MARKET PERSPECTIVE

# WAF del lado del cliente: la siguiente frontera en seguridad

Christopher Rodriguez

## RESUMEN EJECUTIVO

## FIGURA 1

**Resumen ejecutivo: Amenazas del lado del cliente y soluciones emergentes**

En el 2018, los investigadores de seguridad identificaron una nueva forma de ciberdelito llamado clonación de tarjetas en línea o web skimming. Los ataques de Magecart aprovecharon una tendencia creciente para cambiar la funcionalidad de las aplicaciones desde el servidor hacia el cliente. Los agentes de amenazas pudieron inyectar códigos maliciosos en las fuentes de aplicaciones de confianza, el cual se ejecutó en los navegadores de los usuarios que no tenían la protección de una WAF. Finalmente, los ataques representaron una filtración de datos prolongada que expuso un punto débil en las prácticas de seguridad de las aplicaciones web empresariales.

### Conclusiones clave

- Los scripts del lado del cliente son una herramienta valiosa en la arquitectura de las aplicaciones, la cual ofrece los beneficios de una mejor experiencia de usuario, rendimiento de la aplicación, análisis y seguridad.
- Los scripts están por todas partes. En la actualidad, los sitios web tienen decenas de scripts diferentes, en donde los scripts de terceros representan hasta dos de cada tres scripts.
- Los scripts del lado del cliente representan un ecosistema de funcionalidad susceptible pero dinámico, con muchos interesados.
- Existen prácticas recomendadas de referencia para la seguridad del lado del cliente. Sin embargo, las complejidades y los desafíos de la seguridad del lado del cliente impulsarán la demanda de soluciones de seguridad empresarial para este vector de amenazas.

### Acciones recomendadas

- Las soluciones disponibles en el mercado varían drásticamente según la funcionalidad. Para los compradores, el objetivo principal es llegar a un equilibrio entre la seguridad y el requisito comercial de "no romper cosas".
- La visibilidad y el control del lado del cliente no son un área fácil ni familiar para muchos proveedores. Los nuevos candidatos del mercado deberán considerar cuidadosamente si deben crear sus propias soluciones o si deben adquirir o asociarse con las capacidades existentes.
- Muchas organizaciones de TI carecen de información sobre los scripts o los entornos del lado del cliente. Pocas comprenden los problemas de seguridad. Se requiere un alto grado de educación en el mercado que incluye demostraciones, investigación, pruebas de concepto y versiones de prueba.

Fuente: IDC, 2021

April 2021, IDC #US47623221

## NUEVOS DESARROLLOS Y DINÁMICAS DEL MERCADO

Esta perspectiva de mercado de IDC proporciona un análisis del vector de amenazas, de las soluciones emergentes y del futuro del mercado de *firewall* de aplicaciones web (WAF, por sus siglas en inglés) del lado del cliente.

Akamai, Cymatic, PerimeterX y Tala Security están abriendo nuevos horizontes mediante la extensión de la protección de WAF para abordar las amenazas del lado del cliente. Los *scripts* del lado del cliente representan un vector de amenazas emergente, y el mercado de la seguridad está evolucionando para atender tal necesidad.

Estas soluciones de seguridad se denominan categóricamente *"WAF del lado del cliente", anti-scripting* o *seguridad de scripts*, pero la terminología puede ser confusa. Considere las siguientes opciones:

- El WAF evoca un conjunto específico de controles que se emplean en las aplicaciones web, aunque los *scripts* del lado del cliente son inherentemente un punto de control diferente en el paradigma de seguridad de las aplicaciones.
- "WAF del lado del cliente" es un término útil para establecer una conexión con un control de seguridad bien establecido en el WAF, mientras que el término "seguridad de *scripts*" puede ser difuso y confuso en comparación.
- El *anti-scripting* generaliza los *scripts* como una tecnología no deseada, defectuosa o completamente maliciosa. En realidad, los *scripts* representan una herramienta valiosa y potente en la arquitectura de las aplicaciones.

En general, IDC se refiere a estas soluciones como WAF del lado del cliente, principalmente por las ventajas de familiaridad asociadas al WAF. Además, el término "WAF del lado del cliente" mantiene la posibilidad de una futura expansión de los tipos de amenazas del lado del cliente que van más allá de los *scripts*.

## Introducción

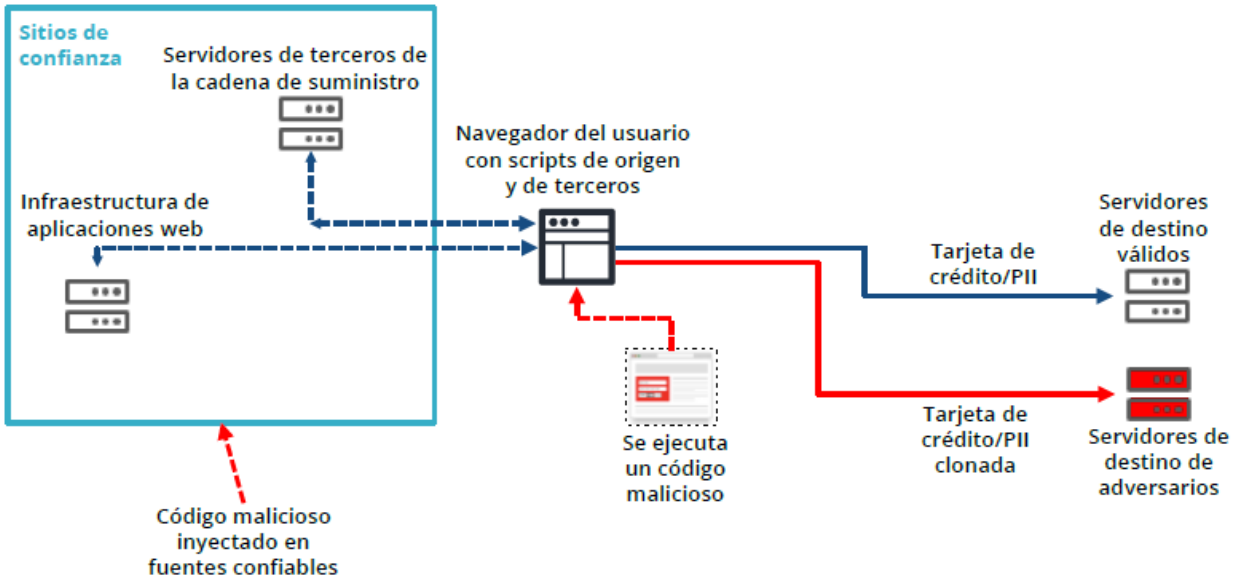
En el 2018, surgió una nueva técnica de clonación de datos de tarjetas de pago que se atribuyó al grupo de *hackers* Magecart. Los ataques de Magecart aprovecharon un nuevo vector de amenazas: los *scripts* que se ejecutan en los navegadores de clientes. Una vez que se detectó la campaña de ataque, las investigaciones demostraron que el grupo Magecart había comprometido los sitios web de grandes empresas online durante meses, incluidas Ticketmaster, NewEgg y British Airways.

La campaña de Magecart utilizó ataques del lado del cliente para realizar *web skimming* (que también se conoce como clonación de tarjeta en línea o como *formjacking*). El *web skimming* es un aspecto muy visible de este vector de amenazas, pero el vector de amenazas facilita otros ataques, tales como los ataques de abrevadero y la minería de criptomonedas maliciosa. El objetivo de estos ataques puede variar, pero, en general, la seguridad del lado del cliente tiene potencial para campañas de robo de datos que generan enormes filtraciones de datos prolongadas.

En la figura 2, se ofrece una descripción general del ciclo de vida de un ataque del lado del cliente. Obsérvese que el código malicioso se ejecuta en el navegador, lejos de las protecciones que brinda un WAF. Además, el código malicioso se puede inyectar en fuentes externas e internas.

## FIGURA 2

**Anatomía de un ataque de *web skimming* (dentro del navegador)**




Fuente: Akamai, 2021

## Dinámica de la industria

El WAF del lado del cliente es un mercado emergente con un fuerte potencial de crecimiento. Esta tecnología aborda un vector de amenazas emergente, que es el resultado de un cambio en las prácticas de desarrollo de aplicaciones. La funcionalidad de las aplicaciones ha estado pasando de los servidores a los clientes en los últimos años y es poco probable que la tendencia se ralentice. El cambio en la funcionalidad desde el servidor hacia el cliente libera las demandas de rendimiento del servidor, lo que permite un mejor funcionamiento y una experiencia más interactiva para los usuarios finales. Como resultado, los *scripts* son herramientas cada vez más populares que impulsan experiencias interactivas en línea. Los *scripts* se utilizan para un amplio y variado conjunto de fines legítimos, incluidos el seguimiento, el análisis, la experiencia de usuario y la seguridad. Actualmente, los *scripts* son muy comunes en los sitios web, ya que estos contienen 15 o más *scripts* diferentes, según algunas estimaciones.

Además, la simplicidad de JavaScript ha impulsado la adopción del *scripting* por parte de profesionales que no pertenecen a la TI. Los *scripts* permiten que las unidades empresariales distintas del departamento de TI creen e inserten un código en los activos web para diversos propósitos. Los *scripts* también permiten una integración e inserción más fáciles de los servicios de terceros. Sin embargo, se sigue ignorando en gran medida el aspecto de la seguridad de los *scripts*, en especial entre las organizaciones que siguen centrándose en herramientas esenciales como el WAF.

En general, la amenaza no se comprende bien. Las filtraciones más ampliamente analizadas en esta categoría se centran en los *scripts* de terceros. La campaña de Magecart ofrece un ejemplo pertinente. En ese caso, los *hackers* de Magecart tenían acceso al código de un socio proveedor de la organización objetivo y pudieron insertar un código malicioso en *scripts* de confianza. A algunas organizaciones, el vector de amenazas puede parecerles una práctica para "cambiar las reglas del juego". Proteger un sitio web contra las diversas amenazas que enfrentan las grandes empresas en línea ya no es una tarea trivial, y el requisito de considerar las vulnerabilidades en los sistemas asociados parece prácticamente injusto. Los *scripts* de terceros son los más problemáticos, ya que las organizaciones de TI carecen de visibilidad o control sobre el código, las actualizaciones o los cambios de los socios.

Lamentablemente, el *web skimming* es solo una parte del problema, ya que los *scripts* de terceros representan solo una demografía de los *scripts* presentes en la mayoría de las páginas web. Como referencia, los investigadores de Akamai han estimado que alrededor del 67% de los *scripts* proviene de terceros. En última instancia, la mayoría de las páginas web son un ecosistema de *scripts* provenientes de interesados internos y de terceros. Estos sistemas internos también pueden enviar código malicioso si se piratean los servidores.

Existen algunas prácticas recomendadas que pueden ayudar a reducir el riesgo. Un control más estricto de los *scripts* de terceros es un comienzo inteligente. Las revisiones de los códigos y las pruebas de aplicaciones frecuentes también son prácticas confiables. Además, las organizaciones de TI pueden aprovechar las tecnologías, como Subresource Integrity (SRI), para hacer hash y detectar cambios en los *scripts*. Si bien estas opciones pueden proporcionar una protección de referencia necesaria, el historial ha demostrado que los sofisticados agentes de amenazas emplean de manera consistente tácticas inteligentes y avanzadas para evitar la detección. Como resultado, la SRI y otras prácticas son inicios útiles, pero son limitadas frente a ataques avanzados.

Además, es poco probable que los agentes de amenazas hagan una pausa en sus esfuerzos, a menos que se vean forzados a hacerlo. Desde los ataques de Magecart que acapararon los titulares, los *hackers* han modificado estos ataques de muchas maneras. Por ejemplo, los *hackers* pueden apuntar a las redes de publicidad como medio para inyectar un código malicioso a través de anuncios publicitarios. Otros medios incluyen apuntar a repositorios de código, como GitHub. Estos repositorios incluyen bibliotecas de código abierto y segmentos de códigos que muchas organizaciones utilizan y en las que confían generalmente para usar en sus aplicaciones web. Como resultado, estas fuentes confiables representan un posible vehículo para inyectar *scripts* maliciosos en sitios web que parecieran ser seguros.

Cada proveedor aborda el problema de manera ligeramente diferente. Las soluciones en la tendencia del mercado se implementan en gran medida a través de etiquetas JavaScript, que permiten insertar la función de seguridad antes de que se puedan ejecutar los *scripts*. Desde allí, las soluciones difieren drásticamente. Las capacidades principales tienden a incluir la visibilidad y asignación de *scripts* y comunicaciones (por ejemplo, origen y destino). Las capacidades adicionales incluyen la gestión de vulnerabilidades, el cumplimiento de políticas y la detección de actividad maliciosa y eventos sospechosos. Es posible contar con capacidades más avanzadas, como el cifrado de claves y datos incorporados, la ofuscación de códigos, el uso de entornos aislados y otras medidas de defensa. Por ahora, parece que el enfoque es proporcionar suficiente visibilidad y automatización de las capacidades principales de seguridad. Si bien, con el tiempo, se le podría dar la bienvenida a medidas de detección más sofisticadas, el énfasis sigue estando en proporcionar suficiente seguridad sin interrumpir la experiencia del usuario final ni "romper" la funcionalidad del sitio web.

## Ejemplos de proveedores

Actualmente, existen algunas ofertas comerciales para el WAF del lado del cliente que varían en cuanto al alcance y la capacidad. Hay varios especialistas en el mercado, como Digital.ai (anteriormente denominado Arxan), Source Defense, Cymatic, Tala Security y ChameleonX (adquirido por Akamai en el 2019). Otros tienen amplias carteras de seguridad de aplicaciones web. Por ejemplo, Akamai presentó Page Integrity Manager en el 2020 como parte de su enfoque para la protección contra los ataques multivectoriales a través de una aplicación web holística y una cartera de seguridad de API. De manera similar, PerimeterX presentó su oferta en el 2019 como complemento de su solución empresarial de administración de *bots*. El nuevo participante es Cloudflare, que presentó su nueva solución en marzo del 2021. IDC señala que estas empresas tienen antecedentes en la administración de *bots* que pueden haber ayudado a proporcionar un nivel de familiaridad con las señales de seguridad del lado del cliente. La administración de *bots* es un proceso desafiante para hacerlo bien y las mejores soluciones tienden a emplear múltiples técnicas (incluido JavaScript) para detectar y categorizar el comportamiento de los *bots*.

Los ataques del lado del cliente pueden ser difíciles de detectar. Sin embargo, una vez que se detectan, estas amenazas son bastante claras en términos de los costos financieros para las empresas afectadas y sus clientes. Por ejemplo, estos tipos de filtraciones de datos a menudo se pueden medir en términos de la cantidad de registros de clientes robados. Los competidores existentes en el espacio han demostrado un alto grado de eficacia en la detección y mitigación de amenazas basadas en los *scripts*. Esto hace que los agentes de las amenazas enfoquen sus esfuerzos en otros lugares, lo que da como resultado un juego similar al de “aplasta al topo” en la industria. Para los atacantes, el objetivo es encontrar sitios web no seguros o poco seguros que atacar. A pesar de la visibilidad de los ataques de Magecart, el conocimiento del mercado sobre el vector de amenazas sigue siendo bajo, lo que les permite a los agentes de amenazas encontrar nuevos objetivos. Es probable que todos estos factores aumenten el conocimiento general del vector de amenazas, lo que impulsará la demanda y atraerá empresas adicionales al mercado en los próximos años.

## Estrategias de mercado

Las amenazas del lado del cliente serán un desafío para las grandes empresas en línea mientras los ciberdelincuentes perciban que el vector de ataque es rentable. Sin embargo, este es un tipo de ataque más dirigido que los ataques masivos transmitidos, como el *malware* de rescate. Llevará tiempo para que la mayoría de las organizaciones objetivo detecten y mitiguen los ataques basados en los *scripts*. También requerirá tiempo y esfuerzo que el conocimiento general del mercado sobre estos problemas aumente. Los proveedores tienen el desafío de generar conciencia a través de la educación continua, las demostraciones y la examinación de las pruebas de concepto.

Es probable que más empresas presenten sus propios productos y capacidades. Akamai presentó Page Integrity Manager hace un año para abordar la creciente superficie de ataque creada por *scripts* cargados en navegadores, en los que se envía información de identificación personal (PII, por sus siglas en inglés) y se accede a esta. También es donde las amenazas del lado del cliente han proliferado en el 2020, ya que el uso de internet para realizar transacciones se impulsó en el entorno de la COVID-19.

Cloudflare es la incorporación más reciente al mercado y presenta una nueva solución llamada Cloudflare Page Shield. Antes de este acuerdo, Cloudflare abordó este vector de amenazas a través de una asociación tecnológica con Tala Security.

Aunque Cloudflare ha decidido desarrollar sus propias capacidades de seguridad del lado del cliente, IDC señala que el enfoque puede no ser tan fácil de seguir para los demás. Para la mayoría de los proveedores del mercado, el desarrollo del WAF del lado del cliente fue precedido por técnicas de detección de *bots* que aprovechan los clientes de JavaScript. Las soluciones de WAF heredadas no tienen estas capacidades ni otras experiencias con el código del lado del cliente.

En el caso de los proveedores que están reforzando sus líneas de productos de seguridad de API y de aplicaciones web, la adquisición de soluciones especializadas puede presentar la mejor opción incluso para el campo de juego. La adquisición de ChameleonX por parte de Akamai proporciona un ejemplo de los posibles beneficios de la combinación de tecnologías especialmente diseñadas con la amplitud de la nube. Page Integrity Manager ahora protege más de 3700 millones de visualizaciones de páginas cada mes mediante el análisis de 6400 millones de ejecuciones de *scripts* cada día. Cada semana se observan aproximadamente 40 millones de interacciones sospechosas y maliciosas de usuario final, lo que le permite a Akamai proporcionar notificaciones en tiempo real, análisis de la causa raíz, mitigación inmediata y creación de políticas de automatización.

## EL PUNTO DE VISTA DE IDC

Los ataques del lado del cliente serán una creciente brecha de seguridad mientras que los ciberdelincuentes perciban que el vector de ataque es rentable, lo que podría durar muchos años. Una razón importante para esto es el hecho de que no se comprende bien el vector de amenazas del lado del cliente. Tradicionalmente, las soluciones de WAF funcionan mediante el análisis del tráfico de aplicaciones web dirigido al servidor web. A medida que JavaScript se ha vuelto más popular a lo largo de los años, grandes cantidades de funcionalidad han migrado al navegador del cliente. Sin embargo, muchas organizaciones pasan por alto estos hechos o no han realizado una evaluación adecuada de los riesgos y las consecuencias en la seguridad de esta migración de la funcionalidad web al navegador del cliente.

El hecho de que este tipo de ataque sea más específico que los ataques transmitidos a gran escala, como el *malware* de rescate, contribuye aún más a los altos niveles de confusión del mercado. Por ejemplo, la mayoría de las organizaciones están bien familiarizadas con los tipos de ataques que abordan las soluciones de mitigación de ataques de WAF y DDoS. El riesgo de seguridad que presentan los *bots* no deseados o maliciosos es otra práctica que está ganando conciencia general. Sin embargo, las áreas más nuevas, como la seguridad de API y la seguridad del lado del cliente, representan áreas emergentes de riesgo que simplemente no son visibles y, por lo tanto, presentan un riesgo significativo, muy similar a la mitad sumergida de un iceberg (consulte la figura 3).

## FIGURA 3

### El iceberg de la seguridad de las API y las aplicaciones web


Fuente: IDC, 2021

Una vez que una organización entiende el posible vector de amenaza, el proceso de catalogar y comprender los *scripts* que se ejecutan en un entorno de TI complejo con varios dominios, páginas web y aplicaciones web puede representar una tarea heroica. En el momento de los ataques de Magecart, el proceso de detección de los *scripts* maliciosos inyectados representó una revisión manual línea por línea del código para detectar cambios. El proceso ahora es más eficiente, ya que los investigadores comprenden los problemas subyacentes y las prácticas recomendadas. Sin embargo, el punto sigue siendo que se requerirá tiempo para que la mayoría de las organizaciones objetivo detecten y mitiguen los ataques basados en los *scripts*, ya que se necesita tiempo para comprender el vector de amenaza y tiempo adicional para identificar cualquier brecha de seguridad o vulnerabilidad existente. Además, el vector de amenaza es un objetivo en movimiento, ya que el 75% de los *scripts* se cambia cada trimestre. Cada nuevo cambio abre la posibilidad de introducir nuevas vulnerabilidades y códigos maliciosos.

Sin embargo, el tiempo es esencial. Las brechas conocidas debido a los ataques del lado del cliente fueron duraderas y les proporcionaron a los atacantes meses de ventaja. En ese momento, se robaron un número incontable de tarjetas de crédito, así como otra PII. Una vez que se detecta un ataque, los atacantes pueden cesar sus actividades y empezar de nuevo con la siguiente víctima. Básicamente, los ataques del lado del cliente tienen un tiempo masivo para la detección y este desequilibrio es una enorme ventaja para los ciberdelincuentes que debe reducirse.

Por lo tanto, el tiempo es el mayor obstáculo para la industria de la seguridad con el fin de educar y mejorar la conciencia del comprador sobre el problema. Los proveedores tienen el desafío de generar conciencia a través de la educación continua, las demostraciones y la examinación de las pruebas de concepto. Akamai, por ejemplo, ofrece una versión de prueba gratuita de Page Integrity Manager. La solución proporciona una descripción general del ecosistema de *scripts* de las páginas web objetivo, junto con un análisis de los distintos *scripts*, vulnerabilidades y factores de riesgo. Otros proveedores también ofrecen versiones de prueba, demostraciones y recursos educativos.

IDC elogia estos enfoques. Nada transmite más la urgencia de una situación o el valor y la eficacia de una solución de seguridad que una prueba de concepto. Para los proveedores, el beneficio de una posible conversión de suscripción *premium* es claro. Los compradores también se benefician en gran medida, ya que obtienen visibilidad de un vector de amenazas que tradicionalmente ha sido un completo punto ciego para la mayoría de las organizaciones.

Además, en el futuro, IDC monitoreará el mercado del WAF del lado del cliente para comprender su impacto en mercados establecidos, tales como WAF, mitigación de DDoS, administración de *bots* y prevención de fraudes en línea. Una vez que se aborde el punto ciego de seguridad del lado del cliente, se requerirán debates más profundos sobre el impacto de la posible visibilidad y las capacidades de aplicación del lado del cliente, como un punto de control de seguridad.

## MÁS INFORMACIÓN

## Investigación relacionada

- *IDC FutureScape: Worldwide Future of Trust 2021 Predictions* (IDC #US46912920, octubre del 2020)
- *Pervasive Application Edge Defense: An Application-Based Framework for Trust* (IDC #US46810219, septiembre del 2020)
- *IDC Market Glance: Software-Defined Secure Access, 2Q20* (IDC #US46291520, mayo del 2020)
- *Worldwide Internet Defense Forecast, 2020-2023: Infrastructure and Application Security Drive Business Value* (IDC #US46022619, febrero del 2020)
- *Security Convergence at the Edge: Emerging Pervasive Data Defense and Response Platforms* (IDC #US46075520, febrero del 2020)

## Síntesis

Esta market perspective de IDC proporciona un análisis del vector de amenazas, de las soluciones emergentes y del futuro del mercado del WAF del lado del cliente. Pocas organizaciones de TI tienen una comprensión completa de las amenazas dirigidas a los *scripts* del lado del cliente que se ejecutan en sus entornos web. Los ciberdelincuentes han apuntado a los *scripts* del lado del cliente para ejecutar códigos maliciosos de manera clandestina y así obtener grandes ganancias financieras sin correr el riesgo de ser capturados. A medida que este vector de amenazas se acentúe más en los próximos años, se espera que la demanda de soluciones empresariales de WAF del lado del cliente aumente de manera constante.

"Los *scripts* del lado del cliente son la siguiente frontera en seguridad. Los ciberdelincuentes siguen siendo implacables en su búsqueda de vulnerabilidades lucrativas y han encontrado una nueva brecha en los digital security stacks empresariales", dice Christopher Rodriguez, Research Manager, IDC Network Security Products and Strategies.

## Acerca de IDC

International Data Corporation (IDC) es el principal proveedor mundial de inteligencia de mercado, servicios de consultoría y eventos para los mercados de tecnología de la información, telecomunicaciones y tecnología de consumo. IDC ayuda a que los profesionales de TI, los ejecutivos comerciales y la comunidad inversora tomen decisiones fundamentadas respecto de compras de tecnología y estrategia empresarial. Más de 1100 analistas de IDC ofrecen una experiencia global, regional y local en cuanto a las oportunidades y tendencias en la industria y la tecnología en más de 110 países de todo el mundo. Durante 50 años, IDC ha proporcionado perspectivas estratégicas que permiten a nuestros clientes alcanzar sus objetivos comerciales principales. IDC es una subsidiaria de IDG, la empresa líder del mundo en medios tecnológicos, investigación y eventos.

## Sede central

5 Speen Street
Framingham, MA 01701
EE. UU.
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

---