- **IntelMind Cyber DD**

INFORME DE CYBER DUE DILIGENCE · M&A

Acme Industries Corp

Análisis completo de ciberriesgo outside-in de la empresa objetivo. 10 indicadores clave (KRIs), 130+ fuentes consultadas, generado en menos de 5 minutos. Verificable por timestamp RFC 3161.

JURISDICCIÓN

Estados Unidos

DOMINIO

Acme Industries.com

IDENTIFICADORES

CIK 9999999999 · LEI 0000ACME00CDFSAMPLE00 · EIN 00-0000000 · Reg. ACME-PUBLIC-SAMPLE

FECHA DEL ANÁLISIS

24 de mayo de 2026, 15:31

CONFIDENCIAL · SOLO DESTINATARIO

IMD-CDF-MPJXR35X-1TNV

RESUMEN EJECUTIVO

Veredicto en una página

Para directivos · 30 segundos de lectura · Decisión Go/No-Go

16

RIESGO CIBER GLOBAL: BAJO

Sin riesgos materiales detectados outside-in.

Media ponderada de 10 KRIs (Key Risk Indicators) sobre ciberseguridad, exposición ejecutiva, sanciones legales, fugas en dark web y typosquatting. 10/10 indicadores evaluados con éxito.

0	2	8
CRÍTICOS	MEDIOS	BAJOS

MAPA DE LOS 10 INDICADORES

01 Executive Digital Exposure — 44 El equipo directivo de Acme Industries Corp está públicamente identificado — lis...	02 Known Breaches & Credentials — 23 Exposición de credenciales de usuarios/terceros externos de Acme Industries
03 DNS Weaknesses & Hygiene — 12 Higiene de autenticación de correo mejorable en Acme Industries	04 Perimeter Security / EASM — 4 Sin servicios críticos expuestos en Acme Industries
05 Reputational & Sentiment — 0 Acme Industries Corp tiene cobertura de prensa (21 artículos en 12 meses) sin se...	06 Legal & Regulatory — 0 Acme Industries Corp no figura en las listas de sanciones de la OFAC (OFAC SDN L...
07 Supply Chain Risk — 16 Acme Industries Corp depende de 1 proveedores tecnológicos de terceros — superfi...	08 Malicious Infrastructure / Typosquatting — 35 9 dominios parecidos a Acme Industries
09 Shadow IT / Code Leaks — 0 No se detectaron ficheros que expongan Acme Industries	10 Dark Web Intelligence — 18 Datos asociados a Acme Industries Corp circulan en canales de cibercrimen

INDICADORES RESUMIDOS

Los 10 KRIs en formato tarjeta

Una tarjeta por indicador con **qué hemos encontrado** y **qué acción concreta debería tomar el equipo**. Pensado para revisión rápida y delegación a los equipos correspondientes. El detalle exhaustivo y las fuentes están en las secciones siguientes.

1 Executive Digital Exposure

PRE-CIERRE **44**/100 MEDIO

QUÉ SIGNIFICA

La empresa tiene información pública sobre su equipo directivo, lo que aumenta el riesgo de que se hagan pasar por ellos para estafar a la empresa o a sus clientes.

IMPACTO ECONÓMICO

€130k-2M. Esto puede resultar en pérdidas significativas si se engaña a la empresa o a sus clientes.

CÓMO ARREGLARLO

Concienciación anti-BEC para el C-suite y barrido de su PII personal en data brokers con solicitudes de retirada.

2 Known Breaches & Credentials

PRE-CIERRE **23**/100 BAJO

QUÉ SIGNIFICA

Existen credenciales de acceso a aplicaciones de Acme Industries en circulación pública, lo que aumenta el riesgo de que se produzcan fraudes o suplantaciones.

IMPACTO ECONÓMICO

€130k-2M. Esto puede resultar en estafas por suplantación de directivos o acceso no autorizado a sistemas críticos.

CÓMO ARREGLARLO

Forzar reseteo de las cuentas de usuario afectadas y revisar los accesos de terceros.

3 DNS Weaknesses & Hygiene

PRE-CIERRE **12**/100 BAJO

QUÉ SIGNIFICA

La empresa tiene debilidades en la autenticación de correos electrónicos, lo que puede facilitar fraudes y suplantaciones.

IMPACTO ECONÓMICO

€130k-2M. Esto representa el coste potencial de una estafa por suplantación de directivos.

CÓMO ARREGLARLO

Completar la autenticación de correo (DKIM / MTA-STS) y endurecer la política.

4 Perimeter Security / EASM

PRE-CIERRE 4/100 BAJO

QUÉ SIGNIFICA

La seguridad perimetral se refiere a la protección de la red de la empresa contra accesos no autorizados. Un mal control de los subdominios puede facilitar ataques.

IMPACTO ECONÓMICO

€5-15k. Una mala gestión de subdominios puede llevar a pérdidas por ataques que comprometan la operación.

CÓMO ARREGLARLO

Reducir el inventario de subdominios al mínimo necesario y retirar de internet los entornos de test.

5 Reputational & Sentiment

0/100 BAJO

QUÉ SIGNIFICA

Acme Industries Corp tiene cobertura de prensa (21 artículos en 12 meses) sin señales de crisis reputacional.

CÓMO ARREGLARLO

Sin acción reputacional inmediata. Mantener monitorización de prensa hasta el cierre.

6 Legal & Regulatory

0/100 BAJO

QUÉ SIGNIFICA

Acme Industries Corp no figura en las listas de sanciones de la OFAC (OFAC SDN List + OFAC Consolidated List) consultadas a fecha del análisis.

CÓMO ARREGLARLO

Sin acción requerida en el cribado de sanciones OFAC.

7 Supply Chain Risk

PRE-CIERRE 16/100 BAJO

QUÉ SIGNIFICA

La empresa depende de un proveedor externo que puede comprometer su seguridad.

IMPACTO ECONÓMICO

€380k-20M. Una brecha de datos puede resultar en multas significativas y pérdidas económicas.

CÓMO ARREGLARLO

Inventariar los proveedores críticos, revisar sus certificaciones de seguridad y exigir cláusulas de ciberseguridad en sus contratos antes del cierre.

8 Malicious Infrastructure / Typosquatting

PRE-CIERRE 35/100 MEDIO

QUÉ SIGNIFICA

Existen dominios similares al de Acme Industries que podrían ser utilizados para engañar a sus clientes o suplantar su marca.

IMPACTO ECONÓMICO

€130k-2M. Esto representa el costo potencial de una estafa por suplantación de directivos.

CÓMO ARREGLARLO

Verificar por WHOIS la titularidad, monitorizar los dominios y registrar defensivamente las variantes críticas que sigan libres.

9 Shadow IT / Code Leaks

0/100 BAJO

QUÉ SIGNIFICA

No se detectaron ficheros que expongan Acme Industries.com en contextos de secreto (.env, credenciales) en GitHub.

CÓMO ARREGLARLO

Sin acción inmediata. Mantener vigilancia de repositorios públicos.

10 Dark Web Intelligence

PRE-CIERRE 18/100 BAJO

QUÉ SIGNIFICA

Datos de Acme Industries Corp están en mercados ilegales, lo que indica un riesgo de ataque inminente.

IMPACTO ECONÓMICO

€1-3M. Un ataque podría paralizar la operación y requerir un rescate.

CÓMO ARREGLARLO

Vigilar los canales de cibercrimen y, para una due diligence M&A completa, activar un feed de inteligencia de dark web de pago.

ANÁLISIS DETALLADO

Análisis por indicador

Por cada KRI: amenaza concreta, impacto en el deal, acción al grano (o múltiples si las hay), hallazgos individuales numerados y recomendación personalizada para esta empresa.

KRI 1 Executive Digital Exposure

44/100 MEDIO

PARA EL INVERSOR — PRE-CIERRE

La exposición de los ejecutivos de Acme Industries Corp a ataques de suplantación es preocupante. Con 18 miembros del gobierno corporativo identificados públicamente, el riesgo de que atacantes se hagan pasar por ellos para engañar a la empresa o a sus clientes es alto. Este tipo de ataques puede resultar en pérdidas económicas considerables, ya que los estafadores pueden solicitar pagos de facturas falsas o robar información sensible. En el contexto de una adquisición, este riesgo puede afectar la valoración de la empresa y su reputación, como se evidenció en casos como el de Yahoo-Verizon, donde se aplicó un descuento de $350M tras una brecha de seguridad.

IMPACTO ECONÓMICO

€130k-2M. Esto puede resultar en pérdidas significativas si se engaña a la empresa o a sus clientes.

CÓMO ARREGLARLO

Realizar una concienciación anti-suplantación para el equipo directivo y limpiar la información personal en data brokers.

QUIÉN	Consultora ciber mediana tipo Telefónica Tech o S21Sec.
CÓMO	1) Auditoría de la información pública del equipo directivo.,2) Solicitar la retirada de información personal en data brokers.,3) Implementar formación anti-suplantación para el C-suite.
CUÁNDO	Antes del cierre del deal.
TIEMPO	1 mes.
COSTE SOLUCIÓN	**€30-80k.**
DIFICULTAD	MEDIA
SEVERIDAD	MEDIA

DETALLE TÉCNICO — AMENAZA DETECTADA

El equipo directivo de Acme Industries Corp está públicamente identificado — lista de objetivos lista para spear-phishing y suplantación de ejecutivos.

QUÉ PUEDE PASAR (TÉCNICO)

Con los nombres y cargos del C-suite (públicos por mandato SEC), un atacante ensambla un paquete de targeting de precisión: spear-phishing, suplantación de ejecutivos y fraude del CEO se vuelven directamente ejecutables. La exposición se agrava si los datos personales (domicilios, móviles, familiares) figuran además en bases de data brokers — periodos de transición como una operación M&A son un disparador documentado de Business Email Compromise.

ACCIÓN RECOMENDADA (TÉCNICO)

Concienciación anti-BEC para el C-suite y barrido de su PII personal en data brokers con solicitudes de retirada.

HALLAZGOS INDIVIDUALES (1)

1 **Gobierno corporativo de Acme Industries Corp públicamente identificado: 18 personas (7 con cargo ejecutivo, 10 consejeros).** Confianza 82

A partir de las declaraciones SEC (Forms 3/4) se identifican 18 miembros del gobierno corporativo con nombre y cargo. Esta información es pública por mandato regulatorio — un atacante dispone de la lista de objetivos de spear-phishing y fraude del CEO sin esfuerzo. Identificados: Julie Mchugh; Sam R Leno; Gary J Pruden; Phuong Khanh Morrow; Minnie Baylor-henry; Gerard Ber; James H Thrall; Heinz Christoph Maeusli; Ludger Dinkelborg (See Remarks); Robert J. Jr. Marshall (CFO and Treasurer); Daniel Niedzwiecki (See Remarks); Kimberly Brown (Chief Accounting Officer); Amanda Michelle Morgan (Chief Commercial Officer); Julia Marie Eastland.

RECOMENDACIÓN PERSONALIZADA

Plan de exposición ejecutiva para Acme Industries Corp:
1. Gobierno corporativo identificado de Acme Industries Corp (18): Julie Mchugh — Consejero; Sam R Leno — Consejero; Gary J Pruden — Consejero; Phuong Khanh Morrow — Consejero; Minnie Baylor-henry — Consejero; Gerard Ber — Consejero; James H Thrall — Consejero; Heinz Christoph Maeusli — Consejero; Ludger Dinkelborg — See Remarks; Robert J. Jr. Marshall — CFO and Treasurer; Daniel Niedzwiecki — See Remarks; Kimberly Brown — Chief Accounting Officer; Amanda Michelle Morgan — Chief Commercial Officer; Julia Marie Eastland — Consejero; Mary Anne Heino — Executive Chair; Rajiv A Patel; Paul Blanchfield — President; Partners L L C/ca Farallon.
2. Prioridad de protección — cargos de máxima exposición a fraude del CEO/BEC: Robert J. Jr. Marshall, Kimberly Brown, Amanda Michelle Morgan, Mary Anne Heino, Paul Blanchfield. Barrido de su PII personal (domicilio, móvil, familiares) en data brokers y solicitudes de retirada (opt-out).
3. Activar formación anti-BEC específica para el C-suite y verificación fuera de banda obligatoria para órdenes de pago/transferencia, especialmente durante el periodo de la operación.
4. Para cuantificar la exposición de PII personal del C-suite en data brokers se requiere activar un feed de data brokers — recomendado para completar este indicador.

FUENTES VERIFICABLES DE ESTE INDICADOR

HALLAZGO / CONSULTA	FUENTE	VERIFICABLE EN
Gobierno corporativo de Acme Industries Corp públicamente identificado: 18 personas (7 con cargo ejecutivo, 10 consejeros).	SEC EDGAR (Forms 3/4)	www.sec.gov/

Confianza global: **MEDIA** Fuentes consultadas: **1**

KRI 2

Known Breaches & Credentials

23/100 BAJO

PARA EL INVERSOR — PRE-CIERRE

La exposición de credenciales de usuarios y terceros de Acme Industries en registros de ataques aumenta el riesgo de que un atacante acceda a sus sistemas. Esto puede llevar a fraudes, como suplantar a un directivo para que sus clientes paguen facturas falsas. En el contexto de una compra, este riesgo puede traducirse en pérdidas significativas y en un coste adicional para mitigar el problema. Por ejemplo, incidentes similares han llevado a descuentos en valoraciones, como el caso de Yahoo-Verizon, que sufrió un ajuste de $350M tras una brecha de seguridad. La falta de atención a este problema puede resultar en un coste oculto entre el 5% y el 15% del precio del acuerdo.

IMPACTO ECONÓMICO	**€130k-2M. Esto puede resultar en estafas por suplantación de directivos o acceso no autorizado a sistemas críticos.**

CÓMO ARREGLARLO

Forzar el reseteo de las cuentas de usuario afectadas y revisar los accesos de terceros.

QUIÉN	Consultora de ciberseguridad mediana tipo Telefónica Tech o S21Sec.
CÓMO	1) Identificar las cuentas afectadas.,2) Forzar el reseteo de contraseñas de los usuarios implicados.,3) Revisar y limitar los accesos de terceros.,4) Implementar formación sobre seguridad para los empleados.
CUÁNDO	Antes del cierre del deal.
TIEMPO	1 semana.
COSTE SOLUCIÓN	**€5-15k.**
DIFICULTAD	BAJA
SEVERIDAD	MEDIA

DETALLE TÉCNICO — AMENAZA DETECTADA

Exposición de credenciales de usuarios/terceros externos de Acme Industries.com en stealer logs; sin equipos de empleados comprometidos.

QUÉ PUEDE PASAR (TÉCNICO)

Los empleados de la empresa no figuran comprometidos — el riesgo interno es bajo. Sí hay credenciales de usuarios externos / terceros: riesgo para las cuentas de cliente y para accesos de proveedores a las aplicaciones de la empresa.

ACCIÓN RECOMENDADA (TÉCNICO)

Forzar reseteo de las cuentas de usuario afectadas y revisar los accesos de terceros.

HALLAZGOS INDIVIDUALES (2)

1 **3 usuario(s) de aplicaciones de Acme Industries.com aparecen en stealer logs.** Confianza 80

HudsonRock detecta 3 máquina(s) de usuarios externos infectadas con credenciales de acceso a aplicaciones de Acme Industries.com. Aplicaciones afectadas: https://ecommerce.Acme Industries.com/cgi-bin/lansaweb, http://visitor.Acme Industries.com/ar/Login.aspx, https://help.Acme Industries.com.

2 **2 tercero(s) con acceso relacionado con Acme Industries.com aparecen en stealer logs.** Confianza 75

HudsonRock detecta 2 máquina(s) de terceros (proveedores/colaboradores) infectadas con credenciales relacionadas con Acme Industries.com.

RECOMENDACIÓN PERSONALIZADA

Plan de remediación de credenciales para Acme Industries Corp (Acme Industries.com):
1. 3 usuario(s) de aplicaciones de Acme Industries.com comprometidos (https://ecommerce.Acme Industries.com/cgi-bin/lansaweb, http://visitor.Acme Industries.com/ar/Login.aspx, https://help.Acme Industries.com). Forzar reseteo de esas cuentas y activar MFA obligatorio en esas aplicaciones.
2. 2 tercero(s) con accesos comprometidos — revisar y rotar las credenciales de los proveedores/colaboradores con acceso a sistemas de Acme Industries Corp.
3. Ampliar el cribado a bases de brechas históricas (HIBP) y a la monitorización continua de nuevos stealer logs.

FUENTES VERIFICABLES DE ESTE INDICADOR

HALLAZGO / CONSULTA	FUENTE	VERIFICABLE EN
3 usuario(s) de aplicaciones de Acme Industries.com aparecen en stealer logs.	HudsonRock Cavalier	www.hudsonrock.com/
2 tercero(s) con acceso relacionado con Acme Industries.com aparecen en stealer logs.	HudsonRock Cavalier	www.hudsonrock.com/

Confianza global: **MEDIA** Fuentes consultadas: **1**

KRI 3 DNS Weaknesses & Hygiene

12/100 BAJO

PARA EL INVERSOR — PRE-CIERRE

La falta de una política restrictiva en la autenticación de correos electrónicos expone a Acme Industries a riesgos de suplantación, donde atacantes pueden hacerse pasar por la empresa para estafar a clientes o proveedores. Aunque actualmente no hay una exposición crítica, el riesgo de que un atacante aproveche esta debilidad es real y podría resultar en pérdidas significativas. En el contexto de una fusión o adquisición, este tipo de vulnerabilidad puede afectar la valoración de la empresa y generar costes adicionales en caso de un incidente. Ejemplos como el caso de Yahoo, que sufrió un descuento de $350M en su valoración por problemas de seguridad, subrayan la importancia de abordar estas debilidades antes de cerrar un trato.

IMPACTO ECONÓMICO **€130k-2M. Esto representa el coste potencial de una estafa por suplantación de directivos.**

CÓMO ARREGLARLO

Completar la autenticación de correo y endurecer la política de seguridad.

QUIÉN	Consultora ciber mediana tipo Telefónica Tech o S21Sec.
CÓMO	1) Realizar una auditoría de la configuración actual de DNS.,2) Implementar DKIM y MTA-STS.,3) Endurecer la política SPF para incluir un mecanismo restrictivo.,4) Capacitar al personal sobre la importancia de la seguridad en la comunicación.
CUÁNDO	Antes del cierre del deal.
TIEMPO	1 semana.
COSTE SOLUCIÓN	**€5-15k.**
DIFICULTAD	BAJA
SEVERIDAD	MEDIA

DETALLE TÉCNICO — AMENAZA DETECTADA

Higiene de autenticación de correo mejorable en Acme Industries.com, sin exposición crítica de suplantación.

QUÉ PUEDE PASAR (TÉCNICO)

Margen de mejora en la configuración; el riesgo de suplantación directa del dominio es limitado con la política actual.

ACCIÓN RECOMENDADA (TÉCNICO)

Completar la autenticación de correo (DKIM / MTA-STS) y endurecer la política.

HALLAZGOS INDIVIDUALES (1)

1 **El SPF de Acme Industries.com no termina en '-all' ni '~all' — política ambigua.** Confianza 85

Registro SPF actual: v=spf1 redirect=_sssh9fwyv.sdmarc.net. Sin un mecanismo 'all' restrictivo, los receptores no saben qué hacer con remitentes no listados.

RECOMENDACIÓN PERSONALIZADA

Plan de remediación para Acme Industries Corp (Acme Industries.com):
1. Cerrar el SPF de Acme Industries.com terminándolo en "-all" (hard fail). Registro actual: v=spf1 redirect=_sssh9fwyv.sdmarc.net

FUENTES VERIFICABLES DE ESTE INDICADOR

HALLAZGO / CONSULTA	FUENTE	VERIFICABLE EN
El SPF de Acme Industries.com no termina en '-all' ni '~all' — política ambigua.	DNS (consulta directa)	–

Confianza global: **BAJA** Fuentes consultadas: **1**

KRI 4 **Perimeter Security / EASM** 4/100 BAJO

PARA EL INVERSOR — PRE-CIERRE

La empresa Acme Industries Corp presenta una amplia superficie de ataque con 54 subdominios, lo que aumenta el riesgo de que un atacante encuentre un punto de entrada. Aunque actualmente no hay servicios críticos expuestos, la falta de control sobre tantos subdominios puede facilitar ataques que comprometan la seguridad de la empresa. En el contexto de una fusión o adquisición, esto es crucial, ya que cualquier incidente podría resultar en pérdidas significativas y afectar la valoración de la empresa. Por ejemplo, el caso de Yahoo-Verizon, donde se aplicó un descuento de $350M tras una brecha de seguridad, subraya la importancia de abordar estos riesgos antes del cierre.

IMPACTO ECONÓMICO **€5-15k. Una mala gestión de subdominios puede llevar a pérdidas por ataques que comprometan la operación.**

CÓMO ARREGLARLO

Reducir el número de subdominios a los estrictamente necesarios y eliminar entornos de prueba de internet.

QUIÉN	Consultora de ciberseguridad tipo S21Sec o Telefónica Tech.
CÓMO	1) Realizar un inventario de todos los subdominios.,2) Evaluar la necesidad de cada subdominio.,3) Eliminar los subdominios innecesarios.,4) Asegurar que los entornos de prueba no estén accesibles desde internet.
CUÁNDO	Antes del cierre del deal.
TIEMPO	1 semana.
COSTE SOLUCIÓN	**€5-15k.**
DIFICULTAD	BAJA
SEVERIDAD	MEDIA

DETALLE TÉCNICO — AMENAZA DETECTADA

Sin servicios críticos expuestos en Acme Industries.com; superficie de ataque contenida.

QUÉ PUEDE PASAR (TÉCNICO)

La exposición perimetral se limita a servicios web estándar. El riesgo principal es la extensión del inventario, que amplía la superficie a vigilar.

ACCIÓN RECOMENDADA (TÉCNICO)

Reducir el inventario de subdominios al mínimo necesario y retirar de internet los entornos de test.

HALLAZGOS INDIVIDUALES (1)

1 **Superficie de ataque amplia: 54 subdominios de Acme Industries.com.** Confianza 85

Netlas inventaría 54 subdominios bajo Acme Industries.com. Cada subdominio es un punto de entrada potencial; un inventario tan amplio dificulta el control y suele incluir activos olvidados o sin mantenimiento.

RECOMENDACIÓN PERSONALIZADA

Plan de perímetro para Acme Industries Corp (Acme Industries.com):
1. Inventariar los 54 subdominios de Acme Industries.com, dar de baja los obsoletos y dejar expuestos solo los imprescindibles.

FUENTES VERIFICABLES DE ESTE INDICADOR

HALLAZGO / CONSULTA	FUENTE	VERIFICABLE EN
Superficie de ataque amplia: 54 subdominios de Acme Industries.com.	Netlas.io	netlas.io/

Confianza global: **MEDIA** Fuentes consultadas: **1**

KRI 5 Reputational & Sentiment

0/100 BAJO

SITUACIÓN

Acme Industries Corp tiene cobertura de prensa (21 artículos en 12 meses) sin señales de crisis reputacional.

ACCIÓN RECOMENDADA (TÉCNICO)

Sin acción reputacional inmediata. Mantener monitorización de prensa hasta el cierre.

HALLAZGOS INDIVIDUALES (0)

Sin hallazgos individuales en este indicador.

RECOMENDACIÓN PERSONALIZADA

No se detectaron señales de crisis reputacional para Acme Industries Corp en la prensa global (GDELT, últimos 12 meses). Mantener la monitorización hasta el cierre de la operación.

FUENTES VERIFICABLES DE ESTE INDICADOR

HALLAZGO / CONSULTA	FUENTE	VERIFICABLE EN
— consultada, sin hallazgos en esta ejecución —	*GDELT*	*www.gdeltproject.org/*

Confianza global: **MEDIA** Fuentes consultadas: **1**

KRI 6 Legal & Regulatory

0/100 BAJO

SITUACIÓN

Acme Industries Corp no figura en las listas de sanciones de la OFAC (OFAC SDN List + OFAC Consolidated List) consultadas a fecha del análisis.

ACCIÓN RECOMENDADA (TÉCNICO)

Sin acción requerida en el cribado de sanciones OFAC.

HALLAZGOS INDIVIDUALES (0)

Sin hallazgos individuales en este indicador.

RECOMENDACIÓN PERSONALIZADA

Acme Industries Corp no aparece en las listas OFAC consultadas. Para una due diligence legal completa, ampliar el cribado a las listas de la UE y la ONU, y revisar la sección "Legal Proceedings" del último 10-K para litigios y acciones regulatorias materiales.

FUENTES VERIFICABLES DE ESTE INDICADOR

HALLAZGO / CONSULTA	FUENTE	VERIFICABLE EN
— consultada, sin hallazgos en esta ejecución —	***OFAC SDN List***	–
— consultada, sin hallazgos en esta ejecución —	***OFAC Consolidated List***	–

Confianza global: **ALTA** Fuentes consultadas: **2**

KRI 7 Supply Chain Risk

16/100 BAJO

PARA EL INVERSOR — PRE-CIERRE

Acme Industries Corp tiene dependencia de un proveedor tecnológico que, si sufre un incidente de seguridad, puede afectar directamente a la empresa. Esto incluye la posibilidad de que datos sensibles sean robados o que los sistemas queden inoperativos, lo que podría paralizar la operación durante días. En el contexto de una fusión o adquisición, este riesgo puede traducirse en una pérdida de valor significativo, como se evidenció en casos como el de Marriott-Starwood, donde la multa por una brecha alcanzó los €110M. Es crucial evaluar la seguridad de los proveedores antes de cerrar el trato.

IMPACTO ECONÓMICO

€380k-20M. Una brecha de datos puede resultar en multas significativas y pérdidas económicas.

CÓMO ARREGLARLO

Inventariar los proveedores críticos y revisar sus certificaciones de seguridad.

QUIÉN	Consultora ciber mediana tipo Telefónica Tech o S21Sec.
CÓMO	1) Identificar todos los proveedores tecnológicos críticos.,2) Revisar las certificaciones de seguridad de cada proveedor.,3) Exigir cláusulas de ciberseguridad en los contratos.,4) Establecer un plan de auditoría continua.
CUÁNDO	Antes del cierre del deal.
TIEMPO	1 mes.
COSTE SOLUCIÓN	**€30k-80k.**
DIFICULTAD	MEDIA
SEVERIDAD	MEDIA

DETALLE TÉCNICO — AMENAZA DETECTADA

Acme Industries Corp depende de 1 proveedores tecnológicos de terceros — superficie de riesgo heredada.

QUÉ PUEDE PASAR (TÉCNICO)

Cada proveedor SaaS, cloud o de seguridad es un punto de fallo que el comprador hereda. Un atacante puede pivotar hacia la empresa a través de un proveedor comprometido (ataque de cadena de suministro), y una brecha en cualquiera de ellos expone datos del objetivo. El 60% de las brechas se originan en un tercero — y se heredan con la adquisición.

ACCIÓN RECOMENDADA (TÉCNICO)

Inventariar los proveedores críticos, revisar sus certificaciones de seguridad y exigir cláusulas de ciberseguridad en sus contratos antes del cierre.

HALLAZGOS INDIVIDUALES (1)

1 **1 proveedores tecnológicos de terceros identificados en la cadena de suministro de Acme Industries Corp.** Confianza 80

Mediante señales DNS/HTTP públicas se identifican 1 proveedores de terceros de los que depende Acme Industries.com: Email / Workspace (Microsoft 365). Cada proveedor es una dependencia cuya seguridad el comprador hereda — el 60% de las brechas se originan en un tercero.

RECOMENDACIÓN PERSONALIZADA

Cadena de suministro de Acme Industries Corp (Acme Industries.com):
1. Proveedores de terceros identificados: Microsoft 365 [Email / Workspace].
2. Para cada proveedor crítico (cloud, email, identidad/SSO): solicitar sus informes de seguridad (SOC 2 / ISO 27001) y verificar su historial de brechas.
3. Revisar los contratos para confirmar cláusulas de notificación de incidentes y responsabilidad — el comprador hereda este riesgo.
4. Para un scoring de riesgo por proveedor (brechas conocidas, rating de seguridad), activar un feed dedicado de supply-chain risk.

FUENTES VERIFICABLES DE ESTE INDICADOR

HALLAZGO / CONSULTA	FUENTE	VERIFICABLE EN
1 proveedores tecnológicos de terceros identificados en la cadena de suministro de Acme Industries Corp.	**DNS / HTTP (consulta directa)**	–
— consultada, sin hallazgos en esta ejecución —	*DNS / HTTP*	*www.iana.org/*

Confianza global: **MEDIA** Fuentes consultadas: **1**

KRI 8

Malicious Infrastructure / Typosquatting

35/100 MEDIO

PARA EL INVERSOR — PRE-CIERRE

Se han detectado múltiples dominios registrados que imitan el nombre de Acme Industries. Estos dominios pueden ser utilizados para engañar a los clientes, haciéndose pasar por la empresa y solicitando pagos de facturas falsas. Esto no solo afecta la reputación de la empresa, sino que también puede resultar en pérdidas financieras significativas. En el contexto de una adquisición, este riesgo puede traducirse en un descuento en el valor de la transacción, similar al caso de Yahoo y Verizon, donde se aplicó un descuento de $350M tras una brecha de seguridad. La falta de acción puede llevar a un daño considerable en la confianza del cliente y en la estabilidad financiera de la empresa.

IMPACTO ECONÓMICO **€130k-2M. Esto representa el costo potencial de una estafa por suplantación de directivos.**

CÓMO ARREGLARLO

Registrar defensivamente los dominios críticos y monitorizar los existentes.

QUIÉN	Consultora ciber mediana tipo S21Sec o Telefónica Tech.
CÓMO	1) Verificar la titularidad de los dominios a través de WHOIS.,2) Monitorizar los dominios registrados para detectar actividad sospechosa.,3) Registrar defensivamente las variantes críticas que estén disponibles.
CUÁNDO	Antes del cierre del deal.
TIEMPO	1 mes.
COSTE SOLUCIÓN	**€5-15k.**
DIFICULTAD	BAJA
SEVERIDAD	MEDIA

DETALLE TÉCNICO — AMENAZA DETECTADA

9 dominios parecidos a Acme Industries.com están registrados por terceros; 1 con servidor de correo — vector latente de phishing.

QUÉ PUEDE PASAR (TÉCNICO)

Estos dominios lookalike pueden activarse en cualquier momento para enviar correo casi idéntico al de la empresa o alojar páginas falsas. Es exposición latente: el atacante ya tiene la infraestructura, falta solo que la use.

ACCIÓN RECOMENDADA (TÉCNICO)

Verificar por WHOIS la titularidad, monitorizar los dominios y registrar defensivamente las variantes críticas que sigan libres.

HALLAZGOS INDIVIDUALES (9)

1 **Dominio similar registrado: antheus.com — con web activa** — Confianza 88

antheus.com es una variación tipográfica de Acme Industries.com, registrada y sin compartir la infraestructura DNS del dominio legítimo. Su titularidad (defensiva vs. de un tercero) no está confirmada — verificar por WHOIS. Registrador: GoDaddy.com, LLC.

2 **Dominio similar registrado: latheus.com — con servidor de correo activo** — Confianza 88

latheus.com es una variación tipográfica de Acme Industries.com, registrada y sin compartir la infraestructura DNS del dominio legítimo. Su titularidad (defensiva vs. de un tercero) no está confirmada — verificar por WHOIS. Registrador: NameCheap, Inc.. Tiene servidor de correo — capaz de suplantar a la empresa por email.

3 **Dominio similar registrado: Acme.com — con web activa** — Confianza 88

Acme.com es una variación tipográfica de Acme Industries.com, registrada y sin compartir la infraestructura DNS del dominio legítimo. Su titularidad (defensiva vs. de un tercero) no está confirmada — verificar por WHOIS. Registrador: TurnCommerce, Inc. DBA NameBright.com.

4 **Dominio similar registrado: Acme.com — con web activa** — Confianza 88

Acme.com es una variación tipográfica de Acme Industries.com, registrada y sin compartir la infraestructura DNS del dominio legítimo. Su titularidad (defensiva vs. de un tercero) no está confirmada — verificar por WHOIS. Registrador: Wild West Domains, LLC.

5 **Dominio similar registrado: pantheus.com — con web activa** — Confianza 88

pantheus.com es una variación tipográfica de Acme Industries.com, registrada y sin compartir la infraestructura DNS del dominio legítimo. Su titularidad (defensiva vs. de un tercero) no está confirmada — verificar por WHOIS. Registrador: NameSilo, LLC.

6 **Dominio similar registrado: Acme Industries.net — con web activa** — Confianza 88

Acme Industries.net es una variación tipográfica de Acme Industries.com, registrada y sin compartir la infraestructura DNS del dominio legítimo. Su titularidad (defensiva vs. de un tercero) no está confirmada — verificar por WHOIS. Registrador: Network Solutions, LLC.

7 **Dominio similar registrado: Acme Industries.org — con web activa** — Confianza 88

Acme Industries.org es una variación tipográfica de Acme Industries.com, registrada y sin compartir la infraestructura DNS del dominio legítimo. Su titularidad (defensiva vs. de un tercero) no está confirmada — verificar por WHOIS. Registrador: Network Solutions, LLC.

8 **Dominio similar registrado: Acme Industries.biz — con web activa** — Confianza 88

Acme Industries.biz es una variación tipográfica de Acme Industries.com, registrada y sin compartir la infraestructura DNS del dominio legítimo. Su titularidad (defensiva vs. de un tercero) no está confirmada — verificar por WHOIS. Registrador: Network Solutions, LLC.

9 **Dominio similar registrado: Acme Industries.info — con web activa** — Confianza 88

Acme Industries.info es una variación tipográfica de Acme Industries.com, registrada y sin compartir la infraestructura DNS del dominio legítimo. Su titularidad (defensiva vs. de un tercero) no está confirmada — verificar por WHOIS. Registrador: Network Solutions, LLC.

RECOMENDACIÓN PERSONALIZADA

Plan de typosquatting para Acme Industries Corp (Acme Industries.com):
1. Dominios con servidor de correo capaces de suplantar a Acme Industries Corp: latheus.com. Verificar su titularidad por WHOIS; los que no sean defensivos, vigilar y solicitar takedown si se activan.
2. Vigilar estos dominios lookalike registrados (sin correo aún): antheus.com, Acme.com, Acme.com, pantheus.com, Acme Industries.net, Acme Industries.org, Acme Industries.biz, Acme Industries.info.
3. Nota: la confirmación de uso malicioso activo requiere activar una clave de URLhaus/abuse.ch (gratuita) — recomendado para distinguir amenaza activa de exposición latente.
4. Registrar defensivamente las variantes tipográficas críticas de Acme Industries.com que sigan libres y activar monitorización continua.

FUENTES VERIFICABLES DE ESTE INDICADOR

HALLAZGO / CONSULTA	FUENTE	VERIFICABLE EN
Dominio similar registrado: antheus.com — con web activa	DNS (consulta directa)	–
Dominio similar registrado: latheus.com — con servidor de correo activo	DNS (consulta directa)	–
Dominio similar registrado: Acme.com — con web activa	DNS (consulta directa)	–
Dominio similar registrado: Acme.com — con web activa	DNS (consulta directa)	–
Dominio similar registrado: pantheus.com — con web activa	DNS (consulta directa)	–
Dominio similar registrado: Acme Industries.net — con web activa	DNS (consulta directa)	–
Dominio similar registrado: Acme Industries.org — con web activa	DNS (consulta directa)	–

HALLAZGO / CONSULTA	FUENTE	VERIFICABLE EN
Dominio similar registrado: Acme Industries.biz — con web activa	DNS (consulta directa)	–
Dominio similar registrado: Acme Industries.info — con web activa	DNS (consulta directa)	–
— consultada, sin hallazgos en esta ejecución —	*RDAP*	*about.rdap.org/*

Confianza global: **MEDIA** Fuentes consultadas: **2**

KRI 9 Shadow IT / Code Leaks

0/100 BAJO

SITUACIÓN

No se detectaron ficheros que expongan Acme Industries.com en contextos de secreto (.env, credenciales) en GitHub.

ACCIÓN RECOMENDADA (TÉCNICO)

Sin acción inmediata. Mantener vigilancia de repositorios públicos.

HALLAZGOS INDIVIDUALES (0)

Sin hallazgos individuales en este indicador.

RECOMENDACIÓN PERSONALIZADA

No se hallaron secretos del dominio Acme Industries.com en contextos de riesgo en GitHub a fecha del análisis. Recomendado ampliar la vigilancia continua a GitLab y Pastebin. Ausencia de evidencia no equivale a evidencia de ausencia.

FUENTES VERIFICABLES DE ESTE INDICADOR

HALLAZGO / CONSULTA	FUENTE	VERIFICABLE EN
— consultada, sin hallazgos en esta ejecución —	*GitHub Code Search*	*github.com/search*

Confianza global: **MEDIA** Fuentes consultadas: **1**

KRI 10 Dark Web Intelligence

18/100 BAJO

PARA EL INVERSOR — PRE-CIERRE

La presencia de datos de Acme Industries Corp en canales de cibercrimen sugiere que los atacantes pueden intentar suplantar a la empresa o extorsionarla. Esto puede resultar en un secuestro de sistemas, lo que podría paralizar las operaciones durante días o semanas. En el contexto de una adquisición, esto representa un riesgo significativo, ya que el comprador podría enfrentar pérdidas económicas directas y daños a su reputación. Ejemplos como el caso de Equifax, que sufrió pérdidas de $1.4B tras un incidente, subrayan la importancia de abordar este riesgo antes del cierre del acuerdo.

IMPACTO ECONÓMICO **€1-3M. Un ataque podría paralizar la operación y requerir un rescate.**

CÓMO ARREGLARLO

Implementar un monitoreo activo de los canales de cibercrimen y activar un servicio de inteligencia de la dark web.

QUIÉN	Consultora ciber mediana tipo S21Sec o Telefónica Tech.
CÓMO	1) Realizar un análisis inicial de los datos en la dark web.,2) Establecer un servicio de monitoreo continuo de amenazas.,3) Desarrollar un plan de respuesta ante incidentes.,4) Capacitar al personal sobre riesgos asociados.
CUÁNDO	Antes del cierre del deal.
TIEMPO	1 mes
COSTE SOLUCIÓN	**€30-80k**
DIFICULTAD	MEDIA
SEVERIDAD	MEDIA

DETALLE TÉCNICO — AMENAZA DETECTADA

Datos asociados a Acme Industries Corp circulan en canales de cibercrimen.

QUÉ PUEDE PASAR (TÉCNICO)

Datos relacionados con la empresa circulan en canales de cibercrimen, sin credenciales de empleados entre ellos. Riesgo de dark web contenido según la cobertura disponible.

ACCIÓN RECOMENDADA (TÉCNICO)

Vigilar los canales de cibercrimen y, para una due diligence M&A completa, activar un feed de inteligencia de dark web de pago.

HALLAZGOS INDIVIDUALES (1)

1 **Datos asociados a Acme Industries.com circulan en canales de cibercrimen (stealer logs): 5 registro(s).** Confianza 60

HudsonRock —fuente de inteligencia de cibercrimen— detecta 5 registro(s) de stealer logs asociados a Acme Industries.com (0 de empleados, 3 de usuarios, 2 de terceros). Los stealer logs son la mercancía principal de los mercados de dark web: estas credenciales y sesiones son comprables por un atacante.

RECOMENDACIÓN PERSONALIZADA

Inteligencia de dark web para Acme Industries Corp (Acme Industries.com):
1. Datos asociados a Acme Industries.com circulan en canales de cibercrimen (stealer logs): 5 registro(s).
2. Vigilar la evolución de la exposición en los próximos meses.
3. Cobertura parcial: la inteligencia profunda de dark web (foros cerrados de Initial Access Brokers, listados "access for sale") requiere activar un feed de pago. Activarlo es necesario para cubrir los listados "access for sale" de los foros cerrados — el indicador de mayor valor de este KRI en M&A.

FUENTES VERIFICABLES DE ESTE INDICADOR

HALLAZGO / CONSULTA	FUENTE	VERIFICABLE EN
Datos asociados a Acme Industries.com circulan en canales de cibercrimen (stealer logs): 5 registro(s).	HudsonRock Cavalier	www.hudsonrock.com/

Confianza global: **BAJA** Fuentes consultadas: **1**

FUENTES VERIFICABLES

Trazabilidad completa

Cada hallazgo de este informe procede de una **fuente pública verificable**. Esta sección enumera todas las URLs y fuentes consultadas, agrupadas por KRI. **No nos creas — verifica.** Si una URL no responde en el futuro, conservamos la captura del momento del análisis con sello RFC 3161 disponible bajo petición.

1 Executive Digital Exposure

1 hallazgos · 1 fuentes consultadas

HALLAZGO / CONSULTA	FUENTE	VERIFICABLE EN
Gobierno corporativo de Acme Industries Corp públicamente identificado: 18 personas (7 con cargo ejecutivo, 10 consejeros).	SEC EDGAR (Forms 3/4)	www.sec.gov/

2 Known Breaches & Credentials

2 hallazgos · 1 fuentes consultadas

HALLAZGO / CONSULTA	FUENTE	VERIFICABLE EN
3 usuario(s) de aplicaciones de Acme Industries.com aparecen en stealer logs.	HudsonRock Cavalier	www.hudsonrock.com/
2 tercero(s) con acceso relacionado con Acme Industries.com aparecen en stealer logs.	HudsonRock Cavalier	www.hudsonrock.com/

3 DNS Weaknesses & Hygiene

1 hallazgos · 1 fuentes consultadas

HALLAZGO / CONSULTA	FUENTE	VERIFICABLE EN
El SPF de Acme Industries.com no termina en '-all' ni '~all' — política ambigua.	DNS (consulta directa)	–

4 Perimeter Security / EASM

1 hallazgos · 1 fuentes consultadas

HALLAZGO / CONSULTA	FUENTE	VERIFICABLE EN
Superficie de ataque amplia: 54 subdominios de Acme Industries.com.	Netlas.io	netlas.io/

5 Reputational & Sentiment

0 hallazgos · 1 fuentes consultadas

HALLAZGO / CONSULTA	FUENTE	VERIFICABLE EN
— consultada, sin hallazgos en esta ejecución —	*GDELT*	*www.gdeltproject.org/*

6 Legal & Regulatory

0 hallazgos · 2 fuentes consultadas

HALLAZGO / CONSULTA	FUENTE	VERIFICABLE EN
— consultada, sin hallazgos en esta ejecución —	*OFAC SDN List*	–
— consultada, sin hallazgos en esta ejecución —	*OFAC Consolidated List*	–

7 Supply Chain Risk

1 hallazgos · 1 fuentes consultadas

HALLAZGO / CONSULTA	FUENTE	VERIFICABLE EN
1 proveedores tecnológicos de terceros identificados en la cadena de suministro de Acme Industries Corp.	DNS / HTTP (consulta directa)	–
— consultada, sin hallazgos en esta ejecución —	*DNS / HTTP*	*www.iana.org/*

8 Malicious Infrastructure / Typosquatting

9 hallazgos · 2 fuentes consultadas

HALLAZGO / CONSULTA	FUENTE	VERIFICABLE EN
Dominio similar registrado: antheus.com — con web activa	DNS (consulta directa)	–
Dominio similar registrado: latheus.com — con servidor de correo activo	DNS (consulta directa)	–

HALLAZGO / CONSULTA	FUENTE	VERIFICABLE EN
Dominio similar registrado: Acme.com — con web activa	DNS (consulta directa)	–
Dominio similar registrado: Acme.com — con web activa	DNS (consulta directa)	–
Dominio similar registrado: pantheus.com — con web activa	DNS (consulta directa)	–
Dominio similar registrado: Acme Industries.net — con web activa	DNS (consulta directa)	–
Dominio similar registrado: Acme Industries.org — con web activa	DNS (consulta directa)	–
Dominio similar registrado: Acme Industries.biz — con web activa	DNS (consulta directa)	–
Dominio similar registrado: Acme Industries.info — con web activa	DNS (consulta directa)	–
— consultada, sin hallazgos en esta ejecución —	*RDAP*	`about.rdap.org/`

9 Shadow IT / Code Leaks

0 hallazgos · 1 fuentes consultadas

HALLAZGO / CONSULTA	FUENTE	VERIFICABLE EN
— consultada, sin hallazgos en esta ejecución —	*GitHub Code Search*	`github.com/search`

10 Dark Web Intelligence

1 hallazgos · 1 fuentes consultadas

HALLAZGO / CONSULTA	FUENTE	VERIFICABLE EN
Datos asociados a Acme Industries.com circulan en canales de cibercrimen (stealer logs): 5 registro(s).	HudsonRock Cavalier	`www.hudsonrock.com/`

METODOLOGÍA Y ASPECTOS LEGALES

Cómo trabajamos y por qué este informe es defendible

ORIGEN DE LA INFORMACIÓN — ÚNICAMENTE FUENTES PÚBLICAS (OSINT)

Todo el contenido de este informe procede de **fuentes de información públicamente disponibles** (Open Source Intelligence). No se ha accedido en ningún momento a los sistemas de la empresa objetivo, no se ha realizado ninguna acción intrusiva ni se han utilizado credenciales no autorizadas. Las fuentes consultadas incluyen registros mercantiles oficiales (SEC EDGAR, BORME, Companies House, GLEIF), listas internacionales de sanciones (OFAC, Naciones Unidas, UK HMT/OFSI), bases de datos públicas de brechas de seguridad históricas (HudsonRock, Have I Been Pwned, LeakCheck), índices de prensa global (Event Registry, NewsData, Google News), buscadores de infraestructura expuesta (Shodan, Censys, Netlas), agregadores de inteligencia de amenazas (AbuseIPDB, GreyNoise, VirusTotal, AlienVault OTX) y motores de búsqueda de la red Tor (Ahmia). El listado completo y verificable de cada fuente, agrupado por indicador, se aporta en la sección "Fuentes verificables" de este informe.

BASE LEGAL DEL ANÁLISIS

El presente informe se elabora al amparo del **interés legítimo del solicitante** (artículo 6.1.f del Reglamento General de Protección de Datos UE 2016/679, GDPR) en la evaluación previa o paralela a una operación de fusión, adquisición, inversión o relación contractual con la empresa objetivo. El sujeto principal del análisis es una persona jurídica, no datos personales sensibles. La información personal identificable que aparece (típicamente datos profesionales de directivos en registros mercantiles oficiales o filtraciones públicas históricas) se incluye exclusivamente cuando es necesaria para evaluar el riesgo objeto del informe, conforme al principio de minimización del artículo 5.1.c GDPR. El solicitante asume la responsabilidad final del uso del informe dentro de un contexto legítimo y autorizado de due diligence corporativa.

CUSTODIA PROBATORIA — RFC 3161

El contenido de este informe se sella con un **timestamp criptográfico conforme al estándar RFC 3161** emitido por una Autoridad de Sellado Temporal (TSA) en el momento exacto de su generación. El sello demuestra de forma técnicamente verificable que el contenido aquí descrito existía con la fecha y hora indicadas, y no ha sido modificado posteriormente. La verificación independiente puede realizarse con cualquier herramienta compatible RFC 3161 (por ejemplo, `openssl ts -verify`). El fichero de sello (`.tsr`) está disponible bajo petición. Esta custodia es útil en peritajes y procedimientos judiciales españoles. Nota: FreeTSA no es un Prestador de Servicios de Confianza Cualificado eIDAS; para validez probatoria cualificada plena (eIDAS art. 42) se requiere migración a un PSC eIDAS (FNMT, Camerfirma, AC Sectigo). Consultar con el solicitante si se requiere esta migración.

RETENCIÓN Y PRIVACIDAD DEL SOLICITANTE

El informe queda almacenado en los sistemas de IntelMind durante **30 días naturales** a contar desde su emisión, accesible exclusivamente al usuario que lo solicitó desde su panel privado, para permitir reimpresiones y consultas posteriores. Transcurrido ese plazo el PDF y el contenido analítico se eliminan automáticamente; únicamente se conserva el sello de custodia RFC 3161 (que no contiene datos personales, solo un hash) durante el plazo legal aplicable, a

efectos de verificación probatoria futura. El solicitante puede solicitar la eliminación inmediata del informe en cualquier momento contactando con soporte@intelmind.io. Asimismo, está disponible la modalidad "**entrega efímera**": el PDF se envía al correo del solicitante sin quedar almacenado en los sistemas de IntelMind (solo se conserva el sello de custodia). Esta opción se activa al momento de la compra, sin coste adicional.

LIMITACIONES HONESTAS DEL ANÁLISIS

- El informe refleja lo hallado en fuentes públicas dentro de la ventana de análisis. La ausencia de evidencia no equivale a evidencia de ausencia.
- Cada hallazgo es válido a la fecha y hora del escaneo.
- Las coincidencias por nombre (sanciones, dominios similares) requieren verificación de identidad antes de darse por confirmadas.
- Algunos indicadores entregan una evaluación parcial; su profundidad máxima requiere feeds de inteligencia de pago, indicado en cada caso.

DISCLAIMER PROFESIONAL

Este informe constituye un análisis técnico-informativo elaborado por IntelMind con metodología outside-in. No sustituye al asesoramiento legal, fiscal, financiero o de auditoría especializada que corresponda al solicitante. Las recomendaciones de remediación y los benchmarks económicos se aportan a título orientativo y deben validarse caso por caso con los asesores correspondientes. IntelMind no garantiza la exactitud absoluta de la información obtenida de fuentes terceras públicas, si bien aplica los controles disciplinados de verificación cruzada descritos en este apartado. El uso del informe queda sujeto a los términos y condiciones publicados en intelmind.io.

VERIFICACIÓN PÚBLICA DEL SELLO

La integridad de este documento es verificable en `https://intelmind.io/cyber-dd/verify/IMD-CDF-MPJXR35X-1TNV` en cualquier momento futuro, mientras el plazo de custodia esté vigente.