Seguridad & Gestión
Tecnologías de la Información

RESILIENCIA DIGITAL EN LA ERA DE LA IA CUANTICA



CIBERSEGURIDAD GESTIONADA COMO UN SERVICIO - CSMaaS

Seguridad & Gestión
Tecnología de la Información

Habilitador del Negocio

- Fusiones/ Adquisiciones
  - Gestión de Riesgos de Adquisición
  - Costos de Integración
  - Gestión de Identidades
- Computación en la nube
  - Arquitectura en la nube.
  - Estrategia y directrices
  - Evaluación de riesgos en nube.
  - Cumplimiento
  - Responsabilidad/Responsabilidad Legal/ Incidentes
  - Estrategia SaaS
  - Integración de Logs
  - Seguridad de Dispositivos Virtualizados
- Tecnologías Móviles
  - Políticas
  - Tecnologías
  - Dispositivos perdidos / robados
  - BYOD (Aseguramiento de dispositivos personales – VDI)
  - Inventario de aplicaciones móviles

Procesos

- HR incorporación/ Desvinculación
- Relaciones de negocio con terceros.

Venta de Seguridad de la Información (Interna)

- Alineación con objetivos corporativos
- Gestión continua de actualizaciones
- Innovación y creación de valor.

Gobernabilidad

- Estrategia y alineación de negocio
- Marco de gestión riesgos.
- Gestión de recursos.
- Roles and Responsabilidades
- Métricas e informes
- Implementación de normatividad mínima para protección del Dato: ISO 27001, ISO 27701, ISO 22301 E ISO 42001.

Operaciones de Seguridad

Prevención de amenazas

- Network / Firewall de aplicaciones.
- Gestión de Vulnerabilidades
- Seguridad en aplicaciones
- IPS
- Gestión de identidades
- Políticas de Seguridad de la Información
- DLP
- Anti Malware, Anti-spam
- Proxy/Filtrado de Contenido
- Parcheo
- Protección DDoS
- Guías de Hardening
- Encripción SSL
- PKI

Detección de amenazas

- Análisis de Logs/correlación/SIEM
- Alertamiento (IDS/IPS, FIM, WAF, Antivirus, etc)
- Análisis de Netflow
- DLP
- Cacería de amenazas
- Integración MSSP
- Operaciones SOC
- Criptografía post-cuántica y blindaje de datos críticos.

Gestión de Incidentes

- Respuesta a Incidentes
- Relaciones con los medios
- Preparación para Incidentes
- Investigación Forense
- Preparación ante filtraciones de datos
- Gestión de Continuidad de Negocios



Ciclo de vida de la entrega de Proyectos

- Requerimientos
- Diseño
- Pruebas de Seguridad
- Certificaciones y acreditaciones.

Gestión de Identidades

- Gestión de credenciales
- Creación/Borrado Cuentas
- Single Sign On (SSO Simplified Sing On)
- Repositorios (LDAP/Active Directory)
- Federación
- 2-Factor Autenticación
- Control de Acceso basado en roles
- Comercio electrónico y aplicaciones móviles
- Password resets/Self service
- Integración con procesos de recursos humanos
- Integración de identidades basadas en la nube

Presupuesto

- Proyectos de Seguridad
- Desarrollo de casos de negocio
- ROSI – Motor con IA de cuantificación Riesgo Cibernético - CRQ
- Alineación con Proyectos de IT.
- Empleados de tiempo completo y contratistas
- Equilibrio del presupuesto para personal, capacitación y herramientas/Tecnología

Arquitectura de Seguridad

- Segmentación de redes
- Protección de aplicaciones – APP Runtime
- Protección de Código Fuente. Agentic Runtime
- Defensa en profundidad
- Acceso remoto
- Tecnologías de Encripción
- Backup/Replicación/Múltiples Sitios
- Cloud/Hybrid/Múltiples Proveedores de Nube

Cumplimiento y Auditorias

- PCI
- SOX
- HIPAA
- Auditorías periódicas
- SSAE 16
- Otras necesidades de cumplimiento

Asuntos Legales y Recursos Humanos

- Descubrimiento de datos
- Contratos con Proveedores
- Investigación / Informática Forense
- Integración en los procesos de gestión de identidades - IDM

Gestión de Riesgos

- Gestión de vulnerabilidades y remediación.
- Evaluación continua de riesgos/Gestión de accesos privilegiados
- Integración en la entrega de proyectos (PMD)
- Revisiones de Código
- Metodología de Evaluación de Riesgos
- Políticas y Procedimientos
- Concienciación de los colaboradores.
- Enfoque centrado en los Datos (Descubrimiento, clasificación y auditoría de datos sensibles cloud y local con IA).
- Tecnología IoT
- Tecnologías de Operación
- Seguridad Física
- Monitoreo Continuo y Cuantitativo de Terceros

Source: http://rafeeqrehman.com/2015/05/17/the-latest-2015-ciso-mindmap-is-here/

CIBERRESILIENCIA COMO UN SERVICIO - CRaaS

Seguridad & Gestión
Tecnologías de la Información

Mantenga su operación cuando ocurre lo inesperado. **Ayudamos a las organizaciones a anticipar, resistir, responder y recuperarse de ciberataques, interrupciones tecnológicas y crisis operacionales.**

CAPACIDADES ESTRATÉGICAS QUE IMPLEMENTAMOS

Gobierno y Resiliencia
- Estrategia y Gobierno
- Gestión de Riesgos
- Indicadores Ejecutivos

Gestión de Crisis
- War Room
- Gestión de Incidentes
- Comunicación Ejecutiva

Continuidad del Negocio
- BIA y BCP
- Procesos Críticos
- Continuidad Operacional

Recuperación Tecnológica
- DRP
- Clean Room
- Sitio Alterno

Ejercicios y Simulaciones
- Tabletop Exercises
- Simulacros de Crisis
- Pruebas de Recuperación

CICLO DE CIBERRESILIENCIA

🔍 **ANTICIPAR**
↓
🛡 **RESISTIR**
↓
🚨 **RESPONDER**
↓
♻ **RECUPERAR**
↓
📈 **EVOLUCIONAR**

NUESTRO FACTOR DIFERENCIAL

- *Evitamos Puntos Únicos de Falla (PUF) en gente, procesos y tecnología especialmente en tecnologías de Correo electrónico como office 365 y Gmail.*
- *Plataformas robustas de bajo costo en su plataforma tecnológica de recuperación de desastres para reducir altos costos de licenciamiento.*
- *Ofrecemos* ***CROaaS Oficial de Ciberresiliencia como un servicio*****.**

BENEFICIOS

- ✅ Continuidad de servicios críticos
- ✅ Menor impacto financiero y reputacional
- ✅ Recuperación rápida y controlada
- ✅ Cumplimiento normativo
- ✅ Mayor confianza institucional

FIN

Aseguramiento de dispositivos personales (VDI)

Objetivo:

Permitir trabajo remoto seguro mediante escritorios virtuales que aíslan la información corporativa de los dispositivos personales.

Servicios incluidos:

- Virtual Desktop Infrastructure (VDI)
- BYOD Seguro
- Gestión de dispositivos
- Protección de datos corporativos
- Acceso Zero Trust
- MFA y SSO

Beneficio principal: Reducir el riesgo de fuga de información desde computadores personales.

Seguridad en Aplicaciones

Objetivo:

Protección de aplicaciones durante todo el ciclo de vida de desarrollo y operación.

Servicios incluidos:

- SAST
- DAST
- Pentesting
- DevSecOps
- Seguridad API
- Gestión de vulnerabilidades

Beneficio principal: Disminuir riesgos de explotación de aplicaciones críticas.

Criptografía Post-Cuántica y Blindaje de Datos Críticos

Objetivo:

Preparar a las organizaciones para el impacto de la computación cuántica sobre los mecanismos criptográficos actuales.

Servicios incluidos:

- Inventario criptográfico
- Crypto Agility
- PQC Readiness Assessment
- Protección de información crítica
- Estrategia de transición NIST

Beneficio principal: Proteger información sensible frente a amenazas futuras.

.

Motor con IA de Cuantificación de Riesgo Cibernético (CRQ)

Objetivo:

Traducir el riesgo técnico a impacto financiero entendible para la alta dirección.

Servicios incluidos:

- Cyber Risk Quantification
- Análisis FAIR
- ROSI
- Simulación de pérdidas
- Dashboards ejecutivos
- Priorización de inversiones

Beneficio principal: Tomar decisiones de seguridad basadas en impacto económico.

.

APP Runtime Protection

Objetivo:

Proteger aplicaciones en ejecución contra ataques y comportamientos anómalos.

Servicios incluidos:

- Runtime Application Self Protection (RASP)
- Detección de explotación
- Protección API
- Observabilidad de aplicaciones
- Integración SOC

Beneficio principal: Detectar amenazas que no son visibles mediante controles tradicionales.

.

Protección de Código Fuente y Agentic Runtime

Objetivo:

Asegurar el desarrollo de software y proteger entornos impulsados por IA Agéntica.

Servicios incluidos:

- Code Security
- Secret Scanning
- SBOM (Software Bill of Materials)
- Protección de modelos IA
- AI Runtime Security
- AI Agents Governance

Beneficio principal: Evitar manipulación del código o de agentes inteligentes en producción.

.

Gestión de Vulnerabilidades y Remediación

Objetivo:

Identificar, priorizar y corregir vulnerabilidades de manera continua.

Servicios incluidos:

- Vulnerability Assessment
- Scanning continuo
- Priorización basada en riesgo
- Gestión de remediación
- Reporting ejecutivo

Beneficio principal: Reducir superficie de ataque y probabilidad de incidentes.

.

Descubrimiento, Clasificación y Auditoría de Datos Sensibles con IA

Objetivo:

Localizar y proteger información sensible en ambientes locales y cloud.

Servicios incluidos:

- DSPM
- DLP
- Descubrimiento de datos
- Clasificación automática
- Data Governance
- Protección de datos personales

Beneficio principal: Controlar dónde se encuentra la información crítica y quién accede a ella.

Monitoreo Continuo y Cuantitativo de Terceros

Objetivo:

Evaluar continuamente el riesgo de proveedores y terceros.

Servicios incluidos:

- Third Party Risk Management
- Security Rating
- Riesgo de cadena de suministro
- Monitoreo continuo
- Cuantificación de exposición

Beneficio principal: Reducir riesgos provenientes de proveedores críticos.

LAS CUATRO CERTIFICACIONES CLAVE
PARA LA CONFIANZA DIGITAL Y LA RESILIENCIA ORGANIZACIONAL

Seguridad de la información • Privacidad de los datos • Uso responsable de la IA • Continuidad del negocio

PROTEGE LA INFORMACIÓN

Establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI) eficaz, que garantice la confidencialidad, integridad y disponibilidad de la información.

ISO 27001
SEGURIDAD DE LA INFORMACIÓN

PROTEGE LOS DATOS PERSONALES

Extiende ISO 27001 para la gestión de la privacidad de la información personal (PII) en todo su ciclo de vida, fomentando el cumplimiento normativo y el respeto por los derechos de las personas.

ISO 27701
PRIVACIDAD DE LA INFORMACIÓN

CONFIANZA DIGITAL Y RESILIENCIA ORGANIZACIONAL

PERSONAS | DATOS
SERVICIOS | FUTURO

GARANTIZA UNA IA RESPONSABLE Y CONFIABLE

Establece un sistema de gestión para la IA que promueve un desarrollo y uso ético, transparente y confiable, minimizando riesgos y generando valor para la sociedad.

ISO 42001
GESTIÓN DE LA IA RESPONSABLE

GARANTIZA LA CONTINUIDAD DE LOS SERVICIOS CRÍTICOS

Establece los requisitos para un Sistema de Gestión de Continuidad del Negocio (SGCN) que permite responder, recuperar y continuar las operaciones ante incidentes disruptivos, fortaleciendo la resiliencia organizacional.

ISO 22301
CONTINUIDAD DEL NEGOCIO

PERSONAS MÁS SEGURAS
DATOS MÁS PROTEGIDOS
SERVICIOS MÁS RESILIENTES
UN FUTURO MÁS CONFIABLE

INTEGRADAS, SE COMPLEMENTAN.
JUNTAS GARANTIZAN SEGURIDAD, PRIVACIDAD, IA RESPONSABLE Y CONTINUIDAD DEL NEGOCIO.

Seguridad & Gestión
Tecnologías de la Información

Más que certificaciones, **un compromiso con la sociedad.**

Seguridad & Gestión
Tecnologías de la Información

PACKETLIGHT DWDM

Transporte óptico carrier-grade en 1U. Desde 10G hasta 8T sobre la fibra que ya tienes.

PacketLight Networks · Fabricante especializado en DWDM y OTN sobre fibra oscura y redes WDM. Miembro del RAD Group. 25+ años construyendo equipamiento óptico para carriers, datacenters, utilities y redes críticas.

Portfolio completo de transponders, muxponders, ROADM, amplificación, monitorización y cifrado Layer-1 — todo en chasis 1U con arquitectura pay-as-you-grow. Cifrado GCM-AES-256 embebido sin degradación. LightWatch NMS incluido.

Solicitar sesión técnica →

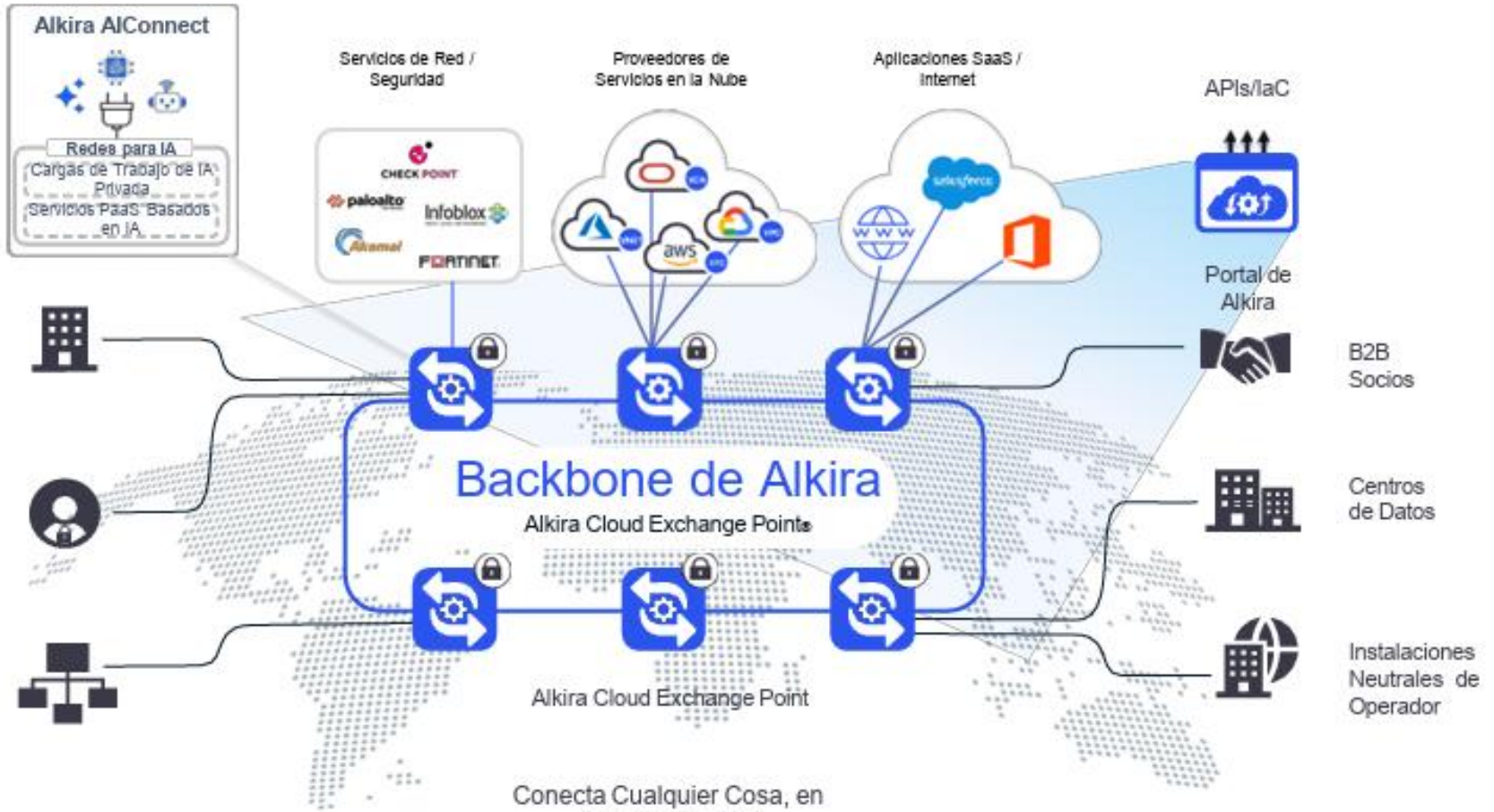
Ver portfolio completo ↓

FABRICANTE	PacketLight Networks · Miembro del RAD Group
CATEGORÍA	DWDM / OTN · Equipamiento óptico carrier-grade
FACTOR DE FORMA	1U · 19" · ETSI · 23" rack
CAPACIDAD	10G a 8T por chasis
ALCANCE	Metro · Long Haul · Ultra Long Haul (hasta 4.000 km)
CIFRADO	Layer-1 GCM-AES-256 embebido (opcional toda la gama)
CERTIFICACIONES	ITU-T G.694.1 · G.709 OTN · OpenROADM · OpenZR+ · FIPS 140-2/3 · CC EAL2
EXPERIENCIA	Fundada en 2000 · Miembro RAD Group

Seguridad & Gestión
Tecnologías de la Información

Alkira: Infraestructura de Red bajo Demanda

- ✓ Sin Hardware
- ✓ Sin Agentes
- ✓ Como Servicio



Conecta Cualquier Cosa, en Cualquier Lugar

Alkira © 2026. Todos los derechos reservados

Seguridad & Gestión
Tecnologías de la Información

