UNIPAGO | UNISHIELD BY UNIPAGO

BOLETÍN · JULIO 2026

El blanco *somos nosotros.*

Seguridad Social, el sector donde el adversario ya no apunta al volumen, sinó al impacto.

PERIODO
Q1–Q3 2026

TLP:AMBER

NOTA DE PRENSA LANZAMIENTO OFICIAL · 5 DE MAYO DE 2026

UNIPAGO lanza UNISHIELD, su escudo digital contra las ciberamenazas

El 5 de mayo de 2026, UNIPAGO presentó oficialmente **UNISHIELD**, un Centro de Inteligencia de Amenazas Cibernéticas concebido en su fase inicial como ISAC sectorial para el ecosistema del Sistema Dominicano de Seguridad Social (SDSS). La iniciativa nace para prevenir, detectar y coordinar la respuesta ante incidentes que afecten a las instituciones y a los millones de ciudadanos que dependen del sector, fortaleciendo la resiliencia digital de toda la cadena de la seguridad social.

Presencia en las VI Jornadas STIC & Congreso RootedCON RD 2026

DEL 27 AL 29 DE MAYO DE 2026 · #STICDOMINICANA

UNISHIELD participó en las VI Jornadas STIC & Congreso RootedCON RD 2026 ("Un escudo digital contra las ciberamenazas"), evento apoyado por el CNCS, la OEA y CSIRTAmericas que lo consolidó como referente sectorial de ciberseguridad.

QUIÉNES SOMOS

UNISHIELD es un espacio colaborativo y neutral que permite a los miembros del ecosistema de la seguridad social compartir información sobre amenazas cibernéticas, mejorar la capacidad de prevención, detección y respuesta ante incidentes, y elevar el nivel de resiliencia digital del sector.

NUESTROS SERVICIOS

CUATRO LÍNEAS DE TRABAJO AL SERVICIO DEL ECOSISTEMA

Inteligencia y Alertas

- Alertas sectoriales
- Indicadores de compromiso (IOC)
- Boletines de inteligencia periódicos
- Informes de riesgo y superficie de ataque

Análisis de Amenazas

- Análisis OSINT de exposición
- Identificación de campañas de amenaza
- Análisis de información expuesta
- Correlación de información compartida

Concientización

- Boletines al ecosistema
- Mejores prácticas sectoriales
- Formación colaborativa

Evaluación de Madurez de Ciberseguridad

- Diagnóstico inicial del nivel de madurez
- Evaluación basada en marcos de referencia.
- Hoja de ruta de mejora continua

Descarga los indicadores *de este boletín.*

Indicadores de compromiso verificados de algunos de los actores maliciosos cubiertos en este boletín, listos para importar en su SIEM o EDR.

https://**www.unishield.com.do/recurso/indicadores-de-compromiso-iocs/**

ESCANEA Y DESCARGA

Conoce tu nivel de madurez *de manera gratuita*

Evaluación de madurez en ciberseguridad basada en el NIST Cybersecurity Framework (CSF 2.0), obtenga un puntaje de su nivel actual por enfoque.

https://**www.unishield.com.do/recurso/evaluacion-de-madurez-en-ciberseguridad/**

ESCANEA

Los indicadores que descargaste, *multiplicados y automatizados.*

Mientras lees este boletín, el adversario ya está moviéndose. La inteligencia fragmentada llega tarde. Únete al ISAC.

- → **IoCs en tiempo real**
  Directos a tu SIEM via STIX/TAXII. Sin descargas manuales, sin retraso.
- → **Alertas tempranas**
  Campañas dirigidas al sector, días antes de que sean públicas.
- → **Reglas Sigma y YARA**
  Mapeadas a MITRE ATT&CK. Listas para importar y ejecutar.
- → **Boletines Mensuales**
  Cada mes. Diseñados para CISOs, alta dirección y analistas.
- → **Comunidad sectorial**
  AFP, ARS, bancos, entidades reguladoras y procesadoras compartiendo señales en confianza.
- → **Soporte directo**
  Acceso al equipo de threat intelligence durante incidentes activos.

Para el sector de la Seguridad Social, *que entendieron que la inteligencia, cuando llega fragmentada y tarde, no protege.*
Solicita acceso: ***unishield.com.do/afiliate***

ÚNETE AL ISAC →

01
INC Ransom

El grupo que más golpeó a los terceros del ecosistema de salud en el primer trimestre del 2026

Modelo operativo: Ransomware-as-a-Service activo desde julio 2023. Opera con socios que ejecutan las intrusiones a cambio de un porcentaje del rescate. Su rasgo distintivo es el uso intensivo de Initial Access Brokers (IABs): compra accesos previamente comprometidos en foros de la deep web, en lugar de generar la intrusión desde cero.

Doble extorsión: primero exfiltran los datos, después cifran los sistemas. Si la víctima no paga, los archivos terminan publicados en su sitio de leaks en Tor. Lo que se filtra suele incluir información médica protegida, datos financieros y registros patronales.

Distintivo técnico: abusan de herramientas legítimas como AnyDesk, ScreenConnect, PowerShell, utilidades nativas de Windows. Es lo que se llama living-off-the-land: moverse usando lo que ya está instalado, en lugar de traer malware propio que el EDR podría detectar

8

Ataques contra terceros del ecosistema salud en el primer trimestre del 2026.

123

Víctimas totales en el sector salud rastreadas en ransomware.live. Es el segundo sector que más golpea, después de servicios empresariales (155).

24

técnicas MITRE ATT&CK documentadas y un giro deliberado hacia el sector salud a nivel mundial desde enero 2025

Top 3

junto a Qilin y SAFEPAY, catalogado entre los tres grupos más activos contra salud global en 2025.

Cadena de ataque típica observada

Trazada en incidentes confirmados de 2025–2026

1. **Acceso inicial** — Compra a IAB, phishing, VPN sin parche
2. **Persistencia** — AnyDesk, ScreenConnect, cuentas de servicio
3. **Evasión EDR** — PowerShell, LOLBins, enumeración AD
4. **Movimiento** — RDP a jump hosts, SMB, WMI
5. **Exfil. + Cifrado** — rclone, MEGA, doble extorsión

Técnicas MITRE ATT&CK confirmadas

Para construir reglas de detección y validar cobertura del EDR

T1078 Valid Accounts — Credenciales compradas a IAB	**T1133 Ext. Remote Services** — VPN, RDP expuestos sin MFA fuerte	**T1566 Phishing** — Spear-phishing dirigido a admins	**T1219 Remote Access Tools** — AnyDesk, ScreenConnect persistencia
T1059.001 PowerShell — Recon, descubrimiento, y movimiento lateral	**T1021.001 RDP Lateral** — Salto a jump-hosts internos	**T1567.002 Exfil to Cloud** — rclone → MEGA / cloud storage	**T1486 Data Encrypted** — Cifrado del entorno víctima

¿SABÍAS QUÉ...?

Endpoint Priviledge Management

El control de Microsoft que otorga permisos de administrador de forma temporal, aislada y totalmente auditada, sin privilegios permanentes.

¿Qué es?: Microsoft cuenta con un nuevo control de seguridad llamado **Endpoint Privilege Management (EPM)**, integrado en Microsoft Intune. Permite que los usuarios estándar realicen tareas específicas que normalmente requieren permisos de administrador, sin necesidad de otorgarles derechos de administrador completos.

Cómo funciona: en lugar de dar permisos permanentes, EPM concede elevaciones temporales y controladas que quedan aisladas y totalmente auditadas. No hay privilegios permanentes ni accesos residuales una vez terminada la tarea.

0
Privilegios permanentes. El acceso caduca al terminar la tarea.

100%
De las elevaciones quedan registradas y auditadas por TI.

Just-in-time
Elevación concedida **solo por el momento** y solo para esa tarea.

Zero Trust
Refuerza el modelo de **Confianza Cero** y reduce la superficie de ataque.

El ciclo de una elevación

Cada tarea elevada sigue el mismo camino controlado, de principio a fin

1. **Solicitud** — El usuario pide ejecutar una app o tarea aprobada
2. **Verificación** — Intune evalúa la política definida por TI
3. **Elevación temporal** — Se otorgan permisos elevados solo por ese momento
4. **Tarea aislada** — Se ejecuta contenida, sin tocar el resto del sistema
5. **Revocación + auditoría** — El permiso caduca y queda registrado, sin acceso residual

Beneficio clave

Menos riesgos, menos permisos innecesarios y mayor visibilidad sobre quién eleva privilegios y por qué

Menos riesgos
Sin cuentas de administrador permanentes que un atacante pueda secuestrar.

Menos permisos innecesarios
Cada elevación es puntual y acotada a una sola tarea aprobada.

Mayor visibilidad
Registro completo de quién elevó privilegios, cuándo y para qué.

Superficie de ataque reducida
Productividad intacta sin comprometer el modelo de Confianza Cero.

02 PANORAMA / MACRO

El precio de un incidente, *se multiplica.*

Menos ataques, pero cada uno es más caro. El semestre cambia el cálculo: el adversario pre-califica a objetivo por ingresos, ciberseguro y dependencia operacional, y reserva la demanda máxima para quien menos puede tolerar caída.

DEMANDA MEDIA DE RESCATE · SALUD Q1 2026

$16.9M

Demanda media (no pago confirmado). +2,824% vs Q4 2025 ($577K). Fuente: Comparitech.

ATAQUES SECTOR SALUD · Q1 2026

201

120 contra proveedores directos + 81 contra terceros (billing, EHR, claims, MSPs). Fuente: Comparitech.

FRAUDE EN CONTACT CENTERS DE SALUD · 2026

50%

Intentos de fraude que ya involucran elementos generados por IA: voz sintética, bots, recon de IVR. Pindrop.

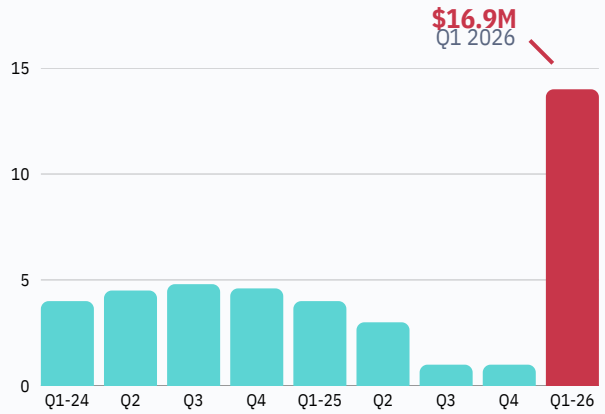
BRECHAS EN SALUD VINCULADAS A TERCEROS

72%

Tres de cada cuatro brechas en salud llegan por un proveedor o socio comercial. Censinet 2026.

Demanda promedio de rescate · sector salud

USD · trimestral · 2024 – Q1 2026



La curva no representa más víctimas, representa **víctimas mejor seleccionadas**. Qilin lidera con 23 reclamos en Q1 2026.

Cinco tendencias estructurales

- **Extorsión sin cifrado:** Qilin, INC Ransom y The Gentlemen exfiltran y publican sin cifrar nada. Tener backups limpios ya no detiene la fuga.
- **Identidad y borde, la nueva puerta:** VPN, IdP, SaaS y consolas cloud concentran los accesos iniciales. El perímetro ahora se mide en credenciales, no en firewalls.
- **Tercerización del riesgo:** 72% de las brechas en salud llegan por un tercero. Un proveedor comprometido arrastra a docenas de entidades del sistema.
- **Ingeniería social con IA:** Voz clonada en 20 segundos. Phishing en español neutro, sin errores. El usuario ya no es la última línea — es el primer eslabón roto.
- **Tiempo a explotar bajo 5 días:** Priorizar parches por CVSS llega tarde. La señal útil es CISA KEV y ENISA EUVD — lo que ya se está explotando.

> *El presupuesto de seguridad ya no compite contra otras áreas de TI — compite contra el costo regulatorio y reputacional de una sola brecha sectorial.*
>
> — LECTURA PARA EL CISO

03 SALUD / DEFENSA COMPENSATORIA

Cinco controles *que mueven la aguja.*

No es un plan de tres años, son cinco intervenciones operativas que reducen el riesgo de un ataque tipo INC Ransom o Qilin en el corto plazo. Cada control responde a una técnica que estos grupos ya están usando contra el sector hoy.

MFA resistente a phishing

Implementar mecanismos passwordless o token físico (FIDO2/WebAuthn) en cuentas privilegiadas y de acceso remoto. Los métodos como SMS y push-approval **ya no se consideran un control fuerte**.

T1078 · T1190

EDR + visibilidad WSL

Extender la cobertura del EDR a la distribución del Subsistema de Windows para Linux (WSL), o, en su defecto, deshabilitar esta funcionalidad para impedir su uso en equipos de usuarios finales y servidores.

T1218

Segmentación

Mantener los equipos y servidores críticos en redes aisladas, limitando su exposición y reduciendo el riesgo de accesos no autorizados o propagación de amenazas.

T1021

Backups inmutables

Configurar respaldos con mecanismos de inmutabilidad (object-lock) o air-gap real, asegurando que no puedan ser alterados o eliminados. Validar de manera frecuente la recuperación mediante pruebas de restauración efectivas.

T1486

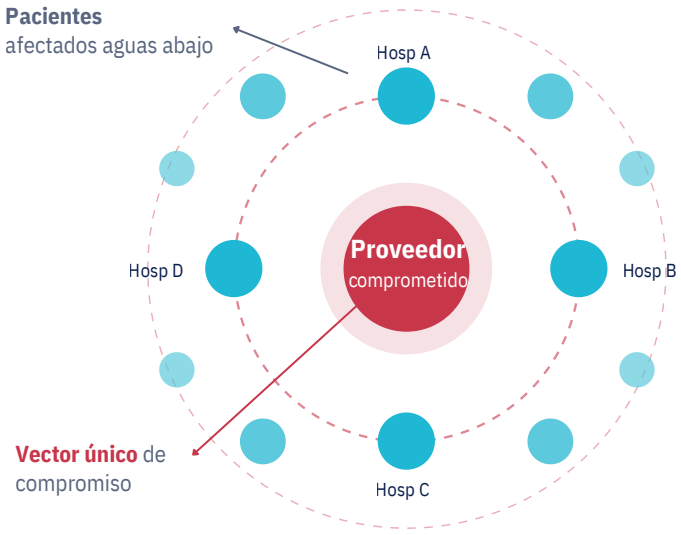
Custodia de la cadena de suministro

Evaluar la seguridad de los proveedores como un proceso continuo, no como un trámite de onboarding.

SUPPLY CHAIN

El efecto "blast radius" en salud

Porqué un solo proveedor comprometido, puede golpear a docenas...



En 2026, **el 72% de las brechas en salud llegan a través de un tercero** (Censinet 2026). El hospital promedio trabaja con más de 1,300 proveedores, y cuando uno cae, el costo medio del incidente sube a 10.22 millones de dólares.

Para una AFP, ARS, ARL, banco, prestadora, procesadora o reguladora, el perímetro propio ya no alcanza. El riesgo empieza desde afuera.

04 AMENAZAS/CAMPAÑAS ACTIVAS

Dos campañas, *una sola región objetivo.*

El semestre dejó dos campañas distintas pero conectadas por el mismo principio: el adversario ya no rompe el control, convence al sistema (o al usuario) de cooperar. Ambas tienen huella confirmada en República Dominicana.

● CAMPAÑA ACTIVA · CRÍTICA

SharePoint ToolShell

Zero-day chain · Pre-auth RCE on-prem

CVE	CVE-2025-53770 · 53771 · 49706 · 49704
DETECCIÓN	Eye Security · 18 jul 2025
CADENA	POST /ToolPane.aspx con Referer /SignOut.aspx → upload spinstall0.aspx → extrae MachineKeys → ViewState forging
ALCANCE	+8,000 SharePoint públicos escaneados; decenas comprometidos
ESTADO	Parche disponible · En CISA KEV · Explotación activa

● CAMPAÑA ACTIVA · ALTA

FileFix → StealC

Social engineering · Esteganografía · Infostealer-as-a-Service

DETECCIÓN	Acronis TRU · 1er caso in-the-wild beyond POC
CRECIMIENTO	ClickFix/FileFix +500% durante 2025
CADENA	Phishing Meta → comando en File Explorer → JPG con stage 2 via esteganografía → loader Go anti-VM → StealC en memoria
ALCANCE	16 idiomas · víctimas confirmadas en República Dominicana
ESTADO	Campaña activa · C2: 77.90.153.225

TU ORGANIZACIÓN FRENTE A ESTAS CAMPAÑAS

- ☐ ¿Tengo SharePoint Server on-premise (2016, 2019 o Subscription Edition)? **SharePoint Online no está afectado, si todo su entorno es M365, este bloque no aplica**.
- ☐ ¿Apliqué los parches de fin de julio 2025 y roté las MachineKeys después? El parche solo cierra la puerta; las llaves robadas siguen siendo válidas hasta que se rotan manualmente en cada Web Application.
- ☐ ¿Mi SharePoint on-prem necesita realmente estar expuesto a Internet? Si la respuesta es no, restringirlo a VPN o ZTNA elimina la mayor parte del vector.
- ☐ MFA resistente a phishing en cuentas privilegiadas: FIDO2 o WebAuthn, no SMS ni push-approval.
- ☐ Backups inmutables probados con restauración real en el último trimestre, no solo verificación de existencia.
- ☐ Procedimiento documentado para extorsión sin cifrado, estos actores publican datos sin cifrarlos antes.

06 FRAUDE POR IA

3-20s basta para clonar la voz *de su director.*

Servicios comerciales de clonación de voz permiten generar **text-to-speech** con la voz objetivo en cuestión de minutos. Combinado con una cuenta de correo comprometida, el resultado es el BEC del 2026: llamada urgente del "CFO" pidiendo una transferencia, respaldada por un correo en la bandeja real.

ANATOMÍA DEL ATAQUE EN 4 FASES

HERRAMIENTAS CON ESTA CAPACIDAD (A JUNIO 2026)

Comerciales: ElevenLabs (Eleven v3) · Resemble AI · Fish Audio S2 · OpenAI Voice Engine · Cartesia · Murf AI · WellSaid Labs. **Open-source:** Coqui XTTS · Voicebox · OpenVoice · Chatterbox · Bark · RVC (real-time voice conversion en Discord o Zoom).

Defensas que no son técnicas, y por eso funcionan

Contra deepfake, los controles más efectivos son procedimentales.

Doble canal

Toda transferencia o cambio de cuenta requiere verificación por canal independiente. No responder al mismo correo, no devolver al número que llamó.

Palabra-código

El comité ejecutivo acuerda una palabra rotada trimestralmente. Toda instrucción urgente por voz exige la palabra correcta antes de proceder.

Ventana de espera

Ninguna transferencia urgente se ejecuta antes de 30 minutos desde su solicitud. La urgencia legítima sobrevive este lapso; el fraude no.

07 ADVERSARIO / PANORAMA 2026

Quién ataca *al sector salud.*

El paisaje del adversario, en datos. El sector salud y seguridad social no enfrenta una amenaza monolítica: tres tipos de grupos dominan el panorama según foco operativo.

GLOSARIO
Reclamo: significa que el grupo publicó a esa víctima en su sitio de leaks o reivindicó el ataque

FOCO OPERATIVO
Proveedores directos
Hospitales, clínicas, PSS

Grupo	Cant. Reclamos
Qilin	23
The Gentlemen	10
Insomnia	9
LockBit	9
Sinobi	7

120 ataques totales · 26 confirmados · 13 TB exfiltrados

FOCO OPERATIVO
Terceros del ecosistema
Billing · EHR · MSPs · Claims · Procesadoras

Grupo	Cant. Reclamos
INC Ransom	8
NightSpire	8
Genesis	6
Akira · Clop · LockBit	5
The Gentlemen	5

81 ataques totales · **29 TB exfiltrados** (más del doble que proveedores directos)

Cifras del Q1 2026 según Comparitech Healthcare Ransomware Roundup. Los terceros del ecosistema —billing, EHR, MSPs, procesadoras de pagos, claims processors, concentran a INC Ransom y NightSpire. **Para AFP, ARS, ARL y reguladores, INC Ransom es el grupo más representativo del riesgo real.**

Top 5 amenazas para 2026

Encuesta a 250 ejecutivos del sector salud · Health-ISAC Global Health Sector Threat Landscape Report 2026

01
AI-enabled attacks
Nuevo #1. Solo el 37% tiene procesos para evaluar IA antes de desplegar.

02
Zero-day exploits
Edge devices y plataformas colaborativas (ToolShell).

03
Ransomware
+55% surge incidentes en salud 2025. Demanda media: $16.9M.

04
Brechas vía terceros
72% de brechas en salud vienen de un tercero (Censinet 2026).

05
Phishing y spear-phishing
Combinado con IA generativa supera 60% de tasa de éxito.

08 PLAN / PRÓXIMOS 30 DÍAS

Antes del próximo boletín, *respóndete esto*.

Dieciséis preguntas para descubrir dónde está el riesgo que no estás viendo.

01 ¿LO SÉ? · *Conocimiento del entorno*

- ☐ ¿Conozco con precisión cuáles APIs están expuestas a Internet y qué entidades las consumen?
- ☐ ¿Sé qué herramientas de IA generativa están utilizando mis colaboradores y qué información introducen en ellas?
- ☐ ¿Sé qué herramientas están utilizando las distintas áreas de la organización al margen del catálogo autorizado por seguridad?
- ☐ ¿Tengo registro completo de las cuentas de servicio activas, con propietario, propósito y fecha de creación documentados?

02 ¿HACIA DÓNDE VA? · *Datos, IA y terceros*

- ☐ ¿Conozco el flujo completo de la información de mis afiliados cuando es procesada por proveedores externos, incluyendo la jurisdicción de almacenamiento final?
- ☐ ¿Cuento con una política formal que regule qué categorías de datos pueden ser introducidas en herramientas de IA públicas?
- ☐ ¿Cómo puedo conocer la postura de seguridad de mis proveedores críticos?
- ☐ ¿Tengo visibilidad sobre cuántos sistemas procesan un mismo registro de afiliado a lo largo de su ciclo de vida?

03 ¿LO VERÍA SI PASARA AHORA? · *Detección y Monitoreo*

- ☐ ¿Qué tiempo tomaría a mi SOC detectar un acceso anómalo durante una madrugada en un día no laborable?
- ☐ ¿Mis colaboradores están entrenados para reconocer que una llamada o mensaje de voz de un ejecutivo puede ser un deepfake generado a partir de 20 segundos de audio público?
- ☐ ¿Tengo trazabilidad de lo que ocurre después de que un usuario interactúa con un correo sospechoso, más allá de saber que el mensaje superó el filtro?
- ☐ ¿Mis logs de seguridad están centralizados y correlacionados, o cada sistema los mantiene de forma aislada?

04 ¿SOBREVIVIRÍA? · *Resiliencia y respuesta*

- ☐ ¿La última prueba de restauración de backups incluyó el montaje efectivo de los datos, o se limitó a verificar la existencia del archivo?
- ☐ ¿Mi equipo tiene definidos los contactos y el procedimiento de escalamiento ante la caída de un sistema crítico en horario no laborable?
- ☐ Cuento con un plan de contingencia documentado si un proveedor crítico (EHR, facturación, procesadora) sufre una indisponibilidad prolongada?
- ☐ ¿Mis logs de seguridad están centralizados, o cada sistema vive en su propio silo donde nadie los correlaciona?

09 CIERRE / LECTURA PARA EL CISO

Lo que cambia, *y lo que no.*

> *El semestre apunta a un escenario donde el adversario es más selectivo, mejor financiado y opera con herramientas que antes solo tenían los estados. La diferencia entre las organizaciones que sobrevivirán bien y las que sufrirán pérdidas materiales no estará en el tamaño de su presupuesto, sino en la disciplina con la que ejecuten los fundamentos: identidad fuerte, parchado rápido, segmentación real y procesos que sobreviven a la urgencia.*
>
> — EQUIPO UNISHIELD

REPORTES CITADOS · 2026

- Health-ISAC — 2026 Global Health Sector Threat Landscape Report
- Censinet — 2026 Healthcare Cybersecurity Benchmarking Study
- Comparitech — Healthcare Ransomware Roundup Q1 2026
- Verizon — Data Breach Investigations Report (DBIR) 2026
- Paubox — 2026 Healthcare Email Security Report
- IBM — Cost of a Data Breach Report 2025
- Pindrop — 2025 Voice Intelligence & Security Report
- CrowdStrike — 2026 Global Threat Report
- Microsoft — Digital Defense Report 2025
- Sumsub — Identity Fraud Report 2025–2026

FEEDS OPERATIVOS RECOMENDADOS

Health-ISAC · Inteligencia compartida del sector salud · health-isac.org

HHS OCR Wall of Shame · Brechas confirmadas en EE.UU.

Censinet RiskOps · TPRM específico para salud

HSCC · Health Sector Coordinating Council · alertas conjuntas

FS-ISAC · Sector financiero · necesario por procesamiento de pagos

MS-ISAC · Estado, local y tribal · referencia útil para reguladores

CSIRT-RD / CNCS · Coordinación nacional dominicana

CISA KEV · Catálogo de vulnerabilidades explotadas activamente

ENISA EUVD · Base europea de vulnerabilidades · contexto UE

FBI IC3 · Alertas operativas y reportes anuales