Mejora de la seguridad y el cumplimiento

Reduzca los riesgos con una plataforma Linux sólida y open source

Red Hat

Conozca el contenido

Linux: la base para el futuro

Linux® es uno de los sistemas operativos líderes del mundo, y cuenta con una amplia adopción en diversos sectores y tecnologías nuevas[1]. Suele utilizarse en cargas de trabajo importantes, confiables y con alta disponibilidad en los centros de datos y los entornos de cloud computing; además, admite varios casos de uso, sistemas objetivo y dispositivos. Todos los proveedores de nube pública importantes ofrecen varias distribuciones de Linux en el mercado.

Sin embargo, las herramientas de gestión y distribución de Linux que elija pueden afectar considerablemente la eficiencia, la seguridad y la interoperabilidad de su entorno de TI. En este ebook se analizan los aspectos fundamentales que se debe tener en cuenta sobre los riesgos relacionados con el cumplimiento normativo y los puntos vulnerables de seguridad en los entornos de Linux, y se proporcionan algunas pautas al respecto.

La seguridad y el cumplimiento normativo son dos de las preocupaciones más importantes en materia de TI

La gestión de los riesgos relacionados con el cumplimento normativo y la seguridad de la TI es una preocupación constante para todas las empresas. De hecho, el 33 % de los directores ejecutivos considera que los ciberataques son una de las principales amenazas al posible crecimiento de sus empresas [2]. Además, el costo de los fallos de seguridad puede ser muy elevado. Por ejemplo, en el caso de una filtración de datos, el costo promedio es de US$ 3,86 millones[3].

A todo esto se suma que las normas gubernamentales y del sector cambian constantemente, así que el mantenerse al día es todo un desafío. Además, la falta de cumplimiento normativo aumenta el costo de una filtración de datos en un promedio de aproximadamente 6 %[3].

Efectos de la falta de eficacia en materia de seguridad

Para reducir los riesgos relacionados con los fallos de seguridad y su impacto, la velocidad es fundamental.

US$ 3,86 millones
es el costo promedio de una filtración de datos en 2020[3]

280 días
es el tiempo promedio que se necesita para identificar y evitar una filtración de datos en 2020[3]

US$ 1,12 millones
es la suma que se puede ahorrar si se identifica y evita un fallo de seguridad en un plazo de menos de 200 días[3]

Desafíos comunes en torno a la seguridad y el cumplimiento normativo

Son varios los factores que dificultan la gestión del cumplimiento normativo y de los puntos vulnerables en materia de seguridad:

Panorama de seguridad y cumplimento normativo en constante cambio

Las amenazas a la seguridad evolucionan a gran velocidad, así que resulta indispensable poder responder rápidamente a ellas y a las normas en constante cambio.

Entornos de nube híbrida y multicloud distribuidos

Es muy difícil obtener un panorama completo de la TI debido a la distribución geográfica y lógica de los entornos.

Entornos grandes y complejos

Las grandes infraestructuras suelen incluir varias herramientas para la seguridad y el cumplimiento normativo, lo cual dificulta la gestión de riesgos.

Directivas de trabajo a distancia y personal limitado

La mayoría de las empresas carecen de la dotación de personal necesaria para gestionar las tareas de seguridad y cumplimiento normativo de forma manual.

1 *The Linux Foundation.* "**Linux is the most successful open source project in history**". *Se consultó el 24 de septiembre de 2020.*

2 *PWC.* "**23rd Annual Global CEO Survey: Navigating the rising tide of uncertainty**". *2020.*

3 *IBM Security.* "**Cost of a Data Breach Report 2020**". *2020.*

Adopte un enfoque efectivo para la gestión de los riesgos de seguridad y cumplimiento normativo

La gestión del cumplimiento de las normas y de los puntos vulnerables en materia de seguridad consiste en supervisar y evaluar los sistemas, para garantizar que cumplan con las políticas correspondientes. Un enfoque ideal para este tipo de gestión le permitirá desarrollar procesos uniformes y repetibles en todo su entorno para:

Realizar evaluaciones
Identifique los sistemas que no cumplan con las normas o que presenten puntos vulnerables; evalúe fácilmente el estado actual de la seguridad de su entorno, desde la infraestructura hasta la carga de trabajo; y de todos los avisos de seguridad que hay, distinga cuáles realmente corresponden a sus sistemas y a su entorno.

Establecer un orden de prioridad
Organice las medidas de corrección en función del esfuerzo, el impacto y la gravedad del problema. Utilice técnicas de gestión de riesgos para determinar el peligro empresarial real que presenta cada problema, y planifique iniciativas para corregirlos en consecuencia. Los riesgos incluyen la posibilidad de que alguno de los problemas dé como resultado un fallo de seguridad, la gravedad potencial de ese fallo y las consecuencias de solucionar el inconveniente. Es posible que resolver ciertos problemas en los sistemas de desarrollo y prueba no tenga la misma importancia que solucionarlos en los de producción.

Solucionar problemas
Ejecute parches en todos los sistemas que lo requieran y vuelva a configurarlos de manera rápida y sencilla. Automatice los procesos de configuración y ejecución de parches para agilizar la resolución de problemas, garantizar la uniformidad en todos los sistemas y reducir el riesgo de que se cometan errores humanos. Si utiliza las herramientas automatizadas de forma eficaz, podrá solucionar los problemas rápidamente y mejorar la seguridad de su entorno y su empresa.

Generar informes
Corrobore que los cambios se hayan implementado correctamente, y automatice la generación de informes sobre las correcciones para agilizar los trabajos de auditoría. La elaboración eficaz de informes le permite proporcionar información con el nivel de detalle adecuado para que los directivos, los auditores y los equipos técnicos entiendan cuáles son las exposiciones y los riesgos actuales en materia de seguridad.

Asimismo, este enfoque prepara a su empresa para las técnicas de desarrollo y gestión modernas, como **DevSecOps**, las cuales evolucionan rápidamente. De hecho, el 38 % de las empresas considera que la evaluación de los puntos vulnerables es el elemento de seguridad más importante en su flujo de trabajo de DevOps[4].

En las siguientes secciones, se analizan los aspectos fundamentales que se deben tener en cuenta para gestionar con mayor eficacia los riesgos relacionados con la seguridad y el cumplimiento normativo, así como las medidas que se deben tomar al respecto.

4 451 Research, parte de S&P Global Market Intelligence. Voice of the Enterprise: DevOps H2 2019.

Identifique y corrija los puntos vulnerables en los entornos de Linux

La identificación de los puntos vulnerables y la aplicación de correcciones es el proceso por el cual se evalúa la infraestructura para detectar los sistemas que son vulnerables a los ataques, con el fin de implementar las soluciones pertinentes. Las amenazas nuevas, los parches desactualizados o faltantes y los errores de configuración del sistema son factores que pueden generar puntos vulnerables. Para eliminarlos, se suelen aplicar medidas de corrección que incluyen la ejecución de parches, la implementación de actualizaciones y la reconfiguración de los sistemas.

¿Por qué es importante?

Los puntos vulnerables de seguridad pueden generar fallos costosos que, a su vez, también podrían influir en la confianza de los clientes, la reputación de la empresa y los ingresos. De hecho, la pérdida de utilidades representa el 39,4 % del costo promedio de una filtración de datos[5].

Los desafíos que implican la identificación y la corrección eficaces de los puntos vulnerables

La mayoría de las empresas no posee una estrategia de seguridad uniforme que se pueda aplicar a las operaciones según sea necesario.

- El personal limitado se siente abrumado y es posible que no tenga las habilidades necesarias para desarrollar y ejecutar una estrategia completa de seguridad.
- Las herramientas genéricas de análisis de seguridad crean listas enormes de posibles puntos vulnerables, pero no todos ellos corresponden a su entorno, lo cual implica que el personal dedica mucho tiempo a investigar esos puntos y las medidas de corrección pertinentes.
- Los procesos manuales de identificación, corrección y seguimiento ralentizan las operaciones. Además, por lo general no se ejecutan los parches correspondientes en los puntos vulnerables conocidos.
- Los métodos de corrección ad hoc dan lugar a una falta de consistencia en la ejecución de parches y a un aumento de los posibles riesgos de seguridad.

Características fundamentales de las herramientas de gestión de la seguridad

Si lo que necesita es mayor efectividad, debe poder identificar y corregir los puntos vulnerables del sistema rápidamente, antes de que generen alguna falla. Para lograrlo, busque herramientas unificadas que:

Realicen análisis para identificar los riesgos de los sistemas y las instancias de su entorno, ya sea en el sistema operativo o en las cargas de trabajo.

Automaticen la corrección de los riesgos que se identifican para mejorar la velocidad, la precisión y la eficiencia de los equipos de TI y de seguridad.

Incorporen los conocimientos de los proveedores para que brinden pautas sobre la corrección de los fallos en sus productos. Posiblemente haya medidas sencillas que pueda implementar para reducir los riesgos.

Accedan con regularidad a los datos más recientes sobre los riesgos de seguridad y los puntos vulnerables conocidos de su sistema operativo y sus proveedores de aplicaciones.

Generen informes bien detallados sobre los riesgos potenciales, las medidas de corrección y las auditorías para los diferentes destinatarios.

5 *IBM Security.* "**Cost of a Data Breach Report 2020**". *2020.*

Gestione el cumplimento normativo en los entornos de Linux

La gestión del cumplimiento normativo es un proceso que garantiza que los sistemas cumplan las políticas corporativas, los estándares del sector y las normas aplicables conforme pasa el tiempo. Realiza una evaluación de la infraestructura para identificar los sistemas que no cumplen con las normativas debido a los cambios relacionados con los estándares, las políticas o las normas; a los errores de configuración, o a otras razones.

¿Por qué es importante?

El incumplimiento de las normas puede derivar en multas, daños a la empresa, pérdida de certificaciones y fallos de seguridad. Además, suele aumentar los costos de las filtraciones de datos[6].

Los desafíos que implica la gestión eficaz del cumplimiento normativo

Muchas empresas gestionan el cumplimento normativo a través de operaciones manuales y scripts personalizados. Estos procesos son demasiado lentos y tienen un alcance muy limitado para seguir el ritmo de las operaciones y el desarrollo modernos, los cuales evolucionan rápidamente.

- Dada la gran variedad de normas y estándares genéricos que hay, resulta difícil comprender la importancia y el efecto que tiene la gestión del cumplimiento normativo sobre su entorno.
- Los procesos manuales retrasan las operaciones de supervisión, corrección y auditoría del cumplimiento normativo, lo cual ocasiona que el tiempo del personal no se emplee adecuadamente, las políticas no se apliquen de forma uniforme y aumente el riesgo de problemas de cumplimiento.
- Muchas empresas utilizan diferentes herramientas para gestionar la seguridad y el cumplimiento normativo, lo cual reduce la eficiencia operativa y dificulta el establecimiento de políticas uniformes y personalizadas.

Características fundamentales de las herramientas de gestión del cumplimiento normativo

Si lo que necesita es mayor efectividad, debe poder definir y aplicar políticas en función del contexto, asegurarse de que los sistemas se ejecuten de conformidad con ellas, y generar y gestionar rápidamente los informes de cumplimiento normativo para realizar auditorías. Para lograrlo, busque herramientas unificadas que:

Realicen análisis para identificar sistemáticamente los riesgos relacionados con el cumplimiento normativo de manera tal que permita ahorrar tiempo.

Apliquen correcciones automáticas en los sistemas que no cumplan con las normas.

Proporcionen un panorama completo de su estrategia de cumplimiento normativo en su entorno.

Generen automáticamente informes de cumplimiento normativo, de acuerdo con los requisitos de auditoría y las necesidades de los destinatarios.

Brinden asesoramiento de expertos e indicaciones en función del contexto, para aplicar correcciones en los sistemas del entorno que no cumplan con las normas.

6 *IBM Security.* "**Cost of a Data Breach Report 2020**". *2020.*

Prácticas recomendadas

Analice los sistemas con frecuencia

Supervisar a diario los sistemas puede ayudarlo a identificar los puntos vulnerables y los riesgos relacionados con el cumplimiento normativo, antes de que interrumpan las operaciones comerciales o den lugar a fallos de seguridad. Asegúrese de utilizar los datos de seguridad más recientes, tanto de su sistema operativo como de sus proveedores de aplicaciones, para mejorar la precisión de los análisis. Además, deberá establecer políticas de seguridad personalizadas que se adapten a su entorno y sus operaciones, para obtener resultados de cumplimiento normativo más precisos.

Detectar y detener un fallo de seguridad en un plazo de **200 días** o menos puede reducir considerablemente el costo resultante[7].

Aplique parches con regularidad y pruébelos

Mantener los sistemas actualizados aumenta la seguridad, la confiabilidad, el rendimiento y el cumplimiento normativo. Aplique parches con regularidad para poder solucionar los problemas importantes en general. En el caso de los errores y los defectos más severos, procure ejecutar los parches a la brevedad. Además, pruebe los sistemas en los que se aplicaron parches para asegurarse de que funcionen correctamente antes de volver a ejecutarlos en la etapa de producción.

Una herramienta efectiva de gestión de parches le permite ejecutarlos en los sistemas hasta un **88,9 % más rápido**[8].

Implemente la automatización

A medida que la infraestructura crece y su complejidad aumenta, se vuelve más complicado gestionarla de forma manual. Implemente la automatización para optimizar la supervisión, agilizar la corrección de errores, mejorar la uniformidad y garantizar la generación de informes periódicos.

Si automatiza la seguridad, puede reducir el costo promedio de un fallo de seguridad en un **93 %**[7].

Combine sus herramientas y coordine sus procesos

Los entornos distribuidos suelen incluir diferentes herramientas de gestión para cada plataforma. Intégrelas a través de interfaces de programación de aplicaciones (API) y utilice sus interfaces preferidas para llevar a cabo las tareas en otras herramientas. Use menos interfaces para optimizar las operaciones y mejorar la supervisión del estado de seguridad y cumplimiento de todos los sistemas de su entorno. Además, coordine sus procesos en todos los entornos para obtener mayor uniformidad y confiabilidad.

El 52 % de las empresas optimiza sus procesos e infraestructura de TI para mejorar la seguridad en la actualidad[9].

Adopte una estrategia de seguridad uniforme y permanente

Para que la seguridad sea eficaz, se necesita un enfoque integral que combine el personal, los procesos y la tecnología. Una estrategia de seguridad permanente se basa en los comentarios y la adaptación, para respaldar las técnicas modernas de desarrollo, DevSecOps y las necesidades de las empresas digitales. Adopte un enfoque de seguridad en capas y con protección integral para aprovechar al máximo las funciones de cada capa de su entorno, las cuales incluyen los sistemas operativos, las plataformas de los contenedores, las herramientas de automatización, los recursos de software como servicio (SaaS) y los servicios de nube.

Si adopta un enfoque de DevSecOps, podrá reducir en un **5 %** el costo promedio de una filtración de datos[7].

7 *IBM Security. "**Cost of a Data Breach Report 2020**", 2020.*

8 *Principled Technologies, patrocinado por Red Hat. "**Utilice Red Hat Insights para automatizar la supervisión, y permita que los administradores ahorren tiempo y dinero**". Septiembre de 2020.*

9 *Qualtrics y Red Hat. "Estudio sobre la optimización de la TI". Febrero de 2020.*

Recomendaciones sobre las herramientas

Las herramientas ideales de seguridad y cumplimiento normativo deben incluir varias características y funciones clave.

Análisis preventivo

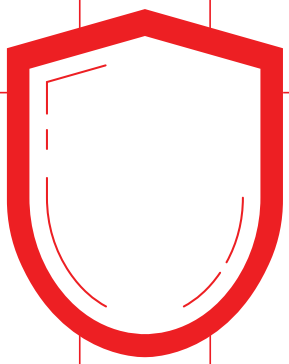
Comprender cuál es su estrategia de seguridad y cumplimiento normativo es el primer paso para mejorarla. Las herramientas que ofrecen análisis automatizados garantizan la supervisión periódica de los sistemas y le advierten sobre los problemas encontrados, sin malgastar el tiempo ni el esfuerzo del personal.

Corrección prioritaria

Si cuenta con herramientas que proporcionan pautas de corrección prescriptivas, ya no tendrá que investigar por su propia cuenta las medidas que se deben implementar, lo cual le permitirá ahorrar tiempo y reducir el riesgo de errores. Poder priorizar las medidas que se deben tomar en función del impacto potencial y de los sistemas que podrían verse afectados le permite aprovechar al máximo los períodos limitados para la ejecución de parches.

Resultados personalizables

Es posible que algunas verificaciones de los puntos vulnerables y el cumplimiento normativo no se apliquen a ciertos sistemas debido a su configuración, uso o carga de trabajo específicos. Las herramientas ideales son aquellas que le permiten definir el contexto empresarial para reducir los falsos positivos, gestionar el riesgo comercial y proporcionar un panorama más realista del estado de la seguridad y el cumplimiento normativo.



Generación intuitiva de informes

Las herramientas que generan informes claros e intuitivos sobre los sistemas que se actualizaron con parches, los que aún los necesitan y los que no cumplen las políticas de seguridad, aumentan la capacidad de auditoría y ayudan a comprender mejor el estado del entorno.

Interfaz unificada

Las herramientas que gestionan más de un elemento o capa de su entorno lo ayudan a simplificar las operaciones de seguridad y a conocer mejor su estrategia de seguridad y cumplimiento normativo. Asimismo, las herramientas unificadas ofrecen un mayor contexto para las revisiones y las pautas sobre la corrección de fallos.

Información útil

Las herramientas que proporcionan información que se adapta a su entorno lo ayudan a identificar, con mayor rapidez, los problemas de cumplimiento normativo y los puntos vulnerables de seguridad presentes, los sistemas que se ven afectados y los posibles efectos que puede esperar. Asimismo, le permiten establecer la prioridad de las medidas de corrección y planificarlas.

Aumente su nivel de seguridad y cumplimiento normativo gracias a Red Hat

Red Hat adopta un enfoque integral para la gestión de los riesgos relacionados con la seguridad y el cumplimiento normativo que mejora la velocidad, la capacidad de expansión y la estabilidad en todo su entorno de TI, desde los servidores sin sistema operativo y los virtualizados hasta las infraestructuras de nube privada, pública e híbrida. Las plataformas de Red Hat® combinan el personal, los procesos y la tecnología para que logre una mayor eficiencia operativa, aumente la capacidad de innovación y mejore el nivel de satisfacción de los empleados.

La esencia de esta estrategia es **Red Hat Enterprise Linux**: una base operativa inteligente y uniforme para las implementaciones modernas de TI y de nube híbrida empresarial que ofrece beneficios insuperables para su empresa. La coherencia en toda la infraestructura le permite implementar aplicaciones, cargas de trabajo y servicios utilizando las mismas herramientas, independientemente de dónde se encuentre.

La seguridad es una parte fundamental de la arquitectura y del ciclo de vida de Red Hat Enterprise Linux. Los sistemas de protección contra fallos en varias capas utilizan controles de seguridad automatizados y repetibles para reducir el riesgo de exposición a puntos vulnerables. Asimismo, las actualizaciones de seguridad importantes y la ejecución activa de parches, que se incluyen como parte de su suscripción a Red Hat Enterprise Linux, mantienen su entorno actualizado y más protegido.

Las herramientas de gestión de Red Hat se integran con Red Hat Enterprise Linux a fin de proporcionar las funciones que se necesitan para gestionar con eficacia el cumplimiento normativo y los riesgos relacionados con los puntos vulnerables.

Los estándares y las herramientas configurables reducen los falsos positivos y le proporcionan un panorama preciso del estado de su infraestructura.

Las funciones de automatización mejoran la precisión de la configuración y de la ejecución de parches, y además reducen la cantidad de errores humanos.

Las vistas personalizables proporcionan la información correcta en el momento adecuado y de forma rápida.

La corrección automatizada y anticipada de errores le permite solucionar los problemas más rápido, sin que necesite comunicarse con el equipo de asistencia técnica.

Una amplia biblioteca de recursos proporciona información detallada y específica de forma ininterrumpida.

Las opciones para las instalaciones y de software como servicio (SaaS) le permiten implementar herramientas en función de sus preferencias.

"Para nuestra empresa de TI es fundamental que desde el primer día podamos crear servidores que se adapten a nuestras necesidades, que estén listos para utilizarse y que sean más seguros. Con Red Hat Enterprise Linux y Red Hat Insights ahora es posible, ya que nos permiten implementar servidores que se pueden poner en marcha de inmediato y que satisfacen nuestras necesidades en cuanto comienzan a utilizarse"[10].

Steve Short
Gerente de plataformas, Unix, Kingfisher PLC

10 *Comunicado de prensa de Red Hat. "**Red Hat ofrece un multiplicador de fuerza para la TI empresarial con supervisión inteligente mejorada, y presenta su última versión de Red Hat Enterprise Linux 8**". 21 de abril de 2020.*

Aproveche las herramientas de gestión integradas

Las herramientas de gestión de Red Hat se basan en años de experiencia en el desarrollo y el soporte de Linux. Ambas se integran para mejorar la administración de la TI y, de esta manera, desarrollar un entorno más seguro, optimizado y confiable, y permitirle a su equipo ahorrar tiempo y esfuerzo.

Red Hat Insights

Análisis predictivo de los riesgos de TI

Red Hat Insights se incluye con todas las suscripciones activas a Red Hat Enterprise Linux y permite que los equipos de TI identifiquen y solucionen de manera anticipada varias amenazas, para evitar interrupciones, downtime imprevisto y riesgos relacionados con la seguridad y el cumplimento normativo.

- Analice los sistemas en profundidad para detectar lo antes posible puntos vulnerables de seguridad, problemas de cumplimiento normativo e infracciones de las políticas.
- Determine las medidas de corrección, póngales prioridades, y genere playbooks de Red Hat Ansible® Automation Platform útiles para tal fin.
- Compare los sistemas con los estándares, los historiales y otros sistemas.
- Realice implementaciones en los entornos de las instalaciones y de nube con facilidad.

Un 96 % más de velocidad en la detección de problemas específicos de las aplicaciones[11].

Un 91 % más de velocidad en la identificación de los puntos vulnerables de seguridad[11].

Un 89 % más de velocidad en la detección de desajustes de configuración[11].

Obtener más información

Red Hat Smart Management

Procesos útiles de gestión y corrección de errores

Red Hat Smart Management combina las funciones sólidas de la infraestructura de Red Hat Satellite con la facilidad de gestión de la nube, para mejorar y complementar las funciones de Red Hat Insights.

- Prepare y controle los hosts de Red Hat Enterprise Linux, y aplique parches en ellos, con Red Hat Satellite. Además, genere informes detallados utilizando la misma herramienta.
- Identifique y corrija los errores a través de la página cloud.redhat.com junto con Red Hat Insights.
- Solucione los problemas que Red Hat Insights identificó con solo presionar un botón a través de Cloud Connector.

Un 56 % más de eficiencia en la ejecución de parches en los sistemas[12].

Un 14 % más de eficacia por parte de los equipos de seguridad de la TI[12].

Un 23 % más de productividad por parte de los equipos encargados del cumplimiento normativo[12].

Obtener más información

11 *Principled Technologies, patrocinado por Red Hat.* "**Utilice Red Hat Insights para automatizar la supervisión, y permita que los administradores ahorren tiempo y dinero**". *Septiembre de 2020.*

12 *Whitepaper de IDC, patrocinado por Red Hat.* "**Red Hat Satellite ayuda a que las empresas optimicen la infraestructura con las herramientas de automatización**". *Marzo de 2020. Documento #US46109220.*

Aspectos destacados de los casos de éxito de los clientes

Metalloinvest

Utilice la información relevante y el análisis predictivo de los riesgos para garantizar el rendimiento de los sistemas más importantes.

El desafío

Metalloinvest es uno de los principales fabricantes y proveedores mundiales de hierro briqueteado en caliente (HBI) y productos de mineral de hierro; además, es productor regional de acero de alta calidad. Tras décadas de actividad en el mercado, la empresa se enfrentó a un nuevo desafío: la industria 4.0, es decir, la adopción de operaciones automatizadas y centradas en los datos por parte del sector encargado de la fabricación. Metalloinvest espera automatizar y digitalizar la producción para poder operar y utilizar los recursos de forma más eficiente. Además, su objetivo no es convertirse solo en la empresa minera más grande del mundo, sino también en la más productiva. Por lo tanto, necesitaba integrar y optimizar su entorno complejo de SAP® a fin de crear una base para esta cuarta revolución industrial.

La solución

Gracias a la ayuda de su proveedor de servicios gestionados, JSA Group, Metalloinvest adoptó Red Hat Enterprise Linux for SAP Solutions para crear una base empresarial sólida para su entorno de SAP S/4HANA®. La solución Red Hat Enterprise Linux for SAP Solutions, que diseñaron **Red Hat y SAP**, incluye Red Hat Insights, para realizar análisis predictivos de datos, y Red Hat Smart Management, para simplificar la gestión de los entornos de Red Hat Enterprise Linux a través de los servicios de gestión de nube y Red Hat Satellite. Esta suscripción única combina la confiabilidad, la capacidad de expansión y el alto rendimiento de Linux con tecnologías que cumplen con los requisitos específicos de las aplicaciones de SAP.

Actualmente, Metalloinvest ejecuta todo su entorno de producción de SAP S/4HANA en Red Hat Enterprise Linux for SAP Solutions. La empresa aprovecha toda la información relevante y el análisis predictivo de los riesgos para garantizar un rendimiento confiable y estable en sus sistemas importantes, mientras se prepara para digitalizar su entorno de producción.

"Gracias a Red Hat, contamos con las herramientas necesarias para aumentar la productividad de nuestro personal y nuestras operaciones".

Konstantin Zelenkov
Director de tecnología, JSA Group

Mayor confiabilidad y rendimiento de los sistemas operativos esenciales

Mayor cantidad de información relevante con una mejor integración de SAP

Menos riesgos gracias a la gestión de la seguridad y a la asistencia técnica integral

Leer el caso de éxito

¿Está listo para aumentar su nivel de seguridad y cumplimiento normativo?

Su empresa depende de las aplicaciones y de la infraestructura de TI. La adopción de enfoques y herramientas para gestionar los riesgos relacionados con el cumplimiento normativo y los puntos vulnerables en materia de seguridad le permitirá proteger su empresa. Red Hat ofrece la plataforma Linux y las herramientas de gestión integradas que se necesitan para generar innovaciones y llevar a cabo operaciones, con la atención puesta en la seguridad.

Ayude a que su equipo dé sus primeros pasos con Red Hat Insights:

redhat.com/insights

Descubra cómo puede acelerar los flujos de trabajo de TI de la mano de Red Hat Insights:

red.ht/insights_savetime

Eche un vistazo al resumen "Gestión de los riesgos de seguridad con Red Hat Insights":

red.ht/insights-security-brief

Vea una demostración de la gestión de riesgos de Red Hat Insights:

red.ht/insights-security-demo

Copyright © 2020 Red Hat, Inc. Red Hat, el logotipo de Red Hat, Red Hat Enterprise Linux y Ansible son marcas comerciales o marcas comerciales registradas de Red Hat, Inc. o sus filiales en Estados Unidos y en otros países. Linux® es la marca comercial registrada de Linus Torvalds en Estados Unidos y en otros países. Las demás marcas comerciales pertenecen a sus respectivos propietarios.

F26049_1120_KVM

Red Hat