VERTIV EBOOK

4 maneras para mejorar la seguridad del centro de datos este año

Reduzca los riesgos por medio de automatizar los procesos y usar las soluciones seguras de Vertiv

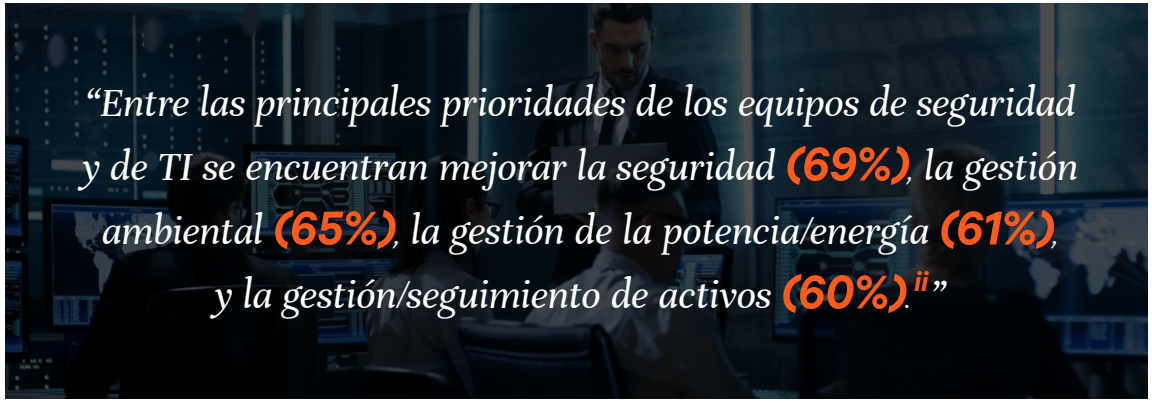
VERTIV

VERTIV EBOOK

4 maneras para mejorar la seguridad del centro de datos

Vertiv.Com

Los propietarios y operadores de centros de datos están promoviendo nueva capacidad para satisfacer la voraz demanda comercial y facilitar la transformación digital de las empresas. Solo en EE. UU., hay 526 megavatios en construcción.[i] Como resultado, los proveedores de servicios de coubicaciones, los hiperescaladores y los equipos empresariales de centros de datos y TI están gestionando espacios más grandes que nunca antes. Mucho de este trabajo tiene lugar de forma remota, lo cual presenta nuevas presiones y desafíos.



Como resultado, los equipos de centros de datos y de TI están desarrollando rápidamente su enfoque en la gestión de los dispositivos. Les gustaría simplificar los procesos por medio de adoptar las mejores herramientas y plataformas de su clase posibles:

- Facilitar un acceso remoto seguro a los dispositivos
- Mejorar la visibilidad y el control de la red
- Centralizar y estandardizar la gestión de TI
- Proteger los datos por medio de herramientas seguras de manejo de información

Ha llegado el momento de comenzar. A medida que las compañías agilizan las estrategias de digitalización, las infraestructuras serán cada vez más complejas y presentarán nuevas brechas que otros podrían aprovechar. Los equipos de centros de datos y de TI pueden usar procesos centralizados y automatizados para aportar nuevos niveles de consistencia y control para las prácticas de gestión. De esta manera, pueden ofrecer la alta disponibilidad y eficiencia que sus empresas exigen.

CONFIDENCIAL DE LA COMPAÑÍA - NO DISTRIBUIR DE FORMA EXTERNA

VERTIV.

VERTIV EBOOK

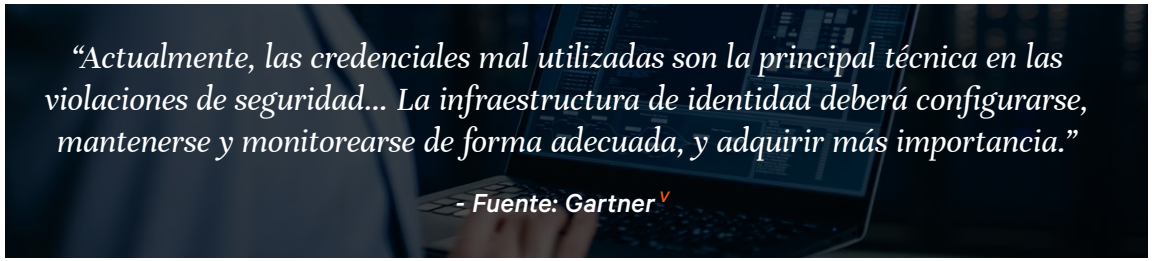
4 maneras para mejorar la seguridad del centro de datos

Vertiv.Com

Facilitar un acceso remoto seguro a los dispositivos

Los equipos de centros de datos y de TI necesitar visualizar, acceder, controlar y gestionar una gran cantidad dispositivos seriales, redes y servidores, que ponen sus negocios en funcionamiento.

Aunque estos equipos solían trabajar in situ, gran parte del personal actualmente trabaja de manera remota debido a la pandemia y seguirán haciéndolo indefinidamente. Estos usuarios son los principales objetivos de los atacantes, ya que cuentan con privilegios elevados que personas malintencionadas pueden usar para acceder a las redes de las organizaciones. En 2021, se utilizaron credenciales comprometidas en un 20% de todos los ataques.[iii] No debería de sorprender que las organizaciones estén adoptando un enfoque en seguridad basado en la identidad.[iv]



Los equipos pueden usar las soluciones de Vertiv para:

- **Otorgar acceso seguro a los dispositivos según la función o el grupo:** los administradores de TI pueden utilizar el Ecosistema Vertiv™ Avocent® ADX para autorizar a los usuarios para que lleven a cabo las principales tareas según sus puestos, como la gestión y el monitoreo de dispositivos específicos. Los administradores de TI pueden conceder privilegios a los diferentes equipos —como TI, seguridad, aplicaciones y pruebas— que necesiten acceder a los servidores y otros dispositivos de acceso a la red. El Ecosistema Avocent ADX se integra a la perfección con la Consola Serial Vertiv™ Avocent® ACS 8000 para ofrecer acceso seguro a los dispositivos seriales, con el fin de que los equipos puedan gestionar los dispositivos, recoger datos y automatizar las configuraciones.
- **Centralizar la autenticación de terceros:** los equipos de TI pueden asignar privilegios de forma dinámica a terceros claves
- **Garantizar la consistencia al otorgar acceso:** la mayoría de las organizaciones usan el concepto de privilegios mínimos, a la vez que facultan a los usuarios para realizar las funciones autorizadas. De esta manera, pueden evitarse los problemas que ocurren a la hora de acceder a derechos que no se gestionan de forma proactiva, como cuando los individuos recorren las redes y realizan acciones no autorizadas en los dispositivos.

Ecosistema Avocent® ADX

Avocent® ACS 8000

CONFIDENCIAL DE LA COMPAÑÍA - NO DISTRIBUIR DE FORMA EXTERNA

VERTIV

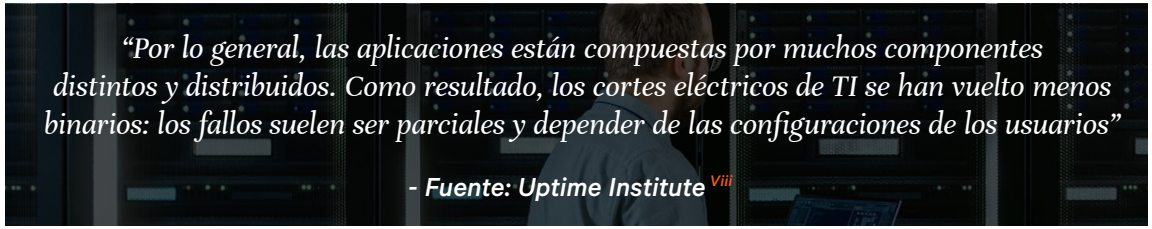
VERTIV EBOOK

4 maneras para mejorar la seguridad del centro de datos

Mejorar la visibilidad y el control de la red

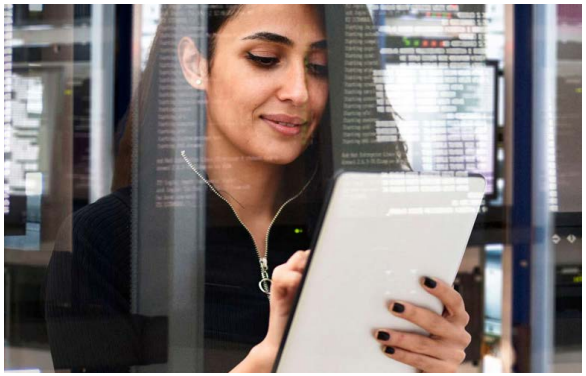
La conectividad está en todas partes: en todos los centros de datos empresariales y sitios de borde, en miles de servicios en la nube de hiperescaladores y en la infraestructura de proveedores de coubicaciones. Para 2025, el 85% de las estrategias de infraestructura integrarán opciones de entrega en la nube, coubicaciones e instalaciones, en comparación con el 20% durante 2020.[vi] Esto se debe a que los equipos de TI colocan las cargas de trabajo estratégicamente para obtener los mejores resultados.[vii]

Los equipos de centros de datos y de TI necesitan mejorar la visibilidad y el control, sin importar dónde trabajen y qué gestionen. Esto resulta mucho más importante para los proveedores externos, ya que el error humano o las brechas de seguridad aprovechadas pueden afectar en gran medida el negocio y perjudicar a miles o millones de clientes.



Los equipos pueden usar las soluciones de Vertiv para:

- **Utilizar un único punto de autenticación:** los equipos pueden usar el Ecosistema Avocent® ADX para un punto único de acceso al servidor y otros dispositivos de TI, mientras que el Avocent® ACS 8000 ofrece acceso agregado a los dispositivos seriales. Al centralizar la visibilidad y el acceso, los profesionales de centros de datos y de TI pueden trabajar de forma más eficiente y cumplir con sus labores de gestión tanto en banda como fuera de banda.
- **Controlar lo que los usuarios pueden ver:** el Ecosistema Avocent ADX permite que los equipos puedan controlar los dispositivos que los usuarios individuales pueden visualizar. Esto resulta crítico para los proveedores de hiperescala y coubicaciones, los cuales querrán segmentar el acceso para que los clientes solo puedan visualizar sus propios dispositivos. De manera similar, los súperusuarios pueden controlar lo que los equipos en otras unidades empresariales, terceros y otras partes autorizadas pueden visualizar.



- **Auditar el comportamiento de los usuarios:** muchas compañías necesitan generar reportes sobre las acciones en los dispositivos y el acceso de los usuarios para fines de auditoría y cumplimiento normativo. El Ecosistema Avocent ADX permite que los administradores puedan monitorear quién hace qué, cuándo lo hace y cómo lo hace. Pueden monitorear cualquier tecla que los usuarios opriman, al acceder a los dispositivos mediante el Avocent ACS 8000. Además, se pueden establecer alertas para secuencias con el fin de recibir alertas tempranas de acciones de alto perfil. Finalmente, el personal de TI puede ofrecer acceso al registro de datos tanto en línea como sin conexión con marcas de tiempo por parte del Avocent ACS 8000 para fines de análisis e informes.

CONFIDENCIAL DE LA COMPAÑÍA - NO DISTRIBUIR DE FORMA EXTERNA

VERTIV

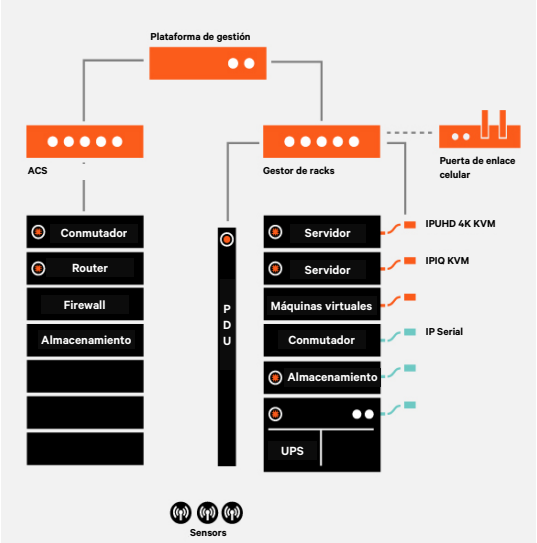
VERTIV EBOOK

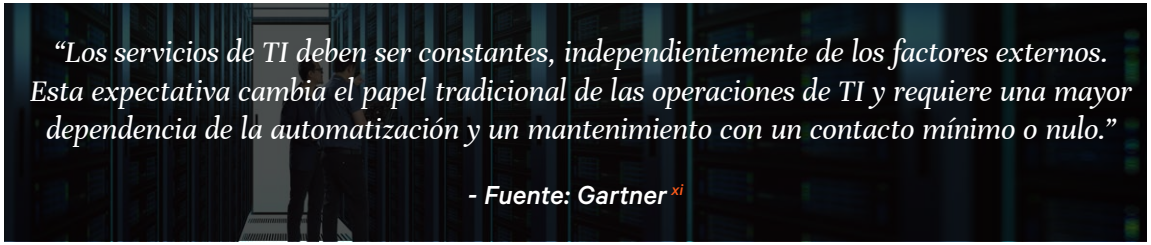
4 maneras para mejorar la seguridad del centro de datos

Centralizar y estandarizar la gestión de TI

La proliferación de dispositivos de red ha creado una mayor complejidad para los equipos de centros de datos y de TI. La mayoría de proveedores ofrece sus propias herramientas para gestionar sus dispositivos. Como resultado, el 64% de las empresas actualmente utiliza entre 4 y 10 herramientas para gestionar las redes.[ix] Usar demasiadas herramientas puede generar brechas de seguridad en los procesos o aumentar los riesgos de errores humanos, tanto en las medidas adoptadas como en las no adoptadas.

Los equipos de centros de datos y de TI quieren centralizar y automatizar la gestión de las redes, los servidores y los dispositivos seriales.





Los equipos que implementan soluciones de Vertiv pueden:

- **Agregar dispositivos para mejorar la seguridad:** conectar cada dispositivo a Internet aumenta drásticamente la superficie de ataque, lo cual incrementa los riesgos. Los equipos pueden utilizar el gestor de racks Vertiv™ Avocent® ADX para conectar hasta 48 dispositivos y ocultarlos de la visualización y el acceso en red mediante colocarlos en una red privada. Solo los usuarios autorizados pueden acceder a los dispositivos y adoptar las medidas para las que están autorizados.

- **Diagnosticar y hacer frente a cualquier problema rápidamente:** se espera que los equipos de TI ofrezcan disponibilidad de las aplicaciones y un funcionamiento continuo que faciliten los procesos empresariales digitales. Como resultado, hay una gran presión en identificar y resolver de forma proactiva los problemas, así como las interrupciones en la red. Los equipos pueden utilizar el Avocent® ACS 8000 para llevar a cabo los procesos de gestión tanto en banda como fuera de banda, por medio de conectividad con módem análogo, Ethernet o móvil para acceder a los dispositivos

- **Automatizar las actualizaciones de firmware:** el firmware fuera de banda es uno de los objetivos principales de los criminales cibernéticos, quienes monitorean activamente las redes en búsqueda de estos problemas. Sin embargo, a pesar de esta realidad, los equipos de seguridad afirman que dedican el 41% de su tiempo a instalar parches de firmware manualmente, los cuales podrían no estar actualizados. Los equipos de seguridad y de TI pueden utilizar la Plataforma de gestión Avocent ADX para automatizar las actualizaciones de firmware de los servidores y eliminar esta brecha de seguridad para siempre.

CONFIDENCIAL DE LA COMPAÑÍA - NO DISTRIBUIR DE FORMA EXTERNA

VERTIV

VERTIV EBOOK

4 maneras para mejorar la seguridad del centro de datos

Vertiv.Com

Proteger los datos por medio de herramientas seguras de manejo de información

Los datos son el alma de las industrias; alimentan las operaciones clave e impulsan el crecimiento empresarial. Las compañías producen y gestionan una amplia variedad de datos confidenciales y sensibles que se rigen estrictamente por las normativas de la industria.

Las compañías biofarmacéuticas quieren proteger la investigación y los datos farmacológicos; las fugas pueden perjudicar su capacidad de mantener y obtener las aprobaciones normativas para sus medicamentos y hacerles perder terreno con respecto a sus competidores. Los equipos de servicios financieros trabajan con los datos comerciales y de los clientes, los cuales están protegidos por normativas como GDPR, GLBA, NYDFS y PCI-DSS. Los empleados gubernamentales necesitan utilizar datos sensibles, clasificados y no clasificados que viajan por la red como JWICS, SIPRNet y NIPRNet. Finalmente, en lo relacionado con la atención médica, los médicos acceden a los registros médicos que contienen información de carácter personal (PII, por sus siglas en inglés) e información médica personal (PHI, por sus siglas en inglés) protegida por HIPAA.

Sin importar cuál sea la industria, los seguros KVM de escritorio Vertiv™ Cybex™ SC pueden ayudar a los trabajadores a acceder a datos sensibles, dentro de los límites de los estrictos controles de seguridad:

- **Navegar fácilmente a través de las fuentes de información:** la conmutación de navegación del cursor permite que los trabajadores puedan visualizar de forma segura información con múltiples niveles de clasificación en la misma pantalla. Esto es ideal para las operaciones gubernamentales sensibles, como la gestión de infraestructuras críticas o las labores militares o de inteligencia.
- **Eliminar la contaminación cruzada de la información:** la información puede contaminarse y filtrarse cuando los usuarios adoptan medidas no aprobadas. Las organizaciones pueden usar los KVM seguros de escritorio Cybex™ SC para evitar que se copie, corte y pegue información en los niveles de clasificación. Aunque las agencias gubernamentales necesitan este tipo de protección periódicamente, otras industrias podrían usarlo para tareas como la revisión de los datos confidenciales de desarrollo de productos o las finanzas de las compañías absorbidas durante las fusiones y las adquisiciones.

- **Eliminar la manipulación de los dispositivos:** los seguros KVM de escritorio Cybex SC ofrecen las siguientes protecciones para evitar la manipulación. La detección de manipulación desactiva los KVM si se penetran sus sellos. Además, el firmware bloqueado evita que los usuarios realicen acciones no autorizadas en las operaciones de KVM.

CONFIDENCIAL DE LA COMPAÑÍA - NO DISTRIBUIR DE FORMA EXTERNA

VERTIV

VERTIV EBOOK

4 maneras para mejorar la seguridad del centro de datos

Vertiv.Com

Conclusión

La red es cada vez más compleja, lo cual crea presiones sobre los equipos de centros de datos y de TI para optimizar los procesos actuales y mejorar la seguridad. Estos profesionales pueden contribuir a alcanzar estos objetivos al facilitar un acceso remoto seguro a los dispositivos, mejorar la disponibilidad y el control de la red, centralizar y estandarizar la gestión de TI y proteger los datos mediante herramientas seguras de manejo de información.

Permita que este sea el año en que pueda beneficiarse de una mayor seguridad y control, una mayor consistencia en los procesos de gestión y la simplificación de la administración diaria por medio de la automatización.

Mejore la seguridad del centro de datos de cuatro maneras con Vertiv.

Conozca más sobre:

Ecosistema Vertiv™ Avocent® ADX

Servidor de consola serial Avocent® ACS 8000

KVM seguros de escritorio Vertiv™ Cybex™ SC

Recursos

¿Le gustaría conocer más sobre cómo mejorar la seguridad del centro de datos? Eche un vistazo a estos recursos:

- Permita que los trabajadores manejen de forma segura la información sensible y confidencial
- El establecimiento de controles específicos para los dispositivos de red de TI ahora es más sencillo que nunca
- ¿Cómo pueden los equipos de ciberseguridad y de TI trabajar hombro a hombro para fortalecer la seguridad en la gestión de los servidores?

[i] "Data Centers," capítulo 8, U.S. Real Estate Market Outlet 2022, informe CBRE, no fechado, https://www.cbre.com/insights/books/us-real-estate-market-outlook-2022/data-centers#.
[ii] Ibid.
[iii] "How much does a data breach cost?" página web, IBM, https://www.ibm.com/security/data-breach
[iv] Kasey Panetta, "The Top 8 Security and Risk Trends We're Watching," artículo, Gartner, 21 de noviembre de 2021, https://www.gartner.com/smarterwithgartner/gartner-top-security-and-risk-trends-for-2021
[v] Ibid.
[vi] Agregar referencia
[vii] David Cappuccio, Henrique Cecci, Your Data Center May Not Be Dead, but It's Morphing, Gartner, informe, 17 de septiembre de 2020, https://www.equinix.com/resources/analyst-reports/data-center-not-dead-morphing-changing?
[viii] Rich Miller, "The Eight Trends That Will Shape the Data Center in 2022," Data Center Frontier, 10 de enero de 2022, https://datacenterfrontier.com/the-eight-trends-that-will-shape-the-data-center-industry-in-2022/
[ix] EMA: Network Management Megatrends, 2020, Kentik, pág. 4, https://www.kentik.com/resources/ema-network-management-megatrends-2020-report/
[x] "New Security Signals study shows firmware attacks on the rise; here's how Microsoft is working to help eliminate this entire class of threats," artículo, Microsoft, 30 de marzo de 2021, https://www.microsoft.com/security/blog/2021/03/30/new-security-signals-study-shows-firmware-attacks-on-the-rise-heres-how-microsoft-is-working-to-help-eliminate-this-entire-class-of-threats/
[xi] "Gartner Top 6 Trends," ibid.
[xii] "How much does a data breach cost?" IBM, ibid.

Vertiv.com | **Sede de Vertiv,** 1050 Dearborn Drive, Columbus, OH, 43085, EE.UU.

© 2022 Vertiv Group Corp. Todos los derechos reservados. Vertiv™ y el logo de Vertiv son marcas o marcas registradas de Vertiv Group Corp. Todos los demás nombres y logos a los que se hace referencia son nombres comerciales, marcas, o marcas registradas de sus dueños respectivos. Aunque se tomaron todas las precauciones para asegurar que esta literatura esté completa y exacta, Vertiv Group Corp. no asume ninguna responsabilidad y renuncia a cualquier demanda por daños como resultado del uso de esta información o de cualquier error u omisión. Las especificaciones, los reembolsos y otras ofertas promocionales están sujetas a cambio a la entera discreción de Vertiv y mediante notificación.

SL-70939 (R010/22)