



CENTRO DE CONFIANZA

# Cuestionario CAIQ Lite respondido

Autoevaluación de Igniten sobre el cuestionario de la Cloud Security Alliance, para el área de seguridad y de compras del Cliente.

| Versión | Fecha                    | Vigencia                        | Acceso            | Contacto                                                     |
|---------|--------------------------|---------------------------------|-------------------|--------------------------------------------------------------|
| 1.0     | 25 de septiembre de 2026 | Desde la disponibilidad general | Documento público | <a href="mailto:security@igniten.io">security@igniten.io</a> |

**Vigencia.** Este documento describe el servicio Igniten tal como se presta desde su disponibilidad general. Entra en vigor en la fecha en que la plataforma esté disponible comercialmente y rige para cada Cliente desde que celebra el contrato. Hasta entonces se publica solo con fines informativos y no genera obligaciones para ninguna de las partes.

## 1. Cómo leer este documento

Este es el cuestionario CAIQ Lite de la Cloud Security Alliance (CSA), respondido por Igniten sobre la versión 4 de su matriz de controles de la nube (CCM). Es una **autoevaluación**: no la emitió un auditor externo. La misma autoevaluación se presenta en el registro público CSA STAR, nivel 1.

Las preguntas están agrupadas por dominio de la CCM y por control, con el identificador del control. Cada respuesta es una de tres:

- **Sí:** el control existe y opera en la plataforma.
- **No:** el control no existe. Donde corresponde, el comentario dice qué lo compensa.
- **N.A.:** no aplica al modelo de Igniten, con el motivo.

Las filas marcadas con un guion en la columna ID son preguntas propias de una plataforma de inteligencia artificial, que los cuestionarios de proveedores suelen incluir y que la CCM no formula por separado.

Igniten es una sociedad de responsabilidad limitada (LLC) constituida en el Estado de Wyoming, Estados Unidos de América, y opera sobre Amazon Web Services, en la región Norte de Virginia (us-east-1). Los controles físicos y de centro de datos son del proveedor de nube y constan en sus propios informes de auditoría.

Si su equipo necesita evidencia de alguna respuesta, se la entregamos.

## 2. A&A · Auditoría y aseguramiento

| ID     | Pregunta                                                                         | Respuesta | Comentario                                                                                                                                                     |
|--------|----------------------------------------------------------------------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A&A-01 | ¿Hay políticas de auditoría y aseguramiento, revisadas al menos una vez por año? | Sí        | La política de gestión de riesgos define la evaluación interna y la independiente. Se revisa cada trimestre                                                    |
| A&A-02 | ¿Se hacen evaluaciones independientes al menos una vez por año?                  | Sí        | Prueba de penetración externa sobre la plataforma, con el conector de red incluido. La auditoría SOC 2 sigue el calendario publicado en el centro de confianza |
| A&A-03 | ¿Las evaluaciones se planifican según el riesgo?                                 | Sí        | El alcance parte del modelo de amenazas. Las auditorías internas se hacen con medición y control negativo, no por declaración                                  |

| ID     | Pregunta                                                                | Respuesta | Comentario                                                                                                                                                                                                                             |
|--------|-------------------------------------------------------------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A&A-04 | ¿Se verifica el cumplimiento de los requisitos legales y contractuales? | Sí        | Marco de referencia: Ley 25.326 de Protección de los Datos Personales y su reglamentación, y el RGPD como estándar de diseño. Cada afirmación pública de seguridad se verifica contra el control que la implementa antes de publicarse |
| A&A-05 | ¿Hay un proceso de gestión de auditorías y de su evidencia?             | Sí        | Una plataforma de cumplimiento recolecta la evidencia de forma automática y continua                                                                                                                                                   |
| A&A-06 | ¿Los hallazgos tienen un plan de remediación con seguimiento?           | Sí        | Todo hallazgo se registra con su medición y un criterio de cierre verificable; se cierra cuando la medición lo confirma                                                                                                                |

### 3. AIS · Seguridad de aplicaciones e interfaces

| ID     | Pregunta                                                             | Respuesta | Comentario                                                                                                                                                                                                                       |
|--------|----------------------------------------------------------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AIS-01 | ¿Hay políticas de seguridad de aplicaciones?                         | Sí        | Ciclo de vida de desarrollo seguro documentado, aplicado a todos los componentes de la plataforma                                                                                                                                |
| AIS-02 | ¿Hay líneas base de seguridad para aplicaciones?                     | Sí        | Compuertas automáticas obligatorias en cada cambio: análisis estático, detección de secretos, análisis de dependencias, calidad y archivos de bloqueo verificados. Cada compuerta tiene su control negativo                      |
| AIS-04 | ¿El diseño y el desarrollo siguen un proceso seguro definido?        | Sí        | Todo cambio entra por solicitud de cambio, con aprobación obligatoria de una persona distinta de quien lo escribió                                                                                                               |
| AIS-05 | ¿Hay pruebas de seguridad automatizadas?                             | Sí        | Análisis estático y de secretos en cada cambio; barrido completo semanal; pruebas dinámicas automatizadas semanales sobre la plataforma                                                                                          |
| AIS-06 | ¿El despliegue es automatizado y seguro?                             | Sí        | Despliegue disparado de forma explícita sobre una etiqueta firmada, con credenciales federadas de corta vida, imágenes firmadas referenciadas por huella y vuelta atrás automática                                               |
| AIS-07 | ¿Las vulnerabilidades de aplicación se remedian en plazos definidos? | Sí        | Crítica: hasta 7 días. Alta: hasta 30 días. Media: hasta 90 días. Baja: en el ciclo siguiente                                                                                                                                    |
| —      | ¿El contenido indexado se evalúa en busca de instrucciones ocultas?  | Sí        | Cada elemento pasa por un evaluador dedicado antes de indexarse, y el contenido marcado se neutraliza antes de llegar al razonamiento. Los criterios del evaluador no se publican; se comparten bajo acuerdo de confidencialidad |
| —      | ¿Toda operación con efecto externo requiere confirmación humana?     | Sí        | Se materializa como borrador persistido y no llega a ningún proveedor sin confirmación explícita. No existe una ruta de ejecución que evite ese paso                                                                             |

| ID | Pregunta                                                                         | Respuesta | Comentario                                                                                                                                                                                                                                 |
|----|----------------------------------------------------------------------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| —  | ¿Las consultas que genera el asistente sobre bases de datos son solo de lectura? | Sí        | Se validan como consultas de lectura y pasan por el control de acceso por tabla y columna. La garantía final es la credencial de solo lectura que el Cliente crea en su base                                                               |
| —  | ¿El análisis de planillas está aislado?                                          | Sí        | Sin ejecución de código: validador por lista de construcciones permitidas, motor analítico sin acceso externo e instanciado por petición, dentro de un proceso aislado sin red, sin credenciales y con sistema de archivos de solo lectura |

## 4. BCR · Continuidad del negocio y resiliencia operativa

| ID     | Pregunta                                                                  | Respuesta | Comentario                                                                                                                                                                   |
|--------|---------------------------------------------------------------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BCR-01 | ¿Hay una política de continuidad y resiliencia?                           | Sí        | Política de continuidad y respaldo, revisada cada trimestre y después de cada ensayo                                                                                         |
| BCR-02 | ¿Hay análisis de impacto y de riesgo de las interrupciones?               | Sí        | El punto de recuperación es el de la recuperación a un punto en el tiempo. La contención de un incidente se hace por organización, sin afectar a las demás                   |
| BCR-03 | ¿Hay estrategias de continuidad?                                          | Sí        | Base de datos gestionada con réplica sincrónica en una segunda zona de disponibilidad, respaldos automáticos y recuperación a un punto en el tiempo                          |
| BCR-04 | ¿Hay un plan de continuidad documentado?                                  | Sí        | Procedimientos de restauración escritos paso a paso, ejecutables por cualquiera de los responsables                                                                          |
| BCR-06 | ¿El plan se ejercita al menos una vez por año?                            | Sí        | Ensayo trimestral de restauración completa y de restauración de una única organización, con acta y tiempos medidos. Cada ensayo lo corre una persona distinta de la anterior |
| BCR-07 | ¿Hay comunicación con las partes durante una interrupción?                | Sí        | Los incidentes que afectan a una organización se comunican a todos sus administradores. El panel muestra el estado de sus conectores                                         |
| BCR-08 | ¿Se respaldan los datos, cifrados, y se verifica que se puedan restaurar? | Sí        | Respaldo automático diario, retenido 14 días, cifrado con una clave de titularidad de Igniten. La restauración se verifica en los ensayos trimestrales                       |
| BCR-09 | ¿Hay un plan de recuperación ante desastres?                              | Sí        | Restauración de la instancia completa o de una sola organización, siempre sobre una instancia temporal, nunca sobre la de producción                                         |
| BCR-10 | ¿El plan de respuesta se prueba?                                          | Sí        | Ver BCR-06 y SEF-04                                                                                                                                                          |
| BCR-11 | ¿Hay redundancia de equipos y de zonas?                                   | Sí        | Réplica sincrónica en una segunda zona de disponibilidad. El plan Empresa tiene un compromiso de disponibilidad del 99,5 %                                                   |

## 5. CCC · Control de cambios y configuración

| ID     | Pregunta                                                          | Respuesta | Comentario                                                                                                                                                                                                             |
|--------|-------------------------------------------------------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CCC-01 | ¿Hay una política de gestión de cambios?                          | Sí        | Ningún cambio llega a producción sin solicitud de cambio, aprobación de otra persona, compuertas en verde, imagen firmada y despliegue sobre etiqueta firmada                                                          |
| CCC-02 | ¿Los cambios se prueban antes de producción?                      | Sí        | Suites automáticas en cada cambio. El despliegue es progresivo, con reemplazo gradual y vuelta atrás automática ante falla                                                                                             |
| CCC-03 | ¿Hay tecnología de gestión de cambios?                            | Sí        | Control de versiones con solicitudes de cambio, infraestructura como código y tubería de despliegue                                                                                                                    |
| CCC-04 | ¿Se impiden los cambios no autorizados?                           | Sí        | La rama principal de cada repositorio está protegida: aprobación obligatoria de otra persona, aprobaciones anteriores descartadas ante un cambio nuevo, verificaciones requeridas y sin excepción para administradores |
| CCC-05 | ¿Los cambios que afectan al Cliente se acuerdan contractualmente? | Sí        | Preaviso de 30 días antes de incorporar un sub-procesador nuevo o de cambiar los términos                                                                                                                              |
| CCC-06 | ¿Hay líneas base de configuración?                                | Sí        | Toda la infraestructura está declarada como código; cada cambio muestra su plan antes de aplicarse                                                                                                                     |
| CCC-07 | ¿Se detectan desvíos de la línea base?                            | Sí        | Detección continua de cambios de configuración en la cuenta de nube, además del plan de cada cambio                                                                                                                    |
| CCC-08 | ¿Hay un proceso de excepciones?                                   | Sí        | Toda excepción se registra con alcance, responsable y vencimiento; una compuerta automática rechaza las vencidas                                                                                                       |
| CCC-09 | ¿Se puede volver atrás un cambio?                                 | Sí        | Vuelta atrás automática en el despliegue, y reversión controlada por el mismo circuito de cambios                                                                                                                      |

## 6. CEK · Criptografía, cifrado y gestión de claves

| ID     | Pregunta                                          | Respuesta | Comentario                                                                                                                                                          |
|--------|---------------------------------------------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CEK-01 | ¿Hay una política de cifrado y gestión de claves? | Sí        | Modelo de claves documentado: clave maestra por organización y cifrado de sobre                                                                                     |
| CEK-02 | ¿Hay roles y responsabilidades sobre las claves?  | Sí        | La aplicación solo puede cifrar y descifrar con la clave de cada organización. Deshabilitar o eliminar una clave queda reservado a un rol humano con segundo factor |

| ID     | Pregunta                                        | Respuesta | Comentario                                                                                                                                                                                                                                                                                                    |
|--------|-------------------------------------------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CEK-03 | ¿Los datos se cifran en reposo y en tránsito?   | Sí        | En reposo, dos capas: cifrado de volumen con clave de titularidad de Igniten y cifrado autenticado en la aplicación con la clave de la organización. En tránsito, TLS en todo trayecto, incluido entre servicios internos, con verificación de certificado. La base y la caché rechazan conexiones sin cifrar |
| CEK-04 | ¿Los algoritmos y los mecanismos son adecuados? | Sí        | Cifrado autenticado con estructura de sobre: una clave de datos por organización, cifrada con la clave maestra de esa organización en un servicio gestionado de claves respaldado por módulo de hardware. Si un dato llega a un contexto ajeno, el descifrado falla de forma ruidosa                          |
| CEK-05 | ¿Los cambios criptográficos se gestionan?       | Sí        | Claves versionadas: rotar no exige ventana de servicio y cada dato registra con qué versión se cifró                                                                                                                                                                                                          |
| CEK-08 | ¿El Cliente puede gestionar su propia clave?    | Sí        | En el plan Empresa, la clave maestra puede vivir en la cuenta de nube del Cliente. Si el Cliente revoca el permiso, Igniten pierde el acceso a sus datos en el acto                                                                                                                                           |
| CEK-10 | ¿Las claves se generan con fuentes seguras?     | Sí        | Las claves maestras se generan dentro del servicio gestionado de claves y no salen de él                                                                                                                                                                                                                      |
| CEK-12 | ¿Se rotan las claves?                           | Sí        | Rotación automática y periódica de las claves maestras; rotación de las claves de datos sin ventana de servicio                                                                                                                                                                                               |
| CEK-13 | ¿Se pueden revocar?                             | Sí        | La clave de una organización se deshabilita de inmediato, lo que vuelve indescifrable su contenido en el acto                                                                                                                                                                                                 |
| CEK-14 | ¿Se destruyen de forma controlada?              | Sí        | En la baja, la clave de la organización se deshabilita y luego se elimina, con constancia entregada al Cliente                                                                                                                                                                                                |
| CEK-21 | ¿Hay inventario de claves?                      | Sí        | Claves de plataforma declaradas como código; claves por organización registradas en el padrón, una por organización                                                                                                                                                                                           |

## 7. DCS · Seguridad del centro de datos

| ID              | Pregunta                                                                                             | Respuesta | Comentario                                                                                                                                                         |
|-----------------|------------------------------------------------------------------------------------------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DCS-01 a DCS-15 | Seguridad física, control de acceso a instalaciones, condiciones ambientales, eliminación de equipos | N.A.      | Igniten no opera centros de datos. Toda la plataforma corre en Amazon Web Services; los controles físicos son del proveedor y constan en sus informes de auditoría |

## 8. DSP · Seguridad y privacidad de los datos

| ID     | Pregunta                                                  | Respuesta | Comentario                                                                                                                                                                                                                                                                                                                                                                               |
|--------|-----------------------------------------------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DSP-01 | ¿Hay una política de seguridad y privacidad de los datos? | Sí        | Acuerdo de tratamiento de datos y política de privacidad publicados en el centro de confianza, con un buzón atendido para privacidad y seguridad (security@igniten.io)                                                                                                                                                                                                                   |
| DSP-02 | ¿Los datos se eliminan de forma segura?                   | Sí        | Dos mecanismos: destrucción de la clave de la organización, que vuelve indescifrable el contenido en todos los respaldos, y eliminación por procedimiento de los metadatos y vectores, con constancia que indica ambos y su fecha                                                                                                                                                        |
| DSP-03 | ¿Hay un inventario de datos?                              | Sí        | Cada tabla está declarada con su ámbito y su dueño; una compuerta automática rechaza tablas no declaradas                                                                                                                                                                                                                                                                                |
| DSP-04 | ¿Los datos se clasifican?                                 | Sí        | Por columna: contenido (cifrado con la clave de la organización), metadatos estructurales necesarios para la búsqueda (en claro) e identidades de las listas de acceso (guardadas como resumen con la clave de la organización)                                                                                                                                                          |
| DSP-05 | ¿Están documentados los flujos de datos?                  | Sí        | El documento técnico de arquitectura, que se entrega a pedido, describe el flujo lógico de cada dato. La lista de sub-procesadores indica qué recibe cada uno                                                                                                                                                                                                                            |
| DSP-06 | ¿Los datos tienen un responsable asignado?                | Sí        | Todo dato está atribuido a una organización, y el motor de base de datos aplica esa atribución en cada consulta                                                                                                                                                                                                                                                                          |
| DSP-07 | ¿Hay protección de datos desde el diseño?                 | Sí        | Seguridad a nivel de fila forzada en cada tabla, cifrado por organización y batería permanente de pruebas de aislamiento entre organizaciones                                                                                                                                                                                                                                            |
| DSP-08 | ¿Hay privacidad desde el diseño y por defecto?            | Sí        | Permisos pedidos en dos niveles sin superposición; sin el nivel de acción, el producto funciona en modo de solo consulta                                                                                                                                                                                                                                                                 |
| DSP-10 | ¿Las transferencias de datos sensibles se protegen?       | Sí        | TLS en todo trayecto, con verificación de certificado                                                                                                                                                                                                                                                                                                                                    |
| DSP-11 | ¿Los titulares de los datos pueden ejercer sus derechos?  | Sí        | Igniten asiste al responsable con exportación y baja por persona, desconexión de fuentes (que borra su contenido indexado) y borrado de la organización con constancia; la supresión de un dato puntual la hace el Cliente en su sistema de origen. Igniten responde dentro de los plazos de la Ley 25.326: 10 días corridos para acceso y 5 días hábiles para rectificación y supresión |
| DSP-12 | ¿El tratamiento se limita al propósito declarado?         | Sí        | Los datos se tratan solo para prestar el servicio. Igniten no entrena ni afina modelos con ellos                                                                                                                                                                                                                                                                                         |

| ID     | Pregunta                                                                                  | Respuesta | Comentario                                                                                                                                                                                                                                                                                                                                         |
|--------|-------------------------------------------------------------------------------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DSP-14 | ¿Se informa al Cliente sobre sub-procesadores y transferencias?                           | Sí        | Lista publicada con qué recibe cada uno, preaviso de 30 días y derecho de objeción, que se ejerce bloqueando al sub-procesador para esa organización. Transferencias hacia Estados Unidos: desde Argentina, bajo las cláusulas modelo de la AAIP; desde el Espacio Económico Europeo, bajo las cláusulas contractuales tipo de la Comisión Europea |
| DSP-16 | ¿La retención y la eliminación siguen reglas definidas?                                   | Sí        | Contenido: mientras dure el contrato, con la profundidad de histórico contratada. Respaldos: 14 días. Registro de accesos: al menos 365 días. Devolución de datos dentro de los 30 días de la terminación y luego borrado con constancia                                                                                                           |
| DSP-17 | ¿Los datos sensibles se protegen durante todo su ciclo de vida?                           | Sí        | Todo el contenido se cifra con la clave de la organización desde la ingesta hasta la baja                                                                                                                                                                                                                                                          |
| DSP-18 | ¿Hay un procedimiento ante pedidos de autoridades?                                        | Sí        | Igniten solo entrega datos ante una orden de autoridad competente, verifica su validez, entrega el mínimo requerido y notifica al Cliente salvo que la ley lo prohíba                                                                                                                                                                              |
| DSP-19 | ¿Se conoce y se declara la ubicación de los datos?                                        | Sí        | Igniten trata los datos en Estados Unidos: Amazon Web Services, región Norte de Virginia (us-east-1). La región de cada otro sub-procesador la determina ese proveedor, y la lista de sub-procesadores remite a cada uno                                                                                                                           |
| —      | ¿El Cliente puede vetar un proveedor de modelos?                                          | Sí        | El proveedor de modelos es un atributo de la organización: si la organización objeta uno, se bloquea para ella en todo el procesamiento generativo, sin instalación ni precio distintos. El proveedor de incrustaciones es único y figura como tal en la lista de sub-procesadores                                                                 |
| —      | ¿Los proveedores de modelos están obligados a no retener los datos ni entrenar con ellos? | Sí        | Cada proveedor de modelos está contratado con compromiso escrito de retención cero y de no entrenamiento. Solo recibe el fragmento necesario para la petición en curso                                                                                                                                                                             |

## 9. GRC · Gobierno, riesgo y cumplimiento

| ID     | Pregunta                                              | Respuesta | Comentario                                                                                            |
|--------|-------------------------------------------------------|-----------|-------------------------------------------------------------------------------------------------------|
| GRC-01 | ¿Hay un programa de gobierno con políticas revisadas? | Sí        | Diez políticas escritas (ver sección 20), con responsable y revisión trimestral                       |
| GRC-02 | ¿Hay un programa de gestión de riesgos?               | Sí        | Parte del modelo de amenazas; cada riesgo se trata, se transfiere o se acepta por escrito y con fecha |
| GRC-03 | ¿Las políticas se revisan periódicamente?             | Sí        | Cada trimestre, y cuando cambia un control que citan                                                  |

| ID     | Pregunta                                               | Respuesta | Comentario                                                                                                                                                                                                                                                                                                                                                          |
|--------|--------------------------------------------------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GRC-04 | ¿Hay un proceso de excepciones a las políticas?        | Sí        | Excepciones con vencimiento escrito y compuerta automática (ver CCC-08)                                                                                                                                                                                                                                                                                             |
| GRC-05 | ¿Hay un programa de seguridad de la información?       | Sí        | Cada control publicado tiene un criterio de verificación medible                                                                                                                                                                                                                                                                                                    |
| GRC-06 | ¿Están definidas las responsabilidades de gobierno?    | Sí        | Cada política nombra a su responsable                                                                                                                                                                                                                                                                                                                               |
| GRC-07 | ¿Se identifican los requisitos legales y regulatorios? | Sí        | Contratos regidos por las leyes del Estado de Wyoming. Protección de datos según la norma imperativa del titular: Ley 25.326 y su reglamentación, con la Agencia de Acceso a la Información Pública (AAIP) como autoridad de control, y el RGPD cuando aplica. Transferencias con cláusulas modelo de la AAIP y cláusulas contractuales tipo de la Comisión Europea |
| GRC-08 | ¿Hay contacto con grupos de interés y con autoridades? | Sí        | Contacto con la AAIP como autoridad de control; buzón de seguridad publicado para la divulgación de vulnerabilidades; autoevaluación en el registro público CSA STAR                                                                                                                                                                                                |

## 10. HRS · Seguridad de recursos humanos

| ID     | Pregunta                                            | Respuesta | Comentario                                                                                                                                                                                                                                                     |
|--------|-----------------------------------------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HRS-01 | ¿Se verifican los antecedentes?                     | Sí        | Antes del alta, en la medida en que la ley lo permite                                                                                                                                                                                                          |
| HRS-02 | ¿Hay una política de uso aceptable?                 | Sí        | Política de uso aceptable y de activos: cuentas y credenciales personales, segundo factor obligatorio, secretos solo en gestores, datos de clientes nunca descargados ni usados en herramientas fuera de la lista de sub-procesadores. Se firma antes del alta |
| HRS-03 | ¿Hay una política de escritorio y pantalla limpios? | Sí        | Bloqueo automático del equipo a los 5 minutos, pantalla compartida por ventana, sin secretos en papel ni información de clientes impresa. Se verifica en el chequeo trimestral de equipos                                                                      |
| HRS-04 | ¿Hay una política de trabajo remoto?                | Sí        | Requisitos mínimos del equipo (cifrado de disco, actualizaciones, bloqueo, protección contra software malicioso, firewall), prohibición de equipos compartidos, procedimiento ante pérdida o robo y chequeo trimestral con evidencia                           |

| ID     | Pregunta                                                          | Respuesta | Comentario                                                                                                                                                                                                                             |
|--------|-------------------------------------------------------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HRS-05 | ¿Se devuelven los activos al terminar la relación?                | Sí        | El mismo día de la baja: revocación de todas las credenciales con verificación por efecto, devolución de todo activo físico entregado y borrado de la información de Igniten y de clientes en equipos propios, con declaración firmada |
| HRS-06 | ¿Hay un procedimiento de baja?                                    | Sí        | El mismo día, en orden fijo y con constancia: credenciales de nube, código, correo e identidad, panel, y rotación de todo secreto que la persona conoció                                                                               |
| HRS-07 | ¿Los acuerdos con el personal incluyen obligaciones de seguridad? | Sí        | Acuerdo de confidencialidad y lectura de las políticas, con constancia, antes del alta                                                                                                                                                 |
| HRS-09 | ¿Están definidos los roles de seguridad del personal?             | Sí        | Roles de respuesta a incidentes con titular y suplente, nombrados de antemano                                                                                                                                                          |
| HRS-10 | ¿Hay acuerdos de confidencialidad?                                | Sí        | Firmados antes del alta                                                                                                                                                                                                                |
| HRS-11 | ¿Hay capacitación en seguridad?                                   | Sí        | Al ingresar y una vez por año                                                                                                                                                                                                          |
| HRS-12 | ¿El personal con acceso a datos recibe capacitación específica?   | Sí        | Incluye el procedimiento de acceso de emergencia y sus obligaciones de registro y aviso                                                                                                                                                |

## 11. IAM · Gestión de identidad y acceso

| ID     | Pregunta                                   | Respuesta | Comentario                                                                                                                                                                                                                                                                  |
|--------|--------------------------------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IAM-01 | ¿Hay una política de identidad y acceso?   | Sí        | Política de control de accesos (ver sección 20)                                                                                                                                                                                                                             |
| IAM-02 | ¿Hay una política de contraseñas robustas? | Sí        | Cada usuario del panel tiene usuario y contraseña propios en un servicio gestionado de identidad, que custodia la contraseña, con segundo factor obligatorio. En el plan Empresa, el acceso puede además federarse contra el proveedor de identidad corporativo del Cliente |
| IAM-03 | ¿Hay un inventario de identidades?         | Sí        | Padrón de administradores por organización, dueños de código declarados y roles de nube declarados como código                                                                                                                                                              |
| IAM-04 | ¿Hay separación de funciones?              | Sí        | Quien despliega el sistema no puede leer datos de clientes. Son permisos distintos, en manos distintas                                                                                                                                                                      |
| IAM-05 | ¿Se aplica el mínimo privilegio?           | Sí        | La aplicación se conecta a la base con un rol que no es dueño de ninguna tabla; cada servicio recibe solo los secretos que necesita                                                                                                                                         |

| ID     | Pregunta                                                   | Respuesta | Comentario                                                                                                                                                                                                                 |
|--------|------------------------------------------------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IAM-06 | ¿Hay un proceso de alta de accesos?                        | Sí        | Se otorga lo que la función pide, siempre con segundo factor y sin acceso permanente a datos de clientes                                                                                                                   |
| IAM-07 | ¿Los accesos se revocan a tiempo?                          | Sí        | El mismo día de la baja; los accesos temporales vencen solos                                                                                                                                                               |
| IAM-08 | ¿Se revisan los accesos periódicamente?                    | Sí        | Revisión trimestral con acta                                                                                                                                                                                               |
| IAM-09 | ¿Los roles privilegiados están segregados?                 | Sí        | El acceso administrativo se obtiene solo asumiendo un rol con segundo factor; ninguna identidad permanente tiene acceso a datos de producción                                                                              |
| IAM-10 | ¿El acceso privilegiado está acotado en el tiempo?         | Sí        | Cero acceso permanente. El acceso a datos se solicita con justificación escrita, se otorga por una ventana acotada y vence solo                                                                                            |
| IAM-11 | ¿El Cliente se entera del acceso privilegiado a sus datos? | Sí        | Cada concesión genera un aviso a todos los administradores de la organización, y el registro está en su panel. Una conciliación automática detecta cualquier acceso sin concesión, que dispara una alarma y el mismo aviso |
| IAM-12 | ¿Los registros de acceso son inmutables?                   | Sí        | Se escriben en almacenamiento con bloqueo de objeto en modo cumplimiento: ni la cuenta administradora de Igniten puede borrarlos ni acortar su retención. A pedido, se exportan al sistema de vigilancia del Cliente       |
| IAM-13 | ¿Los usuarios se identifican de forma única?               | Sí        | La autorización se resuelve contra el padrón propio por el par organización y dirección de correo, nunca por la dirección sola                                                                                             |
| IAM-14 | ¿Hay autenticación fuerte?                                 | Sí        | Segundo factor obligatorio en todas las cuentas de Igniten (nube, código y correo) y en todas las cuentas del panel                                                                                                        |
| IAM-15 | ¿Las credenciales se gestionan de forma segura?            | Sí        | Secretos en un gestor de secretos, nunca en el código ni en las imágenes. Las credenciales de integración del Cliente son de solo escritura: la interfaz no puede devolverlas                                              |
| IAM-16 | ¿Se autoriza el acceso a sistemas y funciones?             | Sí        | Control de acceso en dos capas: habilitación de la persona y permisos por tabla y columna. El proveedor de identidad autentica; nunca autoriza                                                                             |

## 12. IPY · Interoperabilidad y portabilidad

| ID     | Pregunta                                               | Respuesta | Comentario                                                                                             |
|--------|--------------------------------------------------------|-----------|--------------------------------------------------------------------------------------------------------|
| IPY-01 | ¿Hay una política de interoperabilidad y portabilidad? | Sí        | Los compromisos de servicio y el acuerdo de tratamiento de datos cubren la exportación y la devolución |

| ID     | Pregunta                                                   | Respuesta | Comentario                                                                                                                                                                                                                            |
|--------|------------------------------------------------------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IPY-02 | ¿Las interfaces para obtener los datos son estándar?       | Sí        | Exportación autogestionada desde el panel, en un formato abierto y legible, con un manifiesto de conteos                                                                                                                              |
| IPY-03 | ¿Las interfaces de gestión son seguras?                    | Sí        | Usuario y contraseña propios con segundo factor obligatorio, o federación con el proveedor de identidad del Cliente en el plan Empresa; sesión regenerada al iniciar, cookies atadas al host exacto e inaccesibles desde el navegador |
| IPY-04 | ¿El contrato cubre la devolución de los datos al terminar? | Sí        | Devolución en formato exportable dentro de los 30 días de la terminación, y luego borrado con constancia                                                                                                                              |

### 13. IVS · Seguridad de infraestructura y virtualización

| ID     | Pregunta                                           | Respuesta | Comentario                                                                                                                                                                                       |
|--------|----------------------------------------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IVS-01 | ¿Hay una política de seguridad de infraestructura? | Sí        | Infraestructura declarada como código y revisada por el circuito de cambios                                                                                                                      |
| IVS-02 | ¿Se planifica la capacidad?                        | Sí        | Almacenamiento con crecimiento automático y alarmas de capacidad sobre la base, el balanceador y los servicios                                                                                   |
| IVS-03 | ¿La red está segmentada y monitoreada?             | Sí        | La base de datos no tiene ruta a internet; los servicios no tienen dirección pública; detección de amenazas activa con alertas a personas                                                        |
| IVS-04 | ¿Los sistemas están endurecidos?                   | Sí        | Imágenes mínimas fijadas por huella; usuario sin privilegios y sistema de archivos de solo lectura en los componentes expuestos a contenido del Cliente                                          |
| IVS-06 | ¿Los entornos de los clientes están segregados?    | Sí        | La separación la aplica el motor de base de datos, con seguridad a nivel de fila forzada; una consulta sin contexto de organización devuelve cero filas. Segunda línea: cifrado por organización |
| IVS-07 | ¿Las migraciones a la nube son seguras?            | N.A.      | Igniten no migra sistemas de clientes a su nube                                                                                                                                                  |
| IVS-08 | ¿Hay protección en el perímetro?                   | Sí        | Cortafuegos de aplicaciones web con reglas gestionadas y límite de tasa                                                                                                                          |
| IVS-09 | ¿Se defiende contra ataques de red?                | Sí        | Cortafuegos de aplicaciones web y detección de amenazas con alertas a personas                                                                                                                   |

## 14. LOG · Registro y monitoreo

| ID     | Pregunta                                           | Respuesta | Comentario                                                                                                                                |
|--------|----------------------------------------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------|
| LOG-01 | ¿Hay una política de registro y monitoreo?         | Sí        | Definida en las políticas de control de accesos y de respuesta a incidentes                                                               |
| LOG-02 | ¿Los registros de auditoría se protegen?           | Sí        | Almacenamiento con bloqueo de objeto en modo cumplimiento                                                                                 |
| LOG-03 | ¿Hay monitoreo y alertas de seguridad?             | Sí        | Hallazgos de detección de amenazas, acciones sensibles sobre la cuenta de nube y alarmas operativas llegan a personas                     |
| LOG-04 | ¿El acceso a los registros está restringido?       | Sí        | Solo roles con segundo factor; el registro de accesos no lo puede borrar ninguna cuenta de Igniten                                        |
| LOG-05 | ¿Se revisan los registros y se responde?           | Sí        | Conciliación automática periódica de todo acceso humano contra las concesiones; un acceso sin concesión dispara alarma y aviso al Cliente |
| LOG-06 | ¿Los relojes están sincronizados?                  | Sí        | Servicios gestionados del proveedor de nube, con su sincronización de hora                                                                |
| LOG-07 | ¿Está definido el alcance del registro?            | Sí        | Incluye la auditoría a nivel de motor de base de datos para toda sesión humana o de emergencia                                            |
| LOG-08 | ¿Los registros tienen la información necesaria?    | Sí        | Registros estructurados con organización y procedencia                                                                                    |
| LOG-09 | ¿Los registros están protegidos contra alteración? | Sí        | Registro de actividad de la cuenta de nube en todas las regiones, con validación de integridad, y auditoría en almacenamiento inmutable   |
| LOG-10 | ¿Se registran las operaciones con claves?          | Sí        | Toda operación del servicio gestionado de claves queda registrada                                                                         |
| LOG-11 | ¿Se registran las transacciones?                   | Sí        | Registro propio de llamadas a modelos, auditoría de consultas y auditoría a nivel de motor                                                |
| LOG-12 | ¿Se registran los accesos físicos?                 | N.A.      | Heredado del proveedor de nube                                                                                                            |
| LOG-13 | ¿Se reportan las fallas y anomalías?               | Sí        | Alarmas sobre base de datos, balanceador, servicios y tareas fallidas, con aviso a personas                                               |

## 15. SEF · Gestión de incidentes, e-discovery y forense

| ID     | Pregunta                                    | Respuesta | Comentario                                               |
|--------|---------------------------------------------|-----------|----------------------------------------------------------|
| SEF-01 | ¿Hay una política de gestión de incidentes? | Sí        | Procedimiento de respuesta a incidentes (ver sección 20) |

| ID     | Pregunta                                            | Respuesta | Comentario                                                                                                                                                                                                        |
|--------|-----------------------------------------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SEF-02 | ¿Hay gestión de servicio para incidentes?           | Sí        | Un incidente de severidad 1 se atiende de inmediato, a cualquier hora                                                                                                                                             |
| SEF-03 | ¿Hay un plan de respuesta con responsables?         | Sí        | Roles nombrados de antemano, cada uno con titular y suplente: quién decide, quién contiene, quién redacta, quién avisa y quién sostiene el plazo                                                                  |
| SEF-04 | ¿El plan se prueba?                                 | Sí        | Simulacros con escenario no anunciado, incluido uno con el titular ausente                                                                                                                                        |
| SEF-05 | ¿Hay métricas de incidentes?                        | Sí        | Cada incidente queda registrado con su severidad y su cronología. Un reporte mensual automático calcula la cantidad por severidad y los tiempos de detección, contención y resolución, y se revisa cada trimestre |
| SEF-06 | ¿Hay un proceso de clasificación?                   | Sí        | Tres severidades. Una filtración entre organizaciones es siempre severidad 1, cualquiera sea su volumen                                                                                                           |
| SEF-07 | ¿Se notifica a los afectados en plazo?              | Sí        | Sin demora indebida y a más tardar dentro de las 72 horas desde que se toma conocimiento, a todos los administradores de cada organización afectada                                                               |
| SEF-08 | ¿Se mantienen contactos con las autoridades?        | Sí        | AAIP como autoridad de control; la notificación a la autoridad la decide el rol designado dentro del mismo plazo                                                                                                  |
| —      | ¿Se puede aislar a un cliente durante un incidente? | Sí        | Corte por organización que suspende a una sin afectar a ninguna otra. Secuencia fija: contener, preservar evidencia, reparar                                                                                      |

## 16. STA · Cadena de suministro, transparencia y responsabilidad

| ID     | Pregunta                                                  | Respuesta | Comentario                                                                                                                                                                     |
|--------|-----------------------------------------------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| STA-01 | ¿Hay una política de responsabilidad compartida?          | Sí        | Igniten publica qué controles son suyos y cuáles quedan del lado del Cliente, con una guía de configuración de mínimo privilegio                                               |
| STA-02 | ¿Se aplica el modelo de responsabilidad compartida?       | Sí        | Aplicaciones registradas en el directorio del Cliente, lista de destinos del conector editable solo por el Cliente y clave maestra en la cuenta del Cliente en el plan Empresa |
| STA-05 | ¿Hay documentación del modelo compartido para el Cliente? | Sí        | Páginas de seguridad y de recomendaciones, y la ficha técnica del conector                                                                                                     |
| STA-07 | ¿Hay un inventario de la cadena de suministro?            | Sí        | La lista de sub-procesadores se deriva del código, y una compuerta automática impide sumar un proveedor sin clasificarlo                                                       |

| ID     | Pregunta                                            | Respuesta | Comentario                                                                                                                                                 |
|--------|-----------------------------------------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| STA-08 | ¿Se gestionan los riesgos de la cadena?             | Sí        | Imágenes firmadas con inventario de componentes, imágenes base y acciones de integración fijadas por huella, y actualizaciones automáticas de dependencias |
| STA-09 | ¿Los contratos con proveedores cubren la seguridad? | Sí        | Acuerdos de tratamiento de datos con cada sub-procesador, y compromiso escrito de retención cero y no entrenamiento de cada proveedor de modelos           |
| STA-10 | ¿Se revisan los acuerdos con proveedores?           | Sí        | Revisión trimestral, y antes de sumar cualquier proveedor                                                                                                  |
| STA-12 | ¿Se verifica el cumplimiento de los proveedores?    | Sí        | Revisión trimestral de sus informes de auditoría vigentes y de los cambios en sus términos                                                                 |
| STA-14 | ¿Se evalúa la seguridad de los datos en la cadena?  | Sí        | Antes de integrar un proveedor se registra qué dato recibe, en qué región, qué certificaciones tiene y qué compromete sobre entrenamiento y retención      |

## 17. TVM · Gestión de amenazas y vulnerabilidades

| ID     | Pregunta                                                    | Respuesta | Comentario                                                                                                                         |
|--------|-------------------------------------------------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------|
| TVM-01 | ¿Hay una política de gestión de vulnerabilidades?           | Sí        | Parte del ciclo de vida de desarrollo seguro                                                                                       |
| TVM-02 | ¿Hay protección contra software malicioso?                  | Sí        | Evaluación del contenido en la ingesta, análisis de planillas sin ejecución de código y detección de amenazas en la cuenta de nube |
| TVM-03 | ¿Hay plazos de remediación?                                 | Sí        | Ver AIS-07                                                                                                                         |
| TVM-04 | ¿Se actualizan las herramientas de detección?               | Sí        | Actualizaciones automáticas de dependencias y de herramientas en todos los repositorios                                            |
| TVM-05 | ¿Se gestionan las vulnerabilidades de bibliotecas externas? | Sí        | Análisis de dependencias en cada cambio y barrido semanal, con triage semanal                                                      |
| TVM-06 | ¿Se hacen pruebas de penetración?                           | Sí        | Prueba de penetración externa, con el conector incluido, y pruebas dinámicas automatizadas semanales                               |
| TVM-07 | ¿Se identifican vulnerabilidades periódicamente?            | Sí        | Barrido semanal del código y escaneo continuo de las imágenes                                                                      |
| TVM-08 | ¿Se priorizan por riesgo?                                   | Sí        | Por severidad, con los plazos de AIS-07                                                                                            |

| ID     | Pregunta                               | Respuesta | Comentario                                                                                                                                                                                                |
|--------|----------------------------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TVM-09 | ¿Se reportan a las partes interesadas? | Sí        | Política de divulgación de vulnerabilidades publicada y buzón de seguridad declarado en el archivo estándar del sitio                                                                                     |
| TVM-10 | ¿Hay métricas de vulnerabilidades?     | Sí        | Un reporte mensual automático calcula las vulnerabilidades abiertas por severidad, el tiempo medio de remediación y el porcentaje resuelto dentro del plazo de cada severidad, y se revisa cada trimestre |

## 18. UEM · Gestión de dispositivos de usuario

| ID              | Pregunta                                                                                                   | Respuesta | Comentario                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------|------------------------------------------------------------------------------------------------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UEM-01 a UEM-14 | Política de dispositivos, inventario, cifrado de disco, antimalware, borrado remoto y gestión centralizada | Sí        | Política de trabajo remoto y equipos, aplicada con gestión centralizada de dispositivos: inventario, cifrado de disco, actualizaciones, bloqueo automático, protección contra software malicioso y borrado remoto, con reporte de cumplimiento por equipo. Además, todo acceso administrativo exige segundo factor y credenciales de corta vida, y los datos de clientes no se descargan a los equipos de trabajo |

## 19. Resumen de respuestas

| Respuesta | Filas |
|-----------|-------|
| Sí        | 151   |
| No        | 0     |
| N.A.      | 3     |

Contado sobre las filas de las secciones 2 a 18. Los dominios DCS y UEM cuentan como una fila cada uno.

## 20. Las políticas que respaldan estas respuestas

Igniten mantiene diez políticas escritas. Cada una nombra a su responsable, dice dónde está el control que la hace cumplir y se revisa cada trimestre.

| Política           | Qué cubre                                                                                                                                                                                      | Dominio CCM |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| Control de accesos | Cero acceso permanente a datos de clientes, acceso efímero con justificación, aviso y registro, separación entre desplegar y leer, segundo factor obligatorio y revisión trimestral de accesos | IAM         |

| Política                      | Qué cubre                                                                                                                                                                         | Dominio CCM |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| Gestión de cambios            | Solicitud de cambio con aprobación de otra persona, compuertas automáticas, imágenes firmadas por huella, despliegue sobre etiqueta firmada, cambios de emergencia y vuelta atrás | CCC, AIS    |
| Continuidad y respaldo        | RespalDOS cifrados, réplica en una segunda zona, recuperación a un punto en el tiempo, ensayos trimestrales de restauración y custodia de las claves                              | BCR         |
| Gestión de riesgos            | Modelo de amenazas, registro de riesgos con medición y criterio de cierre, aceptación por escrito y evaluación independiente                                                      | GRC, A&A    |
| Gestión de proveedores        | Lista de sub-procesadores derivada del código, alta y revisión de proveedores, compromisos de los proveedores de modelos y veto por organización                                  | STA         |
| Recursos humanos              | Requisitos previos al alta, otorgamiento de accesos con segundo factor, baja el mismo día con constancia y baja de personas de un cliente                                         | HRS         |
| Uso aceptable y activos       | Uso de cuentas y credenciales, tratamiento de datos de clientes, lo prohibido, devolución de activos y borrado al terminar la relación                                            | HRS         |
| Escritorio y pantalla limpios | Bloqueo automático y manual, pantalla en lugares públicos, papel y llaves de seguridad                                                                                            | HRS         |
| Trabajo remoto y equipos      | Requisitos mínimos de cada equipo, conexión, pérdida o robo y chequeo trimestral con evidencia                                                                                    | HRS, UEM    |
| Respuesta a incidentes        | Responsables nombrados, clasificación por severidad, contener antes de reparar, corte por organización, notificación en 72 horas y simulacros                                     | SEF         |