Aumentan las preocupaciones por la seguridad a medida que el IoT se expande

Perspectivas de mercado sobre la seguridad del IoT

ESTUDIO DE INVESTIGACIÓN

REFORZAR LA SEGURIDAD

Cómo mitigar los riesgos de seguridad del IoT en una era de amenazas crecientes

Una de las mayores tendencias preparadas para tener un impacto transformador en la economía digital del futuro es el Internet de las cosas (IoT). El IoT ya está ofreciendo capacidades avanzadas para aplicaciones del mundo real, desde vehículos y hogares conectados hasta contadores inteligentes para servicios y supervisión de la salud. De acuerdo con una estimación, se espera que la cantidad de dispositivos conectados a nivel mundial aumente en un promedio del 12 % por año, y pase de cerca de 27 mil millones en 2017 a 125 mil millones en 2030.[1]

El funcionamiento del IoT se basa en diversas tecnologías subyacentes básicas. Entre las principales se encuentran las redes de comunicaciones, los dispositivos de hardware y los componentes tales como sensores, instrumentos inalámbricos y software. Al igual que cualquier sistema de TI, las redes y los dispositivos son susceptibles a la manipulación, la interrupción y la intromisión. Estos dispositivos están conectados entre sí, y si uno de ellos corre peligro, un hacker podría conectarse a varios de los demás dispositivos de la red.

Si bien el IoT ofrece amplios beneficios, también brinda un punto de entrada atractivo para que personas malintencionadas obtengan acceso a sistemas que se consideraban seguros. En un momento en el que los entornos de seguridad ya están experimentando presiones en materia de escalabilidad y costos, los expertos en seguridad del IoT se enfrentan a la tarea monumental de buscar la forma de proteger las redes y los dispositivos de un conjunto cada vez mayor de riesgos que podrían poner en peligro la privacidad personal y amenazar la seguridad pública.

EL 42 %

de las empresas han experimentado una violación directa en los últimos dos años.

EL 59 %

encuentra difícil el cumplimiento de las normas de seguridad.

Resumen ejecutivo: conocer los riesgos y desafíos del IoT

Para conocer detalladamente cómo las empresas se preparan para las amenazas actuales y emergentes contra la seguridad del IoT y cómo responden ante ellas, UL trabajó en conjunto con Bloomberg Next para llevar a cabo una encuesta entre los ejecutivos y gerentes sénior en sectores industriales clave, incluidos los sectores de venta minorista, fabricación y cuidado de la salud. La encuesta estuvo dirigida a los encargados de la toma de decisiones responsables de la coordinación, supervisión y administración de las prácticas e iniciativas de seguridad del IoT dentro de sus respectivas organizaciones.

El estudio abordó diversos temas:

1. Obtener acceso al alcance y a la profundidad globales de la habilitación del IoT en procesos, productos y servicios.
2. Conocer las actitudes en torno a la vulnerabilidad del IoT, las áreas de preocupación, la evaluación y la mitigación de los riesgos.
3. Determinar el grado de familiarización con las normas de seguridad y evaluar las variaciones en las dificultades de cumplimiento entre las industrias y regiones geográficas.

Los hallazgos revelan perspectivas renovadas sobre la forma en la que las organizaciones contemplan los riesgos de la seguridad del IoT y sobre los pasos que están tomando para abordar las vulnerabilidades, proteger los activos críticos y cumplir con requisitos normativos nuevos y emergentes. La amenaza de una intromisión en la red es una preocupación persistente entre los gerentes del IoT, y así debería ser.

Como las preocupaciones por la seguridad crecen en paralelo con la adopción del IoT, los hallazgos ponen de manifiesto las dificultades que enfrentan las empresas en sus esfuerzos por combatir amenazas crecientes. En otras áreas clave, la encuesta llegó a las siguientes conclusiones:

- La seguridad del IoT es una preocupación dominante en todos los sectores industriales, y el 49 % de las empresas indicaron que estaban “muy preocupadas” por la ciberseguridad en general.
- Aunque el estado de preparación en materia de seguridad sufre un desfase, la expansión global del IoT continúa. En Asia, crece cada vez más la necesidad de una mitigación de los riesgos de seguridad, debido al aumento rápido de implementaciones del IoT en la región.
- Las empresas que han experimentado una violación de la seguridad están tomando, o han tomado, más pasos para mitigar los riesgos en comparación con las que no han experimentado una violación.
- Las violaciones llevan a las empresas a cambiar su enfoque. Más precisamente, aprovechar los recursos externos es más común entre las empresas que han experimentado una violación.
- La mayoría de las organizaciones (59 %) encuentra difícil el cumplimiento de las normas de seguridad. Esta dificultad fue notablemente superior en Europa (71 %), en donde existe un nivel inferior de familiarización con los estándares de cumplimiento.
- Cuando se trata de implementar un nuevo plan de seguridad del IoT, el 52 % de las empresas tienen planificado trabajar con un tercero experto.

Cerca de la mitad

de las empresas encuestadas informaron que han experimentado una violación directa de la seguridad en los últimos dos años. Para las empresas de EE. UU., esta cifra fue notablemente mayor y alcanzó el 53 %.

Las implementaciones del IoT siguen creciendo

La rapidez de los avances en los sectores de fabricación, electrónica y TI están intensificando la demanda de productos y servicios con el IoT. Nuestra encuesta muestra que las empresas están implementando funciones del IoT en un rango de ecosistemas. Las redes de oficinas fueron el entorno de implementación más común (67 %), seguido por las instalaciones/los edificios (56 %), los productos y servicios (50 %), la automatización industrial y los controles automatizados (48 %) y los dispositivos y equipos de los empleados (47 %).

Principales entornos en los que las empresas usan el IoT.

67 %
Redes de oficinas

48 %
Control y automatización industriales

56 %
Instalaciones: Automatización de edificios, gestión energética (iluminación, climatización), acceso/seguridad de los visitantes

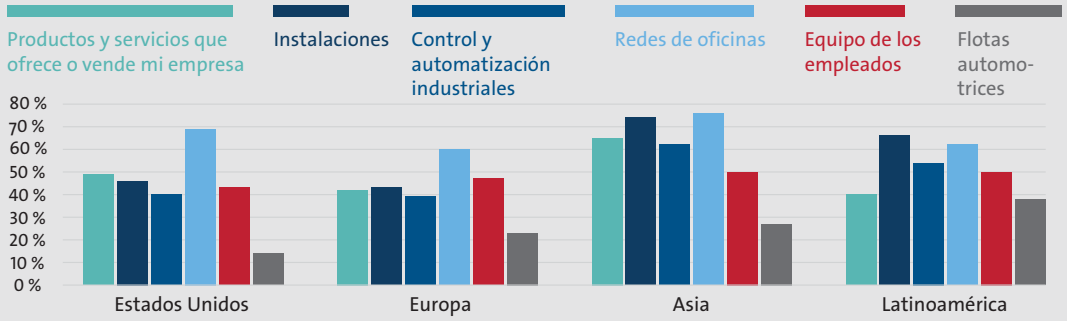
50 %
Productos y servicios que ofrece o vende mi empresa

47 %
Equipo de los empleados (p. ej., BYOD, «traiga su propio dispositivo»)

24 %
Flotas automotrices

Las empresas de Asia aprovechan un rango más amplio de los entornos habilitados para el IoT.

% de empresas en las que cada entorno está habilitado para el IoT

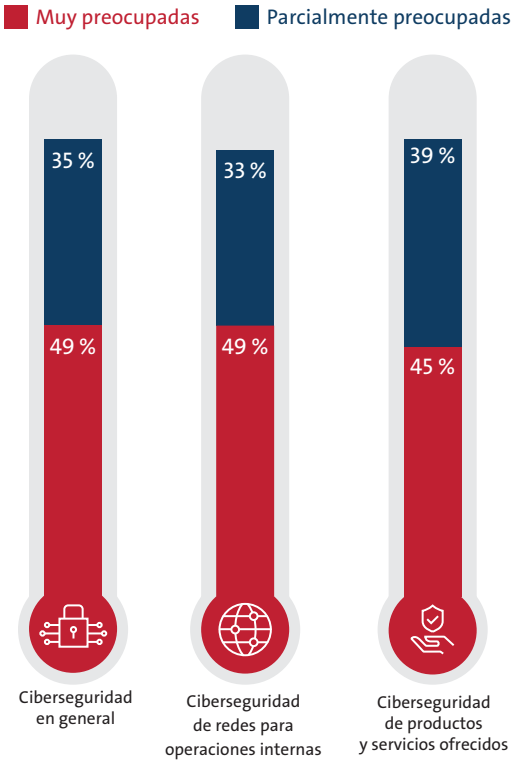


Estados Unidos tiene el mayor mercado para las implementaciones del IoT, seguido por Europa y Asia. En Asia, crece cada vez más la necesidad de una mitigación de los riesgos de ciberseguridad, debido al aumento rápido de las funciones habilitadas para el IoT y al rango mayor de estas funciones. Latinoamérica también espera un crecimiento sustancial, en particular en el mercado de las ciudades inteligentes, en donde se están implementando aplicaciones del IoT en entornos de servicios, transporte público y cuidado de la salud. Será importante supervisar esta región a medida que el mercado vaya madurando.

Preocupaciones que crecen al ritmo de la adopción del IoT

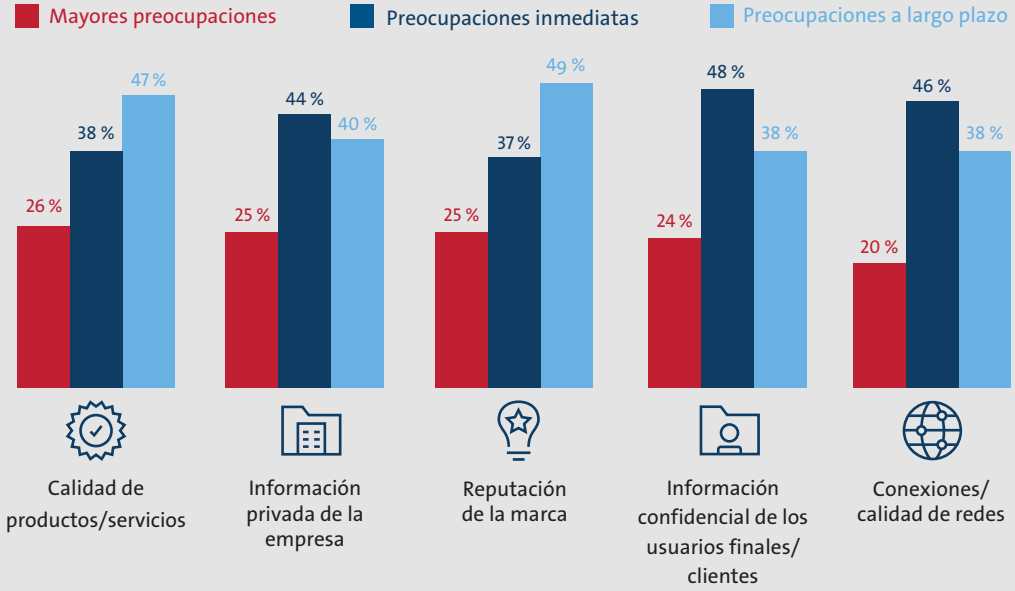
El riesgo de una violación de la seguridad es una preocupación dominante entre gerentes y ejecutivos empresariales, y cerca de la mitad de las empresas indicaron que estaban “muy preocupadas” por la ciberseguridad en general.

Las amenazas de seguridad crean niveles elevados de preocupación entre los ejecutivos de las empresas.



El deseo de respaldar y proteger el valor de la marca es evidente, ya que los problemas que experimentan los clientes impulsan la mayoría de las preocupaciones por la seguridad. Más precisamente, la calidad del producto, la confianza del usuario final y la reputación de la marca se encuentran entre las principales preocupaciones y suelen ser problemas a largo plazo. Los preocupaciones por la privacidad de la información del usuario final y la red en sí son más inmediatas.

Los problemas que experimentan los clientes impulsan la mayoría de las preocupaciones por la seguridad a largo plazo.



Las áreas de preocupación varían dentro de industrias específicas:

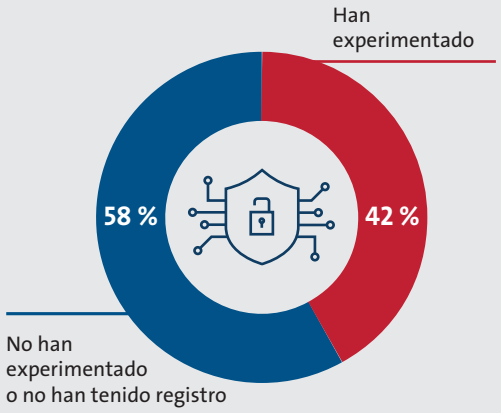
- En el sector del cuidado de la salud, la protección de la información confidencial del usuario final es una prioridad.
- En el sector de fabricación, la calidad y la conexión de la red son lo más importante.
- En el sector de venta minorista, la reputación de la marca y la confianza de los clientes son más importantes.

El peligro oculto de las intromisiones que no se detectan

Cada dispositivo nuevo con el IoT agrega otra ruta de ataque hacia los sistemas de TI, y basta con una sola vulnerabilidad en un solo dispositivo para amenazar todo un ecosistema. Nuestra encuesta muestra que el 42 % de las empresas han experimentado una violación directa en los últimos dos años, y esto las llevó a reforzar sus defensas.

Mientras que la cantidad de violaciones informadas resulta alarmante, quizás lo que resulta más inquietante es la incapacidad dominante entre muchas empresas para detectar una violación de datos en curso, lo que genera una falta de consciencia generalizada. De hecho, cerca de la mitad (48 %) de los negocios no son capaces de detectar las violaciones cuando ocurren, según un informe de investigación publicado por Gemalto, la empresa de seguridad digital.[2]

Casi la mitad de las empresas han experimentado una violación directa.



200 días

— la cantidad de tiempo promedio que se tarda en detectar una intromisión.[3]

Uno de los mayores desafíos es la gran cantidad de tiempo que suele llevar el descubrimiento de una violación, lo que puede elevar el perfil de riesgo de una empresa y crear suposiciones falsas en torno a la potencialidad del impacto y del alcance del peligro de la amenaza. De acuerdo con un informe de Verizon, el tiempo de espera (lo que se tarda en detectar una intromisión) alcanza un promedio de más de 200 días, a pesar de que solo lleva unos minutos poner en peligro datos sensibles.[3]

Si bien estos hallazgos tienen implicaciones convincentes, la pregunta más inmediata es la siguiente: del 55 % de las empresas de nuestro estudio que no han experimentado una violación, ¿cuántas han sufrido ya una intromisión pero aún no lo saben?

Los registros de actividad en la red son una de las fuentes más críticas para la detección de amenazas, pero las investigaciones muestran que solo el 21 % de las organizaciones están usando los datos de sus registros de manera efectiva.[4] No es común que estos registros se sometan a una revisión proactiva en busca de posibles casos de acceso no autorizado o incidentes de seguridad. Como resultado, la mayoría de las organizaciones no son conscientes de las estafas y los ataques que ocurren dentro de sus sistemas del IoT.

Cerca de la mitad

de los negocios no son capaces de detectar las violaciones cuando ocurren.[2]

Cómo prepararse para un ataque: de un estado de complacencia a un estado de preparación

Los riesgos que implican los dispositivos conectados son ampliamente dinámicos, ya que el IoT ya de por sí se está adaptando y expandiendo a un ritmo vertiginoso. Además, los atacantes tienen menos barreras para superar al intentar violar un dispositivo con el IoT. A diferencia de una computadora portátil o de escritorio, que suele estar equipada con software de seguridad y que goza del beneficio de actualizaciones de seguridad regulares, es posible que la única defensa de un dispositivo con el IoT sea un nombre de usuario y una contraseña predeterminados.

El IoT también genera datos con una amplia variedad de requisitos de seguridad. Algunos flujos de datos requieren un nivel mínimo de protección, mientras que otros pueden incluir información muy sensible, como datos financieros y aquellos que incluyen registros médicos confidenciales, y requerir medidas de seguridad más sólidas. La rapidez del crecimiento y de la maduración de los entornos del IoT trae aparejado el correspondiente interés en atacar los activos comerciales para obtener una ventaja financiera o simplemente desatar el caos y provocar una interrupción. Mientras que las empresas de todo el mundo se preocupan por las violaciones del IoT, los preparativos se retrasan, aunque el IoT se expanda.

Las empresas suelen subestimar la posibilidad de un desastre y no estar preparadas ni en lo más mínimo para las violaciones CUANDO suceden.

Las empresas que han experimentado una violación están tomando, o han tomado, más pasos para resolver preocupaciones por la ciberseguridad y, por lo tanto, están mejor preparadas.

Contratar a expertos externos para ayudar a controlar los procesos de seguridad del IoT es más común entre las empresas que han experimentado una violación.

Ataques al IoT: de lo potencial a lo real

Las industrias que respaldan las infraestructuras críticas son especialmente vulnerables a las violaciones de seguridad del IoT que pueden poner en peligro los datos sensibles e interrumpir las operaciones de misión crítica. Tan solo en los últimos años, ha habido una serie de ejemplos de alto perfil de cómo las vulnerabilidades de software pueden traer aparejadas consecuencias costosas y peligrosas.

En 2016, una violación cometida por la botnet Mirai infectó una serie de dispositivos con el IoT y luego los utilizó para dar inicio a un gran ataque de denegación de servicio distribuido (DDoS) en el proveedor de servicios de dominios Dyn.[5] El ataque deshabilitó una larga lista de sitios web, como los de Shopify, Netflix y Twitter. El incidente estableció un precedente peligroso por cómo los atacantes podrían "reclutar" dispositivos conectados y usarlos para fines maliciosos sin que los propietarios de estos dispositivos ni siquiera se enteraran.

En la conferencia sobre seguridad de DEF CON de 2016, las cerraduras para puertas, los termostatos, los refrigeradores y las sillas de ruedas figuraban entre los dispositivos con el IoT que fueron víctimas de hackers durante una serie de demostraciones.[6] Los tipos de vulnerabilidades identificadas durante el evento incluyeron diversos factores, desde malas decisiones de diseño hasta fallas en la codificación. En total, se dieron a conocer 47 vulnerabilidades que afectaron 23 elementos habilitados para el IoT de 21 fabricantes.

En marzo de 2017, WikiLeaks reveló que la CIA contaba con herramientas para hackear dispositivos con el IoT, como televisores inteligentes, para grabar de forma remota conversaciones en habitaciones de hoteles o salas de conferencias; esto abrió una caja de Pandora en cuanto a posibles problemas de privacidad.[7]

En mayo de 2017, el Servicio Nacional de Salud (NHS) del Reino Unido quedó vulnerable al virus WannaCry, que deshabilitó los sistemas de TI de varias de las organizaciones del NHS, incluidas unas 30 fundaciones hospitalarias y 70.000 dispositivos del NHS. Por este malware de cifrado de archivos, muchas de las oficinas del NHS fueron bloqueadas de los sistemas y tuvieron que utilizar lápiz y papel y cancelar miles de operaciones y consultas.[8]

La investigación muestra que se requiere de experiencia personal para impulsar la toma de medidas. Más precisamente, las empresas que han experimentado una violación de la seguridad están tomando, o han tomado, más pasos para mitigar los riesgos en comparación con las que no han experimentado una violación.

Las violaciones también llevan a las empresas a cambiar su enfoque. Más precisamente, aprovechar los recursos externos es más común entre las empresas que han experimentado una violación.

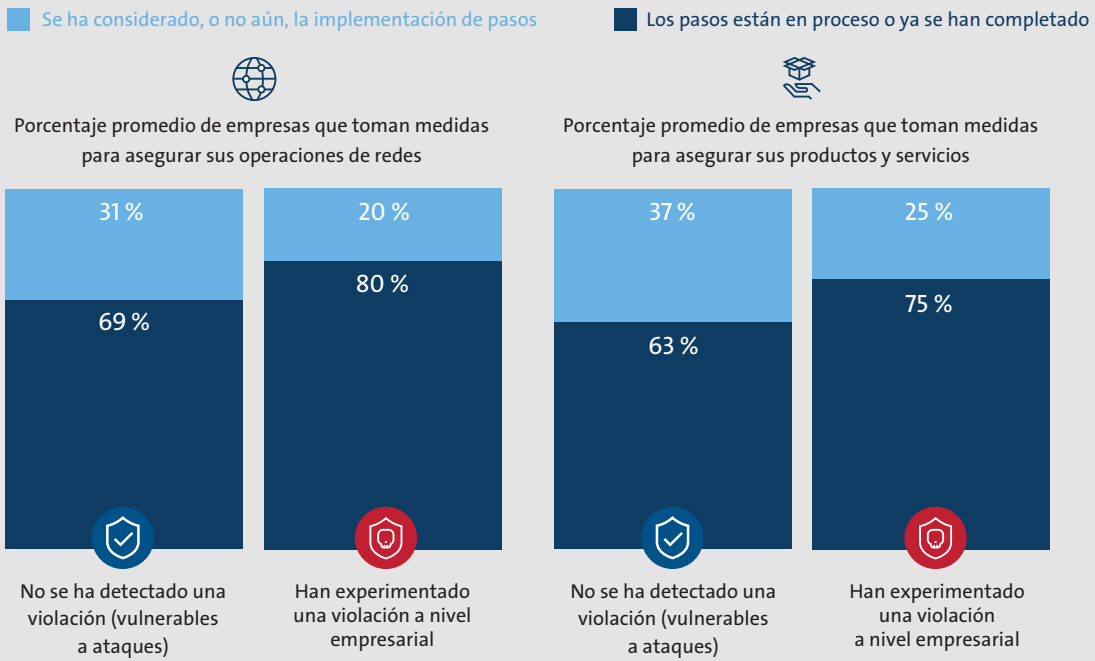
EL 73 %

de las empresas que han experimentado una violación han contratado a recursos externos.

Solo el 14 %

de las empresas han establecido un proceso formal de auditoría para saber si sus dispositivos son seguros y para saber cuántos dispositivos tienen.[10]

Pasos tomados para mitigar los riesgos cuando se trata de operaciones de red vs. productos y servicios.



La experiencia personal le gana a la complacencia

La falta de acciones proactivas es un comportamiento humano común que se caracteriza por el sesgo de la normalidad, es decir, las personas naturalmente subestiman la posibilidad de un desastre y su impacto potencial. Por este mismo motivo, las personas que viven en una zona proclive a las inundaciones por lo general se rehusarán a contratar un seguro contra inundaciones. De hecho, según informes, cerca del 70 % de las personas evidencian el sesgo de la normalidad ante un desastre.[9]

Las personas suelen asumir que, solo porque nunca han experimentado personalmente un desastre, nunca pasará nada malo. En términos de ciberseguridad, esto con frecuencia genera situaciones en las que las personas no se preparan bien para la posibilidad de ser víctimas de una violación de datos, o ni siquiera consideran esta posibilidad.

Cómo abordar las debilidades ocultas

Los desarrolladores de dispositivos abordan proactivamente las vulnerabilidades de seguridad, pero persisten las preocupaciones. Para las empresas de diversas industrias, una de las causas más dañinas, pero con frecuencia menos identificadas, de las violaciones de ciberseguridad se encuentra en el software de terceros comprado o descargado para su uso en operaciones y sistemas internos o para su integración a bienes terminados.

Desafortunadamente, mientras que los componentes de software de terceros pueden ayudar a incrementar la productividad de desarrollo e incluso mejorar la calidad del producto, su uso cada vez mayor también ha generado nuevos riesgos de ciberseguridad, lo que deja a las industrias de infraestructuras críticas incluso más vulnerables a los ciberataques.

Sin la implementación de procedimientos y sistemas adecuados para evaluar y controlar los componentes y el software de terceros que provienen de la cadena de suministro de software, las organizaciones pueden ignorar que usan o integran software a sistemas de operaciones o productos finales sin un nivel de seguridad lo suficientemente sólido, que puede hackearse con facilidad o correr otro tipo de peligros.

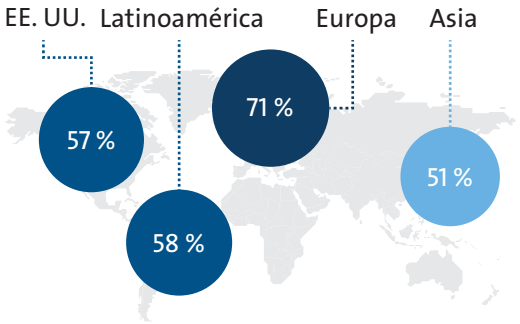
Para las organizaciones de las industrias de infraestructuras críticas, estos factores de riesgo, entre otros, acentúan la importancia de evaluar las vulnerabilidades de la cadena de suministro de software y desarrollar e implementar programas capaces de ayudar a reducir los riesgos relacionados con el software de terceros.

Estándares normativos: en busca de claridad en un mar de complejidades

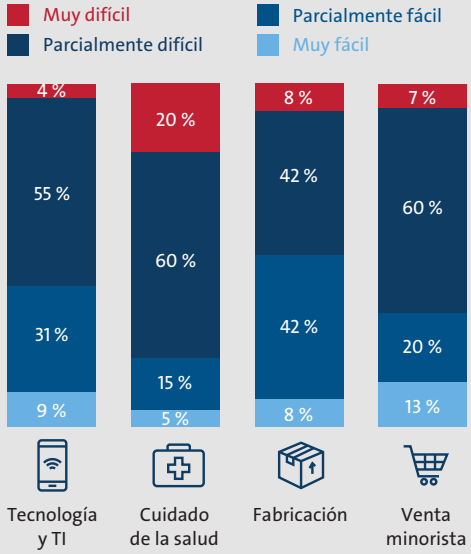
La guía de los gobiernos y sus correspondientes asambleas legislativas pueden ayudar a crear una infraestructura y un ecosistema seguros del IoT. Sin embargo, si bien los estándares de seguridad del IoT son bien recibidos y muy necesarios, el cumplimiento puede ser un desafío.

En nuestra encuesta, la mayoría de las organizaciones (59 %) encuentra difícil el cumplimiento de las normas de seguridad. La dificultad de cumplimiento fue notablemente superior en Europa (71 %), en donde existe un nivel inferior de familiarización con los estándares de cumplimiento: solo el 39 % (muy familiarizados) versus el 66 % en los Estados Unidos.

Porcentaje de empresas para las que el cumplimiento de las normas resulta un desafío.



La percepción del nivel de dificultad del cumplimiento varía dentro de los sectores industriales.



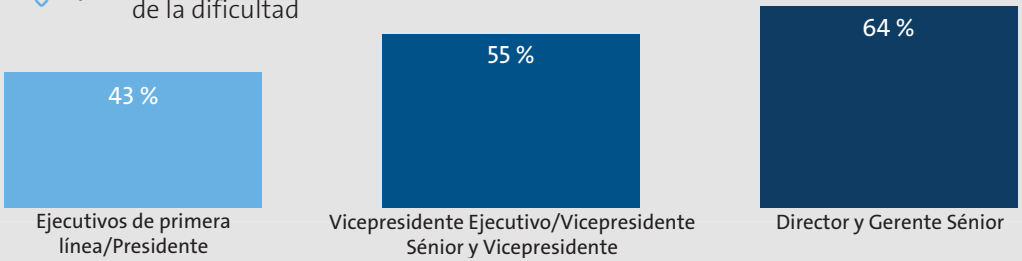
El porcentaje de las empresas que consideran difícil el cumplimiento fue notablemente superior en los sectores del cuidado de la salud y venta minorista, 80 % y 67 % respectivamente. El sector de fabricación considera más fácil el cumplimiento en comparación con otras industrias, ya que solo la mitad indicó que le parecía difícil.

La función también tiene un impacto en la percepción de la dificultad. Esto quiere decir que, cuanto más cerca se encuentra uno del proceso de cumplimiento (tácticas e implementación), más desafiante resulta.

Solo cerca de la mitad están "muy familiarizados" con los estándares de su país para el aseguramiento de los dispositivos conectados. Un nivel de familiarización ligeramente superior con los estándares industriales por sobre los nacionales implicaría que los primeros tienen prioridad.

La percepción del nivel de dificultad varía entre las funciones gerenciales.

Cuanto más se acerca un gerente a lidiar con las tácticas y la implementación de cumplimiento (directores vs. ejecutivos de primera línea), mayor es la percepción de la dificultad



Cómo combatir el aumento de ataques automatizados

El aumento de las botnets y otros ataques automatizados y distribuidos genera una amenaza que va más allá de cualquier empresa o sector individual. A medida que crece la economía conectada, también crece la posibilidad de que estos tipos de ataques generen una variedad de riesgos digitales.

Para abordar estos riesgos, el gobierno de EE. UU. está trabajando con las partes interesadas en un conjunto de objetivos y medidas diseñados para aumentar la resiliencia del ecosistema. A modo de infraestructura de guía, el Departamento de Comercio y el Departamento de Seguridad Nacional de EE. UU. han publicado un informe diseñado para promover la toma de medidas contra estas amenazas. El informe, "Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats" (Cómo mejorar la resiliencia del ecosistema de Internet y comunicaciones frente a las botnets y otras amenazas automatizadas y distribuidas), se ha publicado en respuesta a un Decreto ejecutivo de mayo de 2017 sobre el refuerzo de la ciberseguridad de las redes federales y la infraestructura crítica.[11]

Como parte de un esfuerzo del sector privado, el Council to Secure the Digital Economy (CSDE) ha publicado su International Anti-Botnet Guide de 2018, que ofrece una serie de prácticas voluntarias de referencia, además de capacidades avanzadas. En respuesta a sus preocupaciones por demasiadas normas, el CSDE informó que "las soluciones dinámicas y flexibles que se brindan a través de normas de consenso voluntario, impulsadas por las demandas del mercado e implementadas por las partes interesadas, son la mejor respuesta a estos desafíos sistémicos cambiantes".[12]

Los estándares de seguridad ayudan a darle forma al futuro del IoT

Para equilibrar las mayores preocupaciones y desafíos de seguridad del IoT con el ritmo vertiginoso de la innovación, UL ha desarrollado un Programa de Garantía de Ciberseguridad (CAP) de acuerdo con su nueva serie UL 2900 de estándares. El CAP pretende ofrecer un conjunto de requisitos que los fabricantes de productos conectables en red pueden usar voluntariamente para establecer una base de protección contra vulnerabilidades y debilidades de software.

UL también está liderando y contribuyendo con el desarrollo de una serie de estándares y programas emergentes para el control de riesgos/ciberseguridad, entre los que se incluyen los siguientes:

- Directrices ISO 18013 para el formato de diseño y el contenido de datos de una licencia de manejo conforme a las normas ISO (IDL) para las funciones visuales legibles para humanos y las tecnologías legibles para máquinas de conformidad con las normas ISO.
- Estándares de seguridad informática FIPS 140 del gobierno de EE. UU. que especifican los requisitos para módulos de criptografía que incluyen componentes de hardware y software.
- Recomendaciones de ciberseguridad ISO 2434 para movilidad (incluidos vehículos conectados y autónomos).
- UL 5500 Estándar de UL que cubre las actualizaciones de software remotas, además de la compatibilidad de hardware necesaria para la seguridad de la actualización de software remota.

Si bien no existe una solución mágica para las necesidades de seguridad de los fabricantes, estas directrices y recomendaciones están diseñadas para ir cambiando e incorporando criterios técnicos adicionales a medida que se vayan modificando las necesidades de seguridad en el mercado.

Los gastos en la seguridad del IoT ganan impulso

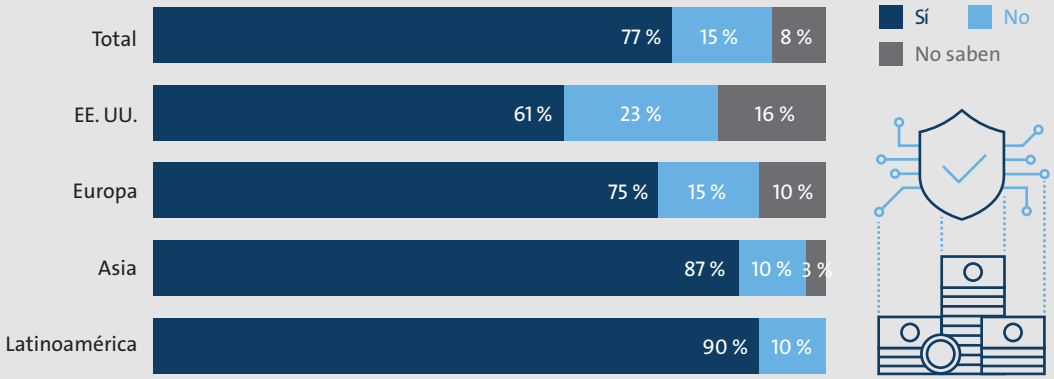
Las organizaciones de diversos sectores industriales se están percatando rápidamente de que la seguridad del IoT no es algo que pueda ignorarse o pasarse por alto. Para las organizaciones, cada dispositivo conectado nuevo representa otro canal proclive a los ataques, y basta con un solo dispositivo para corromper un ecosistema entero y desatar el caos de las operaciones comerciales.

Para capitalizar en su totalidad los inmensos beneficios del IoT, las organizaciones primero deben establecer una base de seguridad sólida. Las inversiones inteligentes y estratégicas en la seguridad del IoT tendrán un papel fundamental en este esfuerzo.

Nuestra encuesta muestra que las empresas siguen invirtiendo en la seguridad del IoT. De hecho, la mayoría de las empresas (77 %) tienen planificado aumentar los gastos en la seguridad del IoT durante los próximos cinco años. La probabilidad de aumentar los gastos fue notablemente superior por parte de los encuestados de las regiones de Asia y Latinoamérica, 87 % y 90 % respectivamente.

El aumento de los gastos en la planificación de la ciberseguridad fue notablemente superior en los sectores del cuidado de la salud y venta minorista, 85 % y 83 % respectivamente.

Porcentaje que tiene planificado aumentar los gastos en la ciberseguridad del IoT durante los próximos 5 años.

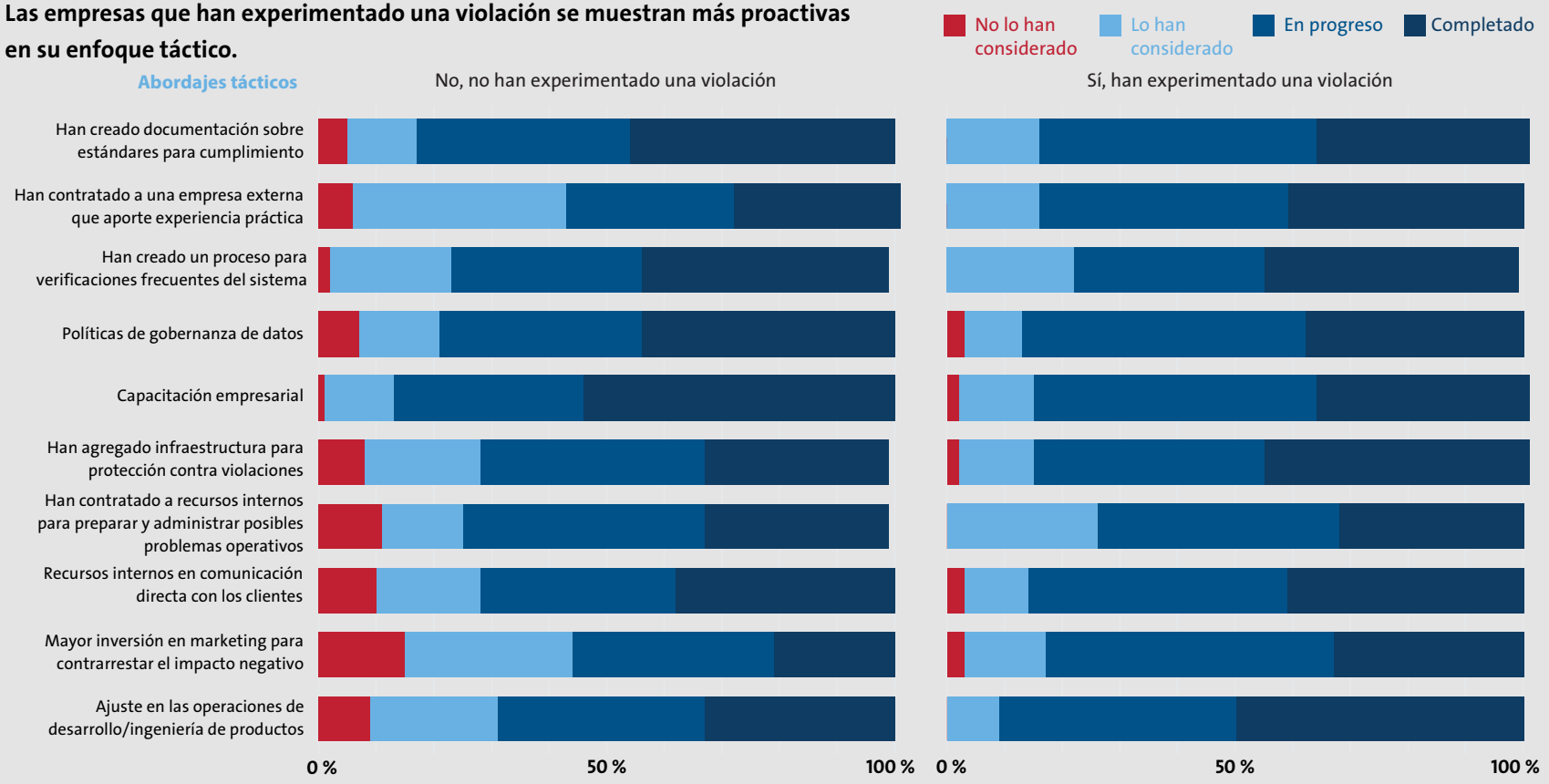


Los incidentes generan la toma de medidas

Las organizaciones están implementando una gama de tácticas para abordar las preocupaciones por la seguridad del IoT, con diferentes estrategias para aquellos que han experimentado una violación de seguridad y los que no. Para las empresas que han experimentado una violación, se informó que una gama de tácticas están en progreso o ya se completaron.

El potencial de las tecnologías con el IoT se ve reflejado en proyecciones de ingresos y de un crecimiento futuros en el mercado del IoT. De acuerdo con una estimación, el mercado global del IoT pasará de 157 mil millones USD en 2016 a **457 mil millones USD en 2020**, y alcanzará una tasa de crecimiento anual compuesto (CAGR) del 28,5 %.[13]

Las empresas que han experimentado una violación se muestran más proactivas en su enfoque táctico.

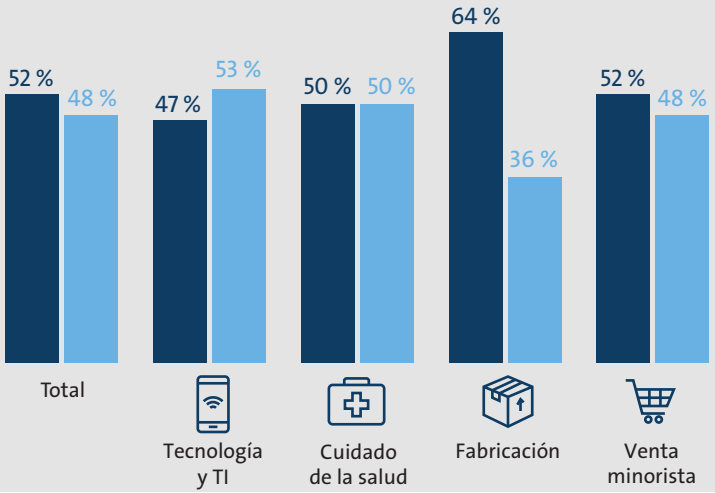


Cuando se trata de implementar un nuevo plan de seguridad del IoT, el 52 % de las empresas tienen planificado trabajar con un tercero experto. Esta cifra fue notablemente superior en el caso de los encuestados del sector de fabricación (64 %). Los principales motivos para considerar recurrir a un tercero experto fueron los siguientes: “un rango de experiencia más amplio” y “una simplificación del cumplimiento con las normas”.

Las empresas del sector de fabricación tienen más probabilidades de aprovechar los recursos externos.

Trabajan con un tercero experto para implementar estrategias de ciberseguridad en redes y productos/servicios relacionados con el IoT

Siguen un estándar o plan de desarrollo existente para redes y productos/servicios relacionados con el IoT



EL 89 %

de los encuestados tienen planificado introducir nuevos productos o servicios que aborden los riesgos dentro de los próximos 5 años. El 62 % indicó que está planificando hacerlo durante el próximo año.

EL 19 %

de las empresas tienen planificado invertir más de 100 millones USD durante los próximos cinco años en el aseguramiento de productos y servicios con el IoT. El 40 % tenía planificado invertir entre 20 y 100 millones USD.

EL 52 %

de las empresas tienen planificado trabajar con un tercero experto para implementar planes nuevos de seguridad del IoT. Los principales motivos para considerar recurrir a un tercero experto fueron los siguientes: “un rango de experiencia más amplio” y “una simplificación del cumplimiento con las normas”.

En busca de orientación sobre el cumplimiento con las normas

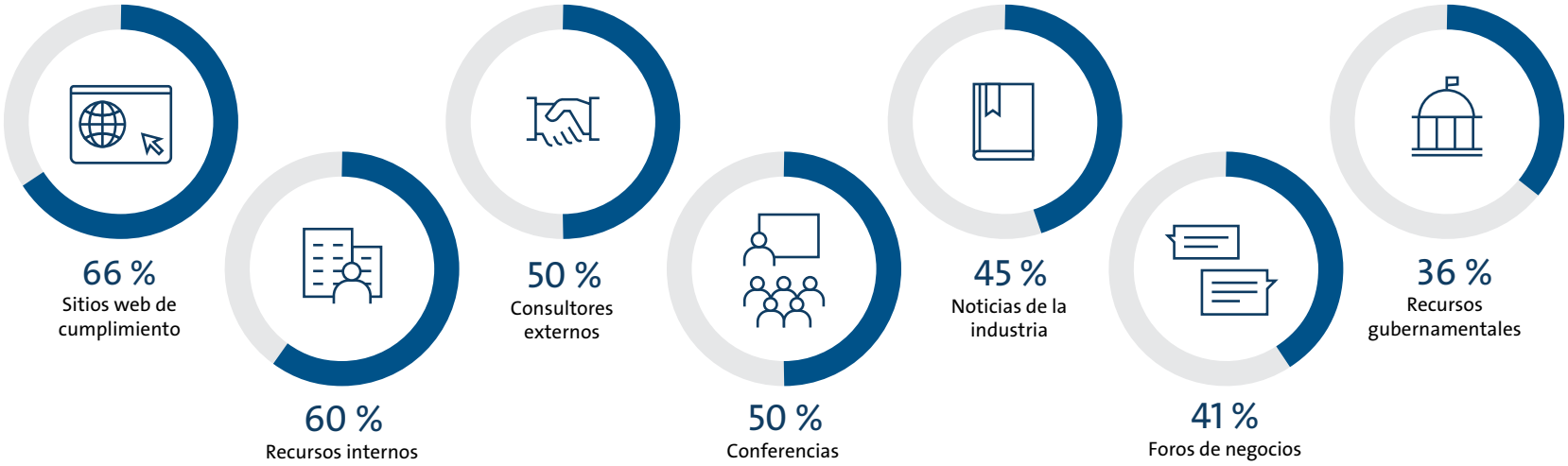
Para mantenerse informadas sobre el cambiante entorno regulatorio de hoy en día, las empresas confían en una combinación de recursos. Los sitios web sobre cumplimiento fueron los primeros de la lista, seguidos por los recursos internos y la experiencia externa.

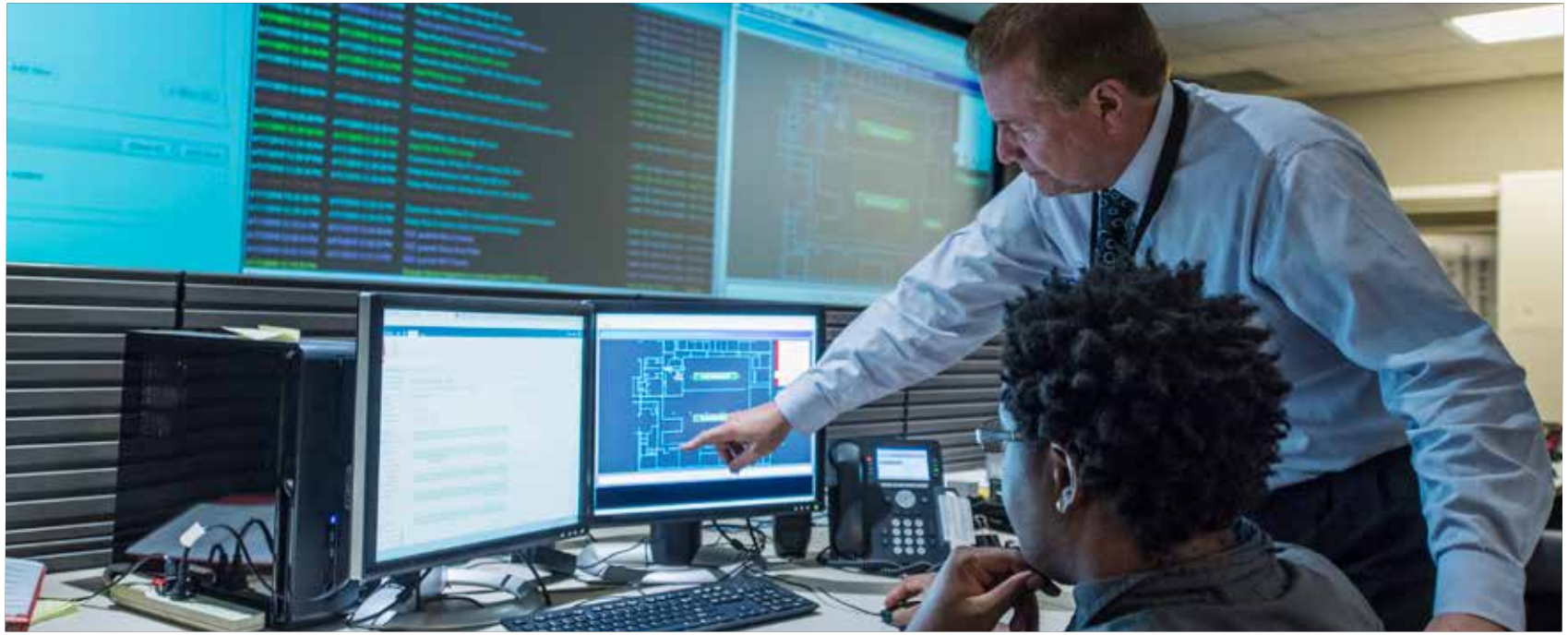
Los recursos gubernamentales fueron mencionados por los encuestados como la herramienta menos utilizada para la orientación y el respaldo en materia de cumplimiento. Si bien las empresas tienen planificado usar los recursos gubernamentales, la posición no preferencial que ocupan podría enfatizar una tendencia a priorizar los estándares de cumplimiento en la industria.

Según Gartner, los gastos en la seguridad del IoT alcanzarán los **840 mil millones USD** para el año 2020[14]. Al mismo tiempo, más del 25 % de los ataques identificados contra las empresas involucrarán sistemas con el IoT, lo que hará que las empresas quieran engrosar aún más sus presupuestos para la seguridad del IoT.

Las empresas utilizan una gama de herramientas de seguimiento del cumplimiento.

Recursos empleados actualmente para capacitaciones sobre cumplimiento





Seguridad efectiva: la piedra angular para el éxito del IoT

El IoT presenta un mundo de oportunidades y desafíos para los negocios de todas las industrias. Por un lado, ofrece una plataforma diversa y personalizada para la interacción con el cliente y la eficiencia operativa. Por otro lado, muchos elementos son muy complejos, y esto eleva el riesgo de alejar a los clientes cuando falla la protección. Encontrar ese equilibrio escurridizo entre la innovación y la protección será un factor de diferenciación importante para las marcas orientadas al cliente en los próximos años.

La seguridad es esencial para la operación segura y responsable de los dispositivos con el IoT. De hecho, es el factor constitutivo que posibilita el IoT. Como tal, es fundamental que las empresas establezcan estrategias de mitigación sólidas capaces de identificar efectivamente las amenazas e impedir los ataques a medida que surjan. Hasta que se implemente una protección adecuada, los dispositivos con el IoT seguirán sufriendo bajo el peso de las vulnerabilidades.

Si bien la creación de una infraestructura efectiva de seguridad del IoT es un proceso a largo plazo, las organizaciones no pueden darse el lujo de vacilar. Hoy en día se están formulando tácticas y estrategias, y las organizaciones previsoras ya están llevando sus planes a la acción para garantizar que sus ecosistemas con el IoT sean capaces de adoptar y respaldar con éxito la rápida escalada de las “cosas” conectadas.

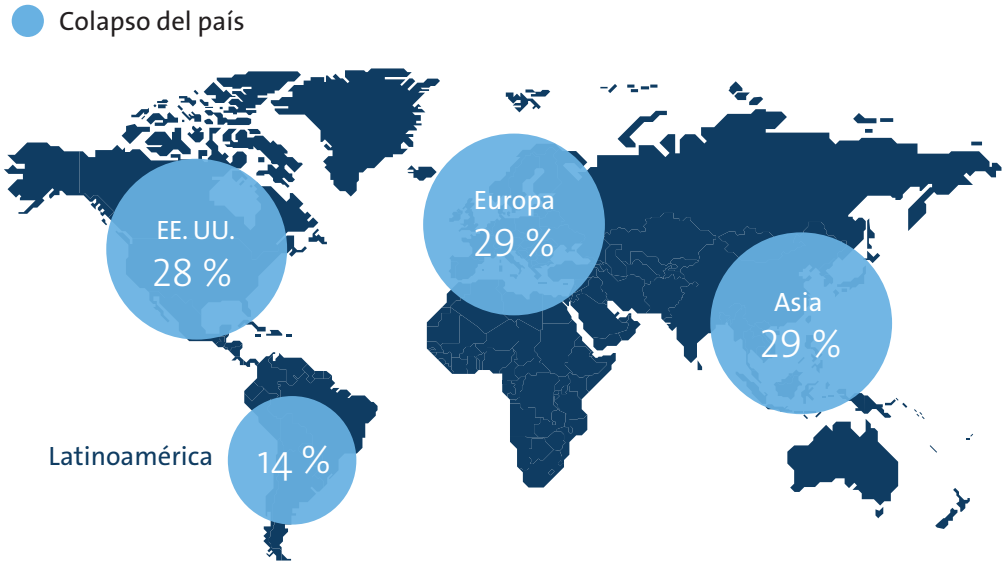
Acerca de UL

UL trabaja alrededor de todo el mundo para ayudar a clientes, compradores y formuladores de políticas a explorar los riesgos y las complejidades del mercado. UL habilita una seguridad de extremo a extremo confiable y vital, diseñada para nuestro mundo interconectado. Contamos con una experiencia única en el desarrollo de infraestructuras de seguridad y la estructuración de programas de seguridad para TI y ecosistemas interconectados. Logramos que las empresas puedan implementar innovaciones sin poner en riesgo la seguridad, ayudando a conservar la confianza del cliente y aumentando el acceso al mercado.

Como un socia y colaboradora de la industria de TI, UL pretende crear estándares y políticas que contribuirán a garantizar una adopción segura de nuevas tecnologías conectadas. UL está preparada para proveer servicios, soluciones y educación para ayudar a las empresas a fortalecer sus marcas. Lo invitamos a hacer uso de nuestra información de vanguardia y de nuestros expertos para posicionar su marca y así lograr un éxito sostenido a largo plazo.

Acerca del estudio

Los hallazgos de este informe se basan en una encuesta de 349 encuestados de los Estados Unidos, Europa, Asia y Latinoamérica. La encuesta estuvo dirigida a los gerentes sénior, los directores y los encargados de la toma de decisiones, y sus superiores, que son responsables de la coordinación y administración de las prácticas e iniciativas de seguridad del IoT dentro de sus respectivas organizaciones.



Para obtener más información, visite UL.com/insights.

Fuentes

1. “The Internet of Things: A movement, Not a Market,” IHS Markit, octubre de 2017
2. “State of IoT Security, informe de investigación,” Gemalto, 2017
3. “Tales of Dirty Deeds and Unscrupulous Activities,” 2018 Data Breach Investigations Report (DBIR), Verizon, 2018
4. “Why Security Breaches Go Unnoticed for Months,” 451 Research, junio de 2017
5. “DDoS attack that disrupted internet was largest of its kind in history, experts say,” The Guardian, 2016
6. “Hackers found 47 new vulnerabilities in 23 IoT devices at DEF CON,” IT World, 2016
7. “WikiLeaks discloses details of CIA hacking IoT, mobile devices,” Internet of Business, 2016
8. “Worldwide ransomware hack hits hospitals, phone companies,” CNET, mayo de 2017
9. “The frozen calm of normalcy bias,” Gizmodo, recuperado, mayo de 2017
10. “Second Cybersecurity Insights Report, Exploring IoT Security,” AT&T, 2016
11. “Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats” — un informe para el Presidente, el Secretario de Comercio y el Secretario de Seguridad Nacional de EE. UU., mayo de 2018
12. “International Anti-Botnet Guide,” the Council to Secure the Digital Economy (CSDE), 2018
13. “Market Pulse Report, Internet of Things (IoT),” GrowthEnabler, 2017
14. “Forecast: IoT Security, Worldwide,” Gartner, 2016.

UL.com