Deloitte.

Together makes progress

Zero Trust como pilar de la adopción empresarial y ***prioridad*** estratégica

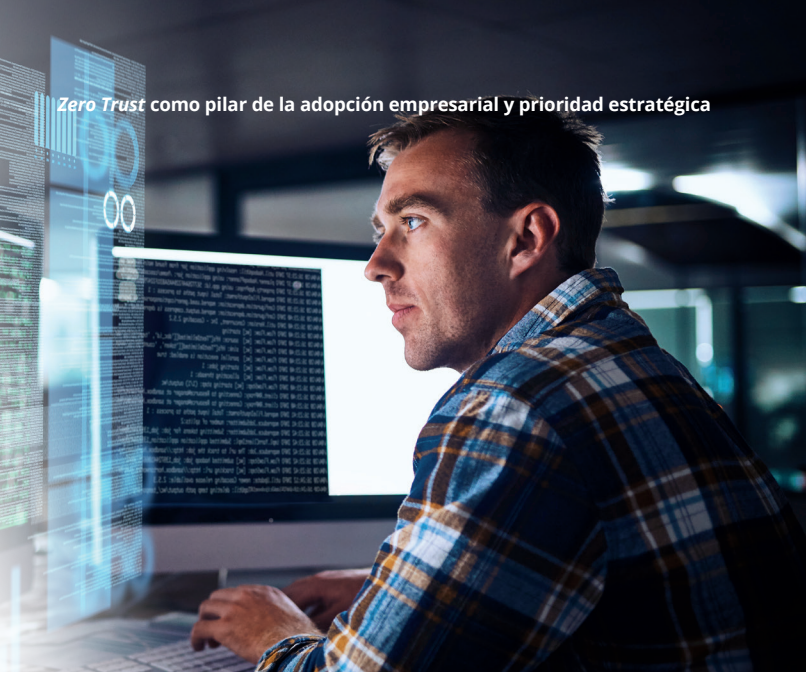
Introducción

Zero Trust (Confianza Cero) ha emergido como un modelo estratégico de ciberseguridad para las organizaciones. A diferencia de los modelos tradicionales basados en la confianza en el interior del perímetro, *Zero Trust* parte de un principio fundamental: "nunca confiar, siempre verificar". Este enfoque responde a la realidad actual donde la frecuencia y gravedad de los ciberataques van en aumento constante.

Ya no bastan las defensas perimetrales tradicionales, pues muchos ataques logran traspasar barreras y explotar la confianza implícita dentro de la red. De hecho, numerosas herramientas de seguridad legadas no protegen frente a amenazas internas, ya sean actores maliciosos con credenciales válidas o errores humanos, lo que permite que, una vez violado el perímetro, un atacante se mueva de forma lateral robando datos confidenciales o escalando privilegios sin ser detectado.

En este contexto, adoptar un modelo *Zero Trust* es, además de una decisión técnica, una decisión estratégica. Este enfoque elimina la confianza por defecto: ningún usuario o dispositivo es confiable a priori, sin importar su ubicación dentro o fuera de la red corporativa. Cada intento de acceso debe ser autenticado, autorizado y registrado de forma continua, aplicando controles basados en la identidad, el dispositivo, la ubicación y otros contextos relevantes. En este modelo, los recursos —entendidos como todos los activos digitales que la organización necesita proteger, incluyendo aplicaciones, datos sensibles, servicios, dispositivos y entornos en la Nube— son gestionados como elementos críticos que deben mantenerse protegidos por defecto. Esto reduce de forma significativa las superficies de ataque y limita las oportunidades para actores maliciosos.

Además, este enfoque distribuye la responsabilidad de la seguridad a toda la organización mediante políticas y controles uniformes, en lugar de depender únicamente de un muro perimetral. Por lo que la interrogante ya no es si adoptar *Zero Trust*, sino cuándo y cómo hacerlo de forma efectiva, antes de que un incidente demuestre las limitantes del enfoque tradicional.



Una *nueva era* de la ciberseguridad tras un ataque global

El ataque a la cadena de suministro de una empresa estadounidense que desarrolla *software*, descubierto en 2020, implicó una infiltración altamente sofisticada en el *software* de monitoreo Orion, utilizado por miles de organizaciones en todo el mundo, incluidas agencias gubernamentales y grandes corporaciones. Los atacantes insertaron un código malicioso en una actualización legítima del *software*, la cual, fue distribuida automáticamente a los clientes de la organización. Esto les permitió obtener acceso encubierto y persistente a las redes afectadas, sin ser detectados, durante meses[1].

El daño fue significativo: los atacantes lograron movimiento lateral dentro de las redes comprometidas, accedieron a correos electrónicos confidenciales, archivos sensibles, credenciales y, en algunos casos, modificaron configuraciones críticas. Entre las víctimas confirmadas estuvieron el Departamento del Tesoro de Estados Unidos y Microsoft, entre otras entidades clave, tanto públicas como privadas. Además del robo de información, el incidente expuso la fragilidad de los modelos de seguridad basados en confianza implícita, especialmente cuando se trata de proveedores tecnológicos.

Este ciberataque no solo causó pérdidas reputacionales y costos operativos para muchas organizaciones, sino que también desencadenó una respuesta institucional sin precedentes. Fue una llamada de atención que impulsó a gobiernos y a empresas a reevaluar sus modelos de seguridad. La principal lección es que se debe adoptar un enfoque *Zero Trust* y asumir que cualquier *software* o proveedor externo podría estar comprometido, limitando estrictamente el acceso de terceros solo a lo imprescindible. Debido a la magnitud del ataque, el gobierno de Estados Unidos emitió la *Orden Ejecutiva 14028* en 2021, que estableció *Zero Trust* como un modelo de seguridad obligatorio para sus agencias federales[2].

Lo ocurrido representa una de las más relevantes lecciones que hacen evidente la necesidad de un cambio de paradigma. Que gobiernos y reguladores adopten el enfoque *Zero Trust* deja claro que no es una moda pasajera, sino una necesidad estratégica para todas las organizaciones, ya que dicho modelo parte de reconocer cómo han cambiado las condiciones del entorno digital y las tendencias asociadas:

Amenazas evolucionadas y entorno sin perímetro definido: el auge del *cloud computing*, el trabajo remoto o híbrido y la proliferación de dispositivos móviles han disuelto el perímetro clásico de las empresas. Hoy, empleados y datos se mueven de manera constante fuera de las oficinas, y los atacantes aprovechan técnicas sofisticadas para infiltrarse en las redes corporativas. *Zero Trust* aborda esta realidad asumiendo, desde el diseño, que la red siempre puede estar comprometida, por lo que se verifica cada interacción como si fuera externa. Esto permite enfrentar amenazas tanto externas como internas de manera proactiva, a diferencia del antiguo modelo de confianza interna que dejaba flancos abiertos[3].

Protección de la transformación digital y la confianza del cliente: las empresas dependen de la digitalización para innovar y crecer, pero esa misma digitalización amplía la superficie de ataque. Invertir en *Zero Trust* es invertir en la confianza digital que la organización ofrece a clientes, Socios y reguladores. Al garantizar que solo las personas y dispositivos autorizados accedan a la información que les atañe para desempeñar sus funciones, se minimiza el riesgo de filtraciones de datos que puedan erosionar la confianza de los clientes. Adoptar dicho enfoque demuestra un compromiso sólido con la seguridad y la privacidad, lo cual, puede convertirse en ventaja competitiva y elemento diferenciador en el mercado.

Zero Trust está diseñado para mitigar de forma proactiva los riesgos más apremiantes del panorama actual de ciberseguridad. Este enfoque no solo redefine cómo se protege el acceso, sino que transforma la arquitectura defensiva frente a las amenazas más frecuentes y dañinas. A continuación, describimos algunos de estos riesgos y cómo el modelo ayuda a enfrentarlos:

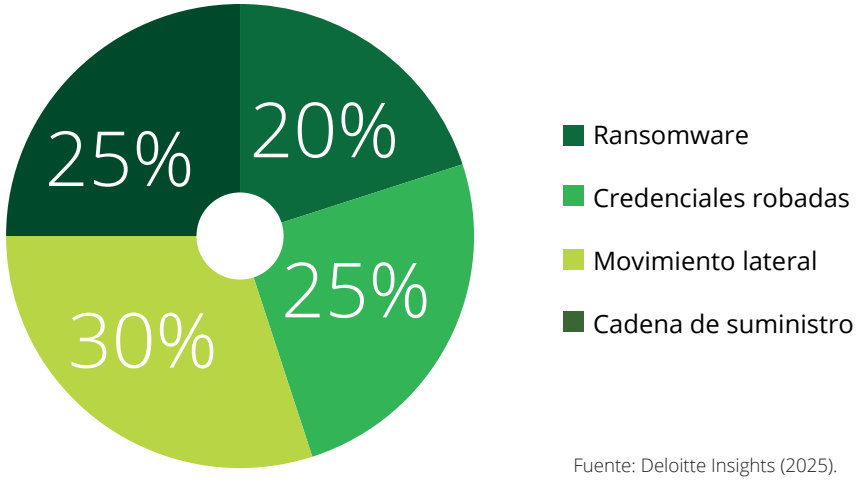
Movimiento lateral y amenazas internas: en entornos tradicionales, una vez que un atacante logra acceder a la red —ya sea mediante *malware* o el uso de credenciales robadas— puede desplazarse libremente entre sistemas conectados. Este desplazamiento, conocido como movimiento lateral, le permite escalar privilegios, acceder a datos sensibles y provocar disrupciones operativas sin grandes obstáculos. *Zero Trust* cierra esta brecha mediante segmentación de red, verificación continua y el principio de mínimo privilegio, que restringe el acceso únicamente a lo necesario. Así, incluso si un punto es comprometido, el atacante queda confinado a un entorno limitado y sujeto a monitoreo constante, dificultando su avance.

Compromiso de credenciales y *phishing:* alrededor de 19% de las brechas de seguridad a nivel mundial se originan por credenciales comprometidas o robadas[4]. *Zero Trust* mitiga este riesgo mediante la implementación de múltiples capas defensivas: autenticación multifactor (*MFA*, por sus siglas en inglés), validación del estado del dispositivo y autorización contextual por sesión. Incluso, si un atacante obtiene la contraseña de un empleado mediante técnicas como el *phishing*, los controles de *Zero Trust* dificultan que dicha credencial sea útil, al requerir comprobaciones adicionales que invalidan el acceso no legítimo[5]. La verificación continua refuerza el modelo, evaluando el comportamiento del usuario y revocando sesiones ante cualquier actividad sospechosa.

Ransomware* y propagación de *malware: una vez que logra infiltrarse, el ransomware tiende a propagarse rápidamente por la red, multiplicando su impacto. *Zero Trust* detiene este avance a través de la microsegmentación, que impide al *malware* moverse libremente entre servidores o dispositivos. Además, al aplicar accesos restringidos por rol, un equipo comprometido tiene capacidades mínimas para interactuar con otros activos críticos. Esta contención, sumada al monitoreo en tiempo real y la respuesta automatizada ante comportamientos inusuales —como el cifrado masivo de archivos—, permite frenar el ataque en sus primeras etapas, protegiendo la continuidad operativa y reduciendo las pérdidas por rescate o interrupciones prolongadas.

Exposición en la cadena de suministro y accesos de terceros: en un ecosistema donde múltiples proveedores, contratistas y plataformas externas interactúan con los sistemas empresariales, las brechas de un tercero pueden convertirse rápidamente en brechas propias. *Zero Trust* aborda este riesgo asumiendo que todo actor externo es potencialmente comprometido. Por ello, restringe el acceso de terceros al mínimo indispensable y lo somete a los mismos controles que los usuarios internos[6]. Así, por ejemplo, si un proveedor solo necesita acceso a un portal específico, sus credenciales no permitirán explorar otras áreas de la red. Además, las conexiones externas son continuamente monitoreadas, y cualquier acceso anómalo es revocado de forma automática. Este enfoque contrasta con los modelos tradicionales, donde los proveedores solían operar con permisos excesivos, y representa una barrera crítica frente a ataques como el ya mencionado previamente.

Gráfica 1.
Distribución de riesgos mitigados con *Zero Trust*



Fuente: Deloitte Insights (2025).

***Zero Trust* como pilar de la adopción empresarial y prioridad estratégica**

Beneficios empresariales clave de *Zero Trust*

Más allá de ser una solución técnica, *Zero Trust* se ha consolidado como una decisión estratégica con impacto directo en los objetivos de negocio. Su adopción fortalece la capacidad de respuesta ante incidentes, reduce costos asociados a brechas de seguridad, asegura el cumplimiento normativo y optimiza el uso de recursos tecnológicos. Todo ello lo posiciona como un habilitador de valor empresarial, alineado con las prioridades del liderazgo ejecutivo. A continuación, se presentan los beneficios empresariales clave que hacen del modelo una apuesta integral para organizaciones que buscan proteger su operación, mantener la continuidad y ganar ventaja competitiva:

Reducción de riesgos y prevención de incidentes: estudios han mostrado que la adopción de este modelo disminuye hasta 50% la probabilidad de sufrir una violación de datos[7]. En caso de que un incidente ocurra, la segmentación y controles de *Zero Trust* ayudan a contenerlo rápidamente, evitando su propagación por la red. Esto se traduce también en ahorro económico, pues las organizaciones con una estrategia *Zero Trust* plenamente implementada suelen experimentar un costo significativamente menor en comparación con las que carecen de este enfoque.

Cumplimiento normativo y reputación corporativa: regulaciones de seguridad y privacidad de datos —como el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (*PCI DSS*, por sus siglas en inglés)— exigen cada vez más controles estrictos de acceso y monitoreo. *Zero Trust* facilita el cumplimiento normativo al implementar visibilidad total sobre quién accede a qué recursos y por qué, registrando cada actividad y aplicando políticas de mínimo privilegio[8]. Esto ayuda a demostrar auditorías exitosas y reduce el riesgo de sanciones por incumplimiento.

Un acceso condicionado y continuamente verificado también dificulta las filtraciones de datos personales, protegiendo a los consumidores y, por añadidura, la reputación de la empresa. En esencia, *Zero Trust* crea un entorno de control y transparencia que alinea la seguridad interna con las expectativas de los reguladores y del público, fortaleciendo la imagen de la organización como entidad confiable y responsable.

Continuidad del negocio y resiliencia operativa: al eliminar la confianza implícita y segmentar la red, se evita que la intrusión en un punto se traduzca en la caída de múltiples sistemas. Los ataques, de ocurrir, quedan confinados a segmentos reducidos, lo cual permite seguir operando funciones críticas en paralelo. Este enfoque *fail-safe* (a prueba de fallos) asegura que la empresa pueda continuar prestando servicios aún bajo ataque, con interrupciones mínimas.

Según datos de la industria, las organizaciones con implementaciones maduras de *Zero Trust* tienen más del doble de probabilidad de lograr alta resiliencia empresarial frente a las que todavía operan con seguridad tradicional limitada[9]. *Zero Trust* protege toda la estructura corporativa, eleva la velocidad de respuesta a amenazas y mantiene el rendimiento del negocio, incluso en momentos de crisis. En términos de continuidad, es un seguro contra tiempos de inactividad prolongados y pérdidas operativas catastróficas.

Eficiencia operativa y retorno de la inversión: *Zero Trust* bien implementado mejora la eficiencia de las operaciones de Tecnología de la Información (TI) y seguridad de la información. Muchas empresas logran consolidar herramientas y simplificar su arquitectura de seguridad bajo el modelo *Zero Trust*, eliminando redundancias. Un ejemplo es la experiencia de organizaciones que, después de adoptar este enfoque, vieron un aumento de 90% en la eficiencia de su centro de operaciones de seguridad (*SOC*, por sus siglas en inglés) gracias a la reducción de alertas irrelevantes y una respuesta más ágil[10].

***Zero Trust* como pilar de la adopción empresarial y prioridad estratégica**

Casos de *uso prácticos* y ejemplos reales

Zero Trust no es especulación, es una realidad que diversas empresas ya están adoptando para resolver desafíos concretos de seguridad, aplicable a múltiples escenarios y sectores: organizaciones líderes en tecnología, entidades financieras, hospitales, agencias gubernamentales e, incluso, compañías de sectores tradicionales (manufactura y *retail*).

A continuación, desarrollamos algunos escenarios para ilustrar cómo la inversión en *Zero Trust* es una práctica probada para proteger a las empresas. La adaptabilidad del enfoque —desde asegurar trabajo remoto hasta blindar entornos de producción— demuestra su versatilidad, ya que cualquier organización, y cualquier industria, pueden beneficiarse de adoptar *Zero Trust* en su estrategia de ciberseguridad:

Acceso remoto seguro y fuerza de trabajo híbrida: las organizaciones han brindado acceso a sus sistemas desde ubicaciones y dispositivos fuera del perímetro corporativo. *Zero Trust* facilita este modelo de forma segura mediante soluciones de *Zero Trust Network Access* (*ZTNA*) que reemplazan a las *VPN* (*Virtual Private Network*) tradicionales, otorgando a cada empleado o proveedor solo el acceso específico a las aplicaciones que necesita.

Un ejemplo es Google, pionero en *Zero Trust* con su iniciativa *BeyondCorp*: a partir de 2010, la empresa implementó un modelo en el que cada empleado puede trabajar desde redes no confiables (como su casa o una *WiFi* pública) sin necesidad de *VPN*, pues la seguridad viaja con el usuario y el dispositivo. *BeyondCorp* aplica autenticación de usuario y verificación del estado del dispositivo para cada conexión, permitiendo que los *Googlers* accedan de forma segura a los recursos corporativos desde prácticamente cualquier lugar del mundo[11].

Protección de datos sensibles en sectores regulados: industrias como la salud y la banca manejan a diario información altamente confidencial (historias clínicas, datos de cuentas, etc.) y están sujetas a estrictas regulaciones de seguridad. *Zero Trust* se ha convertido en un enfoque óptimo para estas organizaciones al garantizar solo el acceso autorizado, bajo una vigilancia continua. Por ejemplo, un hospital puede implementar *Zero Trust* para que el personal médico y de enfermería acceda a expedientes electrónicos con múltiples factores de autenticación, mientras que se monitorea en tiempo real cualquier intento inusual de acceder a grandes volúmenes de registros de pacientes[12].

De igual forma, un banco puede segmentar su red para aislar las bases de datos de clientes y sistemas de pagos, aplicando políticas que verifiquen continuamente el comportamiento de los usuarios financieros y detecten desviaciones (como consultas masivas de datos fuera de horarios habituales). En ambos escenarios, *Zero Trust* refuerza el cumplimiento de normas y previene brechas internas o externas, brindando tranquilidad a la alta dirección de que los datos críticos están fuertemente custodiados.

Unificación de la seguridad en entornos multinube: hoy, muchas corporaciones operan en múltiples nubes públicas y privadas, combinadas con infraestructura local. Esto presenta un reto de seguridad, por lo que *Zero Trust* responde unificando los controles a nivel de identidad y dispositivo en cualquier entorno.

Un ejemplo real es el de empresas tecnológicas que migraron aplicaciones a la Nube y adoptaron *Zero Trust* para que el acceso siempre requiera autenticación robusta, evaluación de contexto y cifrado de extremo a extremo, independientemente de si un recurso está en un centro de datos propio o en servicios como *AWS/Azure*. De esta forma, un desarrollador en la red interna tiene las mismas restricciones de acceso a una base de datos sensible en la Nube que si estuviera conectado desde fuera —nada de confianza implícita por "estar dentro" de una *VPN* corporativa—. Este caso de uso muestra cómo *Zero Trust* habilita la innovación (movilidad a la nube, colaboración global) sin añadir vulnerabilidades, proporcionando una postura consistente de seguridad en todo el ecosistema de TI corporativo.

Tendencias de mercado y regulaciones que *impulsan* la adopción

La adopción de *Zero Trust* no ocurre en vano. Hay tendencias del mercado y mandatos regulatorios crecientes que están impulsando su implementación a nivel global. Comprender estas tendencias refuerza el por qué es importante invertir hoy en *Zero Trust*, anticipándose a las exigencias externas y manteniendo la competitividad. Entre las principales tendencias, y que enseguida detallamos, destacan:

Amplia adopción empresarial y prioridad estratégica: según una encuesta global de Gartner en 2024, casi dos tercios de las organizaciones en el mundo ya han implementado, total o parcialmente, estrategias *Zero Trust* en su ciberseguridad[13]. Esto indica que la mayoría de las compañías avanza ya en esta dirección, muchas veces patrocinadas desde el más alto nivel empresarial, conscientes de que fortalecer la ciberseguridad es clave para la resiliencia del negocio. Asimismo, el auge del trabajo híbrido ha acelerado la adopción, pues la necesidad de habilitar fuerzas laborales distribuidas con seguridad impulsó a innumerables organizaciones a iniciar proyectos *Zero Trust* para sustituir sistemas, aplicaciones o tecnologías obsoletas y enfrentar el aumento de ataques maliciosos[14].

Mandatos gubernamentales y regulaciones emergentes: los gobiernos y entes reguladores están promoviendo activamente *Zero Trust* como parte de sus estrategias de seguridad nacional y sectorial. Además de Estados Unidos, quien emitió la directriz en 2021 obligando a las agencias federales la adopción de modelos *Zero Trust*.

Países como Reino Unido y Australia han emitido lineamientos similares, convirtiendo a *Zero Trust* en un "mandato internacional" para la protección de infraestructuras críticas[15]. Incluso, el Departamento de Defensa de Estados Unidos ha trazado un plan para implementar *Zero Trust* en todos sus sistemas antes de 2027, reconociéndolo como "un cambio transformacional en

cómo el departamento aborda la ciberseguridad", en palabras de su propio *CIO*[16]. Mientras que, en Latinoamérica, no existe por ahora una regulación nacional que obligue explícitamente la implementación del modelo; no obstante, hay países como Brasil, México o Colombia que avanzan en marcos normativos de ciberseguridad y protección de datos que facilitan y promueven implícitamente la adopción de estándares *Zero Trust*.

En el sector privado, reguladores financieros —como comisiones bancarias, bancos centrales y unidades de inteligencia financiera—, así como autoridades de sectores como salud, energía, telecomunicaciones y protección de datos, comienzan a evaluar la madurez de *Zero Trust* de las entidades supervisadas como parte de sus auditorías. Todo apunta a que, más que una recomendación, *Zero Trust* será pronto un requisito formal en normas y estándares, por lo que las empresas que inviertan temprano estarán protegidas y, sobre todo, mejor preparadas para cumplir futuras obligaciones regulatorias sin contratiempos.

Crecimiento del mercado y madurez tecnológica: se estima que el mercado global de tecnologías y servicios *Zero Trust* alcanzó 20 mil millones de dólares en 2020, con una tasa de crecimiento anual compuesta de 15.2% proyectada hasta 2028[17]. Detrás de estas cifras está la inversión sostenida de empresas en modernizar sus infraestructuras de seguridad. Los grandes proveedores de tecnología —como Microsoft, Google, Cisco y Palo Alto, entre otros— han incorporado en sus ofertas marcos *Zero Trust*, facilitando la adopción con soluciones más integradas y casos de éxito documentados.

Asimismo, han surgido arquitecturas de referencia y certificaciones específicas que están profesionalizando el ecosistema (por ejemplo, la especificación *NIST SP 800-207* define el modelo *Zero Trust* a nivel gubernamental). Esta madurez tecnológica significa que adoptar *Zero Trust* hoy es más asequible y viable que hace unos años, con lecciones aprendidas de implementaciones previas, herramientas más automatizadas e integraciones más sencillas con la infraestructura existente.

Presiones de ciberseguros y partes interesadas: otra tendencia impulsora proviene de terceros interesados en la ciberseguridad corporativa. Las aseguradoras de ciberriesgo, al evaluar pólizas, están comenzando a valorar positivamente la adopción de *Zero Trust* como indicador de menor riesgo de siniestro, lo que podría traducirse en primas más bajas o en la propia viabilidad de obtener cobertura.

De igual manera, los consejos y comités de auditoría preguntan cada vez más sobre la estrategia *Zero Trust* de sus empresas, dado que un incidente grave puede impactar las finanzas y la reputación corporativa. Los clientes *B2B*, por su parte, incluyen requisitos de ciberseguridad en las negociaciones comerciales, ya que contar con un enfoque *Zero Trust* robusto puede ser un factor para ganar contratos, especialmente con clientes gubernamentales o de sectores muy sensibles.

En suma, el entorno de negocio en general está elevando las expectativas: se espera que una empresa seria en ciberseguridad haya adoptado o esté en camino de adoptar *Zero Trust*. Esto convierte la iniciativa en algo más que "lo correcto por hacer", es un habilitador para cumplir requisitos de seguros, calificaciones de terceros (por ejemplo, informes ASG en materia de ciberseguridad) y mantener la confianza de inversores y de clientes en el gobierno corporativo.

Estas cuatro tendencias confirman que *Zero Trust* llegó para quedarse. Invertir estratégicamente en este enfoque significa alinearse con las mejores prácticas globales, evitar futuros apuros de cumplimiento y posicionar a la organización como líder en ciberseguridad en su industria. Al contrario, ignorar esta evolución podría dejar a la empresa expuesta tanto a amenazas cibernéticas mayores como a penalizaciones regulatorias y desventajas competitivas.

Un funcionario del Pentágono describió *Zero Trust* como "el enfoque más robusto y confiable para garantizar que nuestros sistemas sean resilientes frente a las amenazas evolutivas"[18]. La afirmación, que es aplicable a la defensa nacional de Estados Unidos y al ámbito empresarial, refleja el consenso emergente: adoptar Zero Trust no es solo una decisión de seguridad, sino de negocio, impulsada por fuerzas externas e internas que ninguna empresa puede darse el lujo de ignorar.

Conclusión

En la economía digital, invertir en *Zero Trust* se ha convertido en una decisión estratégica inteligente para las organizaciones que buscan equilibrar la ciberseguridad y la agilidad empresarial. Los argumentos a favor son contundentes: *Zero Trust* reduce riesgos críticos, protege los activos más valiosos, asegura el cumplimiento regulatorio, fortalece la resiliencia operativa y genera eficiencia con retornos medibles. Todo ello se traduce en valor para el negocio, ya sea evitando pérdidas multimillonarias por ciberincidentes, salvaguardando la confianza de los clientes o permitiendo que la empresa adopte nuevas tecnologías y modelos de trabajo, sin exponer su continuidad.

Es importante resaltar que *Zero Trust* no es un producto que se compra y listo, es un camino de transformación en la cultura y arquitectura de seguridad de la organización. Requiere compromiso desde la alta dirección para liderar el cambio, inversión en las áreas clave (identidades, dispositivos, redes y datos) y una hoja de ruta realista que integre procesos y personas, además de tecnología. No obstante, los ejemplos de la industria muestran que este esfuerzo vale la pena: quienes han recorrido el camino reportan mejoras sustanciales en su postura de seguridad, así como en indicadores de negocio[19]. Además, al adoptar *Zero Trust* proactivamente, la empresa envía un mensaje claro a todos sus stakeholders: la ciberseguridad y la confianza son prioridades innegociables en su estrategia corporativa.

Zero Trust es más que una tendencia en ciberseguridad, es un habilitador estratégico para el crecimiento sostenible en medio de la incertidumbre digital. Apoyar esta iniciativa significa proteger el futuro de la compañía contra amenazas venideras y crear las condiciones de seguridad necesarias para innovar con confianza. Aquellas organizaciones que den este paso estratégico estarán mejor preparadas para afrontar los desafíos del mañana, convirtiendo la ciberseguridad en un diferenciador. Por todo ello, la inversión en *Zero Trust* se justifica de manera sólida como una decisión de negocio que protege y potencia el valor corporativo a largo plazo.

Referencias

1. Lee, R. Et al (2021). *Lessons Learned from the SolarWinds Cyberattack, and the Future for the New York Department of Financial Services' Cybersecurity Regulation.* Arnold & Porter. https://www.arnoldporter.com/en/perspectives/advisories/2021/06/lessons-learned-from-the-solarwinds-cyberattack
2. NIST, (2021). *Improving the Nation's Cybersecurity: NIST's Responsibilities Under the May 2021 Executive Order.* National Institute of Standards and Technology. U. S. Department of Commerce. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity
3. Jakkal, V. (2022). Microsoft Zero Trust solutions deliver 92 percent return on investment, says new Forrester study. Microsoft Security. https://www.microsoft.com/en-us/security/blog/2022/01/12/microsoft-zero-trust-solutions-deliver-92-percent-return-on-investment-says-new-forrester-study/
4. Tyas, A. (2025). *What is the Cost of a Data Breach in 2023?* UpGuard. https://www.upguard.com/blog/cost-of-data-breach
5. Pure Storage, (2025). *How a Zero Trust Architecture Can Help Mitigate Ransomware Risks.* https://blog.purestorage.com/purely-educational/how-a-zero-trust-architecture-can-help-mitigate-ransomware-risks/
6. Lee, R. Et al (2021). *Lessons Learned from the SolarWinds Cyberattack, and the Future for the New York Department of Financial Services' Cybersecurity Regulation.* Arnold & Porter. https://www.arnoldporter.com/en/perspectives/advisories/2021/06/lessons-learned-from-the-solarwinds-cyberattack
7. Jakkal, V. (2022). *Microsoft Zero Trust solutions deliver 92 percent return on investment, says new Forrester study.* Microsoft Security. https://www.microsoft.com/en-us/security/blog/2022/01/12/microsoft-zero-trust-solutions-deliver-92-percent-return-on-investment-says-new-forrester-study/
8. INCIBE, (2023). *Metodología Zero Trust: fundamentos y beneficios. Instituto Nacional de Ciberseguridad.* España. https://www.incibe.es/incibe-cert/blog/metodologia-zero-trust-fundamentos-y-beneficios
9. Cisco, (2022). *Guía de Cisco para la madurez de la confianza cero.* Cisco Secure. https://www.cisco.com/c/dam/global/es_mx/products/collateral/security/zero-trust-field-guide.pdf
10. Cisco, (2022). *Guía de Cisco para la madurez de la confianza cero.* Cisco Secure. https://www.cisco.com/c/dam/global/es_mx/products/collateral/security/zero-trust-field-guide.pdf
11. BeyondCorp. *A new approach to enterprise security.* https://cloud.google.com/beyondcorp
12. Power, C. (2022). *5 Zero Trust Use Cases to Know About.* Power Consulting Group. https://powerconsulting.com/blog/zero-trust-use-cases/
13. Gartner, (2024). *Gartner Survey Reveals 63% of Organizations Worldwide Have Implemented a Zero Trust Strategy.* https://www.gartner.com/en/newsroom/press-releases/2024-04-22-gartner-survey-reveals-63-percent-of-organizations-worldwide-have-implemented-a-zero-trust-strategy
14. Jones, D. (2024). *Majority of businesses worldwide are implementing zero trust, Gartner finds.* TechTarget. https://www.cybersecuritydive.com/news/majority-businesses-zero-trust-gartner/713856/
15. Cisco, (2022). *Guía de Cisco para la madurez de la confianza cero.* Cisco Secure. https://www.cisco.com/c/dam/global/es_mx/products/collateral/security/zero-trust-field-guide.pdf
16. Clark, J. (2024). *DOD Cyber Officials Detail Progress on Zero Trust Framework Roadmap.* U. S. Department of Defense. https://www.defense.gov/News/News-Stories/Article/Article/3729448/dod-cyber-officials-detail-progress-on-zero-trust-framework-roadmap/
17. Cisco, (2022). *Guía de Cisco para la madurez de la confianza cero.* Cisco Secure. https://www.cisco.com/c/dam/global/es_mx/products/collateral/security/zero-trust-field-guide.pdf
18. Clark, J. (2024). *DOD Cyber Officials Detail Progress on Zero Trust Framework Roadmap.* U. S. Department of Defense. https://www.defense.gov/News/News-Stories/Article/Article/3729448/dod-cyber-officials-detail-progress-on-zero-trust-framework-roadmap/
19. Jakkal, V. (2022). *Microsoft Zero Trust solutions deliver 92 percent return on investment, says new Forrester study.* Microsoft Security. https://www.microsoft.com/en-us/security/blog/2022/01/12/microsoft-zero-trust-solutions-deliver-92-percent-return-on-investment-says-new-forrester-study/

Contactos:

Paula Álvarez
Socia | *Technology & Transformation* | Cyber
Deloitte S-Latam
palvarez@deloittemx.com

Andrea Bernales Zapata
Socia | *Technology & Transformation* | Cyber
Deloitte S-Latam
abernales@deloittemx.com

Deloitte.