
# TRANSFORME LA SEGURIDAD DE TI EN TRES PASOS

# ÍNDICE

3 LA SEGURIDAD ES UNA PRIORIDAD PARA TODOS LOS NEGOCIOS

4 LA EVOLUCIÓN DE LOS RIESGOS EN UN PANORAMA DE AMENAZAS DINÁMICO

5 TRES ÁREAS DE ENFOQUE PARA UNA SEGURIDAD DE TI EFICAZ

11 SEGURIDAD PARA UN PANORAMA Y NECESIDADES CAMBIANTES

# LA SEGURIDAD ES UNA PRIORIDAD PARA TODOS LOS NEGOCIOS

A medida que aumenta la conexión entre las personas, los dispositivos y los objetos, la protección de todas estas conexiones y todos estos entornos se vuelve más importante que nunca. En una reciente encuesta sobre las prioridades de TI, el 69 % de los encuestados le expresaron a Tech Pro Research que mejorar la seguridad representaba la principal iniciativa de TI para 2017.[1]

En la misma encuesta, los participantes también dijeron que la seguridad sería el desafío más grande de TI en el año siguiente. Esto se debe a que las organizaciones de TI necesitan proteger cada una de las interacciones entre los usuarios, las aplicaciones y los datos, sin importar cómo y dónde están conectados. Y deben hacerlo en un entorno cada vez más dinámico que cambia constantemente.

1 "IT Budget Research: Where CXOs are placing their bets for 2017", Tech Pro Research, julio de 2016.

2 **https://www.sdxcentral.com/articles/analysis/securing-cloud-sdn/2016/05/**.

3 "Cost of Data Center Outages" Ponemon Institute, enero de 2016.

4 Ibíd.

Los riesgos en materia de seguridad son altos para las empresas de todos los sectores y siguen aumentando. Según un estudio reciente, el costo promedio total de una filtración de datos aumentó de 3,52 millones de USD a 3,79 millones de USD en tan solo un año.[2] Para las organizaciones que están adoptando entornos virtualizados y de nube, la visibilidad y el control máximos son clave para reducir este riesgo.

## HAY MUCHO EN JUEGO PARA LA SEGURIDAD

- El delito cibernético representa la causa de interrupciones del centro de datos en más rápido crecimiento: ha aumentado desde un 2 % en 2010 a un 22 % en 2016.[3]
- El costo promedio de una interrupción del centro de datos ha aumentado a los 740.357 USD en 2016.[4]

# LA EVOLUCIÓN DE LOS RIESGOS EN UN PANORAMA DE AMENAZAS DINÁMICO

Todos los negocios se han convertido negocios digitales. Esta transformación ha dado lugar a cambios importantes en el panorama de TI y, a raíz de esto, la seguridad de TI también representa nuevos desafíos.

Comience con la evolución de las infraestructuras de aplicaciones, que ya realizaron la transición desde centros de datos en las instalaciones que se ejecutan en la infraestructura física a entornos altamente dinámicos que se encuentran en nubes privadas y públicas. Considere también cómo están cambiando las aplicaciones. Las organizaciones están dejando de ser pilas de aplicaciones monolíticas y están optando por aplicaciones distribuidas de múltiples niveles que se basan en microservicios. A medida que la fuerza de trabajo se vuelve más móvil y distribuida, los entornos de usuario final también evolucionan. Ya no se limitan a escritorios administrados desde la empresa, sino que se centran en dispositivos móviles, en iniciativas de dispositivos propios del usuario final (Bring Your Own Device, BYOD) y en el Internet de las cosas (Internet of Things, IoT).

Como resultado, los modelos tradicionales de seguridad perimetral de red ya no son suficientes para proteger la expansión de aplicaciones y usuarios, ni para cumplir con los requisitos normativos en aumento. Los entornos y los usuarios no están contenidos de manera prolija detrás de los firewalls perimetrales, sino que requieren una protección más ágil y flexible contra los atacantes que, a su vez, se han vuelto más sofisticados. El ciberespacio adopta cada vez más armas. Incluso un hacker sin experiencia, que usa kits de herramientas como Zeus y BlackPoS, puede apuntar a un negocio con ataques avanzados que pueden ocasionar daños reales en la productividad, los recursos y la reputación.

A medida que nos adaptamos para tomar en cuenta estos nuevos desafíos cada vez más cercanos, las normas de cumplimiento se tornan cada vez más complejas. Esto hace que el equipo promedio de TI se vea obligado a invertir el 20 % del tiempo en esfuerzos relacionados con el cumplimiento.

# TRES ÁREAS DE ENFOQUE PARA UNA SEGURIDAD DE TI EFICAZ

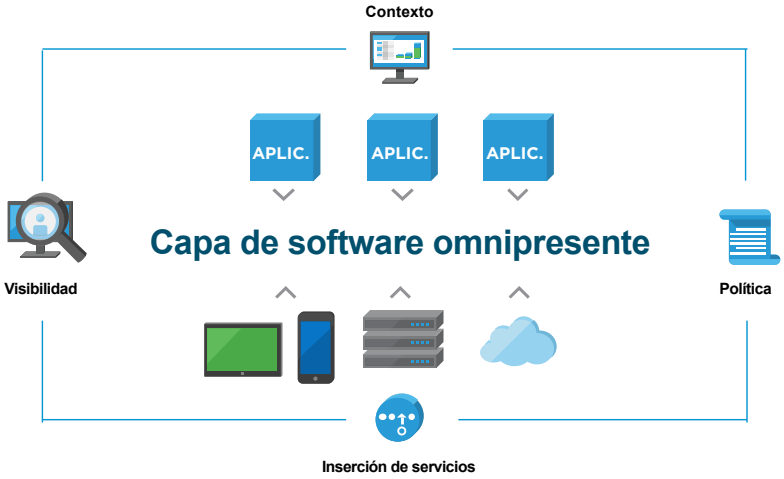
Proteger una organización mediante una solución de seguridad sólida que cumpla con los estándares no es sencillo cuando la infraestructura y los usuarios cambian rápidamente. Las viejas reglas básicas de seguridad de red quedaron obsoletas, y los equipos de TI deben seguir el ritmo de los siguientes cambios:

- **Cambios en la infraestructura:** la infraestructura que se utiliza para ejecutar aplicaciones como servidores de base de datos y web está evolucionando desde entornos en las instalaciones para ser compatible con aplicaciones distribuidas y de nube.
- **Mayor movilidad**: TI necesita ampliar las políticas de seguridad para respaldar la avalancha de nuevos modelos y dispositivos.
- **Aumento del cumplimiento:** el entorno de cumplimiento normativo se vuelve cada vez más complejo a medida que las organizaciones enfrentan nuevos requisitos.

## SUMINISTRO DE VISIBILIDAD Y CONTEXTO PARA TRANSFORMAR LA SEGURIDAD

Para mantenerse un paso adelante de las cambiantes necesidades de seguridad, debe tener una amplia visibilidad de cada interacción entre los usuarios y las aplicaciones. También necesita una solución que proporcione contexto para comprender lo que significan estas interacciones. La combinación de más visibilidad y más contexto le permitirá alinear las políticas y los controles de seguridad con las aplicaciones que se espera que proteja.

¿La base para esta solución? Una capa de software omnipresente en la infraestructura de aplicaciones y los terminales que sea independiente de la ubicación o la infraestructura física subyacente.




De hecho, un modelo de seguridad eficaz requiere de múltiples capas de protección. Y una solución de software adecuada dentro de la infraestructura le permite tener el mejor punto de control posible para aumentar la visibilidad, hacer cumplir las políticas y habilitar la inserción de servicios de terceros, a fin de obtener una protección inteligente adicional.

Analicemos en detalle estos tres pasos clave para transformar la seguridad de TI:

- **Protección de la infraestructura de aplicaciones:** separe la infraestructura de las aplicaciones y, de esta manera, mejorará la visibilidad y podrá alinear mejor la seguridad con las aplicaciones.
- **Protección de identidades y terminales:** utilice una capa de software omnipresente en todos los usuarios y terminales para obtener mejor visibilidad y control, sin que esto afecte la experiencia de usuario.
- **Cumplimiento optimizado:** aplique software en la infraestructura de aplicaciones, la identidad y los terminales para simplificar el cumplimiento.

## 1. PROTECCIÓN DE LA INFRAESTRUCTURA DE APLICACIONES

A medida que evolucionan los modelos de infraestructura de aplicaciones, la estrategia tradicional de seguridad de red centrada en el perímetro no puede proporcionar visibilidad y control suficientes dentro del centro de datos. Al mismo tiempo, los datos estáticos almacenados se han vuelto un blanco mucho más valioso para los atacantes. Para abordar estos problemas, debe transformar la manera en que protege la infraestructura de aplicaciones.

La solución comienza con la virtualización y la capacidad de separar la infraestructura subyacente de las aplicaciones que se ejecutan en ella, independientemente de si esa infraestructura se encuentra en las instalaciones o en la nube pública. Esta capa de separación proporciona una visibilidad completa de la ruta de datos, así como un punto de cumplimiento ideal para compartimentar aplicaciones mediante la microsegmentación de la red. El uso de la microsegmentación en el software les proporciona a las organizaciones la posibilidad de simplificar las políticas de seguridad y alinearlas de manera más estrecha con las necesidades de las aplicaciones. Además, permite que las políticas sigan la aplicación a medida que se desplaza en nubes públicas y privadas. Una capa de separación también proporciona una plataforma para la inserción de servicios adicionales de terceros a fin de obtener una protección de la seguridad más avanzada.

Asimismo, la microsegmentación ayuda a TI a evitar que las amenazas contra la seguridad violen las defensas. Esto se logra habilitando el principio de la estrategia de menor privilegio centrada en las aplicaciones, la cual reduce la superficie de ataque de la infraestructura.

Una capa de separación entre las aplicaciones y la infraestructura subyacente no solo ayuda a TI a evitar los ataques, sino que también proporciona un punto ideal para el cifrado de datos almacenados. Mediante el cifrado de datos estáticos, en el nivel de las cargas de trabajo, las organizaciones pueden garantizar la seguridad de los datos de la infraestructura de aplicaciones, incluso si caen en manos equivocadas.

## 2. PROTECCIÓN DE IDENTIDADES Y TERMINALES

A medida que su negocio se vuelve digital, los dispositivos móviles proliferan con rapidez. Las organizaciones como la suya utilizan toda clase de dispositivos, como dispositivos Android, iOS, Windows, macOS, entre otros, para fortalecer las fuerzas de trabajo y rediseñar los procesos empresariales tradicionales. La compatibilidad con todos estos dispositivos y plataformas es un desafío, especialmente a medida que las empresas adoptan las iniciativas de IoT y BYOD y la movilidad empresarial.

Mediante la aplicación de una capa de software omnipresente en todos los usuarios y terminales que permita verificar la identidad del usuario y la postura del dispositivo, usted tendrá las herramientas necesarias para abordar este desafío. Esta estrategia proporciona un control y una visibilidad integrales del usuario y el terminal, ya que abarcan todo el centro de datos o la nube, donde se encuentra la infraestructura de aplicaciones. Mediante una capa de software, TI puede agregar una capa de seguridad adaptativa y condicional en cada nivel de transacción, desde el usuario hasta los recursos a los que accede. Esto ayuda a proteger los datos corporativos y reducir la superficie del ataque cibernético, sin afectar la experiencia de usuario.

Busque una solución única que pueda proteger todos sus terminales, incluidos teléfonos inteligentes, tabletas, computadoras portátiles, dispositivos portátiles y dispositivos de IoT. Como resultado, TI puede implementar sin inconvenientes cualquier aplicación, incluidas aplicaciones virtuales, remotas, nativas y web, y escritorios de Windows, mediante un catálogo de aplicaciones único con inicio de sesión único, seguridad de datos y cumplimiento de terminales incorporados. Para los espacios de trabajo dinámicos actuales, lo que necesita es una solución que, mediante la microsegmentación, permita extender la seguridad más allá de la interfaz de escritorio virtual (Virtual Desktop Interface, VDI) y terminales móviles hasta el centro de datos.

Dado que cada negocio tiene necesidades de seguridad específicas, la solución también debería ayudarlo a personalizar el entorno para que esté alineado con sus prioridades. De esta manera, tendrá una base para trabajar con los socios de seguridad, quienes pueden aprovechar la visibilidad y los puntos de control suministrados para complementar la solución con sus propias ofertas de servicios.

## 3. OPTIMIZACIÓN DEL CUMPLIMIENTO

La administración de riesgos y el mantenimiento continuo del cumplimiento son siempre preocupaciones cruciales. Esto es sumamente importante para industrias como organizaciones gubernamentales, de servicios de salud y de servicios financieros, que enfrentan requisitos estrictos como la industria de tarjetas de pago (Payment Card Industry, PCI), la Ley de Transferencia y Responsabilidad de Seguro Médico (Health Insurance Portability and Accountability Act, HIPAA), la Ley de Privacidad de las Comunicaciones Electrónicas (Electronic Communications Privacy Act, ECPA) y la Directiva de Protección de Datos para Europa, entre otras. Las normas y los requisitos están creciendo, a la vez que el panorama digital y las amenazas avanzadas continuas siguen evolucionando. Por lo tanto, más que nunca, el desafío es garantizar y demostrar el cumplimiento.

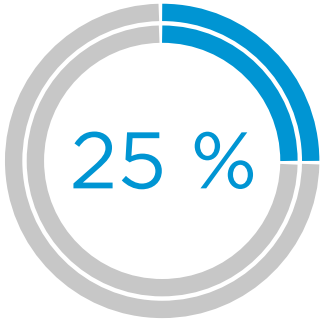
Y, para complicar más las cosas, las organizaciones están realizando rápidamente la transición de los centros de datos en las instalaciones a la nube, lo que dificulta aun más el cumplimiento de las demandas normativas, empresariales y de políticas.

Con una capa de software omnipresente en la infraestructura de aplicaciones y los terminales, usted opta por una estrategia de cumplimiento integral. Esta estrategia única ofrece una ubicación ideal para implementar controles de cumplimiento y obtener la visibilidad necesaria para demostrarlo. La solución adecuada proporciona una plataforma tecnológica en la que las herramientas y los servicios validados de los socios de la red se pueden insertar de manera dinámica para optimizar aun más el proceso de cumplimiento.

> "A medida que aumenta la cantidad de empresas que compiten en busca de talento en un mercado limitado, la brecha en habilidades se volverá un problema aun más grande. Puede que las empresas se vean obligadas a reconsiderar las estrategias y a buscar soluciones (de seguridad) que sean más anticipativas y requieran menos administración a fin de poder aprovechar al máximo los recursos".[5]
>
> **JAMES MAUDE**
> SECURITY ENGINEER, AVECTO

5 http://www.information-management.com/gallery/6-top-it-security-trends-for-2017-10030567-1.html.

Mediante un marco de arquitectura de referencia de cumplimiento, usted puede vincular las capacidades integradas de software y hardware, y los controles normativos específicos, con validación para la auditoría independiente. Además, puede aprovechar un programa validado de forma independiente para ejecutar cargas de trabajo altamente reguladas de manera segura. Ya sea que use un entorno de nube pública o privada, necesita garantizar que su organización siga cumpliendo los requisitos de manera constante. Para esto, se necesita una solución que tenga la velocidad, la eficiencia y la agilidad que usted exige y que, al mismo tiempo, permita optimizar el proceso de cumplimiento.




Para 2020, más del 25 % de todos los ataques identificados en la empresa estarán relacionados con el Internet de las cosas (IoT).[6]

> "Los clientes se están alejando de los negocios que son víctimas de infracciones, y el entorno normativo es tal que las empresas necesitarán una protección significativa, tanto si la incorporan ellos mismos como si tercerizan la responsabilidad."[7]

**FADI ALBATAL**

SENIOR VICE PRESIDENT, ABOVE SECURITY

6 "Gartner Says Worldwide IoT Security Spending to Reach $348 Million in 2016", Gartner Inc., abril de 2016.

7 **http://www.datacenterjournal.com/cybersecurity-trends-2017-companies-fight-back/**.

# SEGURIDAD PARA UN PANORAMA Y NECESIDADES CAMBIANTES

Contar con una seguridad sólida fue siempre fundamental para las redes de negocio y, a medida que se acelera el ritmo del cambio, resulta más indispensable que nunca. Cuanto más evolucionan los modelos de infraestructura, las aplicaciones y la fuerza de trabajo tradicionales, más presionado se ve su equipo de TI para proteger el negocio de las nuevas amenazas emergentes.

Una capa de software omnipresente en la infraestructura de aplicaciones y los terminales puede ayudarlo a transformar la seguridad. Esto le permite maximizar la visibilidad y el contexto de la interacción entre los usuarios y las aplicaciones, de manera que pueda alinear las políticas y los controles de seguridad con las aplicaciones que se protegen. Además, hace que sea más fácil complementar su solución con servicios de seguridad de terceros para obtener una protección inteligente adicional.

## TRANSFORMACIÓN DE LA SEGURIDAD

VMware e Intel transforman la seguridad proporcionando medidas integrales de seguridad basadas en software y hardware en la infraestructura de aplicaciones y los terminales. Estas medidas maximizan la visibilidad, el contexto y el control para proteger las interacciones entre los usuarios, las aplicaciones y los datos.

## COMIENCE HOY MISMO

Transforme su seguridad de TI para el panorama actual
**www.vmware.com/latam/it-priorities/transform-security**

Encuéntrenos en línea:

vmware® | intel®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel. 877-486-9273 Fax 650-427-5001 www.vmware.com/latam

N.º de elemento: TS-0318 Intel Co-Branded-Transform Your Security
07/17