PRYSE

CYBERSECURITY®

Ciberseguridad que no espera al ataque

Protección estratégica para entornos críticos
·Inteligencia, defensa y respuesta de clase mundial.

24/7
Monitoreo SOC

100%
Enfoque en ciberseguridad

EL RIESGO INVISIBLE

La ciberseguridad reactiva ya no es una opción.

70%

De las organizaciones desconocen

Su nivel real de exposición y vulnerabilidad. La mayoría detecta las brechas de seguridad únicamente cuando el incidente ya ocurrió.

El costo del cibercrimen para México supera los $7,000 millones USD anuales.*

¿Qué ocurre cuando no estás preparado?

Pérdida de operación

Interrupción de procesos críticos y cadena de valor.

Fuga de información crítica

Filtración de datos sensibles y propiedad intelectual.

Daño reputacional

Pérdida de confianza de ciudadanos, clientes, socios e inversionistas.

Sanciones regulatorias

Multas por incumplimiento (LFPDPPP, GDPR, PCI-DSS, ISO).

https://www.docusign.com/es-mx/blog/desarrolladores/ciberataques-en-mexico

¿QUIENES SOMOS?

Somos expertos en ciberseguridad.

Protegemos la operación, la reputación y la información de las organizaciones más exigentes de México y Latinoamérica.

Misión

Ayudar a controlar el ciber riesgo de nuestros clientes con inteligencia, tecnología, talento entrenado y certificado.

visión

Ser la empresa de referencia en ciberseguridad de la región.

Valores

Integridad, excelencia técnica, confidencialidad absoluta y compromiso con el resultado del cliente.

PRYSE
CYBERSECURITY

PRYSE CYBERSECURITY

PORTAFOLIO COMPLETO DE SERVICIOS

PORTAFOLIO

Nuestras soluciones empresariales

Un ecosistema de ciberseguridad integral, diseñado bajo marcos internacionales (NIST CSF 2.0, ISO/IEC 27001, CIS Controls v8, MITRE ATT&CK).

Soluciones de Seguridad

Protección integral para infraestructura crítica y datos sensibles.

Servicios Gestionados (SOC)

Centro de monitoreo SOC 24/7 con analistas certificados.

Seguridad Cloud

Protección CSPM/CWPP/CASB en multi nube.

Seguridad Ofensiva

Pentesting, Red Team, Purple Team y ejercicios adversariales.

Auditoría de Código (SAST/ DAST)

Análisis estático y dinámico con enfoque Shift-Left & DevSecOps.

Inteligencia de Amenazas

CTI proactiva con monitoreo de dark web, APTs y actores de amenaza.

Respuesta a Incidentes (DFIR)

Contención, erradicación y análisis forense digital.

Formación y Concientización

Capacitación alineada a NIST, NICE, ISO 27001 y programas anti-phishing.

Cumplimiento Normativo

ISO 27001, PCI-DSS, LFPDPPP, SOC 2, HIPAA y GDPR.

Soluciones Cloud

Despliegue seguro y hardening de entornos híbridos.

Centro de Datos Certificado Tier II

Infraestructura redundante con continuidad operativa garantizada.

Threat Hunting Proactivo

Cacería de amenazas silenciosas basada en TTPs de MITRE ATT&CK.

Servicios Especializados

Take Down

Protegemos a tu organización frente a sitios falsos, phishing, perfiles apócrifos y suplantación digital, gestionando la baja en internet.

Forense y Asesoría Jurídica

Ante un ataque, estaríamos frente a la comisión de un delito, por consiguiente integramos un servicio para análisis forense e investigación cibernética que provea información sustancial para la ministerializacion/judicializacion del caso, con la finalidad de deslindar responsabilidades y procurar justicia.

Monitoreo V.I.P

Monitoreo en deep/dark web para la protección de imagen de funcionarios públicos y ejecutivos de alto nivel evitando el uso indebido de su imagen.

PRYSE
CYBERSECURITY

Inteligencia de Amenazas

Conoce a tu adversario antes de que te encuentre

Detección & Inteligencia
FIRST México Liaison · ISO 27001 LA

EL PROBLEMA

- Las alertas llegan sin contexto: ¿esta amenaza aplica realmente a nuestra organización e industria?
- Los controles reaccionan a lo que ya ocurrió — no anticipan lo que viene contra su sector específico
- No saben que grupos APT tienen activamente a su sector o región geográfica en la mira

CAPACIDADES CLAVE

- Feeds de IOCs: IPs maliciosas, dominios, hashes, URLs y firmas de malware
- Inteligencia estratégica (ejecutivos), tactica (TTPs) y operacional (campañas activas)
- Monitoreo de dark web, foros clandestinos y canales de actores de amenaza
- Perfilado de grupos APT relevantes para el sector y geografía del cliente
- Integración bidireccional con SIEM / EDR / SOAR del cliente
- Informes de IOCs con contexto de impacto para México y LATAM

STACK TECNOLÓGICO

MISP | OpenCTI | MITRE ATT&CK | STIX/TAXII | TLP Framework | VirusTotal

¿CÓMO FUNCIONA?

1. **Planificación** Definición de PIRs basados en sector, activos críticos y perfil de riesgo
2. **Recolección** Fuentes OSINT, dark web, feeds comerciales, ISAC/CERT nacionales e internacionales
3. **Procesamiento** Normalización, deduplicación y correlación de datos crudos para enriquecer contexto
4. **Análisis** Contextualización de IOCs con TTPs del framework MITRE ATT&CK y relevancia para el cliente
5. **Diseminación** Entrega de reportes accionables al stakeholder correcto en el formato adecuado
6. **Feedback** Refinamiento contínuo del ciclo basado en efectividad de detecciones y nuevos requisitos

¿POR QUÉ ELEGIRNOS?

1. Liaisons oficiales ante FIRST — uno de solo 2 representantes en México
2. Inteligencia contextualizada para el threat landscape específico de México y LATAM
3. Correlación activa con TTPs de grupos APT que operan en sectores financiero, gobierno y salud
4. Integración sin fricción: conectores nativos para los SIEM más comunes en el mercado Mexicano

60%
Reducción en MTTR con inteligencia accionable

3
Capas: estratégica, táctica y operacional

100M+
IOCs en base de datos en tiempo real

24/7
Monitoreo continuo de amenazas emergentes

PRYSE
CYBERSECURITY

Threat Hunting

No esperes la alerta — encuentra al atacante antes de que actúe

Detección Proactiva

FIRST México Liaison · ISO 27001 LA

EL PROBLEMA

- Sus EDR y SIEM tienen puntos ciegos: los APT se mueven sin disparar ninguna alerta automatizada
- El tiempo promedio de permanencia de un atacante no detectado es 197 días
- Las amenazas internas y el movimiento lateral usando herramientas legítimas (LotL) son invisibles para controles automáticos

CAPACIDADES CLAVE

- Hunting basado en hipótesis formuladas con MITRE ATT&CK como referencia
- Detección de APTs, movimiento lateral y credenciales comprometidas
- Identificación de actividad Living-off-the-Land (LOLBins) sin malware convencional
- Análisis de comportamiento anómalo en endpoints, red y Active Directory
- Busqueda de backdoors, C2 persistente y exfiltración silenciosa
- Cada hunting genera nuevas reglas de deteccion automatica en el SIEM/EDR

STACK TECNOLÓGICO

MITRE ATT&CK | Velociraptor | YARA | Sigma Rules | Elastic/Splunk | BloodHound

¿CÓMO FUNCIONA?

1. **Hipótesis** Formulacion basada en threat intel del sector y TTPs de adversarios activos en México
2. **Recolección** Extracción de telemetría de EDR, SIEM, logs de red, AD, DNS y sistemas cloud
3. **Investigación** Análisis profundo por analistas L3: correlación manual de IOAs y búsqueda de patrones anómalos
4. **Detección** Confirmación o descarte riguroso; escalamiento inmediato si se confirma una brecha activa
5. **Automatización** Conversión de IOAs detectados en nuevas reglas — el cliente queda mas fuerte tras cada ciclo

¿POR QUÉ ELEGIRNOS?

1. Analistas Nivel 3 certificados en MITRE ATT&CK con experiencia en engagements reales en México
2. Metodología "Assumed Breach" — operamos bajo la premisa de que el atacante ya esta dentro
3. Cada ejercicio produce nuevas detecciones automáticas — mejora acumulativa y permanente
4. Acceso a inteligencia exclusiva de grupos activos en México: financiero, gobierno y salud

197d
Permanencia promedio sin hunting activo

<8d
Detección promedio con nuestro servicio

MITRE
ATT&CK 14 tácticas, 200+ técnicas

L3
Solo analistas senior especializados

PRYSE
CYBERSECURITY

Takedown de Activos Maliciosos

Elimina infraestructura maliciosa que usa tu nombre antes de que dañe a tus clientes

Protección de Marca Digital

FIRST México Liaison · ISO 27001 LA

EL PROBLEMA

- Sitios phishing clonando su marca roban credenciales de sus clientes cada minuto que permanecen activos
- Cuentas falsas en redes sociales suplantando ejecutivos generan fraudes y danan la confianza de clientes
- Sin un proceso estructurado el tiempo de eliminación supera los 5-10 días con daño reputacional irreversible

CAPACIDADES CLAVE

- Detección y monitoreo continuo de sitios phishing que suplantan su marca o dominio
- Identificación de cuentas falsas en LinkedIn, X, Facebook, Instagram y WhatsApp
- Notificación acelerada a ISPs, registrars, hosters y plataformas sociales
- Eliminación de sitios de distribución de malware ligados a su nombre
- Protección de propiedad intelectual: contenido, imágenes y materiales de marca
- Monitoreo post-takedown para detectar re-surgimiento de infraestructura

STACK TECNOLÓGICO

URLScan.io | PhishTank | Spamhaus | Netcraft | WHOIS Tracking | Brand Monitoring

¿CÓMO FUNCIONA?

1. **Detección** Monitoreo automatizado 24/7 de variaciones typosquatting, homoglyphs y similares del dominio
2. **Validación** Confirmación técnica de que el activo es efectivamente malicioso — cero falsos positivos
3. **Notificación** Envío formal con evidencia documentada al ISP, registrar o plataforma social
4. **Eliminación** Seguimiento activo hasta confirmar suspensión total — SLA garantizado de 24-72h
5. **Monitoreo Post** Vigilancia continua para detectar si el actor migra o levanta infraestructura similar

¿POR QUÉ ELEGIRNOS?

1. Red global de contactos con ISPs, registrars y plataformas — respuestas en horas, no semanas
2. SLA de notificación garantizado: menos de 4 horas desde detección hasta primer contacto formal
3. Integración con threat intelligence: detectamos campanas antes de que escalen a los clientes
4. Reportes legales con cadena de custodia para acciones judiciales o ante CONDUSEF/INAI

<4h
Notificación al ISP/hoster desde detección

24-72h
SLA típico de eliminación completa

360
Web + RRSS + app stores + dark web

100%
Documentación legal incluída

PRYSE
CYBERSECURITY

Soluciones de Seguridad

Arquitectura de seguridad integral — de la red hasta el factor humano

Defensa en Profundidad

FIRST México Liaison · ISO 27001 LA

EL PROBLEMA

- La organización crece y se digitaliza pero la seguridad sigue siendo reactiva y fragmentada en silos
- Multiples herramientas que no se integran crean brechas de visibilidad y alertas que nadie correlaciona
- El factor humano es el vector de ataque #1 y no existe un programa formal de cultura de seguridad

CAPACIDADES CLAVE

- Firewalls de próxima generación (NGFW), IDS/IPS y segmentación de redes
- Gestión de Identidades (IAM), cuentas privilegiadas (PAM) y Zero Trust Architecture
- Protección de endpoints con EDR/XDR y gestión centralizada de parches
- SIEM con correlación de eventos en tiempo real y SOC 24/7
- Threat Intelligence integrada para contexto de amenazas en tiempo real
- Programas de capacitación, simulaciones de phishing y cultura de seguridad

STACK TECNOLÓGICO

NGFW | EDR/XDR | SIEM | PAM/IAM | MFA | Zero Trust | Microsegmentacion

¿CÓMO FUNCIONA?

1. **Assessment** Diagnóstico del estado actual: inventario de activos, análisis de brechas y mapa de superficie de ataque
2. **Diseño** Arquitectura de seguridad por capas (defensa en profundidad) alineada con negocio y regulaciones
3. **Implementación** Despliegue por fases con mínima disrupción operativa y transferencia de conocimiento al equipo
4. **Monitoreo** Operación continua del SOC: detección, análisis, respuesta automatizada y escalamiento humano
5. **Mejora Continua** Revisión trimestral, ajuste de controles y actualización ante panorama de amenazas emergente

¿POR QUÉ ELEGIRNOS?

1. Enfoque holístico de 6 capas: red, identidad, endpoint, monitoreo, operaciones y factor humano
2. Zero Trust desde el diseño — "nunca confíes, siempre verifica" como principio arquitectónico central
3. Integración nativa con el stack más común en Mexico: Microsoft, Trend Micro, Fortinet, Palo Alto
4. El cumplimiento normativo (ISO 27001, PCI-DSS, LFPDPPP) es subproducto natural de la arquitectura

6
Capas: red - IAM - endpoint - monitoreo - OpSec - humano

0-Trust
Zero Trust Architecture como principio rector

24/7
Operación del SOC sin interrupciones

85%
Reducción de superficie de ataque explotable

PRYSE
CYBERSECURITY

Soluciones Cloud Seguras

Hardening de entornos híbridos — sin sacrificar agilidad por seguridad

Cloud & Hybrid Security
FIRST México Liaison · ISO 27001 LA

EL PROBLEMA

- La migración a la nube amplia masivamente la superficie de ataque sin controles equivalentes a on-premise
- Configuraciones incorrectas en cloud (S3 abiertos, SSH expuesto) causan el 82% de brechas cloud
- Los equipos de TI no tienen visibilidad unificada de lo que ocurre en la nube versus infraestructura local

CAPACIDADES CLAVE

- Hardening de infraestructura híbrida: on-premise + cloud publica y privada simultáneamente
- IAM centralizado: Active Directory + Azure Entra ID unificados con mínimo privilegio
- Zero Trust con verificación continua de identidades y accesos en todos los entornos
- DevSecOps: seguridad integrada en las etapas iniciales del pipeline de CI/CD
- Cifrado de datos en tránsito (TLS 1.3) y en reposo (AES-256)
- Microsegmentación para limitar el movimiento lateral en caso de brecha

STACK TECNOLÓGICO

Azure Entra ID | AWS IAM | CIS Benchmarks | Terraform | Kubernetes | DevSecOps | AES-256/TLS 1.3

¿CÓMO FUNCIONA?

1. **Inventario Cloud** Mapeo completo de activos en la nube: VMs, buckets, funciones serverless, bases de datos e IAM roles
2. **Hardening** Aplicación de CIS Benchmarks para AWS/Azure/GCP; cierre de puertos y corrección de permisos excesivos
3. **Zero Trust** MFA universal, acceso mínimo privilegio y verificación contínua de cada solicitud de acceso
4. **DevSecOps** SAST, SCA y análisis de IaC integrados en el pipeline de CI/CD desde el inicio
5. **Resiliencia** SIEM con IA para visibilidad unificada cloud + on-premise y plan de recuperación ante incidentes

¿POR QUÉ ELEGIRNOS?

1. Experiencia en entornos híbridos complejos: Azure + AWS + on-premise simultáneamente
2. Gestión de parches automatizada en todos los entornos — sin ventanas de mantenimiento disruptivas
3. Hardening alineado con CIS Benchmarks nivel 2, NIST SP 800-53 y requisitos sectoriales
4. Capacitación incluida para el equipo de TI y DevOps en buenas practicas cloud nativa

99%
Reducción de configuraciones erróneas post-hardening

Multi
AWS - Azure - GCP - on-premise

CIS L2
Alineación CIS Benchmarks nivel 2

90%
Reducción de superficie cloud expuesta

PRYSE
CYBERSECURITY

Servicios Gestionados (SOC)

Tu Centro de Operaciones de Seguridad — sin la inversion de construirlo

Detección & Inteligencia
FIRST México Liaison · ISO 27001 LA

EL PROBLEMA

- Construir un SOC propio requiere $5M+ MXN y 18-24 meses solo para alcanzar madurez operativa mínima
- Las amenazas no respetan horarios: sin cobertura nocturna y fines de semana el atacante tiene ventana libre
- La rotación de analistas de seguridad supera el 50% anual en México — el talento escasea y cuesta retenerlo

CAPACIDADES CLAVE

- Monitoreo continuo 24/7/365 de red, endpoints, cloud y aplicaciones
- SIEM Gestionado: correlación de eventos y alertas priorizadas por nivel de riesgo real
- MDR (Managed Detection & Response): triage profundo, contención activa y análisis de causa raíz
- Threat Intelligence con feeds globales de IOCs, grupos APT y listas negras actualizadas
- Threat Hunting proactivo mensual con analistas L3 certificados MITRE ATT&CK
- Gestión de Vulnerabilidades: escaneo continuo, priorización por CVSS y verificación post-remediación

STACK TECNOLÓGICO

Trend Micro Vision One | Splunk / Elastic | Wazuh | MISP | TheHive | Cortex XSOAR | Velociraptor

¿CÓMO FUNCIONA?

1. **Onboarding** Integración de fuentes de logs, configuración del SIEM y establecimiento del baseline de comportamiento
2. **Monitoreo 24/7** Vigilancia permanente con correlación automática de eventos y primera línea de análisis
3. **Detección** Triage riguroso de alertas: separación de falsos positivos vs amenazas reales confirmadas
4. **Respuesta** Contención activa autorizada, notificación inmediata y coordinación con el equipo interno
5. **Reporte** Dashboards en tiempo real + reportes ejecutivos mensuales + evidencia lista para auditorias

¿POR QUÉ ELEGIRNOS?

1. SOC en español con analistas en México — sin barreras de idioma, zona horaria ni contexto cultural
2. FIRST México Liaison: acceso exclusivo a red global de IR y threat intelligence de primera línea
3. ISO 27001, PCI-DSS y LFPDPPP integrados como subproducto natural del servicio gestionado
4. SLA de notificación en menos de 15 minutos ante incidente crítico — escalamiento directo al CISO

24/7
Cobertura: noches, fines de semana y festivos

<15m
SLA de notificación ante incidente crítico

70%
Ahorro vs construir SOC interno equivalente

ISO+
PCI - LFPDPPP - ISO 27001 incluidos

PRYSE
CYBERSECURITY

Seguridad Ofensiva

Atacamos sus sistemas antes de que lo haga un adversario real

Red Team - Pentesting - Purple Team

FIRST México Liaison · ISO 27001 LA

EL PROBLEMA

- No saben si sus controles realmente funcionan — nunca han sido probados por un adversario hábil y motivado
- Las herramientas automatizadas dan falsa confianza: no simulan el pensamiento creativo del atacante
- El SOC y el Blue Team nunca han sido evaluados bajo presión real de un adversario sofisticado

CAPACIDADES CLAVE

- Pentesting: evaluación técnica acotada sobre alcance y metodología acordados
- Red Team: simulación completa de APT con C2, maximo sigilo y TTPs reales del adversario
- Purple Team: ejercicio colaborativo ofensivo-defensivo para maximizar capacidades de detección
- Ingeniería Social: phishing dirigido, vishing y pretexting contra empleados y ejecutivos
- Tabletop Exercises: simulaciones ejecutivas de crisis cibernética sin sistemas reales
- TIBER-MX: metodologia regulatoria de red teaming para el sector financiero

STACK TECNOLÓGICO

MITRE ATT&CK | Metasploit | Cobalt Strike / Sliver | BloodHound CE | Impacket | Burp Suite Pro

¿CÓMO FUNCIONA?

1. **Scoping** Alcance, objetivos, reglas de engagement, modalidad (black/grey/white box) y criterios de exito
2. **Reconocimiento** OSINT exhaustivo, enumeracion de infraestructura y mapeo completo de la superficie de ataque
3. **Explotacion** Ejecucion controlada con TTPs reales de MITRE ATT&CK para el adversario objetivo a simular
4. **Post-explotacion** Movimiento lateral, escalamiento de privilegios, persistencia y simulacion de impacto maximo
5. **Reporte** Informe ejecutivo (riesgo negocio) + tecnico (CVE, CVSS, evidencias,

¿POR QUÉ ELEGIRNOS?

1. Simulamos los adversarios que actúan realmente contra su sector en México — no escenarios genéricos
2. Red Team con C2 propio, operadores de ingeniería social y especialistas en acceso físico
3. Reportes en dos capas diferenciadas: ejecutivo para C-Suite y técnico para TI/Seguridad
4. Purple Team incluido: cada hallazgo del Red Team se convierte en detección nueva del Blue Team

4+
Pentest - Red Team - Purple Team - Tabletop - TIBER

MITRE
ATT&CK 14 tácticas 200+ técnicas

2-Cap
Reporte ejecutivo + técnico con CVSS

TIBER
Metodología regulatoria para financiero

PRYSE
CYBERSECURITY

Seguridad Cloud (CSPM/CWPP/CASB)

Triada de seguridad cloud — configura, protege y controla todo lo que corre en la nube

Cloud Security Posture
FIRST México Liaison · ISO 27001 LA

EL PROBLEMA

- Un bucket S3 abierto o SSH expuesto puede descubrir millones de registros en minutos
- Los contenedores y funciones serverless corren con privilegios excesivos sin protección de runtime
- Los empleados usan apps SaaS no autorizadas (Shadow IT) con datos corporativos sensibles sin control

CAPACIDADES CLAVE

- CSPM: evaluación continua de postura cloud vs CIS Benchmarks, NIST, ISO 27001 y PCI-DSS
- CWPP: protección de cargas de trabajo en VMs, contenedores Docker, Kubernetes y funciones serverless
- CASB: control de Shadow IT, apps SaaS no autorizadas y prevención de fuga de datos
- Cobertura multi-cloud simultanea: AWS, Azure y GCP desde un solo panel unificado
- Alertas priorizadas por riesgo con opción de remediación automatica para hallazgos críticos
- +Cumplimiento LFPDPPP / GDPR / PCI-DSS en flujos de datos cloud en tiempo real

STACK TECNOLÓGICO

Prisma Cloud / Wiz | Microsoft Defender for Cloud | AWS Security Hub | CSPM/CWPP/CASB | CIS Benchmarks

¿CÓMO FUNCIONA?

1. **CSPM** Conexión a APIs de AWS/Azure/GCP via conectores nativos; score de riesgo por proveedor y cuenta
2. **CWPP** Despliegue de agentes; escaneo de CVEs en imágenes y detección de comportamiento anómalo en runtime
3. **CASB** Modo API o proxy inline; inventario de Shadow IT y políticas de acceso basadas en contexto
4. **Visibilidad 360** Dashboard unificado con score de riesgo total, alertas correlacionadas y trazabilidad de datos
5. **Remediación** Workflows automáticos para hallazgos críticos + reportes de cumplimiento listos para auditorías

¿POR QUÉ ELEGIRNOS?

1. Cobertura de las 3 capas: infraestructura (CSPM) + runtime (CWPP) + acceso (CASB) sin ángulos ciegos
2. Multi-cloud real: AWS, Azure y GCP desde un unico panel de control
3. Remediación automática de hallazgos críticos — corrección activa de configuración
4. Cumplimiento PCI-DSS, LFPDPPP, ISO 27001 y SOC 2 monitoreados en tiempo real

3
Capas: CSPM + CWPP + CASB - 360 sin ángulos ciegos

Multi
AWS - Azure - GCP - un solo panel

100%
Visibilidad de Shadow IT y apps no autorizadas

Auto
Remediación automática de configuraciones criticas

PRYSE
CYBERSECURITY

Respuesta a Incidentes

Cuando cada minuto cuenta — contención, erradicación y recuperación de forma experta

Incident Response - DFIR

FIRST México Liaison · ISO 27001 LA

EL PROBLEMA

- Sin un plan estructurado cada incidente se improvisa — y los errores bajo presion cuestan el doble
- Un ransomware sin respuesta profesional puede costar entre el 1-5% del revenue anual en downtime
- La evidencia mal manejada en los primeros minutos puede ser inadmisible en cualquier proceso legal posterior

CAPACIDADES CLAVE

- Activación inmediata del CSIRT con analistas DFIR especializados en todos los vectores actuales
- Contención rápida y preservación de evidencia forense sin alterar trazas del ataque
- Investigación de causa raíz con análisis forense y cadena de custodia legal garantizada
- Erradicación completa de malware, backdoors, webshells y persistencia del atacante
- Coordinación con aseguradoras de ciberseguridad, reguladores y asesores legales
- Plan de recuperación y retorno controlado y monitoreado a entornos de producción

STACK TECNOLÓGICO

Trend Micro Vision One | Volatility Framework | FTK / Autopsy | YARA | TheHive | Velociraptor

¿CÓMO FUNCIONA?

1. **Preparación** Plan documentado, herramientas listas, CSIRT entrenado y simulacros periódicos
2. **Identificación** Detección y confirmación técnica; clasificación por severidad (P1-P4) y activación del plan
3. **Contención** Aislamiento de sistemas con preservación de evidencia; imagen forense; contención a largo plazo
4. **Erradicación** Eliminación verificada de malware, backdoors, accesos no autorizados y vectores de entrada
5. **Recuperación** Retorno controlado a producción con monitoreo intensivo y validación de integridad
6. **Lecciones** Análisis post-incidente, informe ejecutivo final y actualización del plan para futuros eventos

¿POR QUÉ ELEGIRNOS?

1. CSIRT con experiencia en ransomware, BEC, webshells, skimming y ataques en México
2. Respuesta en horas, infraestructura y playbooks listos para activar inmediatamente con retainer
3. Trend Micro Vision One XDR para visibilidad y contención técnica de alta velocidad
4. Informes con validéz legal y cadena de custodia para procesos judiciales o auditorias regulatorias

<1h
Activación del equipo DFIR desde la llamada

6
Pases NIST: Preparar-Identificar-Contener-Erradicar-Recuperar-Aprender

100%
Documentación legal con cadena de custodia

60%
Reduccion del impacto financiero vs improvisar

PRYSE
CYBERSECURITY

Monitoreo VIP

Protección digital personalizada para ejecutivos y personas de alto perfil

Executive Cyber Protectio

FIRST México Liaison · ISO 27001 LA

EL PROBLEMA

- Los ejecutivos C-Level son el objetivo preferido de spear-phishing, fraudes BEC y extorsiones digitales
- La información personal en dark web y redes sociales es el punto de entrada para ataques dirigidos
- Un ataque al CEO desencadena crisis reputacional, fuga de información estratégica y potenciales fraudes

CAPACIDADES CLAVE

- Monitoreo 24/7 de identidad digital, cuentas corporativas y dispositivos del VIP
- Escaneo activo de dark web: credenciales, datos personales y financieros filtrados
- Análisis de exposición digital completa: redes sociales, repositorios públicos, fuentes abiertas
- Detección de anomalías con IA: comportamientos inusuales en cuentas y dispositivos
- Defensa personalizada contra spear-phishing, vishing, deepfakes y suplantación de identidad
- Evaluación de riesgos del entorno familiar y colaboradores cercanos del VIP

STACK TECNOLÓGICO

Dark Web Intelligence | OSINT Avanzado | AI Anomaly Detection | HUMINT | Digital Forensics | Threat Intelligence

¿CÓMO FUNCIONA?

1. Perfil de Riesgo Construcción del perfil digital completo del VIP: exposición actual, vectores de riesgo y contexto org
2. Configuración Despliegue de sensores en dispositivos, cuentas, dark web y fuentes de inteligencia relevantes
3. Monitoreo 24/7 Vigilancia continua de identidad, dark web, redes sociales y comportamiento de cuentas/dispositivos
4. Alertas Notificación inmediata ante cualquier anomalía, filtración o señal de ataque dirigido detectada
5. Respuesta Activación de protocolos, asesoría directa al VIP y coordinación con seguridad física si se requiere

¿POR QUÉ ELEGIRNOS?

1. Servicio 100% personalizado: analista dedicado por VIP que conoce en profundidad su perfil de riesgo
2. Convergencia digital-física: coordinamos con equipos de seguridad física cuando el riesgo lo exige
3. Discreción total: NDA estricto y protocolos de confidencialidad de nivel ejecutivo garantizados
4. Cobertura del entorno: familia inmediata y colaboradores cercanos como potenciales vectores de ataque

24/7
Monitoreo continuo de identidad y dispositivos

Dark Web
Escaneo activo de datos filtrados en mercados clandestinos

360
Digital - social - familiar - convergencia física

AI/ML
Detección de anomalías conductuales con IA

PRYSE
CYBERSECURITY

Formación y Concientización

Convierte el eslabón más débil en tu primera línea de defensa

Security Awareness Training

FIRST México Liaison · ISO 27001 LA

EL PROBLEMA

- Más del 90% de los incidentes tienen al factor humano como origen — phishing, contraseñas débiles, errores
- Sin un programa continuo, un solo clic en un phishing puede comprometer toda la organización en minutos
- Las regulaciones (LFPDPPP, ISO 27001, PCI-DSS) exigen evidencia documentada de capacitación del personal

CAPACIDADES CLAVE

- Programas de concientización continua adaptados al sector y perfil de riesgo de la organización
- Simulaciones de phishing controladas: campañas reales con métricas precisas de vulnerabilidad
- Capacitación en reconocimiento de ingeniería social, ransomware, BEC y amenazas emergentes
- Buenas prácticas: gestores de contraseñas, MFA y manejo seguro de datos sensibles
- Módulos especializados: trabajo remoto, Wi-Fi públicas y dispositivos móviles BYOD
- Evidencia de cumplimiento lista para auditorías externas de ISO 27001 o PCI-DSS

STACK TECNOLÓGICO

GoPhish | KnowBe4 | Plataforma LMS | SCORM | Metricas de comportamiento | Simuladores ingenieria social

¿CÓMO FUNCIONA?

1. **Diagnóstico** Evaluación baseline del nivel de madurez del personal y vectores de riesgo humano más críticos
2. **Diseno** Plan 100% personalizado: modulos, frecuencia de entrega, formatos didacticos y metricas de exito
3. **Capacitacion** Talleres presenciales, e-learning, microlearning, videos cortos y pildoras semanales
4. **Simulacion** Campanas de phishing controladas con escenarios del sector para detectar personal de alto riesgo
5. **Medicion** Reportes de tasa de clic, reportes de phishing por usuarios y evolucion del nivel de madurez

¿POR QUÉ ELEGIRNOS?

1. Contenido desarrollado por profesionales con experiencia real en incidentes — no material generico importado
2. Simulaciones de phishing con escenarios del sector del cliente en espanol — no plantillas americanas
3. Formacion con contexto mexicano real: casos, leyes y amenazas de la industria local y LATAM
4. Evidencia documentada lista para auditorias: registros de asistencia, evaluaciones y reportes de phishing

>90%
De los incidentes tienen al factor humano como origen

75%
Reducción tasa de clic en phishing tras 6 meses

12m
Pograma anual continuo — no un evento puntual

100%
Evidencia para auditorias ISO 27001 y LFPDPPP

PRYSE
CYBERSECURITY

Informatica Forense

Evidencia digital con validez legal — del incidente al proceso judicial

DFIR - Peritaje Digital - Legal

FIRST Mexico Liaison · ISO 27001 LA

EL PROBLEMA

- La evidencia digital mal manejada en los primeros minutos puede ser inadmisible en cualquier proceso legal
- Sin analisis forense riguroso no es posible determinar el alcance real del ataque ni si el atacante persiste
- Las empresas enfrentan responsabilidades legales que requieren informes tecnicos con validez juridica

CAPACIDADES CLAVE

- Adquisicion y preservacion de evidencia digital con cadena de custodia legalmente valida
- Analisis forense de equipos, servidores, dispositivos moviles y volcados de memoria RAM
- Analisis de malware: ingenieria inversa, identificacion de familia y determinacion de comportamiento
- Investigacion de trafico de red: PCAP, logs de firewall, proxy y sistemas de autenticacion
- Peritaje judicial: informes con validez legal para procesos penales, civiles y laborales
- Asesoria normativa: Convenio de Budapest, CPF Arts. 211 Bis, LFPDPPP e INAI

STACK TECNOLÓGICO

FTK Imager | Autopsy | Volatility Framework | Wireshark | YARA | Cellebrite

¿CÓMO FUNCIONA?

1.. **Preservación** Aseguramiento inmediato de la escena digital — no apagar sistemas, preservación in-situ
2. **Adquisición** Imagen forense bit-a-bit con herramientas certificadas y verificación por hash SHA-256
3. **Análisis** Examen de artefactos: logs, registry, malware, metadatos, línea de tiempo y actividad de usuario
4. **Documentación** Informe técnico pericial: hallazgos, metodología, cadena de custodia y conclusiones objetivas
5. **Peritaje** Presentación de evidencias y testimonio experto ante autoridades judiciales o reguladores

¿POR QUÉ ELEGIRNOS?

1. Experiencia forense en incidentes reales mexicanos: ransomware, webshells, BEC, skimming y municipios
2. Cadena de custodia garantizada: nuestros informes han sido utilizados en procesos judiciales en México
3. Alianza con asesores jurídicos especializados en delitos informáticos según la legislación mexicana vigente
4. Capacidad de análisis de malware avanzado incluyendo implantes APT, rootkits y herramientas de acceso remoto

100%
Cadena de custodia legal en toda adquisición de evidencia

48h
informe forense preliminar en incidentes críticos

Legal
Validéz judicial para procesos penales y civiles en México

CPF
Alineado con Arts. 211 Bis del Codigo Penal Federal

PRYSE
CYBERSECURITY

Cumplimiento Normativo

De la brecha regulatoria a la certificación — sin interrumpir la operación

Compliance - GRC - Auditoria

FIRST México Liaison · ISO 27001 LA

EL PROBLEMA

- Las multas por incumplimiento de LFPDPPP, PCI-DSS o ISO 27001 pueden superar $5M MXN más daño reputacional
- Los equipos internos no saben exactamente que controles implementar ni como demostrar cumplimiento ante un auditor
- El cumplimiento se trata como esfuerzo puntual anual en lugar de un proceso continuo de gestion de riesgos

CAPACIDADES CLAVE

- GAP Analysis contra ISO 27001, PCI-DSS, LFPDPPP, SOC 2 y marcos sectoriales aplicables
- Diseno e implementacion del Sistema de Gestion de Seguridad de la Información (SGSI)
- Gestión de riesgos: identificación, evaluación, tratamiento y monitoreo continuo
- Elaboración de toda la documentación: políticas, procedimientos, planes y registros obligatorios
- Preparación y acompanamiento en auditorías externas de certificación
- Regulación mexicana: CPF Arts. 211 Bis, Ley de Instituciones de Crédito, normativa INAI

STACK TECNOLÓGICO

ISO 27001 | PCI-DSS v4.0 | LFPDPPP / INAI | NIST CSF 2.0 | SOC 2 Type II | GRC Platforms

¿CÓMO FUNCIONA?

1.. GAP Analysis Evaluación del estado actual vs requisitos del marco normativo; identificación de brechas prioritarias
2. Roadmap Plan de remediación priorizado por nivel de riesgo y costo-beneficio con cronograma realista
3. Implementación Apoyo técnico y documental en implementación de controles: políticas, procedimientos y herramientas
4. Auditoría Interna Simulacro completo para identificar y corregir hallazgos antes de la evaluación externa
5. Certificación Acompanamiento durante la auditoría externa y gestión de planes de acción post-auditoría

¿POR QUÉ ELEGIRNOS?

1. Lead Auditor ISO 27001 certificado en el equipo — conocemos exactamente que buscan los auditores externos
2. Cumplimiento adaptado al marco legal mexicano: LFPDPPP, CPF 211 Bis, Ley de Instituciones de Crédito
3. El cumplimiento se construye sobre arquitectura de seguridad real — no como capa burocrática adicional
4. Experiencia en certificaciones simultáneas: ISO 27001 + PCI-DSS + LFPDPPP en un solo proceso integrado

5+
Marcos: ISO 27001 - PCI-DSS - LFPDPPP - SOC 2 - NIST

100%
Documentación completa elaborada e incluida

90%
Reducción de hallazgos en auditoría externa

LA
Lead Auditor ISO 27001 en el equipo de servicio

PRYSE
CYBERSECURITY

Auditoría de Código (SAST/DAST)

Encuentra vulnerabilidades en tu código antes de que un atacante las explote en producción

Application Security - DevSecOps

FIRST México Liaison · ISO 27001 LA

EL PROBLEMA

- Una SQLi o XSS en producción puede ser detectada y explotada en minutos por herramientas del atacante
- El 80% del código moderno es de terceros (librerías open source) — y casi nunca se audita por CVEs conocidos
- Las auditorías puntuales anuales son insuficientes: el código cambia semanalmente y las vulns aparecen en cada release

CAPACIDADES CLAVE

- SAST: análisis estático del código fuente — detecta vulnerabilidades desde el desarrollo antes del despliegue
- DAST: pruebas dinámicas sobre la aplicación en ejecución — ataque de caja negra como un atacante real
- IAST: agente interno que combina la profundidad de SAST con el contexto real de ejecución del DAST
- SCA (Software Composition Analysis): CVEs en librerías de terceros y dependencias open source
- Secrets Scanning: detección de credenciales, tokens y API keys hardcodeados en código y repositorios
- Integración en pipeline CI/CD: detección automática en cada commit del equipo de desarrollo

STACK TECNOLÓGICO

SonarQube / Semgrep | Burp Suite Pro | OWASP ZAP | Snyk | GitLeaks / TruffleHog | Dependabot

¿CÓMO FUNCIONA?

1. **SAST Setup** Configuración del motor estático e integración con el repositorio; baseline de falsos positivos
2. **DAST Config** Configuración del escaner dinámico contra staging con credenciales reales; definición del scope
3. **Pipeline CI/CD** Integración en el flujo: análisis automático en cada commit, PR y antes de cada despliegue
4. **Triaje** Revisión manual de hallazgos: eliminación de falsos positivos y priorización por CVSS y contexto
5. **Remediación** Guías de corrección específicas al equipo dev con ejemplos de código seguro y verificación post-fix

¿POR QUÉ ELEGIRNOS?

1. SAST + DAST + IAST + SCA + Secrets Scanning en proceso integrado y continuo — no auditorías aisladas anuales
2. Integración real en CI/CD: shift-left genuino — vulns detectadas en desarrollo son 10x mas baratas de corregir
3. Triaje humano experto: eliminamos el ruido de falsos positivos que paraliza a los equipos sin experiencia
4. Cobertura completa: Python - Java - C# - Go - JS/TS - PHP - IaC (Terraform, Kubernetes, Dockerfiles)

Shift-Left
Detección en desarrollo 10x mas barata que en producción

OWASP
Top 10: SQLi - XSS - IDOR - SSRF - A01-A10

5+
SAST - DAST - IAST - SCA - Secrets Scan - RASP

CI/CD
Integración automática en pipeline DevSecOps

PRYSE
CYBERSECURITY

Data Center Tier II

Infraestructura de misión crítica con 99.741% de disponibilidad certificada por Uptime Institute

Infraestructura Certificada
FIRST México Liaison · ISO 27001 LA

EL PROBLEMA

- Una infraestructura sin redundancia es un punto único de falla que puede costar $500K+ MXN por hora de downtime
- El mantenimiento de equipos críticos sin redundancia obliga a parar el servicio — con Tier II ya no es necesario
- Los clientes y reguladores exigen certificaciones de infraestructura como evidencia de disponibilidad y resiliencia

CAPACIDADES CLAVE

- Redundancia N+1 en todos los componentes críticos: energia, refrigeración y conectividad de red
- Generadores de respaldo, sistemas UPS enterprise y unidades de enfriamiento (chillers) redundantes
- Mantenibilidad parcial certificada: tareas de mantenimiento sin detener la operación
- Certificación oficial Uptime Institute Tier II — el estándar mundial de referencia
- Monitoreo DCIM 24/7 de temperatura, energía, conectividad y seguridad física
- PUE (Power Usage Effectiveness) optimizado para eficiencia energética y reducción de costos

STACK TECNOLÓGICO

UPS Enterprise | Generadores Diesel/Gas | CRAC/CRAH Chillers | DCIM Platform | Fibra Redundante | Uptime Institute

¿CÓMO FUNCIONA?

1. **Evaluación** Diagnóstico de necesidades: disponibilidad, capacidad y crecimiento proyectado del cliente
2. **Diseño** Arquitectura redundante N+1 alineada con los estándares del Uptime Institute para Tier II
3. **Implementación** Despliegue de sistemas redundantes: generadores, UPS, CRAC/CRAH, redes y seguridad física
4. **Certificación** Proceso formal de certificación ante el Uptime Institute con documentación técnica validada
5. **Operación** Monitoreo continuo 24/7 con DCIM, mantenimiento preventivo sin interrupción y reporte mensual

¿POR QUÉ ELEGIRNOS?

1. Certificación Uptime Institute Tier II — el estándar de referencia mundial para disponibilidad de data centers
2. 99.741% de uptime anual garantizado: no más de 22 horas de downtime total acumulado por año
3. Mantenibilidad sin interrupción: mantenimiento de equipos críticos durante la operación normal
4. Propuesta única: infraestructura Tier II certificada + servicios de ciberseguridad en un solo proveedor

99.741%
Disponibilidad anual certificada Uptime Institute

N+1
Redundancia en energía, refrigeración y conectividad

<22h
Máximo downtime acumulado permitido por año

Cert.
Certificación oficial Uptime Institute

DEFENSA EN PROFUNDIDAD

Del reconocimiento a la respuesta: cobertura del ciclo completo.

Aplicamos el marco NIST CSF 2.0 (GOVERN · IDENTIFY · PROTECT · DETECT · RESPOND · RECOVER) para garantizar cobertura integral.

GOBIERNO

Gobierno, políticas y gestión del riesgo.

IDENTIFICACIÓN

Inventario de activos y evaluación de riesgos.

PROTECCIÓN

Controles preventivos, hardening y Zero Trust.

DETECCIÓN

Monitoreo 24/7, SIEM, EDR y threat hunting.

RESPUESTA

Contención, DFIR y gestión de crisis.

RECUPERACIÓN

Restauración, lecciones aprendidas y mejora.

< 15 min
Tiempo medio de detección (MTTD)

< 30 min
Tiempo medio de respuesta (MTTR)

+200
Controles mapeados a MITRE ATT&CK

99.95%
SLA de disponibilidad del SOC

TECNOLOGÍA ESTRATÉGICA EXCLUSIVA

Silent Push

Defensa cibernética predictiva basada en tecnología IOFA™ (Indicators Of Future Attack).

Identificamos la infraestructura del adversario desde el momento en que se crea antes del primer ataque.

Mientras las soluciones tradicionales reaccionan a IOCs conocidos, Silent Push rastrea el comportamiento de los actores maliciosos y anticipa los ataques semanas antes de su ejecución.

Bloquea amenazas emergentes. Protege marca e infraestructura. Reduce la ventana de exposición a cero.

Detección proactiva de dominios maliciosos

Phishing y suplantación institucional bloqueados antes de su activación.

Monitoreo de infraestructura adversarial

Rastreo de IPs, ASNs y certificados TLS vinculados a grupos APT.

Alertas en tiempo real

Notificación automática al detectar infraestructura dirigida a su dominio.

Integración SIEM / SOAR

Inteligencia accionable lista para automatización y orquestación.

Resultado: una ventana de anticipación promedio de 45 días frente a campañas activas de phishing y ransomware.

RESPALDO Y CREDIBILIDAD

Certificaciones y alianzas que nos avalan.

Un equipo entrenado por las instituciones de ciberseguridad más reconocidas del mundo y respaldado por los fabricantes líderes del mercado.

CERTIFICACIONES DEL EQUIPO

TIER DESIGN® Grupo de Seguridad Privada PRYSE de México PRYSE Cybersecurity DC Cuernavaca Expires 27 January 2028 UPTIME INSTITUTE CERTIFIED

EMPRESA CERTIFICADA MB CERTIFICATION ISO 9001:2015

ISO 22301:2019 CERTIFICACIÓN

EMPRESA CERTIFICADA MB CERTIFICATION ISO 20000-1:2018

EMPRESA CERTIFICADA MB CERTIFICATION ISO 27001:2022

EMPRESA CERTIFICADA MB CERTIFICATION ISO 37001:2025

ALIANZAS ESTRATÉGICAS

Somos asociados de las tecnologías líderes de la industria de ciberseguridad.

¿POR QUÉ PRYSE CYBERSECURITY?

01 **Enfoque personalizado**
Creamos soluciones alineadas a las necesidades del negocio.

02 **Inteligencia ofensiva**
Pensamos como el adversario para defender mejor.

03 **Ejecución impecable**
Metodologías probadas y entregables ejecutivos.

04 **Infraestructura propia**
Centro de datos TIER II, SOC/NOC y CERT

NUESTRO

SOC Y CENTRO DE DATOS

Tu adversario ya te está perfilando

Anticípate con PRYSE CYBERSECURITY.

Transformamos la ciberseguridad de costo operativo a ventaja competitiva.

AGENDE UNA EVALUACIÓN EJECUTIVA

Diagnóstico inicial sin costo · 45 minutos · **Conclusiones accionables.**

WEB
www.prysecybersecurity.com

CORREO
ventas@prysecybersecurity.com

TEL
+52 5620808483