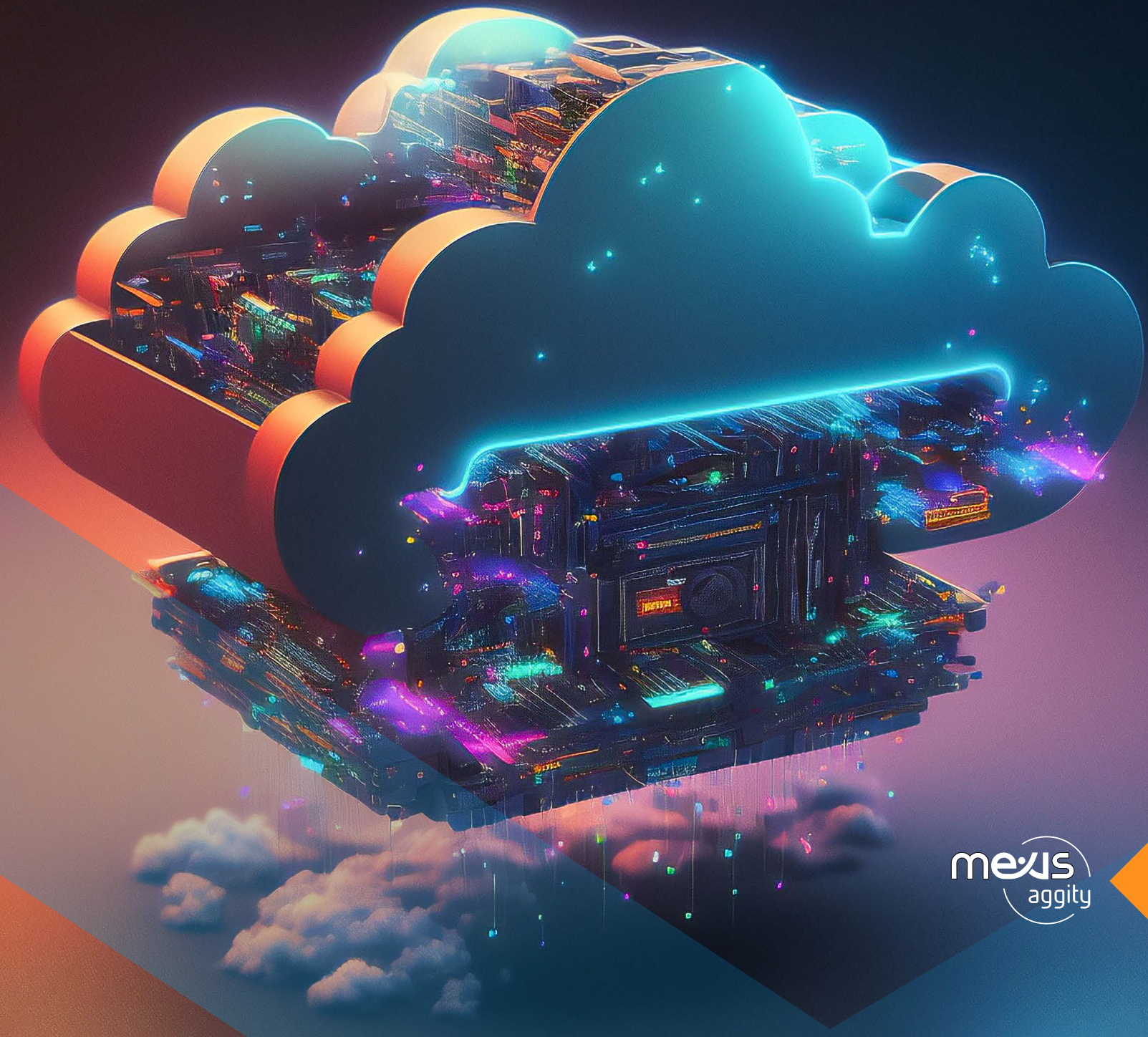
Cinco pasos para un entorno empresarial de automatización



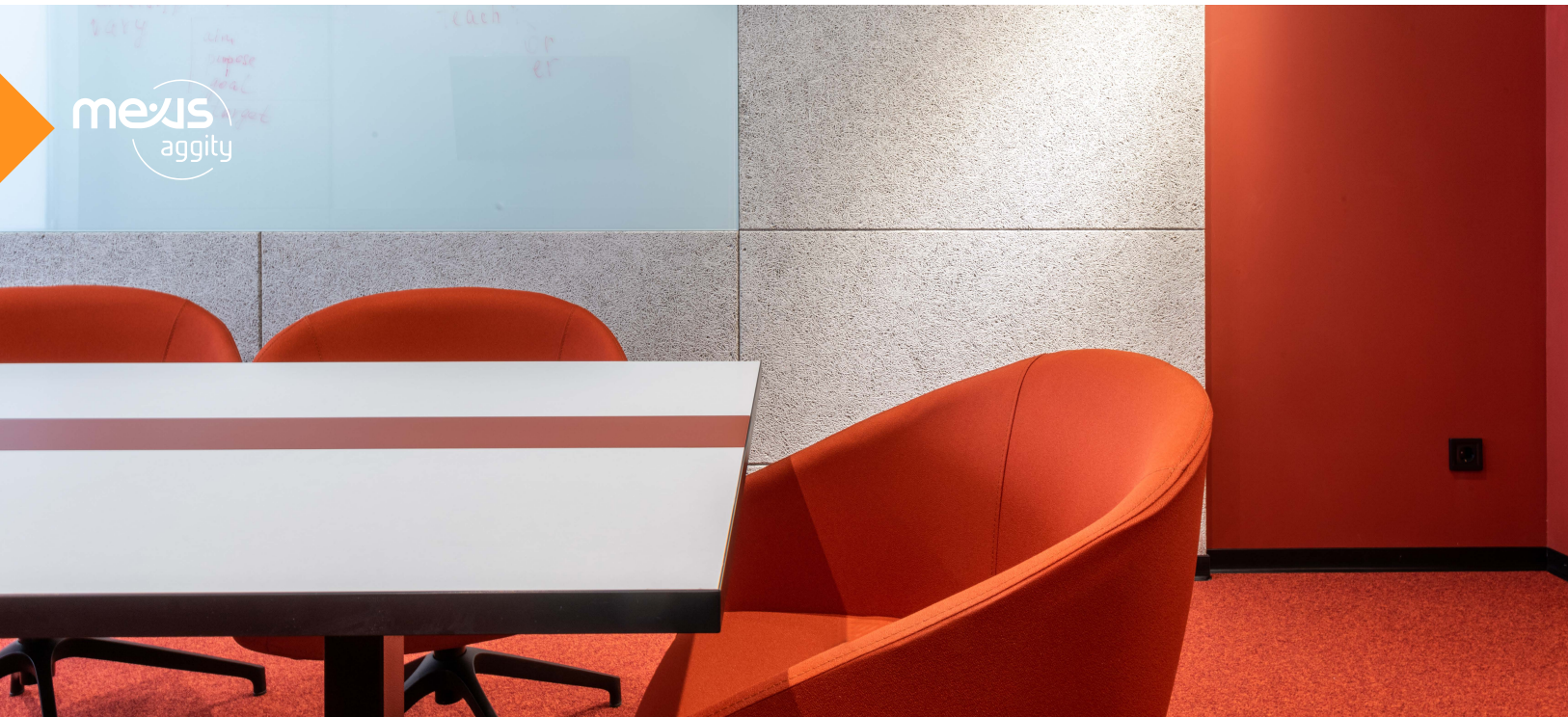
nexus aggity

Automation Anywhere describió cinco pasos para que las empresas tengan un entorno de automatización seguro, compatible y protegido en la nube.

A medida que las empresas se han movido para automatizar procesos mundanos para reducir costos y mitigar los desafíos de recursos durante la pandemia, también han tenido que lidiar con nuevos desafíos de seguridad debido al trabajo remoto y al acceso a datos confidenciales literalmente desde cualquier lugar y en cualquier momento.

Según la consultora Gartner, actualmente 60% de los trabajadores del conocimiento son remotos y al menos 18% no volverá a la oficina. Con el trabajo remoto puede venir una mayor exposición que conduce a un mayor riesgo cibernético. Los atacantes cibernéticos son ágiles, rápidos y persistentes. Siempre están buscando vulnerabilidades que puedan explotarse para obtener acceso a los datos confidenciales de las empresas. Desafortunadamente, han tenido bastante éxito.

La Escuela de Negocios Fuqua de la Universidad de Duke en Carolina del Norte, EU menciona que “más del 80% de las empresas estadounidenses indican que sus sistemas han sido pirateados con éxito en un intento de robar, cambiar o hacer públicos datos importantes. [...] Más del 85% de las empresas en Asia, Europa, África y América Latina dice que también han sido pirateadas”. Y los resultados pueden ser costosos. Una infracción puede costarle a una empresa millones de dólares en esfuerzos de remediación y pérdida de negocios y reputación.



¿Cómo migrar hacia la automatización de forma segura?
La migración de la automatización a una arquitectura nativa de la Nube permite un escalado más rápido, una mayor disponibilidad, seguridad granular e innovación. Para moverse a la velocidad de los negocios, su plataforma de automatización necesita:

. Minimizar el riesgo de exposición e incidentes de seguridad.

. Proporcione fuertes políticas proactivas de mitigación de riesgos y recuperación ante desastres.

. Cumplir con los estándares clave de la industria.

. Ofrezca autenticación y control de acceso sólidos y centralizados, así como extensiones a través de integraciones.

Además de estas consideraciones de la plataforma, indicó Campos, aquí hay cinco pasos que puede seguir para proteger su plataforma de automatización, el ciclo de vida del desarrollo y los datos.

PASO 1: Asegúrese de que la autenticación y el acceso estén definidos y controlados
Para comenzar, asegúrese de que cualquier persona que acceda a su sistema esté autenticada, por lo que la autenticación de múltiples capas y el control de acceso detallado son esenciales para un entorno estrictamente controlado. Estas son algunas de las mejores prácticas para lograrlo:

. Cree roles distintos, como administrador de RPA, creador de bots, probador de bots y operador de RPA dentro de la arquitectura básica y las funciones principales de la plataforma de automatización. Este tipo de control permite separar funciones y establecer roles de alta fidelidad con controles de acceso detallados suficientes para satisfacer las necesidades de los entornos más estrictos, seguros y regulados por el cumplimiento.

. Asegúrese de que su plataforma de automatización ofrezca una bóveda de credenciales integrada o la capacidad de integrarse pues almacena todas las credenciales del sistema y del usuario.

PASO 2: Cree un entorno de desarrollo que tenga alta disponibilidad y soporte
Una vez que el acceso sea seguro, puede pasar a otras áreas para eliminar posibles vulnerabilidades. Por ejemplo, las siguientes mejores prácticas pueden conducir al desarrollo exitoso y seguro de bots de software de automatización:

. Considere un plan/protocolo de seguridad para el desarrollo de código que requiera un escaneo continuo de múltiples herramientas y múltiples capas para detectar y eliminar las vulnerabilidades del software.

. Asegúrese de que su proveedor de plataforma pueda realizar pruebas de penetración de forma proactiva a través de escaneos de código en busca de vulnerabilidades.

. Garantice la postura de seguridad del dispositivo que ejecuta la automatización aprovechando las soluciones de detección y Respuesta de Punto Final (EDR) y Prevención de Pérdida de Datos (DLP) para hacer cumplir políticas, detectar anomalías y remediar amenazas de manera proactiva.

. Evalúe la arquitectura de componentes que debe ser capaz de adaptarse perfectamente a su infraestructura y procesos existentes de alta disponibilidad/recuperación ante desastres (HA/DR).

PASO 3: Proteja los datos en reposo, en uso y en tránsito

¿Tiene protección de datos de extremo a extremo? Es necesario mantener la confidencialidad y la integridad de los procesos críticos para el negocio y los datos confidenciales. Su plataforma de automatización debe proporcionar medidas de seguridad que no solo protejan los datos en reposo y en tránsito, sino también mientras están en uso en sistemas individuales. Algunos ejemplos de salvaguardas incluyen:

. Cifrado de credenciales locales y selección de datos de tiempo de ejecución empleados por bots, utilizando la bóveda de credenciales para proporcionar almacenamiento seguro.

. Emplear el procedimiento de gestión de datos y desidentificación mediante seudonimización que transforma los datos en identificadores artificiales, de modo que ya no es posible utilizar los datos para identificar a una persona física sin información adicional que se mantiene por separado.

. Todos los servicios de red deben usar Transport Layer Security (TLS) 1.2 (u otros estándares de la industria) para garantizar la seguridad e integridad de los datos durante el transporte entre componentes.

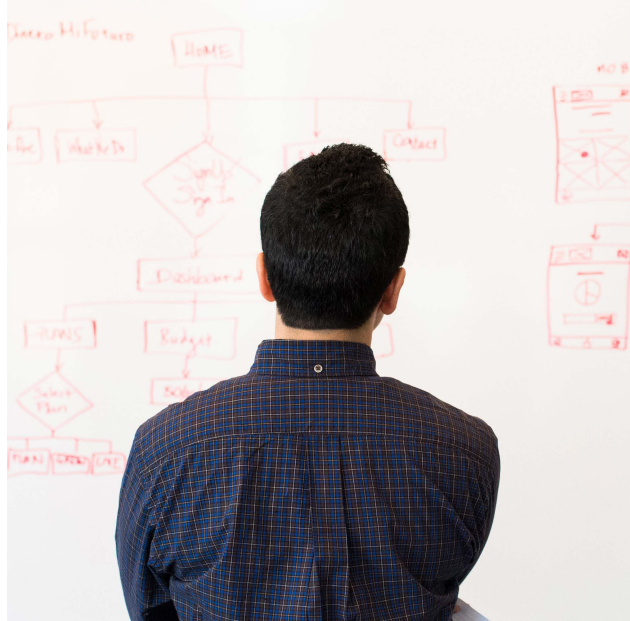
. La plataforma de automatización debe seguir las tecnologías de encriptación estándar de la industria para garantizar que sus datos estén encriptados.

PASO 4: Cumplimiento

Ahora que su gente tiene acceso a las áreas apropiadas para su trabajo en su empresa y están trabajando en un entorno seguro, puede dar un paso atrás y observar el cumplimiento.

La evaluación y gestión del cumplimiento se centra en la evaluación de sistemas y procesos para garantizar que se cumplan los estándares de la industria y los requisitos reglamentarios. Esto debería ser una práctica continua. A medida que crece el negocio, los departamentos aportan soluciones para ayudar a escalar. Las nuevas aplicaciones deben verificarse para que no pongan en peligro varios cumplimientos de seguridad.

Las capacidades integrales y continuas de registro de auditoría en su plataforma ayudarán a garantizar el cumplimiento de la seguridad y la calidad a nivel empresarial. En indus-



trias muy reguladas, como las ciencias de la salud o finanzas, las organizaciones pueden recibir multas y otras sanciones si no se cumplen los estándares de cumplimiento, incluidos HIPAA, PCI-DSS y FISMA.

PASO 5: Monitoree proactivamente las operaciones de seguridad

La seguridad no es un evento de una sola vez. En cualquier momento pueden surgir nuevas vulnerabilidades y técnicas de ciberataques. Por lo tanto, sus operaciones de seguridad deben monitorearse continuamente y mantenerse en un alto nivel. Con ese fin, aquí hay algunas mejores prácticas a seguir:

, Asegúrese de que su plataforma de automatización proporcione un proceso de ciclo de vida de desarrollo de software (SDLC) seguro con verificaciones y certificaciones realizadas por distintos administradores con diferentes roles y privilegios.

. Se debe incorporar una estricta separación de funciones y controles de múltiples capas para garantizar que el desarrollo de software sea confiable, escalable, eficiente, segura y compatible.

. Tener un equipo de ingeniería de seguridad especializado que sea responsable de la revisión del diseño, el modelado de amenazas, la revisión manual del código y las comprobaciones puntuales y las pruebas de penetración continuas garantiza la seguridad de su Nube.

. Junto con las operaciones, la recuperación ante desastres debe administrarse de manera proactiva para que el monitoreo y la notificación de incidentes le permitan manejar las situaciones de manera oportuna.

Fuente de información: cio.com.mx/