Evaluación del impacto de las transferencias de Elastic

EE. UU.

Los clientes son responsables de realizar su propia evaluación independiente de la información en este documento. Este documento: (a) tiene fines meramente informativos, (b) representa las ofertas de productos, servicios y prácticas actuales de Elastic, que están sujetas a cambios sin previo aviso, y (c) no crea ningún compromiso ni garantía por parte de Elastic y sus afiliadas, proveedores o licenciantes. Las responsabilidades y obligaciones de Elastic frente a sus clientes se rigen por los acuerdos de Elastic, y este documento no forma parte ni modifica ningún acuerdo entre Elastic y sus clientes.

Última revisión: octubre de 2025

Introducción al marco de trabajo de evaluación y transferencias de datos de Elastic

Las ofertas de Elastic

Elastic proporciona un conjunto de productos de Elasticsearch, Observability y Security y características asociadas, que están diseñados para brindar a los clientes información en tiempo real y robustas capacidades de gestión de datos.

Elastic puede tratar datos personales por cuenta de nuestros clientes en calidad de encargado del tratamiento ("Datos personales del cliente") cuando los clientes implementan productos y funciones de Elastic en Elastic Cloud, o cuando utilizan los Servicios de soporte o los Servicios de consultoría de Elastic (las "Ofertas de Elastic"), cada uno con alcances específicos de tratamiento de datos personales.

Elastic Cloud ofrece una plataforma alojada para que los clientes puedan implementar las soluciones de búsqueda, observabilidad y seguridad de Elastic en Amazon Web Services, Microsoft Azure y Google Cloud. Puedes elegir tu región de alojamiento de datos preferida entre muchas opciones globales, incluidas numerosas ubicaciones dentro del Espacio Económico Europeo (EEE). De forma predeterminada, los backups se almacenan en la misma región que tu despliegue. Si bien controlas la residencia de tus datos, el personal y los subprocesadores de Elastic pueden requerir acceso limitado a datos desde fuera del EEE para servicios esenciales como la gestión de la plataforma, las operaciones técnicas y la atención al cliente.

Los servicios de soporte ofrecen asistencia integral a los usuarios de productos Elastic, que abarcan desde la ingesta inicial de datos hasta el escalado de los despliegues y la obtención de información valiosa. En el contexto de los datos personales de los clientes, las actividades de procesamiento de Elastic durante los compromisos de soporte están altamente restringidas. Los agentes de soporte interactúan principalmente con la capa administrativa de Elastic Cloud, lo que minimiza el acceso directo al contenido de los datos de los clientes almacenados en los índices. En caso de que un problema excepcional requiera el acceso directo al contenido del cliente o a los índices de datos del cliente, lo cual podría incluir datos personales implicados (por ejemplo, para analizar un volcado de memoria), la aprobación del cliente es un requisito previo. Estos procesos están sujetos a controles estrictos, auditabilidad y adherencia a estándares de cumplimiento reconocidos.

Los Servicios de consultoría ofrecen orientación basada en resultados para ayudar a las organizaciones a optimizar el uso de Elastic Stack, agilizar los plazos de los proyectos y alcanzar objetivos empresariales específicos. Estos servicios se proporcionan globalmente con opciones de entrega flexibles y virtuales. De manera similar al soporte, la prestación de servicios de consultoría puede implicar el procesamiento de los datos personales del cliente según sea necesario para ayudar en la prestación del servicio de consultoría acordado.

© 2025 Elasticsearch B.V. Todos los derechos reservados.

Procesamiento de datos personales de Elastic

Al proporcionar servicios a sus clientes, Elastic actúa como encargado del tratamiento de los datos. La naturaleza definitiva y las categorías de los Datos personales del cliente procesados se determinan y controlan por los clientes de Elastic a su entera discreción. Elastic no supervisa de forma activa los datos específicos que los clientes ingestan en sus servicios.

La siguiente tabla resume el procesamiento de los datos personales del cliente para cada una de las ofertas de Elastic:

Oferta de Elastic	***Propósito del procesamiento primario***	***Naturaleza de los datos personales tratados***	***Categorías de interesados***	***Control de ubicación de alojamiento / procesamiento***
Elastic Cloud	Información en tiempo real, búsqueda, observabilidad, analítica de seguridad, gestión de plataformas, operaciones técnicas	Datos personales del cliente (contenido determinado por el cliente, no supervisado por Elastic), datos operativos limitados (por ejemplo, registros de uso, identificadores en línea, comunicaciones electrónicas, datos de actividad de red) para la gestión de la plataforma.	Administradores de clientes, usuarios finales, personal de los clientes/socios del cliente	El cliente selecciona su región preferida para el alojamiento de datos (hay opciones disponibles en el EEE), los backups se realizan en la misma región. Determinadas actividades de procesamiento (gestión de la plataforma, operaciones técnicas, soporte) pueden implicar un acceso limitado desde fuera del EEE.
Servicios de soporte	Asistencia integral, resolución de problemas y orientación técnica	Acceso a los datos personales del cliente muy limitado (principalmente interacción a nivel de la capa administrativa). Acceso directo al contenido del cliente (por ejemplo, volcado de memoria) solo con la aprobación del cliente.	Administradores de clientes, usuarios finales	Esto puede implicar que Elastic y los subprocesadores accedan a la información desde lugares fuera del EEE.
Servicios de consultoría	Consultoría basada en resultados, optimización de proyectos, resultados empresariales con Elastic Stack	Datos personales del cliente, en la medida en que sean necesarios para facilitar la prestación del servicio.	Administradores del cliente, usuarios finales	Esto puede implicar que Elastic y los subprocesadores accedan a la información desde lugares fuera del EEE.

Base legal para transferencias internacionales: Cláusulas contractuales estándar (SCC) y Marcos de privacidad de datos

El marco de trabajo de Elastic para las transferencias internacionales de datos se basa firmemente en el uso de cláusulas contractuales estándar (SCC). Este mecanismo se utiliza tanto para transferencias directas, en las que los datos fluyen del cliente a Elastic, como para transferencias posteriores, de Elastic a sus subprocesadores internos y subprocesadores externos, con el fin de alinearse directamente con los requisitos establecidos por el Tribunal de Justicia de la Unión Europea (TJUE) en su sentencia “Schrems II”. La decisión “Schrems II”, emitida el 16 de julio de 2020, invalidó el Escudo de Privacidad UE-EE. UU., pero al mismo tiempo reafirmó la validez de las Cláusulas contractuales estándar (SCC) como una herramienta legítima para la transferencia de datos personales desde el Espacio Económico Europeo (EEE) a terceros países. Sin embargo, la sentencia del TJUE también estableció que los importadores y exportadores de datos deben realizar una evaluación detallada, caso por caso, de la transferencia e implementar salvaguardas adicionales cuando sea necesario, para garantizar que los datos personales mantengan un nivel de protección “esencialmente equivalente” al garantizado dentro del EEE.

 © 2025 Elasticsearch B.V. Todos los derechos reservados.

Además, Elasticsearch, Inc. cumple con el Marco de privacidad de datos UE-EE. UU., la extensión del Reino Unido al Marco de privacidad de datos UE-EE. UU. y el Marco de privacidad de datos Suiza-EE. UU. (conjuntamente, el "Marco de privacidad de datos"), según lo establecido por el Departamento de Comercio de los Estados Unidos. Elastic ha certificado ante el Departamento de Comercio que cumple con los principios del Marco de privacidad de datos en relación con el procesamiento de datos personales recibidos de la Unión Europea, el Reino Unido y Suiza, según corresponda, en virtud del Marco de privacidad de datos.

Esta evaluación ofrece una revisión exhaustiva de los aspectos legales y prácticos relacionados con las transferencias de datos al país correspondiente que se enumeran a continuación. Analizamos la legislación de acceso gubernamental relevante, evaluamos la efectividad de las SCC y detallamos las medidas específicas de Elastic para mitigar los riesgos.

Evaluación de impacto de transferencias en EE. UU.

Esta sección ofrece una evaluación detallada del panorama legal y práctico de las transferencias de datos a Estados Unidos de América (EE. UU.), y analiza la legislación aplicable sobre acceso gubernamental, la eficacia de las SCC y las medidas específicas de mitigación implementadas por Elastic.

Legislación aplicable sobre acceso gubernamental y alcance de la vigilancia

El marco legal de Estados Unidos incluye varias leyes y órdenes ejecutivas que pueden permitir a las autoridades gubernamentales acceder a datos personales con fines de seguridad nacional, inteligencia y aplicación de la ley.

- **Ley de Vigilancia de Inteligencia Extranjera (FISA), Sección 702:** esta ley permite al gobierno de EE. UU. dirigir a los "proveedores de servicios de comunicaciones electrónicas" (ECSP) a cooperar en las actividades de recopilación de inteligencia. Si bien el término ECSP ha sido ampliamente interpretado por los tribunales estadounidenses y el Departamento de Comercio para incluir potencialmente a empresas como Elastic, es muy poco probable que las agencias de inteligencia estadounidenses apunten a la información comercial ordinaria que Elastic procesa para los clientes. Además, Elastic no está sujeta a órdenes de vigilancia "aguas arriba", que se dirigen a proveedores de infraestructura central de internet y que fueron una de las principales preocupaciones en la decisión Schrems II. Hasta la fecha, Elastic no había recibido ninguna solicitud del gobierno de EE. UU. en virtud del artículo 702 de la FISA.
- **Orden Ejecutiva 12333 (EO 12333) y Directiva de Política Presidencial 28 (PPD 28):** a diferencia de la FISA 702, la EO 12333 no otorga al gobierno de Estados Unidos la facultad de obligar a empresas o personas a revelar datos. Las actividades de vigilancia de conformidad con la EO 12333 están sujetas a las restricciones descritas en PPD 28, que están diseñadas para proteger la privacidad y las libertades civiles. Estas restricciones incluyen limitar la recolección masiva a fines específicos de seguridad nacional y minimizar la difusión y retención de la información personal recopilada. Estas restricciones

© 2025 Elasticsearch B.V. Todos los derechos reservados.

son medidas de protección adicionales que reducen la probabilidad de que se produzcan búsquedas o incautaciones indiscriminadas o ilegales de datos personales. Hasta la fecha, Elastic no recibió ninguna solicitud del gobierno de EE. UU. de conformidad con la EO 12333.

- **Ley CLOUD ("Ley de Clarificación del Uso Legal de Datos en el Extranjero") de EE. UU.:** promulgada en marzo de 2018, la Ley CLOUD aborda los conflictos relacionados con datos almacenados fuera de Estados Unidos, al exigir una orden judicial para obligar a la divulgación de dichos datos en virtud de la Ley de Comunicaciones Almacenadas (SCA) de EE. UU. La SCA incluye medidas de protección para la privacidad que son preservadas por la Ley CLOUD. La Ley también proporciona un mecanismo para que los proveedores de servicios impugnen las solicitudes que entran en conflicto con las obligaciones de privacidad extranjeras. Elastic no prevé que la Ley CLOUD tenga un impacto práctico en su gestión de los datos personales de los clientes.
- **Nueva Orden Ejecutiva 14086 sobre el mejoramiento de las medidas de protección para las actividades de inteligencia de señales de Estados Unidos (7 de octubre de 2022):** esta Orden Ejecutiva (NEO) introduce medidas de protección vinculantes que limitan el acceso a datos (incluidos los datos de personas no estadounidenses) por parte de las autoridades de inteligencia de EE. UU. a lo que sea "necesario y proporcional" para la seguridad nacional. Exige una supervisión rigurosa, prioriza la recopilación dirigida y minimiza la difusión y la retención. De manera crucial, la NEO establece un mecanismo de reparación independiente e imparcial, que incluye un nuevo Tribunal de Revisión de Protección de Datos, para investigar y resolver quejas relacionadas con el acceso a datos por parte de las autoridades de seguridad nacional de EE. UU. Se considera que este desarrollo ha "incrementado significativamente" el nivel de protección de los datos de ciudadanos de la UE en EE. UU.
- **Comisión Federal de Comercio (FTC) de EE. UU.:** la FTC desempeña un papel en la aplicación de los principios de práctica de información justa (FIPP) y emprendió activamente acciones legales contra empresas por violaciones de la privacidad, e impuso multas sustanciales.
- **Constitución de los Estados Unidos (Cuarta Enmienda) y Ley de Privacidad de Comunicaciones Electrónicas (ECPA):** estos instrumentos legales restringen la capacidad del gobierno de los Estados Unidos para obligar a los proveedores de servicios a divulgar información del usuario final. Por lo general, requieren citaciones para datos básicos de registro de usuarios y direcciones IP, y órdenes judiciales u órdenes de búsqueda para registros sin contenido y contenido de comunicación, respectivamente.

Evaluación de la eficacia de la herramienta de transferencia y desafíos legales

La eficacia de las SCC para transferencias de datos a EE. UU. fue un punto central de controversia tras la decisión Schrems II, que puso de manifiesto preocupaciones sobre el alcance de las leyes de vigilancia estadounidenses. Históricamente, un desafío principal fue el alcance amplio percibido de FISA 702 y EO 12333, que llevó al CJEU a invalidar el Privacy Shield. Aunque los servicios de Elastic son objetivos poco probables, el *potencial* para una interpretación amplia de estas leyes presentó un desafío legal a la efectividad de las SCC, lo que requirió medidas complementarias robustas.

 © 2025 Elasticsearch B.V. Todos los derechos reservados.

Sin embargo, el panorama cambió fundamentalmente con la adopción del Marco de privacidad de datos (DPF) UE-EE. UU. y la subyacente nueva orden ejecutiva (NEO). La NEO introduce garantías vinculantes que limitan el acceso a los datos a lo necesario y proporcionado, exige una supervisión rigurosa y establece un mecanismo independiente de reparación, incluido un Tribunal de Revisión de Protección de Datos. Estos desarrollos abordan directamente las principales deficiencias identificadas en Schrems II, lo que lleva a la Comisión de la UE a otorgar una decisión de adecuación a los Estados Unidos. Esto significa que ahora se considera formalmente que Estados Unidos proporciona un nivel de protección "esencialmente equivalente", como la Comisión Europea reconfirmó en su último reporte periódico sobre el funcionamiento del DPF (COM(2024)451 final, de 8 de octubre de 2024). Este desarrollo reduce significativamente la carga de demostrar medidas complementarias efectivas para transferencias a EE. UU., ya que la certificación DPF de Elastic es un fuerte indicador de cumplimiento.

Dada la naturaleza y la finalidad de los servicios de Elastic, es muy poco probable que la información personal de los clientes que procesa Elastic sea objeto de una solicitud en virtud de la Sección 702 de la FISA, la Orden Ejecutiva 12333 o la Ley CLOUD. No tenemos conocimiento de ningún acceso directo a los datos personales del cliente conforme a la Orden Ejecutiva 12333. No creamos ni mantenemos puertas traseras ni llaves maestras de nuestros productos o servicios, y no permitimos que ninguna autoridad gubernamental tenga acceso irrestricto o directo a nuestros servidores.

Medidas específicas de Elastic para proteger y mitigar los riesgos relacionados con la protección de datos

El compromiso de Elastic con la privacidad y la seguridad de los datos se sustenta en un conjunto completo y escalonado de medidas de protección técnicas, organizativas y contractuales. Estas medidas están diseñadas para proteger los datos personales a lo largo de todo su ciclo de vida dentro de las ofertas de Elastic y para garantizar el cumplimiento de los principios de las SCC, en conformidad con el GDPR, el GDPR del Reino Unido y la Ley Federal de Protección de Datos de Suiza (FDPA).

Salvaguardas técnicas:

- **Residencia de datos:** Elastic Cloud ofrece a los clientes la flexibilidad de seleccionar su región de alojamiento de datos preferida entre una amplia gama de opciones globales en AWS, GCP y Azure, incluidas numerosas ubicaciones dentro del EEE. Esto permite a los clientes cumplir con requisitos específicos de residencia de datos, ya que los backups se almacenan automáticamente en la región elegida.
- **Cifrado en transferencia y en reposo:** los datos del cliente se cifran tanto en tránsito, utilizando TLS 1.2, como en reposo, empleando un mínimo de cifrados AES-256. Elastic también mantiene procedimientos sólidos de gestión de claves de cifrado.
- **Actualizaciones y parches regulares del sistema:** para minimizar los riesgos de vulnerabilidad, las instancias de Elasticsearch se despliegan en función de los núcleos del sistema operativo más recientes, con la aplicación continua de parches para abordar vulnerabilidades y exposiciones comunes (CVE).
- **Uso de proveedores de servicios líderes en la industria:** los servicios de Elastic están alojados en centros de datos gestionados por los principales proveedores de servicios en el cloud, reconocidos por sus medidas de seguridad técnicas y organizacionales de vanguardia, diseñados para proteger los datos alojados.

- **Controles de acceso:** Elastic aplica controles lógicos y administrativos estrictos para limitar el acceso a los datos exclusivamente a los usuarios autorizados. Esto incluye autenticación multifactor, estándares de contraseña sólidos y el uso de VPN para el acceso administrativo. El principio de privilegio mínimo se cumple estrictamente, lo que garantiza que los empleados solo tengan el acceso necesario para sus funciones, con revisiones regulares de los derechos de acceso. El logging centralizado, que incluye los logs de proxy, de acceso, de Elasticsearch y de Auditbeat, registra minuciosamente todos los accesos a los datos de los clientes y a los sistemas donde se almacenan. Para los servicios de soporte, el acceso a los Datos personales del cliente es muy limitado, y los agentes interactúan principalmente con la capa administrativa y requieren autorización del cliente para acceder al contenido.
- **Detección y respuesta de incidentes:** Elastic mantiene y actualiza continuamente reglas sofisticadas de detección para actividades sospechosas y accesos no autorizados, incluyendo el monitoreo de integridad de archivos e indicadores de apropiación de cuenta. Estas detecciones se integran en flujos de trabajo automatizados que alertan al equipo de detección y respuesta a amenazas, desencadenando investigaciones inmediatas.

Medidas de seguridad de la organización:

- **Sistema de Gestión de Seguridad de la Información (ISMS):** Elastic adoptó formalmente un ISMS certificado de conformidad con las normas ISO 27001, ISO 27017 e ISO 27018. Este sistema constituye la base de todas las políticas, normas y directrices de seguridad de la información, y garantiza medidas técnicas y organizativas integrales para la protección de datos.
- **Marco de privacidad de datos (DPF):** Elastic cuenta con la certificación de conformidad con el Marco de privacidad de datos para los datos personales que se reciben de la Unión Europea, el Reino Unido y Suiza.
- **Privacidad y seguridad por diseño:** estos principios están integrados en cada producto Elastic desde su concepción hasta su despliegue, lo que garantiza que la protección de datos sea un aspecto fundamental del desarrollo del producto.
- **Principios para las solicitudes de información de las autoridades públicas:** Elastic estableció principios y procedimientos claros para gestionar las solicitudes de información de clientes por parte de las autoridades públicas. Estos protocolos incluyen impugnar solicitudes, notificar a las partes relevantes y solicitar exenciones de las prohibiciones de notificación. Elastic nunca creó puertas traseras ni claves maestras para sus productos y nunca permitió que ninguna autoridad gubernamental tenga acceso irrestricto o directo a sus servidores.
- **Gestión de la cadena de suministros:** Elastic lleva a cabo un proceso exhaustivo de debida diligencia interfuncional que involucra a los equipos de seguridad, privacidad y cumplimiento para todos los proveedores de servicios. Esto incluye revisar el tipo y el nivel de riesgo de los datos que se van a compartir, las políticas y medidas de seguridad del proveedor, las auditorías de terceros y realizar evaluaciones de impacto en la privacidad.
- **Otras políticas internas:** Elastic mantiene políticas internas que regulan el uso y acceso a datos personales, la gestión de brechas de datos, las solicitudes de acceso de los interesados, la retención de datos y el control de acceso.
- **Marcos de cumplimiento:** Elastic Cloud demuestra el cumplimiento con una amplia gama de marcos de la industria, incluidos SOC 2 Tipo II, CSA CCM 4.0, PCI-DSS, HIPAA, Cyber Essentials+, la Directiva NIS2 para proveedores de servicios en el cloud, TISAX y FedRAMP Moderado.
- **Pruebas periódicas:** se realizan pruebas periódicas de vulnerabilidades y de penetración en la red y las aplicaciones, con procedimientos establecidos para documentar y abordar cualquier vulnerabilidad detectada.

© 2025 Elasticsearch B.V. Todos los derechos reservados.

- **Capacitación de empleados:** todos los empleados deben completar la capacitación en seguridad de la información, protección de datos y privacidad al momento de su contratación y, posteriormente, de forma anual.

Salvaguardias contractuales:

- **Anexo de procesamiento de datos (DPA):** Elastic se compromete contractualmente a aplicar sólidas medidas de protección de datos y privacidad en virtud de nuestro Anexo de protección de datos, que incluye las SCC y sus variantes para Suiza y el Reino Unido, así como nuestro Anexo de seguridad de la información. Revisamos y actualizamos regularmente nuestro Anexo de procesamiento de datos para que refleje los requisitos de privacidad de datos aplicables y las mejores prácticas.
- **Instrucciones para el cliente:** el procesamiento de los datos personales del cliente se realiza estrictamente solo siguiendo las instrucciones del cliente.
- **Confidencialidad:** todo el personal autorizado para procesar los Datos Personales del Cliente está sujeto a estrictos acuerdos, políticas y procedimientos de confidencialidad.
- **Control:** los clientes mantienen la capacidad de recuperar, corregir o eliminar cualquier dato personal que suban a Elastic Cloud en cualquier momento.
- **Notificación de solicitudes de divulgación:** Elastic se compromete contractualmente a notificar a los clientes en caso de recibir una solicitud de divulgación de sus datos, salvo que la ley prohíba hacerlo.
- **Obligaciones de los subprocesadores:** somos totalmente transparentes respecto a nuestros subprocesadores, que también están sujetos a los mismos estrictos estándares y requisitos organizacionales. Somos responsables de los actos y las omisiones de nuestros subprocesadores en la misma medida que si prestáramos los servicios nosotros mismos.

© 2025 Elasticsearch B.V. Todos los derechos reservados.