

Guías de Riesgo de Proveedores por Industria

Respuestas de diligencia debida en materia de seguridad para sectores regulados específicos: salud, educación, gobierno, defensa, servicios públicos, servicios financieros, comercio minorista, sector legal y seguros, presentadas para el revisor de riesgo de proveedores. Se indica claramente qué información posee y no posee Cyber Crucible.

- [¿Cómo respalda Cyber Crucible el cumplimiento de HIPAA, y firmará un Acuerdo de Asociado Comercial \(Business Associate Agreement\)?](#)
- [¿Cómo respalda Cyber Crucible el cumplimiento de FERPA y la privacidad de datos estudiantiles para escuelas y universidades?](#)
- [¿Cyber Crucible cuenta con autorización FedRAMP y cómo presta servicio a organismos gubernamentales?](#)
- [¿Cumple Cyber Crucible con los requisitos de CMMC y DFARS para la base industrial de defensa?](#)
- [¿Cómo encaja Cyber Crucible con NERC CIP y la seguridad de infraestructuras críticas?](#)
- [¿Cómo se alinea Cyber Crucible con la norma IEC 62443 para sistemas de control industrial?](#)
- [¿Cómo respalda Cyber Crucible el cumplimiento de PCI-DSS para el comercio minorista y la hostelería?](#)
- [¿Cómo presta servicio Cyber Crucible a entornos de fuerzas del orden y CJIS?](#)
- [¿Cómo respalda Cyber Crucible a las aseguradoras y los requisitos de suscripción cibernética?](#)
- [¿Cómo protege Cyber Crucible la confidencialidad de bufetes de abogados y servicios profesionales?](#)

¿Cómo respalda Cyber Crucible el cumplimiento de HIPAA, y firmará un Acuerdo de Asociado Comercial (Business Associate Agreement)?

Respuesta breve: Cyber Crucible respalda las obligaciones de HIPAA de una entidad cubierta principalmente al nunca recopilar información de salud protegida (PHI). El análisis se realiza localmente en el endpoint, por lo que la PHI no se carga a una nube de terceros para el procesamiento de seguridad. Debido a que Cyber Crucible no crea, recibe, mantiene ni transmite PHI en nombre de una entidad cubierta, normalmente no cumple con la definición de asociado comercial (business associate); sin embargo, cuando el proceso de riesgo de un cliente lo requiere, se puede ejecutar un Acuerdo de Asociado Comercial (Business Associate Agreement).

Por qué la arquitectura se adapta al sector salud

- **La PHI nunca sale del dispositivo para el análisis de seguridad.** Muchos acuerdos de SOC/MDR alojados por proveedores cargan archivos, claves o telemetría a una nube de terceros; Cyber Crucible analiza en el endpoint, por lo que se evita esa exposición.
- **Continuidad clínica.** Solo se suspende el proceso malicioso — sin aislamiento total del sistema ni reinicio forzado — de modo que los dispositivos conectados y los sistemas clínicos siguen funcionando mientras se neutraliza un ataque.
- **Ransomware sin necesidad de un SOC 24/7.** La prevención autónoma detiene los ataques antes de su ejecución sin requerir analistas que un hospital podría no tener la capacidad de contratar.

El límite honesto

Cyber Crucible no está "certificado en HIPAA" — no existe tal certificación. Respalda su programa de cumplimiento; sus responsables de privacidad y seguridad son quienes determinan lo adecuado

para su entorno. Un BAA está disponible a solicitud escribiendo a **dpo@cybercrucible.com**.

¿Cómo respalda Cyber Crucible el cumplimiento de FERPA y la privacidad de datos estudiantiles para escuelas y universidades?

Respuesta breve: Cyber Crucible ayuda a las instituciones educativas de dos maneras: detiene el ransomware de forma autónoma sin necesidad de un centro de operaciones de seguridad (SOC) 24/7, y — a través de FortressAI — evalúa el acceso a datos de herramientas de IA en el dispositivo para que los registros estudiantiles y los datos familiares no lleguen accidentalmente a un sistema de IA público. Dado que el análisis es local y no se recopilan registros estudiantiles, los registros educativos protegidos permanecen dentro del perímetro de la institución.

Los dos problemas educativos que aborda

- **Ransomware sin un SOC.** La prevención a nivel de kernel detiene los ataques en menos de 200 milisegundos, sin necesidad de contratar analistas ni financiar un contrato de monitoreo ininterrumpido.
- **Gobernanza de IA para el aula.** FortressAI verifica cada solicitud (prompt) en el dispositivo, de modo que los registros educativos protegidos y los datos personales familiares no se envíen a un sistema de IA público, ni siquiera como datos de entrenamiento.

Notas para la selección de proveedores

- Cyber Crucible actúa como funcionario escolar / proveedor de servicios bajo la dirección de la institución y no utiliza los datos estudiantiles para ningún fin secundario.
- Las leyes estatales de privacidad estudiantil (por ejemplo, en California, Nueva York y Colorado) añaden obligaciones adicionales para los proveedores; el diseño de procesamiento local y de no recopilación respalda su cumplimiento. La documentación está disponible bajo acuerdo de confidencialidad (NDA).

¿Cyber Crucible cuenta con autorización FedRAMP y cómo presta servicio a organismos gubernamentales?

Respuesta breve: No — Cyber Crucible no cuenta actualmente con una autorización FedRAMP, y no da a entender lo contrario. FedRAMP autoriza ofertas de servicios en la nube que albergan datos de organismos gubernamentales; el modelo de Cyber Crucible es distinto. Se ejecuta localmente en el endpoint y puede implementarse totalmente en las instalaciones (on-premises) o de forma aislada (air-gapped) dentro del propio perímetro del organismo, de modo que los datos del organismo nunca salen de ese perímetro hacia una nube de terceros.

Cómo encaja la arquitectura en el ámbito gubernamental

- **Implementación en las instalaciones / aislada (air-gapped).** La plataforma puede ejecutarse íntegramente dentro de la infraestructura protegida de un organismo, sin ningún flujo de datos externo, lo que resulta idóneo para entornos clasificados, desconectados y de alta seguridad.
- **No se recopilan datos del organismo.** Nunca se recopila contenido de clientes, credenciales ni claves, lo que elimina gran parte de lo que una autorización en la nube está diseñada para proteger.
- **Fabricado en EE. UU. y sujeto a control de exportaciones.** El software está sujeto a las EAR del Departamento de Comercio de EE. UU. (no a ITAR), y cuenta con patente internacional tras una revisión de la USPTO que incluyó la revisión del Departamento de Defensa.

El límite, con honestidad

Cuando un organismo requiere una autorización específica (FedRAMP, StateRAMP), Cyber Crucible no la posee actualmente; el modelo de implementación en las instalaciones es la vía que permite mantener los datos dentro del perímetro del organismo. Los detalles de implementación y control se proporcionan bajo acuerdo de confidencialidad (NDA).

¿Cumple Cyber Crucible con los requisitos de CMMC y DFARS para la base industrial de defensa?

Respuesta breve: Cyber Crucible no cuenta con certificación CMMC, y lo indica claramente. Respalda las obligaciones de un contratista de defensa bajo DFARS 252.204-7012 y CMMC principalmente al no recopilar Información No Clasificada Controlada (CUI) y al admitir implementaciones locales (on-premises) o aisladas de la red (air-gapped) dentro del perímetro propio del contratista, donde la CUI permanece bajo el control del contratista.

Cómo respalda las obligaciones del contratista

- **No se recopila CUI.** El agente de endpoint analiza el comportamiento de forma local sin extraer los archivos que protege, por lo que la CUI no se transfiere a Cyber Crucible.
- **Implementación que preserva el perímetro.** Los modelos on-premises y air-gapped mantienen todos los datos dentro del perímetro evaluado del contratista.
- **Controles de protección de endpoints.** La prevención y el monitoreo de malware/ransomware se corresponden con las prácticas CMMC pertinentes y los controles de NIST SP 800-171 que el contratista debe implementar.
- **Cadena de suministro estadounidense.** Los datos estadounidenses son gestionados por recursos con sede en EE. UU.; los contratistas externos (offshore) no manejan datos de EE. UU. ni desarrollan los agentes. El software está controlado por EAR, no por ITAR.

El límite honesto

La certificación CMMC la posee el entorno del contratista, no una herramienta de seguridad individual; Cyber Crucible es un control que respalda varios requisitos de 800-171, no un sustituto de la evaluación del contratista. El detalle de la correspondencia (mapping) está disponible bajo NDA.

¿Cómo encaja Cyber Crucible con NERC CIP y la seguridad de infraestructuras críticas?

Respuesta breve: Cyber Crucible es adecuado para entornos de infraestructuras críticas y servicios públicos porque protege los endpoints de forma autónoma y puede funcionar sin conexión o en entornos aislados (air-gapped), sin depender de la nube en la ruta de protección. Esto encaja con los BES Cyber Systems y otros entornos donde la conectividad está restringida y la disponibilidad es primordial.

Por qué encaja con los servicios públicos y las infraestructuras críticas

- **Capacidad sin conexión / air-gapped.** Protección completa sin necesidad de conexión a internet, adecuada para redes OT aisladas y subestaciones.
- **Respuesta que preserva la disponibilidad.** Solo se suspende el proceso malicioso, de modo que los sistemas operativos siguen funcionando; no se produce un bloqueo total del sistema durante un incidente.
- **Decisiones locales y deterministas.** Detect-Decide-Respond se ejecuta en el propio dispositivo, sin ida y vuelta a la nube ni modelo de IA en vivo.

Notas sobre la selección de proveedores

Las obligaciones de NERC CIP recaen sobre la entidad registrada, no sobre un proveedor individual; Cyber Crucible es un control que respalda varios objetivos de CIP (prevención de malware, monitoreo, gestión de incidentes). No es una entidad registrada y no se presenta como certificado en CIP. La documentación de respaldo está disponible bajo NDA.

¿Cómo se alinea Cyber Crucible con la norma IEC 62443 para sistemas de control industrial?

Respuesta breve: Cyber Crucible respalda el modelo de defensa en profundidad de IEC 62443 para sistemas de automatización y control industrial mediante la incorporación de protección autónoma de endpoints a nivel de kernel que no interrumpe la producción. Funciona de forma local, tolera la operación sin conexión y suspende únicamente los procesos maliciosos, lo cual se alinea con el énfasis de la norma tanto en la seguridad como en la disponibilidad operativa.

Cómo se corresponde con el propósito de la norma

- **Protección de zonas y conductos.** La prevención residente en el endpoint refuerza los dispositivos dentro de una zona sin depender de una comunicación de ida y vuelta con la red.
- **La disponibilidad ante todo.** La suspensión selectiva de un proceso malicioso evita el tiempo de inactividad de la planta que provoca la contención indiscriminada.
- **Funciona en entornos de baja conectividad.** Es adecuado para plantas de fabricación, flotas logísticas y sitios periféricos donde la conectividad en la nube es poco confiable o deliberadamente inexistente.

El límite honesto

La certificación IEC 62443 se aplica a sistemas y procesos, no a una única herramienta de endpoint; Cyber Crucible es un componente que respalda los objetivos de la norma. La correspondencia de controles está disponible bajo acuerdo de confidencialidad (NDA).

¿Cómo respalda Cyber Crucible el cumplimiento de PCI-DSS para el comercio minorista y la hostelería?

Respuesta breve: 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 respalda los objetivos de control de PCI-DSS del comerciante, en particular el requisito de proteger los sistemas contra el malware. Reduce, en lugar de ampliar, el alcance de PCI.

Cómo respalda los objetivos de PCI-DSS

- **Protección contra malware (Requisito 5).** La prevención autónoma a nivel de kernel detiene el ransomware y los ataques en memoria en los sistemas del entorno de datos de titulares de tarjetas.
- **No se recopilan datos de titulares de tarjetas.** El agente observa el comportamiento de los procesos y nunca ingiere datos de tarjetas, incluso en hosts que manejan tarjetas, por lo que no amplía el alcance de la evaluación.
- **Continuidad.** Solo se suspenden los procesos maliciosos, de modo que los sistemas de punto de venta y de pago siguen funcionando.

Notas para la selección de proveedores

El cumplimiento de PCI-DSS corresponde al comerciante y a su evaluador; Cyber Crucible es un control de apoyo, no un servicio validado por un QSA. No cuenta con certificación PCI-DSS ni afirma poseerla.

¿Cómo presta servicio Cyber Crucible a entornos de fuerzas del orden y CJIS?

Respuesta breve: Cyber Crucible se adapta a los entornos de Criminal Justice Information Services (CJIS) porque procesa los datos de forma local, nunca recopila información de justicia penal (CJI, por sus siglas en inglés) y puede ejecutarse en las instalaciones o de forma aislada (air-gapped) dentro del perímetro de la agencia. Los datos de EE. UU. son gestionados por personal ubicado en EE. UU., lo cual respalda las expectativas de la CJIS Security Policy en materia de personal y manejo de datos.

Por qué la arquitectura se adapta

- **La CJI permanece dentro del perímetro.** No se recopila contenido del cliente; el análisis se realiza en el endpoint, por lo que la CJI no se transfiere a una nube de terceros.
- **Personal de EE. UU. para datos de EE. UU.** Los contratistas externos ubicados fuera del país no manejan datos de EE. UU. ni desarrollan los agentes.
- **Cifrado y control de acceso.** La autenticación robusta, el control de acceso basado en roles y el cifrado respaldan los controles técnicos de la política.

El límite honesto

La CJIS Security Policy es aplicada por la agencia y su CJIS Systems Agency estatal correspondiente; Cyber Crucible respalda varias de sus áreas de control, pero en sí misma no constituye una "certificación" CJIS. Los detalles sobre la verificación de antecedentes del personal y los controles están disponibles bajo acuerdo de confidencialidad (NDA).

¿Cómo respalda Cyber Crucible a las aseguradoras y los requisitos de suscripción cibernética?

Respuesta breve: Cyber Crucible fortalece la postura de ciberseguro de una organización porque proporciona los controles que los suscriptores ahora exigen — prevención autónoma de ransomware, protección de endpoints y acceso respaldado por MFA — al tiempo que reduce la superficie de pérdida al nunca recopilar los datos que un atacante podría monetizar. Para las aseguradoras como clientes, el mismo diseño de procesamiento local y sin recopilación protege los datos de los asegurados.

Por qué ayuda en el momento de la suscripción

- **Prevención de ransomware, no solo detección.** Los suscriptores distinguen cada vez más la prevención de la detección; la interceptación previa a la ejecución es el control más sólido.
- **Menor exposición a brechas.** Dado que los archivos, credenciales y claves de los clientes nunca se recopilan, la pregunta "qué pasa si sufren una brecha" tiene una respuesta más acotada.
- **Informes listos para la junta directiva.** La prevención reduce la exposición en materia de divulgación, algo que importa tanto a los suscriptores como a las juntas directivas.

Notas sobre la selección de proveedores

Para una aseguradora que evalúe a Cyber Crucible como su propio proveedor, el rol de procesador, la minimización de datos y la opción local (on-premises) respaldan las obligaciones de protección de los datos de los asegurados. La documentación está disponible bajo acuerdo de confidencialidad (NDA).

¿Cómo protege Cyber Crucible la confidencialidad de bufetes de abogados y servicios profesionales?

Respuesta breve: Cyber Crucible protege el material privilegiado y confidencial de los clientes al mantener el análisis en el endpoint y nunca recopilar archivos, credenciales o claves; de modo que las confidencias de los clientes no quedan expuestas a una nube de terceros en el proceso de ser protegidas. Detiene el ransomware y los infostealers de forma autónoma, lo cual es importante para firmas sin un equipo de seguridad numeroso.

Por qué se ajusta a los servicios profesionales

- **Confidencialidad por diseño.** Ningún documento del cliente sale del dispositivo para su procesamiento de seguridad; no existe una copia en poder del proveedor que pueda ser objeto de una citación judicial o de una filtración.
- **Prevención del robo de identidad y de datos.** Los infostealers que apuntan a tokens de sesión y credenciales son interceptados antes de que los datos salgan del dispositivo.
- **Bajo costo operativo.** La prevención autónoma funciona sin necesidad de un SOC que opere las 24 horas.

Notas sobre la selección de proveedores

Los deberes éticos de confidencialidad y, para muchas firmas, los anexos de seguridad para clientes, impulsan un escrutinio riguroso de los proveedores; el modelo de no recopilación y procesamiento local respalda ambos aspectos. Hay un acuerdo de procesamiento de datos disponible a solicitud.