Guías de Cumplimiento por País

Respuestas jurisdicción por jurisdicción: lo que exige específicamente la ley de protección de datos de cada país y cómo la arquitectura de Cyber Crucible lo aborda. Golfo, África, Europa y Reino Unido.

¿Cumple Cyber Crucible con la PDPL de Arabia Saudita?

Respuesta breve: Cyber Crucible ha revisado sus operaciones conforme a la Ley de Protección de Datos Personales de Arabia Saudita, utiliza Cláusulas Contractuales Estándar aprobadas por la SDAIA para cualquier transferencia de datos personales de origen saudita, y puede implementarse en su totalidad dentro del Reino sin ningún flujo transfronterizo. Solo recopila telemetría de sistema y de seguridad, nunca contenido de archivos, documentos, correos electrónicos o comunicaciones.

Lo que exige la ley

La PDPL entró en vigor el 14 de septiembre de 2023, con un período de gracia hasta el 14 de septiembre de 2024. Arabia Saudita mantiene una de las preferencias de localización más estrictas del Golfo, y la Autoridad Saudita de Datos e Inteligencia Artificial (SDAIA) supervisa su cumplimiento. Las transferencias fuera del Reino requieren una salvaguarda reconocida y, en la mayoría de los casos, una Evaluación de Riesgo de Transferencia.

Lo que aplica específicamente aquí

- **Las SCC preaprobadas por la SDAIA** se utilizan para cualquier transferencia de datos personales de origen saudita hacia Estados Unidos, adoptadas sin modificaciones salvo los campos requeridos, y extendidas a cualquier subencargado posterior.
- **Se ha completado una Evaluación de Riesgo de Transferencia** siguiendo la guía estructurada de la SDAIA: flujos de datos, régimen legal de destino, controles, riesgo residual, mitigaciones documentadas.
- **Rol de encargado** — Cyber Crucible normalmente actúa como encargado del tratamiento bajo un DPA por escrito; el cliente saudita es el responsable.
- **Representante local del Artículo 33** — como encargado, esa obligación recae en usted como responsable.

La ruta más clara

Dada la preferencia de localización, la implementación totalmente local y con air-gap (sin conexión externa) es la respuesta más sólida: toda la gestión del backend dentro de sus propios racks físicamente asegurados, sin telemetría saliente. Cuando nada cruza la frontera, no surgen obligaciones de transferencia.

> Las SCC y la Evaluación de Riesgo de Transferencia (TRA) están disponibles en **dpo@cybercrucible.com**. Estado vigente al momento de redacción; confirme los requisitos actuales con asesoría legal local.

¿Cyber Crucible cumple con la ley de protección de datos de los EAU?

Respuesta breve: Sí, bajo la misma arquitectura: recopilación mínima, procesamiento local y opciones de implementación donde los datos nunca salen del país. Un aspecto específico de los EAU es importante: si su entidad se encuentra en el DIFC o el ADGM, se aplica un régimen diferente al de la ley federal.

Lo que exige la ley

El Decreto-Ley Federal N.º 45 de 2021 de los EAU establece el marco federal de protección de datos personales. Permite una gama más amplia de bases legales que los regímenes del Golfo más centrados en el consentimiento, y adopta un enfoque basado en el riesgo y orientado a las salvaguardas para las transferencias transfronterizas, en lugar de una localización estricta. La implementación ha dependido de los Reglamentos de Ejecución, un ámbito que ha ido evolucionando, por lo que conviene confirmar la situación actual.

La cuestión de las zonas francas

Esto suele sorprender a la gente. El DIFC (Dubai International Financial Centre) y el ADGM (Abu Dhabi Global Market) operan sus propios regímenes de protección de datos, separados de la ley federal. Si su entidad está establecida en cualquiera de ellos, las normas aplicables y la autoridad supervisora son distintas.

Determine qué marco lo rige antes de evaluar a cualquier proveedor: la respuesta cambia lo que necesita demostrar.

Qué se aplica específicamente aquí

- **Flexibilidad de base legal** — la gama más amplia de bases significa que el razonamiento tipo interés legítimo para el procesamiento de seguridad es, en general, más viable que en regímenes centrados en el consentimiento.
- **Salvaguardas de transferencia** — el almacenamiento regional mantiene el procesamiento dentro de los EAU; la implementación con air gap elimina por completo la

transferencia.
- **Rol de encargado del tratamiento** bajo un DPA por escrito, conforme a sus instrucciones documentadas.

> Estado al momento de redactar este documento: confirme los requisitos vigentes, incluidos los Reglamentos de Ejecución y la aplicabilidad en zonas francas, con asesoría legal local.

¿Cumple Cyber Crucible con la ley de protección de datos de Baréin?

Respuesta breve: Sí. La ley de Baréin está fuertemente inspirada en el RGPD y tiene alcance extraterritorial, por lo que los mismos controles que satisfacen el RGPD se aplican aquí: recopilación mínima, función de encargado documentada, salvaguardas de seguridad sólidas y transferencia controlada.

Qué exige la ley

Baréin cuenta con una ley de protección de datos independiente vigente desde 2019. A menudo se cita como una de las más claras y maduras del Golfo, con sólidos derechos de los titulares de datos, obligaciones de responsabilidad explícitas y **aplicación extraterritorial**, lo que significa que puede alcanzar a proveedores fuera de Baréin que procesen datos de residentes bareiníes.

Qué se aplica específicamente aquí

El alcance extraterritorial es el punto que merece destacarse. Significa que la cuestión no es solo si *usted* cumple, sino si sus proveedores lo hacen.

- **Responsabilidad**: la lista de datos excluidos (sin claves, credenciales, tokens ni contenido) es explícita y está documentada en lugar de describirse en términos generales, que es exactamente lo que exigen las obligaciones de responsabilidad.
- **Derechos de los titulares de datos**: en la práctica son limitados aquí, porque la telemetría de comportamiento está seudonimizada y el contenido nunca se recopila, por lo que el volumen de datos personales sujetos a solicitudes de derechos es mínimo.
- **Transferencia**: preparación regional o implementación con air gap.

Por qué ayuda la alineación con el RGPD

Dado que la ley de Baréin sigue de cerca el RGPD, el mapeo del RGPD se aplica casi directamente. Si su organización ya ha realizado el trabajo de evaluación de proveedores conforme al RGPD, la mayor parte de ese trabajo es aplicable.

> Estado en el momento de redacción — confirmar con asesoría legal local.

¿Cumple Cyber Crucible con la ley de protección de datos de Qatar?

Respuesta breve: Sí. El régimen de Qatar está más centrado en el consentimiento que el de sus vecinos, lo que hace que la recopilación mínima sea especialmente valiosa: cuantos menos datos personales se procesen, menor será la carga de consentimiento.

Qué exige la ley

Qatar cuenta con una ley de protección de datos independiente vigente desde 2017, lo que la convierte en una de las más tempranas de la región. Mantiene un modelo más estricto y centrado en el consentimiento en comparación con el conjunto más amplio de bases legales de los EAU, junto con un enfoque basado en el riesgo para las salvaguardas de transferencia.

Por qué el enfoque centrado en el consentimiento favorece esta arquitectura

En un régimen centrado en el consentimiento, cada categoría de datos personales que se procesa es una categoría para la que puede ser necesaria una base legal de procesamiento. Esto hace que *no recopilar* sea considerablemente más valioso que proteger bien.

Cyber Crucible nunca recopila claves de cifrado, credenciales, tokens de sesión ni contenido de archivos. La telemetría de comportamiento se seudonimiza cuando podría identificar a una persona, y las fuentes de telemetría son configurables para que pueda reducir aún más la recopilación.

El resultado es que la superficie de consentimiento para la propia herramienta de seguridad es inusualmente pequeña.

Transferencia

El almacenamiento provisional regional mantiene el procesamiento cerca de la jurisdicción o dentro de ella; la implementación con air gap elimina por completo el flujo transfronterizo.

> Estado en el momento de redacción; confirme con asesoría legal local.

¿Cyber Crucible cumple con la ley de protección de datos de Omán?

Respuesta breve: Sí — y Omán es actualmente la jurisdicción más sensible al tiempo en el Golfo. La ley de protección de datos personales de Omán entra en plena vigencia el **5 de febrero de 2026**, tras un período de gracia de dos años, por lo que los proveedores que cumplían por defecto ahora entran en el ámbito de aplicación.

Qué exige la ley

La ley de Omán refleja de cerca los principios del GDPR, al tiempo que incorpora requisitos locales en torno al consentimiento y el tratamiento de datos. El período de gracia de dos años finaliza el 5 de febrero de 2026, momento a partir del cual se espera el cumplimiento total.

Por qué esto importa ahora para la selección de proveedores

Los períodos de gracia crean un patrón predecible: las organizaciones postergan la revisión de proveedores hasta que se acerca la fecha límite, y luego descubren que una herramienta de seguridad que exporta continuamente telemetría de endpoints a otra jurisdicción es difícil de justificar bajo el nuevo régimen.

Si está revisando su conjunto de herramientas de cara a la fecha de febrero de 2026, las preguntas que vale la pena hacerle a cualquier proveedor de endpoints son:

1. ¿Qué datos personales recopila, de manera específica y enumerada?
2. ¿Dónde se procesan esos datos, y pueden mantenerse dentro de Omán?
3. ¿Cuál es el mecanismo de transferencia si salen del país?
4. ¿Puede operar sin ninguna telemetría saliente?

Las respuestas de Cyber Crucible son: exclusiones enumeradas (sin claves, credenciales, tokens ni contenido); el procesamiento es local en el endpoint; disponibilidad de almacenamiento intermedio regional; y sí — la implementación con air gap produce cero telemetría saliente.

> Estado al momento de redactar este texto — confirme la posición actual y cualquier prórroga con su asesoría legal local.

Kuwait no tiene una ley integral de protección de datos: ¿qué significa esto para la selección de proveedores?

Respuesta breve: Kuwait ha adoptado un enfoque sectorial específico en lugar de promulgar una ley nacional integral de protección de datos, con la regulación de la CITRA que rige la forma en que los sectores de telecomunicaciones y TI gestionan el contenido de los usuarios. Esto convierte la soberanía de datos en una decisión comercial y de seguridad más que en una obligación de cumplimiento, pero la decisión sigue siendo importante.

La situación actual

Kuwait sigue siendo la notable excepción entre los principales estados del Golfo al no contar con una ley nacional integral de protección de datos personales. En su lugar, la regulación de la CITRA aborda específicamente el manejo del contenido de los usuarios en telecomunicaciones y TI.

Por qué "sin ley" no es lo mismo que "sin riesgo"

Tres razones por las que las organizaciones en Kuwait siguen sopesando esto cuidadosamente:

1. **Las normas sectoriales siguen aplicándose.** Si opera en telecomunicaciones o TI, los requisitos de la CITRA son obligaciones vigentes.
2. **Las contrapartes imponen condiciones.** Los socios multinacionales, las aseguradoras y los clientes frecuentemente exigen contractualmente un manejo equivalente al RGPD, independientemente de la legislación local.
3. **La regulación tiende a llegar.** Todos los demás estados del CCG han promulgado ya una ley integral. Elegir proveedores que ya cumplan con regímenes más estrictos evita una migración forzosa más adelante.

La postura práctica

Dado que Cyber Crucible nunca recopila claves, credenciales, tokens ni contenido, y puede implementarse completamente aislado de la red (air-gapped), satisface los regímenes más estrictos de la región. Elegirlo en Kuwait significa elegir no tener este problema cuando cambie la ley.

> Estado en el momento de redacción: confirme los requisitos sectoriales vigentes con asesoría legal local.

¿Cumple Cyber Crucible con la Ley de Protección de Datos de Kenia?

Respuesta breve: Sí. La Ley de Protección de Datos de Kenia de 2019 restringe la transferencia transfronteriza a países con salvaguardas adecuadas y aplica una regla más estricta a los datos personales sensibles. Cyber Crucible no recopila datos personales sensibles en absoluto, y puede implementarse de manera que ningún dato salga de Kenia.

Lo que exige la ley

Las secciones 48 y 49 de la Ley de Protección de Datos de 2019 prohíben transferir datos personales a un país que carezca de salvaguardas adecuadas de seguridad de datos, con varias bases permitidas, incluida la adecuación.

La regla más estricta que importa: la transferencia de datos personales *sensibles* solo está permitida cuando el titular de los datos ha dado su consentimiento **y** existen salvaguardas adecuadas. Ambas condiciones, no solo una u otra.

Por qué la regla sobre datos sensibles es el punto clave

Ese requisito doble es difícil de cumplir operativamente: obtener y documentar el consentimiento individual de cada titular de datos afectado, de forma continua, para una herramienta de seguridad.

Cyber Crucible evita este problema: **no se recopilan datos personales sensibles.** Ni datos biométricos, de salud o genéticos; ni datos que revelen origen racial o étnico, creencias religiosas u opiniones políticas. La telemetría describe el comportamiento del sistema y los eventos de seguridad, no atributos personales.

Cuando la telemetría de comportamiento pudiera identificar indirectamente a una persona, los identificadores se seudonimizan o enmascaran.

Transferencia

El almacenamiento provisional regional mantiene el procesamiento dentro de Kenia. La implementación con air-gap produce cero telemetría saliente, por lo que las secciones 48 a 49 no se aplican.

> Estado al momento de redactar este documento: confirmar con asesoría legal local.

¿Cumple Cyber Crucible con el requisito de localización de datos de Nigeria?

Respuesta breve: Sí — y esta es la jurisdicción donde la arquitectura importa más. La Ley de Protección de Datos de Nigeria de 2023 impone un requisito de localización de datos: los datos personales de los ciudadanos nigerianos deben almacenarse dentro de Nigeria. La implementación local (on-premises) de Cyber Crucible mantiene todo dentro de su propia infraestructura, en el país, sin telemetría saliente.

Qué exige la ley

Las secciones 41 a 43 de la Ley de Protección de Datos de Nigeria de 2023 establecen condiciones para la transferencia transfronteriza, incluidas salvaguardas del país de destino y el consentimiento del titular de los datos. Más allá de esas condiciones, **Nigeria impone un requisito de localización** — los datos personales de los ciudadanos nigerianos deben almacenarse dentro de Nigeria. Las normas sectoriales en servicios financieros añaden obligaciones de localización adicionales.

Por qué la mayoría de los proveedores de seguridad tienen dificultades aquí

Este es el ejemplo más claro de una norma que la seguridad de endpoints dependiente de la nube no puede satisfacer por diseño. Una herramienta cuya arquitectura consiste en "recopilar telemetría en el endpoint y enviarla a nuestra nube para su análisis" está, estructuralmente, trasladando datos personales fuera de Nigeria como condición para funcionar. Las salvaguardas contractuales no resuelven un requisito de ubicación de almacenamiento.

Por qué esta arquitectura sí lo satisface

- **El análisis es local.** La evaluación de amenazas y la interdicción ocurren en el endpoint, típicamente en menos de 200 milisegundos. No se requiere un viaje de ida y vuelta a la nube para la protección.

- **El backend puede estar completamente en el país.** El modelo on-premises ejecuta todo el software de gestión dentro de sus propios racks físicamente asegurados.
- **Cero telemetría saliente** en la configuración con air gap — nada sale, por lo que nada se almacena en el extranjero.
- **De todos modos hay menos que localizar** — las claves, credenciales, tokens y contenidos de archivos nunca se recopilan en primer lugar.

> Estado al momento de escribir esto — confirme los requisitos vigentes, incluidas las normas del sector financiero, con asesoría legal local.

¿Cyber Crucible cumple con la POPIA de Sudáfrica?

Respuesta breve: Sí. La POPIA restringe la transferencia transfronteriza a menos que el destino ofrezca una protección sustancialmente similar o que el titular de los datos otorgue su consentimiento. Cyber Crucible minimiza desde el inicio lo que se procesa, y puede implementarse de manera que no se produzca ninguna transferencia.

Lo que exige la ley

La Ley de Protección de la Información Personal de Sudáfrica (2013) prohíbe transferir información personal fuera del país sin el consentimiento del titular de los datos, a menos que la jurisdicción receptora esté sujeta a una ley que proporcione una protección sustancialmente similar.

Lo que se aplica específicamente aquí

La prueba de "protección sustancialmente similar" es una evaluación que usted debe poder demostrar. Dos factores facilitan esa evaluación:

1. **El alcance es reducido.** Nunca se recopilan claves de cifrado, credenciales, tokens de sesión ni contenidos de archivos. Lo que queda es telemetría de comportamiento, seudonimizada cuando pudiera identificar a una persona.
2. **Protecciones contractuales** — el procesamiento se realiza conforme a un DPA por escrito con cláusulas de seguridad, confidencialidad y notificación de brechas, extendidas a cualquier subencargado.

O evite la prueba por completo

El almacenamiento regional mantiene el procesamiento dentro de Sudáfrica. La implementación con air gap no genera ningún flujo saliente en absoluto, en cuyo caso las disposiciones de transferencia simplemente no se aplican, lo cual suele ser una vía más rápida que demostrar la adecuación.

> Estado vigente al momento de redactar este documento — confirme con asesoría legal local.

¿Cyber Crucible cumple con la ley de protección de datos de Egipto?

Respuesta breve: Sí. Egipto exige aprobación previa para las transferencias transfronterizas de datos personales, un estándar sustancialmente más exigente que las salvaguardas contractuales. Cyber Crucible puede implementarse de modo que no se produzca ninguna transferencia, eliminando así el requisito de aprobación en lugar de tener que gestionarlo.

Qué exige la ley

El marco de protección de datos de Egipto exige **aprobación previa** para las transferencias de datos personales fuera del país. Se trata de un modelo basado en autorización, y no en salvaguardas: no basta con establecer protecciones contractuales y proceder.

Por qué el modelo de aprobación cambia la selección de proveedores

Bajo un modelo de salvaguardas, un proveedor con cláusulas contractuales sólidas resulta viable. Bajo un modelo de aprobación, cada flujo transfronterizo constituye un proceso administrativo con plazos, discrecionalidad y riesgo de renovación asociados.

Una herramienta de seguridad que exporta telemetría de forma continua genera un flujo permanente que requiere que dicha aprobación siga vigente. Si la aprobación caduca o las condiciones cambian, el funcionamiento normal de la herramienta se convierte en un problema de cumplimiento.

La respuesta directa

La implementación local con air-gap (aislada de la red) no genera telemetría saliente: no se transfiere nada, por lo que no se requiere aprobación alguna. El almacenamiento provisional regional mantiene el procesamiento local en los casos en que se prefiera un modelo híbrido.

Las categorías con mayor probabilidad de atraer la atención regulatoria —claves, credenciales, tokens, contenido de archivos— nunca se recopilan, independientemente del modelo de implementación.

> Estado vigente al momento de la redacción: confirme los requisitos actuales y el procedimiento de aprobación con asesoría legal local.

¿Cyber Crucible cumple con la Ley de Protección de Datos de Ghana?

Respuesta breve: Sí, y Ghana es comparativamente sencilla. Ghana destaca entre las jurisdicciones africanas por **no** imponer requisitos adicionales sobre la transferencia transfronteriza más allá de sus obligaciones generales de protección de datos; por lo tanto, se aplican los controles estándar sin un régimen especial de transferencia.

Lo que exige la ley

Ghana cuenta con un marco establecido de protección de datos y una autoridad de supervisión. El análisis de las jurisdicciones africanas identifica sistemáticamente a Ghana como la excepción: a diferencia de la mayoría de sus vecinos, no añade condiciones adicionales específicamente al intercambio transfronterizo de datos.

Esto no significa que la transferencia no esté regulada; las obligaciones generales relativas al tratamiento lícito, la seguridad y los derechos de los interesados siguen aplicándose. Significa que no existe un obstáculo separado de aprobación o de adecuación que superar.

Qué se aplica específicamente en este caso

Una vez simplificada la cuestión de la transferencia, la evaluación se reduce a las cuestiones habituales:

- **¿Qué se recopila?** Únicamente telemetría del sistema y de seguridad. Ninguna clave, credencial, token o contenido.
- **¿Cómo se protege?** TLS 1.3 en tránsito, cifrado de carga útil JWE por agente, cifrado en reposo, acceso basado en roles.
- **¿Quién es responsable?** Cyber Crucible actúa como encargado del tratamiento en virtud de un DPA por escrito, conforme a sus instrucciones documentadas.

Aun así, vale la pena considerar la soberanía

Incluso sin una restricción de transferencia, sigue estando disponible el despliegue local o con aislamiento físico (air-gapped), y las organizaciones que atienden a clientes regionales a menudo lo prefieren, ya que las jurisdicciones vecinas son considerablemente más estrictas.

> Estado al momento de redactar este documento: confírmelo con asesoría legal local.

¿Cyber Crucible cumple con el requisito de localización de datos de Zambia?

Respuesta breve: Sí. La Ley de Protección de Datos de Zambia exige a los controladores procesar y almacenar datos personales y datos personales sensibles en un centro de datos o servidor **ubicado dentro de Zambia**. La implementación local (on-premises) de Cyber Crucible satisface esto directamente: el backend se ejecuta dentro de su propia infraestructura, en el país.

Qué exige la ley

La Parte X de la Ley de Protección de Datos de Zambia regula la transferencia transfronteriza, y la Sección 70 obliga a un controlador de datos a procesar y almacenar datos personales y datos personales sensibles en un centro de datos o servidor ubicado dentro de Zambia.

Se trata de un **mandato de ubicación de almacenamiento**, no de una prueba de salvaguardas. Las protecciones contractuales no lo satisfacen.

Por qué esto elimina a la mayoría de las herramientas de seguridad basadas en la nube

Un proveedor cuyo producto requiere enviar la telemetría del endpoint a una región de nube fuera de Zambia no puede cumplir con la Sección 70 mejorando sus contratos o su cifrado. El requisito se refiere a *dónde se encuentran físicamente los datos*.

Por qué esta arquitectura lo satisface

- **Backend local (on-premises)** — todo el software de gestión se ejecuta en servidores que usted controla, dentro de Zambia.
- **Análisis local** — la evaluación de amenazas y la interdicción ocurren en el propio endpoint, de modo que la protección nunca depende de un servicio fuera del país.

- **Cero telemetría saliente** en la configuración con air gap.
- **Alcance mínimo** — las claves, credenciales, tokens y contenido nunca se recopilan, por lo que el volumen de datos personales sujetos a la Sección 70 es reducido desde el principio.

> Estado al momento de escribir esto — confirme con asesoría legal local, incluyendo cualquier normativa específica del sector.

¿Cumple Cyber Crucible con la ley de protección de datos de Ruanda?

Respuesta breve: Sí. La ley de protección de datos de Ruanda está supervisada por la Autoridad Nacional de Ciberseguridad, y las normas específicas por sector añaden obligaciones de localización — en particular para los bancos con licencia, que deben mantener los datos primarios dentro de Ruanda. La implementación en las instalaciones satisface ambos requisitos.

Qué exige la ley

Ruanda promulgó una ley de protección de datos con la **Autoridad Nacional de Ciberseguridad (NCSA)** designada como autoridad de supervisión; su oficina de protección de datos se puso en marcha en marzo de 2022.

Junto con la ley general, la normativa sectorial añade la localización: la regulación de ciberseguridad exige que los bancos con licencia del Banco Central mantengan los datos primarios dentro del territorio ruandés.

Por qué la norma sectorial es la más importante

Para los servicios financieros en Ruanda, el requisito de localización bancaria suele ser la restricción vinculante — más estricta y específica que las disposiciones generales de protección de datos. Un producto de seguridad implementado en los endpoints de un banco procesa datos que quedan comprendidos dentro de ella.

Qué se aplica específicamente aquí

- **La implementación en las instalaciones** mantiene los datos primarios dentro de Ruanda, satisfaciendo directamente el requisito de localización.
- **El análisis local** significa que la protección no depende de ningún servicio fuera del país.

- **La alineación con la supervisión** — dado que la NCSA es tanto la autoridad de ciberseguridad como la de protección de datos, poder demostrar *qué* recopila una herramienta de seguridad, en términos enumerados, resulta especialmente útil.

> Estado al momento de escribir este documento — confirme los requisitos generales y sectoriales vigentes con asesoría legal local.

¿Cumple Cyber Crucible con la ley de protección de datos de Marruecos?

Respuesta breve: Sí. La Ley N.º 09-08 de Marruecos y su decreto de aplicación regulan el tratamiento de datos personales, bajo la supervisión de la CNDP. Se aplican los mismos controles: recopilación mínima, rol de encargado del tratamiento documentado, salvaguardas sólidas e implementación en el país o aislada de la red (air-gapped) cuando se prefiera.

Qué exige la ley

El marco jurídico de Marruecos se basa en la **Ley N.º 09-08** relativa a la protección de las personas físicas en lo referente al tratamiento de datos de carácter personal, junto con el **Decreto N.º 2-09-165** de aplicación. La **CNDP** (Commission Nationale de contrôle de la protection des Données à caractère Personnel) es la autoridad de control, y participa activamente en la cooperación internacional sobre temas emergentes, incluida la IA.

Qué se aplica específicamente aquí

El régimen de Marruecos se encuentra entre los más consolidados del norte de África, con una autoridad en funcionamiento y procedimientos de notificación/autorización que varían según el tipo de tratamiento. Implicaciones prácticas para la evaluación de proveedores:

- **Enumerar lo que se recopila.** La lista de datos excluidos de Cyber Crucible es explícita: sin claves, credenciales, tokens ni contenido, lo que respalda la precisión de las notificaciones.
- **Rol de encargado del tratamiento** conforme a un DPA (acuerdo de tratamiento de datos) escrito, sobre instrucciones documentadas.
- **Transferencia**: alojamiento provisional regional o implementación aislada de la red (air-gapped); esta última elimina la cuestión.

Para organizaciones que operan en el Magreb

Los requisitos difieren considerablemente entre Marruecos, Túnez, Argelia y Libia. Seleccionar un proveedor que cumpla con el régimen aplicable más estricto —en lugar de evaluar cada uno por separado— suele ser el camino que exige menos esfuerzo.

> Estado al momento de redactar este documento: confirmar con asesoría legal local.

¿Cuáles son los requisitos de protección de datos en Libia?

Respuesta breve: Libia aún no ha desarrollado una normativa integral de protección de datos. Esto convierte la soberanía de los datos en una decisión comercial, de seguridad y de contraparte, más que en una obligación de cumplimiento local, pero para las organizaciones que gestionan operaciones sensibles, sigue siendo una decisión que vale la pena tomar de manera deliberada.

La situación actual

Libia aún no ha promulgado un marco integral de protección de datos. No existe un equivalente al PDPL saudí, a la Ley 09-08 de Marruecos ni a la NDPA de Nigeria.

Por qué la soberanía sigue siendo importante sin una ley local

1. Las contrapartes imponen requisitos. Los socios internacionales, las aseguradoras, los clientes multinacionales y los financiadores exigen habitualmente, por contrato, un tratamiento equivalente al RGPD, independientemente de la legislación local. Cumplir con el estándar más estricto evita tener que renegociar más adelante.

2. Los sectores sensibles conllevan su propio riesgo. Las operaciones de energía, telecomunicaciones, finanzas y gobierno atraen atención independientemente de la legislación en materia de privacidad. Adónde envía la telemetría una herramienta de seguridad, y quién puede exigir acceso a ella allí, es una cuestión operativa genuina.

3. La regulación tiende a seguir. Las jurisdicciones vecinas en el norte de África han promulgado o actualizado sus marcos normativos. Las decisiones sobre proveedores que se tomen ahora seguirán vigentes cuando la posición de Libia cambie.

La postura práctica

Dado que Cyber Crucible nunca recopila claves, credenciales, tokens ni contenido, y puede funcionar completamente aislado (air-gapped) sin telemetría saliente, satisface los regímenes más estrictos de la región. En Libia, esto es una opción y no una obligación, pero es una opción que

envejece bien.

> Estado en el momento de redacción — confirme la situación legislativa actual con asesoría jurídica local antes de basarse en ella.

¿Cumple Cyber Crucible con el RGPD?

Respuesta breve: Sí, por diseño y no solo por política. El contenido, las credenciales, las claves de cifrado y los tokens de sesión nunca se recopilan; el análisis se realiza en el endpoint; Cyber Crucible actúa como encargado del tratamiento en virtud de un DPA por escrito; y las opciones de implementación mantienen los datos personales dentro de la UE, o dentro de sus propias instalaciones.

Correspondencia con los principios del RGPD

- **Minimización de datos (Art. 5)** — la lista de datos excluidos está enumerada de forma específica, no descrita en términos generales. La telemetría se limita a lo que la detección de amenazas requiere y es configurable.
- **Integridad y confidencialidad (Art. 5, 32)** — TLS 1.3 en tránsito, cifrado de carga útil JWE por agente, cifrado en reposo, control de acceso basado en roles, rotación de claves, registro de auditoría.
- **Obligaciones del encargado del tratamiento (Art. 28)** — DPA por escrito que especifica el alcance; tratamiento únicamente conforme a instrucciones documentadas; subencargados sujetos a condiciones equivalentes.
- **Transferencias (Capítulo V)** — almacenamiento provisional regional en la UE, o implementación con air-gap que elimina por completo la transferencia.
- **Protección de datos desde el diseño (Art. 25)** — la afirmación más sólida posible: las categorías de mayor riesgo no están protegidas por política, sino que nunca se recopilan.

Seudonimización

Cuando la telemetría de comportamiento pudiera identificar indirectamente a una persona, los identificadores se seudonimizan o enmascaran, una salvaguarda que el RGPD reconoce explícitamente.

Lo que esto no hace

Esto no hace que su organización cumpla con el RGPD. Sus obligaciones dependen de sus propios fines de tratamiento, bases jurídicas, avisos y registros. Lo que se elimina es una dificultad habitual: un proveedor de seguridad que exporta continuamente datos personales a un tercer país.

¿Cyber Crucible cumple con el UK GDPR?

Respuesta breve: Sí. El UK GDPR y la Data Protection Act 2018 siguen de cerca al GDPR de la UE, por lo que se aplica el mismo mapeo: recopilación mínima, rol de encargado del tratamiento bajo un DPA escrito, salvaguardas técnicas sólidas y opciones de implementación que mantienen los datos en el Reino Unido o completamente en sus instalaciones.

Qué aplica

Tras la salida del Reino Unido de la UE, el UK GDPR opera junto con la Data Protection Act 2018, supervisada por la Information Commissioner's Office (ICO). Los principios, las bases legales y las obligaciones del encargado del tratamiento reflejan estrechamente al GDPR de la UE.

Dónde las organizaciones deben prestar atención

- **Transferencias internacionales** utilizan los propios mecanismos del Reino Unido — el International Data Transfer Agreement (IDTA) o el UK Addendum a las SCC de la UE, en lugar de únicamente las SCC de la UE.
- **Cumplimiento dual** — las organizaciones que operan tanto en el Reino Unido como en la UE deben satisfacer ambos regímenes, aunque los controles prácticos se superponen casi por completo.

Qué aplica específicamente aquí

La evaluación es la misma que para el GDPR de la UE, y las respuestas son las mismas:

- Nunca se recopilan claves, credenciales, tokens ni contenidos de archivos.
- El análisis ocurre en el endpoint; la protección no requiere que los datos se muevan.
- Almacenamiento regional en el Reino Unido, o implementación con air-gap que elimina por completo la transferencia.
- Rol de encargado del tratamiento bajo un DPA escrito con subencargados vinculados a términos equivalentes.

> Para el instrumento de transferencia adecuado a sus circunstancias, contacte a **dpo@cybercrucible.com**. Estado al momento de escribir esto — confirme la guía actual de la ICO con su asesor legal.