Diligencia Debida del Proveedor y Confianza en la Seguridad

Cómo Cyber Crucible responde a los cuestionarios de riesgo de proveedores para empresas e instituciones financieras: qué datos conserva y cuáles no, cómo respalda las obligaciones regulatorias, cómo se gobierna la IA, los niveles de servicio y cómo su arquitectura reduce el riesgo de terceros. Expuesto de forma clara y honesta.

¿Cuenta Cyber Crucible con un informe SOC 2?

Respuesta breve: No. Cyber Crucible no cuenta actualmente con una certificación SOC 2, y lo indica con claridad en lugar de dar a entender lo contrario. El motivo es arquitectónico: Cyber Crucible es un producto de software que se ejecuta localmente, no un custodio en la nube de los datos del cliente, por lo que el modelo de organización de servicios de SOC 2 —que certifica cómo un proveedor almacena, procesa y transmite *sus* datos en sus propios sistemas— no se aplica de forma directa en este caso.

Por qué la mayoría de los clientes no lo han requerido

SOC 2 certifica los controles de una organización de servicios que custodia datos del cliente. El diseño de Cyber Crucible elimina esa premisa:

- La detección y respuesta ante amenazas se ejecutan en el endpoint, a nivel de kernel, en el propio dispositivo del cliente.
- Cyber Crucible nunca recopila, transmite ni almacena archivos, credenciales, claves de cifrado ni tokens de sesión del cliente.
- La plataforma puede implementarse completamente en las instalaciones del cliente o de forma aislada (air-gapped), dentro de su propia infraestructura.

Dado que las categorías de datos de mayor riesgo nunca están bajo la custodia de Cyber Crucible, gran parte de la superficie de riesgo de proveedores que un SOC 2 pretende abordar se elimina por diseño, en lugar de simplemente controlarse.

Qué se ofrece en su lugar

Para los evaluadores que trabajan con un cuestionario, Cyber Crucible proporciona un paquete de seguridad para proveedores previamente preparado que aporta directamente la evidencia de los controles subyacentes, y relaciona sus controles con los Criterios de Servicios de Confianza (Trust-Service Criteria) de SOC 2 y con el NIST Cybersecurity Framework, de modo que un evaluador pueda completar un cuestionario estándar a partir de él. El paquete está disponible bajo un acuerdo de confidencialidad mutuo (NDA) escribiendo a **dpo@cybercrucible.com**.

La hoja de ruta de aseguramiento se mantiene bajo evaluación conforme a las necesidades de los clientes; esta página se actualizará si dicha postura cambia.

¿Cuenta Cyber Crucible con certificación ISO 27001, PCI-DSS, CMMC o FedRAMP?

Respuesta breve: No. Cyber Crucible no ha obtenido, ni afirma tener, certificación o autorización ISO/IEC 27001, PCI-DSS, HIPAA, CMMC o FedRAMP. Esto se indica de manera directa, ya que afirmar poseer una certificación que un proveedor no tiene es precisamente el tipo de inconsistencia que socava la confianza en una revisión de debida diligencia.

Qué significa esto en la práctica

- **PCI-DSS:** Cyber Crucible no procesa, almacena ni transmite datos de titulares de tarjetas, por lo que queda fuera del alcance como procesador de datos de tarjetas, al tiempo que sigue respaldando los objetivos de control de seguridad de endpoints del cliente.
- **HIPAA:** dado que no se recopila contenido del cliente, Cyber Crucible evita crear una relación de custodia de información de salud protegida; se puede ejecutar un Acuerdo de Asociado Comercial (Business Associate Agreement) cuando un cliente lo requiera.
- **ISO 27001 / CMMC / FedRAMP:** no se poseen, ni se representan como poseídos.

Qué posee Cyber Crucible

Existe una validación independiente y objetiva donde más importa; consulte *What independent security validation does Cyber Crucible have?* (¿Qué validación de seguridad independiente tiene Cyber Crucible?). Las referencias a marcos de referencia en otras partes de esta base de conocimientos son mapeos autoevaluados que ayudan a un revisor a relacionar los controles de Cyber Crucible con un estándar que ya utiliza; no constituyen opiniones de auditoría de terceros.

¿Qué validación de seguridad independiente tiene Cyber Crucible?

Respuesta breve: Los controladores del kernel de Windows de Cyber Crucible se someten a pruebas objetivas y se firman criptográficamente bajo el Windows Hardware Compatibility Program (WHCP) de Microsoft. Se trata de una certificación externa e independiente de la calidad y la resistencia a la manipulación del componente más privilegiado del producto: el código en el que la corrección es más crítica.

Por qué el WHCP es relevante

La mayor parte del mercado de endpoints evitó el desarrollo a nivel de kernel porque es genuinamente difícil y costoso. Cyber Crucible opera deliberadamente en el kernel y somete sus controladores al programa de Microsoft para que una parte externa —no solo Cyber Crucible— valide que el código más sensible es correcto y resistente a la manipulación.

- La validación está **acotada específicamente al controlador**, y no se presenta como una certificación del producto en su conjunto.
- Se trata de una prueba objetiva y repetible, en lugar de una auditoría administrativa subjetiva.

Cómo encaja en el panorama general

Para un revisor acostumbrado a buscar un informe SOC 2, el WHCP es un dato concreto e independiente que un SOC 2 no proporciona: la validación directa del componente del kernel. Complementa —en lugar de reemplazar— la evidencia de controles incluida en el paquete para proveedores preparado por Cyber Crucible.

¿Cómo respalda Cyber Crucible los requisitos de GLBA y de proveedores de instituciones financieras?

Respuesta breve: Como proveedor de servicios de software para una institución financiera, Cyber Crucible respalda las obligaciones de la institución bajo las expectativas de las Safeguards Rule de GLBA y las directrices interagenciales de seguridad de la información, principalmente al no recopilar nunca la información personal no pública (NPI) que dichas normas están diseñadas para proteger. Cyber Crucible es un proveedor de software, no una institución financiera autorizada, por lo que no es examinado directamente; sus controles están diseñados para ser examinables como parte del programa de gestión de riesgos de terceros de la institución.

Dónde la arquitectura hace el trabajo

- **No se recopila NPI.** El producto se ejecuta en los endpoints que pueden manejar NPI sin extraerla. No existe información financiera del consumidor que Cyber Crucible pueda usar, compartir o volver a divulgar, lo cual respalda directamente la posición de la Regla de Privacidad de GLBA / Regulación P.
- **Programa de seguridad documentado.** El control de acceso, el cifrado, la respuesta a brechas y el control de cambios están documentados y pueden verificarse con evidencia: las salvaguardas que el programa de un banco busca en un proveedor de servicios.
- **Evidencia de debida diligencia disponible.** Un paquete de proveedor preparado está estructurado para servir como la evidencia de debida diligencia y monitoreo continuo que un banco necesita conforme a la guía interagencial vigente sobre riesgo de terceros.

El límite honesto

Cyber Crucible respalda las obligaciones de cumplimiento de un cliente; no logra, por sí mismo, que una organización sea conforme, y esto no constituye asesoría legal. Se proporciona información detallada y con nivel de evidencia a los revisores de un banco bajo un acuerdo de confidencialidad (NDA). Véase también *¿Cumple Cyber Crucible con las expectativas de la FFIEC y de gestión de riesgos de terceros?*

¿Cyber Crucible cumple con las expectativas de la FFIEC y de gestión de riesgos de terceros?

Respuesta breve: Cyber Crucible está diseñado para ser examinable frente a las expectativas de seguridad, operaciones y continuidad del negocio que los examinadores aplican a la tecnología bancaria, y su paquete de proveedor preparado está organizado para servir como la evidencia de diligencia debida que una institución financiera necesita conforme a la guía interagencial de 2023 sobre relaciones con terceros.

En qué puede apoyarse el programa de un banco

- Detalle de controles mapeado a los dominios que se encuentran en los cuestionarios estándar (SIG, CAIQ) y a los Criterios de Servicios de Confianza de SOC 2 y al NIST CSF.
- Validación independiente de controladores (WHCP) como una atestación de calidad externa.
- Una postura de continuidad del negocio documentada y probada, con la propiedad importante de que la protección de endpoints continúa incluso durante una interrupción del backend de gestión.
- Evidencia de seguro, información financiera y una lista de subprocesadores disponibles para los revisores bajo solicitud.

Por qué la arquitectura reduce el riesgo de terceros

El dato más útil para un analista de riesgo de proveedores de un banco es que Cyber Crucible nunca recopila archivos, credenciales o claves de los clientes. Los datos que preocupan a un revisor de que un proveedor maneje mal no están bajo la custodia de Cyber Crucible para ser mal manejados. Se trata de una reducción estructural del riesgo, no de una promesa de gestionarlo bien.

¿A qué marcos de seguridad y cumplimiento se alinea Cyber Crucible?

Respuesta breve: Cyber Crucible asigna sus controles al NIST Cybersecurity Framework, a las familias de controles pertinentes de NIST SP 800-53 y a los CIS Critical Security Controls, y los relaciona con los Trust-Service Criteria de SOC 2 para conveniencia del revisor. Se trata de **alineaciones autoevaluadas**, ofrecidas para que un revisor pueda relacionar los controles de Cyber Crucible con un estándar que conozca, y no de certificaciones ni de opiniones de auditoría de terceros.

Alineación, expresada con honestidad

Marco	Estado
NIST Cybersecurity Framework (CSF)	Controles autoasignados; no es una certificación
Familias de controles de NIST SP 800-53	Alineado donde corresponde; no es una autorización
CIS Critical Security Controls	Alineado; no certificado
Trust-Service Criteria de SOC 2	Relacionado para conveniencia del revisor; no se posee un informe
Microsoft WHCP (controlador)	Obtenido — una validación externa e independiente

Por qué se expresa de esta manera

Un proveedor que enumera marcos frente a los cuales no ha sido auditado invita al revisor a desconfiar de cualquier otra respuesta. Cyber Crucible indica claramente qué es una certificación (WHCP) y qué es una asignación autoevaluada (el resto), de modo que el revisor pueda ponderar cada una en su justa medida.

¿Cyber Crucible utiliza IA, y es un modelo de lenguaje grande?

Respuesta breve: Cyber Crucible utiliza IA propietaria — pero únicamente durante el desarrollo, no en su endpoint, y no es un modelo de lenguaje grande. Su Genetic AI es una herramienta de descubrimiento en tiempo de diseño que identifica el conjunto determinista de variables de comportamiento que indican un ataque. Esos hallazgos se convierten en heurísticas fijas y deterministas a nivel de kernel. En tiempo de ejecución, no se ejecuta ninguna IA, ningún LLM ni ningún modelo adaptativo en el dispositivo.

Por qué esto es una posición más sólida, no más débil

- **La ausencia de un modelo en tiempo de ejecución significa que no hay deriva (drift).** El comportamiento del endpoint es determinista, repetible y comprobable, no probabilístico.
- **No existe una superficie de inferencia en vivo.** No hay ningún modelo en el dispositivo que un atacante pueda manipular o envenenar.
- **Ningún dato de cliente forma parte de ningún modelo.** El contenido, las credenciales y las claves del cliente nunca se utilizan para entrenar, alimentar o ajustar un modelo, y ningún dato del cliente sale del endpoint para su procesamiento por IA.

Para un revisor de una institución financiera o de un organismo regulador, esta suele ser la respuesta sobre IA que esperan escuchar: capacidad sin un modelo opaco y en vivo tomando decisiones en el endpoint.

Relacionado

Consulte *¿Cómo se gobierna la IA en el ciclo de vida de desarrollo de Cyber Crucible?* para conocer cómo se controla el trabajo en tiempo de diseño.

¿Cómo se gobierna la IA en el ciclo de vida de desarrollo de Cyber Crucible?

Respuesta breve: Dado que la Genetic AI de Cyber Crucible se utiliza únicamente en el momento del diseño, se rige bajo el ciclo de vida de desarrollo seguro (SDLC) en lugar de como un sistema de producción en vivo. El trabajo de descubrimiento se realiza en un entorno interno controlado, su resultado se valida y se traduce en heurísticas de kernel deterministas, y los controladores resultantes se firman de forma independiente bajo Microsoft WHCP antes de su publicación.

El ciclo de vida gobernado

Fase	Gobernanza
Diseño	Se establecen los requisitos de seguridad; el descubrimiento con IA forma parte de la fase de diseño, bajo el SDLC
Descubrimiento	Genetic AI identifica variables deterministas indicadoras de ataques utilizando únicamente conjuntos de datos de investigación internos
Derivación	Los hallazgos se convierten en heurísticas de kernel fijas y deterministas: no se implementa ningún modelo en vivo
Validación	Los resultados deterministas son repetibles y comprobables; los modelos y controladores se validan mediante control de calidad (QA)
Publicación	Los controladores de Windows se firman bajo WHCP; los cambios siguen una gestión formal del cambio

Datos e integridad

No se utiliza ningún contenido de clientes, credenciales ni claves para entrenar, alimentar o ajustar un modelo. Los modelos son propietarios y se desarrollan internamente, sin dependencia de modelos de terceros. La integridad del modelo se mantiene mediante control de versiones, validación SDLC/QA y firma WHCP; la confidencialidad se mantiene mediante un entorno de desarrollo controlado.

¿Dónde se procesan los datos de Cyber Crucible? ¿Se almacenan en la nube?

Respuesta breve: El análisis de amenazas y la respuesta se realizan localmente en el endpoint, no en la nube. Cyber Crucible no recopila archivos, credenciales ni claves de los clientes, y no almacena contenido de los clientes con un proveedor de nube pública externo. El backend de gestión e informes se ejecuta en infraestructura operada por Cyber Crucible en Estados Unidos, y existe una implementación totalmente local (on-premises) o con air-gap disponible para las organizaciones que requieren un flujo de datos externo nulo.

Por qué importa el procesamiento local

- **La decisión de protección nunca sale del dispositivo.** Detect-Decide-Respond se ejecuta en el kernel del endpoint, típicamente en menos de 200 milisegundos, sin ida y vuelta a la nube en la ruta crítica.
- **Protección independiente del backend.** Una interrupción del backend de gestión no reduce la protección del endpoint.
- **Opción de implementación.** Las organizaciones con mandatos estrictos de residencia o soberanía de datos pueden ejecutar Cyber Crucible completamente dentro de su propia infraestructura protegida.

En qué puede confiar un revisor

Dado que el contenido de los clientes nunca se recopila, la pregunta "¿adónde van nuestros datos?" tiene una respuesta simple para las categorías de mayor riesgo: no van a ningún lado. La información detallada sobre la infraestructura y los subprocesadores se proporciona a los revisores bajo un acuerdo de confidencialidad (NDA).

¿Cuál es el acuerdo de nivel de servicio (SLA) de disponibilidad y soporte de Cyber Crucible?

Respuesta breve: El Acuerdo de Nivel de Servicio publicado por Cyber Crucible se compromete a una **disponibilidad mensual del servicio del 99,9%** (excluyendo el mantenimiento programado y las causas que estén fuera de su control razonable), con una compensación definida en forma de créditos por tiempo de inactividad. Los tiempos de respuesta del soporte están clasificados por niveles de gravedad, medidos desde el registro del ticket a través del portal de soporte.

Objetivos de tiempo de respuesta del soporte

Gravedad	Descripción	Respuesta
SEV1 — Crítico	Servicio caído o afectando de forma crítica a producción; aún sin solución alternativa	≤ 2 horas
SEV2 — Mayor	Servicio deteriorado de una forma que limita la protección o la respuesta	≤ 4 horas
SEV3 — Menor	Servicio deteriorado sin afectar a la protección o la respuesta	≤ 12 horas
SEV4 — Menor	Problema no crítico, solicitud de información o mejora	≤ 48 horas

Dónde encontrarlo

El Acuerdo de Nivel de Servicio completo está disponible públicamente en cybercrucible.com/service-level-agreement, y los tickets de soporte se registran en support.cybercrucible.com. Se puede establecer contractualmente un plazo comprometido de notificación de incumplimiento o incidente para clientes regulados.

Una nota sobre la disponibilidad

Dado que la protección de los endpoints se ejecuta de forma local, la cifra de disponibilidad se aplica al backend de gestión y generación de informes. La protección en el propio dispositivo continúa incluso si el backend no está disponible temporalmente.

¿Cómo gestiona Cyber Crucible la retención y eliminación de datos?

Respuesta breve: Cyber Crucible minimiza lo que almacena y retiene los datos solo durante el tiempo necesario para prestar el servicio. Nunca recopila el contenido, las credenciales o las claves del cliente en primer lugar, por lo que las categorías de mayor riesgo no tienen nada que retener. La telemetría de comportamiento y los metadatos de seguridad derivados se eliminan según calendarios definidos, y al final de un contrato todos los datos asociados se ponen a disposición para su eliminación, con la correspondiente confirmación.

El principio

- **Minimizar primero.** Los datos más sensibles nunca se recopilan, por lo que no hay nada que retener ni destruir en esas categorías.
- **Retener según el propósito.** La telemetría de comportamiento y los metadatos de seguridad se conservan solo mientras sirvan para la detección, la investigación y la elaboración de informes, y luego se eliminan.
- **Eliminar al finalizar.** Al término del contrato, los datos asociados se ponen a disposición para su eliminación y Cyber Crucible proporciona la confirmación correspondiente.

Qué está documentado

Un proceso de destrucción documentado abarca tanto la información impresa como la electrónica. Los períodos de retención específicos por tipo de datos se proporcionan a los revisores bajo acuerdo de confidencialidad (NDA) y pueden restringirse mediante contrato.

¿Cuenta Cyber Crucible con un Delegado de Protección de Datos?

Respuesta breve: Sí. Cyber Crucible ha contratado a un DPO externo con experiencia interjurisdiccional que abarca el RGPD de la UE/Reino Unido, la CCPA/CPRA de California, HIPAA, PCI-DSS y regímenes globales de protección de datos, incluida la PDPL de Arabia Saudita. El DPO puede contactarse a través de la casilla de correo supervisada **dpo@cybercrucible.com**.

Qué abarca el DPO

- El programa de privacidad y los acuerdos de tratamiento de datos.
- Las evaluaciones de impacto en la protección de datos y de riesgo de transferencia, incluidas las Cláusulas Contractuales Tipo para transferencias transfronterizas.
- Las determinaciones de notificación de brechas y el apoyo a las propias obligaciones de notificación del cliente.
- Un punto de contacto especializado para preguntas de privacidad y cumplimiento durante el proceso de contratación.

Por qué contar con un DPO externo con experiencia global

Varios regímenes fuera de EE. UU. —entre ellos la PDPL saudita— pueden ser más restrictivos que la legislación estadounidense actual. Contar con un DPO con dominio del RGPD, la CCPA/CPRA, HIPAA y las PDPL globales permite a Cyber Crucible respaldar a los clientes conforme al estándar más estricto, lo que generalmente satisface el estándar básico de EE. UU. como un subconjunto.

¿Cyber Crucible está sujeto a los controles de exportación de EE. UU.?

Respuesta breve: Sí — el software de Cyber Crucible está sujeto a las Regulaciones de Administración de Exportaciones (EAR) del Departamento de Comercio de EE. UU. **No** está controlado por ITAR y no es administrado por el Departamento de Estado. No se requiere una licencia especial para proporcionar el software a los clientes, y la clasificación de exportación y el proceso de verificación se gestionan como parte del programa de cumplimiento de Cyber Crucible.

Lo que esto significa para un comprador

- **EAR, no ITAR.** El producto se encuentra bajo la jurisdicción del Departamento de Comercio, el marco que se aplica a la mayoría del software comercial con capacidades de cifrado — no bajo el régimen de artículos de defensa.
- **Patentado y revisado.** La tecnología ha sido patentada a nivel internacional tras una revisión de la Oficina de Patentes y Marcas de EE. UU. (USPTO) que incluyó una revisión por parte del Departamento de Defensa.
- **Sin barreras de licenciamiento.** Proporcionar el software a un cliente no requiere una licencia de exportación especial.

El detalle de la clasificación de exportación está disponible para los revisores que lo soliciten.

¿Cómo reduce Cyber Crucible el riesgo de terceros y proveedores para compradores regulados?

Respuesta breve: Eliminando el riesgo en lugar de solo gestionarlo. Los tres hechos que responden a las preguntas más difíciles sobre riesgo de proveedores son: Cyber Crucible no recopila contenido, credenciales ni claves de los clientes; la protección se ejecuta de forma local y sobrevive a cualquier interrupción del backend; y su IA reside únicamente en el desarrollo, nunca en su endpoint. Juntos, estos factores reducen la superficie que una revisión de debida diligencia está diseñada para examinar.

Los tres reductores estructurales de riesgo

- **Cero contenido.** Nunca se recopilan archivos, credenciales ni claves de los clientes. Este único hecho responde a las líneas de cuestionamiento sobre PCI, datos confidenciales y "qué pasa si sufren una vulneración" — los datos simplemente no están ahí para perderse.
- **Protección independiente del backend.** Detect–Decide–Respond se ejecuta localmente, con un objetivo de tiempo de recuperación efectivo de cero en el endpoint. Una interrupción total del backend no reduce la protección.
- **IA determinista.** La IA se utiliza únicamente en el desarrollo; en tiempo de ejecución operan heurísticas deterministas. No hay modelo en vivo, no hay desviación (drift), y los resultados son verificables.

Refuerzo independiente

Donde la certificación independiente tiene peso, Cyber Crucible señala lo que es real: la firma de controladores Microsoft WHCP y, para el backend gestionado, las certificaciones de terceros de los proveedores de infraestructura en los que se apoya. Sin un SOC 2 propio, estos elementos sostienen la carga de manera honesta en lugar de ser sobrevalorados.

¿Cómo obtengo el paquete de diligencia debida de seguridad de Cyber Crucible?

Respuesta breve: Solicítelo a **dpo@cybercrucible.com**. Bajo un acuerdo mutuo de confidencialidad (NDA), Cyber Crucible proporciona un paquete de seguridad para proveedores ya preparado que responde a los dominios de los cuestionarios estándar (SIG, CAIQ) y sustituye a un informe SOC 2 en los casos en que un revisor normalmente esperaría encontrar uno.

Qué incluyen el paquete y sus documentos complementarios

- Un paquete preparado de seguridad y confianza para proveedores: arquitectura, manejo de datos, cifrado, gestión de accesos, desarrollo seguro, respuesta ante incidentes, continuidad del negocio, alineación regulatoria y una correspondencia con marcos de control.
- Resúmenes de una página sobre los programas de cumplimiento, auditoría y gobernanza de IA/SDLC.
- Un certificado de seguro, el formulario W-9 e información financiera, disponibles a solicitud.
- Cláusulas Contractuales Estándar, una Evaluación de Riesgo de Transferencia y un Acuerdo de Procesamiento de Datos, disponibles a solicitud.

Documentos públicos que puede consultar ahora

Documento	Ubicación
Acuerdo de Nivel de Servicio	cybercrucible.com/service-level-agreement
NDA Mutuo	cybercrucible.com/mutualNDA
MSA y EULA	cybercrucible.com/msa-and-eula
Política de Privacidad	cybercrucible.com/privacy-policy

Todo lo que va más allá de los acuerdos públicos se proporciona a los revisores bajo NDA, sujeto a medidas razonables de confidencialidad.