

# Una guía para cumplir los requisitos de privacidad de datos con Akamai Identity Cloud



## ¿Cómo le puede ayudar Akamai Identity Cloud a cumplir las normativas?

En todo el mundo, se promulgan continuamente leyes y normativas relacionadas con la información personal (PI, por sus siglas en inglés) debido a la persistencia de filtraciones y uso indebido de datos. Conocer las variaciones entre las numerosas leyes de privacidad y protección de datos diferentes puede resultar difícil para las organizaciones, desde el Reglamento General de Protección de Datos (RGPD) de la Unión Europea hasta la Ley de Privacidad del Consumidor de California (CCPA) de Estados Unidos, la Ley de Privacidad de Australia (APA), la Ley sobre Protección de Datos Personales (APPI) de Japón y la Ley de Protección de Datos Personales y Documentos Electrónicos (PIPEDA) de Canadá, cada normativa tiene sus propios matices.

Nuestros clientes a menudo preguntan sobre secciones específicas de leyes de privacidad y sobre las formas en que Akamai ayuda al cumplimiento. Para ayudarle a proteger la privacidad de sus datos, hemos recopilado una lista de requisitos generales que se pueden encontrar en muchas normativas de privacidad y protección de datos de todo el mundo. Describimos cada obligación brevemente y, a continuación, explicamos cómo nuestra solución de gestión de acceso e identidades de clientes (CIAM), [Akamai Identity Cloud](#), puede ayudar a atenderlas.

CIAM es un enfoque sistemático que se combina con soluciones de software específicas que han sido críticas para ayudar a las marcas a recopilar y gestionar datos personales de los clientes de forma que se garantice la seguridad y el cumplimiento de las medidas normativas. CIAM permite a las organizaciones utilizar los datos de los clientes dentro de sus sistemas de gestión de contenidos y automatización de marketing para que las marcas puedan seguir creando experiencias de cliente altamente personalizadas, satisfaciendo al mismo tiempo los requisitos normativos y el creciente deseo de los clientes de privacidad de los datos.

A continuación, se presenta una guía de uso de Akamai Identity Cloud para ayudar al cumplimiento de 11 obligaciones comunes de protección de datos de distintas leyes y normativas de privacidad de todo el mundo.

Una guía para cumplir los requisitos de privacidad de datos con Akamai Identity Cloud

# Tabla de contenido

- Obtención y gestión del consentimiento ..... 2
- Derecho de oposición ..... 3
- Consentimiento parental para menores ..... 4
- Derecho de acceso del interesado ..... 5
- Derecho de rectificación ..... 6
- Derecho de supresión o eliminación de los datos personales ("derecho al olvido") ..... 7
- Portabilidad de los datos ..... 8
- Gestión de riesgos de proveedores ..... 9
- Notificación de filtraciones ..... 10
- Responsabilidad de la organización ..... 11
- Residencia y transferencia de datos ..... 12
- Conclusión ..... 13
- Arquitectura de referencia de Global Compliance ..... 14

## Obtención y gestión del consentimiento

En determinadas actividades que llevan a cabo las organizaciones, el uso de datos subyacente se basa en el consentimiento previo de la persona. Los requisitos para obtener el consentimiento válido y las circunstancias de su obligatoriedad para el uso de datos varían entre cada normativa. Gestionar el consentimiento y respetar la elección de la persona de conceder o retirar el consentimiento son esenciales de acuerdo con las leyes de protección de datos mundiales, aunque su implementación puede ser difícil.

### Cómo puede ayudar Identity Cloud

**Identity Cloud** permite a las organizaciones obtener el consentimiento y ofrece un portal de autoservicio con un centro de preferencias para que los usuarios vean, modifiquen y revoken su consentimiento.

Las experiencias y los formularios de los usuarios se pueden personalizar para las situaciones de aceptación y oposición, y el consentimiento se puede solicitar en el momento del registro de la cuenta, después de iniciar sesión o en cualquier etapa de la trayectoria del cliente. También puede otorgar a los usuarios la capacidad de gestionar su consentimiento mediante autoservicio en cualquier momento.

Los consentimientos y las preferencias se almacenan de modo que se puedan auditar junto con los datos de usuario como parte del registro de datos del cliente. Todos los datos de usuario se cifran en movimiento y en reposo. Los registros de acceso sirven de prueba de las acciones realizadas por un usuario por cuestiones de transparencia y responsabilidad.

OBLIGACIÓN	Obtención y gestión del consentimiento
RGPD DE LA UE	Artículos 4 (11) y 7 (3)
CCPA DE CALIFORNIA	Sección 1798.120
PIPEDA DE CANADÁ	Anexo 1, cláusula 4.3
LFPDPPP DE MÉXICO	Artículos 8 y 9 de la ley
APA DE AUSTRALIA	Directrices de la APP, capítulo B.34
APPI DE JAPÓN	Artículo 16
PDPA DE SINGAPUR	Artículos 13 y 16
LGPD DE BRASIL	Artículo 7 (1) y artículo 8
LPDP DE ARGENTINA	Sección 5
PROYECTO DE LEY PDP DE INDIA DE 2019	Cláusula 11

## Derecho de oposición

El derecho de oposición autoriza a una persona a denegar el uso de datos personales para determinados tipos de procesamiento de datos, como marketing directo o análisis estadísticos.

## Cómo puede ayudar Identity Cloud

Identity Cloud ofrece un centro de preferencias personalizable que permite a los usuarios seleccionar o anular la selección de los tipos de procesamiento de datos que aprueban.

La interfaz de usuario y el diseño se integran con la experiencia de registro e inicio de sesión, en la que los usuarios pueden seleccionar los tipos de procesamiento de datos que aceptan, así como realizar otras acciones en su perfil. Las preferencias se almacenan junto con los datos de usuario como parte del registro del cliente y los datos se cifran en movimiento y en reposo. Los ajustes de preferencias también se pueden actualizar a través de una API desde cualquier página alojada por el cliente.

OBLIGACIÓN	Derecho de oposición a cualquier actividad de procesamiento
RGPD DE LA UE	Artículo 21
CCPA DE CALIFORNIA	Sección 1798.120
PIPEDA DE CANADÁ	Anexo 1, cláusula 4.3.8
LFPDPPP DE MÉXICO	Artículo 22 y artículo 27 ff
APA DE AUSTRALIA	No se cubre explícitamente
APPI DE JAPÓN	Artículo 30 de APII
PDPA DE SINGAPUR	No se cubre explícitamente
LGPD DE BRASIL	Artículo 18 VIII
LPDP DE ARGENTINA	Artículo 16 y artículo 30
PROYECTO DE LEY PDP DE INDIA DE 2019	Cláusulas 7 (d) y 11 (e)

## Consentimiento parental para menores

Para que el consentimiento sea válido, la persona debe tener una edad determinada. En el caso de que la persona no alcance la edad correspondiente, un tutor legal puede otorgar el consentimiento válido en su nombre. Tenga en cuenta que la edad mínima para que el consentimiento sea válido varía en cada país.

## Cómo puede ayudar Identity Cloud

Identity Cloud incluye una función de clasificación por edades para proteger contra la aceptación de datos personales de menores que no pueden otorgar un consentimiento válido de acuerdo con las leyes aplicables debido a su edad.

OBLIGACIÓN	Consentimiento parental para menores
RGPD DE LA UE	Artículo 8
CCPA DE CALIFORNIA	Sección 1798.120 (c)
PIPEDA DE CANADÁ	Anexo 1, cláusula 4.3
LFPDPPP DE MÉXICO	Artículo 89 III de la normativa y páginas 11 y 12 de la guía
APA DE AUSTRALIA	Directrices de la APP, capítulos B.47, 52 y 53
APPI DE JAPÓN	No se cubre explícitamente
PDPA DE SINGAPUR	Directrices de asesoramiento sobre temas seleccionados por la PDPA, revisadas el 31 de agosto de 2018
LGPD DE BRASIL	Artículo 14 § 1
LDPD DE ARGENTINA	Artículo 18
PROYECTO DE LEY PDP DE INDIA DE 2019	Cláusula 16 (2)

## Derecho de acceso del interesado

Permite a las personas acceder a los datos personales que se están procesando, lo que en algunos casos incluye el derecho a reclamar información adicional sobre los usos y divulgaciones de dichos datos.

## Cómo puede ayudar Identity Cloud

**Identity Cloud** ofrece un centro de preferencias personalizable, que permite a los usuarios acceder a sus datos en cualquier momento y lugar. El portal de autoservicio permite a los usuarios controlar las preferencias de datos comprobando fácilmente el alcance y la precisión de la información proporcionada sin necesidad de servicios de atención al cliente.

OBLIGACIÓN	Derecho de acceso del interesado
RGPD DE LA UE	Artículos 15 y 20
CCPA DE CALIFORNIA	Sección 1798.100
PIPEDA DE CANADÁ	Anexo 1, cláusula 4.9
LFPDPPP DE MÉXICO	Artículos 22-23 y 29-35 de la ley y artículo 101 de la normativa
APA DE AUSTRALIA	APP 12 y capítulo 12 de las directrices de APP
APPI DE JAPÓN	Artículo 19
PDPA DE SINGAPUR	Artículo 21
LGPD DE BRASIL	Artículo 9 y artículo 18 (2)
LPDP DE ARGENTINA	Artículo 27
PROYECTO DE LEY PDP DE INDIA DE 2019	Cláusula 17 (3)

## Derecho de rectificación

Proporciona a las personas el derecho a corregir los datos personales procesados.

### Cómo puede ayudar Identity Cloud

**Identity Cloud** permite a los usuarios y representantes de servicio editar registros de datos en cualquier momento y lugar para garantizar que los elementos de datos estén actualizados y sean precisos. Las actividades de rectificación se registran y se pueden auditar, y pueden servir como prueba del control de los datos por parte de los usuarios.

OBLIGACIÓN	Derecho de rectificación
RGPD DE LA UE	Artículos 5 (1) d y 16
CCPA DE CALIFORNIA	Sección 1789.100 (a)
PIPEDA DE CANADÁ	Anexo 1, cláusula 4.9.5
LFPDPPP DE MÉXICO	Artículos 11 (2), 22 y 24, 28-31 y 35 de la ley
APA DE AUSTRALIA	APP 13 y apartado 13 de las directrices de APP
APPI DE JAPÓN	Artículo 19
PDPA DE SINGAPUR	Artículo 22
LGPD DE BRASIL	Artículo 8 y artículo 18 (III)
LPDP DE ARGENTINA	Artículo 29
PROYECTO DE LEY PDP DE INDIA DE 2019	Cláusula 18

## Derecho de supresión o eliminación de los datos personales ("derecho al olvido")

Muchas leyes incluyen el derecho de las personas a que sus datos personales se borren y no se distribuyan más a terceros ni se sometan al procesamiento por parte de estos, lo que también se conoce como "derecho al olvido".

### Cómo puede ayudar Identity Cloud

Identity Cloud permite una eliminación segura (no restaurable) de los registros de datos, incluida la eliminación de copias de seguridad, para ayudar a evitar la distribución accidental de los datos. Los usuarios o representantes de servicio pueden ejercer fácilmente el derecho al olvido en cualquier momento y lugar.

OBLIGACIÓN	Derecho de supresión ("derecho al olvido")
RGPD DE LA UE	Artículo 17
CCPA DE CALIFORNIA	Sección 1798.105 Exenciones: 1798.145 (g)(3)
PIPEDA DE CANADÁ	Anexo 1, cláusula 4.9.5
LFPDPPP DE MÉXICO	Artículos 11 (3), 22, 28-32 y 35 de la ley
APA DE AUSTRALIA	APP 4, capítulo 4.2 de las directrices de APP y APP 13 y capítulo 13 de las directrices de APP
APPI DE JAPÓN	Artículo 19 de APPI
PDPA DE SINGAPUR	Artículo 25
LGPD DE BRASIL	Artículo 18 (VI) de LGPD
LPDP DE ARGENTINA	Artículo 31
PROYECTO DE LEY PDP DE INDIA DE 2019	Cláusulas 18 y 20

## Portabilidad de los datos

Exige a las organizaciones que proporcionen a los consumidores copias de sus datos en un formato de uso común y legible por máquina, que les permita transferir sus datos a otra organización sin complicaciones.

## Cómo puede ayudar Identity Cloud

**Identity Cloud** ofrece un centro de preferencias personalizable, que permite a los usuarios solicitar la descarga de sus datos. Las organizaciones pueden responder fácilmente a una solicitud de portabilidad de los datos y descargar estos de Identity Cloud y cualquier otro sistema en el que se conserven datos de usuario. Es posible que Identity Cloud active un evento para iniciar el proceso de recopilación y entrega de los datos necesarios para satisfacer los requisitos normativos. Los datos de usuario de Identity Cloud se pueden proporcionar en formato JSON, un formato de archivo de estándar abierto legible por humanos y máquinas.

OBLIGACIÓN	Derecho a la portabilidad de los datos
RGPD DE LA UE	Artículo 20
CCPA DE CALIFORNIA	Sección 1798.100
PIPEDA DE CANADÁ	No se cubre explícitamente
LFPDPPP DE MÉXICO	No se cubre explícitamente
APA DE AUSTRALIA	Propuesta de Ley de Derechos de Datos de los Consumidores de 2019 (aplicable únicamente a consumidores)
APPI DE JAPÓN	No se cubre explícitamente
PDPA DE SINGAPUR	El derecho está en periodo de consulta
LGPD DE BRASIL	Artículos 11, 17, 18 y 40
LPDP DE ARGENTINA	Artículo 33
PROYECTO DE LEY PDP DE INDIA DE 2019	Cláusula 19

## Gestión de riesgos de proveedores

Las organizaciones deben garantizar la protección y seguridad de los datos, independientemente de que procesen internamente los datos personales o recurran a un proveedor de servicios de terceros para procesar los datos en su nombre. Por esta razón, la gestión de riesgos de proveedores es una parte fundamental del cumplimiento general.

### Cómo puede ayudar Identity Cloud

Akamai es un proveedor de servicios de confianza que garantiza la protección y seguridad de los datos que procesa en nombre de sus clientes mediante la implementación de medidas técnicas y organizativas. Las certificaciones y la declaración de cumplimiento que respaldan Akamai Identity Cloud son evidencia de la idoneidad de estas medidas, que sirven como mitigación eficaz de los riesgos.

**Identity Cloud** ofrece una sólida autenticación de usuarios y sofisticados mecanismos de protección contra amenazas basadas en la red, todo ello protegido detrás del firewall de aplicaciones web **Kona Site Defender** de Akamai. Además, permite a las organizaciones mantener controles de acceso en función de la necesidad de conocimiento. Identity Cloud, a fin de obtener los **certificados correspondientes**, se somete a auditoría y evaluación para asegurar que cumple los principales programas de garantía de seguridad, que incluyen:

- ISO 27001:2013
- ISO 27018:2014 (protección de PII en la nube)
- SOC 2 tipo 2 (los cinco principios del servicio de confianza: criterios comunes/seguridad, disponibilidad, confidencialidad, integridad de procesamiento y privacidad)
- Cumplimiento de la norma de seguridad HIPAA/HITECH (protección de la información sanitaria en reposo y en tránsito)
- Marco de Escudo de Privacidad UE-EE. UU.

OBLIGACIÓN	Gestión de riesgos de proveedores
RGPD DE LA UE	Artículo 32
CCPA DE CALIFORNIA	Sección 1798.81.5
PIPEDA DE CANADÁ	Anexo 1, cláusula 4.7
LFPDPPP DE MÉXICO	Artículo 19
APA DE AUSTRALIA	APP 11
APPI DE JAPÓN	Artículo 20
PDPA DE SINGAPUR	Artículo 24
LGPD DE BRASIL	Artículo 46 ff
LPDP DE ARGENTINA	Artículo 19
PROYECTO DE LEY PDP DE INDIA DE 2019	Cláusula 24

## Notificación de filtraciones

Las organizaciones deben informar de cualquier filtración de datos en un periodo determinado después de tener conocimiento de la situación. En general, la notificación incluye una descripción de la organización víctima de la filtración, los tipos de datos a los que se ha accedido, el número aproximado de personas afectadas, los daños previstos o reales a las personas y las medidas de mitigación. Los detalles de lo que se debe notificar, el periodo y el destinatario del informe difieren en cada país.

## Cómo puede ayudar Identity Cloud

Akamai ha implementado una política de gestión de eventos de seguridad de la información con procedimientos y una política de comunicación relacionada para ayudar a las organizaciones con obligación de notificar filtraciones de datos. Estas políticas y procedimientos forman parte de nuestro sistema de gestión de la seguridad de la información [Identity Cloud](#), que cuenta con la certificación ISO 27001:2013.

OBLIGACIÓN	Notificación de filtraciones
RCPD DE LA UE	Artículo 33
CCPA DE CALIFORNIA	Secciones 1798.29 (a) y 1798.82 (a)
PIPEDA DE CANADÁ	Cláusula 10.1 ff.
LFPDPPP DE MÉXICO	Artículo 20
APA DE AUSTRALIA	Apartado IIIC de APA
APPI DE JAPÓN	No se cubre explícitamente
PDPA DE SINGAPUR	<a href="#">Directrices</a> sobre filtraciones de datos de 2019
LGPD DE BRASIL	Artículo 48
LPDP DE ARGENTINA	Artículo 20
PROYECTO DE LEY PDP DE INDIA DE 2019	Cláusula 25

## Responsabilidad de la organización

Toda organización que controle datos personales es responsable de la protección y seguridad de los datos que procesa de acuerdo con las leyes de protección de datos. Esto exige que la organización conozca en todo momento los datos que procesa, dónde, para qué fin y qué terceros acceden a los datos.

## Cómo puede ayudar Identity Cloud

**Identity Cloud** ayuda a las organizaciones a establecer la responsabilidad de las actividades de procesamiento de datos. Mantiene un registro auditable de los elementos de datos recopilados, lo que incluye cualquier edición de los registros de datos.

Además de proteger los datos almacenados con medidas técnicas y organizativas apropiadas, Identity Cloud ofrece controles de acceso detallados basados en atributos y funciones, además de un mecanismo de registro para demostrar cualquier acceso a los datos. Estas medidas de seguridad demuestran que las organizaciones que utilizan Identity Cloud para procesar datos personales actúan de manera responsable.

OBLIGACIÓN	Responsabilidad de una organización
RGPD DE LA UE	Artículo 5 (2)
CCPA DE CALIFORNIA	Sección 1798.100
PIPEDA DE CANADÁ	Anexo 1, cláusula 4.1
LFPDPPP DE MÉXICO	Artículo 14
APA DE AUSTRALIA	APP 1 y capítulo 1 de las directrices
APPI DE JAPÓN	Artículo 15 ff
PDPA DE SINGAPUR	Artículo 3
LGPD DE BRASIL	Artículo 6 (10)
LPDP DE ARGENTINA	Artículo 10
PROYECTO DE LEY PDP DE INDIA DE 2019	Cláusulas 22 ff. y 29

## Residencia y transferencia de datos

La residencia de datos puede tener un papel importante en las organizaciones debido a los requisitos corporativos o legales internos. En Rusia y China, por ejemplo, se aplican leyes de residencia de datos. En muchos países no existen requisitos de residencia de datos, pero se establecen requisitos de transferencia de datos para garantizar que se mantiene el nivel de protección de datos del país.

### Cómo puede ayudar Identity Cloud

**Identity Cloud** ofrece varios ajustes de residencia de datos para satisfacer las solicitudes relacionadas de los clientes, incluidas las regiones de China y Rusia. En el caso de China, de acuerdo con las leyes aplicables, esto incluye no cifrar en reposo la información de identificación personal almacenada en la región.

En el caso de Rusia, la solución Identity Cloud Russia ofrece un enfoque de tipo "escribir primero en Rusia", en el que el alojamiento de aplicaciones y el almacenamiento de datos de PI de los clientes se realizan en una región secundaria de la Unión Europea.

Akamai cuenta con la certificación del programa Escudo de Privacidad y acuerda con sus clientes cláusulas contractuales estándar para garantizar que se mantiene el nivel de protección de datos del país al transferir datos a otros países.

OBLIGACIÓN	Requisitos de residencia de datos/transferencia de datos
RGPD DE LA UE	Artículo 46 ff.
CCPA DE CALIFORNIA	No aplicable
PIPEDA DE CANADÁ	Anexo 1, cláusula 4.1.3
LFPDPPP DE MÉXICO	Artículo 36 ff.
APA DE AUSTRALIA	APP 8
APPI DE JAPÓN	Artículo 24
PDPA DE SINGAPUR	Artículo 26
LGPD DE BRASIL	Artículo 33 ff.
LPDP DE ARGENTINA	Artículo 23 ff.
PROYECTO DE LEY PDP DE INDIA DE 2019	Cláusula 33 ff.

## Conclusión

Las leyes y normativas de privacidad de datos responsabilizan a las organizaciones del procesamiento de los datos personales y permiten a las personas mantener el control del procesamiento de sus datos personales por parte de terceros. Akamai Identity Cloud permite a las personas gestionar sus datos y ofrece a las organizaciones un registro que permite la transparencia y responsabilidad en el procesamiento de datos personales. Identity Cloud ofrece herramientas y procesos fáciles de usar que le ayudan a mantener el cumplimiento de las leyes de protección de datos aplicables, conservar la seguridad de los datos personales y fomentar la confianza de los clientes.

## Descripción general de las leyes y normativas

REGIÓN	LEY	ENLACE
Unión Europea (UE)	Reglamento General de Protección de Datos (RGPD)	<a href="#">RGPD</a>
California	Ley de Privacidad del Consumidor de California (CCPA)	<a href="#">CCPA</a>
Canadá	Ley de Protección de Datos Personales y Documentos Electrónicos (PIPEDA)	<a href="#">PIPEDA</a>
México	Ley Federal de Protección de Datos Personales en Posesión de los Particulares de 2010 y las normativas relacionadas de 2011	<a href="#">LFPDPPP</a>
Australia	Ley de Privacidad de Australia (APA); Ley de Privacidad de 1988/Principios de Privacidad de Australia (APP)	<a href="#">APA</a> <a href="#">APP</a>
Japón	Ley sobre Protección de Datos Personales (APPI)	<a href="#">APPI</a>
Singapur	Ley de Protección de Datos Personales de 2012 (PDPA)	<a href="#">PDPA</a>
Brasil	Ley General de Privacidad de Datos (LGPD)	<a href="#">LGPD</a>
Argentina	Ley de Protección de Datos Personales (LPDP)	<a href="#">LPDP</a>
India	El Parlamento de India ha presentado el Proyecto de Ley de Protección de Datos Personales de India (Proyecto de Ley PDP de 2019), que en mayo de 2020 se seguía debatiendo. Se ha incluido en este white paper por cuestiones de integridad.	<a href="#">Proyecto de Ley PDB de 2019 (propuesta)</a>

# Arquitectura de referencia de Global Compliance

Al recopilar y procesar datos de clientes, los responsables de todo el mundo deben cumplir varias normativas de privacidad y protección de datos. Una solución de gestión de identidades como **Akamai Identity Cloud** puede ayudar a afrontar estos desafíos.

## Global Compliance: Cliente

### GLOBAL COMPLIANCE: CLIENTE

**Arquitectura de referencia**

#### DESCRIPCIÓN GENERAL

Al recopilar y procesar datos de clientes, los responsables de todo el mundo deben cumplir varias normativas de privacidad y protección de datos. Una solución de gestión de identidades como Akamai Identity Cloud puede ayudar a afrontar estos desafíos.

- 1 El usuario final accede a las propiedades digitales de una empresa desde una variedad de canales diferentes (navegadores de escritorio, aplicaciones móviles o dispositivos IoT), a menudo a través de inicio de sesión mediante redes sociales.
- 2 Akamai Intelligent Edge Platform y sus soluciones de seguridad protegen Identity Cloud frente a ataques maliciosos.
- 3 Los servidores en el borde de Internet protegen las aplicaciones web orientadas al público, las páginas de inicio de sesión y las páginas de registro frente a los ataques DDoS y de aplicaciones web.
- 4 La gestión de bots detecta y mitiga amenazas automatizadas, como el scraping web y el Credential Stuffing.
- 5 Akamai Intelligent Edge Platform dirige el tráfico legítimo a las páginas de registro e inicio de sesión de las propiedades digitales de la empresa.
- 6 Identity Cloud ayuda a las empresas a cumplir las normativas de protección de datos relevantes.
- 7 Identity Cloud es una solución de identidad como servicio (IDaaS) que permite a las organizaciones ofrecer a los usuarios finales control sobre la creación, el uso y la gestión de sus datos.
- 8 La base de datos central de perfiles de clientes es la única fuente de confianza para las identidades y los derechos de acceso de los usuarios finales.
- 9 Los clientes pueden acceder a su consentimiento, verlo, editarlo y revocarlo a través de un autoserivicio gestionado de forma centralizada.
- 10 Controla el acceso hasta al nivel de campos individuales de un registro de datos, tanto de usuarios como de aplicaciones.
- 11 Identity Cloud se integra con sistemas de terceros para el procesamiento adicional de los datos, como la pila de tecnología de marketing.

#### PRODUCTOS CLAVE

- Gestión de acceso e identidades de clientes ▶ Identity Cloud
- Firewall de aplicaciones web y protección contra DDoS ▶ Kona Site Defender
- Aceleración del rendimiento ▶ Ion
- Gestión de bots y protección contra Credential Stuffing ▶ Bot Manager

Publicado en mayo de 2020

Descubra más arquitecturas de referencia en <https://www.akamai.com/es/es/solutions/akamai-architectures.jsp>.



Akamai garantiza experiencias digitales seguras a las empresas más importantes del mundo. La plataforma inteligente de Akamai en el Edge llega a todas partes, desde la empresa a la nube, para garantizar a nuestros clientes y a sus negocios la máxima eficacia, rapidez y seguridad. Las mejores marcas del mundo confían en Akamai para lograr su ventaja competitiva gracias a soluciones ágiles que permiten destapar todo el potencial de sus arquitecturas multinube. En Akamai mantenemos las decisiones, las aplicaciones y las experiencias más cerca de los usuarios que nadie; y los ataques y las amenazas, a raya. La cartera de soluciones de seguridad en el Edge, rendimiento web y móvil, acceso empresarial y distribución de vídeo de Akamai está respaldada por un servicio de atención al cliente y análisis excepcional, y por una supervisión ininterrumpida, durante todo el año. Para descubrir por qué las marcas más importantes del mundo confían en Akamai, visite [www.akamai.com](https://www.akamai.com) y [blogs.akamai.com](https://blogs.akamai.com), o siga a [@Akamai](https://twitter.com/Akamai) en Twitter. Puede encontrar los datos de contacto de todas nuestras oficinas en <https://www.akamai.com/locations>. Publicado en julio de 2020.

Una guía para cumplir los requisitos de privacidad de datos con Akamai Identity Cloud