LocKNet

# CONSULTORES EN CIBERSEGURIDAD



# NUESTROS SERVICIOS

- Aseguramiento perimetral.
- Servicios de Red Team.
- Análisis de vulnerabilidades, Hacking Ético.
- Centro de operaciones de seguridad y de red (SOC-NOC).
- Asesorías en la implementación de estrategias de seguridad de la información y de Ciberseguridad.
- Aseguramiento de infraestructura tecnológica.
- Asesorías en la implementación de sistemas de gestión. (ISO27001, ISO22301, ISO9000), BCP, DRP, ITIL y COBIT. Gestión de riesgos bajo ISO31000.
- WPT (Web Penetration Testing).
- Informática forense.
- Aseguramiento de ingresos ISOC.
- Documentos legales asociados a la seguridad de la información.



# FORTALEZAS

## INGENIEROS CERTIFICADOS EN:

- ☑ Especialistas y Magisters en Seguridad de la Información
- ☑ CISSP
- ☑ CISM, CISA, CRISK
- ☑ CEH, eWPT, CHFI, RHCE, RHCSA
- ☑ PECB Certified Trainer
- ☑ PECB ISO/IEC 27032 Lead Cybersecurity Manager
- ☑ PECB ISO/IEC 27001 Lead Implementer
- ☑ PECB ISO 22301 Lead Implementer
- ☑ PECB ISO 31000 Lead Risk Manager
- ☑ Auditores líder e interno ISO 27001 e ISO 22301
- ☑ ITIL y COBIT
- ☑ Certificación IPv6

**14**
AÑOS
DE EXPERIENCIA

# NUESTROS SERVICIOS

## 1
Entendimiento de la organización para la correcta gestión del riesgo en Ciberseguridad.

- ISO31000
- Gestión de riesgos de la información
- Análisis de vulnerabilidades
- Hacking ético
- Web Penetration Testing
- Pruebas de carga

## 2
Implementación de medidas de aseguramiento que protejan la información corporativa.

- UTM / Firewalls
- Seguridad perimetral
- Seguridad en redes y dispositivos
- Seguridad WEB
- Seguridad de acceso
- Conciencia y entrenamiento
- Procesos proactivos

## 3
Identificar la ocurrencia de eventos de Ciberseguridad.

- Monitoreo continuo
- SOC (Centro de operaciones de Seguridad)
- NOC (Centro de operaciones de Red)
- Administración delegada
- Revisión de código seguro

## 4
Implementar las actividades apropiadas ante la ocurrencia de un evento de Ciberseguridad.

- Gestión de incidentes
- Información Forense
- Evaluaciones e inteligencia
- Procesos reactivos
- Conciencia y entrenamiento continuo
- Gestión de Backups

## 5
Recuperación y resiliencia de los servicios corporativos afectados en un evento de Ciberseguridad.

- Continuidad del negocio y plan de crisis
- BCP (Plan de Continuidad del Negocio)
- BIA (Análisis de Impacto del Negocio)
- DRP (Plan de Recuperación de Desastres)
- ISO 22301
- ISO 31000




LocKNet

# IDENTIFICACIÓN

1

Entendimiento de la organización para la correcta gestión del riesgo en Ciberseguridad.

- ISO31000
- Gestión de riesgos de la información
- Análisis de vulnerabilidades
- Hacking ético
- Web Penetration Testing
- Pruebas de carga



# FIREWALLS
## (UNIFIED THREAT MANAGEMENT)(HUAWEI)

Venta, instalación y configuración de firewalls.

Las redes empresariales están evolucionando hacia redes de próxima generación que cuentan con banda ancha móvil, Big data, redes sociales y servicios en la nube, aplicaciones móviles, Web 2.0 y redes sociales.

La serie HUAWEI Secospace USG6000 (Unified Security Gateway) está diseñada para abordar estos desafíos de Carrier, grandes, medianas, pequeñas empresas y centros de datos de nueva generación.

La familia de Firewalls de nueva generación (NGFW) de Huawei USG 6000 ofrece la cobertura más completa, el control más preciso, siendo los número 1 en la industria con la identificación de más de 6000 aplicaciones.

HUAWEI











# HACKING ÉTICO

**Locknet** ejecuta servicios de hacking ético técnico siguiendo la línea tradicional ofensiva, que simula la conducta de los cibercriminales para evaluar la posición de defensa de las infraestructuras computacionales del cliente.

Adicionamos componentes de ejercicios modernos de Red Team.

Se mapean las amenazas sobre los hallazgos de la ejecución de herramientas especializadas y potenciales tácticas y técnicas de ataques vigentes para el nicho particular del cliente.

Se obtienen resultados más precisos del nivel particular de exposición de cada objetivo.

# RED TEAM SERVICES

Este enfoque moderno de hacking ético entrega resultados muchos más reales de la posición de defensa de la organización en contexto con la actividad vigente ciber criminal.

- Procesos holísticos de tipo ofensivo que cubren todas las variables que contempla un ciber delincuente real.
- Se soportan en las bases de datos mundiales de ataques ocurridos, seleccionando los del mismo nicho de negocio y replicándolos en una actividad denominada campaña.
- Una campaña involucra actividades ofensivas que cubren desde el plano físico, ingeniería social, hasta el plano técnico, destacándose el uso de dispositivos especializados de intrusión (bad usb, rogué AP, surveillance devices, etc.)



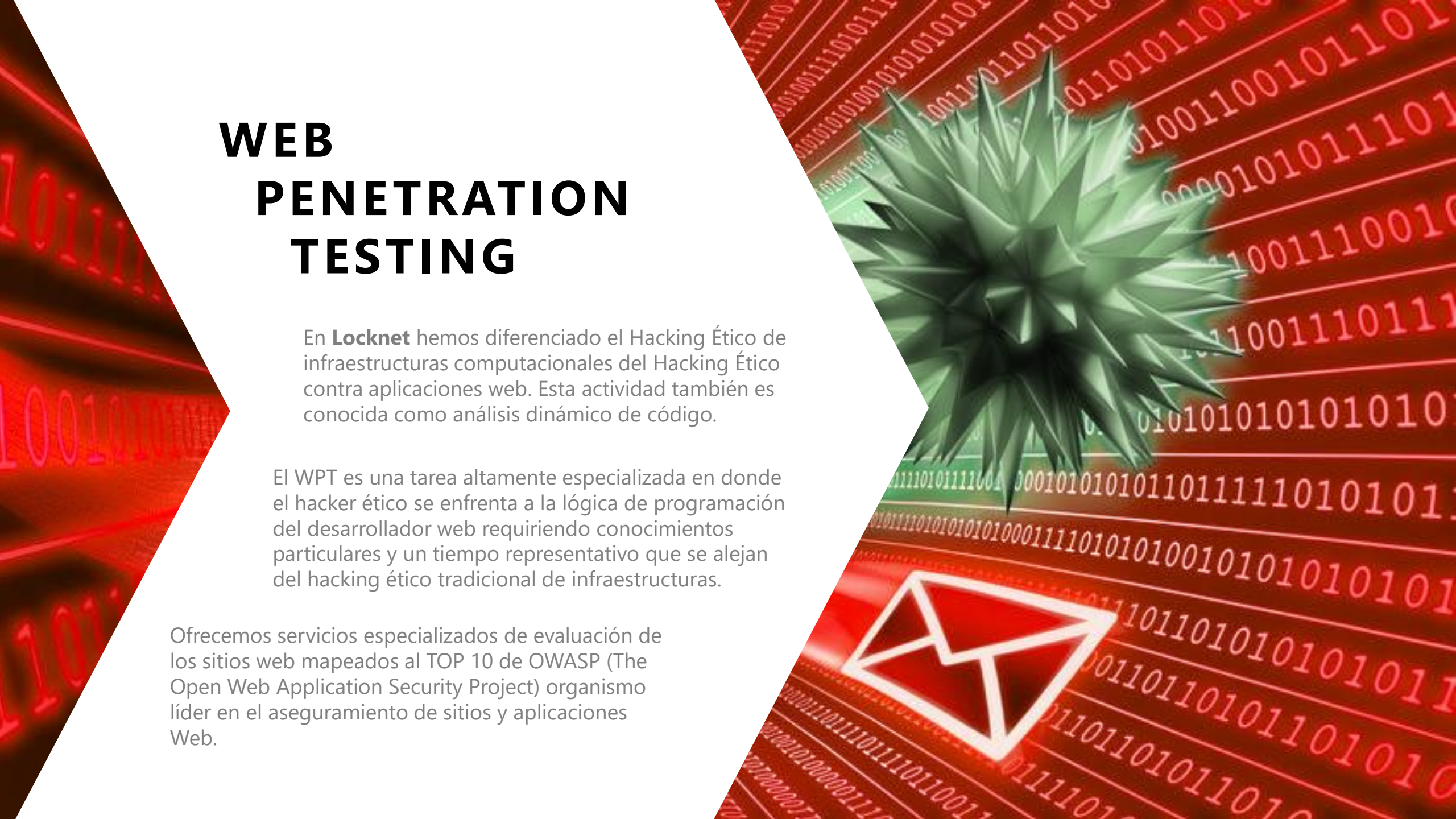


# WEB PENETRATION TESTING

En **Locknet** hemos diferenciado el Hacking Ético de infraestructuras computacionales del Hacking Ético contra aplicaciones web. Esta actividad también es conocida como análisis dinámico de código.

El WPT es una tarea altamente especializada en donde el hacker ético se enfrenta a la lógica de programación del desarrollador web requiriendo conocimientos particulares y un tiempo representativo que se alejan del hacking ético tradicional de infraestructuras.

Ofrecemos servicios especializados de evaluación de los sitios web mapeados al TOP 10 de OWASP (The Open Web Application Security Project) organismo líder en el aseguramiento de sitios y aplicaciones Web.

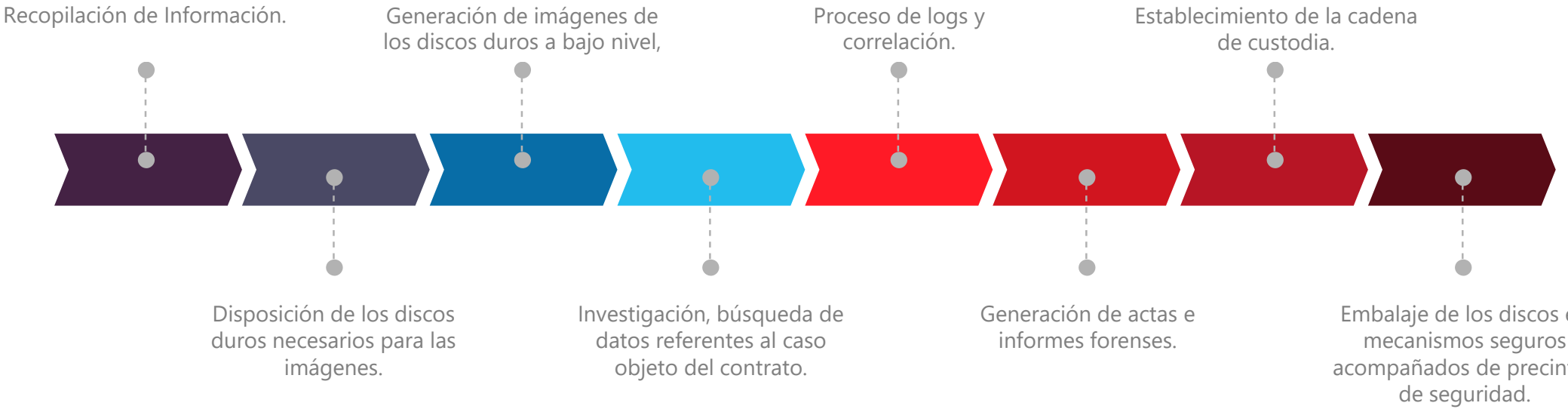


# INFORMÁTICA FORENSE



**Locknet** como compañía experta en ciberseguridad, cuenta con un servicio informático forense que ofrece la experiencia y conocimiento de profesionales altamente calificados y certificados.

Aplicamos técnicas científicas y analíticas en infraestructuras tecnológicas que permiten identificar, preservar, analizar y presentar datos y/o evidencia que puedan ser vitales en un proceso legal o no legal, relacionado al esclarecimiento de unos hechos sobre un entorno informático.



# CONSULTORÍAS METODOLÓGICAS EN ISO 27001, 22301 y 27032.

- **Locknet** cuenta con consultores certificados y experimentados en diagnóstico, auditorías e implementación de Sistemas de Gestión de Seguridad de la Información (SGSI) basados en la Norma ISO 27001.

- Nuestros ingenieros están certificados para realizar consultorías en relación a las normas ISO 22301 específicamente en “Planes de Continuidad del Negocio (BCP)” y “Planes de Recuperación de Desastres (DRP)” de nuestros clientes.

- Nuestras consultorías cubren la moderna adopción de sistemas de gestión de Ciberseguridad que complementan los ya existentes SGSI ISO 27001 de las organizaciones, para esto se utilizan como referentes las Normas ISO 27032 (Guidelines For Cybersecurity) y NIST Cybersecurity Framework.



# CENTRO DE SEGURIDAD Y VIGILANCIA DIGITAL SOC

Es un lugar central donde los servicios críticos de la organización son monitoreados, analizados y protegidos frente a riesgos y ciberataques.



**CSVD LOCKNET**



LocKNet

## OBJETIVOS:

**PRINCIPAL:**

Reducir y mitigar riesgos mejorando la visibilidad, el control y la seguridad.

**SECUNDARIOS:**

Cumplimiento, control de fraude interno/externo, inteligencia operativa y de negocio.

## COMPONENTES:

Plataforma tecnológica

- **Servicio de Monitoreo** — Prevención, detección, respuesta a incidentes de seguridad y *contención automática*
- **Servicio de Soporte** — Actualización y mantenimiento de la infraestructura soportada.
- **Servicios Profesionales** — Nuevas integraciones o desarrollos solicitados de acuerdo a las GB contratadas

*Las acciones de contención automáticas, se realizan con el modelo de conocimiento SIEM.

# INCUBADORA DE SERVICIOS EN CIBERSEGURIDAD

***NUEVAS ESTRATEGIAS EVOLUCIONADAS E INNOVADORAS***

El panorama de CIBER **IN**SEGURIDAD con corte a agosto de 2019 es preocupante y la sociedad esta siendo atropellada por la delincuencia informática, secuestro informático de ciudades de países desarrollados (Baltimore, Riviera Beach y Lake City en US), robo electrónico de millones de dólares a los bancos (Robo de US$ 10M al Banco de Chile), robo de información de millones de ciudadanos a empresas privadas y de gobierno (Hotel Marriot, Equifax, etc.).



**ISOC**

Aplicación de SOC al aseguramiento de ingresos. Se pretende monitorear procesos de negocio involucrando correlación de eventos que permitan generar alerta sobre comportamientos anómalos o posible fraude.



**CIBERDEFENSA CON MITRE ATT&CK**

Framework con mapa de actuales tácticas, técnicas y procedimientos que están utilizando los adversarios o ciber delincuentes para perpetrar sus violaciones, incluye la identificación de grupos particulares de atacantes o adversarios, su nicho y técnicas preferidas de ataque.

**Locknet** ofrece un servicio de evaluación de la posición actual real de defensa de las organizaciones, utilizando herramientas que de forma precisa y rápida permiten mapear las defensas contra las TTP (tactics, techniques or procedures) del nicho de negocio del cliente.



**BUG BOUNTY**

Son plataformas de revisión de vulnerabilidades por parte de grupos élites de hackers éticos que trabajan en una modalidad de recompensa por vulnerabilidad descubierta.

**Locknet** ofrece el servicio de administración e intermediación de servicios continuos de evaluación de tipo “Bug Bounty” surtiendo el rol de receptores de las potenciales vulnerabilidades, evaluadores a través de Triage de la veracidad y pertinencia de los reportes de vulnerabilidades y administradores de las campañas de Bug Bounty.

# ALIANZAS

Huawei Enterprise
Channel Partner Program

HUAWEI
Enterprise Partner
Service

Certified Service Partner
Enterprise Networking

mitnicksecurity.com
Kevin Mitnick and the Global Ghost Team™

LocKNet – EC
Ecuador

Somos el único Gold Channel CSP 4 Estrellas en Seguridad Huawei en la región.
Único canal experto en UTM's Huawei en la región.
Ingenieros certificados en: HCNA Security, HCNA Routing & Switching, HCNP Security, HCNA Wlan.
Más de 30 UTM's vendidos e instalados en la región.

# CLIENTES LOCKNET















































































