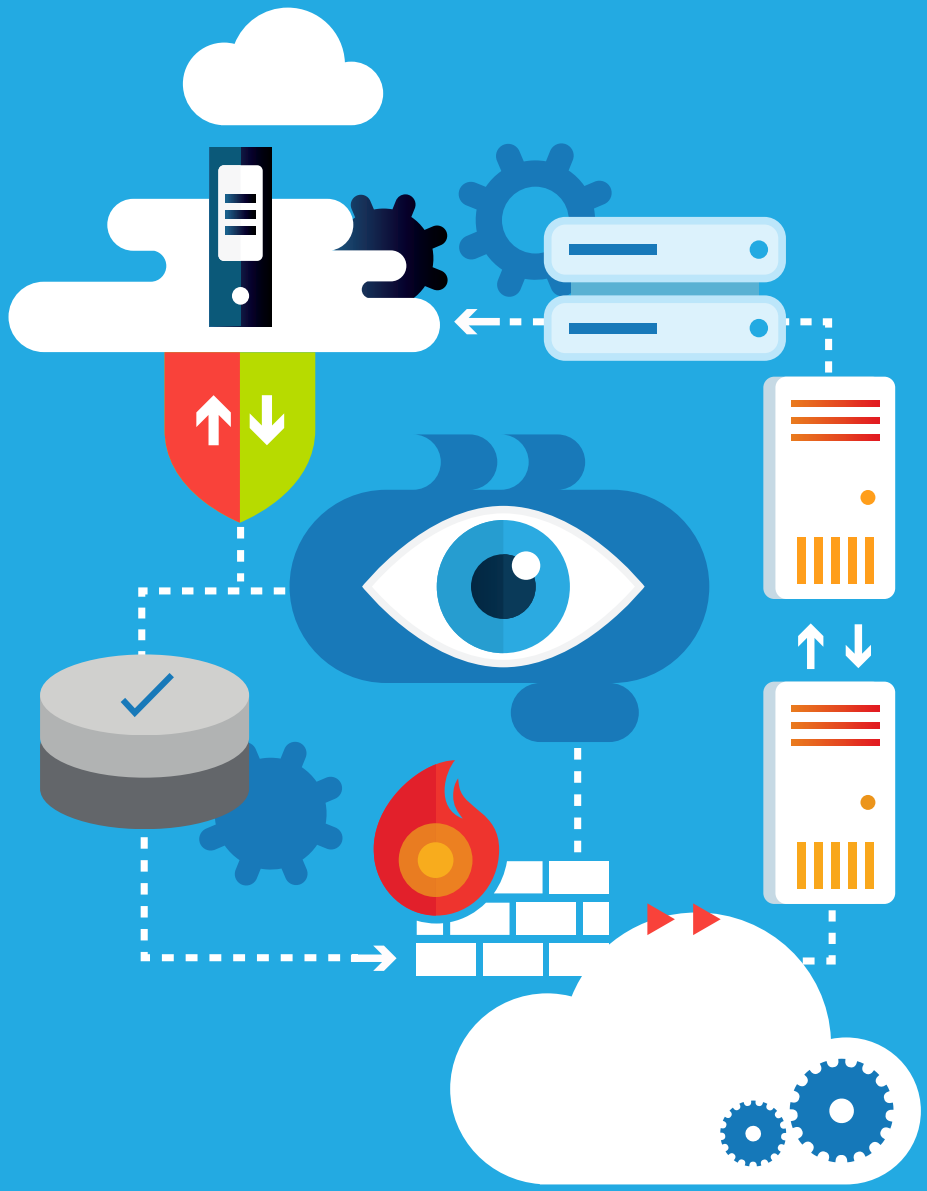
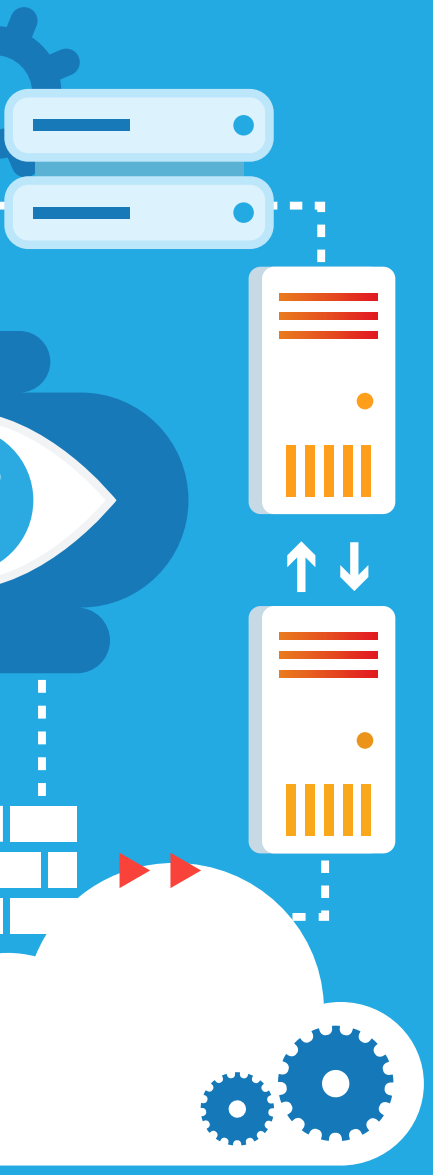
CITRIX®

Cree un enfoque estratégico para la seguridad de redes y aplicaciones

Cómo proteger la totalidad de su ecosistema digital.





Contenido

Introducción 3
El equilibrio entre seguridad y usabilidad 4
Las amenazas se transforman para burlar la seguridad 5
Los métodos tradicionales ya no funcionan 6
Por qué es primordial un nuevo enfoque de seguridad 7
Un enfoque de seguridad ideal es holístico: 9
Seguridad completa con un espacio de trabajo digital seguro 10
Ofrezca la experiencia adecuada 11
Beneficios empresariales adicionales 12

Sofisticados ataques a las aplicaciones, tales como WannaCry y NetPetya, atrajeron con razón mucha atención en las noticias. Evolucionan, son persistentes y están aumentando rápidamente en cuanto a frecuencia se refiere.

Pero los ataques a las aplicaciones no deberían ser las únicas amenazas a considerar. Las amenazas de cualquier tipo pueden propagarse por doquier. Desde la red hasta las aplicaciones, los ataques continúan afectando a las organizaciones en cada capa de la infraestructura. Históricamente, la solución ha sido agregar otro producto puntual, pero este enfoque conlleva gaps en la seguridad. Solo una solución integral, de extremo a extremo puede proteger completamente sus datos, independientemente de dónde se encuentren.

← Pág. 2 | Pág. 4 →

Volver a los contenidos

El equilibrio entre seguridad y usabilidad

Los usuarios desean poder elegir en lo relacionado con sus aplicaciones y dispositivos y la flexibilidad para trabajar en cualquier lugar y en cualquier momento. Pero eso añade mucha complejidad a enmendar, riesgos de seguridad y dispersión de los sistemas a administrar por TI. Con la solución adecuada, las organizaciones no tienen que dar a una prioridad sobre la otra; pueden tener ambas.

Independientemente de dónde residan los datos, su organización puede brindar a los empleados las herramientas que desean, al tiempo que garantiza que TI tenga la visibilidad y el control para monitorizar activamente todo su ecosistema desde una consola unificada.

← Pág. 3 | Pág. 5 →

Volver a los contenidos

Las amenazas se transforman para burlar la seguridad

Los ataques evolucionan constantemente para burlar la seguridad.
Ahora están omnipresentes en todos los niveles de su infraestructura de TI.
He aquí una foto de cómo los ataques están cambiando.

Tipos comunes de ataques de red:
Históricamente, las redes han sido el objetivo de la mayoría de los ataques. Las mejores formas de defensa incluían firewalls, parches y educación, que nunca fueron grandes opciones, pero mientras que los datos estuvieran resguardados detrás de un firewall, las organizaciones normalmente podían mantener el control. Así fue, hasta que las amenazas fueron subiendo por la cadena y avanzaron hacia fuera del centro de datos.

Ataques a la red

- Fuerza bruta
- Ataques de gusanos informáticos
- DNS
- Escaneo de puertos
- Otros

Tipos comunes de ataques a web y aplicaciones:
A medida que los datos comienzan a difundirse fuera del centro de datos y a través de las nubes, web, dispositivos y aplicaciones, es más difícil protegerlos. Los ataques sofisticados comenzaron a seguir a los datos hacia las capas superiores y fuera del firewall, hacia la nube, la web y las capas de aplicación.

Ataques a la web y aplicaciones

- Navegador
- Ataques de interpretación de URL
- Ataques de inyección SQL
- Ataques de suplantación de identidad
- Ataques de desbordamiento de búfer
- DDoS (denegación de servicio distribuida)

← Pág. 4 | Pág. 6 →
Volver a los contenidos

Los métodos tradicionales ya no funcionan

En un intento por superar las amenazas emergentes, muchas organizaciones han agregado soluciones puntuales individuales para abordar las necesidades individuales de seguridad. Una para la protección de terminales finales, otra para las aplicaciones y otra para la red. Estos sistemas dispares no funcionan porque:

- **Añaden complejidad.** A medida que los datos pasaban del centro de datos a la nube, e incluso a los dispositivos finales más allá del firewall, los equipos de TI tenían que administrar y proteger diferentes sistemas.

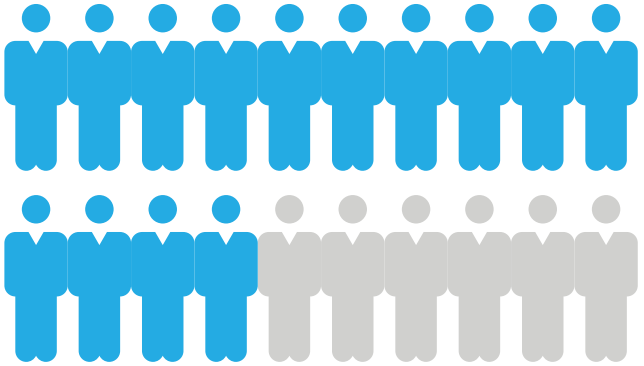
- **Dejan agujeros.** Los diferentes sistemas no se diseñaron para una cobertura de extremo a extremo y dejaban gaps por donde el malware puede pasar.

- **No se hablan entre sí.** Las soluciones puntuales en silos no pueden detectar anomalías o alteraciones y, por lo tanto, no pueden prevenir de forma proactiva que las amenazas traspasen su red.

- **No pueden identificar los ataques desconocidos:** Un gran problema para muchos sistemas dispares de seguridad son las amenazas que no pueden ver. También conocidos como ataques de día cero, pueden pasar desapercibidos durante largos períodos de tiempo, lo que permite a los piratas informáticos acceder a datos confidenciales durante el tiempo que tardan en ser descubiertos.

- **No prevén amenazas internas.** La mayoría de las soluciones de seguridad están orientadas a mantener alejados a los malos, pero no están diseñadas para detener las fugas desde el interior. Las soluciones puntuales no están diseñadas para reconocer y detener el comportamiento inusual. Como resultado, no pueden evitar que la información confidencial salga fuera de la red.

- **No pueden segmentar el acceso según las necesidades del usuario:** Administrar el comportamiento del usuario en los terminales, especialmente aquellos en dispositivos BYOD, es mucho más difícil con las soluciones puntuales individuales y supone un lastre adicional para los sobrecargados equipos de TI.



Más del **70%**

de los ejecutivos dicen que el principal culpable del riesgo para la ciberseguridad es la proliferación de dispositivos BYO y las aplicaciones que los empleados llevan al lugar de trabajo.[1]

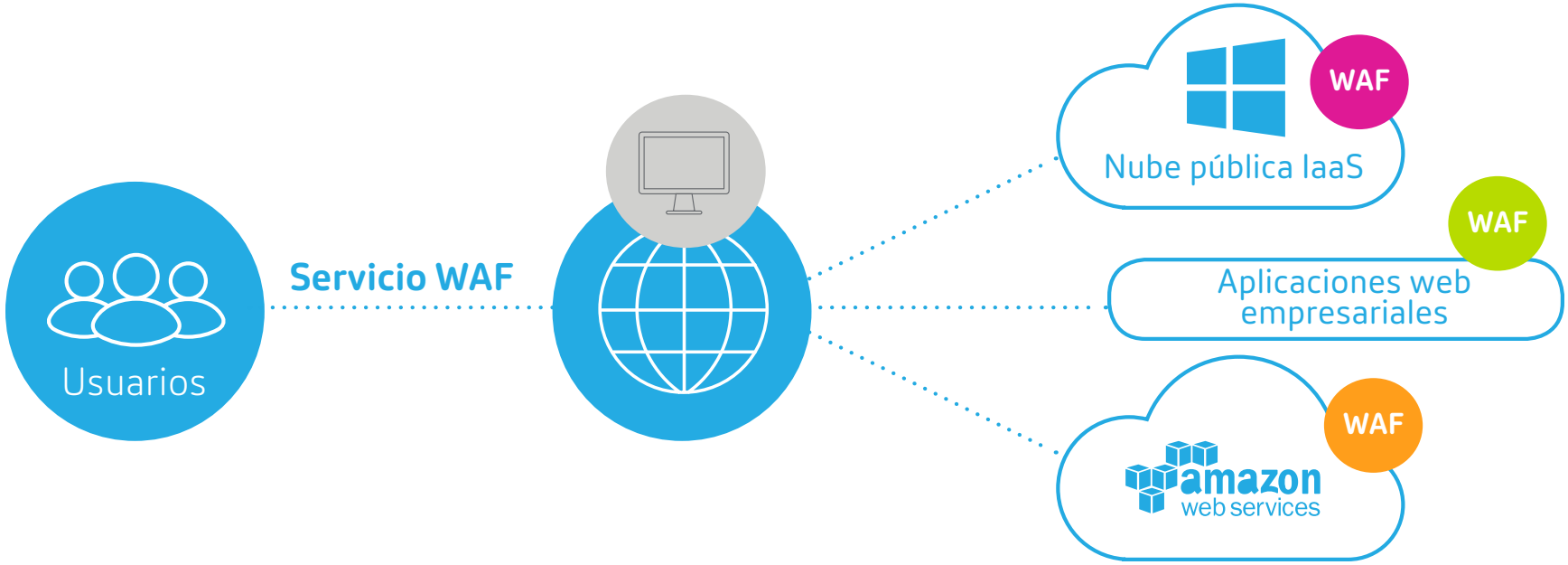
← Pág. 5 | Pág. 7 →

Volver a los contenidos

Por qué es primordial un nuevo enfoque de seguridad

Con una proliferación de servicios en la nube hoy en día, es muy probable que su organización se enfrente a nuevos tipos de amenazas. Y necesita una plataforma que pueda proteger sus datos en cualquier lugar, independientemente de si se trata de la red, la web o la capa de aplicación.

Un enfoque de extremo a extremo, que incluya un firewall de aplicación web totalmente integrado (WAF), le permite gestionar las amenazas en todas las nubes, redes, dispositivos y usuarios. También garantiza una experiencia de usuario y TI coherente.



← Pág. 6 | Pág. 8 →
Volver a los contenidos

74%

de las empresas están de acuerdo en que se necesita un nuevo marco de seguridad informática para mejorar el estado de seguridad y reducir el riesgo.[1]

← Pág. 7 | Pág. 9 →

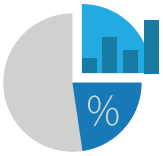
Volver a los contenidos

Un enfoque ideal de seguridad es holístico.

Un método unificado, contextual y seguro proporciona sistemas disponibles y fiables al tiempo que garantiza la confidencialidad y protección de los datos gracias a:

Visibilidad de 360 grados

Necesita una vista completa del tráfico y las transacciones que atraviesan su ecosistema para poder detectar las amenazas o la actividad inusual, como, por ejemplo, una señal de que una credencial utilizada en un momento atípico desde una ubicación improbable.



Proporcionar información procesable de los análisis

La telemetría avanzada le permite recopilar datos de cualquier fuente (registros de dispositivos, registros de servidores, registros y contadores de aplicaciones, correos electrónicos, productos SIEM de terceros, etc.). Después, podrá rastrear, analizar y detectar anomalías en sus redes, nubes, aplicaciones, tráfico web y usuarios, alertando proactivamente a TI sobre posibles problemas antes de que infecten sus sistemas.

Acceso simplificado

Ya sea BYOD, un escritorio dedicado o un dispositivo compartido, el inicio único de sesión (SSO) simplifica el proceso de acceso para usuarios mientras minimiza la carga de TI resolviendo problemas de contraseñas de empleados o privilegios de acceso caducados.

Capacidad para administrar, renovar, establecer y aplicar políticas

Asegúrese de que su organización pueda controlar los niveles de acceso para que los datos confidenciales solo sean confidenciales para las personas autorizadas.

Actualizaciones push y parches a nivel global

Parchear y actualizar los innumerables dispositivos utilizados es casi imposible. Administrar sistemas desde una ubicación centralizada significa que los equipos pueden implementar parches y actualizaciones en minutos en lugar de horas.

Protegerse contra ataques dirigidos a la capa de aplicación

Aplicar un conjunto de reglas para proteger los servidores firewall de aplicaciones web (WAF) que le ayudarán a defenderse de ataques comunes, tales como secuencias de comandos entre sitios (XSS) e inyecciones SQL.

Ofrecer cifrado de extremo a extremo

Gestionar el tráfico y los certificados para dar resiliencia al centro de datos y protección en entornos híbridos y multinube.

← Pág. 8 | Pág. 10 →

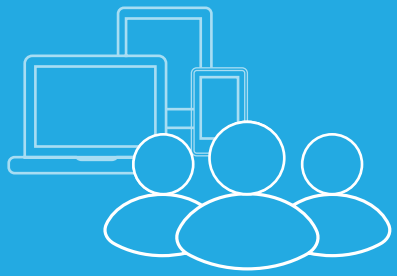
Volver a los contenidos

Seguridad completa con un espacio de trabajo digital seguro

Unificar

TI puede configurar, supervisar y administrar toda su infraestructura informática a través de un solo panel para ofrecer una experiencia de usuario unificada.

Seguridad



Un enfoque de seguridad centrado en las personas sitúa al usuario en el centro de su marco de seguridad, sintetizando todo lo que se conoce sobre el usuario y su comportamiento para proporcionar acceso contextual, controles de seguridad y análisis predictivo a fin de obtener una visibilidad completa en todo el ecosistema de redes y usuarios.

Contextual

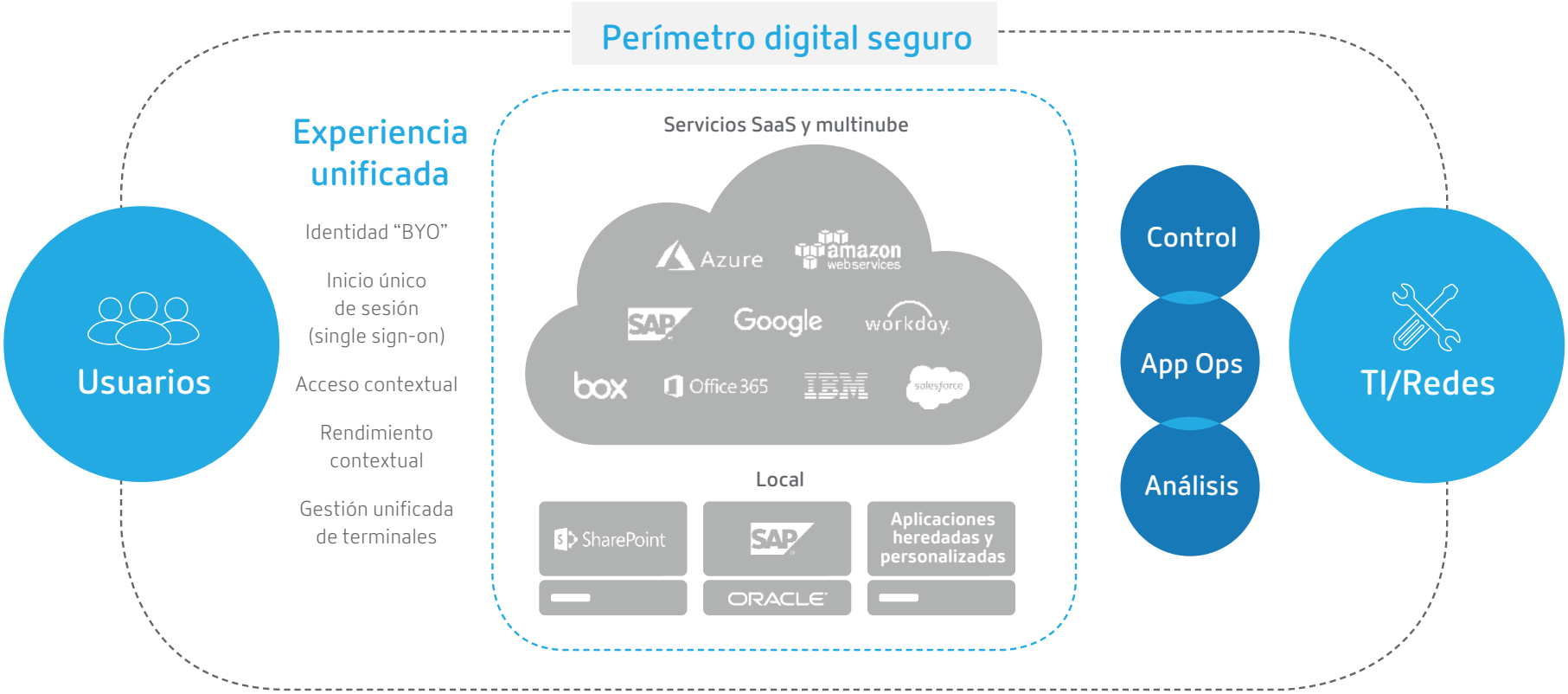
Los espacios de trabajo digitales utilizan el aprendizaje automatizado para adaptarse a los patrones y las excepciones de cada trabajador con el fin de que puedan hacer el trabajo de manera segura siendo productivos dondequiera que estén.

← Pág. 9 | Pág. 11 →

Volver a los contenidos

Proporcione la experiencia adecuada al usuario correcto en el momento más oportuno

La gestión de la creciente complejidad de las redes y el número de aplicaciones que se ejecutan en múltiples nubes no solo es difícil, sino que aumenta sus riesgos de seguridad. Citrix Workspace le permite tomar el control y administrar proactivamente las amenazas de seguridad en los entornos distribuidos de multinube híbrida y los múltiples dispositivos de hoy en día. En lugar de gestionar múltiples productos puntuales que no se integran y que, en consecuencia, pueden tener brechas en la prestación de seguridad de extremo a extremo, Citrix opta por ser el único proveedor que permite un planteamiento integral para la seguridad de las aplicaciones y la red en diferentes niveles. Vincula la oferta de seguridad con Citrix Analytics para proporcionarle un único panel para supervisar, administrar y resolver los riesgos de seguridad.



← Pág. 10 | Pág. 12 →

Volver a los contenidos

Beneficios empresariales adicionales de nuestro enfoque de seguridad

Colaboración segura con protección de la propiedad intelectual:
Creado desde cero para una seguridad de clase empresarial, Citrix permite a los usuarios empresariales compartir y colaborar en documentos de manera fácil, segura y profesional, al tiempo que garantiza el cifrado AES 256 estándar del sector de todos los metadatos y contenidos.

Gobierno, riesgo y cumplimiento normativo (GRC):
Al cubrir el alcance de GRC en el marco del enfoque de seguridad de Citrix y al respaldarlo a través de nuestras capacidades analíticas integrales, podemos ofrecer un enfoque mucho más sincronizado que satisfaga todas sus necesidades de seguridad y cumplimiento normativo.

← Pág. 11 | Pág. 13 →

Volver a los contenidos

> Nuestra dirección aspiraba a una forma flexible y eficiente de trabajar, pero nos tuvimos que asegurar de que era fiable. Con Citrix Workspace, sabemos que tenemos la seguridad óptima, lo que es esencial teniendo en cuenta la clase de información financiera confidencial que maneja Stater.
>
> — Frank Veldink, arquitecto de infraestructura de TIC en Stater

← Pág. 12 | Pág. 14 →

Volver a los contenidos

Descubra en **Citrix.es/secure** cómo un enfoque integrado e inteligente de la seguridad puede ayudarle a proporcionar el acceso, control y seguridad que necesita.

Fuentes:
* “The Need for a New IT Security Architecture”, Ponemon Institute, patrocinado por Citrix, 2017

Volver a los contenidos