Deloitte.

Together makes progress

Los *desafíos* que marcan la adopción de entornos híbridos

Introducción

Hablar de transformación digital en Latinoamérica ya no es solo hablar de innovación: es hablar de supervivencia. Ante el aumento de los ciberataques, los desastres naturales recurrentes y las economías volátiles, los entornos híbridos se han convertido en la apuesta estratégica que equilibra lo mejor de dos mundos.

La flexibilidad que ofrece un entorno híbrido —conectando la infraestructura local con servicios en la nube pública o privada— está estrechamente relacionada con nuevos desafíos de seguridad. Un entorno híbrido es aquel que combina infraestructura propia (*on-premises*) con recursos de nube pública o privada de forma integrada. Por ejemplo, una empresa puede alojar sistemas críticos en sus propios servidores por cumplimiento regulatorio, mientras aprovecha nube pública para aplicaciones escalables y una nube privada para respaldos sensibles. Se trata de una arquitectura que ofrece escalabilidad y flexibilidad sin renunciar al control local.

Sin embargo, dicho modelo multiplica la superficie de ataque y genera silos de seguridad difíciles de gestionar. El crecimiento de entornos híbridos y *multicloud*, cada uno con sus propias herramientas y políticas, ha creado brechas de visibilidad, gobernanza e identidad que los atacantes pueden explotar. La promesa de lo híbrido no está exenta de desafíos, pero son pruebas que las empresas deben enfrentar con visión integral si quieren convertir el riesgo en ventaja y transformar la seguridad en un verdadero motor de competitividad.

En otras palabras, mientras la nube híbrida impulsa la transformación digital, también exige una visión de seguridad unificada para no dejar puntos ciegos que comprometan la innovación lograda.

Desafíos y oportunidades del ecosistema híbrido

En Latinoamérica, los entornos híbridos se han consolidado como el camino más viable para acelerar la transformación digital sin comprometer el control sobre infraestructuras críticas. Cuando se combina la escala y la flexibilidad de la nube con la seguridad y la gobernanza de los sistemas locales, este modelo permite a las organizaciones responder a marcos regulatorios estrictos, gestionar costos de manera más eficiente y, al mismo tiempo, impulsar la innovación con rapidez. Sectores como banca, salud o manufactura han encontrado en lo híbrido un habilitador clave para modernizar operaciones, aprovechar analítica avanzada y cumplir con normativas de soberanía de datos, todo, en un solo esquema tecnológico integrado.

La importancia de este modelo va más allá de lo técnico: se convierte en un factor estratégico para la resiliencia y la continuidad de negocio en una región expuesta a ciberataques crecientes, desastres naturales y dinámicas económicas volátiles. Cuando un entorno híbrido es bien gestionado ofrece la capacidad de mover cargas de trabajo entre nubes y servidores locales, responder más rápido ante incidentes y asegurar disponibilidad constante de los servicios críticos. Además, esto no solo reduce riesgos financieros y operativos, sino que fortalece la confianza de clientes, reguladores y socios, posicionando a las empresas que lo adoptan como jugadores más sólidos y sostenibles en mercados altamente competitivos.

A medida que los entornos híbridos se consolidan como pilares de transformación digital, también emergen desafíos que las organizaciones debieran abordar con urgencia. La gestión de equipos distribuidos, la interoperabilidad entre sistemas locales y en la nube, y la necesidad de mantener una cultura organizacional cohesionada en medio de la dispersión geográfica, son solo algunos de los retos que pueden comprometer la efectividad del modelo si no se enfrentan con una visión integral. No obstante, con la estrategia correcta de ciberseguridad, los desafíos pueden convertirse en una ventaja competitiva en el camino hacia la transformación digital. A continuación, listamos retos clave *versus* una postura robusta de ciberseguridad en lo híbrido:

Desafíos

Falta de visibilidad y monitoreo fragmentado

Un desafío principal es la falta de visibilidad integrada entre sistemas *on-premise* y *multicloud*. Los hallazgos de una encuesta global reflejan que solo 23% de las organizaciones reporta tener visibilidad completa de sus entornos *cloud*;[1] esto implica que la mayoría opera con "puntos ciegos" en su superficie de ataque. Se trata de lagunas que dificultan la detección de amenazas a tiempo, pues los equipos de seguridad deben alternar entre múltiples herramientas y paneles inconexos. La fragmentación del monitoreo conlleva políticas inconsistentes, alertas duplicadas y eventos pasados por alto.

Complejidad normativa

Un desafío enorme es mantener estándares regulatorios consistentes en un entorno híbrido/*multicloud*. Organismos reguladores en todo el mundo —desde la Unión Europea hasta Latinoamérica— han endurecido la fiscalización. Por ejemplo, las multas bajo el *Reglamento General de Protección de Datos de la Unión Europea (GDPR*, por sus siglas en inglés) alcanzaron 1,200 millones de euros en 2024, afectando principalmente a compañías que no supieron proteger la información personal[3]. Sectores como el sanitario o el financiero enfrentan, además, sanciones por violar normativas específicas. Un entorno híbrido mal controlado puede derivar en datos sensibles expuestos en la nube pública, violando soberanía de datos o acuerdos de nivel de servicio, con el correspondiente castigo de entes reguladores.

Costos financieros crecientes

El costo promedio de una brecha de datos a nivel global alcanzó 4.88 millones de dólares (mdd) en 2024, reflejando un salto anual de ~10%[5]. Se trata del promedio más alto registrado a la fecha, con una tendencia al alza impulsada por la complejidad adicional de contener brechas en infraestructuras híbridas. Cuando los datos comprometidos residen en múltiples entornos, los incidentes tardan más en controlarse y salen significativamente más caros —en torno a 5 mdd o más, al involucrar esfuerzos de remediación en distintos sistemas[6]. Además de los costos directos, están las pérdidas por interrupción del negocio, demandas legales y ausencia de clientes. Por ello, una postura reactiva o segmentada frente a la seguridad híbrida puede traducirse literalmente en costos multimillonarios que habrían sido evitables con una estrategia preventiva más sólida. En esencia, pagar ahora por prevención cuesta mucho menos que pagar después por el desastre.

Oportunidades

Visibilidad unificada

Una monitorización centralizada de toda la infraestructura permite detección temprana de amenazas y respuesta coordinada desde un solo panel de control (*single pane of glass*). Integrar telemetrías[2] de nube y locales elimina los puntos ciegos y reduce drásticamente el tiempo para identificar incidentes. Las herramientas de gestión unificadas proporcionan alertas correlacionadas y el contexto completo de un ataque que atraviese múltiples dominios, algo imposible de lograr con visibilidad fragmentada.

Cumplimiento eficaz

Una gestión de seguridad unificada facilita aplicar políticas consistentes y demostrar cumplimiento normativo de punta a punta. Herramientas de gobierno *multicloud* permiten auditar configuraciones, cifrado y accesos en todos los entornos desde un marco común, simplificando las evaluaciones de cumplimiento. Adicionalmente, adoptar estándares internacionales de forma holística genera una cultura corporativa centrada en la protección de datos sin importar dónde residan. Las organizaciones líderes integran la seguridad en sus procesos de *DevOps*[4] para que cada nuevo despliegue en la nube cumpla los requisitos desde el diseño. El resultado es un menor riesgo de brechas regulatorias y la capacidad de obtener certificaciones que avalan la madurez de seguridad.

Reducción de brechas y costos

Al implementar principios de Zero Trust,[7] segmentación de la red y automatización, se limita el movimiento lateral de atacantes y se contienen los incidentes más rápido. Por ejemplo, eliminar privilegios por defecto y usar acceso *just-in-time* minimiza el impacto de credenciales comprometidas. Asimismo, tecnologías de seguridad como *EDR* (detección y respuesta de *endpoints*), *SOAR* (orquestación, automatización y respuesta de seguridad) e IA (inteligencia artificial) pueden aislar sistemas afectados en segundos, evitando que un ataque pequeño se vuelva una brecha mayor. Estas prácticas proactivas reducen la probabilidad de incidentes consumados y también el costo en caso de que ocurran, al acortar el ciclo de vida del ataque. Las empresas que adoptan de forma robusta la IA y la automatización en seguridad logran, en promedio, detectar/contener intrusiones 98 días más rápido que las que no lo hacen, ahorrándose millones de dólares[8].

Zero Trust: protección que define el éxito

Los ciberataques, como el *ransomware* o los accesos no autorizados, representan una amenaza directa para la continuidad operativa. En 2024, 86% de los incidentes provocó interrupciones significativas del negocio, afectando tanto infraestructuras en la nube como sistemas internos[9]. La complejidad de los entornos digitales híbridos amplifica el riesgo: una sola brecha puede paralizar cadenas de suministro, servicios hospitalarios o transacciones financieras. Además, las brechas por credenciales comprometidas tardan, en promedio, 292 días en ser detectadas y contenidas, lo que permite a los atacantes permanecer casi 10 meses dentro de la red[10].

Controlar el acceso de usuarios y sistemas a través de dominios híbridos es complejo sin el enfoque *Zero Trust*. En muchos casos, cada entorno (local o nube) opera con su propio directorio e inicio de sesión, generando identidades fragmentadas y cuentas con privilegios residuales. Esto deriva en que credenciales privilegiadas puedan quedar activas sin los debidos controles, convirtiéndose en objetivos jugosos para atacantes. Las brechas actuales demuestran que el robo de credenciales y el abuso de accesos son causas destacadas de incidentes, dado que muchas empresas no implementan adecuadamente el principio de mínimo privilegio, lo que permite a los atacantes escalar permisos y acceder a datos críticos si consiguen una cuenta comprometida.

Informes revelan que 28% de los incidentes en la nube han involucrado el uso de credenciales legítimas, muchas de las cuales, estaban sobreprivilegiadas, lo que permitió a los atacantes realizar acciones más dañinas[11]. Otra causa frecuente de incidentes es la mala configuración de entornos: poco más de 20% de los incidentes de seguridad *cloud* se atribuye a errores de configuración —por ejemplo, permisos mal gestionados o claves *API* expuestas[12]. En entornos híbridos, esta heterogeneidad tecnológica agrava el riesgo: cada plataforma tiene configuraciones distintas, aumentando las probabilidades de fallos humanos o técnicos. Un simple descuido (como una base de datos en la nube sin cifrar, o un servidor local con un puerto abierto) puede exponer datos sensibles de forma inadvertida.

La complejidad de administrar parches, actualizaciones y políticas de configuración a través de infraestructuras dispares significa que una mala configuración en un entorno puede crear una puerta de entrada hacia los demás. Las organizaciones deben reforzar sus procesos de configuración segura, así como llevar a cabo auditorías constantes para evitar que "lo más débil de la cadena" comprometa todo el ecosistema.

La exposición de datos sensibles por un error humano o técnico puede activar sanciones regulatorias, demandas colectivas y la pérdida de contratos estratégicos con socios internacionales que exigen altos estándares de protección. Dada la competitividad de los mercados, y donde la confianza digital es un diferenciador tangible, un incidente de este tipo afecta las finanzas inmediatas y erosiona la capacidad de la organización de mantenerse relevante, atraer inversión y consolidarse como un actor confiable en el largo plazo.

Hay empresas que han sufrido brechas masivas por las que han aparecido en titulares noticiosos, sembrando dudas sobre su fiabilidad. En 2024, Deloitte llevó a cabo una encuesta a casi 1,200 responsables de la toma de decisiones cibernéticas a nivel directivo. Parte de los resultados revela que 63% de los encuestados reportó pérdida de confianza del cliente y afectación a la marca, como resultado de las brechas de seguridad[13]. Es decir, una sola brecha puede ahuyentar a clientes potenciales y hasta provocar la fuga de los actuales; por lo que reconstruir la reputación después de un incidente requiere tiempo, transparencia y mejoras tangibles, pero, aun así, muchas empresas no logran recuperar la credibilidad en el mercado.

En este contexto, incorporar la seguridad en el ADN operativo se traduce en confianza y en lealtad de los clientes. Hoy, usuarios y socios valoran profundamente que sus datos estén protegidos, pues una empresa con historiales limpios de seguridad y transparencia en su manejo de datos gana reputación. Las organizaciones más exitosas están convirtiendo la ciberseguridad en un argumento de venta: publicidad de "tus datos seguros con nosotros", distintivos de cumplimiento y un historial sin brechas significativas pueden inclinar la balanza a favor. La seguridad deja de ser solo un centro de costos y pasa a ser un habilitador de negocio, potenciando la marca y diferenciándola por confiable. En la economía digital, la confianza es un activo; y pocas cosas construyen más confianza que demostrar un compromiso serio con la ciberseguridad.

Conclusión

Los entornos híbridos representan la evolución lógica de la infraestructura moderna, al permitir innovar con rapidez, apoyándose en la nube, sin perder el control de sistemas legados críticos. Pero esa dualidad conlleva riesgos que deben abordarse de forma cohesionada y multidimensional. No basta con proteger cada entorno por separado; es imprescindible integrar estrategias, tecnologías y cultura organizacional bajo una misma visión de seguridad.

En este sentido, la ciberseguridad en lo híbrido debe elevarse de ser un tema meramente técnico a una función directiva estratégica. Solo así la empresa estará en posición de detectar brechas de forma temprana, reducir el costo de los incidentes, asegurar la continuidad operativa incluso bajo ataque, mantener el cumplimiento regulatorio en todas sus operaciones y generar confianza como un diferenciador digital. *CIOs* y responsables de transformación digital que prioricen visibilidad unificada, gestión de identidades bajo principios de *Zero Trust* y cumplimiento regulatorio transversal van a colocarse un paso adelante en la reducción de riesgos, en la contención de costos y en la generación de confianza.

Referencias

[1] Cloud Security Alliance. (2024). *Cloud Security Alliance Survey Finds 77% of Respondents Feel Unprepared to Deal with Security Threats.* CSA. cloudsecurityalliance.org/press-releases/2024/02/14/cloud-security-alliance-survey-finds-77-of-respondents-feel-unprepared-to-deal-with-security-threats

[2] Telemetría: también conocido como "telemedición", se refiere a un sistema de comunicación a distancia que permite recoger, procesar, medir y transmitir información de un dispositivo electrónico a otro. www.proofpoint.com/es/threat-reference/telemetry

[3] Lindström, K. (2025). *"GDPR fines hit €1.2 billion in 2024 on 8.3% more breach reports".* CSO Online. www.csoonline.com/article/3808871/gdpr-fines-reduced-in-2024.html

[4] *DevOps:* abreviación en inglés de *Development* (desarrollo) y *Operations* (operaciones de TI). Se trata de un enfoque que integra ambos equipos para acelerar el desarrollo y la entrega de *software.* Este modelo elimina las barreras tradicionales entre desarrollo y operaciones, promoviendo la colaboración, la responsabilidad compartida y la automatización. Como resultado, permite entregar *software* de forma más rápida, confiable y con mayor calidad a los clientes. aws.amazon.com/devops/what-is-devops/

[5] IBM. (2024). *IBM Report: Escalating Data Breach Disruption Pushes Costs to New Highs.* IBM Newsroom. newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs

[6] IBM. (2025). *Cost of data breach report 2025.* IBM Security. www.ibm.com/security/data-breach

[7] *Zero Trust* o en español Confianza Cero: Modelo estratégico de ciberseguridad que parte del principio fundamental de "nunca confiar, siempre verificar". *Zero Trust* elimina la confianza implícita de los modelos tradicionales y exige validación continua de cada acceso, sin importar la ubicación del usuario o dispositivo. Deloitte (2025). *"Zero Trust* como pilar de la adopción empresarial y prioridad estratégica". https://www.deloitte.com/latam/es/services/consulting/perspectives/zero-trust-prioridad-estrategica.html

[8] IBM. (2024). IBM Report: *Escalating Data Breach Disruption Pushes Costs to New Highs.* IBM Newsroom. newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs

[9] Palo Alto Networks. (2025). Informe global sobre respuesta a incidentes (2025). www.paloaltonetworks.es/resources/research/unit-42-incident-response-report

[10] Singh, P. (2025). *Breaking Silos: Why Unified Security is Critical in Hybrid World.* Darktrace. www.darktrace.com/blog/breaking-silos-why-unified-security-is-critical-in-hybrid-world

[11] IBM. (2024). *X-Force Cloud Threat Landscape Report 2024.* www.ibm.com/downloads/documents/us-en/10a99803d4afd20a

[12] IBM. (2024). *X-Force Cloud Threat Landscape Report 2024.* www.ibm.com/downloads/documents/us-en/10a99803d4afd20a

[13] Deloitte. (2024). *The global future of cyber survey, 4th edition. The promise of cyber.* www.deloitte.com/content/dam/assets-shared/docs/services/risk-advisory/2024/deloitte-global-future-of-cyber-survey-4th-edition-the-promise-of-cyber.pdf

Contacto

Daniel Ortiz Castillo
Socio de Ciberseguridad
Deloitte Spanish Latin America
dortizcastillo@deloitte.com

Centro de contacto
+52 55 5080 6633
centrodecontacto@deloittemx.com

Deloitte.