

ISO/IEC 27018:2025, Seguridad de la información, ciberseguridad y protección de la privacidad: Directrices para la protección de la información de identificación personal (PII) en nubes públicas que actúan como encargados del tratamiento de PII (3.ª edición, 2025-08)

Protección de PII en la nube pública

36 requisitos. Para esta norma no existe un certificado acreditado. Versión de 07/2026.

ISO/IEC 27018 no es una norma de sistema de gestión, sino un conjunto de directrices con controles adicionales sobre la base de ISO/IEC 27002:2022. No existe un certificado acreditado independiente para ISO/IEC 27018. Los controles se incorporan a la Declaración de Aplicabilidad de un sistema ISO/IEC 27001, y el certificado se emite entonces conforme a ISO/IEC 27001 con referencia a ISO/IEC 27018. La norma se dirige al proveedor de un servicio de nube pública que trata información de identificación personal por cuenta de sus clientes del servicio en la nube. Una organización que simplemente consume servicios en la nube no asume ese papel y debe evaluar de forma razonable los requisitos frente a sus proveedores, no frente a sí misma. Para Leanshift, esta lista de verificación es por tanto ante todo una matriz de evaluación de proveedores. Cada punto puede plantearse al proveedor como una pregunta y respaldarse mediante el contrato de encargado del tratamiento conforme al artículo 28 del RGPD. El resultado de dicha evaluación es un registro interno de conformidad o un perfil de valoración del proveedor, no un certificado. Sobre la numeración: los apartados A.2 a A.12 siguen los principios de privacidad del anexo A de la norma, los puntos numerados como A.11.6 son los controles adicionales allí enumerados. Los puntos numerados como 8.10 o 5.34 remiten a controles de ISO/IEC 27002:2022 que la norma concreta para la nube. Los puntos con el sufijo "(Grundsatz)", que significa principio, se derivan del principio del propio apartado, en los casos en que el anexo A no recoge un control adicional específico.

Empresa		Fecha	Elaborado por

A.2 Consentimiento y elección2

A.2.1El proveedor del servicio en la nube apoya al cliente del servicio en la nube para atender los derechos de los interesados, como el acceso, la rectificación, la supresión y la oposición. Las responsabilidades y los plazos se establecen contractualmente.Documento

Cómo se demuestra: Como evidencia sirve el contrato de encargado del tratamiento conforme al artículo 28 del RGPD con una cláusula de asistencia en el ejercicio de los derechos de los interesados, junto con los medios técnicos del propio servicio: funciones de exportación, corrección y eliminación, o un procedimiento de soporte documentado con un plazo de respuesta. Pregunta al proveedor: qué función o procedimiento ofrece para que podamos atender una solicitud de acceso o supresión en el plazo de un mes?

AbiertoEn cursoCumplidoNo aplicable

Evidencia / justificación

A.2 (Grundsatz)La información de identificación personal de los clientes del servicio en la nube se trata únicamente conforme a las instrucciones documentadas del cliente. La obtención del consentimiento de los interesados sigue siendo tarea del cliente en su calidad de responsable del tratamiento, y el proveedor no se anticipa a ello.

Cómo se demuestra: Como evidencia sirve la cláusula de instrucciones del contrato de encargado del tratamiento, junto con la prueba de que el proveedor no hace un uso secundario de los datos, por ejemplo el aviso de privacidad del servicio y la documentación del producto. Pregunta al proveedor: trata usted los datos de nuestros clientes de alguna forma ajena a nuestras instrucciones, por ejemplo para la mejora del producto o el entrenamiento de modelos?

AbiertoEn cursoCumplidoNo aplicable

Evidencia / justificación

A.3 Legitimidad y especificación de la finalidad2

A.3.1La finalidad para la que el proveedor trata la información de identificación personal se limita a la prestación del servicio acordado y se especifica en el contrato. No se produce ningún tratamiento para fines propios del proveedor.Documento

Cómo se demuestra: Como evidencia sirve el contrato de encargado del tratamiento que indica el objeto, la naturaleza, la finalidad y la duración del tratamiento, así como las categorías de interesados conforme al artículo 28.3 del RGPD. Pregunta al proveedor: facilite el anexo contractual que describa de forma exhaustiva la finalidad del tratamiento. Para organizaciones pequeñas basta con el anexo estándar de tratamiento de datos del proveedor, siempre que contenga esta información.

AbiertoEn cursoCumplidoNo aplicable

Evidencia / justificación

A.3.2

La información de identificación personal confiada al proveedor no se utiliza para publicidad, marketing u otros fines comerciales propios del proveedor sin consentimiento expreso previo. La prestación del servicio no se condiciona a dicho consentimiento.

Cómo se demuestra: Como evidencia sirve una cláusula contractual explícita que excluya el uso comercial secundario, junto con las condiciones del servicio. Pregunta al proveedor: confirme por escrito que los datos de los clientes no se utilizan para publicidad, elaboración de perfiles o entrenamiento de modelos de IA. Si falta este compromiso, el servicio no es adecuado para tratar información de identificación personal.

Abierto

En curso

Cumplido

No aplicable

Evidencia / justificación

A.4 Limitación de la recopilación

1

A.4 (Grunds

Más allá de los datos que el cliente introduce en el servicio, el proveedor no recopila información de identificación personal adicional para fines propios, como telemetría, perfiles de uso o análisis de contenido. Los datos operativos y los metadatos que se recopilan están identificados y justificados.

Cómo se demuestra: Como evidencia sirve una lista de los datos que el servicio registra además de los datos de contenido (registros de acceso, telemetría, datos de diagnóstico), con su finalidad y plazo de conservación, junto con una captura de pantalla del ajuste que desactiva la telemetría opcional. Pregunta al proveedor: qué datos de uso, telemetría y diagnóstico recopila adicionalmente, para qué los utiliza y podemos desactivar esa recopilación?

Abierto

En curso

Cumplido

No aplicable

Evidencia / justificación

A.5 Minimización de datos

2

A.5.1

Los archivos temporales generados al tratar información de identificación personal, como almacenamiento provisional, cachés o registros de reversión, se eliminan de forma segura dentro de un plazo definido.

Cómo se demuestra: Como evidencia sirve un procedimiento operativo o de eliminación con un plazo de conservación definido para los datos temporales, respaldado por la configuración del sistema, por ejemplo un TTL de caché o una tarea de limpieza programada con su registro de ejecución. Pregunta al proveedor: tras qué plazo se eliminan las cachés, los archivos temporales y los estados intermedios, y cómo se supervisa esto?

Abierto

En curso

Cumplido

No aplicable

Evidencia / justificación

8.11

Siempre que las operaciones, las pruebas o el soporte no requieran datos reales, la información de identificación personal se enmascara, seudonimiza o anonimiza. El volumen de datos tratados se limita a lo que el servicio realmente necesita.

Cómo se demuestra: Como evidencia sirve una norma que determine qué entornos pueden acceder a datos reales, junto con capturas de pantalla o scripts del enmascaramiento aplicado en los sistemas de prueba y desarrollo. Pregunta al proveedor: trabajan sus equipos de soporte y desarrollo con datos de producción y, en caso afirmativo, bajo qué garantías? Para organizaciones pequeñas basta con una norma que establezca que los sistemas de prueba funcionan exclusivamente con datos de muestra generados.

Abierto

En curso

Cumplido

No aplicable

Evidencia / justificación

A.6 Limitación del uso, la conservación y la divulgación

3

A.6.1

Cuando el proveedor recibe una solicitud jurídicamente vinculante de divulgación de información de identificación personal, por ejemplo de una autoridad pública, informa previamente al cliente del servicio en la nube, en la medida en que la ley lo permita.

Cómo se demuestra: Como evidencia sirve una cláusula contractual de notificación y un proceso interno para solicitudes de autoridades con un responsable designado. Pregunta al proveedor: nos notifica antes de entregar datos, y publica un informe de transparencia sobre las solicitudes de las autoridades? Un informe de transparencia actualizado constituye una evidencia sólida.

Abierto

En curso

Cumplido

No aplicable

Evidencia / justificación

A.6.2 Cuando el proveedor divulga información de identificación personal a terceros, registra el hecho de forma que pueda rastrearse: quién recibió los datos, cuándo ocurrió, qué datos se vieron afectados y en qué base se sustenta la divulgación. [Documento](#)

Cómo se demuestra: Como evidencia sirve un registro de divulgaciones o un historial de tickets con esos campos, aunque no contenga entradas. Un registro vacío pero mantenido es aceptable y es la vía práctica para organizaciones pequeñas. Pregunta al proveedor: lleva un registro de las divulgaciones de datos, y podemos obtener extractos de él?

Abierto En curso Cumplido No aplicable

Evidencia / justificación

8.10 La información de identificación personal se elimina una vez vencido el plazo de conservación acordado o finalizado el contrato, incluidas las copias conservadas en las copias de seguridad tras su ciclo de rotación.

Cómo se demuestra: Como evidencia sirve un concepto de eliminación con plazos de conservación por categoría de datos, el plazo de conservación de las copias de seguridad y un registro o confirmación de eliminación. Pregunta al proveedor: cuánto tiempo permanecen nuestros datos en sus copias de seguridad tras la finalización del contrato, y recibimos confirmación por escrito de su eliminación?

Abierto En curso Cumplido No aplicable

Evidencia / justificación

A.7 Exactitud y calidad

2

A.7 (Grund) El proveedor no modifica por iniciativa propia la información de identificación personal que se le ha confiado. Las correcciones y actualizaciones se realizan únicamente por instrucción del cliente del servicio en la nube o mediante funciones que el propio cliente gestiona.

Cómo se demuestra: Como evidencia sirven las funciones de edición del servicio junto con su historial de cambios, además de la cláusula de instrucciones del contrato de encargado del tratamiento. Pregunta al proveedor: podemos corregir los registros nosotros mismos, y queda registrado cada cambio de forma que pueda rastrearse?

Abierto En curso Cumplido No aplicable

Evidencia / justificación

8.13 La integridad de la información de identificación personal está protegida durante el almacenamiento, la transmisión y la restauración. Existen copias de seguridad y su capacidad de restauración ha sido probada.

Cómo se demuestra: Como evidencia sirve la configuración de las copias de seguridad, los mecanismos de suma de comprobación o integridad, y al menos una prueba de restauración documentada al año con fecha y resultado. Pregunta al proveedor: con qué frecuencia prueba las restauraciones, y qué tiempo de recuperación garantiza en el nivel de servicio?

Abierto En curso Cumplido No aplicable

Evidencia / justificación

A.8 Apertura, transparencia y aviso

2

A.8.1 El uso de subencargados que traten información de identificación personal se comunica antes de la celebración del contrato. Los cambios en la lista se notifican al cliente con la antelación suficiente, de modo que este pueda oponerse o resolver el contrato. [Documento](#)

Cómo se demuestra: Como evidencia sirve una lista actualizada de subencargados, publicada o puesta a disposición contractualmente, con nombre, país y finalidad del tratamiento, junto con una regla de notificación conforme al artículo 28.2 del RGPD. Pregunta al proveedor: dónde encontramos su lista de subencargados, con cuánta antelación notifica los cambios, y cómo podemos oponernos?

Abierto En curso Cumplido No aplicable

Evidencia / justificación

A.8 (Grund) Antes de la celebración del contrato, el proveedor pone a disposición información comprensible sobre cómo se trata la información de identificación personal, qué garantías existen y en qué jurisdicciones tiene lugar el tratamiento.

Cómo se demuestra: Como evidencia sirven el aviso de privacidad, un documento técnico de seguridad, una página de centro de confianza y el contrato de encargado del tratamiento con las medidas técnicas y organizativas como anexo. Pregunta al proveedor: facilite la lista actualizada de medidas técnicas y organizativas como anexo contractual, no solo como material de marketing.

Abierto En curso Cumplido No aplicable

Evidencia / justificación

A.9 Participación individual y acceso

2

A.9 (Grundsatz) El servicio proporciona al cliente del servicio en la nube los medios técnicos para atender por sí mismo las solicitudes de acceso, rectificación y supresión de los interesados, por ejemplo mediante funciones de exportación, búsqueda y eliminación.

Cómo se demuestra: Como evidencia sirve la documentación del producto sobre las funciones de exportación y eliminación, respaldada por una prueba interna: tramitar de principio a fin una solicitud de acceso y anotar cuánto tiempo lleva. Pregunta al proveedor: podemos localizar, exportar y eliminar todos los datos de una persona concreta sin su soporte?

Abierto En curso Cumplido No aplicable

Evidencia / justificación

5.34 Cuando el cliente no pueda atender por sí mismo una solicitud de un interesado, el proveedor presta asistencia dentro de un plazo acordado. Las solicitudes que los interesados envían directamente al proveedor se remiten al cliente en lugar de ser respondidas por el proveedor.

Cómo se demuestra: Como evidencia sirve la cláusula correspondiente del contrato de encargado del tratamiento con un plazo de respuesta concreto, junto con un historial de tickets de soporte como ejemplo real. Pregunta al proveedor: qué plazo garantiza para la asistencia en el ejercicio de los derechos de los interesados, y qué coste tiene?

Abierto En curso Cumplido No aplicable

Evidencia / justificación

A.10 Responsabilidad proactiva

4

A.10.1 Las violaciones de seguridad que afecten a información de identificación personal se comunican al cliente del servicio en la nube sin dilación indebida, indicando el alcance, los datos afectados, la causa y las medidas adoptadas. Se define un proceso de notificación con responsabilidades y plazos.[Documento](#)

Cómo se demuestra: Como evidencia sirve el plan de respuesta a incidentes con su cadena de escalado, el plazo contractual de notificación (entre 24 y 48 horas funciona en la práctica, de modo que el cliente pueda cumplir el plazo de 72 horas del artículo 33 del RGPD) y los registros de incidentes anteriores o de un simulacro. Pregunta al proveedor: en qué plazo notifica un incidente, por qué canal, y qué información aporta junto con la notificación?

Abierto En curso Cumplido No aplicable

Evidencia / justificación

A.10.2 Las políticas de seguridad, los procedimientos operativos y los registros correspondientes se conservan durante un plazo definido, de modo que el tratamiento pueda reconstruirse a posteriori.[Documento](#)

Cómo se demuestra: Como evidencia sirve una norma de conservación con el historial de versiones de las políticas, por ejemplo mediante un registro documental o un sistema de control de versiones con la fecha de aprobación. Pregunta al proveedor: durante cuánto tiempo conserva las versiones de las políticas y los registros correspondientes, y tenemos acceso a ellos en caso de auditoría?

Abierto En curso Cumplido No aplicable

Evidencia / justificación

A.10.3 Existe un procedimiento definido para la devolución, transferencia y destrucción de la información de identificación personal al finalizar el contrato, que especifica formatos, plazos y el tratamiento de las copias.[Documento](#)

Cómo se demuestra: Como evidencia sirve la cláusula de salida del contrato de encargado del tratamiento, junto con una confirmación de eliminación tras la finalización del contrato. Pregunta al proveedor: en qué formato y en qué plazo recuperamos nuestros datos, cuándo se destruyen todas las copias, y recibimos confirmación por escrito?

Abierto En curso Cumplido No aplicable

Evidencia / justificación

5.35 La eficacia de las garantías se revisa de forma independiente a intervalos regulares, por ejemplo mediante auditorías internas, pruebas de penetración o informes de aseguramiento de terceros. Los resultados se ponen a disposición del cliente del servicio en la nube en una forma adecuada.

Cómo se demuestra: Como evidencia sirve un certificado ISO/IEC 27001 con una Declaración de Aplicabilidad que incluya los controles de ISO/IEC 27018, o un informe SOC 2, junto con resúmenes actualizados de pruebas de penetración. Pregunta al proveedor: facilite el certificado, su alcance y la confirmación de que ISO/IEC 27018 se refleja en la Declaración de Aplicabilidad. Compruebe si el alcance cubre realmente el servicio que utiliza.

Abierto En curso Cumplido No aplicable

Evidencia / justificación

A.11 Seguridad de la información 13

A.11.1 Todas las personas con acceso a información de identificación personal están sujetas a un deber de confidencialidad, ya sean empleados directos o colaboradores externos. [Documento](#)

Cómo se demuestra: Como evidencia sirven los acuerdos o compromisos de confidencialidad firmados que permanecen vigentes tras finalizar la relación. Pregunta al proveedor: están todos los empleados y proveedores de servicios con acceso a los datos sujetos a un compromiso de confidencialidad por escrito?

Abierto En curso Cumplido No aplicable

Evidencia / justificación

A.11.2 Las impresiones y otras copias en papel que contengan información de identificación personal se generan únicamente cuando resulta estrictamente necesario. El alcance permitido se regula mediante una norma.

Cómo se demuestra: Como evidencia sirve una norma sobre el manejo de impresiones, que en los centros de datos suele consistir en una prohibición general de imprimir en las áreas donde se alojan datos de clientes. Pregunta al proveedor: se imprimen datos de clientes en sus operaciones y, en caso afirmativo, bajo qué condiciones?

Abierto En curso Cumplido No aplicable

Evidencia / justificación

A.11.3 Las restauraciones a partir de copias de seguridad se autorizan previamente y se registran, incluyendo la persona que las inició y los datos afectados. [Documento](#)

Cómo se demuestra: Como evidencia sirve el registro de restauraciones con marca temporal, origen y alcance, generado normalmente de forma automática por la herramienta de copia de seguridad. Pregunta al proveedor: registra todas las restauraciones, y podemos consultar esos registros en caso de auditoría?

Abierto En curso Cumplido No aplicable

Evidencia / justificación

A.11.4 Los soportes de almacenamiento con información de identificación personal que salen de las instalaciones están protegidos frente al acceso no autorizado y la pérdida, por regla general mediante cifrado y un registro de transporte.

Cómo se demuestra: Como evidencia sirve la prueba del cifrado (cifrado completo del soporte), los registros de transporte y entrega, y un inventario de soportes. Pregunta al proveedor: salen alguna vez de sus instalaciones soportes con datos de clientes, por ejemplo para copias de seguridad, y cómo se protegen durante el transporte?

Abierto En curso Cumplido No aplicable

Evidencia / justificación

A.11.5 El uso de soportes y dispositivos portátiles sin cifrar para información de identificación personal está prohibido o limitado a excepciones justificadas con aprobación documentada.

Cómo se demuestra: Como evidencia sirve una política de soportes extraíbles junto con su aplicación técnica, por ejemplo el cifrado obligatorio de dispositivos o el bloqueo de los puertos USB mediante gestión de dispositivos. Pregunta al proveedor: puede el personal copiar datos de clientes en dispositivos sin cifrar, y qué lo impide técnicamente?

Abierto En curso Cumplido No aplicable

Evidencia / justificación

A.11.6	La información de identificación personal transmitida por redes públicas se cifra. Los mecanismos empleados reflejan el estado actual de la técnica.
Cómo se demuestra: Como evidencia sirve la configuración TLS (versión de protocolo actual, sin cifrados obsoletos) y una prueba externa de configuración documentada en un informe. Práctico para organizaciones pequeñas: realizar un análisis TLS gratuito una vez al año y archivar el resultado. Pregunta al proveedor: qué cifrado de transporte aplica de forma obligatoria, y está activo el cifrado en reposo?	
AbiertoEn cursoCumplidoNo aplicable	
Evidencia / justificación	
A.11.7	Los documentos en papel que contienen información de identificación personal se destruyen de forma que se excluya cualquier reconstrucción.
Cómo se demuestra: Como evidencia sirven destructoras de papel con un nivel de seguridad adecuado o certificados de destrucción de un proveedor de servicios que trabaje conforme a la norma DIN 66399 o una norma equivalente. Pregunta al proveedor: cómo destruye los documentos en papel relativos a clientes, y se conservan los certificados de destrucción?	
AbiertoEn cursoCumplidoNo aplicable	
Evidencia / justificación	
A.11.8	Los identificadores de usuario se asignan de forma exclusiva a una persona y no se reasignan ni se comparten. Las cuentas compartidas solo existen en excepciones justificadas y con trazabilidad adicional.
Cómo se demuestra: Como evidencia sirve una lista de usuarios del sistema de identidad libre de cuentas de grupo, junto con la norma de que las tareas administrativas se realizan desde una cuenta personal. Pregunta al proveedor: trabaja su personal de operaciones con cuentas personales, y es obligatoria la autenticación multifactor?	
AbiertoEn cursoCumplidoNo aplicable	
Evidencia / justificación	
A.11.9	El proveedor puede indicar en todo momento qué personas o roles tienen permiso para acceder a la información de identificación personal, y mantiene actualizada esa relación.
Cómo se demuestra: Como evidencia sirve una relación de derechos de acceso por rol, respaldada por una revisión periódica de accesos con fecha y resultado. Para organizaciones pequeñas basta con una exportación semestral de la lista de usuarios, firmada. Pregunta al proveedor: cuántos de sus empleados pueden acceder a nuestros datos, y con qué frecuencia lo revisa?	
AbiertoEn cursoCumplidoNo aplicable	
Evidencia / justificación	
A.11.10	Las cuentas de usuario se gestionan a lo largo de todo su ciclo de vida: creación, modificación y desactivación inmediata cuando alguien deja la organización o cambia de función.
Cómo se demuestra: Como evidencia sirve un procedimiento de alta y baja con una lista de verificación, junto con registros de cuentas desactivadas con marca temporal. Pregunta al proveedor: en qué plazo retira el acceso al personal que deja la organización, y cómo lo acredita?	
AbiertoEn cursoCumplidoNo aplicable	
Evidencia / justificación	
A.11.11	Las obligaciones de seguridad y privacidad del proveedor se establecen contractualmente, incluidas las medidas técnicas y organizativas, el carácter vinculante de las instrucciones del cliente y el derecho de auditoría del cliente.
Cómo se demuestra: Como evidencia sirve el contrato de encargado del tratamiento firmado conforme al artículo 28 del RGPD, con el anexo de medidas y un derecho de auditoría o de información. Pregunta al proveedor: facilite el contrato de encargado del tratamiento firmado incluidos sus anexos, no solo una remisión a las condiciones generales del servicio.	
AbiertoEn cursoCumplidoNo aplicable	
Evidencia / justificación	

A.11.12 Los subencargados que traten información de identificación personal están sujetos al menos a las mismas obligaciones que el propio proveedor. Su selección y su supervisión continuada se rigen por un proceso definido.

Cómo se demuestra: Como evidencia sirve el traslado de obligaciones en los contratos con los subencargados (artículo 28.4 del RGPD) y una evaluación de proveedores con fecha. Pregunta al proveedor: cómo evalúa a sus subencargados, y qué evidencias les exige?

Abierto En curso Cumplido No aplicable

Evidencia / justificación

A.11.13 Antes de reutilizar el espacio de almacenamiento, se garantiza que no queden accesibles datos de usuarios anteriores, ni en soportes físicos ni en entornos virtualizados.

Cómo se demuestra: Como evidencia sirve el procedimiento de saneamiento o sobrescritura aplicado al liberar el almacenamiento, los registros de destrucción de soportes y la separación entre clientes descrita en el documento de arquitectura. Pregunta al proveedor: cómo garantiza que el almacenamiento reutilizado no conserve datos residuales de otros clientes?

Abierto En curso Cumplido No aplicable

Evidencia / justificación

A.12 Cumplimiento en materia de privacidad

3

A.12.1 Los países en los que se almacena y trata la información de identificación personal están identificados y son conocidos por el cliente del servicio en la nube. Los cambios en las ubicaciones de almacenamiento se notifican.

[Documento](#)

Cómo se demuestra: Como evidencia sirve la relación de sedes y regiones del proveedor, en el contrato o en la documentación, junto con una captura de pantalla del ajuste de región del servicio utilizado. Pregunta al proveedor: en qué países reposan nuestros datos, desde qué países se accede a ellos, por ejemplo en soporte, y podemos fijar la región?

Abierto En curso Cumplido No aplicable

Evidencia / justificación

A.12.2 Las transferencias de información de identificación personal a terceros países son conocidas, están justificadas y cuentan con garantías adecuadas.

[Documento](#)

Cómo se demuestra: Como evidencia sirven las cláusulas contractuales tipo o una decisión de adecuación, respaldadas por una evaluación de impacto de la transferencia, que en organizaciones pequeñas puede ser breve: categorías de datos afectadas, país de destino, riesgo, medidas adicionales adoptadas. Pregunta al proveedor: en qué base legal se apoya para transferir datos a terceros países, y qué medidas adicionales aplica?

Abierto En curso Cumplido No aplicable

Evidencia / justificación

5.31 Los requisitos legales y contractuales aplicables al tratamiento de la información de identificación personal están identificados y se mantienen actualizados conforme cambia la situación legal. Se evalúan los conflictos entre jurisdicciones.

Cómo se demuestra: Como evidencia sirve una relación de los requisitos aplicables (RGPD, normativa nacional, obligaciones sectoriales) con un responsable y una fecha de revisión. En una organización pequeña basta con una lista de una página revisada anualmente. Pregunta al proveedor: está usted o sus subencargados sujetos a jurisdicciones que permitan a las autoridades acceder a nuestros datos, y cómo lo gestiona?

Abierto En curso Cumplido No aplicable

Evidencia / justificación