Cerrando la Brecha de Seguridad de TI con Automatización y AI en la Era de IoT: Global

Patrocinado por Aruba, una compañía de Hewlett Packard Enterprise

Llevado a cabo independientemente por Ponemon Institute LLC

Fecha de Publicación: Septiembre 2018

Cerrando la Brecha de Seguridad de TI con Automatización y AI en la Era de IoT: Global

Preparado por Ponemon Institute, Septiembre 2018

Parte 1. Introducción

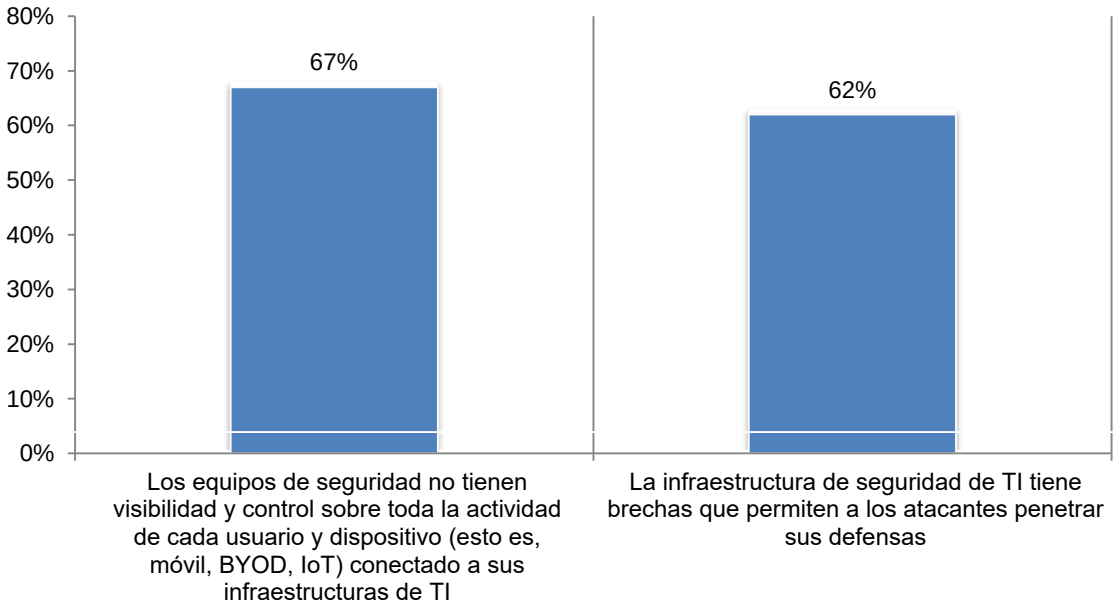
El propósito de esta investigación, patrocinada por Aruba, es entender los motivos de la peligrosa brecha en los modernos programas y estrategias de seguridad de TI, una brecha que está disminuyendo la capacidad de las organizaciones para identificar, detectar, contener y resolver violaciones de datos y otros incidentes de seguridad. Las consecuencias de la brecha pueden incluir pérdidas financieras, disminución en la reputación y la incapacidad de cumplir con regulaciones de privacidad, como la Regulación General de Protección de Datos (General Data Protection Regulation - GDPR) de la Unión Europea.

Ponemon Institute encuestó a 3,866 practicantes de TI y de seguridad de TI en las siguientes tres regiones y ocho países: Asia Pacífico, Europa el Medio Oriente y Asia (EMEA), América del Norte, Australia, Brasil, Alemania, India, Japón, México, Singapur y el Reino Unido. En este reporte, proporcionamos los hallazgos globales.

La brecha de seguridad de TI permite que los atacantes penetren las defensas de las compañías. En el contexto de esta investigación, la brecha de seguridad de TI se define como la incapacidad de las personas, procesos y tecnologías de una organización de mantenerse al día con un panorama de amenaces constantemente cambiante. Como se muestra en la Figura 1, 62 por ciento de los encuestados creen que esta brecha en la infraestructura de TI hace que sea más fácil que los atacantes penetren las defensas de las compañías. La brecha es causada por una falta de visibilidad y control sobre toda la actividad de cada usuario y dispositivo (esto es, móvil, BYOD, IoT) conectado a la infraestructura de TI de sus organizaciones, de acuerdo con el 67 por ciento de los encuestados.

Figura 1. Consecuencias de una brecha de seguridad de TI

Respuestas Totalmente de Acuerdo y de Acuerdo combinadas



Los siguientes hallazgos ilustran los motivos por los cuales se provoca la brecha de seguridad de TI y los problemas creados por ésta.

La expansión y la difuminación del perímetro de TI es el motivo principal por el cual las compañías tienen una brecha de seguridad de TI. Cincuenta y cinco por ciento de los encuestados dicen que es difícil proteger al perímetro de TI en expansión y está difuminado a la luz de IoT, BYOD, movilidad y la nube. Otros motivos por la brecha de seguridad de TI son la escasez en personal calificado y la falta de visibilidad de lo que cada usuario y dispositivo está haciendo mientras se encuentra conectado a la infraestructura de TI (ambos 49 por ciento de encuestados).

Usuarios legítimos comprometidos se consideran el mayor riesgo. Usuarios comprometidos y negligentes que tienen acceso legítimo adentro de la organización presentan la mayor amenaza.

La brecha de seguridad de TI deja a la infraestructura de TI vulnerable a ataques. Sólo el 38 por ciento de los encuestados están confiados que los ataques adentro de la infraestructura de TI se pueden detectar antes de que causen una violación de seguridad cibernética, resultando en robo, modificación o visualización de datos por entidades no autorizadas. Cincuenta y uno por ciento de los encuestados dicen que los ataques que han llegado adentro de la red tienen el potencial de provocar el daño más grande.

A pesar de todas las inversiones en programas de seguridad cibernética, las violaciones aún continúan ocurriendo. Como resultado de la brecha de seguridad de TI, las compañías no son capaces de detener muchas violaciones de datos. Casi la mitad (49 por ciento de los encuestados) dicen que es difícil proteger superficies de ataque complejas y que cambian dinámicamente, como móvil, BYOD, la nube e IoT. Adicionalmente, 48 por ciento de los encuestados dicen que la falta de personal de seguridad con la experiencia necesaria es otro problema clave. Un tercer motivo es que los atacantes de la actualidad son persistentes, sofisticados, bien entrenados y bien financiados (46 por ciento de los encuestados).

La incapacidad de asegurar dispositivos y apps IoT es un impulsor primario atrás de la brecha de seguridad de TI. Sesenta y seis por ciento de los encuestados dicen que sus organizaciones no son capaces, o tienen poca capacidad, de asegurar sus dispositivos y apps IoT. Más de la mitad de los encuestados (51 por ciento) dicen que la visibilidad de IoT es importante para detectar ataques.

Para lograr un fuerte nivel de seguridad IoT, 52 por ciento de los encuestados dicen que se requiere el monitoreo continuo del tráfico de red para cada dispositivo IoT para detectar anomalías en forma temprana y lograr un fuerte nivel de seguridad. NAC también es importante para responder a riesgos de IoT, de acuerdo con 41 por ciento de los encuestados.

Por qué los dispositivos IoT están ampliando la brecha de seguridad de TI. Solamente el 23 por ciento de los encuestados creen que los dispositivos IoT que simplemente monitorean o efectúan tareas menores presentan poca amenaza a la seguridad general de sus organizaciones. Setenta y uno por ciento de los encuestados están de acuerdo de que las tecnologías IoT legadas son difíciles de asegurar. Como consecuencia, solamente el 24 por ciento de los encuestados dicen que los dispositivos IoT de sus organizaciones están asegurados apropiadamente con una estrategia de seguridad correcta implementada.

Los siguientes hallazgos describen las soluciones para cerrar la brecha de seguridad de TI.

Se requieren nuevas tecnologías para cerrar la brecha de seguridad de TI. Sesenta y cuatro por ciento de los encuestados dicen que nuevas tecnologías, como aprendizaje de máquina (machine learning - ML), se requieren para descubrir y entender amenazas que están activas en la infraestructura de TI. En la actualidad, solamente 45 por ciento de los encuestados dicen que

sus organizaciones están obteniendo el valor completo de sus inversiones de seguridad en curso. Pasos que los encuestados consideran importantes para minimizar los peligros de amenazas clandestinas y ocultas dentro de la infraestructura de TI incluyen el monitoreo de usuarios privilegiados (53 por ciento), sistemas SIEM (Security Information and Event Management) (47 por ciento) y Analíticos del Comportamiento de Usuarios y Entidades (40 por ciento), lo cual cada vez más se observa como una forma de monitorear activos de alto valor mientras se "turbocargan" instalaciones SIEM existentes.

La visibilidad de aplicaciones y de puntos terminales es crítica para detectar ataques desde adentro. Setenta y uno por ciento de los encuestados dicen que la visibilidad de las aplicaciones es crítica para detectar ataques y 69 por ciento de los encuestados consideran que la visibilidad de los puntos terminales es importante. También importante es la visibilidad del tráfico de nube y de la red (64 por ciento y 63 por ciento, respectivamente).

¿Es ML basado en AI bombo o realidad? Más de la mitad de los encuestados (51 por ciento) están de acuerdo que tecnologías de AI, como ML y analíticos de comportamiento, son esenciales para detectar ataques desde adentro antes de que causen daños. Los tres beneficios de seguridad más importantes de utilizar esas tecnologías son un aumento en efectividad de los equipos de seguridad, investigaciones más eficientes y la capacidad de encontrar amenazas clandestinas que hayan evadido las defensas de seguridad estándar (63 por ciento, 60 por ciento y 56 por ciento de los encuestados, respectivamente).

La mayoría de las organizaciones están planeando utilizar ML para propósitos de seguridad. En la actualidad, 29 por ciento de los encuestados dicen que ML se implementa extensamente a través de sus infraestructuras de TI (12 por ciento) o parcialmente (17 por ciento). Cuarenta y seis por ciento de los encuestados dicen que tendrán ML en los siguientes 12 meses (26 por ciento) o en más de un año (20 por ciento).

El aspecto más benéfico de la automatización es reducir la cantidad de tiempo y esfuerzo requeridos para investigar una alerta. Los encuestados creen que el beneficio más importante de la tecnología de automatización es la capacidad de reducir la cantidad de tiempo y esfuerzo requeridos para investigar una alerta (71 por ciento de los encuestados), seguido por una reducción del número de falsos positivos que los analistas deben investigar (68 por ciento de los encuestados).

Esto es especialmente importante para cumplir con la recientemente promulgada norma de privacidad GDPR de la Unión Europea. Un requerimiento clave es que, en el caso de una violación de datos personales, los controladores de datos deberán notificar a la autoridad supervisoria en un plazo no mayor a 72 horas. Dicha notificación debe incluir información detallada acerca de quiénes fueron afectados, el impacto general de la violación y las acciones adoptadas para remediar la violación.

NAC se considera importante para proporcionar visibilidad acerca de lo que se encuentra en las redes. Los encuestados creen que sus productos NAC proporcionan visibilidad acerca de lo que se encuentra en la red (53 por ciento) o que es un componente clave de su estrategia general de seguridad (52 por ciento). Sin embargo, más de la mitad (51 por ciento) dicen que los productos NAC son difíciles de configurar y de administrar.

Parte 2. Hallazgos clave

En esta sección del reporte, proporcionamos una visión más profunda de los hallazgos de la investigación. Los hallazgos auditados completos se presentan en el Apéndice de este reporte.

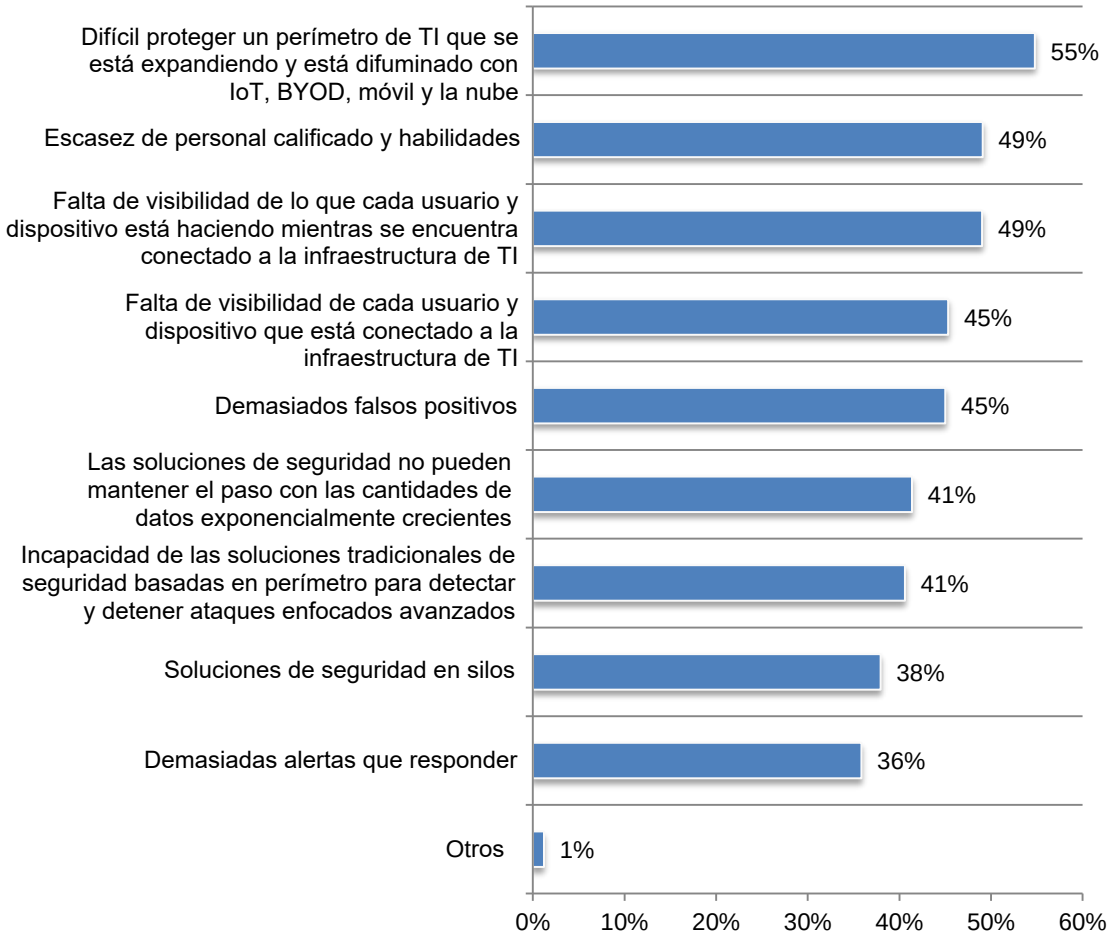
Hemos organizado los hallazgos de acuerdo con los siguientes temas:

- La brecha de seguridad de TI
- El riesgo de incumplimiento con GDPR y con otras regulaciones de privacidad
- ¿Está IoT ampliando la brecha de seguridad de TI?
- Soluciones para cerrar la brecha de seguridad de TI

La brecha de seguridad de TI

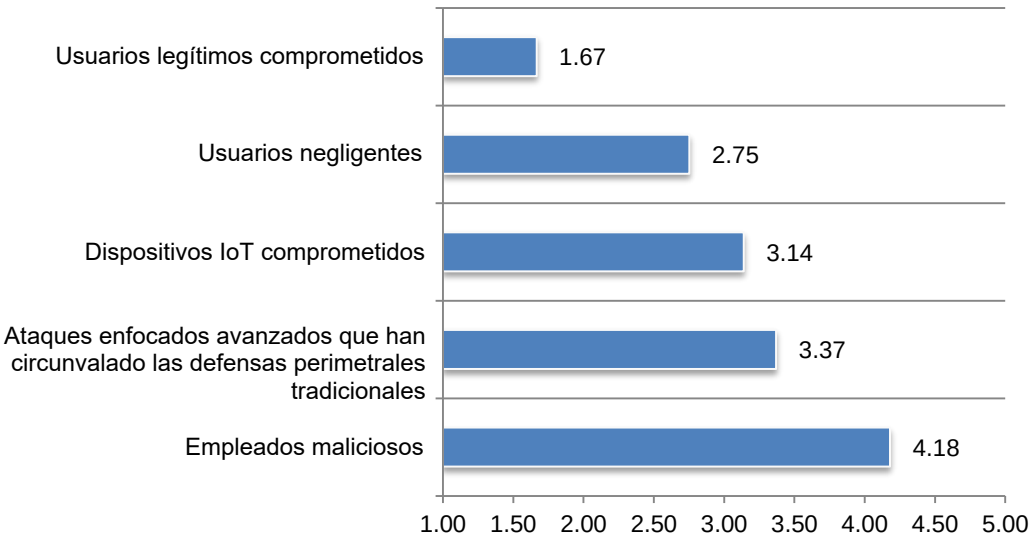
La expansión y la difuminación del perímetro de TI es el motivo principal por el cual las compañías tienen una brecha de seguridad de TI. De acuerdo con la Figura 2, 55 por ciento de los encuestados dicen que es difícil proteger un perímetro de TI que se está expandiendo y está difuminado con IoT, BYOD, móvil y la nube. Otros motivos por la brecha de seguridad de TI son la escasez en personal calificado y la falta de visibilidad de lo que cada usuario y dispositivo está haciendo mientras se encuentra conectado a la infraestructura de TI (ambos 49 por ciento de encuestados).

Figura 2. Por qué existe la brecha de seguridad de TI
Cuatro respuestas permitidas



Usuarios legítimos comprometidos se consideran el mayor riesgo. Se les preguntó a los encuestados que calificaran cinco factores que presentan la mayor amenaza interna desde 1 = mayor amenaza a 5 = menor amenaza. Como se muestra en la Figura 3, las personas que tienen acceso legítimo adentro de la organización presentan la mayor amenaza. Estos son usuarios legítimos comprometidos, así como usuarios negligentes. La incapacidad de ver y detectar dispositivos IoT comprometidos también está creando un riesgo significativo para las organizaciones.

Figura 3. ¿En dónde están las mayores amenazas desde adentro?
1 = mayor amenaza a 5 = menor amenaza



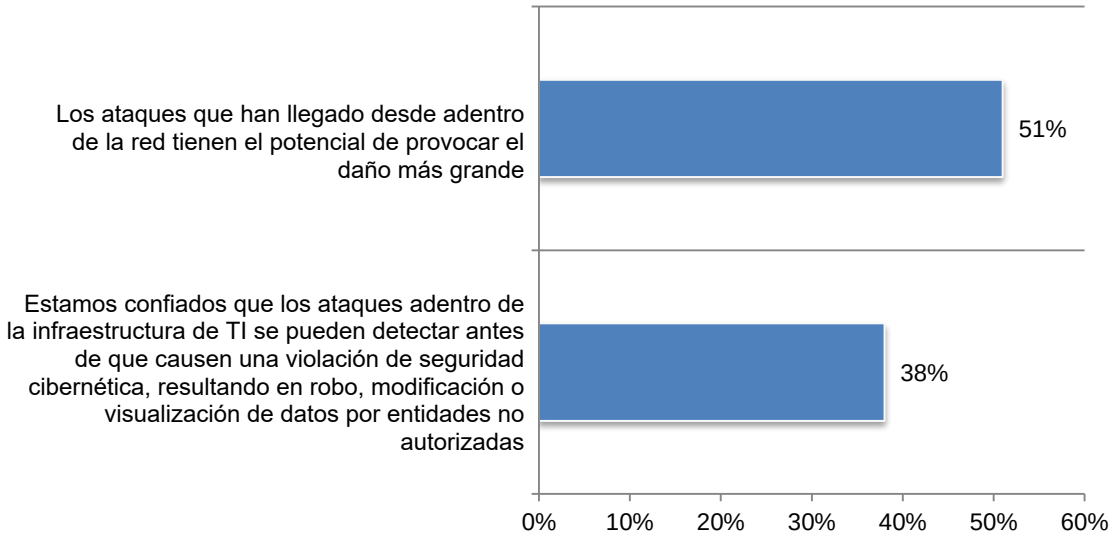
El riesgo de incumplimiento con GDPR y con otras regulaciones de privacidad

Las brechas de seguridad de TI exacerban el riesgo de incumplimiento con ciertas obligaciones de GDPR. De acuerdo con otro estudio reciente de Ponemon Institute, muchas empresas creen que sus organizaciones se encuentran en alto riesgo si no cumplen con obligaciones específicas de GDPR. Los participantes en este estudio creen que el mayor riesgo es por multas y acción regulatoria. Otros riesgos citados incluyen obligaciones de notificación, incluyendo operacionalizar el derecho de ser olvidado, llevando a cabo actividades de inventario de datos/mapeo de datos, obteniendo/administrando el consentimiento de usuarios y estableciendo un interés legítimo por el procesamiento de datos.

La brecha de seguridad de TI deja a la infraestructura de TI vulnerable a ataques. Como se muestra en la Figura 4, sólo el 38 por ciento de los encuestados están confiados que los ataques adentro de la infraestructura de TI se pueden detectar antes de que causen una violación de seguridad cibernética, resultando en robo, modificación o visualización de datos por entidades no autorizadas.

Cincuenta y uno por ciento de los encuestados dicen que los ataques que han llegado desde adentro de la red tienen el potencial de provocar el daño más grande. De acuerdo con el GDPR, en el caso de una violación de datos personales, los controladores de datos deberán notificar a las autoridades en un plazo no mayor a 72 horas. En el caso de que exista un retraso, las compañías deberán proporcionar una "justificación razonada."

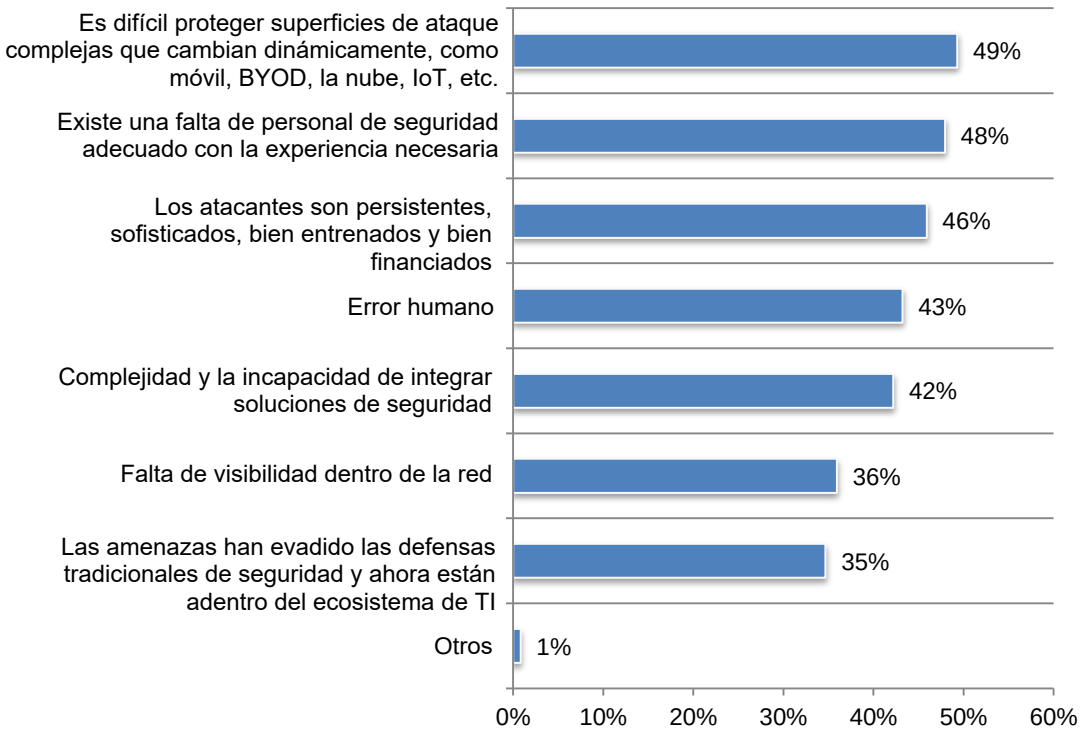
Figura 4. La brecha de seguridad de TI en la infraestructura de TI
Respuestas Totalmente de Acuerdo y de Acuerdo combinadas



[1] *The Race to GDPR: A Study of Companies in the United States & Europe,* efectuado por Ponemon Institute y patrocinado por McDermott, Will & Emery, LLP, Abril 2018

A pesar de todas las inversiones en programas de seguridad cibernética, las violaciones aún continúan ocurriendo. Como resultado de la brecha de seguridad de TI, las compañías no son capaces de detener todas las violaciones de datos. De acuerdo con la Figura 5, casi la mitad (49 por ciento de los encuestados) dicen que es difícil proteger superficies de ataque complejas que cambian dinámicamente, como móvil, BYOD, la nube e IoT y 48 por ciento dicen que existe una brecha en habilidades por la falta de personal de seguridad adecuado con la experiencia necesaria. Otro motivo es que los atacantes de la actualidad son persistentes, sofisticados, bien entrenados y bien financiados (46 por ciento).

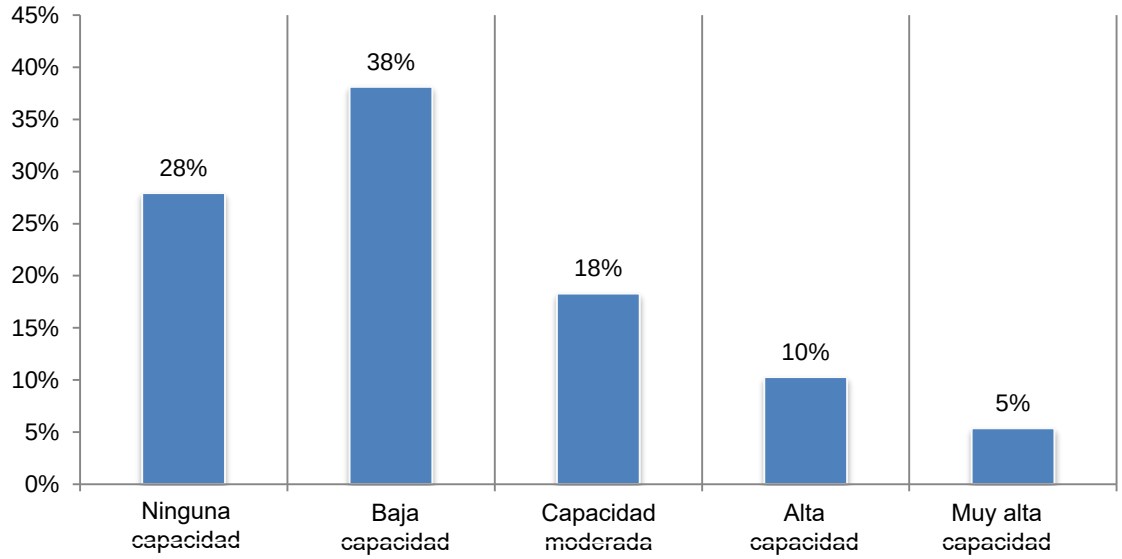
Figura 5. Por qué las violaciones de datos aún ocurren
Tres respuestas permitidas



¿Está IoT ampliando la brecha de seguridad de TI?

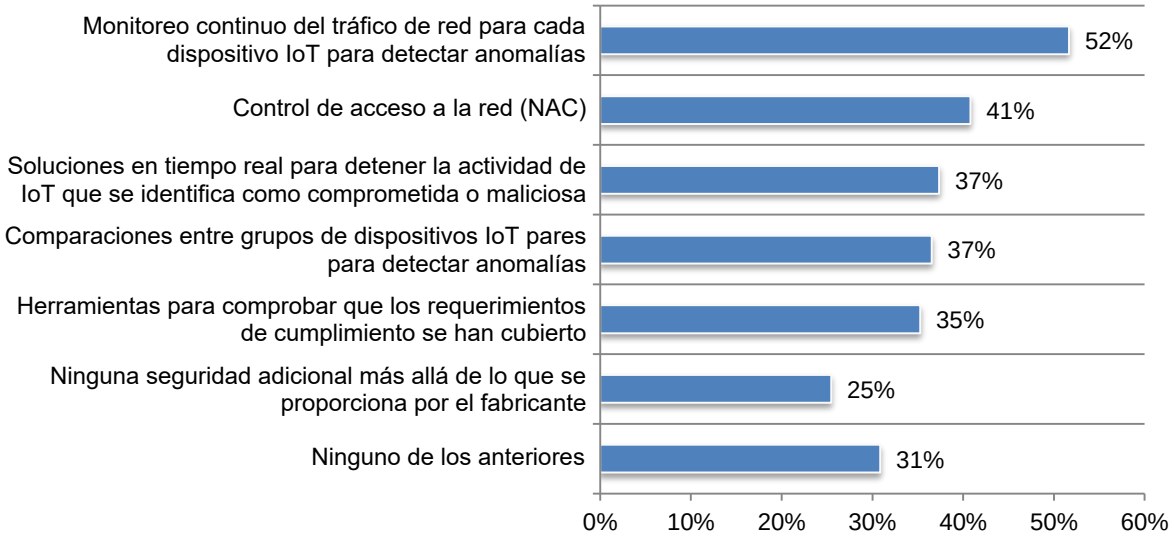
La incapacidad de asegurar dispositivos y apps IoT está exacerbando la brecha de seguridad de TI. Se les solicitó a los encuestados calificar la capacidad de sus organizaciones para asegurar dispositivos y apps IoT desde 1 = ninguna capacidad a 5 = muy alta capacidad. Como se muestra en la Figura 6, 66 por ciento de los encuestados dicen que su organización no tiene, o tiene una baja capacidad, de asegurar sus dispositivos y apps IoT. Más de la mitad de los encuestados (51 por ciento) dicen que la visibilidad de IoT es importante para detectar ataques.

Figura 6. La capacidad de asegurar dispositivos y apps IoT
1 = ninguna capacidad a 5 = muy alta capacidad



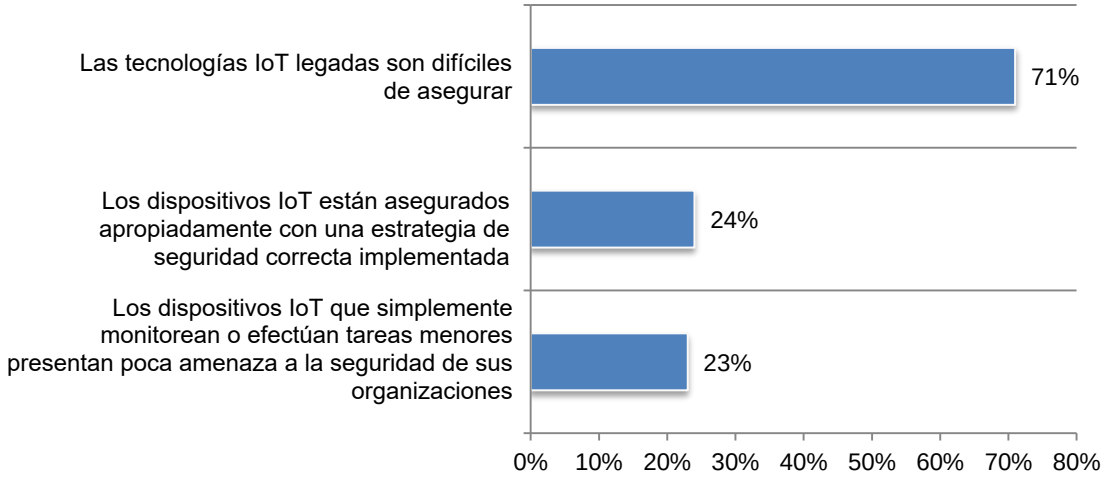
Como se muestra en la Figura 7, 52 por ciento de los encuestados dicen que se requiere el monitoreo continuo del tráfico de red para cada dispositivo IoT para detectar anomalías y lograr un fuerte nivel de seguridad. NAC también es importante para responder a riesgos de IoT de acuerdo con 41 por ciento de los encuestados.

Figura 7. Cómo lograr un fuerte nivel de seguridad IoT
Más de una respuesta permitida



Por qué los dispositivos IoT están ampliando la brecha de seguridad de TI. Como se describió en la Figura 8, el 23 por ciento de los encuestados creen que aun los dispositivos IoT que simplemente monitorean o efectúan tareas menores presentan poca amenaza a la seguridad de sus organizaciones. Setenta y uno por ciento de los encuestados están de acuerdo de que las tecnologías IoT legadas son difíciles de asegurar. Como consecuencia, solamente el 24 por ciento de los encuestados dicen que los dispositivos IoT de sus organizaciones están asegurados apropiadamente con una estrategia de seguridad correcta implementada.

Figura 8. Percepciones acerca de la seguridad
Respuestas Totalmente de Acuerdo y de Acuerdo combinadas

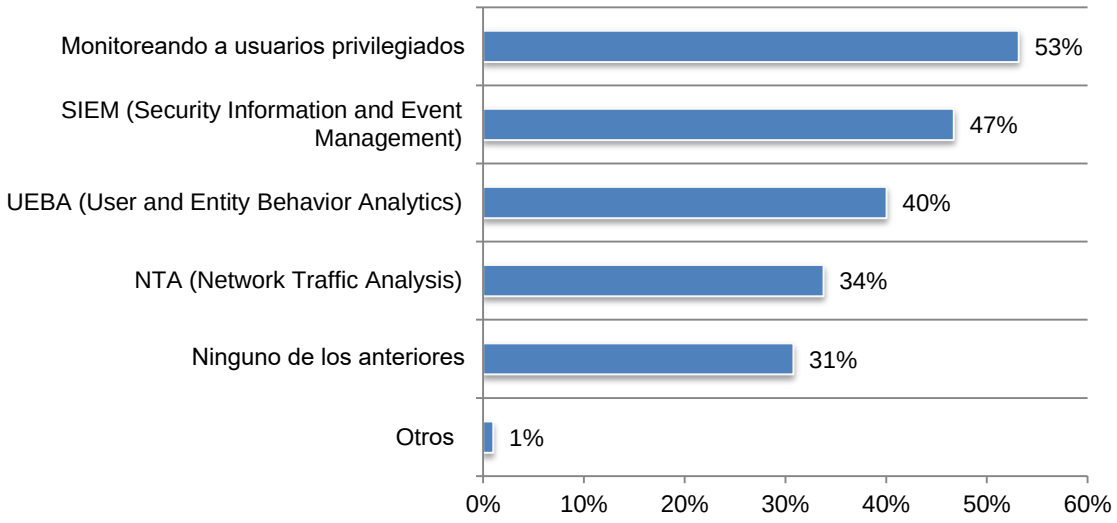


Soluciones para cerrar la brecha de seguridad de TI

Se requieren nuevas tecnologías para cerrar la brecha de seguridad de TI. Sesenta y cuatro por ciento de los encuestados dicen que nuevas tecnologías, como ML, se requieren para descubrir y entender amenazas que están activas en la infraestructura de TI. En la actualidad, solamente 45 por ciento de los encuestados dicen que sus organizaciones están obteniendo el valor completo de sus inversiones de seguridad en curso.

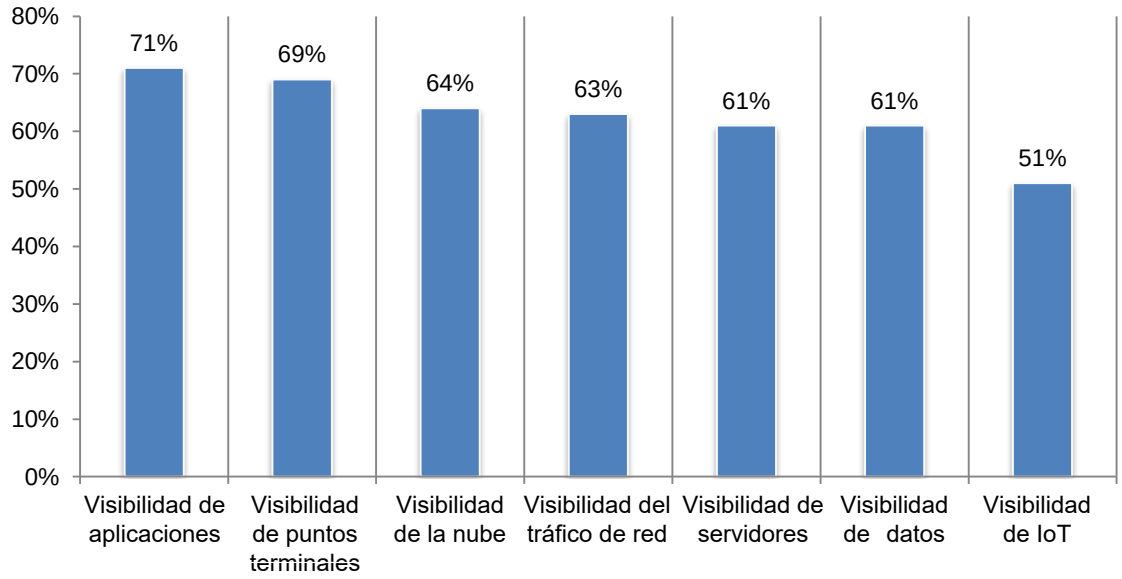
La Figura 9 describe pasos que los encuestados consideran importantes para minimizar los peligros de amenazas clandestinas y ocultas dentro de la infraestructura de TI e incluyen el monitoreo de usuarios privilegiados (53 por ciento), SIEM (47 por ciento) y Analíticos del Comportamiento de Usuarios y Entidades (40 por ciento), lo cual cada vez más se observa como una forma de monitorear activos de alto valor mientras se "turbocargan" instalaciones SIEM existentes.

Figura 9. Cuáles pasos pueden minimizar amenazas clandestinas y ocultas dentro de la infraestructura de TI
Más de una respuesta permitida



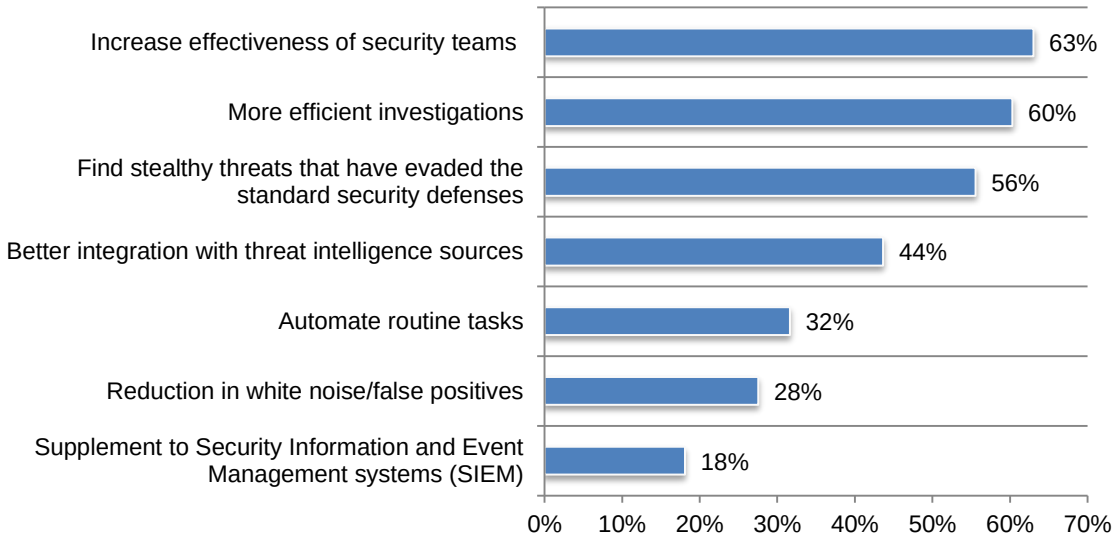
La visibilidad de aplicaciones y de puntos terminales es lo más importante para detectar ataques desde adentro. Se les solicitó a los encuestados calificar los diversos tipos de visibilidad en términos de detectar ataques de adentro desde 1 = no es importante a 5 = muy alta importancia. La Figura 10 muestra que 71 por ciento de los encuestados dicen que la visibilidad de las aplicaciones es crítica para detectar ataques y 69 por ciento de los encuestados consideran que la visibilidad de los puntos terminales es importante. También importante es la visibilidad del tráfico de nube y de la red (64 por ciento y 63 por ciento, respectivamente).

Figura 10. La importancia de la visibilidad en detectar ataques desde adentro
Muy Alta importancia y Alta importancia combinadas



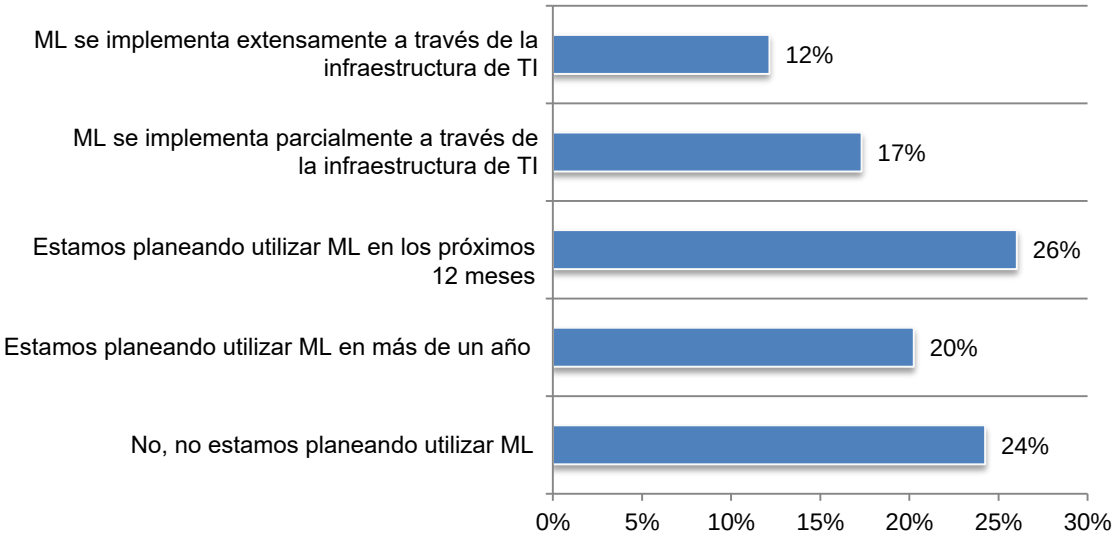
Es ML basado en AI ¿bombo o realidad? Más de la mitad de los encuestados (51 por ciento) están de acuerdo que tecnologías de AI, como ML y analíticos de comportamiento, son esenciales para detectar ataques desde adentro antes de que causen daños. Como se muestra en la Figura 11, los tres beneficios de seguridad más importantes de utilizar esas tecnologías son un aumento en efectividad de los equipos de seguridad, investigaciones más eficientes y la capacidad de encontrar amenazas clandestinas que hayan evadido las defensas de seguridad estándar (63 por ciento, 60 por ciento y 56 por ciento de los encuestados, respectivamente).

Figura 11. Los beneficios de seguridad más importantes de ML y de analíticos avanzados
Tres respuestas permitidas



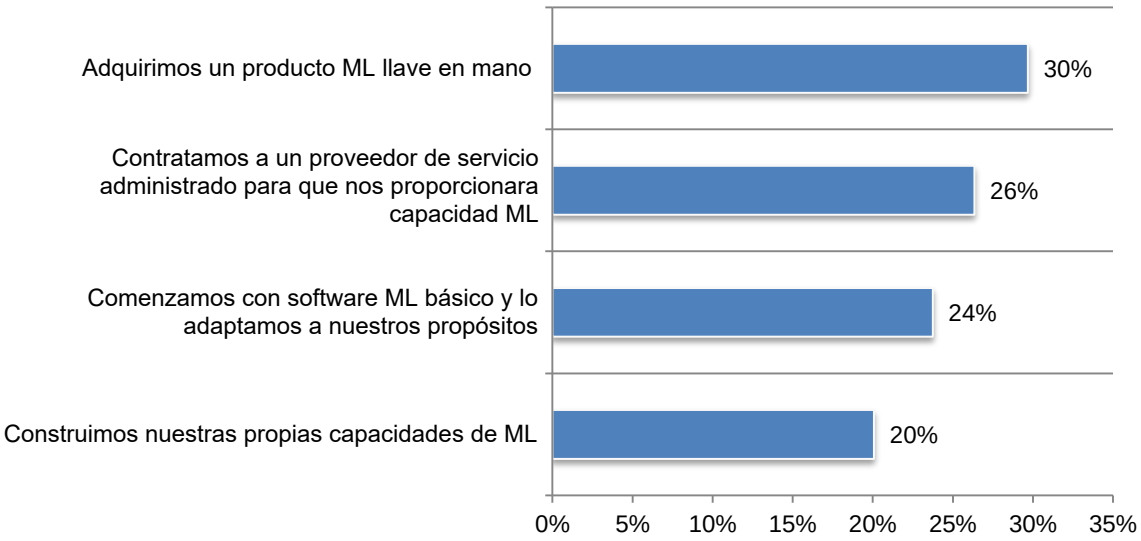
La mayoría de las organizaciones están planeando utilizar ML para propósitos de seguridad. Como se muestra en la Figura 12, en la actualidad, 29 por ciento de los encuestados dicen que ML se implementa extensamente a través de sus infraestructuras de TI (12 por ciento) o parcialmente (17 por ciento). Cuarenta y seis por ciento de los encuestados dicen que tendrán ML en los siguientes 12 meses (26 por ciento) o en más de un año (20 por ciento).

Figura 12. Cómo se utiliza ML



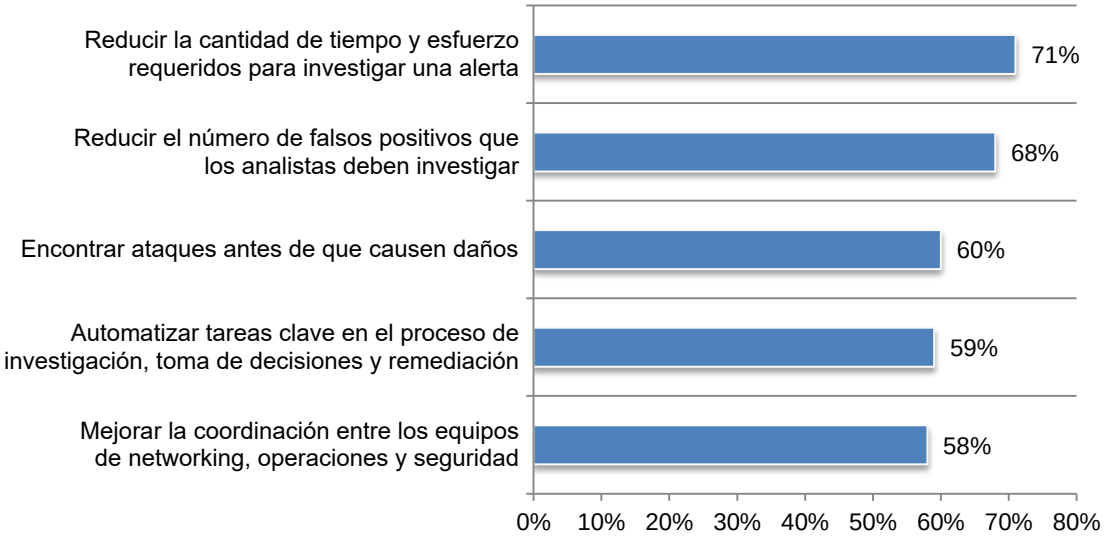
De aquellas organizaciones que tienen ML, 30 por ciento dicen que adquirieron un producto ML llave en mano o contrataron a un proveedor de servicio administrado (26 por ciento. Solamente el 20 por ciento de los encuestados dicen que construyeron sus propias capacidades ML.

Figura 13. Cómo está desplegado ML para detección de ataques



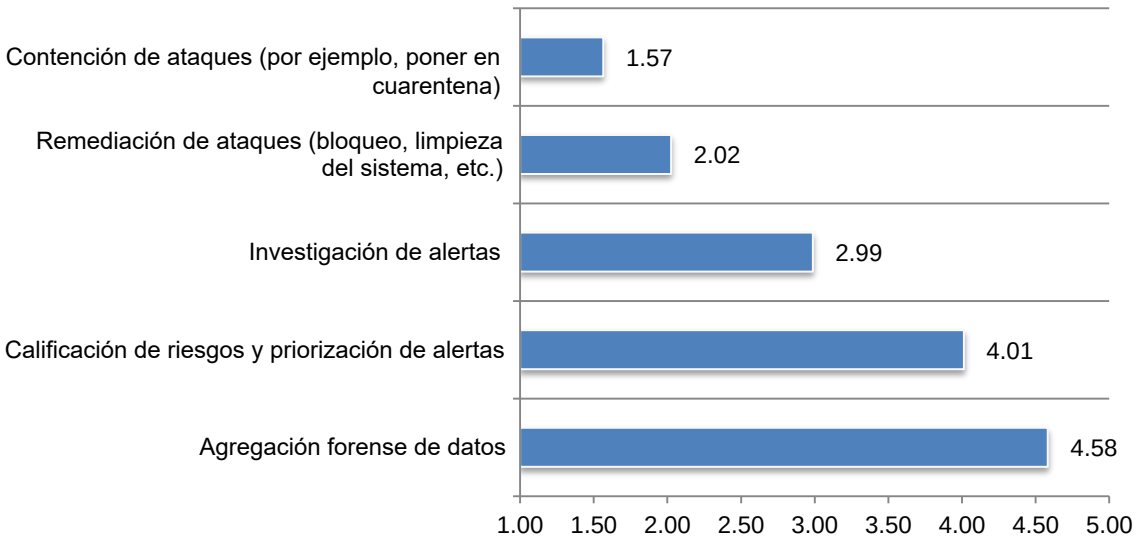
Se considera que el beneficio más grande de la automatización es reducir la cantidad de tiempo y esfuerzo requeridos para investigar una alerta. Se solicitó a los encuestados calificar la importancia de beneficios específicos de automatización para lograr una postura de seguridad más eficiente y efectiva desde 1 = no es importante a 5 = muy alta importancia. La Figura 14 muestra que el beneficio más importante de la tecnología de automatización es la capacidad de reducir la cantidad de tiempo y esfuerzo requeridos para investigar una alerta (71 por ciento de los encuestados), seguido por una reducción del número de falsos positivos que los analistas deben investigar (68 por ciento de los encuestados).

Figura 14. Importancia de beneficios de la automatización
Muy Alta importancia y Alta importancia combinadas



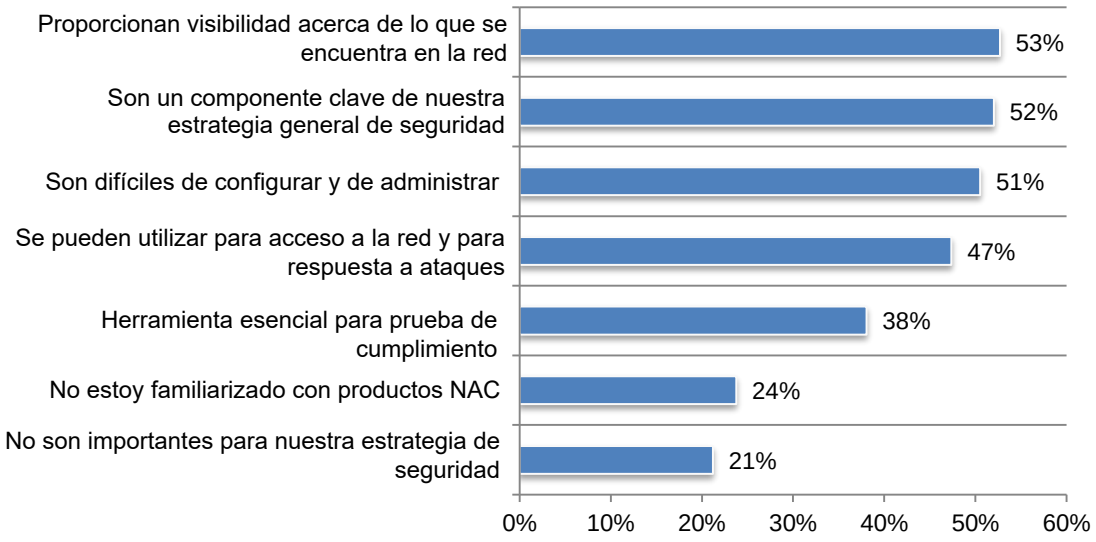
Se solicitó a los encuestados calificar los siguientes procesos que tienen más probabilidad de ser automatizados por sus organizaciones desde 1 = más probable a 5 = menos probable. Como se muestra en la Figura 15, los procesos que más probablemente serán automatizados son contención de ataques y remediación de ataques.

Figura 15. Procesos con más probabilidad de ser automatizados
1 = más probable 5 = menos probable



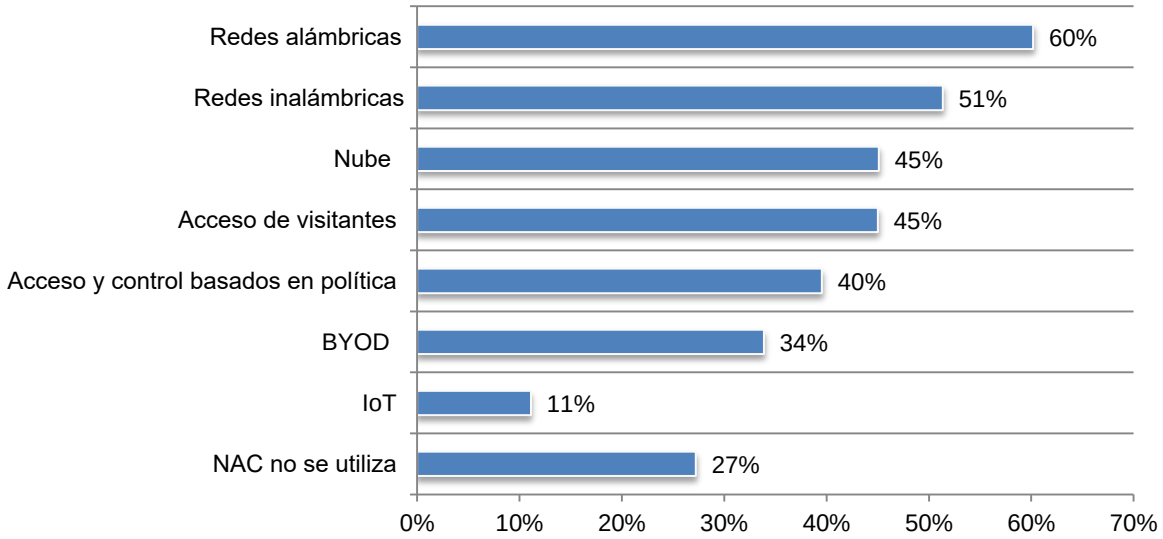
NAC se considera importante para proporcionar visibilidad acerca de lo que se encuentra en las redes. Los encuestados creen que sus productos NAC proporcionan visibilidad acerca de lo que se encuentra en la red (53 por ciento) o que son un componente clave de su estrategia general de seguridad (52 por ciento). Sin embargo, más de la mitad (51 por ciento) dicen que los productos NAC son difíciles de configurar y de administrar, de acuerdo con la Figura 16.

Figura 16. Cómo están desplegados los productos NAC
Más de una respuesta permitida



Setenta y tres por ciento de los encuestados dice que sus organizaciones despliegan NAC. La mayoría están desplegados para redes alámbricas (60 por ciento de los encuestados) o para redes inalámbricas (51 por ciento de los encuestados). Sin embargo, solamente 18 por ciento de los encuestados están muy confiados o confiados de que conocen a todos los usuarios y dispositivos conectados a sus redes todo el tiempo.

Figura 17. Propósitos para los productos NAC
Más de una respuesta permitida



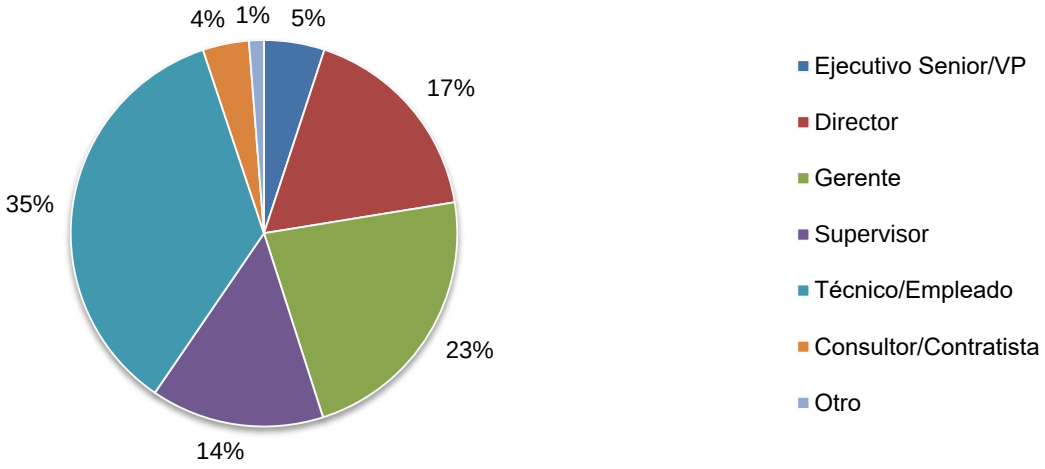
Parte 3. Métodos

El marco de muestreo está compuesto de 115,471 practicantes de TI y de seguridad de TI en las siguientes tres regiones y ocho países: Asia Pacífico, Europa, Medio Oriente y Asia (EMEA), América del Norte, Australia, Brasil, Alemania, India, Japón, México, Singapur y el Reino Unido. Como se muestra en la Tabla 1, 4,385 encuestados completaron la encuesta. El proceso de inspección removió a 519 encuestas. La muestra final fue de 3,866 encuestas (o una tasa de respuesta de 3.3 por ciento).

Tabla 1. Respuesta muestra	Frec	Pct%
Marco de muestra total	115,471	100.0%
Devoluciones totales	4,385	3.8%
Encuestas rechazadas o inspeccionadas	519	0.4%
Muestra final	3,866	3.3%

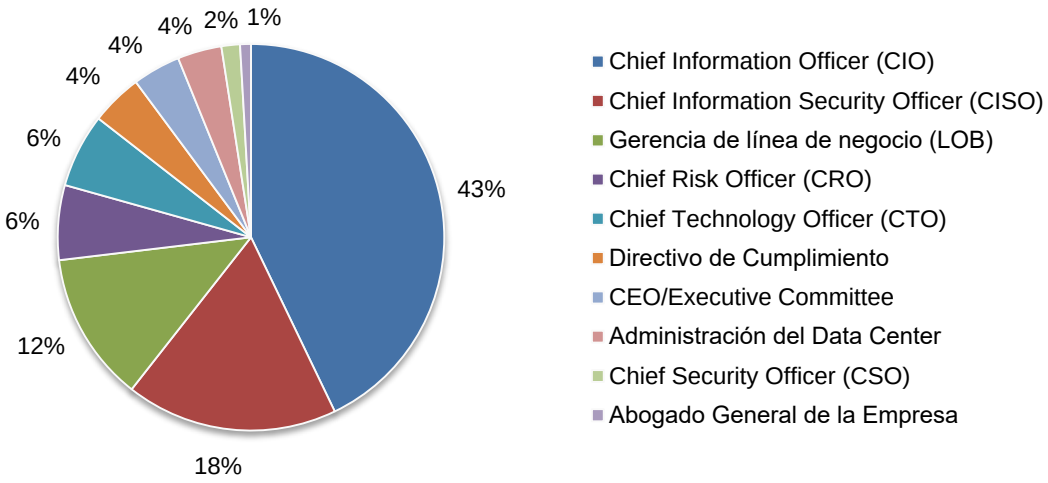
La Gráfica Circular 1 reporta el puesto actual o nivel organizacional de los encuestados. Cincuenta y nueve por ciento de los encuestados reportaron supuesto actual como supervisor o superior.

Gráfica Circular 1. Distribución de encuestados de acuerdo con el nivel del puesto



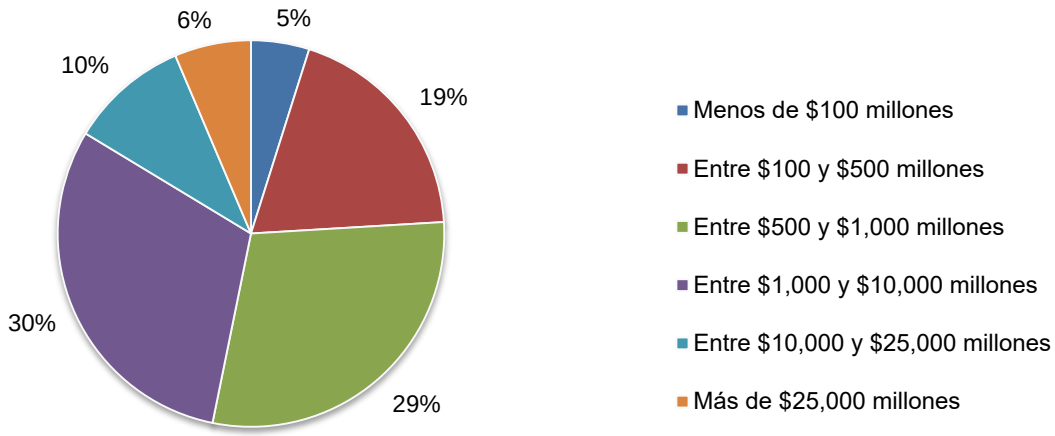
La Gráfica Circular 2 identifica a la persona primaria a la cual reporta el encuestado o su líder de seguridad de TI. Cuarenta y tres por ciento de los encuestados identificaron al Chief Information Officer (CIO) como la persona a la cual reportan. Otro 18 por ciento indicaron que reportan directamente al Chief Information Security Officer y 12 por ciento de los encuestados reportan a un líder de línea de negocio.

Gráfica Circular 2. Distribución de encuestados de acuerdo con el canal de reporte



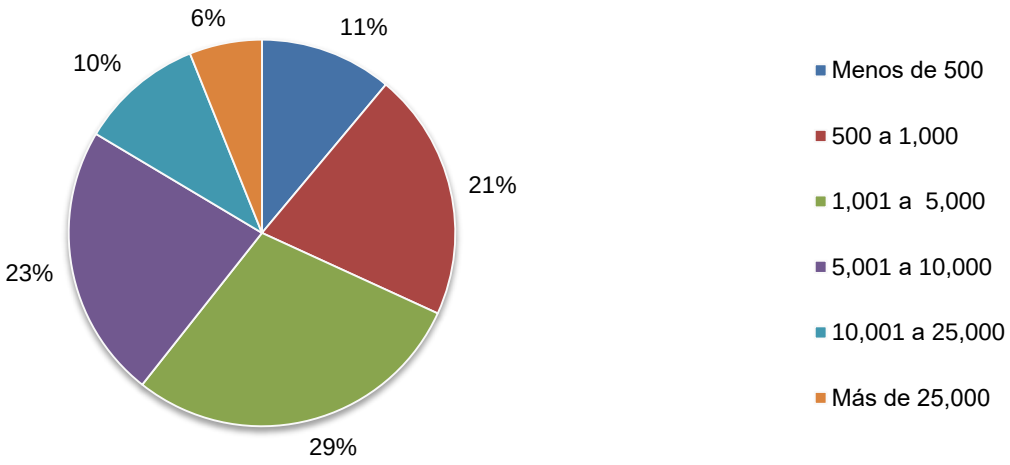
La Gráfica Circular 3 reporta el ingreso a nivel mundial de las organizaciones de los encuestados. Setenta y seis por ciento de los encuestados reportaron que el ingreso de sus organizaciones a nivel mundial anual es más de USD $500 millones.

Gráfica Circular 3. Distribución de encuestados de acuerdo con el ingreso a nivel mundial
Dólares de los Estados Unidos



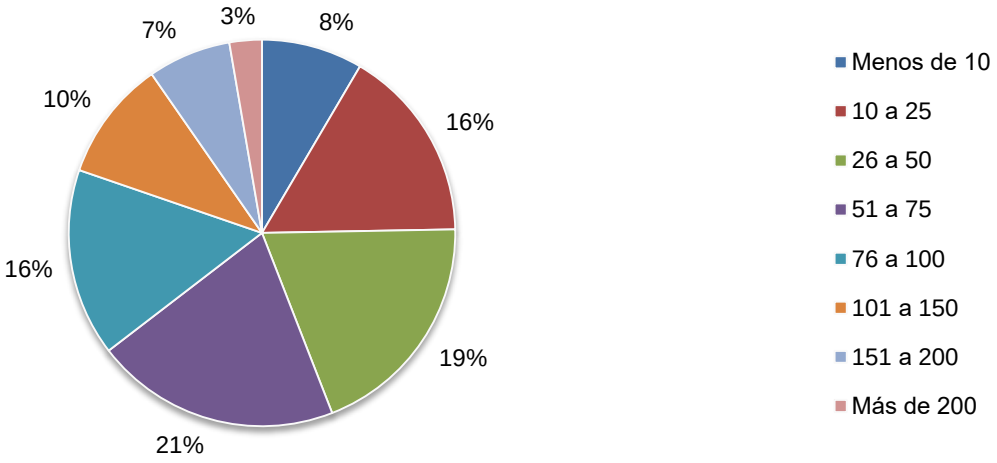
De acuerdo con la Gráfica Circular 4, 68 por ciento de los encuestados son de organizaciones con un número de empleados a nivel global de más de 1,000 empleados.

Gráfica Circular 4. Distribución de encuestados de acuerdo con el número de empleados dentro de la organización



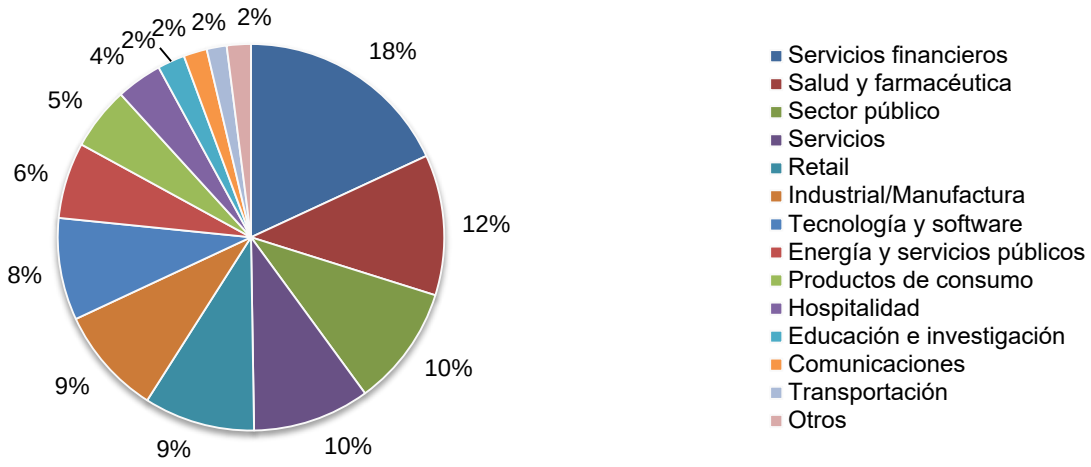
La Gráfica Circular 5 reporta el número de soluciones de seguridad en uso dentro de las organizaciones de los encuestados. Setenta y seis por ciento de los encuestados reportaron que sus organizaciones están utilizando la actualidad más de 25 soluciones de seguridad.

Gráfica Circular 5. Distribución de encuestados de acuerdo con el número de soluciones de seguridad



La Gráfica Circular 6 reporta la clasificación primaria de industria de las organizaciones de los encuestados. Esta gráfica identifica servicios financieros (18 por ciento de los encuestados) como el segmento más grande, seguido por salud y farmacéutica (12 por ciento de los encuestados), el sector público (10 por ciento de los encuestados) y el sector de servicios (10 por ciento de los encuestados.

Gráfica Circular 6. Distribución de encuestados de acuerdo con la clasificación primaria de industria



Parte 4. Advertencias

Existen limitaciones inherentes a la investigación de encuestas que necesitan considerarse cuidadosamente antes de sacar inferencias de los hallazgos. Los siguientes aspectos son limitaciones específicas que son pertinentes a la mayoría de las encuestas basadas en web.

Sesgo por falta de respuesta: Los hallazgos actuales están basados en una muestra de las encuestas devueltas. Enviamos encuestas a una muestra representativa de personas, resultando en un gran número de respuestas devueltas utilizables. A pesar de pruebas por falta de respuesta, siempre es posible que las personas que no participaron sean substancialmente diferentes en términos de las creencias subyacentes de aquellas que completaron el instrumento.

Sesgo del marco de muestreo: La exactitud está basada en información de contacto y el grado al cual la lista es representativa de las personas que son practicantes de TI o de seguridad de TI en diversas organizaciones en Asia-Pacífico, EMEA, América del Norte, Australia, Brasil, Alemania, India, Japón, México, Singapur y el Reino Unido. También reconocemos que los resultados pueden estar sesgados por eventos externos, como cobertura de los medios. También reconocemos un sesgo provocado por compensar a los sujetos para completar esta investigación dentro de un periodo de tiempo especificado.

Resultados auto reportados: La calidad de la investigación de encuestas está basada en la integridad de las respuestas confidenciales recibidas de los sujetos. Aun cuando ciertas verificaciones y controles se pueden incorporar en el proceso de encuestas, siempre existe la posibilidad de que un sujeto no haya proporcionado respuestas exactas.

Apéndice: Resultados Detallados de la Encuesta

Las siguientes tablas proporcionan la frecuencia o porcentaje de frecuencia de las respuestas a todas las preguntas de encuesta contenidas en este estudio. Todas las respuestas de la encuesta se capturaron del 6 de marzo al 20 de marzo de 2018.

Respuesta a la encuesta	Global
Marco de muestreo	115,471
Devoluciones totales	4,385
Encuestas rechazadas	519
Muestra final	3,866
Tasa de respuesta	3.3%
Mismos pesos	1.00

Parte 1. Inspección

S1. ¿Qué es lo que mejor describe su involucramiento en las inversiones de seguridad de TI dentro de su organización?	Global
Nada (alto)	0%
Responsable por la solución general/adquisición	50%
Responsable por la administración/manejo	58%
Involucrado en evaluar soluciones	68%
Total	176%

S2. ¿Qué es lo que mejor describe su rol dentro del departamento de TI o de seguridad de TI de su organización?	Global
Liderazgo de seguridad (CSO/CISO)	38%
Administración de TI	43%
Operaciones de TI	50%
Administración de seguridad	53%
Monitoreo y respuesta de seguridad	65%
Administración de datos	29%
Administración de cumplimiento	16%
Desarrollo de aplicaciones	25%
Oficina de protección de datos	2%
No estoy involucrado en la función de seguridad de TI o de seguridad de TI (alto)	0%
Total	321%

S3. ¿Qué tan enterado está usted de la estrategia y tácticas de seguridad de TI de su organización?	Global
Muy enterado	36%
Enterado	48%
Algo enterado	16%
Ligeramente enterado (alto)	0%
No tengo conocimientos (alto)	0%
Total	100%

Parte 2: Atribuciones

Q1. Por favor califique cada uno de los siguientes enunciados utilizando la escala de acuerdo proporcionada abajo de cada artículo.	
Q1a. Los equipos de seguridad no cuentan con visibilidad y control de todas las actividades de cada usuario y dispositivo (esto es, móvil, BYOD, IoT) conectado a su infraestructura de TI.	Global
Totalmente de acuerdo	32%
De acuerdo	35%
No estoy seguro	14%
En desacuerdo	11%
Totalmente en desacuerdo	8%
Total	100%

Q1b. Las nuevas tecnologías, como aprendizaje de máquina, se requieren para descubrir y entender amenazas que están activas en la infraestructura de TI.	Global
Totalmente de acuerdoa	29%
De acuerdo	35%
No estoy seguro	16%
En desacuerdo	13%
Totalmente en desacuerdo	7%
Total	100%

Q1c. In my experience, the IT security infrastructure has gaps that allow attackers to penetrate its defenses.	Global
Totalmente de acuerdo	29%
De acuerdo	33%
No estoy seguro	20%
En desacuerdo	11%
Totalmente en desacuerdo	8%
Total	100%

Q1d. My organization is getting the full value from our current security investments.	Global
Totalmente de acuerdo	20%
De acuerdo	25%
No estoy seguro	27%
En desacuerdo	18%
Totalmente en desacuerdo	10%
Total	100%

Q2. ¿Cuáles son las brechas primarias en la infraestructura de seguridad de TI de su organización? Por favor seleccione sus cuatro mejores opciones.	Global
Personal de seguridad y escasez de habilidades	49%
Demasiadas alertas que responder	36%
Demasiados falsos positivos	45%
Las soluciones de seguridad no pueden mantener el paso con cantidades de datos exponencialmente crecientes	41%
Difícil de proteger un perímetro de TI en expansión y difuminado con IoT, BYOD, móvil y la nube	55%
Soluciones de seguridad en silos	38%
Incapacidad de las soluciones de seguridad tradicionales basadas en perímetro para detectar y detener ataques enfocados avanzados	41%
Falta de visibilidad de cada usuario y dispositivo conectado a la infraestructura de TI	45%
Falta de visibilidad de lo que cada usuario y dispositivo está haciendo mientras está conectado a la infraestructura de TI	49%
Otro (por favor especifique)	1%
Total	400%

Q3. A pesar de todas las inversiones en seguridad cibernética efectuadas por compañías, ¿por qué continúan ocurriendo las violaciones? Por favor seleccione sus tres mejores opciones.	Global
Es difícil proteger superficies de ataque complejas y que cambian dinámicamente (móvil, BYOD, nube, IoT, etc.)	49%
Existe una falta de personal de seguridad adecuado con las habilidades necesarias	48%
Los atacantes son persistentes, sofisticados, bien entrenados y bien financiados	46%
Complejidad y la incapacidad de integrar soluciones de seguridad	42%
Falta de visibilidad dentro de la red	36%
Las amenazas han evadido las defensas tradicionales de seguridad y ahora están adentro del ecosistema de TI	35%
Error humano	43%
Otro (por favor especifique)	1%
Total	300%

Parte 3. Ataques desde adentro

Q4. Por favor califique cada una de los siguientes enunciados utilizando la escala de acuerdo proporcionada abajo de cada artículo.	
Q4a. Los ataques que han llegado adentro de la red tienen el potencial de provocar el daño más grande.	Global
Totalmente de acuerdo	26%
De acuerdo	25%
No estoy seguro	21%
En desacuerdo	17%
Totalmente en desacuerdo	11%
Total	100%

Q4b. Estamos confiados que los ataques adentro de la infraestructura de TI se pueden detectar antes de que causen una violación de seguridad cibernética que resulta en robo, modificación o visualización de datos por entidades no autorizadas.	Global
Totalmente de acuerdo	18%
De acuerdo	20%
No estoy seguro	20%
En desacuerdo	26%
Totalmente en desacuerdo	16%
Total	100%

Q5. ¿Cuál de los siguientes usted cree que presenta la amenaza interior más grande a su infraestructura de TI? Por favor califique cada amenaza desde 1=mayor amenaza a 5=menor amenaza.	Global
Usuarios legítimos comprometidos	1.67
Empleados maliciosos	4.18
Usuarios negligentes	2.75
Dispositivos IoT comprometidos	3.14
Ataques enfocados avanzados que han circunvalado las defensas perimetrales tradicionales	3.37
Promedio	3.06

Q6. ¿Cuáles pasos se deben tomar para minimizar amenazas clandestinas y ocultas dentro de la infraestructura de TI? Por favor marque todos los que apliquen.	Global
UEBA	40%
SIEM	47%
NTA (Network Traffic Analysis)	34%
Monitoreo de usuarios privilegiados	53%
Ninguno de los anteriores	31%
Otro (por favor especifique)	1%
Total	206%

Q7. Utilizando la siguiente escala de 5 puntos, por favor califique la importancia de los diversos tipos de visibilidad en términos de detectar ataques de adentro desde 1 = no es importante a 5 = muy alta importancia.	
Q7a. Visibilidad del tráfico de red	Global
1 = no es importante	6%
2 = baja importancia	11%
3 = importancia moderada	20%
4 = alta importancia	37%
5 =muy alta importancia	26%
Total	100%
Valor extrapolado	3.65

Q7b. Visibilidad de servidores	Global
1 = no es importante	9%
2 = baja importancia	11%
3 = importancia moderada	18%
4 = alta importancia	31%
5 =muy alta importancia	30%
Total	100%
Valor extrapolado	3.62

Q7c. Visibilidad de aplicaciones	Global
1 = no es importante	1%
2 = baja importancia	5%
3 = importancia moderada	22%
4 = alta importancia	31%
5 =muy alta importancia	40%
Total	100%
Valor extrapolado	4.03

Q7d. Visibilidad de datos	Global
1 = no es importante	7%
2 = baja importancia	11%
3 = importancia moderada	22%
4 = alta importancia	29%
5 =muy alta importancia	32%
Total	100%
Valor extrapolado	3.69

Q7e. Visibilidad de la nube	Global
1 = no es importante	7%
2 = baja importancia	13%
3 = importancia moderada	15%
4 = alta importancia	35%
5 =muy alta importancia	29%
Total	100%
Valor extrapolado	3.65

Q7f. Visibilidad de IoT	Global
1 = no es importante	9%
2 = baja importancia	15%
3 = importancia moderada	24%
4 = alta importancia	26%
5 =muy alta importancia	25%
Total	100%
Valor extrapolado	3.43

Q7g. Visibilidad de puntos terminales	Global
1 = no es importante	1%
2 = baja importancia	10%
3 = importancia moderada	20%
4 = alta importancia	35%
5 =muy alta importancia	34%
Total	100%
Valor extrapolado	3.91

Parte 4. Aprendizaje de Máquina basado en – ¿Bombo o Realidad?

Q8. Las tecnologías AI (aprendizaje de máquina, analíticos de comportamiento) son esenciales para detectar ataques desde adentro antes de que provoquen daños.	Global
Totalmente de acuerdo	22%
De acuerdo	29%
No estoy seguro	25%
En desacuerdo	17%
Totalmente en desacuerdo	6%
Total	100%

Q9. ¿Cuáles son los tres beneficios clave de seguridad de utilizar ML y analíticos avanzados? Por favor seleccione sus tres mejores opciones.	Global
Automatizar tareas rutinarias	32%
Encontrar amenazas clandestinas que hayan evadido las defensas de seguridad estándar	56%
Aumentar la efectividad de los equipos de seguridad	63%
Mejor integración con fuentes de inteligencia de amenazas	44%
Investigaciones más eficientes	60%
Reducción en el ruido blanco/falsos positivos	28%
Suplemento a sistemas SIEM	18%
Total	300%

Q10a. ¿Cuál frase mejor describe el uso de ML para propósitos de seguridad dentro de su organización?	Global
ML está implementado extensivamente a través de la infraestructura de TI	12%
ML está implementado parcialmente a través de la infraestructura de TI	17%
Estamos planeando utilizar ML en los siguientes 12 meses (por favor salte a la Q12)	26%
Estamos planeando utilizar ML después de un año (por favor salte a la Q12)	20%
No, no estamos planeando utilizar ML (por favor salte a la Q12)	24%
Total	100%

Q10b. ¿Cuál frase mejor describe cómo ML está desplegado para detección de ataques?	Global
Hemos construido nuestras propias capacidades de ML	20%
Comenzamos con software ML básico y lo adaptamos para nuestros propósitos	24%
Contratamos a un proveedor de servicios administrados para proporcionar capacidades de ML	26%
Adquirimos un producto ML llave en mano	30%
Total	100%

Q11. ¿Qué es lo que mejor describe la forma en la cual el mercado considera soluciones de detección de ataques basadas en ML?	Global
Es importante ser una función autónoma como la última línea de defensa	21%
Se considera un suplemento importante a SIEM	15%
Será una característica en otros productos de seguridad	29%
Demasiado pronto para decir	35%
Total	100%

Parte 5. Automatización

Q12. Utilizando la siguiente escala de 5 puntos, por favor califique la importancia de beneficios específicos de automatización para lograr una postura de seguridad más eficiente y efectiva desde 1 = no es importante a 5 = muy alta importancia.	
Q12a. Reduce el número de falsos positivos que los analistas deben investigar	Global
1 = no es importante	3%
2 = baja importancia	7%
3 = importancia moderada	21%
4 = alta importancia	38%
5 = muy alta importancia	30%
Total	100%
Valor extrapolado	3.84

Q12b. Reduce la cantidad de tiempo y esfuerzo requeridos para investigar una alerta	Global
1 = no es importante	1%
2 = baja importancia	5%
3 = importancia moderada	23%
4 = alta importancia	41%
5 = muy alta importancia	30%
Total	100%
Valor extrapolado	3.95

Q12c. Encuentra ataques antes de que causen daños	Global
1 = no es importante	4%
2 = baja importancia	10%
3 = importancia moderada	26%
4 = alta importancia	36%
5 = muy alta importancia	24%
Total	100%
Valor extrapolado	3.67

Q12d. Mejora la coordinación entre los equipos de networking, operaciones y seguridad	Global
1 = no es importante	6%
2 = baja importancia	10%
3 = importancia moderada	26%
4 = alta importancia	30%
5 = muy alta importancia	28%
Total	100%
Valor extrapolado	3.63

Q12e. Automatiza tareas clave en el proceso de investigación, toma de decisiones y remediación	Global
1 = no es importante	5%
2 = baja importancia	12%
3 = importancia moderada	24%
4 = alta importancia	29%
5 = muy alta importancia	30%
Total	100%
Valor extrapolado	3.65

Q13. ¿Cuál de los siguientes procesos tiene mayor probabilidad de ser automatizado por su organización? Por favor califiqué cada proceso desde 1 = más probable a 5 = menos probable.	Global
Calificación de riesgos y priorización de alertas	4.01
Agregación forense de datos	4.58
Investigación de alertas	2.99
Contención de ataques (por ejemplo, poner en cuarentena)	1.57
Remediación de ataques (bloqueo, limpieza del sistema, etc.)	2.02
Promedio	3.03

Parte 6. NAC (Network Access Control)

Q14. ¿Cuál es su nivel de confianza de que conoce a TODOS los usuarios y dispositivos conectados a su red en TODO momento?	Global
Muy confiado	5%
Confiado	13%
Algo confiado	16%
No confiado	32%
Ninguna confianza	34%
Total	100%

Q15. ¿Cuáles enunciados mejor describen su opinión acerca de los productos NAC implementados por su organización? Por favor marque todos los que apliquen.	Global
No son importantes para nuestra estrategia de seguridad	21%
Proporcionan visibilidad de lo que se encuentra en la red	53%
Son difíciles de configurar y administrar	51%
Son un componente clave de nuestra estrategia general de seguridad	52%
Se pueden utilizar para acceso a la red y para respuesta a ataques	47%
No estoy familiarizado con productos NAC	24%
Herramienta esencial para prueba de cumplimiento	38%
Total	286%

Q16. ¿Para cuáles propósitos están implementados los sistemas NAC dentro de su organización? Por favor marque todos los que apliquen.	Global
Redes alámbricas	60%
Redes inalámbricas	51%
Acceso de visitantes	45%
BYOD	34%
IoT	11%
Nube	45%
Acceso y control basado en política	40%
No se utiliza NAC	27%
Total	313%

Parte 7. IoT (Internet of things)

Q17. Utilizando la siguiente escala de 5 puntos, por favor califique la capacidad de su organización para asegurar dispositivos y apps IoT desde 1 = ninguna capacidad a 5 = muy alta capacidad.	Global
1 = ninguna capacidad	28%
2 = baja capacidad	38%
3 = capacidad moderada	18%
4 = alta capacidad	10%
5 = muy alta capacidad	5%
Total	100%
Valor extrapolado	2.27

Q18. ¿Qué se requiere para lograr un fuerte nivel de seguridad IoT dentro de su organización? Por favor marque todos los que apliquen.	Global
NAC	41%
Continuous monitoring of network traffic for each IoT device to spot anomalies	52%
Peer group IoT device comparisons to spot anomalies	37%
Real time solutions to stop IoT activity that is identified as compromised or malicious	37%
Tools to prove compliance requirements have been met	35%
No additional security beyond what is provided by the manufacturer	25%
Other (please specify)	0%
None of the above	31%
Total	258%

Q19. Por favor califique cada uno de los siguientes enunciados utilizando la escala de acuerdo proporcionada abajo de cada artículo.	
Q19a. Los dispositivos IoT están asegurados adecuadamente con una estrategia de seguridad correcta implementada.	Global
Totalmente de acuerdo	11%
De acuerdo	13%
No estoy seguro	14%
En desacuerdo	33%
Totalmente en desacuerdo	29%
Total	100%

Q19b. Las tecnologías IoT legadas son difíciles de asegurar.	Global
Totalmente de acuerdo	33%
De acuerdo	38%
No estoy seguro	18%
En desacuerdo	9%
Totalmente en desacuerdo	2%
Total	100%

Q19c. Los dispositivos IoT que simplemente monitorean o efectúan tareas menores presentan poca amenaza a la seguridad general de nuestra organización.	Global
Totalmente de acuerdo	11%
De acuerdo	12%
No estoy seguro	17%
En desacuerdo	29%
Totalmente en desacuerdo	31%
Total	100%

Q20. ¿Quién dentro de su organización es más responsable de asegurar la seguridad de los dispositivos y apps IoT?	Global
Chief information officer (CIO)	34%
Chief technology officer (CTO)	5%
Chief information security officer (CISO)	18%
Chief security officer (CSO)	3%
Liderazgo de línea de negocio	11%
Usuarios finales de dispositivos IoT	13%
Data Protection Officer (DPO)	0%
Ninguna de las funciones tiene la responsabilidad general	15%
Otro (por favor especifique)	1%
Total	100%

Parte 8. Su rol y organización

D1. ¿Cuál nivel organizacional mejor describe su puesto actual?	Global
Ejecutivo Senior/VP	5%
Director	17%
Gerente	23%
Supervisor	14%
Técnico/Empleado	35%
Consultor/Contratista	4%
Otro	1%
Total	100%

D2. Marque la Persona Primaria a la cual reporta usted o su líder dentro de la organización.	Global
CEO/Executive Committee	4%
General Counsel	1%
Chief Information Officer (CIO)	43%
Chief Technology Officer (CTO)	6%
Chief Information Security Officer (CISO)	18%
Directivo de Cumplimiento	4%
Administración de línea de negocios (LOB)	12%
Chief Security Officer (CSO)	2%
Administración del Data Center	4%
Chief Risk Officer (CRO)	6%
Otro	0%
Total	100%

D3. ¿Cuál rango mejor describe el ingreso a nivel mundial de su organización? (dólares de Estados Unidos)	Global
Menos de $100 millones	5%
Entre $100 y $500 millones	19%
Entre $500 millones y $1,000 millones	29%
Entre $1,000 millones y $10,000 millones	30%
Entre $10,000 millones y $25,000 millones	10%
Más de $25,000 millones	6%
Total	100%

D4. ¿Cuántos empleados están en su organización?	Global
Menos de 500	11%
500 a 1,000	21%
1,001 a 5,000	29%
5,001 a 10,000	23%
10,001 a 25,000	10%
Más de 25,000	6%
Total	100%

D5. ¿Cuántas soluciones de seguridad utiliza su organización?	Global
Menos de 10	8%
10 a 25	16%
26 a 50	19%
51 a 75	21%
76 a 100	16%
101 a 150	10%
151 a 200	7%
Más de 200	3%
Total	100%
Valor extrapolado	68

D6. ¿Cuál es la que mejor describe la clasificación primaria de industria de su organización?	Global
Agricultura y servicios de alimentos	1%
Comunicaciones	2%
Productos de consumo	5%
Defensa y aeroespacio	0%
Educación e investigación	2%
Energía y servicios públicos	6%
Entretenimiento y medios	1%
Servicios financieros	18%
Salud y farmacéutica	12%
Hospitalidad	4%
Industrial/manufactura	9%
Sector público	10%
Retail	9%
Servicios	10%
Tecnología y software	8%
Transportación	2%
Total	100%

Por favor póngase en contacto con research@ponemon.org o llámenos al 800.887.3118 si tiene cualquier pregunta.

Ponemon Institute

Avanzando la Administración Responsable de Información

Ponemon Institute está dedicado a investigación y educación independiente que avanzan las prácticas de administración responsable de información y privacidad dentro de las empresas y el gobierno. Nuestra misión es llevar a cabo estudios empíricos de alta calidad sobre aspectos críticos que afectan la administración y seguridad de información sensible acerca de personas y organizaciones.

Apoyamos la estricta confidencialidad de datos, la privacidad y las normas de investigación éticas. No recolectamos ninguna información personalmente identificable de personas (o información identificable de compañías en nuestra investigación de negocios). Más aún, tenemos normas estrictas de calidad para asegurar que no se les formulen a las personas preguntas extrañas, irrelevantes, o impropias.