GBM

# Cybersecurity Center

alonsoramirezcybersecurity laramirez@gbm.net +506 8827-3344

# Bio


*CEH, CHFI, CISM, CRISC, CISA, CDPSE, CRMA, CBCP, ISO27SLI, CLCM, CLPI, CCNA Sec, PSEA, FJSE, NSE3, NSA4011*

Regional Cyber Security Manager en GBM Corporation y Profesor para las escuelas de Ingeniería de Sistemas, Postgrados y Maestrías en cursos de Ciberseguridad y Continuidad de Negocio de las universidades INCAE y CENFOTEC. Es Máster en Auditoría de Tecnologías de Información y Máster en ISO/IEC 27001.

Cuenta con el CNSS 4011 Recognition de la NSA (National Security Agency) donde certifica al profesional en seguridad de redes que tiene el conocimiento para trabajar en sector privado y público en Estados Unidos.

Posee más de 15 años de experiencia en ciberseguridad, es implementador y consultor en servicios tipo SOC y CSIRT. Desarrolla consultorías de prevención y defensa de amenazas cibernéticas avanzadas, así como de identificación de mejoras de seguridad informática corporativa, estrategia y tácticas para el diseño e implementación de arquitecturas de seguridad. Se ha desempañado como Gerente Comercial y de Arquitectura de Seguridad para las soluciones y servicios de IBM y Cisco.

Es asesor externo en materia de protección, privacidad y seguridad de datos corporativos, y es instructor de cursos de certificación de seguridad para PECB, expositor en seminarios y conferencias sobre seguridad de la información dentro y fuera del país.

# TENDENCIAS DE CIBERSEGURIDAD 2023


***Alonso Ramírez,*** *NSA4011, CEH, CHFI, CISM, CRISC, CISA, CDPSE, CRMA, CBCP, ISO27SLI, CLCM, CLPI, CCNA Sec, PSEA, FJSE, NSE3*

***Regional Cyber Security Manager***

***GBM Corporation***

# Mayor inversión en ciberseguridad

### Digitalización

Ciberseguridad, es el sector que se lleva la mayor inversión.

### Nube

Servicios y soluciones en la nube serán usadas por las medianas y grandes empresas a mayor escala.

### Entorno Digital

Aumentando el número de operaciones.

### Modernización de Aplicaciones

Competitividad de las compañías en la nube y la ciberseguridad aumenta.

# Actitud de seguridad para IoT

- En 2023, **43.000 millones** de dispositivos conectados al IoT en el mundo. Fuente: Gartner.
- Punto ciego de seguridad como puertas de entrada para acceder a otros dispositivos en red con datos sensibles.
- Legislación para la protección de los consumidores usuarios del IoT.

# Seguridad para el trabajo en casa

En 2023, los trabajadores son más propensos que nunca a utilizar dispositivos personales para conectarse de forma remota a las redes de trabajo.

Surge un nuevo conjunto de desafíos.

y a distancia

# Derechos de privacidad

## para los consumidores

2023, año de la mayor cantidad de medidas regulatorias para los derechos de privacidad de los consumidores.

El resguardo de información en Data Centers con altos estándares de seguridad para evitar vulnerabilidades será primordial para las empresas.

En 2023,

# +70

países.

# Daños colaterales en procesos electorales

Elecciones gubernamentales, acontecimientos que suelen ser objeto de ataques por parte de intereses extranjeros hostiles. Las empresas y las organizaciones no gubernamentales se encuentren en el punto de mira de los *estados-nación*.


# Ransomware y la ley de Ciberseguridad

- El Ransomware continua ocasionado pérdidas multimillonarias a diversas empresas alrededor del mundo.
- Para el año 2025 el 30% de los estados y empresas del país deberán tener establecida una legislación ante estos ciberataques.
- En 2023 los países comensarán a crear legislación sobre ciberseguridad.

# Inteligencia Artificial

Las empresas que utilizan la IA y la automatización para detectar y responder a las brechas de datos ahorran una media de 3 millones de dólares en comparación con las que no lo hacen.

Fuente: IBM.

## en ambos bandos

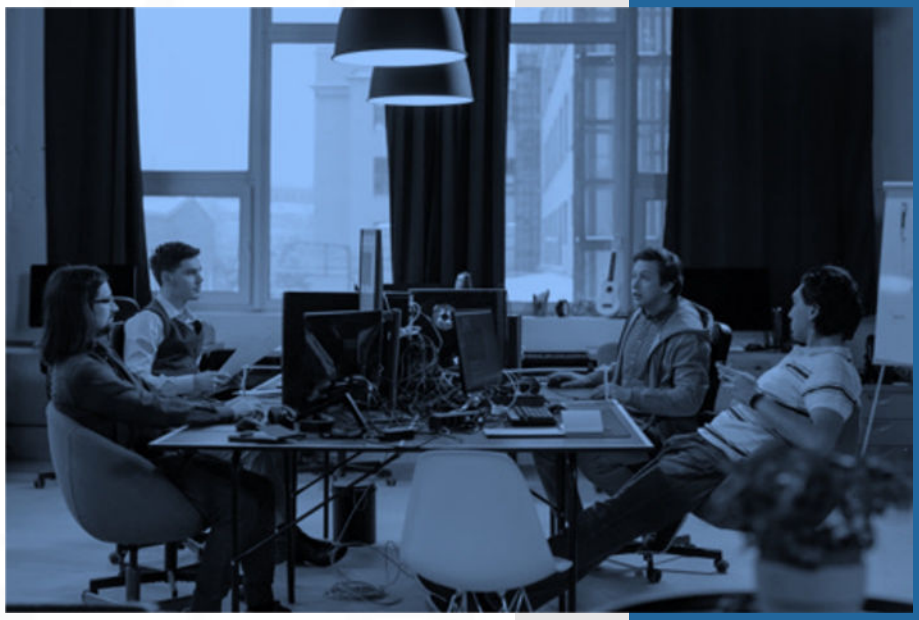
En 2023, más delincuentes usarán los algoritmos de IA para identificar sistemas con una seguridad débil.

Para 2030 el mercado de productos de ciberseguridad con IA tendrá un valor cercano a los 139.000 millones de dólares, lo que supone un aumento de casi diez veces el valor del mercado de 2021.

# Fuerzas de tareas para la seguridad de la nube

El **35 %** de las organizaciones tienen más del **50 %** de sus cargas de trabajo en la nube y desarrollan nuevas aplicaciones a alta velocidad.

En 2023, las organizaciones van a utilizar equipos de trabajo especiales con habilidades y soluciones en la prevención avanzada de amenazas para todos los activos en la nube.



# 70%

C-Level con enfoque resilente.
Fuente: Gartner.

## Resiliencia organizacional

En 2023, C-Level tendra una mejor cultura de resiliencia que les permita surfear la ola de posibles amenazas.

El 70% de estos ejecutivos implementan soluciones resilientes ante eventos adversos al negocio de sus compañías.

# FAQ'S

# Muchas gracias

laramirez@gbm.net

W: +506 8827-3344

# Cyber Security Services

Portfolio

## Managed Detection & Response

Benefíciese de la visibilidad completa de las amenazas, la búsqueda proactiva de amenazas y la detección y respuesta unificadas de amenazas para sus entornos de TI, nube, puntos finales, OT/ICS.

## Managed Vulnerability Scanning

Reduzca su exposición al riesgo con un servicio de análisis de vulnerabilidades administrado que identifica y prioriza las vulnerabilidades en todos los tipos de infraestructura de TI, servicios y aplicaciones web.

## Incident Response 24/7

En caso de una brecha de seguridad, obtenga soporte garantizado para contener rápidamente el incidente, mitigar el riesgo y construir una estrategia más ofensiva contra las amenazas.

GDM Cybersecurity Center

## Security Device Management

Obtenga acceso a analistas altamente calificados en nuestro ***Cybersecurity Center*** las 24 horas del día, los 7 días de la semana para monitorear, configurar, aplicar parches y actualizar la seguridad en todos los dispositivos.

## Red Team Operations

Conozca su susceptibilidad a un ataque cibernético de manera integral en todas las áreas de la organización, para determinar cómo un actor malicioso puede abusar y explotar vulnerabilidades y puntos ciegos en su seguridad.

## Cybersecurity Assessment

Para proteger con éxito a su organización contra las amenazas cibernéticas, es imperativo comenzar por identificar dónde se encuentran sus debilidades de seguridad.

GDM