
GBM
CYBERSECURITY
CENTER

Alonso Ramírez

Perfil del expositor

Alonso Ramírez es **Regional Cyber Security Manager en GBM Corporation** y profesor en las universidades **INCAE y CENFOTEC**, donde imparte cursos de Ciberseguridad y Continuidad de Negocio a nivel de ingeniería, postgrado y maestría. Con más de **20 años de experiencia en ciberseguridad**, es **Hacker Ético Certificado**, Máster en Auditoría de Tecnologías de Información y Máster en ISO/IEC 27001.

Cuenta con la certificación **CNSS 4011 Recognition** otorgada por la NSA (**National Security Agency**), que avala a los profesionales en seguridad de redes con los conocimientos necesarios para desempeñarse tanto en el sector privado como en el público en Estados Unidos.

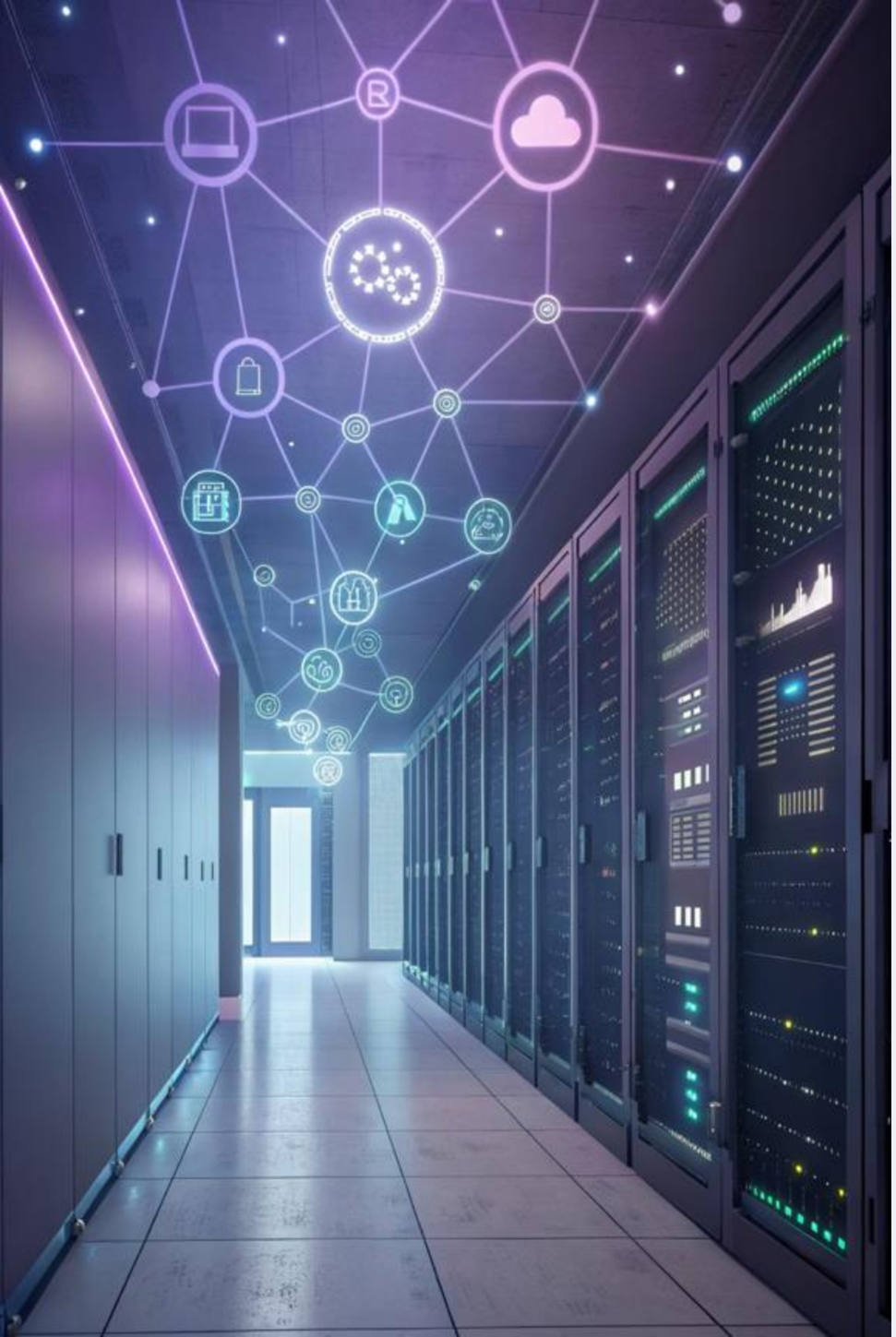
Miembro de las **Comisiones de Ciberseguridad de Infocom**, de la **Junta Directiva del Clúster de Ciberseguridad de Costa Rica** y miembro corporativo del **Global Forum of Incident Response and Security Teams**.

Ha ocupado cargos de **Gerente de Consultoría y Arquitectura de Ciberseguridad**, liderando soluciones y servicios para empresas como **Deloitte, IBM, Cisco, Palo Alto Networks, Microsoft y Splunk**.

Ha sido **Comandante de Incidentes** frente a ataques cibernéticos contra infraestructuras críticas en la región, y se ha destacado como expositor en seminarios y conferencias dentro y fuera del país.

“En los próximos cinco años, su empresa será tan segura como el eslabón más débil de su nube”

GBM CYBERSECURITY CENTER | GBM



Arquitectura del Futuro: Ciberseguridad para la IA y la Nube Conectadas

Alonso Ramírez

Regional Cybersecurity Manager
GBM Corporation | Managed Security Service Provider

GBM CYBERSECURITY CENTER | GBM

Agenda

Contexto y tendencias globales

Panorama actual de amenazas emergentes y adopción tecnológica

Riesgos y amenazas en LATAM

Análisis de vulnerabilidades específicas para la región

Casos de uso regionales

Ejemplos prácticos de los últimos 3 años

Datos y estadísticas

Cifras relevantes 2022-2025 sobre ciberseguridad en IA y nube

Metodología 4D aplicada

Detección, Defensa, Disuasión y Disrupción

Recomendaciones estratégicas

Acciones concretas para empresas y gobiernos

GBM CYBERSECURITY CENTER | GBM

Contexto y Tendencias Globales

El escenario de ciberseguridad está evolucionando rápidamente con la adopción masiva de inteligencia artificial y servicios en la nube, creando un nuevo panorama de vulnerabilidades y desafíos para organizaciones en todo el mundo.

La convergencia de estas tecnologías ha generado una nueva generación de amenazas que requieren enfoques innovadores de protección.

Tendencias Preocupantes en IA y Nube

La rápida adopción de la Inteligencia Artificial y los servicios en la nube presenta desafíos significativos en ciberseguridad, a pesar de sus beneficios evidentes.

Adopción Masiva de IA

Más del 85% de las empresas del Fortune 500 utilizan soluciones de IA de Microsoft.

El uso de IA generativa creció del 55% al 75% en 2024 (IDC).

Brechas en IA

Según **IBM** (julio 2025), el 13% de las organizaciones sufrió brechas en modelos o aplicaciones de IA.

De estas, el 97% carecía de controles de acceso adecuados, resultando en compromiso de datos (60%) e interrupciones operativas (31%).

Baja Preparación

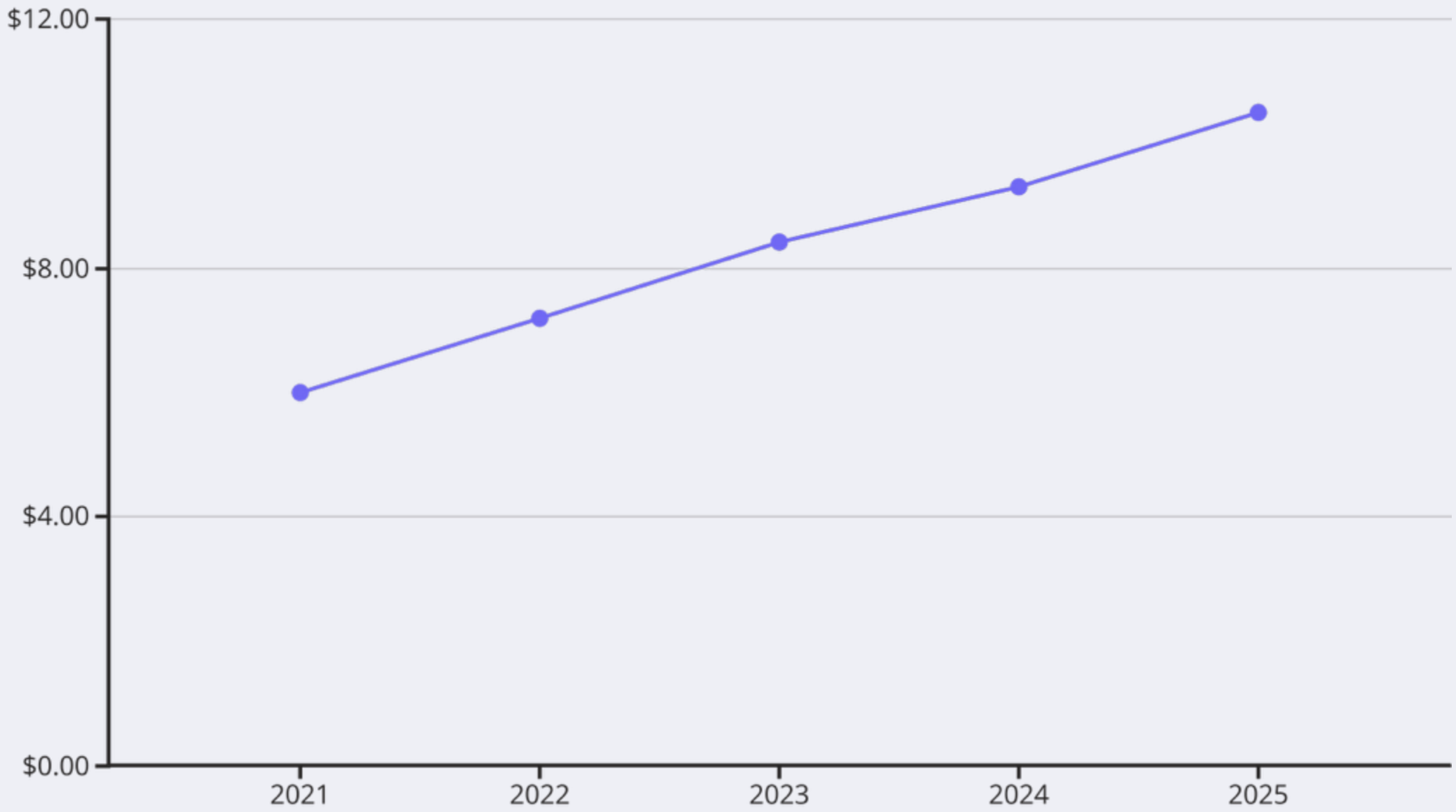
Solo el 13% de las organizaciones están "totalmente preparadas" para la IA, una disminución respecto al 14% del año anterior (AI Readiness Index 2024).

IA en Ciberseguridad

El 89% de las organizaciones utilizan IA para entender amenazas, el 85% para detección de ataques y el 70% para respuesta y recuperación (***Cisco Cybersecurity Readiness Index 2025***).

CYBERSECURITY CENTER | GBM

Impacto Económico del Cibercrimen



Se proyecta que el costo global del cibercrimen alcanzará los USD 10,5 billones en 2025, impulsado por la sofisticación de ataques basados en IA y vulnerabilidades en infraestructuras cloud.

GBM CYBERSECURITY CENTER | GBM

Riesgos y Amenazas en LATAM

Latinoamérica enfrenta desafíos únicos en ciberseguridad debido a la rápida adopción tecnológica, la brecha de habilidades técnicas y el creciente interés de actores maliciosos en la región.

La transformación digital acelerada post-pandemia ha creado nuevos vectores de ataque que explotan vulnerabilidades específicas del contexto regional.

GBM CYBERSECURITY CENTER | GBM

México: Epicentro de Ciberataques en LATAM

Datos alarmantes

- Concentra más del 50% de los ciberataques en toda la región
- 31.000 millones de intentos de ataque registrados solo en el primer semestre de 2024
- Grupos criminales emplean tecnologías de IA para evadir detección y automatizar ataques
- Sectores críticos como manufactura, logística y automotriz son objetivos prioritarios

En 2024, la inversión extranjera y el nearshoring convertío a México en un objetivo de alto valor para ciberdelincuentes.

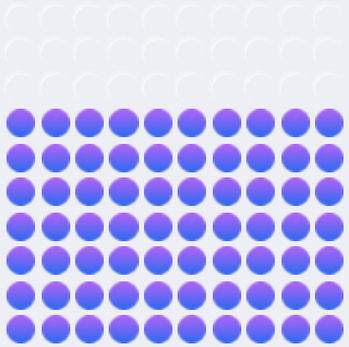
GBM CYBERSECURITY CENTER | GBM

Panorama Regional de Amenazas

86%

Impacto Directo en Negocio

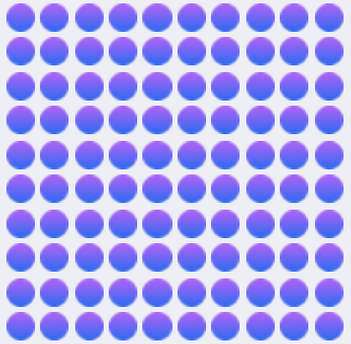
De más de 500 ciberataques importantes respondidos por el equipo **Unit 42** en 2024, el 86% generó un impacto directo en las operaciones, reputación o finanzas de las organizaciones.



70%

Ataques Multivectoriales

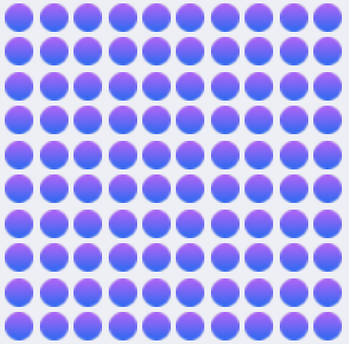
El 70% de los incidentes abarcó tres o más vectores de ataque (endpoints, red, nube, factor humano), destacando la creciente complejidad y naturaleza simultánea de los ciberataques modernos.



+311 mil MM

Aumento Global de Ciberataques

En su reporte **State of the Internet 2025**, Akamai reveló un **aumento del 33%** interanual en ataques web y a APIs a nivel global, con más de 311 mil millones de intentos en 2024.



+419%

LATAM: Ciberataques al Sector Financiero

Para América Latina, el sector financiero experimentó un alarmante incremento del 419% en ataques dirigidos a aplicaciones web y APIs, generando costos estimados de $90 mil millones de dólares anuales.

GBM CYBERSECURITY CENTER | GBM

Casos de Uso Regionales

La región está experimentando transformaciones significativas en su postura de ciberseguridad, con casos notables que demuestran tanto vulnerabilidades como avances estratégicos en la protección de infraestructuras críticas.

Estos ejemplos recientes revelan tendencias específicas para la región y oportunidades de mejora.

Casos de Impacto en la Región

1

México (2023-2025)

El auge del nearshoring ha convertido sectores logístico, automotriz y manufacturero en objetivos prioritarios. Ataques sofisticados han comprometido cadenas de suministro críticas y propiedad intelectual.

2

Chile (2023)

Inversión estratégica de AWS de USD 4 mil millones en infraestructura cloud y soporte para IA. El proyecto enfrenta desafíos de seguridad para datos críticos y consideraciones ambientales.

3

Costa Rica (2024)

Desarrollo de marcos regulatorios alineados con estándares europeos sobre IA, 5G y ciberseguridad, estableciendo precedentes para la región en gobernanza tecnológica.

Impacto del Nearshoring en Ciberseguridad

Nueva superficie de ataque

La relocalización de empresas manufactureras a México ha creado una superficie de ataque ampliada con sistemas OT/IT interconectados y vulnerables.

Interés de actores maliciosos

Grupos de amenazas persistentes avanzadas (APTs) han reorientado sus operaciones hacia instalaciones industriales mexicanas, buscando propiedad intelectual y oportunidades de extorsión.

Caso: Sector Automotriz

Una importante planta automotriz en Guanajuato sufrió una interrupción de producción de 3 días tras un ataque ransomware que comprometió sistemas de control industrial conectados a la nube.

Lecciones aprendidas

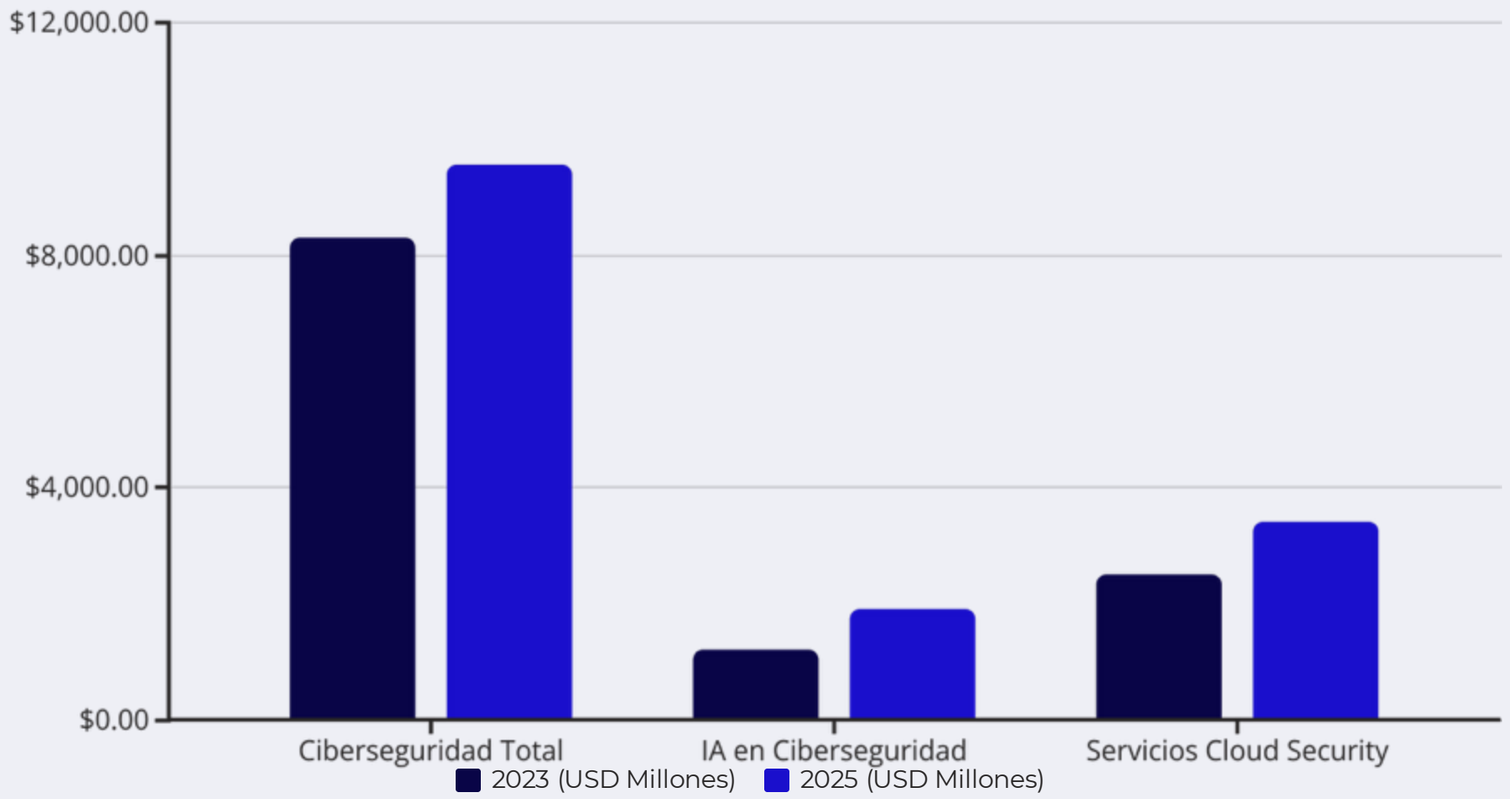
- Necesidad de segmentación OT/IT rigurosa
- Protección específica para cargas de IA en entornos híbridos
- Monitoreo de amenazas específicas para la cadena de suministro

Datos y Estadísticas Recientes

El mercado de ciberseguridad en Latinoamérica está experimentando un crecimiento acelerado, impulsado por la necesidad de proteger infraestructuras críticas y el aumento de amenazas sofisticadas.

Las inversiones en soluciones de IA para ciberseguridad reflejan la evolución del panorama de amenazas en la región.

Mercado de Ciberseguridad en LATAM



El mercado de ciberseguridad en LATAM alcanzará los USD 9,54 mil millones en 2025, con un crecimiento proyectado del 6,95% anual.

La IA aplicada a ciberseguridad muestra el crecimiento más acelerado, con un CAGR del 26,2% hasta 2030.

Indicadores Clave del Mercado

69 % de ingresos Q1-2025

Akamai Cloud revenues +25 % YoY (2024); infraestructura cloud +32 %; seguridad y cloud representan 69 % de ingresos Q1-2025; previsión de ARR cloud +40–45 %.

22,2%

CAGR proyectado para el mercado de seguridad en la nube en LATAM (2025-2030), superando el promedio global

75%

De auditores internos en LATAM identifican la ciberseguridad como principal riesgo organizacional (Risk in Focus)

La disrupción digital (incluyendo IA) se posiciona como el segundo riesgo más importante para las organizaciones latinoamericanas, impulsando inversiones en protección avanzada.

GBM CYBERSECURITY CENTER | GBM

Metodología 4D: Un Nuevo Paradigma

Para enfrentar amenazas avanzadas en entornos de IA y nube, proponemos un enfoque integral basado en cuatro dimensiones complementarias que forman un sistema de defensa adaptativo y resiliente.

GBM CYBERSECURITY CENTER | GBM

Modelo 4D para Ciberseguridad Avanzada

Detección

Identificación temprana de amenazas mediante IA y análisis avanzado de comportamientos anómalos.

Defensa

Protección proactiva de infraestructuras y datos críticos mediante controles técnicos robustos.

Disuasión

Estrategias para aumentar el costo percibido del ataque y reducir su atractivo.

Disrupción

Interrumpir operaciones maliciosas mediante respuesta coordinada y contramedidas efectivas.

Este enfoque integral garantiza la protección de entornos híbridos donde IA y nube están profundamente integradas, atendiendo vulnerabilidades específicas de la región.

GBM CYBERSECURITY CENTER | GBM

Detección: Primera Línea de Defensa

Capacidades Avanzadas

- Analítica de comportamiento impulsada por IA para identificar anomalías sutiles en patrones de acceso y uso
- Monitoreo continuo de cargas de trabajo en nube con aprendizaje automático para detectar configuraciones inseguras
- Detección de fugas de datos sensibles mediante análisis semántico y contextual

Caso LATAM

Malware brasileño **Ousaban**, que infecta sistemas bancarios utilizando múltiples servicios en la nube para ejecutar su cadena de ataque. Descarga payloads desde Amazon S3 o Azure, recupera configuraciones desde Pastebin o Google Docs y usa **Telegram webhooks** como canal de comando y control (C2).

GBM CYBERSECURITY CENTER | GBM

Defensa: Protección Estructurada

Hardening en Cargas de IA

El 70% de las cargas de trabajo con componentes de IA presentan vulnerabilidades críticas, frente al 50% de cargas tradicionales

Segmentación OT/Cloud

Fortinet reporta reducción del 65% en ataques exitosos gracias a estrategias de segmentación e inteligencia contextual

Arquitectura Zero Trust

Implementación de controles de acceso dinámicos basados en contexto, identidad y comportamiento

La defensa efectiva requiere un enfoque multicapa que considere la convergencia entre tecnologías de IA, servicios en la nube y sistemas tradicionales, especialmente en entornos industriales latinoamericanos con infraestructura híbrida.

GBM CYBERSECURITY CENTER | GBM

Disuasión: Elevando el Costo del Ataque

Marco Regulatorio

Brasil y Colombia lideran el desarrollo de regulaciones para IA y transparencia en ciberseguridad, creando consecuencias legales claras para actores maliciosos.

Monitoreo Activo

Sistemas de vigilancia digital que demuestran capacidad de detección, aumentando la percepción de riesgo para potenciales atacantes.

Atribución Pública

La identificación y exposición pública de atacantes actúa como elemento disuasorio, especialmente para grupos patrocinados por estados o grandes organizaciones criminales.

Cooperación Internacional

Alianzas entre países latinoamericanos para compartir inteligencia y coordinar respuestas legales contra ciberdelincuentes transnacionales.

Disrupción: Neutralizando Amenazas

1

Equipos de Respuesta Rápida

Formación de equipos especializados en incidentes (IR) con capacidad para neutralizar amenazas en entornos de IA y nube, reduciendo el tiempo de respuesta en un 60%.

2

Centro de Ciberseguridad e IA

Propuesta **tica (N.° 24.939)** para establecer un centro gubernamental dedicado a coordinar respuestas a incidentes y compartir inteligencia sobre amenazas regionales.

3

Plataformas Unificadas

Palo Alto Networks reporta 11 mil millones de amenazas bloqueadas mediante plataformas integradas, frente a soluciones fragmentadas tradicionales.

La capacidad de disrupción depende de la velocidad de respuesta y la efectividad de las contramedidas, especialmente en entornos complejos donde la IA puede multiplicar el impacto de los ataques.

GBM CYBERSECURITY CENTER | GBM

Recomendaciones Estratégicas

Para construir arquitecturas de seguridad efectivas en el contexto latinoamericano, es necesario implementar estrategias específicas que consideren las particularidades regionales y el panorama de amenazas emergentes.

Las siguientes recomendaciones proporcionan un marco de acción para diferentes actores del ecosistema.

GBM CYBERSECURITY CENTER | GBM

Estrategias para Empresas

Implementar Modelo 4D

- Adoptar el enfoque integral con énfasis en detección avanzada
- Evaluar madurez actual en cada dimensión
- Priorizar inversiones según brechas identificadas

Reforzar Controles Técnicos

- Aplicar parches prioritarios en cargas de IA
- Implementar segmentación rigurosa OT/Cloud
- Adoptar plataformas integradas SASE y Zero Trust

Desarrollar Capacidades

- Formar equipos multidisciplinarios
- Establecer programa de concientización específico
- Crear planes de respuesta a incidentes adaptados

Según Palo Alto Networks, las organizaciones que implementan un enfoque integrado experimentan un 45% menos de brechas significativas que aquellas con soluciones fragmentadas.

GBM CYBERSECURITY CENTER | GBM

Estrategias para Gobiernos

Marco Regulatorio

- Desarrollar regulaciones específicas para IA y cloud que incluyan requisitos de transparencia
- Establecer estándares mínimos de seguridad para sectores críticos
- Crear incentivos fiscales para inversiones en ciberseguridad avanzada

Inversión Estratégica

- Establecer centros nacionales de ciberseguridad e IA
- Financiar investigación aplicada en protección de infraestructuras críticas
- Desarrollar capacidades de atribución y persecución de ciberdelincuentes

Colaboración Regional

- Implementar mecanismos de intercambio de inteligencia sobre amenazas
- Coordinar respuestas a incidentes transfronterizos
- Armonizar marcos legales para facilitar la cooperación internacional

Desarrollo de Talento

- Crear programas educativos especializados en IA y ciberseguridad
- Establecer alianzas con sector privado para formación práctica
- Retener talento local mediante programas de incentivos

Alianzas Público-Privadas

Colaboración Estratégica

Crear ecosistemas de innovación con participación de gobierno, empresas y academia para desarrollar soluciones adaptadas al contexto regional

Desarrollo de Talento

Mitigar el déficit de 1,3 millones de profesionales en IA/ciberseguridad mediante programas conjuntos de formación y certificación

Innovación Segura

Invertir en startups regionales que desarrollan soluciones específicas para entornos latinoamericanos

Las alianzas entre múltiples actores son esenciales para crear un ecosistema de ciberseguridad resiliente que pueda hacer frente a los desafíos específicos de la región.

GBM CYBERSECURITY CENTER | GBM

Construyendo el Futuro Seguro

La convergencia de IA y nube define la nueva arquitectura digital

Esta transformación trae oportunidades sin precedentes, pero también riesgos significativos que deben gestionarse estratégicamente

El modelo 4D proporciona un marco integral de protección

La combinación de Detección, Defensa, Disuasión y Disrupción crea una postura de seguridad adaptativa y resiliente

LATAM tiene la oportunidad de liderar en ciberseguridad

Con las estrategias adecuadas y la colaboración entre actores clave, la región puede construir un ecosistema digital seguro y confiable

Contacto: [correo@organizacion.com] | [teléfono] | [sitio web]

GBM CYBERSECURITY CENTER | GBM

¿Está nuestra arquitectura preparada para las amenazas que vendrán en los próximos 12 meses?

GBM CYBERSECURITY CENTER | GBM

¡Muchas gracias por su atención!

Ha sido un placer compartir estas estrategias de respuesta efectiva a incidentes de ciberseguridad con ustedes.

Contacto:

📧 Correo electrónico: **laramirez@gbm.net**

📞 WhatsApp: **+506 8827-3344**

🔗 LinkedIn: www.linkedin.com/in/**alonsoramirezcybersecurity**

GBM CYBERSECURITY CENTER | GBM