Más allá de la detección

Por qué la confianza y la transparencia marcan el futuro de la ciberseguridad

kaspersky

Proven.
Transparent.
Independent.

Kaspersky lidera la evaluación independiente sobre confianza

La transparencia es una ventaja competitiva que construye una relación de confianza entre proveedores, clientes y reguladores.

Elementos diferenciadores clave:

- Múltiples Centros de Transparencia, con capacidad para inspeccionar las actualizaciones y acceso a las listas de materiales de software (SBOM)
- Almacenamiento de datos en distintas regiones
- Control granular de las actualizaciones y opciones de despliegue más flexibles
- Servicios en la nube, locales o con funciones de reputación desactivadas
- Sin recopilación innecesaria de datos de telemetría

60 criterios conforman la base del análisis, agrupados en tres grandes ámbitos

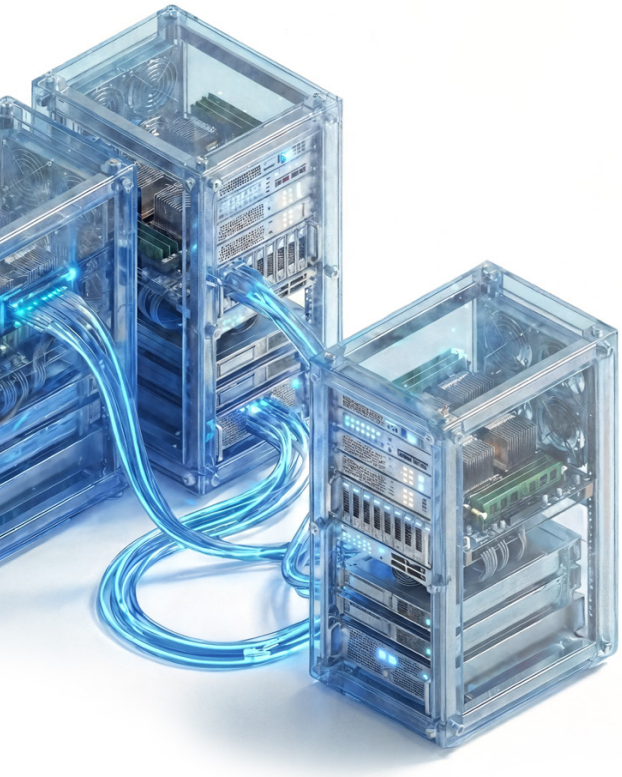
kaspersky

Proven.
Transparent.
Independent.

La fórmula de la confianza: **preguntas esenciales que tu proveedor debe poder responder**

El coste cada vez mayor de las amenazas cibernéticas, los estrictos requisitos regulatorios y el aumento de los ataques a la cadena de suministro llevan a los responsables de seguridad a replantearse cómo proteger sus organizaciones. Si bien las tecnologías EDR/EPP constituyen la base de la ciberdefensa, su acceso profundo a los sistemas y su amplia capacidad de procesar grandes volúmenes de datos abren serios interrogantes sobre transparencia, cumplimiento y confianza.

Aquellos que combinan una seguridad sólida con transparencia aseguran resiliencia, cumplimiento normativo y confianza



Algunas consideraciones clave

- ¿Qué datos recopilan las soluciones de seguridad?
- ¿Dónde y cómo se almacenan?
- ¿Cuánto control tiene el cliente sobre el funcionamiento del producto?
- ¿Qué herramientas ofrece el proveedor para verificar la fiabilidad del producto y del fabricante?

Un estudio independiente[1], encargada por la Cámara de Comercio del Tirol (WKO), aborda estas cuestiones críticas.

Conclusiones principales del estudio

Si bien todos los proveedores satisfacen los requisitos básicos de transparencia, sus prácticas difieren notablemente en el nivel de detalle y apertura. Aquellos que combinan una seguridad sólida con mecanismos de transparencia estructurados ofrecen las mayores garantías de resiliencia, cumplimiento normativo y confianza.

Implicaciones para las empresas

Selección del proveedor: Evalúa la transparencia y el cumplimiento de los estándares de seguridad tanto como las capacidades de protección.
Diligencia: Solicita certificaciones, SBOM y políticas de retención de datos; no te conformes con las afirmaciones genéricas.
Respuesta ante incidentes y aspectos legales: Evalúa los procesos de respuesta ante incidentes, las cláusulas de Safe Harbor y la jurisdicción aplicable.
Privacidad y configuración: Configura con cuidado los datos de la telemetría, la carga de archivos y las funciones de reputación para obtener un equilibrio entre la seguridad y la privacidad.

[1] "Transparency Review and Accountability in Cybersecurity", edición 2025, encargado por la WKO (Cámara de Comercio del Tirol) y llevado a cabo por AV-Comparatives, MCI | The Entrepreneurial School® y Studio Legale Tremolada.

kaspersky

Proven.
Transparent.
Independent.

Kaspersky es líder en materia de confianza

Características únicas que generan confianza:

- Uno de los pocos proveedores que ofrecen Centros de Transparencia para clientes empresariales
- Disponibilidad de SBOM y capacidades para inspeccionar las actualizaciones de bases de datos
- Cuenta con instalaciones de datos en todas las regiones analizadas
- Control absoluto sobre el despliegue de los servicios de reputación tanto en la nube o como en entornos locales

Un paso por delante de los estándares de la industria:

- **Kaspersky destacó en la mayoría de los criterios evaluados** y alcanzó, e incluso superó, los estándares de la industria en 57 de 60 categorías.[2]
- **Kaspersky superó el promedio de la industria en categorías como:** elección del usuario, transparencia, control de actualizaciones, desarrollo seguro, respuesta ante incidentes, gestión de datos y su minimización.

El estudio comparó las medidas de transparencia y responsabilidad de los principales proveedores de ciberseguridad y evaluó sus prácticas empresariales, el cumplimiento de normas jurídicas internacionales y medidas de protección de datos.
El análisis jurídico se apoyó en un estudio técnico para examinar cómo se aplican los principios declarados en los productos.
El producto de Kaspersky evaluado en el estudio fue Kaspersky Next EDR Optimum.

Kaspersky supera los estándares de la industria en un tercio de las categorías

[2] Consulte el documento complementario para conocer el recuento detallado de las categorías y sus definiciones.

kaspersky

Proven.
Transparent.
Independent.

La transparencia como una prioridad a nivel empresarial

Si bien los pliegos y condiciones de adquisición ya son exhaustivos, la inclusión de criterios de transparencia y confianza ayuda a mitigar riesgos empresariales. El estudio "Transparency Review and Accountability in Cybersecurity" ("Revisión de Transparencia y Responsabilidad en Ciberseguridad") evidencia las diferencias en el nivel de apertura de los proveedores: algunos ofrecen visitas a centros de transparencia y divulgaciones detalladas de seguridad, mientras otros se limitan a usar lenguaje contractual poco concreto y afirmaciones genéricas de cumplimiento[3].

Esta disparidad va más allá de las preferencias de licitación y adquisición: tiene un impacto directo en la exposición al riesgo de la compañía. Cuando se producen incidentes de ciberseguridad, la capacidad de una organización para responder de forma eficaz, demostrar debida diligencia regulatoria y mantener la confianza de las partes interesadas depende del conocimiento previo de las prácticas y metodologías del proveedor. La opacidad de un fabricante se traduce de manera directa en vulnerabilidades de cumplimiento, exposición legal y puntos ciegos operativos que pueden paralizar la respuesta a incidentes.

Los entornos empresariales actuales exigen un mayor nivel de responsabilidad, y los fabricantes de ciberseguridad no son una excepción. El estudio demuestra que la transparencia se relaciona estrechamente con la madurez operativa: aquellos que publican sus resultados de auditorías, mantienen SBOM actualizados y ofrecen controles de privacidad granulares mantienen prácticas de seguridad más sólidas.

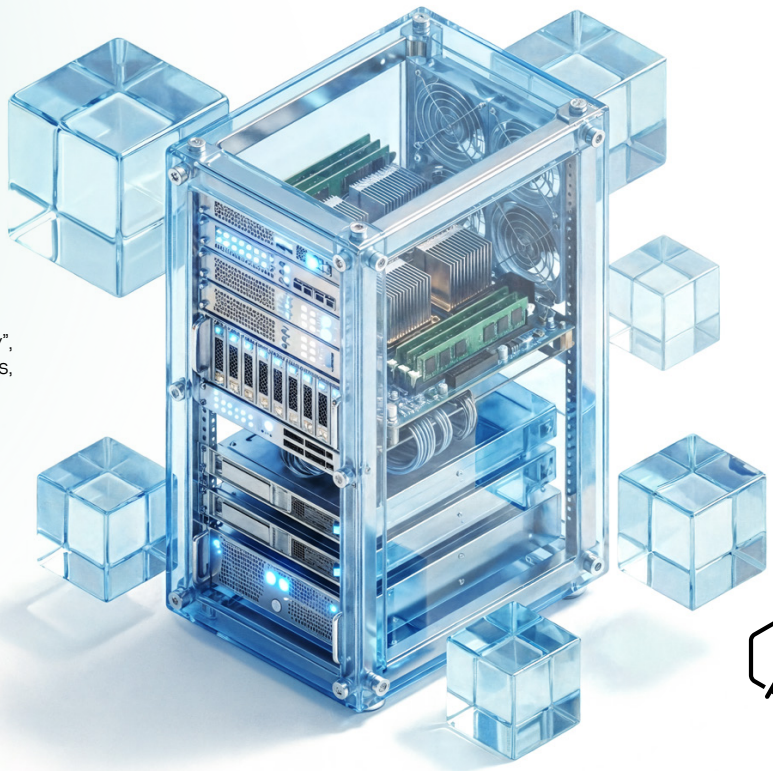
Los líderes empresariales deben exigir relaciones con proveedores que garanticen verificación independiente, documentación detallada y estructuras claras de responsabilidad. Este enfoque refuerza la ciberresiliencia, asegura el cumplimiento de normativas estrictas y aporta una ventaja competitiva en un panorama de amenazas cada vez más complejo.

Las conclusiones del estudio contribuyen directamente a mejorar la gobernanza, la adquisición informada y la gestión responsable del riesgo digital

14

principales

fabricantes de seguridad para endpoints evaluados



[3] "Transparency Review and Accountability in Cybersecurity", edición 2025, AV-Comparatives, MCI | The Entrepreneurial School®, y Studio Legale Tremolada, p. 39.

kaspersky

Proven.
Transparent.
Independent.

Resumen de estándares **de la industria**

Aunque muchas prácticas, como la adhesión al SDLC y el cumplimiento del RGPD, ya se han convertido en un estándar de la industria, otras siguen siendo poco frecuentes entre los 14 principales proveedores de seguridad evaluados:

Criterio	Adopción en la industria (nº de proveedores que ofrecen esta característica)	Kaspersky
Centros de Transparencia para revisión de código fuente y análisis de datos	Baja (3/14) 	Sí ✓
Descarga directa de firmas/definiciones para inspección	Media (6/14) 	Sí ✓
Disponibilidad de SBOM (Software Bill of Materials)	Baja (3/14) 	Sí ✓
Informes de transparencia regulares	Baja (4/14) 	Sí ✓
Servicio de reputación on-premise	Media (8/14) 	Sí ✓
Diferentes opciones de centros de datos	Baja (4/14) 	Sí ✓
Publicación regular de avisos de seguridad	Media (7/14) 	Sí ✓
Resultados de auditorías de seguridad independientes	Media (7/14) 	Sí ✓
Despliegue gradual de actualizaciones	Media (8/14) 	Sí ✓
Historial público de actualizaciones del producto	Alta (13/14) 	Sí ✓
Informes públicos sobre solicitudes de datos de fuerzas del orden	Media (9/14) 	Sí ✓
Informes de incidentes exhaustivos	Media (7/14) 	Sí ✓
Flexibilidad jurisdiccional para resolución de disputas	Media (11/14) 	No[4]
Cumplimiento con CCPA	Alta (12/14) 	Sí ✓
Cumplimiento con CRA	Ninguno (0) 	No

[4] Es posible cambiar la jurisdicción para la resolución de disputas mediante un contrato independiente (consulte la página 7 para más detalles).

kaspersky

Proven.
Transparent.
Independent.

Análisis detallado: prácticas clave

Código fuente y SBOM

Todos los fabricantes evaluados utilizan modelos de código cerrado, y 13 de los 14 revelan el uso de OSS de terceros. Sin embargo, solo 3 proveedores cuentan con centros de transparencia que permiten a las empresas revisar su código fuente.
De estos, uno solo da acceso a organismos gubernamentales, mientras que otro limita su alcance al código fuente y a la propiedad intelectual no especificada. Kaspersky destaca por ofrecer el Centro de Transparencia más completo, que permite revisar las reglas de detección de amenazas y verificar que las compilaciones coincidan con las versiones públicas.
Solo tres proveedores, entre ellos Kaspersky, ofrecen acceso a SBOM.

Control granular de actualizaciones

Muchos proveedores destacan sus buenas prácticas de actualización, por ejemplo procesos de implementación por fases, pruebas rigurosas y controles de calidad. Solo 5 proveedores, con Kaspersky a la cabeza, ofrecen una gestión integral del ciclo de las actualizaciones:

Función	Proveedores
Historial público de actualizaciones	13/14
Descarga de actualización de definiciones	6/14
Actualizaciones automáticas	14/14
Entornos de validación prelanzamiento	14/14
Despliegue escalonado de actualizaciones	8/14

Una mirada al Centro de Transparencia

Kaspersky opera más de 10 instalaciones de transparencia en todo el mundo, donde reguladores, gobierno y clientes pueden revisar de forma independiente el código fuente, las reglas de detección de amenazas, las actualizaciones de software y los procesos de desarrollo. Se ofrecen tres niveles de evaluación: “Blue Piste” para demostraciones generales, “Red Piste” para análisis dirigido de código y “Black Piste” para revisiones exhaustivas. Los visitantes pueden examinar la documentación de desarrollo seguro, reconstruir el código fuente para verificar que los módulos públicos coinciden con las compilaciones y revisar las actualizaciones de las bases de datos antivirus con la asistencia de expertos.

Nivel de seguridad

Una gestión sólida de vulnerabilidades, divulgación transparente, auditorías independientes y procesos SDLC seguros indican que un proveedor es fiable y resiliente. Solo Kaspersky y otros dos proveedores ofrecen todas las capacidades que se evaluaron:

Función	Proveedores
Informe de vulnerabilidades	14/14
Avisos de seguridad	7/14
Colaboración y Safe Harbor	7/14
Resultados de auditorías de seguridad	7/14
Prácticas SDLC	14/14

El estudio ha demostrado que varios proveedores se están preparando para implementar la Cyber Resilience Act (CRA), además de los marcos regulatorios más comunes. Tras aportar sus comentarios durante la fase de consulta pública del proceso legislativo, Kaspersky sigue de cerca la implementación gradual de la CRA con el fin de cumplir los requisitos regulatorios en cuanto entren en vigor

Transparencia y políticas corporativas

La divulgación pública de incidentes y requerimientos de autoridades da cuenta de la transparencia del proveedor. Aunque la mayoría se compromete en sus contratos a divulgar incidentes, solo 7 de los proveedores evaluados documentan divulgaciones detalladas. A su vez, solo 3, incluido Kaspersky, publican informes de transparencia con detalles sobre solicitudes de autoridades y fuerzas de seguridad:

Función	Proveedores
Compromiso contractual de divulgación y respuesta ante incidentes	13/14
Documentación detallada y reporte de incidentes	7/14
Notificación a los clientes afectados sobre solicitudes legales	9/14
Informes de transparencia publicados	3/14 públicos, 1 a solicitud

Cumplimiento normativo y certificaciones

El cumplimiento con normas internacionales, marcos regulatorios y principios de gobernanza legal es un requisito indispensable para la transparencia y la confianza en un proveedor. El estudio determinó que todos los proveedores cumplen con el RGPD y mantienen las certificaciones ISO/IEC 27001 y SOC 2 Tipo II. Asimismo, 12 de los 14, incluido Kaspersky, cumplen con la normativa CCPA. 11 de los proveedores ofrecen múltiples jurisdicciones para la resolución de disputas y, si bien el contrato general de Kaspersky no incluye esta opción por defecto, sí contempla disposiciones que permiten a los clientes reemplazar el acuerdo general por contratos individuales que cubran esta necesidad.

Telemetría y almacenamiento de datos

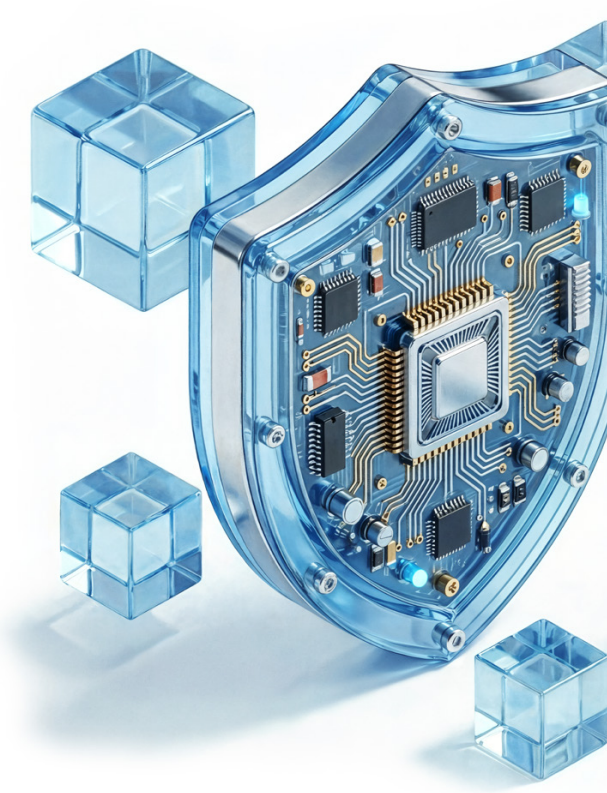
La forma en la que los proveedores gestionan los entornos de despliegue, la recopilación de telemetría y el almacenamiento de datos es fundamental tanto para la transparencia como para el cumplimiento normativo. Las opciones de despliegue flexibles y un tratamiento transparente de los datos refuerzan la credibilidad del proveedor. Aunque el funcionamiento sin conexión es habitual, solo la mitad de los proveedores ofrece alternativas al servicio de reputación en la nube, y únicamente cuatro mantienen instalaciones de datos en todas las regiones analizadas. Kaspersky ofrece ambas cosas:

4 proveedores mantienen instalaciones de datos en todas las regiones

Función	Proveedores
Soporte sin conexión / en entornos aislados (air-gapped)	14/14
Servicio de reputación on-premise	8/14
Anonimización y eliminación periódica de datos	14/14
Centros de datos en la UE	14/14
Centros de datos en Norteamérica	14/14
Centros de datos en Oriente Medio	4/14

Análisis de transmisión de datos

Los productos empresariales evaluados están diseñados para recopilar y transmitir datos como parte de su funcionamiento normal, con el fin de ofrecer protección frente a amenazas. Cada elemento de datos puede ser telemetría de seguridad esencial, pero también podría considerarse información sensible que se envía a un centro de datos de un tercero. Las organizaciones deben alinear la recopilación de datos con su perfil de riesgo y sus prioridades, utilizando las opciones de control disponibles.



Kaspersky recopiló la mínima cantidad de datos durante las pruebas

Los investigadores observaron que el producto transmitía los indicadores más comunes (nombre de host, nombre de usuario de Windows, IP interna) en un nivel comparable al del resto de competidores, evitando enviar datos sensibles como los registros de errores.
Kaspersky también permite desactivar por completo Kaspersky Security Network (envío de reputación de archivos) y la funcionalidad EDR.

kaspersky

Proven.
Transparent.
Independent.

Acciones recomendadas para los CISO

1. Código fuente y componentes del producto

- ☐ Solicitar una SBOM detallada durante el proceso de adquisición y para la futura gestión continua de riesgos
- ☐ Verificar los procesos del proveedor para supervisar y mitigar vulnerabilidades en la cadena de suministro
- ☐ Solicitar acceso a un centro de transparencia para revisar el código fuente y verificar las compilaciones

2. Actualizaciones del producto y gestión de cambios

- ☐ Exigir acceso a historiales de cambios completos y notas de versión
- ☐ Confirmar la existencia de programas de despliegue escalonado y pruebas beta para validación previa

3. Almacenamiento de datos, privacidad y telemetría

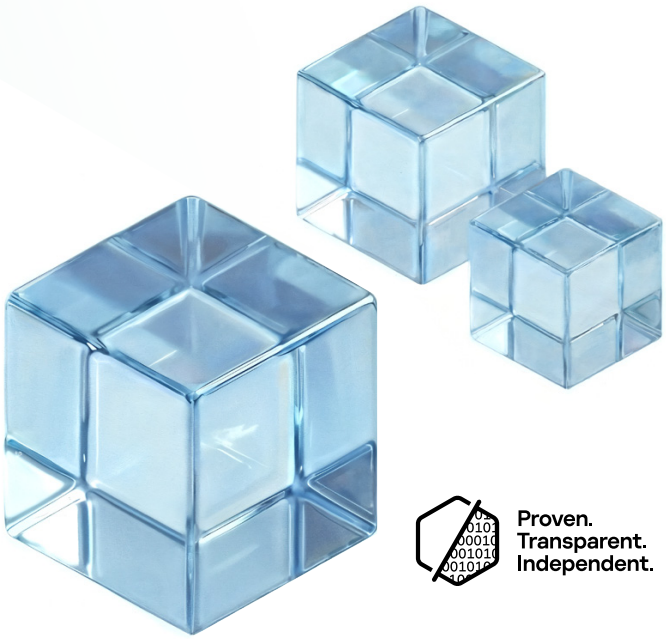
- ☐ Exigir configuraciones de privacidad claras y personalizables para la telemetría, la carga de archivos y la recopilación de datos
- ☐ Solicitar plazos explícitos de retención, procedimientos de eliminación y ubicación de los centros de datos
- ☐ Verificar la compatibilidad y soporte con despliegues sin conexión o en entornos aislados

4. Postura de seguridad, respuesta a incidentes y políticas

- ☐ Exigir divulgación transparente de vulnerabilidades y avisos de seguridad públicos
- ☐ Solicitar resultados de auditorías de terceros y documentación del SDLC
- ☐ Garantizar que las obligaciones contractuales incluyan la notificación rápida de brechas y análisis de causa raíz, alcance y mitigación
- ☐ Revisar el historial del proveedor para analizar divulgaciones públicas de incidentes y claridad de las respuestas
- ☐ Solicitar informes de transparencia regulares y políticas sobre solicitud de información por parte de autoridades

5. Cumplimiento y certificación

- ☐ Verificar el alcance de las certificaciones (ISO/IEC 27001, SOC 2) mediante documentación oficial, no solo logotipos o declaraciones
- ☐ Asegurarse de que las certificaciones cubran explícitamente centros de datos, sistemas de compilación y servicios en la nube



kaspersky

Proven.
Transparent.
Independent.

Continúa aprendiendo acerca de la transparencia

Lee el informe completo

Conoce más sobre Kaspersky Next EDR Optimum

Coordina una visita a un Centro de Transparencia

Consulta el informe de transparencia de Kaspersky

Descubre todo el porfolio empresarial de Kaspersky

kaspersky

Proven.
Transparent.
Independent.