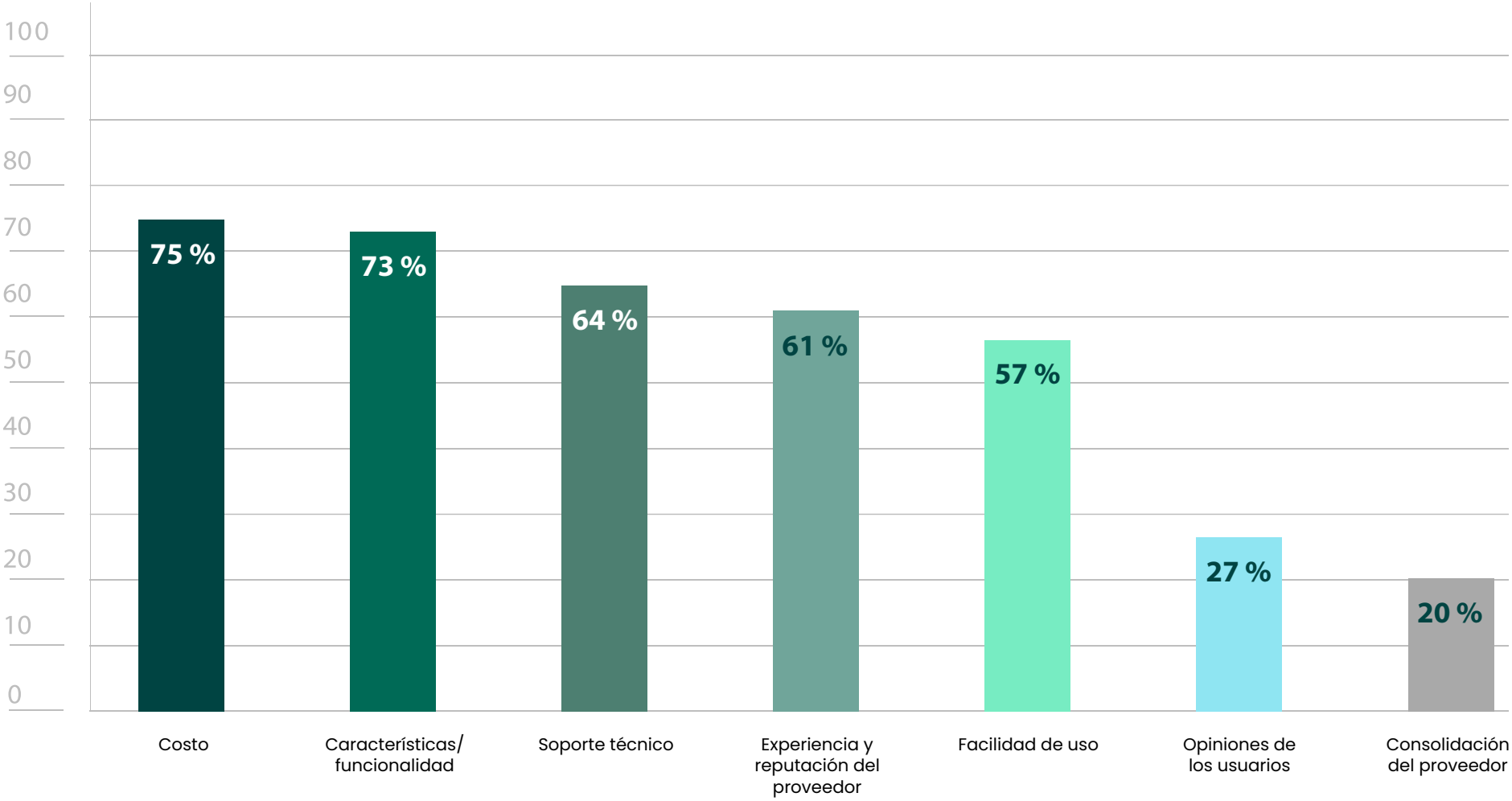


Figura 19: Criterios más importantes para evaluar las soluciones de Seguridad proactiva

Red Teaming

¿Su organización gestiona ejercicios de *red teaming* o usa servicios de *red teaming*?

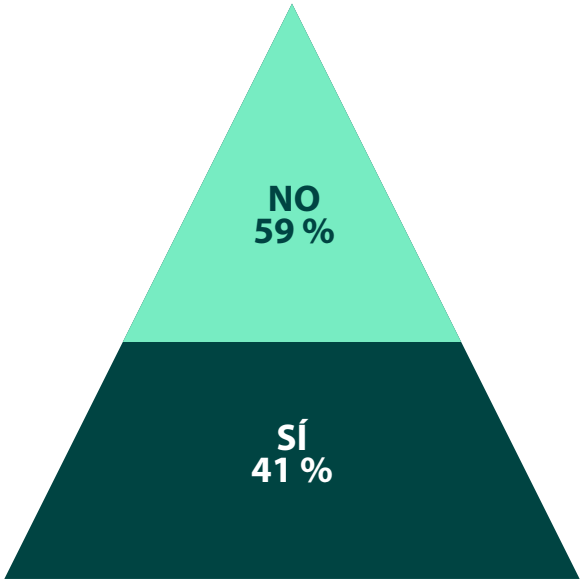


Figura 20: Uso del red teaming

¿Cree que el *red teaming* ha evitado una brecha en su organización?

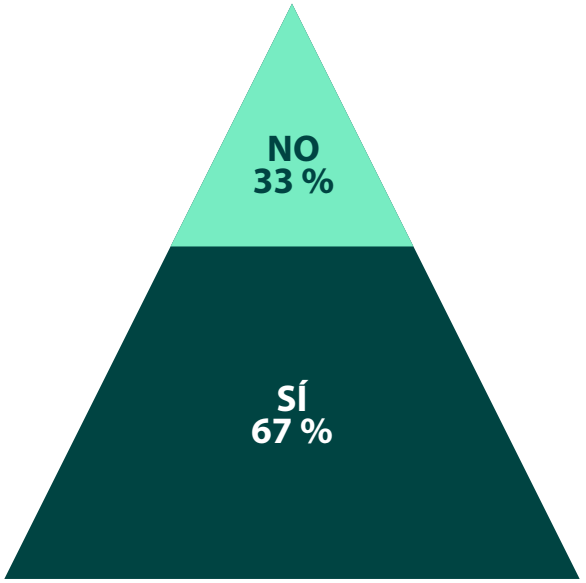


Figura 21: Eficacia del *red teaming* para la prevención de brechas

El pentesting y los ejercicios de *red teaming* a menudo se confunden, y muchos utilizan los términos indistintamente. Sin embargo, existen diferencias significativas entre ambos. El *red teaming* consiste en simulaciones realistas de ciberataques, mientras que el pentesting ofrecen un enfoque más específico, centrado en la explotación de vulnerabilidades en sistemas, redes o aplicaciones concretas. El objetivo del *red teaming* es poner a prueba las defensas de la organización y mejorar las respuestas del blue team, mientras que el objetivo del pentesting es evaluar la eficacia de los controles de Seguridad. Una estrategia de Seguridad ofensiva por capas incluye estas dos evaluaciones de Seguridad complementarias para cerrar las brechas de Seguridad y mejorar sus defensas técnicas.

Es lógico que solo el 41 % de los encuestados gestione o use servicios de *red teaming* (Figura 20), ya que estos deberían reservarse a organizaciones que han alcanzado un nivel de madurez de Seguridad bastante avanzado. Aunque la mayoría de los participantes (67 %) consideraron que las intervenciones de *red teaming* eran eficaces para prevenir las brechas de Seguridad (Figura 21), es posible que aquellos que las consideraron ineficaces no tuvieran la madurez suficiente para beneficiarse plenamente de ellas. Si una organización aún no ha implementado la detección avanzada de amenazas o no dispone de capacidades de respuesta a incidentes, no está preparada para practicar la respuesta a un simulacro de ataque en vivo.

Consolidación del proveedor

¿Cuál es la importancia de consolidar los proveedores para las soluciones de Seguridad?

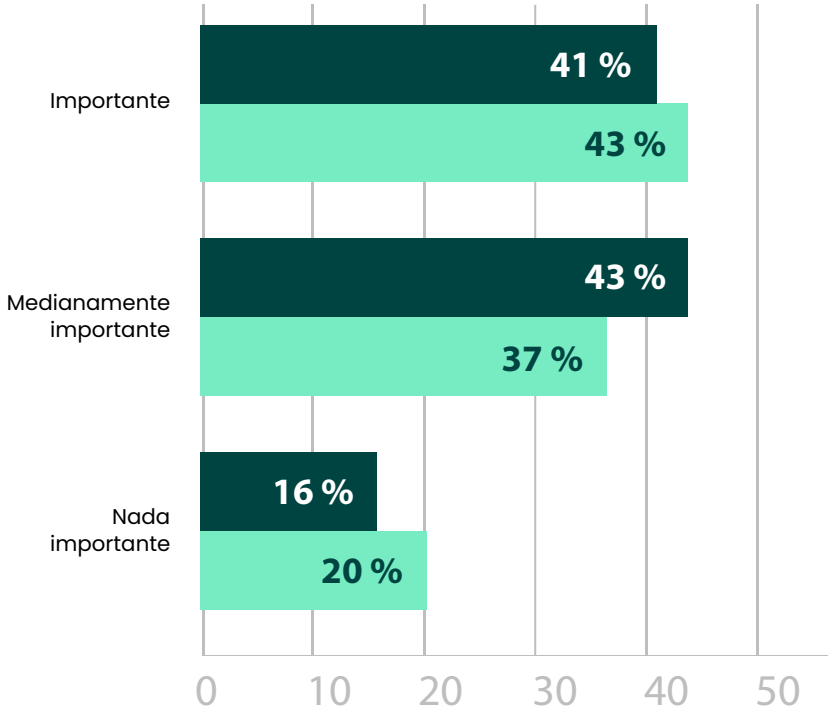


Figura 22: Importancia de la consolidación de proveedores

¿Consideraría agregar el pentesting u otras soluciones proactivas a su cartera si uno de sus proveedores actuales las ofreciera?

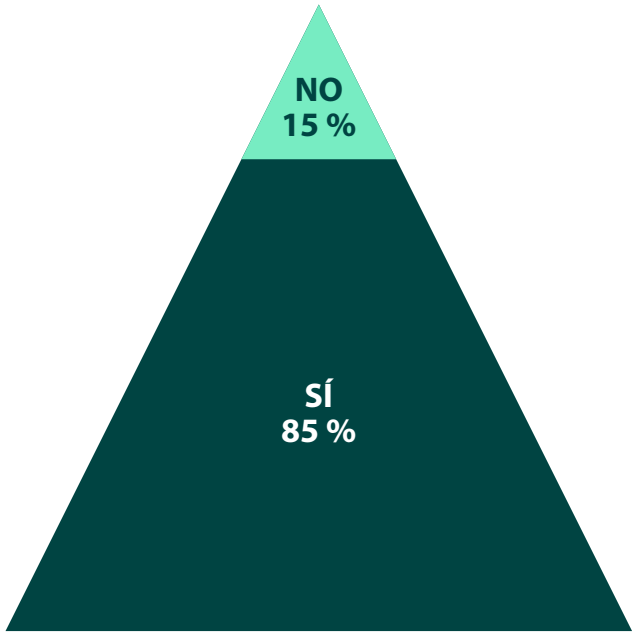


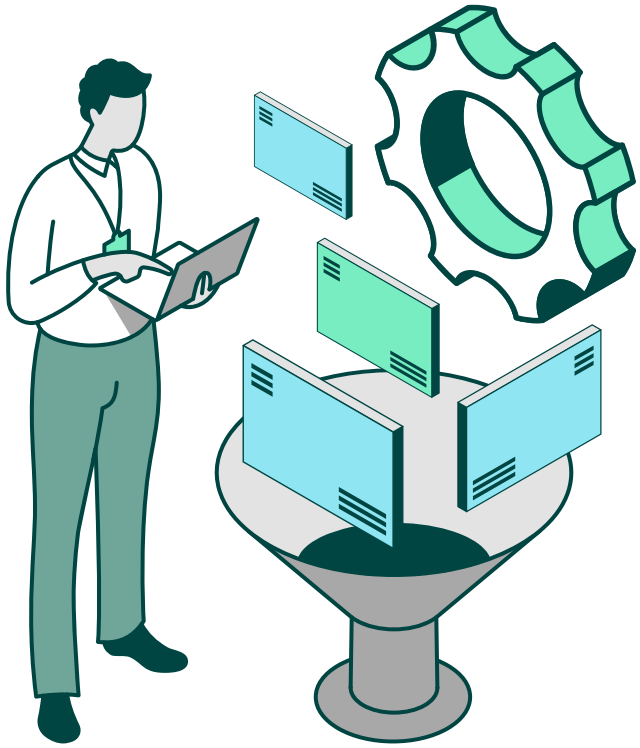
Figura 23: Probabilidad de consolidación de proveedores para quienes no realizan pentesting

Consolidación del proveedor

La consolidación de proveedores sigue interesando a los encuestados, y el 84 % afirma que es al menos algo importante para su organización (Figura 22). La consolidación de proveedores ofrece varias ventajas. A medida que las infraestructuras informáticas se hacen más complejas, las organizaciones se encuentran con que cada vez dedican más tiempo a la inesperada tarea de gestionar numerosos proveedores. Tratar con menos proveedores simplifica la gestión y reduce el tiempo dedicado a tareas administrativas relacionadas. Establecer relaciones con un número selecto de proveedores también puede facilitar la comunicación y las negociaciones contractuales.

Tener varios proveedores también agrega involuntariamente más riesgo, especialmente con el espectacular aumento de los ataques a la cadena de suministro el año pasado. De hecho, según Gartner, el 60 % de las organizaciones de la cadena de suministro utilizarán el riesgo de Ciberseguridad como factor para determinar con qué terceros trabajan. Con una mayor necesidad de diligencia debida y evaluación de riesgos antes de firmar un contrato, contar con un conjunto más reducido de proveedores de confianza puede aumentar significativamente la eficiencia.

La consolidación de proveedores también puede incentivar a las organizaciones a mejorar sus estrategias de Seguridad. El 85 % de los participantes que no utilizan actualmente pentesting afirmaron que considerarían la posibilidad de agregar soluciones proactivas si un proveedor actual las ofreciera (Figura 23). Las soluciones ofrecidas por un proveedor existente son especialmente ventajosas cuando ofrecen interoperabilidad e integración entre productos, lo que puede simplificar la implementación inicial, agilizar las operaciones y reducir la complejidad. Cuando las organizaciones empiezan a buscar proveedores que ofrezcan la solución que buscan actualmente, puede ser prudente encontrar aquellos que también proporcionen opciones adicionales para futuras inversiones.



Pentesting en distintos entornos

¿Qué entornos o Sistemas Operativos le preocupan más a la hora de ejecutar el pentesting?

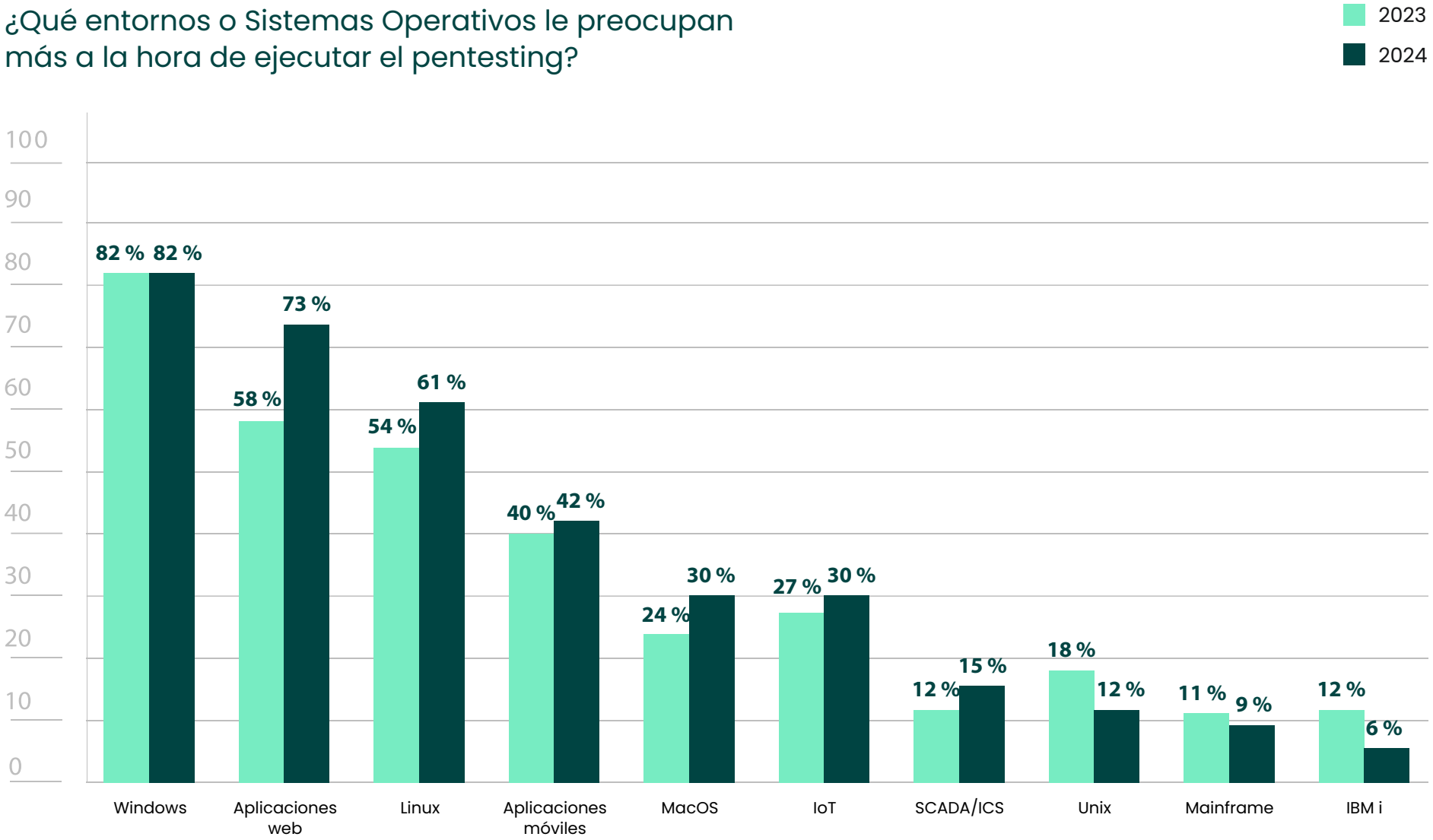


Figura 24: Entornos que necesitan pentesting

Pentesting en distintos entornos

Windows (82 %), presente en diversos activos de la organización, como estaciones de trabajo, servidores y otros puntos finales, vuelve a destacarse como el Sistema Operativo que más preocupa (Figura 24). Windows Active Directory es un objetivo de alto valor para los atacantes, ya que sirve como repositorio centralizado para la autenticación, autorización e información de configuración. Si Active Directory se ve comprometido, los actores de amenazas pueden tener el control total de toda la red, por lo que asegurar los entornos Windows y salvaguardar Active Directory contra la explotación es crucial para minimizar los riesgos de Ciberseguridad y proteger los activos de la organización.

Las aplicaciones web siguen siendo entornos habituales para el pentesting, pero es oportuno destacar el aumento del 15 % con respecto al año pasado (Figura 24). Es posible que refleje el aumento de participantes del sector financiero, cuyas aplicaciones web se convirtieron en un objetivo aún más popular el año pasado (Figura 29). De hecho, los ataques a aplicaciones web fueron responsables del 77 % de todas las brechas en el sector de las finanzas y los seguros, según el Informe de Verizon sobre investigaciones de filtraciones de datos (DBIR). Además, el DBIR descubrió que el 95 % de los ataques tenían motivaciones económicas, por lo que las aplicaciones financieras resultan especialmente tentadoras, ya que pueden almacenar números de cuentas bancarias, datos de tarjetas de crédito, números de la Seguridad Social e historial de transacciones.

El aumento del 20 % en el pentesting para infraestructuras en la nube (Figura 25) fue un cambio prometedor, especialmente a medida que se depende cada vez más en los entornos en la nube. Por ejemplo, la computación nativa en la nube creció un 175 % de 2022 a 2023. Por desgracia, una tendencia al alza en el uso suele significar una tendencia al alza en los ataques. Efectivamente, más del 80 % de las brechas de datos del año pasado estuvieron relacionadas con el almacenamiento de datos en la nube. Las organizaciones harían bien en seguir incluyendo los entornos en la nube en sus estrategias de pentesting.

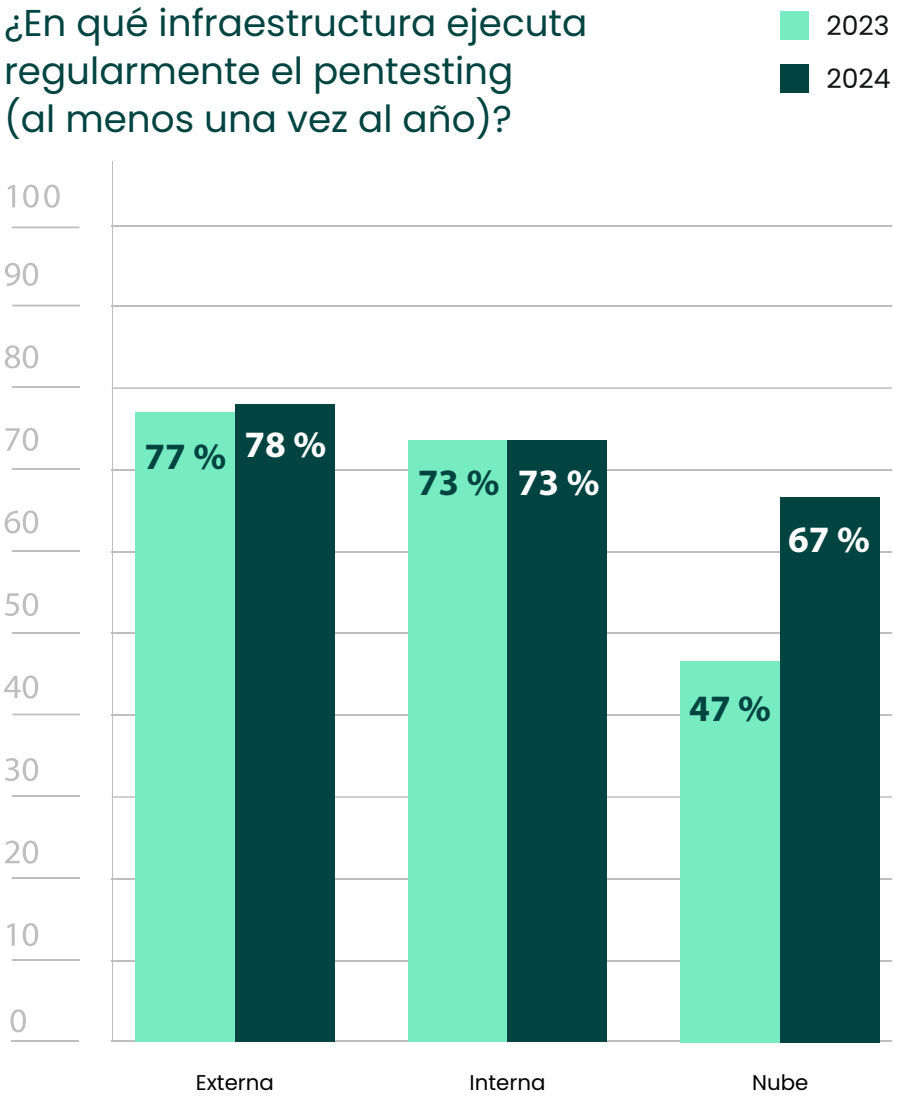


Figura 25: Infraestructuras con pentesting regular

Datos demográficos

Este informe se basa en los resultados de una encuesta enfocada en presentar una imagen precisa de las cuestiones de Ciberseguridad que aborda el pentesting, cómo los implementan las diferentes organizaciones y los desafíos en la creación y administración de un programa de pentesting. Han participado del informe profesionales de la Ciberseguridad de todo el mundo, con encuestados que representaban una muestra representativa diversa de sectores, tamaños de empresa, niveles de trabajo y región.

¿En qué región tiene la sede su organización?

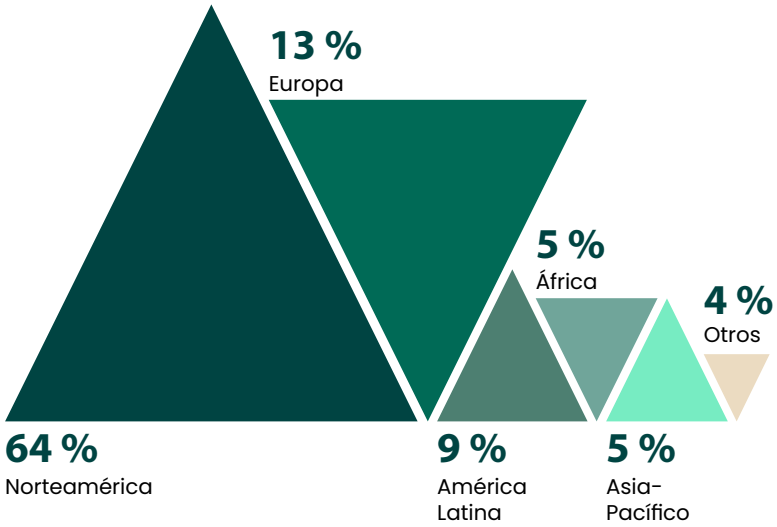


Figura 26: Regiones encuestadas

¿Cuál es su sector principal?

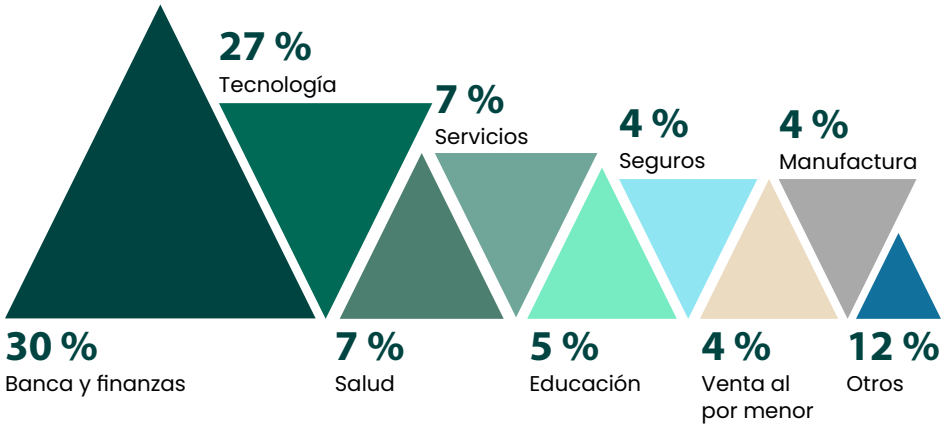


Figura 27: Sectores encuestados

Datos demográficos

¿Cuál es su cargo en la empresa?

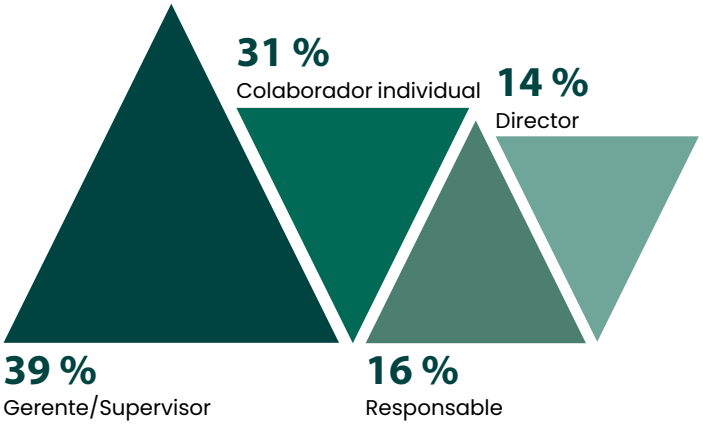


Figura 28: Nivel laboral de los encuestados

¿Cuántos empleados tiene su organización?

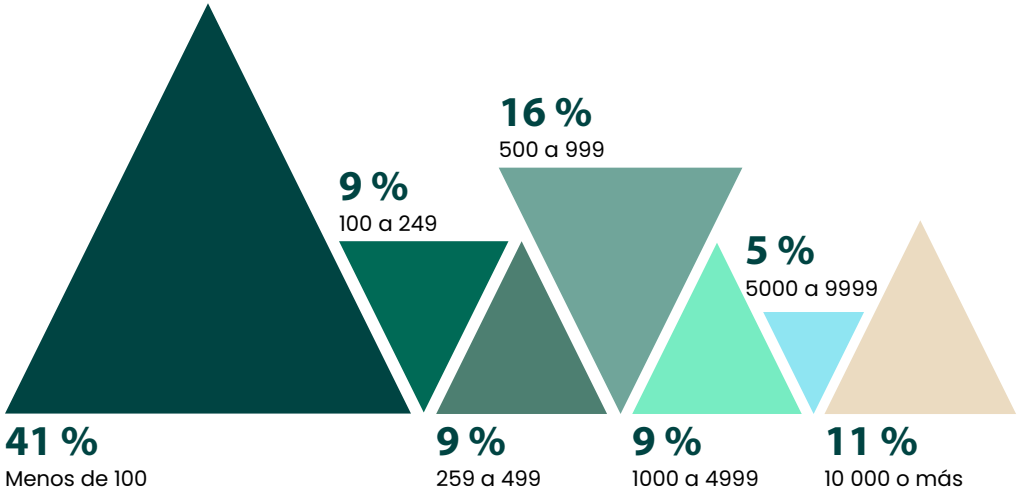


Figura 29: Tamaño de las organizaciones encuestadas

Conclusión

Los resultados de esta encuesta destacan la importancia del pentesting como componente estratégico de la cartera de Ciberseguridad proactiva de una organización. De la misma manera que el pentesting evalúa la Seguridad de la infraestructura, las organizaciones también deben evaluar periódicamente su enfoque de pentesting, y considerar cuidadosamente las herramientas y la metodología disponibles para asegurarse de que están abordando eficazmente sus necesidades y requisitos de Seguridad únicos.

Los programas de pentesting no están exentos de obstáculos. La omnipresencia de los recursos limitados se puso de manifiesto en todo el análisis de la encuesta, con menos equipos internos de pentesting, más organizaciones que prescinden de herramientas comerciales de pentesting y el costo convertido en el principal criterio tanto para las soluciones de pentesting como para otras herramientas de Seguridad proactiva. Aunque las organizaciones puedan reducir costos mediante la consolidación de proveedores, los continuos desafíos financieros pueden requerir decisiones difíciles sobre cuántas pruebas deben realizarse, cuál debe ser su alcance y quién debe realizarlas.

Pero la importancia del pentesting va más allá del alcance inmediato de las propias pruebas. La incorporación del pentesting en cualquiera de sus formas abre la puerta a la adopción de una mentalidad de Seguridad proactiva.

FORTRA™

Sobre Fortra

Fortra es una compañía de Ciberseguridad como ninguna otra. Creamos un futuro más simple y sólido para nuestros clientes. Nuestro equipo de expertos junto con el mejor portfolio de soluciones integradas y escalables aportan equilibrio y control a organizaciones en todo el mundo. Somos impulsores del cambio positivo y su aliado de confianza para darle tranquilidad en cada paso de su camino de Ciberseguridad. Conozca más en fortra.com/es.

fta-cs-gd-0424-db