La ciberseguridad en la era cognitiva

Optimizar su sistema inmune digital

IBM Institute for Business Value

Cómo IBM puede ayudarle

El delito informático es una insidiosa amenaza que ha alcanzado niveles de crisis. Aunque es difícil de cuantificar con precisión, el coste del delito informático para la economía global se estima entre 375 y 575 miles de millones de dólares anuales. Ninguna zona ni sector es inmune. IBM® tiene una amplia cartera integrada de software y servicios de seguridad que abordan la prevención, detección, respuesta y remediación para ayudar a las organizaciones a anticiparse y emprender acción temprana para mitigar los impactos de los riesgos para la ciberseguridad. IBM Security ayuda a los clientes a establecer un sistema inmune respaldado por analítica, defensas en tiempo real: y expertos de demostrada capacidad. Para obtener más información sobre cómo IBM colabora con distintas organizaciones para proteger sus infraestructuras digitales, visite **ibm.com**/security.

Nuevas capacidades para una era llena de desafíos

Los responsables de seguridad trabajan para abordar tres lagunas en sus capacidades actuales: en inteligencia, velocidad y precisión. Algunas organizaciones están comenzando a explorar el potencial de las soluciones de seguridad cognitiva para abordar estas tres lagunas y ponerse por delante de los riesgos y amenazas. Se trata de unas expectativas muy elevadas para esta tecnología. El 57% de los responsables de seguridad entrevistados consideran que puede frenar significativamente los esfuerzos de los delincuentes informáticos. El 22% de los entrevistados a los que hemos denominado 'Bien preparados' ya han comenzado su viaje hacia la era cognitiva de la ciberseguridad: consideran que poseen la familiaridad, la madurez y los recursos que necesitan. Para comenzar este viaje, es importante explorar sus puntos débiles, determinar cómo quiere aumentar sus capacidades con soluciones cognitivas y pensar en preparar planes de formación e inversión para todas las partes interesadas.

Resumen ejecutivo

El estado de la ciberseguridad está llegando a un punto de inflexión. El número de riesgos y eventos está experimentando un crecimiento exponencial y los equipos operativos de seguridad se esfuerzan por mantener este ritmo. El panorama de amenazas cambia con gran rapidez, con una sofisticación y número de variantes demasiado elevados para los enfoques tradicionales. También aumenta la repercusión de los incidentes y filtraciones, y los costes y riesgos financieros crecen con rapidez. Por último, muchas organizaciones se encuentran con la falta de expertos en seguridad con los conocimientos adecuados. Ante todos estos obstáculos, las empresas tienen serias dificultades para mantener sus sistemas inmunes digitales en un estado de salud adecuado para protegerse.

Para este informe entrevistamos a 700 directores de seguridad informática (CISO) y otros responsables de seguridad de 35 países representando a 18 sectores. Nuestros objetivos eran descubrir cuáles son los problemas a los que se enfrentan estos directivos, cuáles son sus carencias y qué están haciendo al respecto. También quisimos conocer sus impresiones sobre las soluciones de seguridad cognitiva: cómo opinan que estas soluciones pueden serles de ayuda, hasta qué punto están preparados para implementarlas y qué obstáculos encuentran.

Descubrimos que para los responsables de seguridad el problema radica en la complejidad de las amenazas y la velocidad con la que han de darles respuesta. Están preocupados por la forma en que los incidentes relacionados con la seguridad afectan a sus actividades hoy y cómo pueden marcar sus reputaciones en el futuro. Los responsables de seguridad perciben que no son todo lo eficaces que podrían a la hora de abordar la protección de sus redes y datos y de dar una respuesta rápida e inteligente a las amenazas. Sin embargo, buscan formas de abordar estas deficiencias en los próximos años. Conseguir los recursos adecuados para hacer frente a estos problemas no será fácil. Enfrentados al aumento de los costes y la escasez de recursos especializados, los responsables de seguridad buscan formas de justificar mejor sus inversiones ante la alta dirección de sus empresas.

El **principal desafío para la ciberseguridad** hoy y mañana es **reducir los tiempos de respuesta y resolución de incidentes**.

57% de los responsables de seguridad creen que **las soluciones de seguridad cognitiva** pueden frenar significativamente **los esfuerzos de los delincuentes informáticos**.

Se prevé que el **número de profesionales** que implementan soluciones de seguridad cognitiva **se multiplique por tres** en los próximos 2–3 años.

A medida que las organizaciones recopilan más datos de seguridad y aplican más capacidades analíticas, las cargas de trabajo aumentan hasta alcanzar los límites de lo posible con medios manuales. Algunas están considerando soluciones de seguridad cognitiva para gestionar esta situación y abordar lagunas en inteligencia, velocidad y precisión. Aunque las tecnologías cognitivas aplicadas a la seguridad aún se encuentran en un estadio temprano, su potencial ofrece grandes esperanzas y motivos para el optimismo. Los participantes en el estudio dijeron que los principales beneficios que esperan de las soluciones de seguridad cognitiva son mejoras en la detección y capacidades para acelerar las respuestas, reducción de los tiempos de respuesta ante incidentes y mayor confianza al discriminar entre eventos e incidentes reales. A pesar de su gran promesa, aún se necesita mucha formación y preparación antes de que se extienda su adopción.

Pero sí identificamos un grupo 'bien preparado para la era cognitiva' de las soluciones de seguridad. Cuando examinamos la efectividad, preparación para los sistemas cognitivos y comprensión de la seguridad, identificamos unos líderes entusiastas que se consideran preparados para entrar hoy mismo en la era cognitiva de las soluciones de seguridad. En general, estos líderes tienden a tener más conocimiento de las soluciones cognitivas, más confianza general en sus capacidades en relación con la seguridad y menos problemas para conseguir recursos.

A medida que las soluciones de seguridad cognitiva se establezcan y extiendan más, cualquier organización podrá beneficiarse de ellas. Si considera que está preparado y decide comenzar el viaje, el primer paso es identificar los puntos débiles que espera abordar mediante las soluciones de seguridad cognitiva. A continuación, estudie distintos casos de uso y busque correspondencias con sus puntos débiles. En un entorno en el que se espera una justificación de la inversión, dedique un tiempo a poner en común los beneficios de las soluciones de seguridad cognitiva con las distintas partes interesadas. Destaque, en un lenguaje que puedan comprender los ejecutivos, que estas soluciones pueden contribuir a mejorar la posición general de la empresa en relación con la seguridad. Estos pasos iniciales prepararán a su organización para la era cognitiva de la ciberseguridad.

Contexto actual

Al arañar la superficie del actual panorama de la ciberseguridad, es posible que las respuestas de los responsables de seguridad entrevistados den a entender que la situación es manejable. De hecho, estos profesionales tienen fe y confianza en sus crecientes capacidades tecnológicas y organizativas. Una mayoría, (el 77 por ciento) de los consultados sobre su preparación en materia de ciberseguridad opinan que están al nivel de otras empresas del sector. Los consultados también son optimistas sobre su posición en relación con la ciberseguridad en los próximos dos-tres años, y un 86 por ciento dicen que estarán *mejor* posicionados que otras empresas del sector.

Posiblemente estas respuestas no parezcan sorprendentes, pero es importante examinarlas: Los responsables de seguridad creen que no lo están haciendo peor que los demás y tienen confianza en que están progresando positivamente y que seguirán haciéndolo. Casi tres cuartas partes consideran que son efectivos a la hora de abordar los elementos básicos de la seguridad organizativa, y el 72 por ciento dicen que son eficaces en cuanto a higiene de TI y el 71 que son efectivos en conocimiento de los riesgos en toda su empresa. Pero veamos con un mayor grado de detalle qué es lo que está ocurriendo en realidad con los desafíos, impactos, capacidades, financiación y rendimiento de las inversiones en seguridad.

Necesidad de velocidad

El principal desafío actual para los responsables de seguridad es reducir los tiempos medios de respuesta y resolución de incidentes. El 45% de los consultados identificaron estos tiempos como un gran desafío actual para la ciberseguridad. Las organizaciones no ven cambios en este problema en los próximos dos-tres años. Pensando en el futuro, el 53 por ciento de los consultados consideran que mejorar la respuesta seguirá siendo un importante desafío para la seguridad (ver Figura 1).

"Es literalmente como ser un marino mercante en la edad de oro de los piratas: no hay fuerzas navales ni policía: uno está solo, abandonado a su propia suerte. Además, muchos no saben cómo dirigir sus naves y no pueden responder a sus atacantes (es ilegal). Uno se encuentra en un mundo hostil con ambas manos atadas a la espalda. Sin embargo, sí existen algunas herramientas interesantes y sofisticadas que puede utilizar para conocer a fondo sus amenazas".

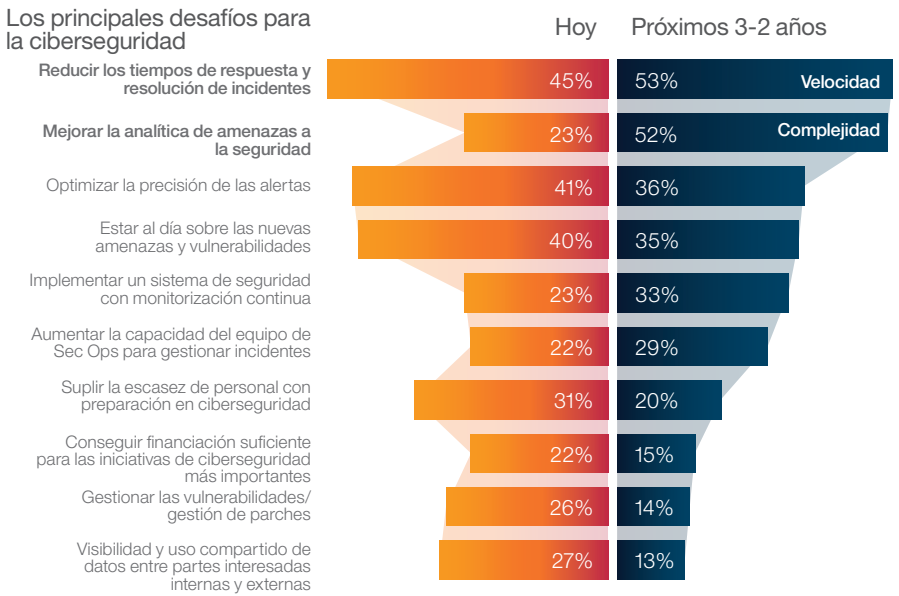
David Shipley, Director de iniciativas estratégicas y servicios de tecnología de la información de la Universidad de New Brunswick

Más tiempo significa más riesgo

En un estudio de 2016, el Ponemon Institute descubrió que el tiempo medio necesario para identificar una filtración era de 201 días, y el tiempo medio necesario para contener la filtración era de 70 días. Asimismo, el instituto determinó que utilizar un equipo de respuesta ante incidentes constituía el principal factor para reducir el coste de una filtración de datos.[1]

Figura 1

Los responsables de seguridad identificaron los principales desafíos actuales para la seguridad y los que consideran que serán los más importantes en el futuro cercano.



Estas preocupaciones persisten a pesar de que el 80 por ciento de las organizaciones nos dicen que las velocidades de respuesta ante incidentes son muy superior a hace dos años (por término medio un 16 por ciento más rápidas). El 86 por ciento quiere mejoras de la velocidad aún mayores en los próximos dos-tres años (con un objetivo medio de mejora del 24 por ciento).

Se trata de un asunto extremadamente importante para las empresas. Cuanto más tiempo tarde una organización en responder a un incidente, mayores daños podrá sufrir y más dinero perderá gestionando la crisis. El tiempo es un factor que aumenta claramente el riesgo de pérdidas.

Otro problema que preocupa cada vez más a los responsables de seguridad se refiere a mejorar el análisis de las amenazas. En 23 por ciento de los consultados identifican este problema como uno de los más importantes en la actualidad, pero el 52 porcientotiene previsto que mejorar la analítica de amenazas a la seguridad sea el principal reto para la ciberseguridad en los próximos dos-tres años. Los analistas de seguridad precisan ayuda para recopilar conocimientos, determinar qué amenazas son las más urgentes y buscar rápidamente patrones de actividad y desviaciones. Los responsables de seguridad se interesarán por todo lo que pueda contribuir a mejorar su velocidad y gestionar la complejidad de las amenazas a las que se enfrentan.

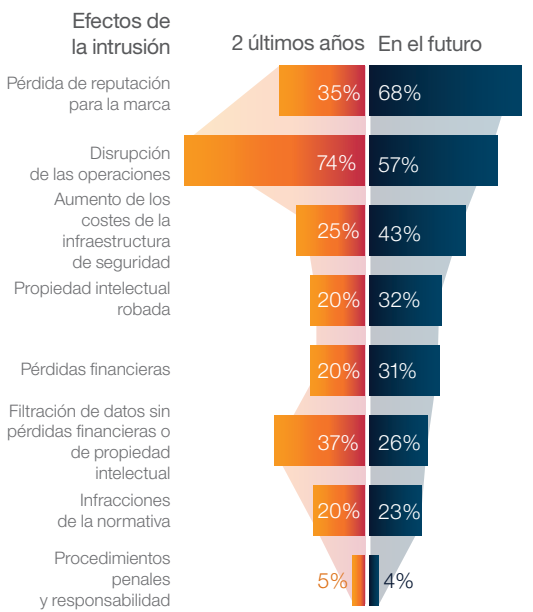
Las preocupaciones se extienden

Casi tres cuartas partes de los consultados dijeron que las intrusiones produjeron disrupciones operativas en los dos últimos años. Sin embargo, lo que esperan para los próximos años es drásticamente distinto.

Las empresas están cada vez más preocupadas de que en el futuro las intrusiones supongan una pérdida de reputación para la marca, por delante de las disrupciones operativas. La preocupación sobre la pérdida de reputación casi se duplica cuando los entrevistados piensan en el futuro: el 35 por ciento dicen que esto ha sucedido durante los dos últimos años pero el 68 por ciento está preocupado de que pueda suceder en los próximos años (ver Figura 2). El cambio indica que muchos responsables de seguridad sienten temor ante el efecto en aumento de las intrusiones. Cada vez más, las consecuencias no se limitan a las operaciones, sino que se refieren también a la reputación; una reputación dañada puede provocar un descenso de los beneficios si supone pérdida de confianza por parte de los clientes.

Figura 2

Las organizaciones detallaron distintas ramificaciones de las intrusiones durante los dos últimos años, pero esperan que las consecuencias sean diferentes en el futuro



El creciente coste de la infraestructura de seguridad también se convierte en un problema más sustancial en el futuro, con un nivel muy superior al actual. A medida que persiste el riesgo de que las intrusiones tengan éxito, las organizaciones proceden a aumentar el gasto para resolver este problema. Los responsables de seguridad suelen asumir que si sufren una intrusión es porque algo ha fallado y recurren a sustituir personas, soluciones puntuales e infraestructura para no correr riesgos.

Carencias de los sistemas de seguridad

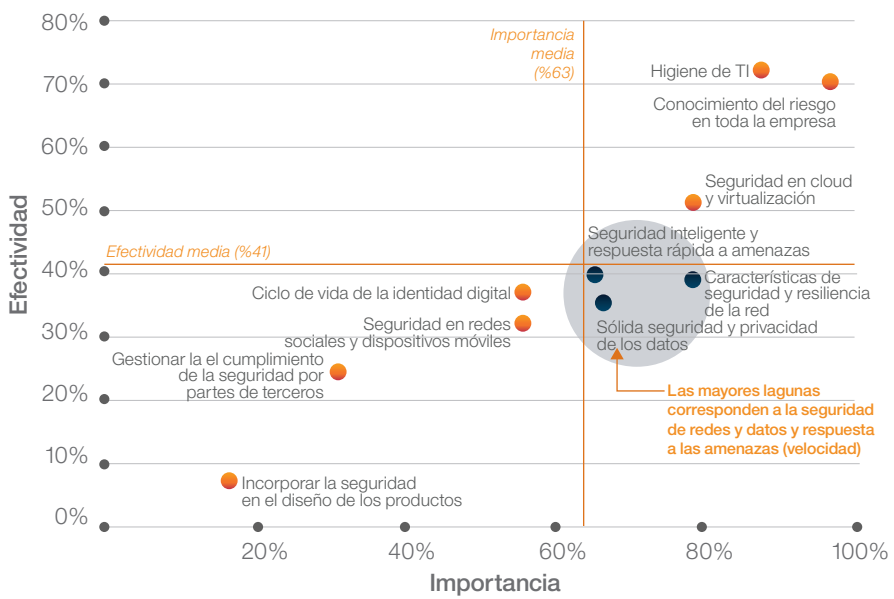
Preguntamos a personas con gran diversidad de responsabilidades relacionadas con la seguridad qué consideran importante en su posición de seguridad y en qué se consideran más eficaces. Generalmente, los responsables de seguridad consideran que han de conceder importancia prácticamente a todo, porque no quieren dejar ningún espacio abierto. Sin embargo, cuando los recursos son limitados, nadie puede mantenerse en primera línea de todas las áreas de forma constante, en especial cuando continuamente surgen nuevas tecnologías, nuevos enfoques y nuevos retos.

La mayoría de los consultados dijeron que se sienten cómodos con la forma en que gestionan la higiene de TI y gestionan el conocimiento de los riesgos en la empresa, los elementos básicos desde el punto de vista tecnológico y organizativo. Las áreas que los consultados consideran importantes, pero que no abordan eficazmente, son las que queremos examinar (ver Figura 3). La protección de la red y los datos, junto con la respuesta ante amenazas caen en esta categoría.

Los consultados dijeron que no son todo lo efectivos que deberían en lo relativo a su velocidad de respuesta ante amenazas, gestión de eventos de seguridad de la información (SIEM), detección de actividad en la red, filtrado y clasificación de datos y prevención de pérdidas. Por supuesto, es vital para las organizaciones mantenerse por delante del cada vez mayor volumen y complejidad de los riesgos para la seguridad; centrándose en sus velocidades de respuesta y gestionando la complejidad mediante mejor analítica de amenazas, las organizaciones pueden reforzar significativamente sus defensas.

Figura 3

Importancia frente a efectividad de distintas capacidades relacionadas con la seguridad



"Hemos desvelado una serie de ahorros de costes tangibles en todos los niveles de la empresa originados en la monitorización y análisis de la seguridad. Hemos reducido los costes de ancho de banda, hemos puesto fuera de servicio recursos con bajo nivel de utilización y hemos aumentado la productividad de los empleados mediante una importante reducción del correo no deseado, por mencionar solo algunos ejemplos".

Responsable de protección financiera, patrimonio y gestión de activos de una empresa canadiense

Gestionar la cuenta de resultados

Los responsables de seguridad tienen una enorme cantidad de cosas en las que centrarse. También anticipan importantes aumentos en los costes de una ciberseguridad eficaz y no creen que estos costes vayan a disminuir en un futuro próximo. El 75 por ciento ha visto aumentar el coste de la ciberseguridad en los dos últimos años y el 84 por ciento prevé que siga aumentando en los próximos dos-tres años. De hecho, más del 70 por ciento de los consultados dedican a ciberseguridad más del 10 por ciento de su presupuesto total para TI (la mayoría entre un 10 y un 15 por ciento). Estos gastos se dedican principalmente a prevención y detección. En un extremo, hemos visto instituciones financieras que gastan anualmente más de 500 millones de USD en ciberseguridad.[2] Más dinero no garantiza necesariamente más protección, por lo que este aumento no es sostenible a largo plazo: los responsables de seguridad van a estar sometidos a mayor presión para justificar sus inversiones.

El 92 por ciento de los consultados dicen que sus solicitudes de fondos para iniciativas de ciberseguridad requieren un rendimiento de la inversión (ROI) u otro análisis financiero para la correspondiente justificación y autorización. Los dos principales factores utilizados para justificar inversiones incluyen una comunicación clara de la actual exposición a riesgos en la organización (según el 61 por ciento de los consultados) y obtener el respaldo de finanzas, gestión de riesgos, operaciones y otros ejecutivos clave (según el 51 por ciento de los consultados). Los responsables de seguridad tienen que comunicar sus necesidades en lenguaje de negocios y asegurarse de contar con el respaldo de otros ejecutivos.[3] En el futuro, deberán buscar nuevas formas de justificar el coste de las inversiones en ciberseguridad y demostrar su valor. Es preciso eliminar la idea de que la seguridad es una simple póliza de seguros o uno de los costes del negocio.

Abordar las deficiencias

La buena noticia es que los responsables de seguridad entrevistados parecen ser conscientes de sus limitaciones y tienen previsto corregirlas en un futuro cercano. Las organizaciones están emprendiendo distintas iniciativas destinadas a mejorar su preparación ante riesgos de ciberseguridad (ver Figura 4). Los esfuerzos actuales se centran principalmente en mejorar el comportamiento de los empleados mediante formación y educación; el 67 por ciento de las organizaciones han emprendido actuaciones de este tipo. El 40 por ciento de los consultados también están implementando software de monitorización de identidades. Estas opciones generalmente se considerarían más fundamentales.

Figura 4

Las iniciativas que están emprendiendo los responsables de seguridad para mejorar la preparación ante riesgos de ciberseguridad

Clasificación hoy		Clasificación en 2-3 años	Iniciativas
1	▼-30%	5	Mejorar los comportamientos de los empleados mediante formación y preparación
2	▼-25%	7	Implementar software de monitorización de identidades (actividad de los usuarios)
3	▲+8%	4	Información sobre las medidas de seguridad operativa / estratégica con nuevas herramientas de análisis
4	▲+28%	1	**Mejorar la monitorización de la seguridad a nivel de red, aplicaciones: y datos**
5	▲+17%	3	**Mejorar la respuesta, procedimientos y velocidad de respuesta ante incidentes**
6	▼-9%	8	Contratar y formar más analistas de seguridad
7	▼-16%	10	Comprobación de la seguridad de las aplicaciones (incluidos dispositivos móviles, API)
8	▲+36%	2	**Crear o renovar las capacidades del SOC**
9	▲+14%	6	Implementar soluciones de seguridad preparadas para la tecnología cognitiva
10	▲+1%	9	Incorporar capacidades forenses en las operaciones de seguridad

"Los ejecutivos son cada vez más reacios a dedicar grandes cantidades de dinero en seguridad, al no tener un feedback positivo de que el gasto anterior haya conseguido resultados tangibles. Los responsables de seguridad han de ir aún más lejos para justificar las inversiones: no basta con realizar una evaluación, identificar carencias y pedir dinero para cubrir estas lagunas".

Chad Holmes, Director de estrategia informática, tecnología y crecimiento (CTO) de Ernst & Young LLP

Durante los próximos dos-tres años está previsto un importante cambio en estas iniciativas de mejora. De hecho, los consultados indicaron que las tres principales iniciativas serán totalmente distintas de las actuales. La número uno será mejorar la seguridad a nivel de redes, aplicaciones y datos, con lo que se identifica el 57 por ciento. Construir o renovar las capacidades del SOC será la número dos. Por último, mejorar la velocidad de respuesta ante incidentes será la futura iniciativa número tres. Las tres áreas se corresponden con las carencias de efectividad identificadas con anterioridad.

Es positivo ver que los responsables de seguridad abordan sus carencias, pero un cambio tan importante en las prioridades puede provocar nuevas lagunas o ampliar las actuales. En cualquier caso, los responsables de seguridad deberán asegurarse de abordar los problemas más relevantes para su negocio. La cuestión real es si estos futuros esfuerzos previstos serán suficientes.

Hacer visibles las carencias

Todos estos desafíos, puntos débiles, esfuerzos y presiones destacan tres carencias críticas: en inteligencia, en velocidad y en precisión. Los responsables de seguridad han de abordar estas carencias gestionando a la vez las presiones relacionadas con costes y ROI.

Falta de inteligencia

- El área más comprometida debido a la falta de recursos es la investigación sobre amenazas, según el 65 por ciento de los consultados.
- El 40 por ciento dice que mantenerse al tanto de las nuevas amenazas y vulnerabilidades constituye un importante problema para la ciberseguridad.

Falta de velocidad

- El primer desafíos para la ciberseguridad hoy y mañana es reducir los tiempos de respuesta y resolución de incidentes, a pesar de que el 80 por ciento dice que las velocidades de respuesta ante incidentes son muy superiores a las de hace dos años.
- Los consultados tienen previsto concentrarse más en esta área en los próximos años. Solo el 27 por ciento dice que ya existen iniciativas para mejorar su respuesta ante incidentes, pero esta cifra aumentará hasta el 43 por ciento en los próximos dos-tres años.

Falta de precisión

- Según los consultados, la segunda área más problemática de la actualidad es optimizar la precisión de las alertas (actualmente hay demasiados falsos positivos).
- El 61 por ciento de los consultados dice que otra área que plantea un importante problema debido a la falta de recursos es la identificación de amenazas, evaluar las amenazas y saber qué incidentes potenciales escalar.

Los beneficios más habitualmente esperados de una solución de seguridad cognitiva

1. Inteligencia
Mejorar las capacidades de toma de decisiones para detección y respuesta ante incidentes

2. Velocidad
Mejorar significativamente los tiempos de respuesta ante incidentes

3. Precisión
Ofrecer mayor confianza para discriminar entre eventos e incidentes reales

3 veces más en la adopción prevista de soluciones de seguridad cognitiva en los próximos 2-3 años

¿Cómo se utilizará la seguridad cognitiva?
Los sistemas cognitivos se utilizarán para analizar tendencias en seguridad y convertir enormes volúmenes de datos estructurados y no estructurados en conocimientos útiles. Los responsables y analistas de seguridad no pueden absorber la información de seguridad existente generada por personas, como documentos de estudios, publicaciones sectoriales, informes de analistas y blogs. Los sistemas cognitivos tratan de combinar esta información con datos de seguridad más tradicionales. Las soluciones de seguridad cognitiva se utilizarán en combinación con tecnologías, técnicas y procesos de seguridad automatizados y orientados a los datos,

Las soluciones de seguridad cognitiva pueden contribuir a aumentar las capacidades de los analistas del SOC ayudándoles a aumentar la velocidad de respuesta, identificar mejor las amenazas, reforzar la seguridad de las aplicaciones y reducir el nivel general de riesgo empresarial. El objetivo es evitar a los analistas las tareas de seguridad más mundanas y repetitivas para que puedan dedicarse a trabajos que precisen una mayor dedicación intelectual.

El momento de las soluciones de seguridad cognitiva

Para cubrir estas carencias se precisan distintas tecnologías y enfoques. A largo plazo, las organizaciones no pueden limitarse a contratar más y más personal para alcanzar sus objetivos. Con la evolución de las tecnologías de inteligencia de seguridad a lo largo de los años, estas han pasado de ser simples controles perimetrales (centrarse en defensas estáticas) a tener capacidades de inteligencia de seguridad más avanzadas (centrarse en desviaciones de los patrones e información en tiempo real).

Hoy estamos comenzando a entrar en la era cognitiva de la seguridad, definida por soluciones que pueden comprender el contexto, comportamiento y significado mediante el análisis de datos de seguridad estructurados y no estructurados. La seguridad cognitiva busca la forma de establecer una nueva colaboración entre los analistas de seguridad y su tecnología. Estas soluciones pueden interpretar y organizar la información y ofrecer explicaciones de su significado, junto con una base sólida para obtener conclusiones. Además, aprende continuamente a medida que se acumulan datos y se derivan informaciones útiles a partir de la interacción.

Beneficios de las soluciones de seguridad cognitiva
Imagine un conjunto de soluciones obtenidas mediante tecnologías cognitivas que le permitan:

- Mejorar las capacidades de los analistas del SOC con menos experiencia proporcionándoles acceso a mejores prácticas e información útil que antes precisaba años de experiencia
- Aumentar la velocidad de respuesta aplicando inteligencia de blogs y otras fuentes para emprender acciones antes de que las signaturas estén disponibles
- Identificar rápidamente amenazas y acelerar la detección de comportamientos peligrosos de los usuarios, exfiltración de datos e infecciones de malware utilizando métodos de análisis avanzados
- Obtener un mayor contexto en torno a los incidentes relacionados con la seguridad mediante automatización de la recopilación y análisis de datos locales y externos.

La promesa y sus problemas

Muchos de los consultados consideran que los beneficios de las soluciones de seguridad cognitiva abordarán las carencias a las que han de hacer frente. Aunque la seguridad cognitiva es un área de tecnología emergente, el 57 por ciento considera que las soluciones de seguridad cognitiva pueden frenar significativamente los esfuerzos de los delincuentes informáticos: ven la promesa y los beneficios potenciales.

Cuando pedimos a los responsables de seguridad que seleccionasen los beneficios de una solución de seguridad cognitiva, el 40 por ciento mencionó la mejora en la detección y las capacidades para la toma de decisiones de respuesta ante incidentes, el 37 por ciento indicó la importante mejora de los tiempos de respuesta ante incidentes y el 36 por ciento mencionó el aumento de confianza para discriminar entre eventos e incidentes reales. Los consultados quieren soluciones de seguridad cognitiva capaces de abordar sus principales carencias. Necesitan la ayuda de estas soluciones mediante inteligencia, velocidad y precisión.

Hoy, solo el siete por ciento de los consultados trabajan en implementar soluciones de seguridad cognitiva para aumentar su preparación ante riesgos relacionados con la ciberseguridad. Esto es de esperar, ya que se trata de una capacidad muy reciente. Sin embargo, en un futuro cercano, la cifra de los interesados en implementar estas soluciones se multiplica por tres, hasta alcanzar el 21 por ciento. A lo largo de los próximos años veremos acelerarse la adopción, a medida que los responsables de seguridad utilicen esta capacidad para mejorar sus sistemas inmunes digitales.

Los consultados también vieron potenciales problemas para la adopción de soluciones de seguridad cognitiva. No es que los responsables de seguridad no comprendan los conceptos de la tecnología ni que no estén convencidos de su valor o beneficios respecto a otras soluciones; los problemas se refieren más bien a las destrezas, procesos y métodos. El 45 por ciento de los encuestados dijeron que los principales problemas para la adopción son no estar preparados desde la perspectiva de las competencias y la falta de destrezas internas que implementar (ver Figura 5). Para apaciguar estas preocupaciones deberá contarse con una mayor formación y preparación.

Figura 5

Los responsables de seguridad identificaron los principales problemas para la implementación de soluciones de seguridad cognitiva

"Estamos bien posicionados para emprender el próximo paso con soluciones cognitivas inteligentes capaces de recibir, organizar ycontextualizar una enorme cantidad de datos relacionados con la seguridad que actualmente consumen gran cantidad de tiempo y recursos".

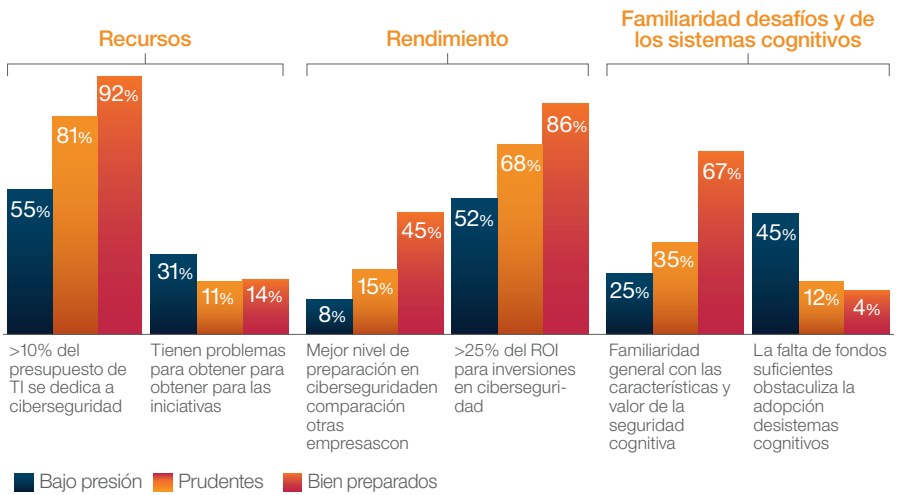
Responsable de protección financiera, patrimonio y gestión de activos de una empresa canadiense

Bien preparados para la era cognitiva

Para comprender quién está preparado para dar ya el salto a la era cognitiva de la seguridad, creamos perfiles para nuestros entrevistados basándonos en el nivel de eficacia de la seguridad, comprensión de los sistemas cognitivos y preparación que ellos mismos nos indicaron. El análisis de las respuestas reveló tres grupos diferenciados (ver Figura 6).

Figura 6

Dividimos las organizaciones en Bajo presión, Prudentes y Bien preparadas según su nivel de preparación



El grupo *Bajo presión*, que abarca el 52 por ciento de nuestra muestra, se caracteriza por sus problemas de financiación y personal y un menor conocimiento general de las características y valor de la seguridad cognitiva. Generalmente dedican a ciberseguridad un porcentaje menor del presupuesto de TI y tienen mayor probabilidad de encontrarse con problemas para obtener fondos suficientes y satisfacer sus necesidades de personal. También mencionaron la falta de fondos suficientes como obstáculo para la adopción de

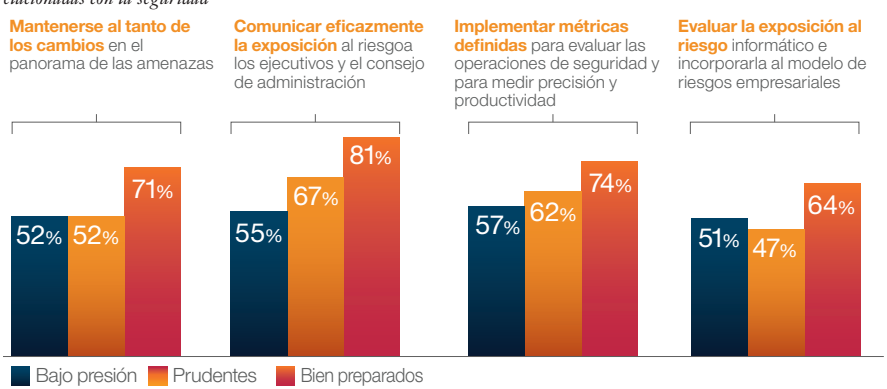
sistemas cognitivos (Encontrará información detallada sobre cómo establecimos y definimos estos grupos en la sección 'Demografía y metodología' en la página 20).

El grupo *Prudentes*, que constituye el 27 por ciento de la muestra, no tiene los mismos problemas de recursos que el grupo Bajo presión, pero aún no están suficientemente preparados para implementar la próxima generación de seguridad cognitiva.

El grupo *Bien preparados*, el 22 por ciento de la muestra, es el que muestra más conocimientos y entusiasmo sobre las soluciones de seguridad cognitiva. Este grupo está más familiarizado con la seguridad cognitiva y tiene más confianza, presupuesto y ROI que los otros. Consideran que sus prácticas de seguridad son más maduras, y un elevado porcentaje dice que su equipo de operaciones de seguridad es capaz de mantenerse al ritmo de los cambios en el panorama de las amenazas. Comunican eficazmente a los directivos y consejos de administración cuál es la exposición al riesgo e incorporan la exposición al riesgo informático en su modelo de riesgos empresariales (ver Figura 7).

Figura 7

Las organizaciones Bajo presión, Prudentes y Bien preparadas indican sus distintas formas de enfocar las prácticas relacionadas con la seguridad



"Hay mucho ruido ahí fuera; el cerebro humano no puede procesarlo todo a diario. Necesitamos algo que nos ayude, como la inteligencia artificial o las tecnologías cognitivas".

Chad Holmes, Director de estrategia informática, tecnología y crecimiento (CTO) de Ernst & Young LLP

"La naturaleza ininterrumpida ypermanente de las operaciones de seguridad suponen un problema que para la mayoría de las organizaciones supone un importante coste laboral, que es donde radica el atractivo de la seguridad cognitiva: nunca descansa".

Michael Pinch, Director de seguridad de la información de la Universidad de Rochester

¿Qué esperan y desean los responsables de seguridad de las soluciones de seguridad cognitiva en los primeros pasos de la implementación? En conversaciones con el grupo Bien preparados, encontramos que querían soluciones de seguridad cognitiva capaces de:

- Funcionar ininterrumpidamente y ofrecer asistencia continua
- Ayudar a reducir los falsos positivos y encontrar anomalías en los comportamientos
- Comprender mejor el panorama de amenazas y ofrecer contexto para los incidentes
- Soportar tareas de gobierno, gestión de riesgos y conformidad, basándose en los requisitos particulares de su sector, zona geográfica y normativa
- Cambiar la naturaleza del trabajo de seguridad y ayudar a los analistas a trabajar de forma más inteligente y ofrecer un nivel de valor más elevado.

Es de esperar que los responsables de seguridad con más madurez y menos limitaciones de recursos sean los primeros en explorar una tecnología emergente como la seguridad cognitiva. Sin embargo, es importante advertir que, con más experiencia y conocimientos, todos pueden aplicar las tecnologías cognitivas para abordar sus carencias y extender los límites del análisis para mejorar sus operaciones de seguridad.

Recomendaciones

Exploramos el actual panorama de la seguridad para comprender los problemas, presiones y prioridades de nuestros entrevistados. Basándonos en estas observaciones, hemos recopilado una serie de recomendaciones que le ayudarán a usted y a su organización a estar mejor preparados para la era cognitiva de la ciberseguridad.

Reconozca sus puntos débiles
Los responsables de seguridad quieren aumentar su capacidad de respuesta y reducir complejidades, y están cada vez más preocupados por la pérdida de reputación como consecuencia de este tipo de incidentes. Examine los principales puntos débiles y vulnerabilidades de su organización. ¿Qué conexiones existen? ¿Cuáles son las prioridades?

- ¿Carece de la información e investigación sobre amenazas que necesita?
- ¿Sus tiempos de respuesta y resolución de incidentes son adecuados para sus operaciones?
- ¿Tiene problemas para discriminar entre eventos e incidentes reales o para poner las cosas en un contexto adecuado?

Documéntese sobre las capacidades de la seguridad cognitiva
Adopte un enfoque holístico y formal para informarse sobre las soluciones de seguridad cognitiva. Podría haber en su organización ideas erróneas desde el punto de vista de las capacidades, coste e implementación.

- Comprenda los casos de uso potenciales para las soluciones de seguridad cognitiva y correlaciónelos con sus puntos débiles. ¿Necesita más contexto para los incidentes relacionados con la seguridad, mejor evidencia para tomar decisiones más informadas o nuevas formas de evaluar el riesgo proactivamente?
- Prevea cómo puede comunicar los beneficios de las soluciones de seguridad cognitiva a los responsables técnicos y de negocio: prepare un plan de formación para su equipo y sus directivos

"La seguridad cognitiva tiene un enorme potencial: le permite dar solución a la falta de personal, reducir el perfil de riesgo y dar una respuesta más eficaz. Puede ayudarle a comprender la historia narrativa. Las personas consumen historias: sucedió esto, luego sucedió esto, tuvo este impacto, y lo hizo esta persona. Asimismo, los sistemas cognitivos pueden reducir el nivel de especialización necesario para trabajar en ciberseguridad. Le permite It aportar nuevas perspectivas de entornos distintos de TI para resolver el problema".

David Shipley, Director de iniciativas estratégicas y servicios de tecnología de la información de la Universidad de New Brunswick

- Identifique y aborde las lagunas en cuanto a personal especializado que puedan estar retrasando la adopción de la tecnología desde dentro de su propia organización

Defina un plan de inversiones
Es difícil justificar una inversión cuando se trata de una tecnología nueva y no demostrada en el mercado: usted no dispone de muchos ejemplos puede ser difícil conseguir la confianza de las partes interesadas. Como la gran mayoría de nuestros entrevistados dijo que sus solicitudes de fondos precisan un ROI u otro análisis financiero, es imperativo que los responsables de seguridad adopten un enfoque diferente para las soluciones de seguridad cognitiva.

- Trate las soluciones de seguridad cognitiva como algo claramente diferenciado. No se centre solo en la justificación tradicional de las inversiones en seguridad, como el coste de las reparaciones. En vez de ello, céntrese en que la seguridad cognitiva puede mejorar la efectividad general de las operaciones de seguridad
- Presente el plan de formación que haya desarrollado y utilícelo para conseguir la colaboración de otros ejecutivos y consiga que le ayuden a prepara la justificación comercial
- Sea creativo y busque formas novedosas en que su inversión en seguridad cognitiva ayudará a la empresa, además del ROI.

Trate de aumentar sus capacidades, independientemente del grado de madurez
Las empresas que identificamos como Bien preparadas tendían a tener más recursos a su disposición, más confianza en sus capacidades y estaban preparados para implementar hoy soluciones de seguridad cognitiva, pero esto no significa que la seguridad cognitiva sea solo para un grupo selecto. Las soluciones de seguridad cognitiva son un área de tecnología emergente y sus características únicas pueden beneficiar a organizaciones de todos los tamaños.

- *Si está Bajo presión:* Identifique medidas empresariales específicas y carencias de destrezas que las soluciones de seguridad cognitiva podrían contribuir a mejorar, y a continuación prepare la justificación comercial.
- *Si es Prudente:* Céntrese en informarse para reducir la ansiedad en torno a las carencias de destrezas
- *Si está Bien preparado:* Canalice su entusiasmo, escoja un caso de uso muy específico para una implementación piloto y asegúrese de que no quede aislada de las operaciones generales de seguridad.

Más información
Para obtener más información sobre el estudio del IBM Institute for Business Value, diríjase a iibv@us.ibm.com. Siga a @IBMIBV en Twitter; y si desea un catálogo completo de nuestra investigación o si desea suscribirse en nuestro boletín mensual, visite: **ibm.com**/iibv.

Acceda a los informes ejecutivos de IBM Institute for Business Value desde su dispositivo móvil descargando las apps gratuitas 'IBM IBV' para teléfono o tablet iPad o Android desde su app store.

El socio adecuado para un mundo cambiante
En IBM colaboramos con nuestros clientes para fusionar perspectivas empresariales, investigaciones avanzadas y tecnologías para ofrecerles una ventaja clara en el entorno de cambios rápidos de hoy día.

IBM Institute for Business Value
El IBM Institute for Business Value, parte de los IBM Global Business Services, elabora análisis estratégicos basados en hechos para ejecutivos de alto nivel sobre problemas críticos dentro del sector público y privado.

Colaboradores
Lisa van Deth, Program Marketing Manager y Campaign & Thought Leadership Strategy de IBM Security; Christophe Veltsos, profesor asociado del Departamento de Ciencias de la Computación en la Universidad Estatal de Minnesota, Mankato.

Agradecimientos
Caleb Barlow, Vicepresidente, de WW Portfolio Marketing de IBM Security; Maria Battaglia, CMO de Resilient, IBM Security; Wangui McKelvey, Director de Portfolio Marketing - Security Services & Web Fraud en IBM Security; Kevin Skapinetz, Director of Strategy de IBM Security; Oxford Economics por su asistencia en la administración de la recogida de datos.

Notas y fuentes

1 "2016 Cost of Data Breach Study: Global Analysis" (Estudio sobre el coste de las filtraciones de datos: Análisis global). Ponemon Institute. Junio de 2016. http://www-03.ibm.com/security/data-breach/

2 Friedman, Gabe. "JPMorgan Chase Atty: Bank Will Spend $500M on Cyber Security" (JPMorgan Chase Atty: Bank gastará 500 millones de dólares en ciberseguridad). 29 de enero de 2016. https://bol.bna.com/jpmorgan-chase-atty-bank-will-spend-500m-on-cyber-security/. Consultado el 21 de septiembre de 2016.

3 Kelley, Diana y Carl Nordman. "Securing the C-suite: Cybersecurity perspectives from the boardroom and C-suite" (Proteger a la alta dirección: las perspectivas sobre ciberseguridad del consejo de administración y la alta dirección). IBM Institute for Business Value. 2016. ibm.biz/csuitesecurity

Demografía y metodología
Para comprender mejor los retos relacionados con la seguridad a los que se enfrentan las empresas, cómo están abordando estos retos y cómo consideran las soluciones de seguridad cognitiva y su potencial, el IBM Institute for Business Value y Oxford Economics hicieron un estudio entre una distribución equilibrada de 700 directores de seguridad informática y otros profesionales de la seguridad en 35 países representando a 18 sectores entre mayo y julio de 2016.

Para desterminar nuestros grupos (Bien preparados, Prudentes y Bajo presión), aplicamos un algoritmo de agrupamiento en k medias que reveló tres patrones de comportamiento diferenciados. Estos patrones de comportamiento se basaron en preguntas relacionadas con la efectividad de la seguridad, el conocimiento de los sistemas cognitivos y la preparación para estos sistemas cognitivos.

Acerca de los autores
Diana Kelley es asesora ejecutiva de seguridad (ESA) de IBM Security y directora de la IBM Security Newsroom. Como ESA, hace uso de sus más de 25 años de experiencia en seguridad informática par asesorar y orientar a directivos de seguridad informática y profesionales de la seguridad. Ha contribuido en el informe IBM X-Force y con frecuencia publica artículos muy influyentes en el blog Security Intelligence. Actualmente colabora como personal docente en IANS Research y participa en la Junta Asesora de InfoSec World y en el Comité de Contenidos del Executive Women's Forum. Diana es ponente habitual en conferencias sobre seguridad y ha sido citada como experta en seguridad en el *New York Times, TIME*, MSNBC.com, *la revista Information Security* y *el Wall Street Journal*. Es coautora del libro *Cryptographic Libraries for Developers (Bibliotecas de criptografía para desarrolladores)*. La dirección de contacto de Diana es drkelley@us.ibm.com.

Vijay Dheap es director de programas en la División de Seguridad de IBM y está especializado en transformar tecnologías emergentes en productos comerciales. En la actualidad dirige una cartera de productos de Inteligencia de seguridad que abarcan Analítica avanzada, Sistemas cognitivos y SaaS. Con anterioridad dirigió las divisiones de análisis forense informático y seguridad móvil. Vijay es un apasionado de la tecnología y ha sido nombrado IBM Master Inventor. Su cartera de patentes incluye innovaciones para dispositivos móviles, colaboración empresarial y seguridad. Consiguió un MBA internacional en la Duke Fuqua School of Business y tiene un máster en ingeniería informática por la Universidad de Waterloo (Canadá). La dirección de contacto de Vijay es vdheap@us.ibm.com.

David Jarvis es Security and CIO Lead del IBM Institute for Business Value. Es responsable del desarrollo y ejecución de un programa que explora temas empresariales y tecnológicos en estas áreas. Es un apasionado experto en el desarrollo y gestión de informaciones útiles de los mercados, liderazgo de ideas y proyectos de previsión estratégica y ha ocupado numerosos cargos en IBM dentro de estas áreas. Es autor de numerosos informes sobre seguridad muy influyentes, como el 2012 – 2014 IBM CISO Assessments. Además de sus responsabilidades en investigación, David es profesor de previsión empresarial y soluciones creativas de problemas. La dirección de contacto de David es djarvis@us.ibm.com.

Carl Nordman es director global del C-suite Study Program y CFO Research Lead del IBM Institute for Business Value. Es responsable de la realización de investigaciones primarias en ambos campos. Dirige estudios encaminados a descubrir tendencias y perspectivas sobre temas estratégicos actuales. Carl tiene más de 25 años de experiencia en riesgo y fraude financiero. Anteriormente ocupó distintos cargos en IBM Consulting Services, trabajando con directores financieros de empresas del Fortune 1000 y ejecutando servicios de optimización financiera y contable como ejecutivo de cuenta para distintos clientes. La dirección de contacto de Carl es carl.nordman@us.ibm.com.

IBM España S.A.
Hortensia 26-28
28002 Madrid,
España

El sitio web de IBM está disponible

en **ibm.com**/es

SEL03111-ESES-00