



**McAfee**<sup>®</sup>  
An Intel Company

# PROTEGER EL CENTRO DE DATOS

Guía de solución

### *Epsilon después de la filtración*

*En 2011, debido a una fuga de datos ocurrida en la empresa de marketing por correo electrónico Epsilon, se revelaron los nombres y direcciones de correo electrónico de millones de clientes. Son muchas las empresas importantes que utilizan los servicios de Epsilon, por lo que el suceso provocó una avalancha de notificaciones para advertir a los clientes de las posibilidades de fraude. Entre las empresas que tuvieron que informar a sus clientes se encuentran: Barclaycard US, Capital One, Best Buy, JPMorgan, Citigroup, TiVo, Disney Destinations, New York & Company, Walgreens, Marriott, y muchas otras. (Fuente: <http://mcaf.ee15342e>)*

### Security Connected

El marco Security Connected de McAfee Security permite integrar distintos productos, servicios y asociaciones para reducir los riesgos de forma efectiva, eficiente y centralizada. Basada en más de dos décadas de prácticas de seguridad probadas, el enfoque Security Connected ayuda a las organizaciones de todos los tamaños y segmentos, de todas las zonas geográficas, a mejorar sus condiciones de seguridad, optimizar la seguridad para conseguir una mayor rentabilidad y alinear estratégicamente la seguridad con las iniciativas empresariales. La arquitectura de referencia Security Connected ofrece una ruta concreta desde las ideas hasta la implantación. Utilícela para adaptar los conceptos de Security Connected a sus riesgos, infraestructura y objetivos empresariales. En McAfee dedicamos todos nuestros esfuerzos a la búsqueda constante de nuevas soluciones y servicios que garanticen la total seguridad de nuestros clientes.

## Mayor seguridad para centros de datos más ágiles

### Desafíos

Los centros de datos consiguen que las organizaciones funcionen. Entre los papeles que juegan están la generación de ingresos, el almacenamiento de datos confidenciales y la prestación de servicios vitales. Debido a su importancia y valor, son un objetivo. Los datos confidenciales, las aplicaciones comerciales, las bases de datos, los dispositivos de red, el almacenamiento y la infraestructura de soporte han estado durante mucho tiempo en la mira de los delincuentes tanto externos como internos, así como en la de los auditores que vigilan el cumplimiento de las normativas.

Prácticamente cada problema de seguridad del centro de datos y cada obligación de cumplir las normativas ha generado una solución aislada. Este proceso reactivo en el que se agregan nuevas soluciones independientes ha dado lugar a que los controles de los centros de datos sean complejos, numerosos, caros y estén desconectados, lo que abruma a la mayoría de las organizaciones. Además de los requisitos que ya existen, nuevas amenazas y tendencias aparecen continuamente en el campo de batalla. Por ejemplo, las empresas exigen que sus centros de datos den soporte a la movilidad y la Web 2.0, protejan frente a los ataques selectivos y oportunistas, y que hagan todo esto a la vez que reducen el tiempo de inactividad y generan informes frecuentes para demostrar que cumplen las normativas.

La seguridad clásica del centro de datos carece de la agilidad de la empresa para incorporar con rapidez y a la perfección nuevos requisitos, de la gestión de la seguridad para aumentar la eficiencia y la eficacia, de la disponibilidad y la integridad necesarias para las operaciones de misión crítica actuales y del diseño optimizado para ser rentable. Los centros de datos se han convertido en puntos más críticos. Los departamentos de TI de hoy día están abriendo nuevos caminos. Solo podemos especular sobre los "grandes acontecimientos" de los próximos cinco años, pero si los últimos cinco nos sirven de medida, lo que creíamos que nos protegía no va a protegernos en el futuro. Se necesita un marco estratégico para conectar las piezas que siempre han sido dispares.

---

*De acuerdo con el informe "Cost of a Data Breach" (Los costes de las fugas de datos) de 2011 del Ponemon Institute, cada registro en peligro cuesta 214 dólares. El promedio de cada evento de fuga de datos asciende a 7,2 millones de dólares<sup>2</sup>.*

---

### *Heartland Payment Systems después de la filtración*

*En 2010, Heartland llegó a un acuerdo por valor de 60 millones de dólares con VISA para cubrir todas las posibles reclamaciones relacionadas con la filtración de 2009. Un año antes, Heartland había llegado a un acuerdo similar con Amex por valor de 3,5 millones de dólares<sup>1</sup>.*

---



## Soluciones

### Agilidad empresarial

Los equipos de operaciones de los centros de datos tienen la responsabilidad de diseñar soluciones para cumplir las normativas continuamente, para virtualizar, consolidar y sacar partido de Internet. Un marco de seguridad debe ser lo suficientemente ágil para poder realizar los cambios con rapidez y para adoptar las nuevas tendencias sin agregar riesgos adicionales. Un marco de seguridad potente que proporcione esta agilidad tiene un efecto positivo en las operaciones de seguridad y de negocio.

### Gestión de la seguridad

Las fugas de datos son caras, y sus costes pueden deberse a multas por incumplir las normativas, a acciones legales y a relaciones públicas, la disminución de la lealtad a la marca, la pérdida de clientes y, finalmente, la disminución de los ingresos. Dada la complejidad de los centros de datos, en conjunto con algunas de las tendencias y amenazas mencionadas anteriormente, la reducción del riesgo correcta requiere de una estrategia de seguridad que incluya todos los elementos. Cuando se administran centros de datos de todos los tamaños y complejidades, debe utilizarse una solución de gestión de la seguridad centralizada que conecte las soluciones aisladas a través de los datos, los endpoints, las redes e Internet. La gestión ampliable de la seguridad es vital para tener visibilidad de las aplicaciones y bases de datos que procesan las transacciones, y de los dispositivos que almacenan de dichos datos.

### Disponibilidad e integridad

Ante las amenazas internas y externas, es un desafío proveer disponibilidad e integridad, incorporar nuevas tendencias como los equivalentes móviles de sitios web, integrarse con servicios web 2.0 de terceros o aprovechar las distintas infraestructuras de procesamiento en Internet. También puede ser muy arriesgado si no se presta suficiente atención al proporcionar condiciones de seguridad robustas que no se limiten a la seguridad de los contenidos o de las redes, sino que mezclen la seguridad de los endpoints, de los contenidos y de las redes al mismo tiempo que se integran en Internet. Un marco de seguridad debería reducir la latencia, el riesgo que suponen los errores de configuración manual, prohibir la instalación de

software malicioso y proteger la información con independencia del tamaño del centro de datos, o de si está consolidado, virtualizado o basado en Internet. Es esencial proteger los entornos virtualizados —las infraestructuras de servidores y equipos de sobremesa virtualizados—. Las infraestructuras de equipos de sobremesa virtualizados se instalan habitualmente en cualquier equipo, desde smartphones y portátiles a servidores virtuales, y son la norma en los centros de datos. Las soluciones de hoy día deben estar optimizadas para abordar las tendencias de la virtualización, pero sin olvidar que lo básico también es importante. Los entornos vitales no pueden permitirse la latencia ni el tiempo de inactividad no planificado. Las operaciones de red, el control de acceso, la protección de los endpoints y los firewalls deben diseñarse teniendo en mente las necesidades de TI, no solo la seguridad, dado que las soluciones de seguridad insuficientes que introducen latencia pueden ser tan dañinas como los ataques.

### Optimización de la seguridad

La optimización de la seguridad aleja a las organizaciones de la simple pregunta técnica relativa a los controles de seguridad "¿Podemos hacerlo?" y, en su lugar, responde a "¿Cuál es la mejor forma de hacerlo?". Existen muchas soluciones de seguridad en el mercado, y la mayoría funcionan bien. Pero en conjunto, agregan complejidad, el mayor enemigo de la seguridad. Contar con silos y soluciones dispares que carecen de interconexión y dependen de cada vez más recursos para funcionar es insostenible. En cambio, los marcos de seguridad actuales deben ser compatibles con un modelo de seguridad optimizado cuyo objetivo es gestionar centralizadamente los controles de seguridad, permite que se enriquezcan unos a otros y alinea las soluciones con las prioridades de la empresa, a la vez que reduce los costes operativos de seguridad. Dado que las amenazas evolucionan y la rapidez con que se adopta gran número de tendencias, un marco de seguridad optimizado será una necesidad para que las operaciones sean rentables, eficientes y seguras. Las soluciones optimizadas son parte integral de automatizar el proceso del cumplimiento de las normativas, de forma que las tareas y los procesos de seguridad que rodean las disposiciones regulatorias estén alineadas sin crear sobrecargas adicionales.

### Consideraciones sobre las buenas prácticas

- Entender que los centros de datos están sufriendo grandes cambios: consolidación, virtualización e Internet.
- Implantar soluciones para satisfacer las necesidades de agilidad, gestión de la seguridad, disponibilidad e integridad, y la optimización de la seguridad.
- Poner en marcha soluciones que centralizan las operaciones de seguridad de los componentes vitales de los centros de datos: redes, soluciones virtualizadas, bases de datos, servidores y dispositivos de almacenamiento.
- Garantizar que las soluciones de seguridad utilizadas también ayuden a automatizar el cumplimiento de las normativas.
- Además de abordar la seguridad, garantizar que se tienen en cuenta los puntos operativos esenciales que rodean la disponibilidad y la latencia.

---

De acuerdo con el informe *DataLossDB* de abril de 2011 de la *Open Security Foundation*, el 75 % de las pérdidas de datos se debió a actividades malintencionadas y el resto a negligencia<sup>3</sup>.

---

## Motivaciones de valor

Las iniciativas que se tomen para los centros de datos deben aprovechar la tecnología basada en la seguridad para lograr eficiencias operativas. Tenga en cuenta los siguientes aspectos, que pueden optimizarse en los centros de datos:

- **Consolidación:** las soluciones de consolidación deben desplegarse en el hardware, el software y la infraestructura de soporte.
- **Estandarización:** las soluciones deben ser compatibles con la estandarización de las funciones para proteger los endpoints, los datos y las redes. Ayudará a garantizar que el análisis y la respuesta a las amenazas sean eficientes y eficaces.
- **Reducción de los costes de auditoría, cumplimiento y supervisión:** las soluciones deben proporcionar o justificarse por la reducción de los costes de auditoría de TI y de cumplimiento de las normativas, porque se auditan los sistemas y los procesos en lugar de los nodos individualmente.
- **Reducción del tráfico de las redes:** las soluciones centrales que pueden existir sirven para proteger y deberían servir también para eliminar el tráfico de red innecesario y el spam.
- **Reducción de los costes del help desk:** los esfuerzos para proteger el centro de datos deben conducir a la reducción de las llamadas de los usuarios finales al help desk debidas a incidentes relacionados con la seguridad.

## Material relacionado de la arquitectura de referencia Security Connected de McAfee

### Nivel II

- Proteger la información
- Controlar y supervisar el cambio

### Nivel III

- Evaluar las vulnerabilidades
- Imponer el cumplimiento de las normativas en los endpoints
- Impedir ataques de denegación de servicio (DoS y DDoS)
- Proteger los servidores

Si desea obtener más información sobre la arquitectura de referencia Security Connected de McAfee, visite: [www.mcafee.com/es/enterprise/reference-architecture/](http://www.mcafee.com/es/enterprise/reference-architecture/).

## Acerca del autor



*Brian Contos*, CISSP, es Director de la estrategia global de seguridad de McAfee. Es un experto en seguridad reconocido, con casi 20 años de experiencia en ingeniería y gestión de la seguridad. Es autor de varios libros como *Enemy at the Water Cooler* (El enemigo en la fuente) y *Physical and Logical Security Convergence* (Convergencia de la seguridad física y lógica). Ha trabajado en organismos públicos y en empresas de la lista Forbes Global 2000 en todo el continente americano, Europa, Oriente Medio y Asia. Es ponente invitado en importantes eventos del sector como RSA, Interop, SANS, OWASP y SecTor. Además, escribe en publicaciones sectoriales y de negocios como *Forbes*, *New York Times* y *The Times of London*. Brian es miembro distinguido del Ponemon Institute y se licenció en la Universidad de Arizona.

[brian\\_contos@mcafee.com](mailto:brian_contos@mcafee.com) || <http://siblog.mcafee.com/author/brian-contos/> || @BrianContos

<sup>1</sup> <http://mcaf.ee/gvxkh>

<sup>2</sup> <http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2010%20Global%20CODB.pdf>

<sup>3</sup> <http://datalosssdb.org/>

