

cirion

FORTINET

Ciberseguridad:

cuando la IA cambia el riesgo, la seguridad cambia de arquitectura



Índice

1. Introducción: lo que la IA le cambió a la empresa	3
IA y ciberseguridad: datos “amenazantes”	4
2. La seguridad empieza en la conectividad	5
Seguridad avanzada en la arquitectura de red	5
Características del servicio gestionado SD-WAN de Cirion	6
3. La identidad: materia prima para los atacantes	7
Zero trust: el fin de la confianza automática	7
Identidad: los números del riesgo	7
4. La aceleración de los ataques y el límite de la respuesta manual	8
DDoS Mitigation: evitar que el problema llegue al negocio	8
5. El desafío de gestionar una arquitectura de seguridad cada vez más compleja	9
Los compromisos del SNOOC (recuadro)	9
6. La seguridad como capacidad operativa	10
7. Diferenciadores: por qué Cirion	11
8. Conclusiones	12

1. Introducción: lo que la IA le cambió a la empresa



Mucho se habla de cómo la IA evoluciona la forma en que las empresas trabajan, toman decisiones y escalan sus operaciones. Pero, al mismo tiempo, ocurre otra transformación paralela: cómo organizaciones deben proteger sus datos y sus sistemas.

El panorama tecnológico, de por sí, venía creciendo en complejidad durante los últimos años. Las aplicaciones dejaron de estar concentradas en un único entorno. Las organizaciones combinan servidores propios, nubes públicas, *edge*, servicios SaaS, sucursales, trabajadores remotos, dispositivos móviles y proveedores externos. Cada nueva conexión agrega capacidad al negocio, pero también introduce una nueva relación que debe ser gestionada y protegida.

La IA agrega un ingrediente adicional en este mapa de complejidad. Porque así como permite automatizar tareas que antes requerían intervención humana, acelera la toma de decisiones e impulsa la eficiencia, también acelera la generación de ataques y ampliar el volumen de intentos sobre infraestructuras cada vez más distribuidas.

El fenómeno se acelera. Según la consultora McKinsey, el 88% de las organizaciones ya utiliza IA en al menos una función, mientras que el 62% experimenta con agentes de IA. Cerca de dos tercios de las organizaciones todavía se

encuentran en etapas piloto. La tecnología avanza a pasos agigantados mientras que muchas veces las arquitecturas todavía no están adaptadas para soportarla.

Al mismo tiempo, la IA está envuelta en una paradoja, en especial cuando se trata de ciberseguridad. Por un lado, ofrece a las empresas herramientas poderosas para anticipar ataques, indagar patrones de comportamiento anómalos y acelerar las defensas. Pero, por el otro, esas mismas herramientas están disponibles para los atacantes, que puede automatizar tareas y alcanzar escalas nunca antes conocidas.

La carrera está jugándose en este momento: ante un oponente que corre a toda velocidad, depender de estructuras en que las personas reciben una alerta, la interpretan, determinan su relevancia, identifican el activo afectado y deciden qué hacer puede ser sinónimo de llegar demasiado tarde.

El informe M-Trends 2026, de Google Cloud y Mandiant, le pone cifras a esta potencial asimetría: el traspaso mediano de un incidente pasó de más de ocho horas en 2022 a apenas 22 segundos en 2025. Esto, en términos simples, significa que el tiempo que tarda un atacante en pasar de un sistema comprometido a otro cayó drásticamente.

Es decir: hay más amenazas, llegan más rápido y no necesariamente existen más personas para administrarlas. Mientras la velocidad del negocio aumenta, se reduce el tiempo disponible para detectar, analizar y responder ante un incidente.

En este contexto, sumar herramientas de seguridad dejó de ser sinónimo de estar mejor protegido. Cuando cada capa funciona de manera independiente, la organización también suma consolas, políticas, integraciones y procesos que alguien debe administrar. La complejidad puede convertirse, por sí misma, en una nueva superficie de riesgo. La estrategia debe centrarse, entonces, en definir una arquitectura capaz de conectar, proteger, observar y responder de manera consistente.

La cobertura continua, la visibilidad y la capacidad de responder en tiempo real son ahora capacidades imprescindibles. Pero el desafío no se limita a detectar

más rápido. También se vuelve imprescindible hacerlo sin agregar más complejidad. La seguridad debe integrarse a la arquitectura de red, operar de manera consistente y contribuir a que el negocio pueda seguir funcionando incluso frente a una amenaza.

Este *whitepaper* analiza cómo cambia el escenario de ciberseguridad a partir de la expansión de la IA y de infraestructuras cada vez más distribuidas. Aborda el vínculo entre conectividad y seguridad, el rol crítico de la identidad, la aceleración de los ataques y los límites de una respuesta basada exclusivamente en la intervención manual, así como el desafío de gestionar arquitecturas cada vez más complejas. El objetivo es avanzar hacia una concepción de la seguridad como capacidad operativa, integrada a la infraestructura y al funcionamiento del negocio.

IA y ciberseguridad: datos “amenazantes”

- **El atacante no sólo logra vulnerar los sistemas en 22 segundos: el M-Trends detectó que una vez que ingresó, permanece en promedio 14 días antes de ser detectado o de que termine el incidente.**
- **Los reguladores de la región están fijando plazos de detección muy por debajo de esa media: Chile exige alerta temprana en 3 horas y reporte completo en 72 horas (Ley 21.663), Colombia, 24 horas en el sector financiero (Circular Externa 007 de 2018 de la Superintendencia Financiera) y Brasil dos días hábiles ante la ANPD (Agencia Nacional de Protección de Datos). Cirion permite a las empresas cumplir con esos plazos.**
- **Según el World Economic Forum, el 94% señala la IA como principal motor de cambio y 87% ubica las vulnerabilidades de IA como el riesgo de más rápido crecimiento.**
- **De acuerdo al Cost of a Data Breach Report 2026, elaborado por IBM y el Ponemon Institute, el 19% de los ataques maliciosos está habilitado por IA.**
- **FortiGuard Labs indica que las víctimas confirmadas de ransomware pasaron de cerca de 1.600 a 7.831 en un año: un aumento del 389%, impulsado por kits de cibercrimen basados en IA.**

2. La seguridad empieza en la **conectividad**



La conectividad representa hoy en las empresas más que el transporte que lleva un dato de un lugar a otro. De hecho, cuando no está bien resuelta, constituye un importante obstáculo para la innovación y el crecimiento. El informe Enterprise Horizons 2025, de la consultora de mercado IDC, detectó que el 94% de las organizaciones encuentra en su red el límite para avanzar en proyectos tecnológicos de gran escala, en particular los que involucran IA. Además, otro 45% reporta problemas específicos de latencia.

Cuando hablamos del modelo de seguridad, la primera referencia que tenemos es aquel que se construía alrededor de la idea de “proteger el perímetro”. Pero ese perímetro se volvió cada vez más difícil de definir. Hoy, usuarios, aplicaciones y datos pueden encontrarse en diferentes re-des, nubes, sucursales y ubicaciones. Proteger el punto de entrada dista mucho de ser suficiente. El tráfico debe ser observado y protegido a lo largo de la arquitectura.

La red se consolida como un punto estratégico de control. No puede haber ninguna ventana de tiempo entre el momento de la conexión y el instante en el que se activa la protección. Cuando la seguridad forma parte del servicio de conectividad, esa brecha desaparece.

Seguridad avanzada en la arquitectura de red

Ese principio está detrás de Secure SD-WAN de Cirion, que integra seguridad avanzada directamente en la arquitectura de red. La solución optimiza el tráfico, prioriza aplicaciones críticas y administra de manera centralizada las políticas de seguridad, al mismo tiempo que incorpora capacidades como *firewall* de última generación, cifrado y protección de los sitios remotos y su-cursales. También combina distintos tipos de acceso, incluidos enlaces de Cirion y accesos pro-vistos por el cliente.

La ventaja es operativa. Cuando conectividad y seguridad se administran desde una arquitectu-ra integrada, se reduce la cantidad de componentes que deben gestionarse por separado y se obtiene una visión más consistente de lo que ocurre en la red.

La misma lógica aparece en la propuesta SASE de Cirion, que converge funciones de red y segu-ridad en un único servicio basado en la nube. En este modelo, Secure SD-WAN, ZTNA (*zero trust access network*, un concepto sobre el que ampliaremos más adelante) y otras capacidades de seguridad trabajan dentro de una arquitectura unificada, con políticas consistentes y gestión centralizada.

Históricamente, los responsables de ciberseguridad tuvieron el desafío de encontrar mecanis-mos para proteger la red. Hoy, en cambio, se trabaja en diseñar una red que ya incorpore la pro-tección desde el mismo diseño.

Características del servicio gestionado SD-WAN de Cirion



Cirion atiende 7x24x365 las plataformas de SD-WAN y seguridad que administra, con escalamiento a especialistas de nivel 2 y 3 y prácticas de gestión bajo ITIL v4.



Orquesta la administración mediante FortiManager y la analítica y reportería mediante FortiAnalyzer.



No entrega un producto, sino que opera una arquitectura que permite consultar registros y eventos, generar informes y adaptar dashboards a necesidades operativas, auditorías o requerimientos regulatorios.



Los datos de conectividad y seguridad dejan de estar distribuidos entre diferentes herramientas sin una lectura común y pueden convertirse en evidencia para entender qué está sucediendo, acelerar el análisis de causa raíz y tomar decisiones.



Se ofrece en tres modalidades: Connect, cuando la seguridad se concentra en el hub; Protect, cuando cada sede necesita su propia protección; AI, cuando se suman prevención de fuga de da-tos y funciones asistidas por IA.

3. La identidad: materia prima para los atacantes

Otra transformación vuelve insuficiente el antiguo perímetro: la identidad. Un usuario puede conectarse desde una oficina, desde su casa, desde un dispositivo móvil o desde una ubicación de un tercero. Una aplicación puede estar en una nube pública y un proveedor externo puede necesitar acceso temporal a un recurso corporativo. En estos escenarios, saber que alguien posee una contraseña no constituye prueba suficiente.

Las credenciales son un componente central de los incidentes que afectan a entornos *cloud*. El problema va mucho más allá de que una contraseña pueda ser robada: una credencial válida es una puerta legítima hacia recursos que el atacante no debería poder utilizar.

Zero trust: el fin de la confianza automática

En lugar de asumir que una identidad es confiable porque consiguió ingresar, cada sesión debe evaluarse de acuerdo con su identidad, contexto, dispositivo y postura.

Zero trust (confianza cero) es un modelo de seguridad que se basa en la premisa de nunca confiar per sé en que un usuario es válido, aún cuando esté dentro de la red, sino verificar cada vez. Asume que las amenazas ya pueden haber vulnerado los sistemas o que pueden provenir de cualquier lugar. Por lo tanto, no otorga confianza automática a nadie, sin importar si es el director general de la empresa conectado desde la oficina central. El acceso no se hereda: se gana.

ZTNA es la puesta en práctica de este concepto. En Cirion, toma el nombre de User Identity. El permiso deja de ser una propiedad permanente de una credencial y pasa a evaluarse en cada sesión, reduciendo el acceso al mínimo necesario. Esto adquiere especial relevancia cuando participan terceros: contratistas, proveedores, socios tecnológicos y otros colaboradores pueden necesitar acceso a determinados recursos sin que eso signifique que deban incorporarse a la red corporativa con los mismos privilegios que un empleado.

La identidad debe ser vista como una política de seguridad y no como un simple mecanismo de autenticación. Si una credencial puede estar comprometida, es necesario determinar qué condiciones adicionales deben cumplirse para conceder acceso. Una arquitectura integrada es fundamental: SD-WAN puede evolucionar hacia modelos de seguridad más amplios y facilitar la transición hacia arquitecturas SASE/SSE, siempre de acuerdo con la factibilidad y el alcance específico de cada implementación.

En ese recorrido, no es requisito reemplazar de una vez la arquitectura existente. Es posible trasladar progresivamente el control hacia donde se encuentre el riesgo: el usuario, el dispositivo, la aplicación y el contexto de cada conexión. La tendencia, en este sentido, es irrefrenable: Gartner sostiene que el 70% de las compras de SD-WAN serán parte de una plataforma SASE de un único proveedor en 2028, frente al 25% en 2025.

Identidad: los números del riesgo

- **35,4 millones** de accesos corporativos comprometidos disponibles en 2025.
- **67.650 millones** de intentos de fuerza bruta durante el año: unos 185 millones por día.
- **79% de crecimiento interanual** en los registros disponibles de robo de credenciales.

(Fuente: Global Threat Landscape Report 2026, FortiGuard Labs)

4. La aceleración de los ataques y el límite de la respuesta manual



Detectar un ataque no es lo mismo que llegar a tiempo para detenerlo. Los ataques DDoS (de-negación de servicio distribuido), que buscan colapsar un sitio web, servidor o servicio digital inundándolo con una cantidad masiva de tráfico falso de internet hasta que se satura, se vuelve extremadamente lento o se cae por completo, muestran esa diferencia de manera particularmente clara.

Cloudflare registró durante el primer semestre de 2026 un ataque de 31,4 Tbps que duró apenas 35 segundos. En el mismo período, el 90,6% de los ataques de capa de red duró menos de diez minutos. Cuando un incidente puede comenzar y terminar a esa velocidad, las limitaciones de los modelos basados exclusivamente en la reacción humana son más evidentes.

Si la organización primero debe detectar la anomalía, confirmar que se trata de un ataque, abrir un ticket y solicitar una acción, es cada vez más probable que el tiempo de respuesta sea superior a la duración del propio incidente. La protección debe acercarse al lugar donde ocurre el tráfico. Para usar el ejemplo mencionado: un ataque de 35 segundos no se mitiga con un equipo en el borde del cliente ni con una llamada al proveedor, sino en la red troncal, de forma automatizada y siempre activa, antes de que el tráfico llegue al negocio.

DDoS Mitigation: evitar que el problema llegue al negocio

DDoS Mitigation de Cirion detecta, filtra y limpia tráfico volumétrico, de protocolo y de aplicación dentro de su red troncal antes de que llegue a la infraestructura del cliente. El servicio puede operar bajo demanda o de manera siempre activa, con asistencia del centro de operaciones.

El mismo principio aplica al ruteo. La protección contra el secuestro de prefijos y los desvíos maliciosos no comienza necesariamente en un firewall, sino antes, en la propia infraestructura que determina por dónde circula el tráfico.

La implementación de RPKI sobre el backbone AS3356 que Cirion opera en América Latina agrega esa capa de protección en el ruteo. AS3356 identifica un backbone Tier 1 de alcance regional, conectado con miles de sistemas autónomos. Esa escala permite abordar la seguridad del tráfico desde la propia infraestructura de red.

La lógica detrás de esto: algunas amenazas pueden abordarse de manera eficaz sólo cuando se las trata en la capa donde se originan. En un mundo distribuido, la ciberseguridad no puede estar concentrada en el perímetro de la empresa.

5. El desafío de gestionar una arquitectura cada vez más compleja



El atacante trabaja a velocidad de máquina y la región, como se mencionó, no tiene el talento suficiente para hacer frente a esa escala. Nadie gana comprando más herramientas inconexas: la defensa se sostiene con gente, procesos y vigilancia continua.

Aquí aparece el concepto de operación como parte de la seguridad. Históricamente, las empresas gestionaban por un lado el NOC (network operations center), que se ocupaba de que internet no se cayera y de que los servidores funcionaran rápido, y por el otro el SOC (security operations center), que buscaba hackers, virus y brechas de seguridad. Hoy, el SNOC rompe esa barrera: en el mundo real, una caída del sistema y un ciberataque suelen ser el mismo problema visto desde ángulos diferentes.

Si, además, ese servicio es gestionado, la empresa tiene la posibilidad de trasladar buena parte de la carga

cotidiana (monitoreo, gestión de cambios, gestión de incidentes, analítica, reportería y escalamiento) a equipos especializados, sin que la organización pierda el control sobre sus políticas.

Ninguna alerta debería quedar a la espera del siguiente turno para ser interpretada. El desafío no pasa solamente por incorporar más herramientas, sino por contar con cobertura continua y capacidad de correlacionar información en tiempo real. Un centro de operaciones que monitorea la red puede detectar señales antes de que se conviertan en un ticket, porque red y seguridad forman parte de una misma operación y no de sistemas independientes que deben cruzar registros después del hecho. A esa vigilancia 24x7, SNOC suma servicios profesionales que abarcan evaluación, diseño, despliegue y endurecimiento de la infraestructura.

Los compromisos del SNOC

- Los tiempos de escalamiento comprometidos cumplen con las demandas cada vez más exigentes de los reguladores.
- Gestión de cambios.
- Servicios profesionales: evaluación, configuraciones avanzadas, endurecimiento y ethical hacking (pruebas de penetración y análisis de vulnerabilidades).
- Evidencia para el regulador: la analítica centralizada entrega reportería estándar o personalizada y retiene los registros para responder cuándo se detectó, cuándo se contuvo y cuándo se reportó.

6. La seguridad como capacidad operativa



La transformación digital no termina con una tecnología determinada. Después de la nube llegaron los entornos híbridos. Después, el trabajo distribuido. Ahora, la inteligencia artificial y los agentes están incorporando nuevas formas de interacción entre usuarios, aplicaciones y datos. Cada etapa vuelve a poner a prueba la arquitectura.

Por eso la seguridad necesita diseñarse con capacidad de evolución. La convergencia entre conectividad, seguridad y operación modifica el objetivo de la arquitectura.

Antiguas estrategias, como acumular controles para cubrir cada amenaza posible, van quedando obsoletas. Hoy, es necesario definir una arquitectura que permita reducir exposición, aplicar políticas de manera consistente, detectar cambios y responder con velocidad sin trasladar toda la complejidad al equipo interno.

Ese cambio es particularmente relevante a medida que las empresas incorporan más IA. Cada nuevo agente, aplicación o flujo automatizado aumenta la velocidad del negocio, es cierto, pero también incrementa la cantidad de interacciones que deben ser controladas.

La arquitectura debe acompañar ese crecimiento sin

convertirse en un cuello de botella. En este contexto, una red inteligente necesita mucho más que disponibilidad de la conectividad:

- **Visibilidad.**
- **Políticas.**
- **Control de identidades.**
- **Capacidad de inspección.**
- **Mecanismos de respuesta.**
- **Operación.**

Y, tal vez lo más importante: la arquitectura de ciberseguridad debe estar preparada para evolucionar junto con el negocio.

7. Diferenciadores: por qué Cirion



La red de Cirion constituye la base sobre la cual se integran estas capacidades. La compañía cuenta con más de 105.000 kilómetros de fibra propia en América Latina, una red Tier 1, con presencia directa en 12 mercados y alcance de red en más de 20 países. Ese control sobre la infra-estructura permite que determinadas capacidades de seguridad se apliquen más cerca del origen del tráfico y no solamente en el perímetro del cliente.

Pero, más allá de eso, la diferencia entre una estrategia de seguridad y una colección de herramientas está en la capacidad de sostenerla en el tiempo. Cirion integra conectividad, seguridad y operación sobre esa infraestructura regional propia y despliega capacidades que responden a diferentes puntos de la arquitectura: Internet dedicado con seguridad integrada, IP VPN, Cloud Connect, Secure SD-WAN, User Identity (ZTNA), Firewall & UTM y DDoS Mitigation.

El modelo incorpora operación continua. NOC/SOC 24x7x365 sobre la misma red que transporta el tráfico del cliente permite que la seguridad no quede limitada a la tecnología instalada, sino que forme parte de una capacidad permanente de monitoreo y gestión.

En Secure SD-WAN, esa integración se expresa en una

plataforma que combina conectividad, seguridad, analítica y gestión centralizada. Las políticas pueden administrarse desde una capa de orquestación común, mientras que la solución incorpora funcionalidades de seguridad directamente en los puntos de acceso.

En DDoS Mitigation, el diferencial está en otro lugar: la posibilidad de detectar y limpiar tráfico malicioso dentro de la red antes de que alcance la infraestructura protegida.

En ZTNA, el foco pasa a la identidad y al contexto de cada acceso.

En Cloud Connect, a la privacidad y trazabilidad del camino que recorre el dato.

Cuando la IA acelera el negocio y también acelera el riesgo, proteger mejor no significa necesariamente sumar más herramientas. Significa reducir las distancias entre conexión, protección, visibilidad y respuesta. En un entorno donde los ataques pueden desarrollarse en segundos, la seguridad no puede empezar cuando alguien descubre que existe un problema. Tiene que estar presente desde el momento en que la empresa se conecta. Y ofrecer las herramientas para poder seguir operando. Porque la resiliencia se diseña antes del incidente y se demuestra después.

8. Conclusiones



América Latina vive una paradoja estructural: soporta el mayor volumen de ciberataques del planeta y, al mismo tiempo, tiene la mayor escasez de talento de seguridad del planeta.

Cuando la amenaza crece más rápido de lo que una región puede contratar a quien la detenga, la respuesta no puede ser comprar más herramientas para que las utilice un equipo inexistente, sino que la seguridad viva dentro de la red y que la operación se delegue en quien ya gestiona esa red las 24 horas.

Cirion opera la capa donde se decide qué entra y qué sale: una plataforma panamericana con más de 105.000

km de fibra propia, presencia directa en 12 mercados con alcance a más de 20 países, más de 160 data centers interconectados, mitigación de denegación de servicio en la red troncal y operación de NOC/SOC 24x7x365, todo con una neutralidad estructural: no compite con el cliente, ni con su nube, ni con los clientes de ésta.

¿Cómo repercute todo esto en el negocio de nuestros clientes? Menor exposición, mayor continuidad, políticas consistentes entre países, menos terceros que auditar, trazabilidad demostrable ante el regulador y capacidad de detección dentro de los plazos legales de reporte. La resiliencia deja de ser un gasto de TI y se convierte en una protección directa del ingreso y de la reputación.

Fuentes

- McKinsey, <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-2025>
- M-Trends, <https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2026>
- CheckPoint, <https://blog.checkpoint.com/research/cyber-threats-spike-in-april-2026-as-ransomware-expands-and-attack-volumes-climb-after-short-lived-moderation/>
- WEF, <https://www.weforum.org/publications/global-cybersecurity-outlook-2026/>
- IBM, <https://www.ibm.com/downloads/documents/us-en/16dd90a741c46c2c>
- FortiGuard Labs, <https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2026/fortinet-2026-global-threat-landscape-report-reveals-surge-in-ai-enabled-cybercrime-increase-ransomware-victims-year-over-year>
- IDC, citado en <https://www.expereo.com/resources/reports/enterprise-horizons-2025>
- Gartner, citado en <https://www.paloaltonetworks.com/resources/research/gartner-2025-strategic-roadmap-sase-convergence>
- Cloudflare, <https://blog.cloudflare.com/ddos-threat-report-2026-h1>