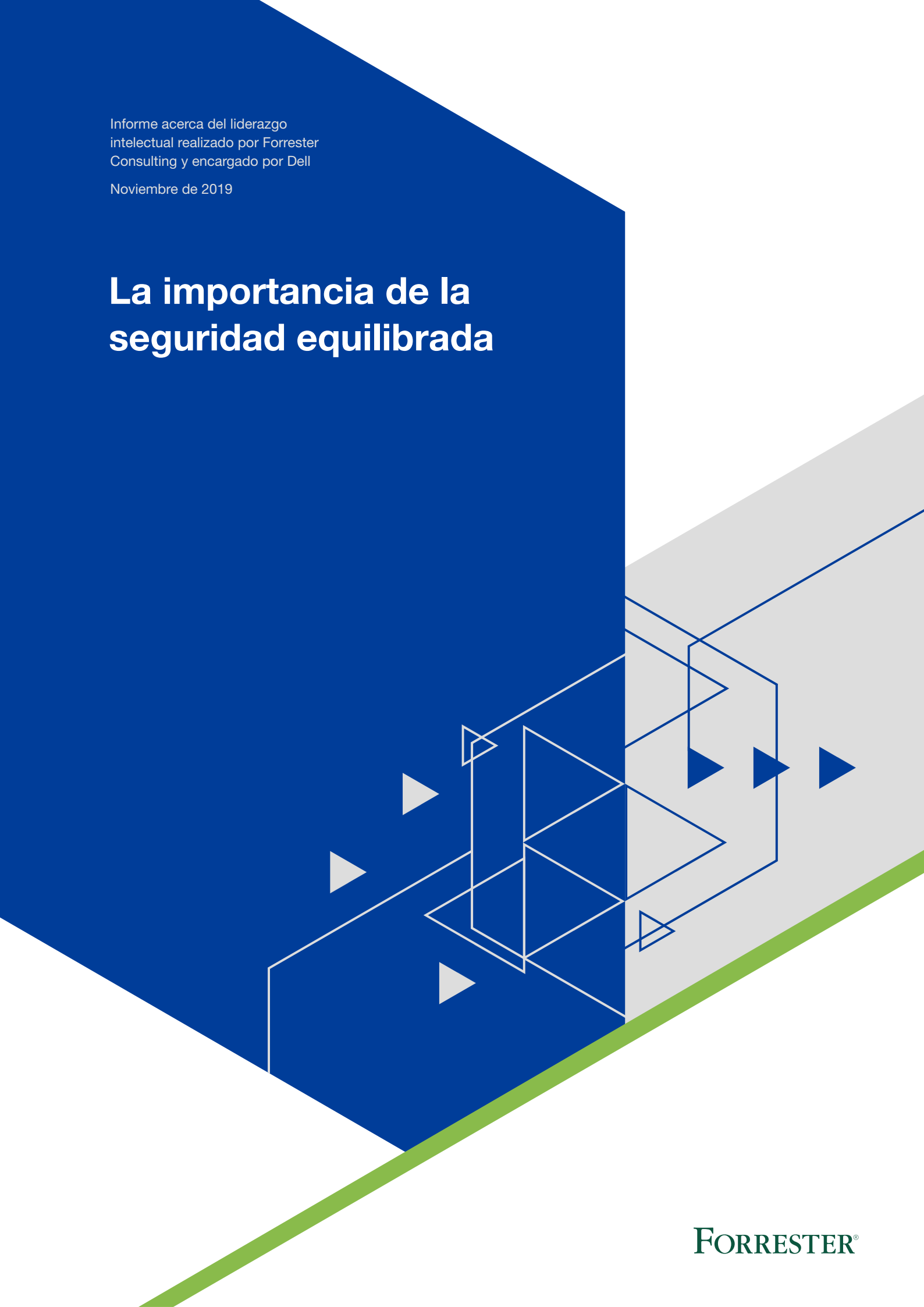
Informe acerca del liderazgo intelectual realizado por Forrester Consulting y encargado por Dell

Noviembre de 2019

La importancia de la seguridad equilibrada



FORRESTER®

Tabla de contenido

1 Resumen ejecutivo

2 Las organizaciones requieren una seguridad equilibrada para impulsar la experiencia de los empleados y la eficiencia operacional

3 La evolución de las amenazas y la complejidad de la TI

6 Su infraestructura de seguridad debe evolucionar junto con los tiempos

9 La seguridad equilibrada beneficia a los empleados y a la empresa

11 Recomendaciones clave

12 Apéndice

Director de proyecto:
Tarun Avasthy,
Consultor de impacto en el mercado

Investigación colaboradora:
Grupo de investigación de infraestructura y operaciones de Forrester

ACERCA DE FORRESTER CONSULTING

Forrester Consulting ofrece consultoría independiente y objetiva basada en investigaciones que ayuda a los líderes a alcanzar el éxito en sus organizaciones. Con un alcance que varía de una breve sesión de estrategia hasta proyectos personalizados, los servicios de consultoría de Forrester establecen conexiones directas entre usted y los analistas de investigación, que aplican perspectivas expertas a los retos específicos para el negocio. Para obtener más información, visite forrester.com/consulting.

FORRESTER®

Resumen ejecutivo

La seguridad equilibrada requiere que las empresas pasen de tratar la privacidad y la seguridad de los datos como requisitos de cumplimiento de normas a defender la privacidad y utilizar su pericia en tecnología para diferenciar la marca. Cualquier traspié relacionado con la TI o un cambio que se realice en su infraestructura puede agravar la complejidad y lo hará, por lo cual la creación de una estrategia de seguridad equilibrada es muy importante. Una estrategia de seguridad equilibrada no da lugar a la complejidad, ya que se mantiene al día tanto con el ritmo de los cambios tecnológicos como con las revoluciones del sector y el cumplimiento de normas en constante cambio.

En marzo de 2019, Dell encargó a Forrester Consulting que evaluara las cambiantes tendencias de seguridad y la tecnología necesarias para proteger y habilitar a los empleados. En nuestro estudio, se descubrió que empoderar a los empleados y cumplir los protocolos de seguridad permite mejorar la productividad. Forrester realizó una encuesta en línea de 887 tomadores de decisiones de empresas de alto nivel y de TI para explorar este tema.

RESULTADOS PRINCIPALES

- **Las amenazas en constante cambio obligan a las empresas del mercado del segmento intermedio a ser más proactivas que reactivas.** Ya que existen muchas violaciones de seguridad de alto perfil o ataques cibernéticos que se informan regularmente en las noticias, las empresas del mercado del segmento intermedio deben ser más previsoras en su enfoque de seguridad.
- **Gastar solo en seguridad no es la panacea.** Las empresas del mercado del segmento intermedio deben establecer una cultura de habilitación, el desarrollo continuo de las habilidades de los empleados y, tal vez lo más importante, una infraestructura de seguridad confiable y sólida.
- **Las políticas de TI restrictivas conducirán a los empleados a evadir las mejores prácticas de seguridad de TI por el mero hecho de realizar el trabajo.** Flexibilizar las reglas en el lugar de trabajo no es infrecuente, pero evitar las políticas de TI para poder trabajar resulta riesgoso.

FORRESTER®

Las organizaciones requieren una seguridad equilibrada para impulsar la experiencia de los empleados y la eficiencia operacional

Un entorno de tecnología diverso y los cambios de estilo de trabajo de los empleados han abierto la puerta a una gran cantidad de riesgos que amenazan la situación de seguridad general de una organización y su reputación. Una infraestructura de seguridad sólida y equilibrada garantiza que se maximice y proteja el rendimiento de la empresa. Mientras tanto, como iniciativa empresarial, la experiencia de los empleados (EX) está creciendo en importancia, ya que más empresas están interesadas en desarrollar una estrategia de experiencia del personal que reduzca la fricción y les permita a los empleados completar sus tareas más importantes en una manera eficaz.

Gastar solo en tecnología no ayudará a mejorar la experiencia de los empleados. Las organizaciones, específicamente las empresas del mercado del segmento intermedio, también deben invertir en la creación de una cultura de habilitación de los empleados, el desarrollo continuo de habilidades y una seguridad sólida con el fin de administrar el riesgo y, al mismo tiempo, respaldar el rendimiento de la empresa. Para ofrecer una gran EX, las empresas necesitan un enfoque equilibrado para la seguridad en tres áreas clave (consulte la Figura 1):

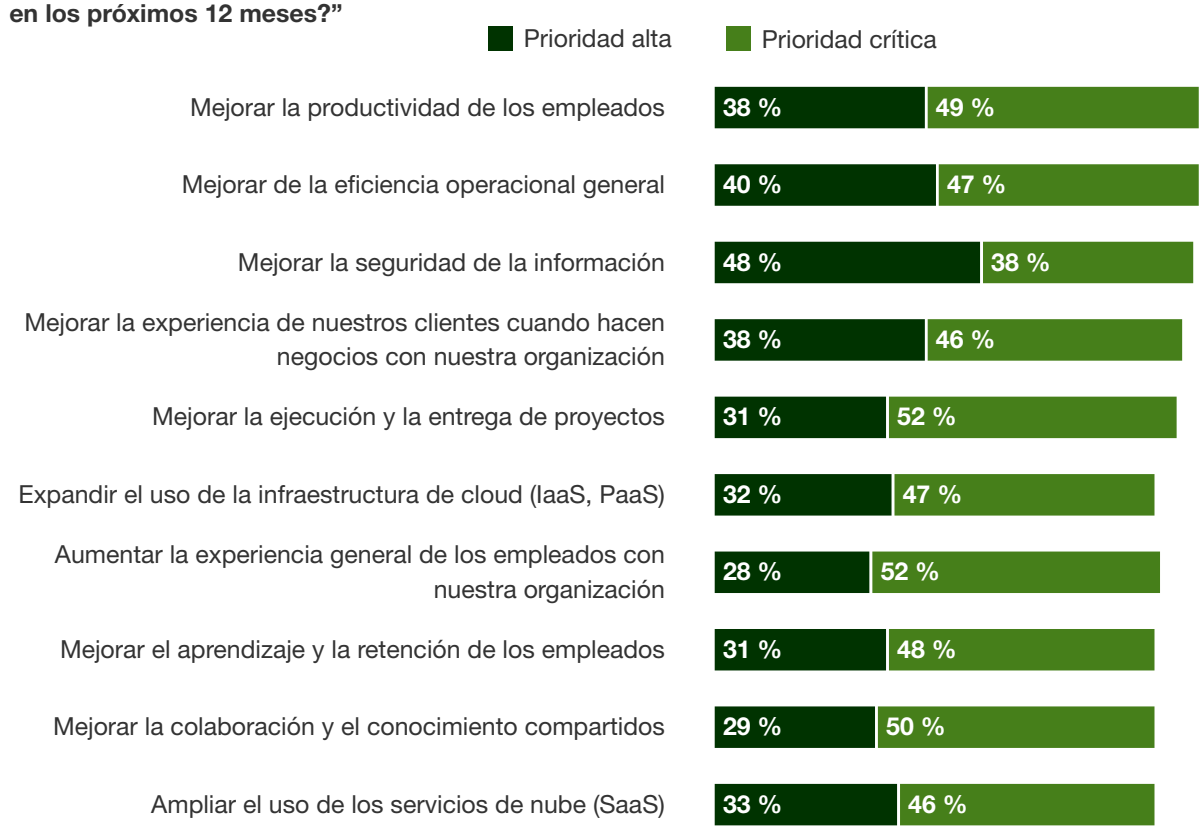
- **Aumento de la productividad del empleado.** Un lugar de trabajo colmado, como el que se observa actualmente, crea exigencias cognitivas intensas para los empleados, por lo cual brindarles ayuda para lograr dominar su trabajo es una dimensión inherente de la buena EX. Sin embargo, muchas medidas de seguridad hacen lo contrario e interrumpen sus niveles de productividad. Teniendo esto en cuenta, las empresas del mercado del segmento intermedio buscan mejorar la productividad de los empleados en los próximos 12 meses (88 %). Como la tecnología continúa evolucionando, los encuestados también informaron que mejorarán la retención y la capacitación de los empleados (79 %), lo que garantiza que las brechas de talento permanezcan lo más cercanas posible.
- **Aumentar la seguridad de la información.** Para que los empleados tengan éxito, también necesitan tener acceso ilimitado a la información requerida para hacer su trabajo, independientemente de la ubicación en la que trabajan y de los dispositivos que utilizan para hacer su trabajo. Sin embargo, las empresas enfrentan aluvión de diferentes tipos de ataques cibernéticos y de eventos que pueden interrumpir las operaciones de la empresa y comprometer la información confidencial, ya sea la información personal de los clientes/empleados o la información corporativa confidencial. Además, las preocupaciones como el riesgo de terceros y la seguridad de la cadena de suministro significan que las organizaciones deben ampliar su visión de los riesgos para la empresa más allá de su propio entorno. No es ninguna sorpresa que el 86 % de las empresas dijera que dará prioridad a la seguridad de la información.
- **Mejorar la eficiencia operacional.** Los equipos de seguridad que respaldan las operaciones de la empresa deben establecer un proceso mucho más coherente en la manera en que operan y se esfuerzan por ser proactivos, en lugar de ser reactivos en su enfoque hacia la seguridad. Las empresas del mercado del segmento intermedio deben ir más allá de un enfoque de casilla de verificación estándar, basando los esfuerzos de seguridad principalmente en los requisitos de cumplimiento de normas, y así llegar a un enfoque más estratégico y basado en el riesgo para la seguridad. Esto requiere procesos que admitan la inteligencia vinculada a los riesgos, la identificación de amenazas y la respuesta a ellas, la evaluación de riesgos y la resiliencia de la empresa a fin de cumplir con la promesa de la ejecución y la entrega del proyecto (83 %).

Las empresas del mercado del segmento intermedio deben invertir en la creación de una cultura de habilitación de empleados y de desarrollo continuo de habilidades, y deben esforzarse por lograr una infraestructura de seguridad sólida.

FORRESTER®

Figura 1

"¿Cuál de las siguientes iniciativas relacionadas con la tecnología priorizará su departamento o división en los próximos 12 meses?"



Base: 887 tomadores de decisiones empresariales y de TI que participan en la toma de decisiones para laptops, computadoras y otros dispositivos
Fuente: un estudio realizado por Forrester Consulting en nombre de Dell, septiembre de 2019

La evolución de las amenazas y la complejidad de la TI

Frente a las prioridades en conflicto, las tecnologías emergentes y los nuevos requisitos normativos, los gerentes de seguridad se encargan de la defensa continua y se aseguran de que los atacantes no logren su objetivo. Sin embargo, cuando le preguntamos a los encuestados cuáles son los principales desafíos de seguridad, encontramos lo siguiente (consulte la Figura 2):

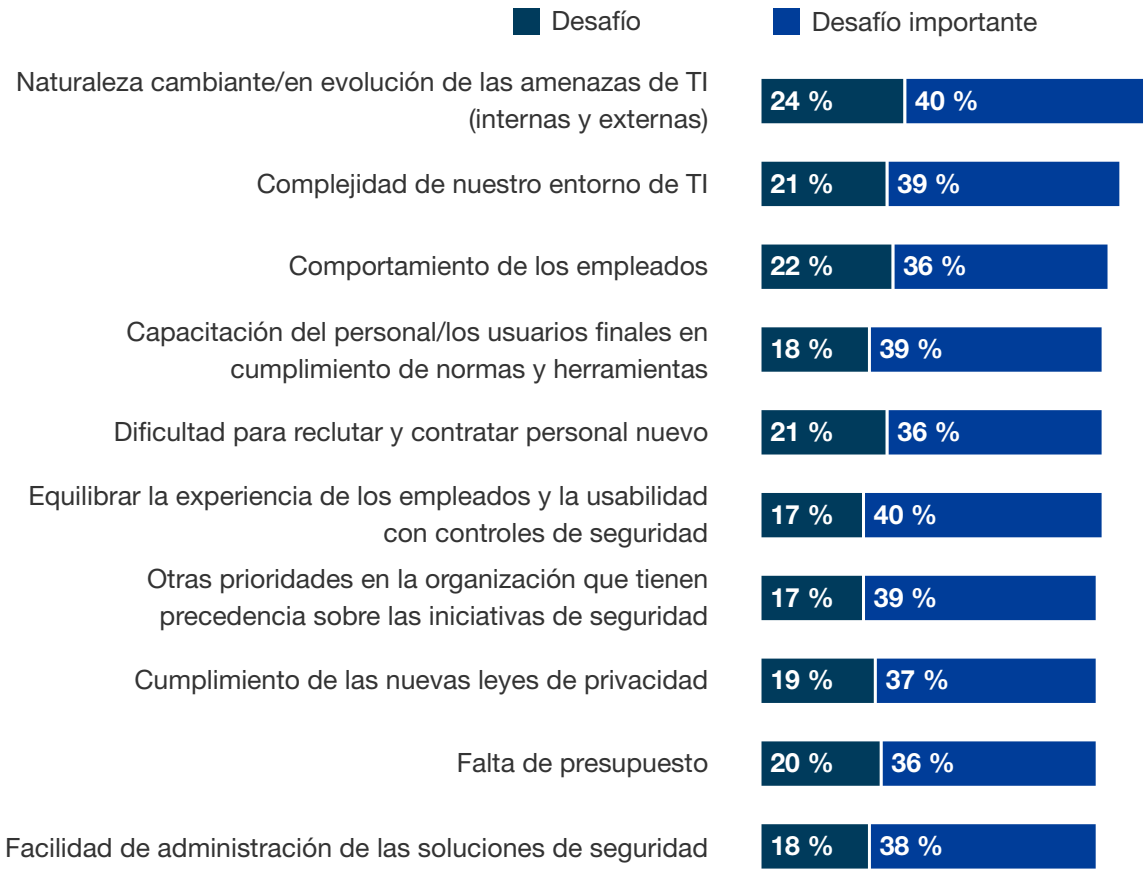
› **La naturaleza cambiante de las amenazas mantiene alerta a las empresas del mercado del segmento intermedio y en constante intento de ponerse al día.** La TI debe contar con una estrategia sólida y adaptable con el fin de generar fricción para los atacantes. En la actualidad, el 65 % de las organizaciones se enfrentan a problemas por la naturaleza cambiante de los ataques de seguridad. A medida que los líderes de la organización ven las últimas menciones de ataques cibernéticos y de eventos en las noticias, y luego se preguntan si eso le podría suceder a su organización, resulta útil evaluar y comunicar el por qué y el cómo ocurren (o el por qué no, según su entorno y los controles). Sin embargo, no permita que este enfoque reactivo lidere su estrategia general de seguridad.

FORRESTER®

› **La complejidad de la TI se traduce en un mayor riesgo y en desafíos de administración de TI.** Cualquier traspié relacionado con la TI o un cambio que se realice en su infraestructura puede agravar la complejidad y lo hará, por lo cual la creación de una estrategia de seguridad sólida es muy importante. Una estrategia de seguridad que pueda seguir el ritmo del cambio de la tecnología, las revoluciones del sector y la evolución de las regulaciones y la evolución y el cumplimiento de las normas servirá como catalizador para el cambio positivo. Es preferible tener una estrategia que le permita construir la seguridad desde el principio que construirla después del hecho, y lo mismo sucede con una estrategia que analice más de cerca la consolidación de la cantidad de productos de seguridad en su entorno para brindar una administración de TI más sencilla. En la actualidad, el 60% de los encuestados consideran que la complejidad de su entorno de TI es una amenaza para la organización.

Figura 2

"¿Cuáles de los siguientes son desafíos de seguridad de TI para su organización?"



Base: 887 tomadores de decisiones empresariales y de TI que participan en la toma de decisiones para laptops, computadoras y otros dispositivos
Fuente: un estudio realizado por Forrester Consulting en nombre de Dell, septiembre de 2019

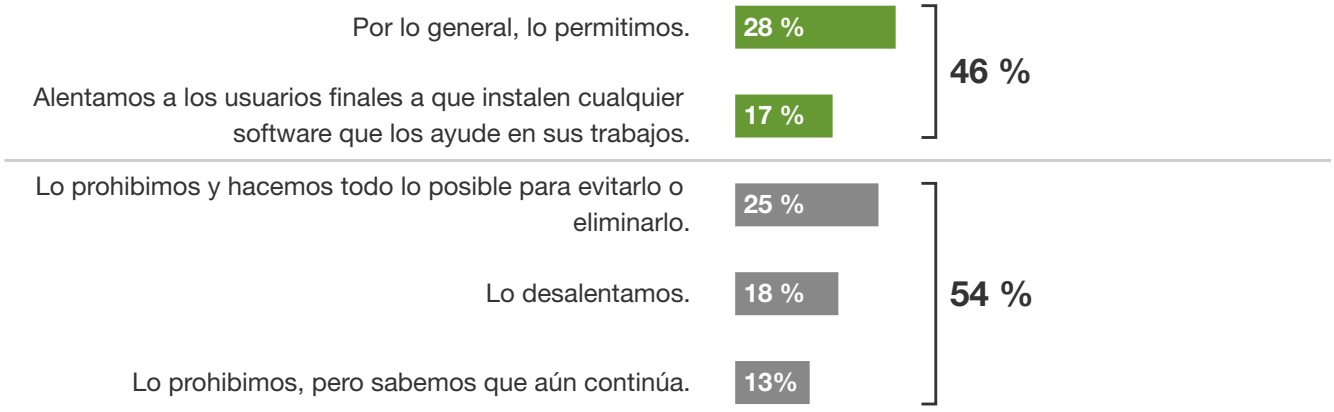
LOS EMPLEADOS DEBEN SENTIRSE EMPODERADOS O ELUDIRÁN LAS POLÍTICAS DE TI

Los empleados elegirán el camino que brinde menor resistencia para hacer su trabajo. El 54 % de los encuestados de las empresas del mercado del segmento intermedio informó que, cuando los empleados desean instalar sus propios softwares/aplicaciones para hacer el trabajo de esta manera, estos sistemas los desalientan o les impiden o prohíben hacerlo; sin embargo, saben que aun así continúan. Los empleados necesitan sentirse respaldados por la empresa (consulte la Figura 3).

Los empleados deben hacer su trabajo de una manera que no afecte su productividad y el personal de seguridad debe asegurarse de que la empresa esté protegida. El 58 % de los encuestados informa que, en ocasiones, los empleados eluden las políticas de TI para llevar a cabo las tareas, poniendo en riesgo la empresa. Es por esto que es importante equilibrar la EX y la usabilidad con los controles de seguridad, pero el 57 % afirmó que esto sigue siendo un desafío. Además, si las organizaciones no pueden medir la eficacia de su programa de seguridad (52 %) correrán una carrera interminable, con la línea de meta (nuestro arco de oro de estrategia de seguridad equilibrada) siempre cerca, es decir siempre en el próximo paso.

Figura 3

"Para su empleado de TI típico, ¿cuál es la política de TI de la organización para el uso o la instalación de su propio software?"



Base: 887 tomadores de decisiones empresariales y de TI que participan en la toma de decisiones para laptops, computadoras y otros dispositivos
Fuente: un estudio realizado por Forrester Consulting en nombre de Dell, septiembre de 2019

Su infraestructura de seguridad debe evolucionar junto con los tiempos

La idea de un perímetro corporativo resulta pintoresca y anticuada hoy en día. Los empleados trabajan desde varias ubicaciones y necesitan acceso a la información desde cualquier lugar. El mercado del consumidor está influyendo en la forma en que los empleados trabajan en un entorno corporativo y con qué dispositivos lo hacen. Una empresa digital no tiene perímetro. Hoy en día, la organización puede pasar a la cloud, brindar soporte al personal móvil, digitalizar los entornos físicos con conectividad a través de sensores y otros dispositivos conectados a Internet. Hay una permutación cada vez mayor de las maneras en que tanto los empleados pueden exponer la información confidencial como los atacantes pueden comprometer su entorno y sus datos. En el entorno de trabajo y las amenazas de hoy en día, la estrategia y la arquitectura de seguridad deben evolucionar para centrarse en los datos y estar arraigados en un enfoque de seguridad de confianza cero.

La confianza cero es un modelo conceptual y arquitectónico para la manera en que los equipos de seguridad deben rediseñar las redes en microperímetros seguros, usar la ofuscación para fortalecer la seguridad de los datos, limitar los riesgos asociados con los privilegios excesivos de los usuarios y usar la automatización y los análisis para mejorar radicalmente la seguridad de detección y la respuesta. Este enfoque ayuda a mejorar radicalmente la seguridad de los datos. Hoy en día, muchas organizaciones adoptan un enfoque de confianza cero. Los encuestados identificaron las siguientes prioridades de infraestructura que indican una preparación para el enfoque de confianza cero (consulte la Figura 4):

- **Capacitar a los usuarios finales para mejorar las prácticas seguras de manejo de datos.** A fin de obtener acceso a la propiedad intelectual, los atacantes se dirigirán a los empleados y contratistas. En el trabajo, los empleados están utilizando dispositivos conectados que interactúan con los servicios de nube en redes o sistemas de propiedad corporativa, pero mientras se encuentran en otro lugar, ya sea en movimiento, en el hogar o en espacios públicos, como aeropuertos y cafeterías, los empleados aún tendrán que acceder a información y datos confidenciales desde dispositivos personales que no estén tan bien protegidos como las redes o los sistemas de propiedad corporativa. La necesidad de que los empleados manejen de forma responsable los datos con prácticas seguras, etc., no es una información necesariamente comprendida y eficaz.
- **Capacitar al personal de TI para mitigar el riesgo.** El desarrollo continuo de las habilidades del personal de TI es importante para garantizar que las personas que son responsables de las infraestructuras de tecnología y seguridad estén actualizadas sobre las prácticas recomendadas actuales. Comprender las opciones de tecnología cambiantes y el panorama de riesgos y amenazas en evolución es necesario para posicionar al equipo de TI para lograr el éxito. Por lo tanto, el 79 % de los encuestados afirmó que mejorarán la capacitación del personal de TI. Esta es una buena noticia en dos frentes: 1) asegura que el personal de TI esté actualizado en relación con sus habilidades y enfoques y 2) ayuda a respaldar los esfuerzos de retención en un momento en que la demanda de talentos es alta.

› **Volver a revisar la estrategia de seguridad.** Las organizaciones se están volviendo cada vez más conscientes de que cumplir con los requisitos de cumplimiento de normas no equivale a construir una seguridad sólida. Los business partners externos exigirán pruebas de una práctica de administración de riesgos y seguridad fuerte como condición para trabajar en conjunto. Una estrategia con visión prospectiva respalda los esfuerzos de una organización para desarrollar un programa de seguridad sólido y para prever las áreas en las que necesitan mejorar o incorporar nuevas habilidades para abordar las preocupaciones, según las prioridades de la empresa. El 80 % de los encuestados indicó que estaba priorizando la necesidad de desarrollar y ejecutar una estrategia de seguridad para TI, dispositivos y datos.

Figura 4

"¿Cuáles de las siguientes iniciativas probablemente sean las principales prioridades de infraestructura de TI de su empresa en los próximos 12 meses?"

Base: 887 tomadores de decisiones empresariales y de TI que participan en la toma de decisiones para laptops, computadoras y otros dispositivos
Fuente: un estudio realizado por Forrester Consulting en nombre de Dell, septiembre de 2019

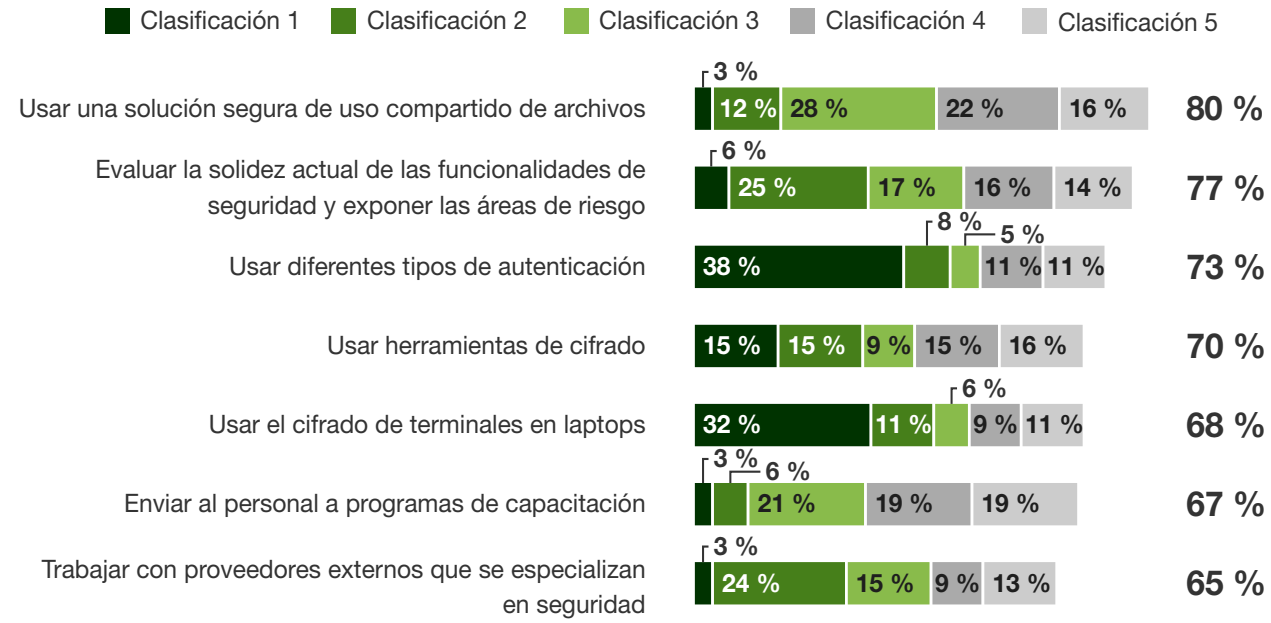
TÁCTICAS PARA MEJORAR LA SEGURIDAD

En la era digital, las amenazas cibernéticas están en todas partes, y las vulneraciones llegan a los titulares casi a diario, lo cual les cuesta la reputación, el capital, el crecimiento y la expansión futuros a las empresas. En otras palabras, la seguridad final de una organización depende de las tecnologías que aseguran los datos, es decir, la pieza fundamental de las empresas digitales. Las vulneraciones de datos son un hecho desafortunado de la vida. El 50 % de los tomadores de decisiones de seguridad de redes globales dijo que, en su conocimiento, la organización sufrió al menos una vulneración en el último año, y esto aumenta al 55 % en el caso los encuestados de las empresas. Teniendo esto en cuenta, las organizaciones revelaron cuáles son los aspectos de seguridad que les gustaría mejorar y mencionaron lo siguiente (consulte la Figura 5):

- **Uso compartido de archivos seguro para respaldar la colaboración de los empleados.** Tanto la tecnología como los empleados juegan un papel crucial en permitir que las organizaciones colaboren y, por lo tanto, crean un valor económico duradero. El 80 % de los encuestados afirmó que usarán una solución segura para compartir archivos con el fin de ayudar a mejorar sus funcionalidades de seguridad. Sin embargo, esto no solo se debe utilizar dentro de la oficina, ya que los trabajadores remotos y aquellos que viajan por trabajo también deben tener acceso a los archivos y compartirlos cuando sea necesario.
- **Autenticación para admitir el acceso seguro de los empleados a los datos.** En su forma más simple, las soluciones de autenticación mantienen a los chicos malos fuera y a los buenos adentro. Con tantas vulneraciones de datos que ocurren en todo el mundo, la importancia de hacer cumplir el control es primordial en la agenda. El 63 % de los encuestados sostuvo que usarán diferentes tipos de autenticación y el 38 % de los encuestados clasificó la autenticación como el esfuerzo estratégico principal que harían para mejorar la seguridad. Sin embargo, estos procesos no deben obstaculizar la productividad de los empleados ni interponerse en el proceso de trabajo; la fluidez de la experiencia de autenticación de los usuarios marca una gran diferencia.
- **Cifrado para controlar los datos y cumplir con los requisitos de cumplimiento de normas.** El 73 % por ciento de los encuestados indicó que emplearían herramientas de cifrado, mientras que el 68 % apuntó específicamente al cifrado de terminales para las laptops de los empleados (cifrado de disco completo) como lo que consideraban importante para mejorar la seguridad. En un mundo en el que es fácil que un empleado pierda un dispositivo o que se lo roben, esta es una opción prudente. El cifrado de datos en reposo también se produce de muchas formas, y las organizaciones pueden elegir en consecuencia, según sus necesidades, es decir, disco completo, nivel de archivos, medios, correo electrónico, aplicación/nivel de campo, cifrado transparente/de base de datos.
- **Evaluación de seguridad para comprender la madurez de la seguridad actual.** Si bien la mayoría de los equipos de seguridad han implementado una amplia variedad de controles y estándares para mantener su empresa segura, muchos no pueden identificar de manera objetiva dónde hay brechas de seguridad. A su vez, se esfuerzan por determinar si han abordado todos los problemas clave o si algún aspecto de las prácticas recomendadas sigue sin abordarse. El 77 % de los encuestados está al tanto de esto y busca mejorar la seguridad mediante el desarrollo de planes de corrección precisos para asegurarse de que todos los componentes cumplan con el estado deseado de la funcionalidad.

Figura 5

"¿Qué le gustaría hacer para ayudar a mejorar la seguridad?"



Base: 887 tomadores de decisiones empresariales y de TI que participan en la toma de decisiones para laptops, computadoras y otros dispositivos
Fuente: un estudio realizado por Forrester Consulting en nombre de Dell, septiembre de 2019

La seguridad equilibrada beneficia a los empleados y a la empresa

Los esfuerzos de seguridad permitirán que una empresa sea más segura, en lugar de ofuscar su progreso con desafíos en la búsqueda de una mayor generación de ingresos. Para liberar de obstáculos a la empresa, los encargados de la toma de decisiones deben adoptar un enfoque centrado en el ser humano y basado en el riesgo para diseñar la experiencia de seguridad. A medida que equilibra la creación de una excelente experiencia del empleado con una seguridad sólida, puede ayudarlo de la siguiente manera (consulte la Figura 6):

- **Permitir el trabajo remoto para mejorar la productividad y la ventaja competitiva.** Ya sea que los empleados exijan un mejor respaldo para el equilibrio entre el trabajo y la vida o que su organización contrate a la mejor persona para el trabajo, independientemente de la cercanía para viajar a una oficina, el respaldo para el trabajo remoto es una ventaja competitiva en la contratación y la permanencia del talento. La tecnología ayuda a hacer posible el trabajo remoto y la seguridad es una base fundamental para la forma en que su empresa habilitará de manera segura el trabajo remoto. El 69 % de los encuestados indicó que permiten el acceso a los datos corporativos desde los dispositivos cuando los empleados trabajan fuera de la oficina.
- **Fomentar la colaboración para estimular la innovación.** Los empleados desean compartir experiencias y, en última instancia, desean compartir archivos e ideas con sus colegas. Tanto la conexión humana como las herramientas para ayudar a facilitar esa conexión son requisitos previos para la curaduría de un entorno o cultura de la innovación, especialmente con un personal distribuido, es decir, empleados que no siempre están frente a frente con sus pares en una oficina. Por ahora, el 49 % de los encuestados afirma que se esfuerza por permitir que los empleados compartan datos de forma fácil y segura. Aún se puede mejorar, con el fin de obtener beneficios.

FORRESTER®

› **Mejorar la experiencia del cliente y reducir la rotación de empleados.** Mejorar la felicidad de los empleados a través de una mejor EX se traduce en clientes felices que reciben mejor soporte e interacciones con sus empleados. Los empleados felices son más propensos a tomar las decisiones correctas y estas decisiones les hacen bien a sus clientes.[1] Un estudio demostró que las organizaciones con empleados felices alcanzaron un 81 % más de satisfacción del cliente y la mitad de la rotación de empleados.[2]

Figura 6

"¿Qué acciones ha tomado su empresa para permitir el trabajo remoto o flexible?"

Base: 887 tomadores de decisiones empresariales y de TI que participan en la toma de decisiones para laptops, computadoras y otros dispositivos
Fuente: un estudio realizado por Forrester Consulting en nombre de Dell, septiembre de 2019

Recomendaciones clave

Invertir en su infraestructura y controles de seguridad es un componente fundamental del programa de seguridad. Sin embargo, las inversiones en tecnología por sí solas no son suficientes. Determine el nivel adecuado de seguridad equilibrada para su organización, en función de sus necesidades específicas y de su tolerancia al riesgo.

Siga cuatro pasos hoy para que la organización logre el éxito en lo que respecta a alcanzar el equilibrio adecuado entre la seguridad y la experiencia de los empleados:

Evalúe el estado actual de madurez de la seguridad. El proceso de pasar por la evaluación en sí también puede ofrecer visibilidad en procedimientos o procesos que estén relacionados con conocimiento institucional. Dado que algunos de estos procedimientos/procesos no están documentados, en el futuro, será importante encontrar los detalles, en caso de que los miembros clave del equipo se retiren o abandonen la organización. Una evaluación le permitirá ver los controles, los procesos y la supervisión de seguridad existentes de su organización para determinar las áreas que tienen posibles brechas y necesitan abordarse. Esta evaluación será útil para ofrecer orientación en su camino hacia el futuro, para saber en dónde necesita centrar la atención y por qué.

Identifique cuál es la información confidencial, por qué y dónde se encuentra. Esto incluye comprender qué datos están regulados por los requisitos de cumplimiento de normas y el valor de los datos para su organización en general. Con los controles de seguridad y las consideraciones adecuadas para el manejo de datos, la comprensión de los datos también crea una base adecuada para respaldar la privacidad y el uso ético de los datos personales. Gracias a la posibilidad de tener una visión y comprensión más claras de los datos, usted está mejor posicionado para determinar qué se requiere para protegerlos y usarlos de manera adecuada.

Comprenda el nivel de tolerancia a riesgos de su organización. Aunque las normativas pueden dictar ciertas acciones y actividades, los tipos de controles y el nivel de control que su organización elige implementar dependerán de su nivel de tolerancia al riesgo. Comprenda los riesgos que enfrentan sus datos y organización y tome decisiones basadas en dichos riesgos para los controles de seguridad, a fin de equilibrar las necesidades de los empleados y la productividad.

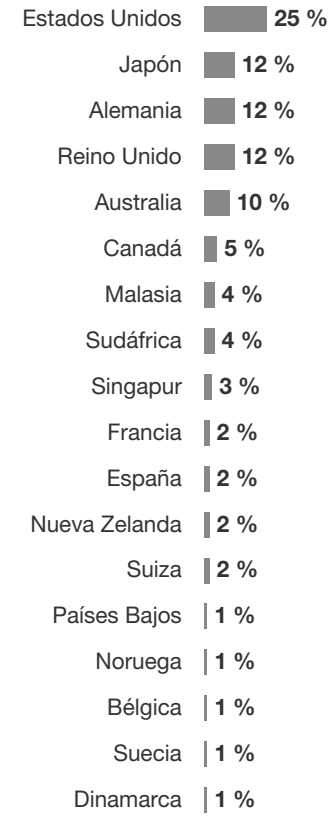
Evalúe la forma en que trabajan los empleados y cómo realizan sus trabajos. Marque las áreas donde los controles de seguridad influyen en la experiencia de trabajo de los empleados y el nivel de impacto que tienen en su jornada laboral y productividad. Los diferentes perfiles de los empleados, desde los roles en los que se encuentran, hasta los datos a los que tienen acceso para hacer su trabajo, también influirán en las necesidades tecnológicas, los riesgos que probablemente enfrenten y los tipos de controles de seguridad que usted necesitará implementar para mitigar esos riesgos. Implemente controles de seguridad necesarios, en lugar de implementar aquellos que causan una fricción innecesaria.

Apéndice A: Metodología

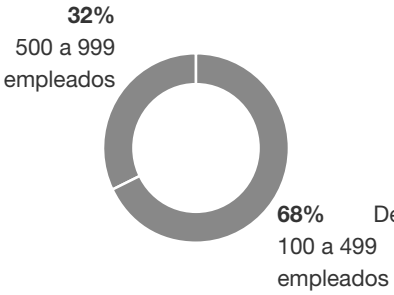
En este estudio, Forrester realizó una encuesta en línea de 887 líderes de empresas y de TI en diversas industrias del mercado. Las preguntas que se hicieron a los participantes analizaron cómo ha cambiado el gasto en seguridad, qué influye en la estrategia de seguridad, el cumplimiento de normas y los desafíos regulatorios, así como también cómo se ve el futuro de la seguridad para su organización. El estudio comenzó en marzo de 2019 y el informe de liderazgo intelectual finalizó en agosto de 2019.

Apéndice B: Demografía

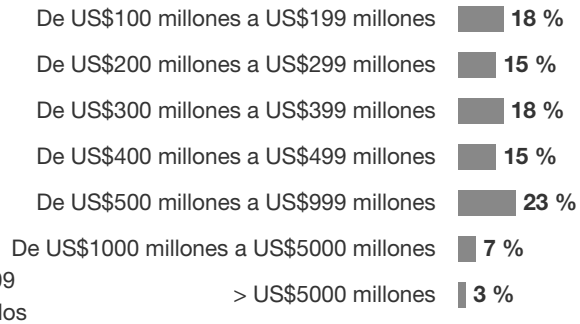
"¿En qué país se encuentra?"



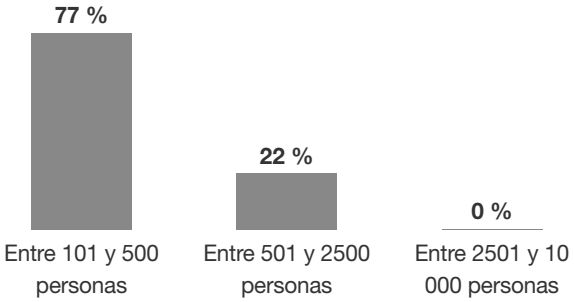
"Según su estimación, ¿cuántos empleados trabajan para su empresa/organización en todo el mundo?"



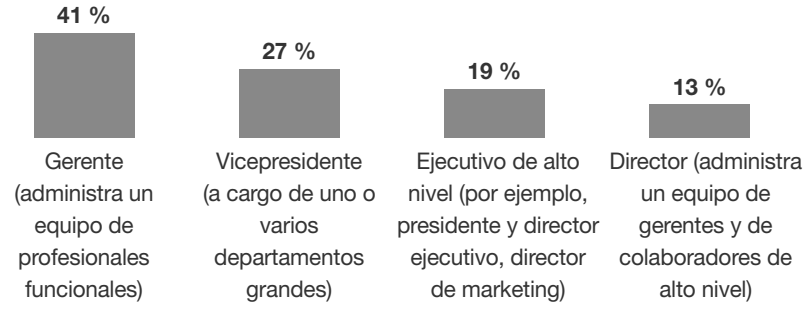
"Según su estimación, ¿cuál es el ingreso anual de su organización (USD)?" (N = 861)



"En relación con las decisiones de compra de tecnología y servicios en las que usted influye más, ¿a cuántos empleados o miembros de la fuerza de trabajo de su organización impactan directamente?"



"¿Qué puesto describe mejor su posición en la organización?"



Base: 887 responsables de la toma de decisiones empresariales y de TI que participan en la toma de decisiones para laptops, computadoras y otros dispositivos
Fuente: un estudio realizado por Forrester Consulting en nombre de Dell, marzo de 2019

FORRESTER®

Apéndice C

NOTAS FINALES

[1] Fuente: “Transform the Employee Experience to Drive Business Performance”, de Forrester Research, Inc., 12 de febrero de 2018.

[2] Fuente: “Business-Unit-Level Relationship Between Employee Satisfaction, Employee Engagement, and Business Outcomes: A Meta-Analysis,” de James K. Harter, Frank L. Schmidt, and Theodore L. Hayes, en Journal of Applied Psychology, abril de 2002 (http://www.factorhappiness.at/downloads/quellen/s17_harter.pdf).