Documentos legales y de confianza

Dónde encontrar los acuerdos y la documentación de confianza de Cyber Crucible: acuerdo mutuo de confidencialidad (NDA), MSA y EULA, acuerdo de nivel de servicio, acuerdos de procesamiento de datos y evidencia de cumplimiento.

¿Dónde puedo encontrar los documentos legales y de confianza de Cyber Crucible?

Respuesta breve: Los acuerdos públicos se publican en cybercrucible.com — el Acuerdo Mutuo de Confidencialidad (NDA), el MSA y el EULA, el Acuerdo de Nivel de Servicio, la Política de Privacidad y las Condiciones de Servicio. La documentación de cumplimiento que se proporciona a solicitud — las Cláusulas Contractuales Estándar, la Evaluación de Riesgo de Transferencia y los Acuerdos de Procesamiento de Datos — se obtiene a través de **dpo@cybercrucible.com**.

Disponible públicamente

Documento	Ubicación
Acuerdo Mutuo de Confidencialidad (NDA)	cybercrucible.com/mutualNDA
Acuerdo Marco de Servicios y EULA	cybercrucible.com/msa-and-eula
Acuerdo de Nivel de Servicio	cybercrucible.com/service-level-agreement
Política de Privacidad	cybercrucible.com/privacy-policy
Condiciones de Servicio	cybercrucible.com/terms-of-service

Proporcionado a solicitud

Contacte a **dpo@cybercrucible.com** para:

- Cláusulas Contractuales Estándar, incluidas las cláusulas preaprobadas por la SDAIA para las transferencias saudíes
- Evaluación de Riesgo de Transferencia
- Acuerdo de Procesamiento de Datos
- Documentación de la política de gobernanza y uso compartido de datos

Estos se proporcionan sujetos a medidas de confidencialidad razonables.

Por qué vale la pena leerlos antes de la adquisición

Los proveedores de seguridad son inusuales en el sentido de que el producto se ejecuta con los privilegios más profundos en sus sistemas, y el contrato rige lo que el proveedor puede hacer con lo que ve. Los acuerdos anteriores definen ambos aspectos. El material de gobernanza de datos, en particular, responde a la pregunta que la mayoría de los cuestionarios de seguridad plantean de manera indirecta: *¿qué recopila realmente este proveedor y a dónde va esa información?*

¿Qué es el Acuerdo Mutuo de Confidencialidad (NDA) de Cyber Crucible, y quién está obligado por él?

Respuesta breve: Es un acuerdo mutuo de confidencialidad vinculante que todo empleado, contratista y proveedor de Cyber Crucible con acceso potencial a los datos operativos del cliente o a los sistemas de gestión debe suscribir **antes de la incorporación**. Está publicado en cybercrucible.com/mutualNDA.

Quién lo firma

Todo el personal con acceso potencial a los datos operativos del cliente o a los sistemas de gestión queda legalmente obligado antes de la incorporación. Esto incluye a empleados, contratistas y proveedores, no solo al personal interno.

Por qué importa que sea "mutuo"

Un acuerdo de confidencialidad unidireccional protege únicamente al proveedor. Un acuerdo mutuo obliga a Cyber Crucible a proteger *su* información confidencial en los mismos términos que espera para la propia. Para un proveedor de seguridad cuyo personal puede tener visibilidad de detalles operativos de su entorno, esa simetría es precisamente el objetivo.

Cómo encaja con los demás controles

El NDA constituye la capa contractual de una postura más amplia frente al riesgo interno:

- **Contractual** — acuerdo mutuo de confidencialidad vinculante antes de otorgar cualquier acceso.
- **Acceso** — el acceso administrativo a las instancias de gestión del cliente se restringe a personal verificado, estrictamente bajo el principio de necesidad de saber, y solo cuando se requiere para una operación de negocio o soporte validada.

- **Desvinculación** — si algún proveedor, vendedor, contratista o empleado representa un riesgo de seguridad, privacidad o propiedad intelectual, Cyber Crucible gestiona y aísla activamente ese riesgo o desvincula al recurso de inmediato.

El NDA establece la obligación. Los controles de acceso limitan cuánto podría llegar a hacer un mal uso cualquier persona en particular. El mandato de desvinculación es lo que hace que ambos sean efectivamente aplicables en la práctica.

¿Qué cubren el MSA y el EULA?

Respuesta breve: El Acuerdo Maestro de Servicios (Master Services Agreement) rige la relación comercial: servicios, obligaciones, responsabilidad y vigencia. El Acuerdo de Licencia de Usuario Final (End User License Agreement) rige el uso del software en sí, incluido el alcance de la licencia, que se aplica al código objeto compilado y no al código fuente.

Puntos clave que conviene conocer antes de firmar

- **Alcance de la licencia** — los derechos otorgados se aplican a la forma de código objeto compilado del software. El acuerdo no otorga derechos para obtener o usar el código fuente.
- **Sin licencias implícitas** — Cyber Crucible conserva todo derecho, título e interés sobre los servicios, la documentación y la propiedad intelectual asociada. No se otorga nada de manera implícita.
- **Servicios de implementación** — la configuración, la personalización, la capacitación de personal o el soporte técnico se establecen en un Formulario de Pedido (Order Form) en lugar de presuponerse.
- **Confidencialidad** — ambas partes pueden tener acceso a la información confidencial de la otra; cada una sigue siendo propiedad de la parte que la divulga.

Dónde consultarlo

El acuerdo completo está publicado en cybercrucible.com/msa-and-eula. Esta página es un resumen de orientación, no un sustituto; el acuerdo publicado es el que rige.

¿Qué cubre el Acuerdo de Nivel de Servicio?

Respuesta breve: El SLA define los compromisos de servicio que Cyber Crucible asume con los clientes: disponibilidad, capacidad de respuesta del soporte y los términos asociados. Se publica en cybercrucible.com/service-level-agreement.

Cómo se relaciona el SLA con el diseño del producto

Vale la pena señalar, para quien esté evaluando: dado que la prevención ocurre de forma autónoma en el endpoint, típicamente en menos de 200 milisegundos, la protección no depende de la disponibilidad del servicio de la misma manera que un producto de análisis en la nube.

Un endpoint cuyo servidor de administración es inalcanzable —o que está deliberadamente aislado (air-gapped)— sigue estando totalmente protegido. La evaluación de amenazas y la interdicción de procesos son locales. La disponibilidad del plano de administración afecta la generación de informes y la administración, no la defensa.

Esa es una distinción importante al comparar SLAs entre proveedores. Para una herramienta dependiente de la nube, el tiempo de inactividad del plano de administración puede significar protección reducida o inexistente. Aquí no es así.

Dónde leerlo

El acuerdo completo está disponible en cybercrucible.com/service-level-agreement. Los compromisos de capacidad de respuesta del soporte y cualquier término específico del entorno deben confirmarse con su representante de Cyber Crucible.

¿Cómo completo un cuestionario de seguridad o una evaluación de riesgo de proveedores para Cyber Crucible?

Respuesta breve: la mayoría de las preguntas se responden con el material de gobernanza de datos: qué se recopila, qué nunca se recopila, cómo se protege en tránsito, dónde se procesa y qué modelos de implementación están disponibles. Para cualquier asunto que requiera documentación firmada, contacte con **dpo@cybercrucible.com**.

Las respuestas que necesitan la mayoría de los cuestionarios

Pregunta típica	Dónde se responde
¿Qué datos de clientes recopila el proveedor?	*¿Qué datos recopila Cyber Crucible, y qué datos nunca recopila?*
¿Se comparten o venden datos a terceros?	*¿Cyber Crucible vende o comparte datos de clientes con terceros?*
¿Cómo se cifran los datos en tránsito?	*¿Cómo se protegen los datos de Cyber Crucible en tránsito?*
¿Dónde se procesan y almacenan los datos?	*¿Dónde se procesan mis datos, y pueden permanecer dentro de mi país?*
¿Subencargados y controles de la cadena de suministro?	*¿Cómo gestiona Cyber Crucible el riesgo de la cadena de suministro y el riesgo interno?*
¿Componentes de código de terceros o extranjeros?	*¿Cyber Crucible incorpora bibliotecas de terceros o código de origen extranjero?*
¿Rol de responsable o encargado del tratamiento?	*¿Cyber Crucible es un responsable del tratamiento o un encargado del tratamiento de datos?*

Pregunta típica	Dónde se responde
¿Mecanismo de transferencia transfronteriza de datos?	*¿Cómo se gestionan las transferencias transfronterizas de datos?*

Dos respuestas que suelen sorprender a los revisores

Sobre certificaciones: el programa de seguridad de Cyber Crucible está alineado con marcos reconocidos de la industria, pero **actualmente no cuenta con la certificación ISO 27001 ni SOC 2**. Si su proceso requiere evidencia certificada, plantéelo con antelación en lugar de al final.

Sobre la divulgación de datos: dado que las claves de cifrado, las credenciales y los archivos de los clientes nunca se recopilan, no hay nada en esas categorías que divulgar a ninguna parte, incluso bajo requerimiento legal. Varios puntos de los cuestionarios sobre divulgación, retención y eliminación se responden por la ausencia de recopilación, en lugar de por un control.

Cualquier aspecto no cubierto

Contacte con **dpo@cybercrucible.com** indicando el requisito específico, su jurisdicción y el modelo de implementación que está evaluando.