Kensington®

Protege su dispositivo, portege sus datos

Cómo la seguridad física puede ayudar a prevenir las violaciones de datos

Introducción

El panorama de la seguridad ha evolucionado drásticamente en los últimos años, impulsado por cambios transformadores en cómo y dónde trabajamos. El factor determinante de esto fue la pandemia de COVID-19, que aceleró la adopción de modelos de trabajo híbridos y flexibles y alteró fundamentalmente las prioridades de seguridad de los dispositivos.

Kensington patrocinó un estudio realizado por Vanson Bourne especialista independiente en investigación de mercado, en el que participaron 1000 responsables de la toma de decisiones de IT de alto nivel con responsabilidad por la seguridad del hardware físico de su organización en EE. UU. y EMEA. Casi todos los encuestados (**92%**) reforzaron sus políticas de seguridad en respuesta a la pandemia, reconociendo los mayores riesgos asociados con los entornos de trabajo descentralizados. De cara a 2025, se espera que aumente el nivel de modelos de trabajo más flexibles, lo que pone de relieve que ahora es el momento de replantear las estrategias de seguridad de los dispositivos.

Las filtraciones de datos no son solo un problema digital: cada dispositivo robado o no protegido representa una puerta de entrada potencial para el acceso no autorizado a información confidencial, lo que plantea riesgos significativos para las organizaciones. Con la carga financiera de una filtración de datos que ahora promedia millones de dólares, lo que está en juego nunca ha sido tan grande. A medida que las organizaciones continúan adaptando sus modelos de trabajo, la urgencia de abordar la seguridad de los dispositivos ha crecido enormemente. Los requisitos de protección de datos más estrictos y un aumento en las filtraciones de datos han aumentado aún más la importancia de salvaguardar tanto los dispositivos físicos como la información confidencial que contienen. Este informe destaca el papel fundamental que desempeñan los candados de seguridad para mitigar estos riesgos y subraya por qué es esencial tomar medidas ahora para mantenerse a la vanguardia de los desafíos emergentes.

A través de estos hallazgos, examinaremos los impactos tangibles del robo de dispositivos, demostraremos cómo soluciones simples pero efectivas como los candados de seguridad pueden mitigar los riesgos y destacaremos cómo la seguridad física brinda tranquilidad en un mundo donde los modelos de trabajo evolucionan constantemente. Desde la comprensión de las asombrosas consecuencias del robo de dispositivos hasta la demostración de la rentabilidad y la tranquilidad de los candados, este informe proporciona información práctica para las organizaciones que navegan por el complejo panorama de seguridad actual.

Ideas clave:

El **76%** de los encuestados afirma que su organización se ha visto afectada por incidentes de robo en los últimos 2 años, y que los incidentes son más comunes en organizaciones con modelos de trabajo más flexibles (**79%**) en comparación con aquellas donde los empleados están completamente en el sitio (**71%**).

Las consecuencias del robo de dispositivos se extienden más allá de la pérdida de hardware e incluyen:

- la necesidad de mejorar las medidas de seguridad existentes (**33%**)
- Consecuencias legales o regulatorias debido a datos comprometidos en dispositivos robados (**33%**)
- Interrupción de la productividad de los empleados debido a dispositivos perdidos o robados (**32%**)

Las organizaciones que utilizan candados de seguridad tienen un **37%** menos de probabilidades de sufrir un robode datos causada por un dispositivo no seguro (**38%** frente al **60%** entre las que no utilizan candados de seguridad).

Las organizaciones que actualmente utilizan candados también tienen más probabilidades de utilizar un enfoque dual para la seguridad: tres cuartas partes (**76%**) utilizan medidas digitales como huellas dactilares o llaves de seguridad para la autenticación de dos factores, en comparación con el **62%** de las que no utilizan cerraduras en absoluto.

El **84%** está de acuerdo en que los candados de seguridad son rentables para mitigar posibles robos de datos y ofrecen un valor significativo por una inversión relativamente baja.

- El **42%** cree que los candados de dispositivos son extremadamente rentables y brindan alta protección a bajo costo, y los líderes más importantes tienen más probabilidades de reconocer su valor (**56%**)en comparación con la gerencia de nivel medio (**36%**).

Casi todos los encuestados (**97%**) creen que los candados de dispositivos previenen el robo, reduciendo la probabilidad de acceso no autorizado a datos confidenciales de la empresa.

Esta percepción se mantiene constante independientemente de si se utilizan actualmente candados de dispositivos (**98%**) o no (**95%**).

Dispositivos robados, consecuencias asombrosas

Es raro que pase un día sin que se escuche hablar de algún tipo de incidente de seguridad, ya sea un ataque a gran escala contra un conglomerado global o una explotación más específica de una infraestructura o servicio crítico. Y aunque estos ejemplos lo sugieren, a menudo son los incidentes cibernéticos de los que más se habla (o al menos se supone que lo son).

Se habla poco de los incidentes de seguridad física, en los que personas no autorizadas obtienen acceso a áreas protegidas o ponen en peligro activos, que tienen consecuencias tan nefastas como el ataque de ransomware promedio. Según nuestra investigación, más de tres cuartas partes (**76%**) de los encuestados afirman que su organización se ha visto afectada por incidentes de robo de dispositivos en los últimos dos años.

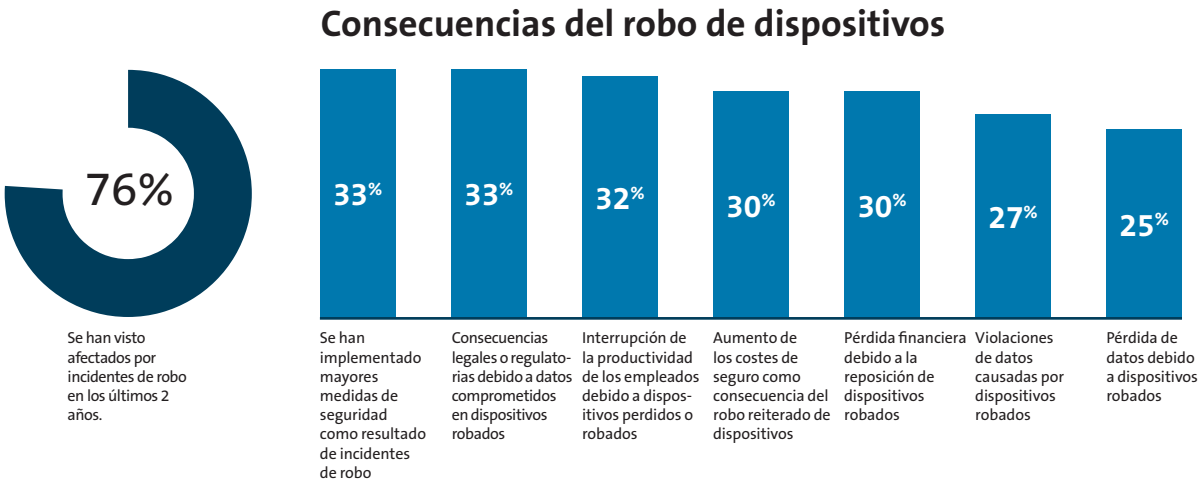


Fig. 1: *¿Cómo se ha visto afectada su organización por incidentes de robo de dispositivos en los últimos dos años? [Pregunta a todos los encuestados: 1000]*

Las organizaciones no solo se enfrentan al costo obvio de reemplazar un dispositivo (**30%**). Los impactos más comunes incluyen un aumento en las medidas de seguridad implementadas como resultado (**33%**) o consecuencias legales o regulatorias debido a datos comprometidos (**33%**), donde esto último suele estar claramente descrito. Por ejemplo, GDPR[1] Las multas pueden alcanzar hasta 20 millones de euros o el **4%** de la facturación global de una organización, e incluso las infracciones menos graves pueden llegar a costar hasta 10 millones de euros, lo que plantea importantes riesgos financieros por incumplimiento. A los impactos financieros se suma el coste de la interrupción de la productividad de los empleados debido a la pérdida o el robo de dispositivos (**32%**). Además de cualquiera de estos impactos, existe una clara implicación financiera o de tiempo en el resultado final de la organización. Por lo tanto, no son solo los incidentes de seguridad digital los que exigen atención: las amenazas físicas también plantean riesgos importantes. Al profundizar su conocimiento de estas vulnerabilidades, las organizaciones pueden tomar medidas sencillas y rentables para proteger sus dispositivos. Dado que las medidas de seguridad física son asequibles y fáciles de implementar (como analizaremos más adelante), representan un primer paso práctico para fortalecer la seguridad general.

"Además de las medidas de ciberseguridad, **la seguridad física es igualmente importante.** Los candados de seguridad son parte de una estrategia de ciberseguridad más sólida"

Alta dirección; Fabricación y producción; 1.000 o más empleados; Modelo de trabajo totalmente presencial; Francia

1 Multas y sanciones del RGPD, Intersoft Consulting,, https://gdpr-info.eu/issues/fines-penalties/

En la actualidad, no se trata de si se produce una filtración de datos, sino de cuándo. De hecho, cada robo de dispositivo es una filtración de datos a punto de ocurrir, y las implicaciones financieras son asombrosas para las organizaciones. Según el informe más reciente de IBM sobre el costo de la filtración de datos[2], el costo promedio global de una filtración de datos en 2024 se sitúa en 4,88 millones de dólares, un aumento del **10%** en un año desde el promedio de 4,45 millones de dólares en 2023. Esta cifra difiere según la industria y el tamaño de la organización, por lo que algunas organizaciones pueden enfrentar costos aún mayores.

Los datos en el punto de mira:

- **Sector:** las organizaciones de los sectores de servicios al consumidor (**95%**), , energía, petróleo/gas y servicios públicos (**90%**) y construcción e inmuebles (**89%**) son las que tienen más probabilidades de verse afectadas por el robo de dispositivos. La mayor movilidad de los empleados y los dispositivos en estas empresas las expone a un mayor riesgo de robo.
- **Tamaño:** los impactos del robo de dispositivos en organizaciones más pequeñas (100-249 empleados) han sido más generalizados (**82%**) que en organizaciones más grandes con más de 1000 empleados (**69%**), destacando el impacto relativo en las organizaciones más pequeñas donde los recursos son más limitados, los impactos son más pronunciados.
- **Antigüedad:** los que ocupan puestos de mayor jerarquía son mucho más propensos a informar que se han visto afectados por incidentes de robo (**87%**) que los gerentes de nivel medio (**67%**). Es probable que quienes están a cargo de la gestión diaria de una empresa estén mal informados sobre las posibles amenazas a las que se enfrentan los dispositivos no seguros. Aumentar su conciencia de las amenazas y las repercusiones asociadas ayudará a alentar a las empresas a incorporar candados de seguridad en sus necesidades culturales y alinear las perspectivas en todos los niveles para respaldar una estrategia de seguridad integral.

¿Qué papel juegan aquí los modelos de trabajo?

Al presentar esta investigación, observamos el gran cambio en las formas de trabajar en los últimos años, con la adopción de modelos de trabajo más flexibles lejos de un lugar de trabajo fijo que se ha visto acelerada por la pandemia de COVID-19.

Donde vemos que más de tres cuartas partes (**76%**) de todos los encuestados informan que su organización se ha visto afectada por el robo de dispositivos en los últimos 2 años, esto se hace más evidente donde los modelos de trabajo son más flexibles, aumentando a más de 9 de cada 10 (**94%**) donde los empleados son completamente remotos.

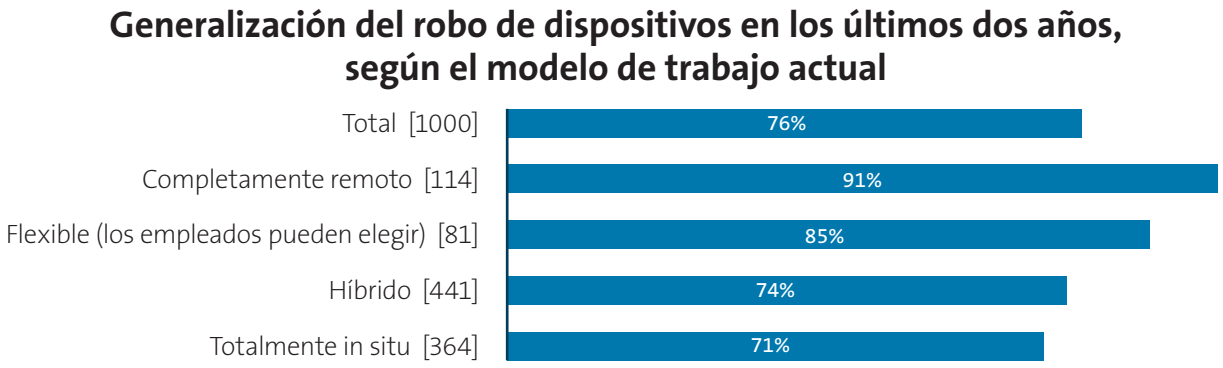


Fig. 2: *Proporción de encuestados cuya organización se vio afectada por incidentes de robo de dispositivos en los últimos dos años [Pregunta realizada a todos los encuestados, mostrando datos divididos por modelo de trabajo actual, números base en el gráfico]*

2 Informe sobre el costo de las violaciones de datos 2024, IBM, julio de 2024, , https://www.ibm.com/reports/data-breach

Si bien es importante que cualquier organización sea consciente de la seguridad de los dispositivos físicos y cautelosa ante los impactos del robo de dispositivos, los modelos de trabajo flexibles y remotos amplifican significativamente el riesgo de robo de dispositivos, lo que hace que las medidas de seguridad sólidas sean más críticas que nunca.

Es importante señalar que el nivel de robo de dispositivos es generalmente alto, incluso cuando los empleados están completamente en la oficina: las organizaciones no tienen margen para la complacencia, independientemente de dónde trabajen sus empleados. La amenaza del robo de dispositivos no es nueva y tampoco ha aparecido como parte de este mundo pospandémico. Nuestra investigación en 2016[3] investigó los riesgos de seguridad creados por el robo de TI en la empresa. Los profesionales de TI encuestados clasificaron el riesgo de robo de dispositivos en la oficina (**23%**) casi tan alto como el robo en automóviles y transporte (**25%**), y más que el robo en aeropuertos y hoteles (**15%**) o restaurantes (**12%**). Esto muestra cómo el robo de dispositivos sigue siendo una amenaza persistente, incluso en entornos completamente in situ, lo que subraya la necesidad de vigilancia y medidas de seguridad física proactivas independientemente del entorno del lugar de trabajo.

Este desafío se ha amplificado aún más en el mundo tras el COVID-19, donde el **93%** de las organizaciones informan un aumento de los riesgos de seguridad debido al cambio a modelos de trabajo flexibles e híbridos. Estos riesgos se extienden más allá del robo de dispositivos físicos e incluyen mayores vulnerabilidades en la protección de datos, acceso no autorizado y violaciones causadas por redes domésticas no seguras y entornos de trabajo descentralizados.

"**Es la forma más sencilla** de garantizar que nuestros dispositivos estén bajo llave. **Nos permite saber que todo está seguro y protegido.**"

Miembro de la junta directiva/nivel C; TI, tecnología y telecomunicaciones; 100-249 empleados; modelo de trabajo flexible; EE. UU.

El riesgo de seguridad aumenta como resultado de entornos de trabajo híbridos o remotos

Fig. 3: *En su opinión, ¿qué riesgos de seguridad han aumentado como resultado de los entornos de trabajo híbridos o remotos tras la pandemia de COVID-19? [Pregunta a los encuestados cuya organización experimentó un cambio hacia el trabajo híbrido/remoto tras la pandemia de COVID-19: 494]*

Con esto en mente, el mejor enfoque en materia de seguridad consiste en combinar medidas físicas robustas con salvaguardas digitales avanzadas, garantizando una protección integral tanto para los dispositivos como para los datos en un mundo cada vez más descentralizado.

3 Encuesta sobre seguridad informática y robo de ordenadores portátiles, Kensington, agosto de 2016, https://www.kensington.com/news/news-press-center/2016-news--press-center/kensington-survey-data-reveals-that-it-theft-in-the-office-ranks-nearly-as-high-as-theft-in-cars-and-more-than-in-airports-or-restaurants/?srsltid=AfmBOooRTMdZ4gjmcNB3viXI-JcIL4GY47XxO5I08AldLhLEB5LjnH0Ts

Candados que evitan pérdidas y ahorran costos

"La falta de un candado de seguridad en los equipos provocó una filtración de datos, **lo que se tradujo en importantes pérdidas para la empresa.**"

Gerencia de nivel medio; TI, tecnología y telecomunicaciones; 1000 o más empleados; Modelo de trabajo flexible; EE. UU.

Hasta ahora, hemos descubierto las consecuencias del robo de dispositivos y lo generalizado que es, independientemente del entorno de trabajo. Sin embargo, esta no es la única preocupación de los responsables de la toma de decisiones de IT a los que hemos encuestado. Existe una amplia gama de aspectos que les preocupan en lo que respecta a la seguridad, tanto en áreas físicas como digitales.

Áreas más preocupantes de la seguridad de los dispositivos

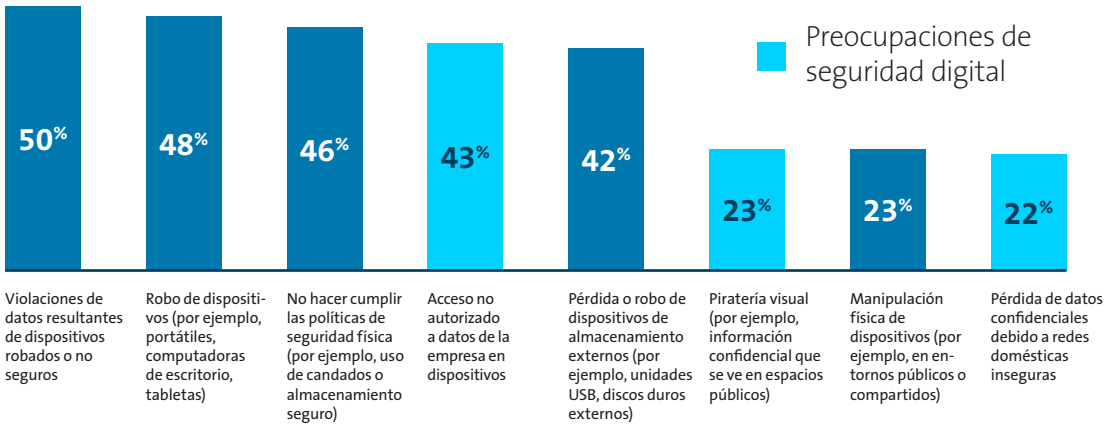


Fig. 4: *¿Qué áreas de seguridad de dispositivos de su organización le preocupan más? [Pregunta a todos los encuestados: 1000, mostrando la combinación de respuestas clasificadas en primer, segundo y tercer lugar]*

Algunas de estas preocupaciones presentan factores más nuevos en torno a la seguridad física. Por ejemplo, casi una cuarta parte (**23%**) está preocupada por el hackeo visual, en el que los datos confidenciales quedan a merced de cualquiera si la pantalla de alguien está expuesta en un lugar público, en una cafetería o en el transporte público. De hecho, quienes trabajan de manera flexible (**48%**) son más propensos que quienes trabajan en configuraciones completamente remotas (**36%**) o híbridas (**33%**) a reportar el hackeo visual como una preocupación. Esto resalta que el hackeo visual no solo está asociado con el trabajo desde casa, sino más bien con la concesión de libertades excesivas que son más difíciles de controlar. Las organizaciones deberán tener en cuenta la protección de sus datos cuando los empleados estén fuera de casa, a través de elementos disuasorios adicionales como las pantallas de privacidad.

Sin embargo, las filtraciones de datos son la principal preocupación, lo cual está bien fundado ya que una proporción notable (**46%**) ha experimentado una filtración de datos como consecuencia directa de un dispositivo no seguro. En mayo de 2024, por ejemplo, un dispositivo robado del condado de Multnomah[4] provocó una filtración de datos que involucraba información médica protegida (PHI), como nombres, direcciones y números de historial médico de clientes del centro de salud. El incidente ocurrió cuando el dispositivo de un ex empleado, que contenía datos confidenciales, fue manipulado, exponiendo a la organización a importantes riesgos de seguridad y regulatorios. Como resultado, el condado tuvo que notificar a las personas afectadas, gestionar las posibles consecuencias legales y de cumplimiento y abordar la pérdida de confianza entre sus partes interesadas.

4 Violación de datos, condado de Multnomah, mayo de 2024, https://multco.us/news/news-release-multnomah-county-notifies-health-center-clinic-clients-potential-breach

En este caso, un candado de seguridad puede resultar de ayuda. Las organizaciones que utilizan candados de seguridad tienen un **37%** menos de probabilidades de sufrir una vulneración de datos debido a un dispositivo no protegido en comparación con aquellas que no utilizan candados de seguridad en absoluto.

Organizaciones que han sufrido un filtración de datos o pérdida de datos confidenciales debido a un dispositivo no asegurado

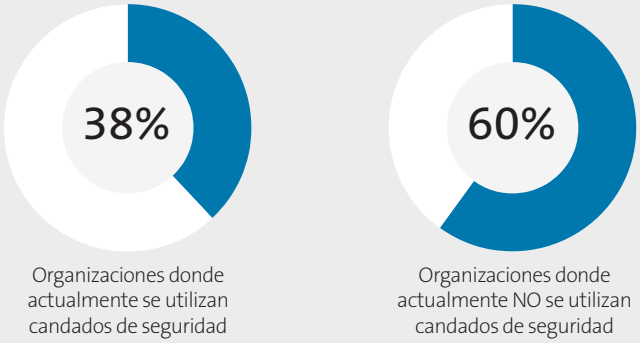


Fig. 5: *¿Su organización ha sufrido una filtración de datos o una pérdida de datos confidenciales como consecuencia directa de que un dispositivo no estuviera protegido? [Pregunta realizada a todos los encuestados, divididos entre los que utilizan actualmente candados de seguridad: 629; y los que no las utilizan actualmente: 371]*

El resultado es claro: demostrar una reducción mensurable de las filtraciones o pérdidas de datos refuerza el valor de los candados de seguridad como un componente fundamental de la protección integral de los dispositivos. Esta evidencia convincente destaca cómo los candados de seguridad mitigan directamente el riesgo, lo que los posiciona como una inversión esencial para las organizaciones comprometidas con la protección de sus datos y la minimización de las vulnerabilidades de seguridad.

Los datos en el punto de mira:

- **Sector:** las organizaciones de los sectores de servicios al consumidor (**65%**) y atención sanitaria pública/privada (**57%**) tienen más probabilidades de haber sufrido una filtración de datos como consecuencia de un dispositivo no protegido. El primero es uno de los sectores con más probabilidades de haberse visto afectado por el robo de dispositivos en general. En el caso del segundo, esto quizás pone de relieve mayores preocupaciones por la naturaleza descentralizada de las instituciones sanitarias y los miembros del público que están en contacto más cercano con los dispositivos. Tener una riqueza de datos tan sensible pone a este sector en un problema aún mayor.
- **Tamaño:** lo que pone de relieve aún más los recursos limitados de las organizaciones más pequeñas es que tienen más probabilidades (**59%**) que sus contrapartes más grandes (**40%**) de haber sufrido una filtración de datos debido a un dispositivo no seguro. No solo tienen problemas con los elementos disuasorios iniciales, sino también con el efecto dominó que sigue.
- **Antigüedad:** los más jóvenes de los encuestados tienen menos probabilidades de denunciar una violación de datos o pérdida de datos confidenciales debido a un dispositivo no seguro (**30%**) que sus colegas de la junta directiva o de nivel C (**59%**). Existe una clara falta de alineación dentro de las empresas cuando se trata de una verdadera comprensión de la seguridad de los dispositivos físicos y las consecuencias de no implementarla, lo que hace un llamado a una educación más amplia y al intercambio de conocimientos.

"Una pequeña inversión inicial en medidas de seguridad (candados) puede **reducir considerablemente la posibilidad de reemplazos costosos de dispositivos** o tiempos de inactividad prolongados."

Alta dirección; Educación (proporcionada por el gobierno o el estado); 1000 o más empleados; Modelo de trabajo híbrido; EE. UU.

Entonces, ¿cómo deberían las organizaciones intentar superar esto?

Las organizaciones se enfrentan a muchos problemas de seguridad física y digital, y las repercusiones del robo de dispositivos son abrumadoras para ellas y sus resultados. Deberían buscar la solución más rentable y, con su éxito demostrado, esa solución podría ser un simple candado de seguridad.

La mayoría (**84%**) de los responsables de la toma de decisiones de IT encuestados afirman que los candados de seguridad son rentables para mitigar posibles filtraciones de datos, ya que ofrecen un valor significativo para prevenir robos y filtraciones. Además, el **42%** cree que son extremadamente rentables.

Esta es una opinión universal compartida por aquellos que ya utilizan candados de seguridad e incluso por aquellos que no las utilizan, lo que plantea la pregunta: ¿por qué no? Las organizaciones pueden considerar que los candados añaden desafíos logísticos a la gestión de dispositivos o tal vez un mayor enfoque en la seguridad digital sobre la física conduce a una subestimación del valor de los candados, lo que dificulta la adopción. Sin embargo, cuando se compara con las asombrosas consecuencias financieras del robo de dispositivos, el costo de un candado de seguridad (que normalmente promedia tan poco como $30 a $50 por dispositivo) representa una inversión mínima para reducir significativamente los riesgos. Profundizando en esto, vemos una clara diferencia de opinión en toda la jerarquía organizacional.

Relación coste-beneficio percibida de los candados de seguridad

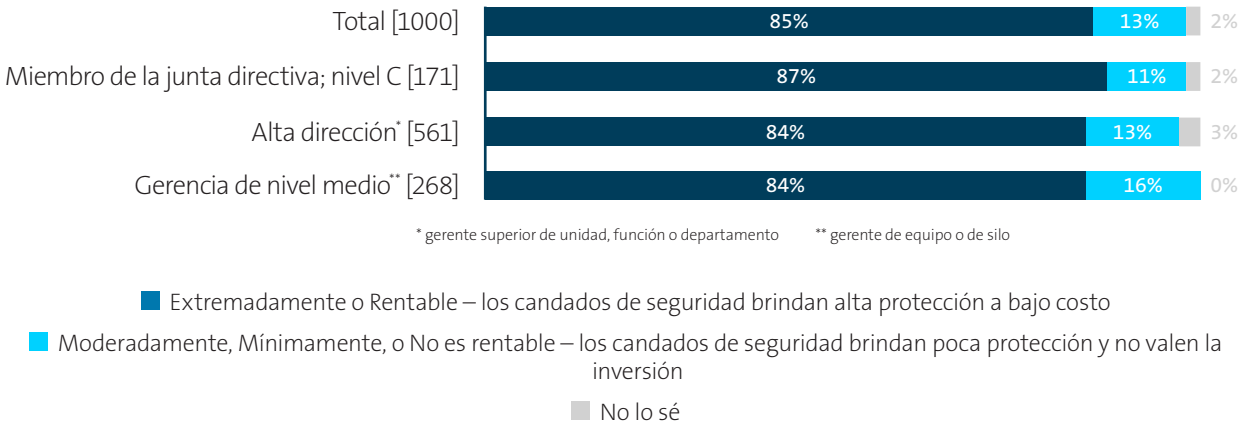


Fig. 6: *En términos de relación costo-beneficio, ¿cómo ve el papel de las candados de seguridad físicas en la mitigación de posibles violaciones o robos de datos? [Pregunta a todos los encuestados, mostrando los datos divididos por antigüedad, números base en el gráfico]*

Estos hallazgos enfatizan la necesidad crítica de abordar las causas fundamentales del robo de dispositivos y sus impactos más amplios en toda la organización. Si bien los líderes superiores son más propensos a considerar que los candados de seguridad son extremadamente rentables (**56%**), esta creencia disminuye en los niveles más bajos de la jerarquía. En última instancia, los líderes superiores siempre se centrarán más en las implicaciones más amplias (por ejemplo, multas regulatorias, reputación), mientras que los gerentes de nivel inferior en los impactos diarios (por ejemplo, pérdida de productividad).

Esta desconexión resalta la importancia de la alineación organizacional y la educación en torno al valor de los candados de seguridad, no solo como una herramienta rentable, sino como una solución proactiva para prevenir pérdidas significativas antes de que ocurran. Superar estas brechas en la percepción garantizará un enfoque unificado y eficaz para mitigar los riesgos de robo de dispositivos y proteger los datos confidenciales.

"Una vez perdido, causará pérdidas significativas. Necesitamos **resolver este problema desde su raíz.**"

Gerencia de nivel medio; Salud - propiedad privada; 1000 o más empleados; Modelo de trabajo híbrido; EE. UU.

Los candados de seguridad funcionan para asegurar y tranquilizar

Hemos seguido explorando cómo los candados de seguridad no solo son eficaces para reducir los robos, sino que también ofrecen una solución rentable para mitigar riesgos de seguridad más amplios. Sus diversas aplicaciones resaltan su versatilidad para abordar los desafíos de seguridad en diversos entornos, un beneficio que muchas organizaciones ya están percibiendo.

Muchos ya están utilizando candados de seguridad para proteger los dispositivos electrónicos de su organización. Los dispositivos más comúnmente protegidos incluyen ordenadores portátiles (**44%**), ordenadores de escritorio (**43%**) y servidores (**42%**), lo que refleja la prioridad que se le da a la protección del hardware crítico que a menudo contiene datos confidenciales. Esta adopción generalizada resalta el reconocimiento de los candados como una herramienta vital para protegerse contra el robo y el acceso no autorizado.

Relación coste-beneficio percibida de los candados de seguridad

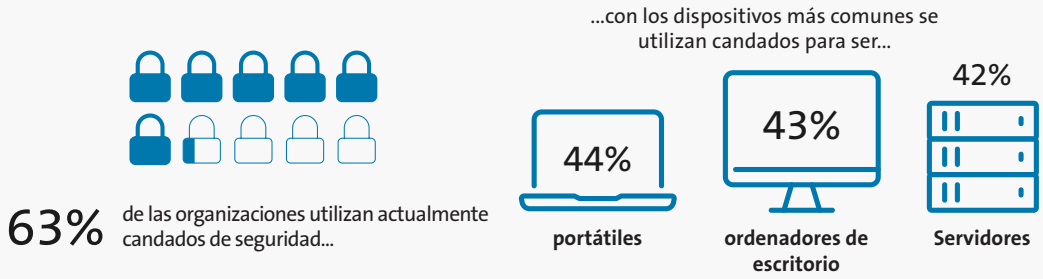


Fig. 7: *¿En cuáles de los siguientes dispositivos electrónicos se utilizan candados de seguridad físicas en su organización? [Pregunta a todos los encuestados: 1000]*

Sin embargo, el hecho de que casi 4 de cada 10 de los encuestados digan que sus organizaciones no utilizan candados plantea preocupaciones sobre vulnerabilidades en las estrategias de seguridad de los dispositivos, especialmente para los dispositivos que se utilizan con frecuencia en entornos de trabajo móviles o híbridos.

Para las organizaciones, estos datos subrayan la necesidad de evaluar de forma exhaustiva sus medidas de seguridad actuales. Si bien los candados son una solución confiable y ampliamente utilizada, ampliar su uso a una gama más amplia de dispositivos y combinarlas con protecciones digitales complementarias puede ayudar a cerrar las brechas de seguridad existentes y mitigar los riesgos de manera más eficaz.

Casi todos los encuestados (**97%**) reconocen el papel fundamental que desempeñan los candados de seguridad para prevenir el robo y el acceso no autorizado que suele derivar de ello. Este reconocimiento generalizado refleja la confianza que las organizaciones depositan en la seguridad física como medida fundamental para salvaguardar los dispositivos y los datos confidenciales. Los candados actúan como una defensa de primera línea, reduciendo las oportunidades de robo y mitigando los riesgos asociados con el hardware comprometido.

"Tener candados en oficinas abiertas, espacios de coworking u otras áreas donde puede haber varias personas **reduce el riesgo de robo.**"

Miembro de la junta directiva/nivel C; Educación – propiedad privada; 100-249 empleados; EE. UU.

Creencia de que las medidas de seguridad física contribuyen a prevenir el robo de dispositivos

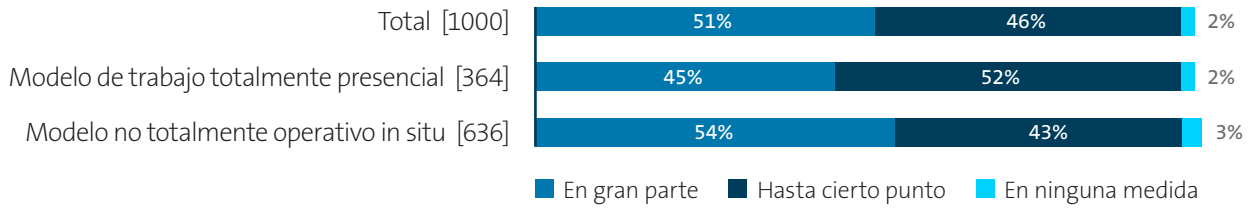


Fig. 8: *¿En qué medida cree que las medidas de seguridad física, como los candados de seguridad, contribuyen a prevenir el robo de dispositivos que podría dar lugar a un acceso no autorizado a los datos de la empresa? [Pregunta a todos los encuestados, mostrando los datos divididos por tipo de modelo de trabajo, números base en el gráfico]*

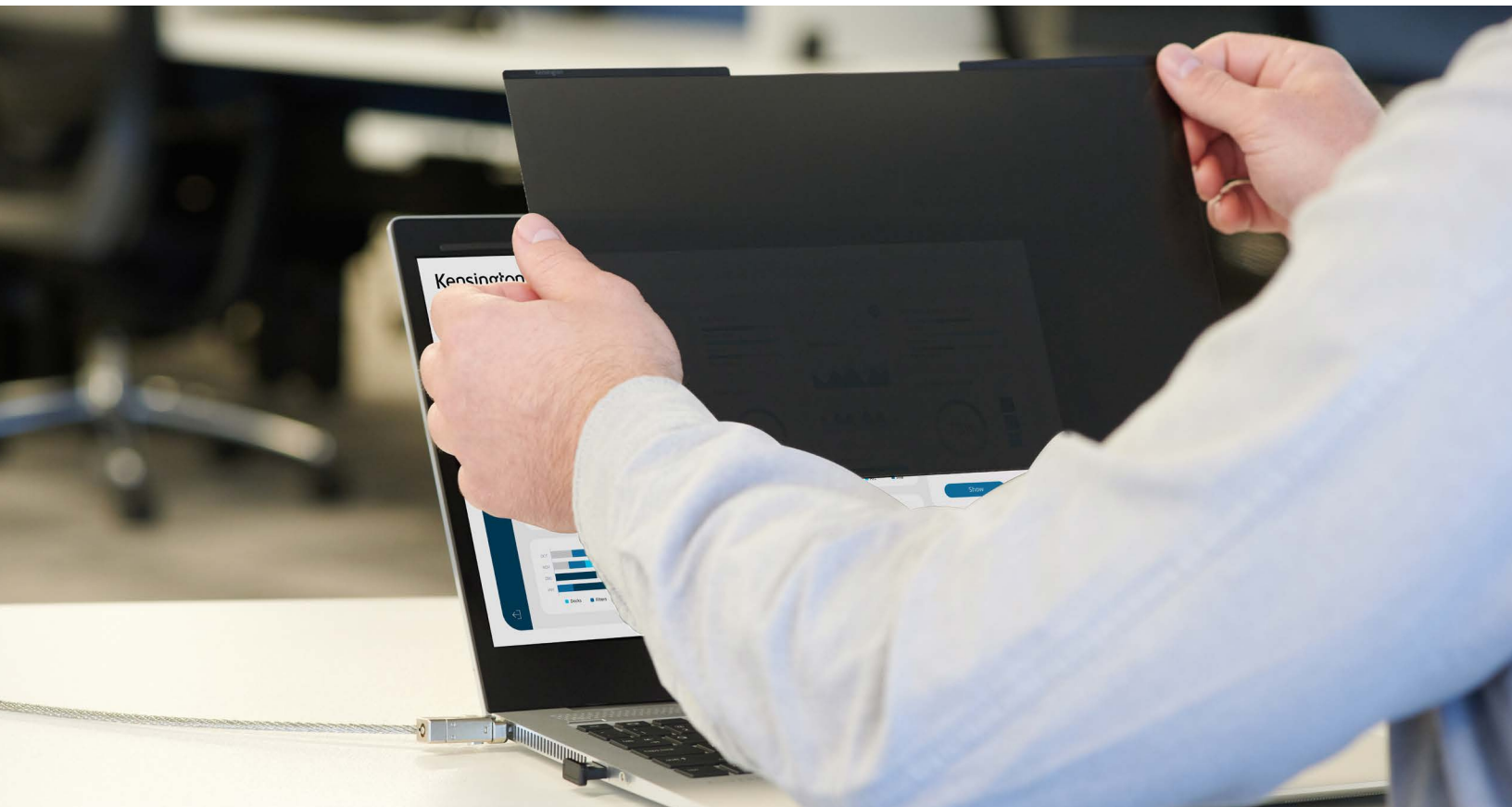
Este reconocimiento se hace más evidente en las organizaciones que han adoptado modelos de trabajo flexibles e híbridos. En estos entornos descentralizados, los dispositivos se utilizan cada vez más en lugares no seguros, como oficinas en casa o espacios públicos, lo que aumenta el riesgo de robo o exposición accidental. Las filtraciones de datos causadas por dispositivos no seguros son significativamente más comunes en las configuraciones de trabajo más flexibles (**50%** en conjunto frente al **39%** en un modelo de trabajo totalmente presencial).

Los candados de seguridad están diseñados para adaptarse a diversos entornos, ofreciendo una protección confiable para los dispositivos ya sea que se utilicen en oficinas, espacios de trabajo remotos o entornos públicos, brindando a las organizaciones tranquilidad en todos los modelos de trabajo.

Las consecuencias financieras del robo de dispositivos son asombrosas, y el costo de reemplazar el hardware robado a menudo se ve eclipsado por los impactos más amplios en la productividad, el cumplimiento normativo y las filtraciones de datos. Para las organizaciones, cada dispositivo robado o no protegido representa un riesgo significativo, no solo para las operaciones sino también para el resultado final. Los candados de seguridad ofrecen una solución probada y rentable, en la que muchos ya confían para reducir la probabilidad de robo y las consecuencias financieras y de reputación resultantes. Al abordar estos riesgos desde la raíz, las organizaciones pueden adoptar una postura proactiva para proteger sus activos y datos confidenciales.

Si bien las medidas de seguridad física, como los candados, son eficaces, deben formar parte de una estrategia más amplia para abordar los riesgos de seguridad en constante evolución asociados con el trabajo híbrido. La combinación de candados con protecciones digitales complementarias, como el cifrado y la autenticación de dos factores, garantiza una cobertura integral contra amenazas físicas y digitales. Los programas de capacitación para educar a los empleados sobre la importancia de este enfoque integrado pueden fortalecer aún más la seguridad organizacional. Para las organizaciones que navegan por las complejidades de los modelos de trabajo modernos, la integración de medidas de seguridad físicas y digitales es esencial para minimizar los riesgos, proteger a su fuerza laboral y mantener la resiliencia operativa.

Prevenir el robo de dispositivos y las filtraciones de datos resultantes es mucho más rentable que lidiar con las consecuencias. Tomar medidas preventivas, como usar candados para ordenadores portátiles hoy, puede proteger a su organización de impactos financieros y operativos significativos en el futuro. Para garantizar que estas medidas sean efectivas, es fundamental que todos los directivos, la gerencia y los equipos estén alineados. Un compromiso compartido con las prioridades de seguridad garantiza que todos comprendan su papel en la protección de activos valiosos y la reducción de riesgos.



Metodología

Kensington ha patrocinado un estudio realizado por Vanson Bourne especialista independiente en investigación de mercado, para llevar a cabo la investigación en la que se basa este informe. En el otoño de 2024, se entrevistó a un total de 1000 líderes de IT sénior que participan o tienen influencia en la seguridad del hardware físico de TI en su organización , con representación en EE. UU., Reino Unido, Francia y Alemania.

Los encuestados debían pertenecer a organizaciones con 100 o más empleados y pertenecer a un rango de sectores públicos y privados.

Las entrevistas se realizaron en línea y se llevaron a cabo mediante un riguroso proceso de selección de varios niveles para garantizar que solo los candidatos adecuados tuvieran la oportunidad de participar. A menos que se indique lo contrario, los resultados analizados se basan en la muestra total.

Acerca de Kensington

Kensington es un proveedor líder de accesorios para dispositivos móviles y de escritorio, en el que confían profesionales de IT, educadores, empresas y oficinas domésticas de todo el mundo desde hace más de 40 años. Kensington se esfuerza por anticipar las necesidades y los desafíos de un lugar de trabajo en constante evolución y crear soluciones galardonadas de nivel profesional para organizaciones comprometidas con brindar a los mejores profesionales las herramientas que necesitan para prosperar. La empresa se enorgullece de ser la elección de los profesionales y de sus valores fundamentales en torno al diseño, la calidad y el soporte.

En entornos de oficina y móviles, la amplia cartera de productos galardonados de Kensington ofrece seguridad confiable, innovaciones en productividad de escritorio, videoconferencias profesionales y bienestar ergonómico.

Con sede en Burlingame, California, Kensington es el inventor y líder mundial en candados de seguridad para ordenadores portátiles. Kensington es una marca registrada de ACCO Brands. Todas las demás marcas registradas y no registradas son propiedad de sus respectivos dueños.

FOR MORE INFORMATION CONTACT: sales@kensington.com

Kensington
The Professionals' Choice™