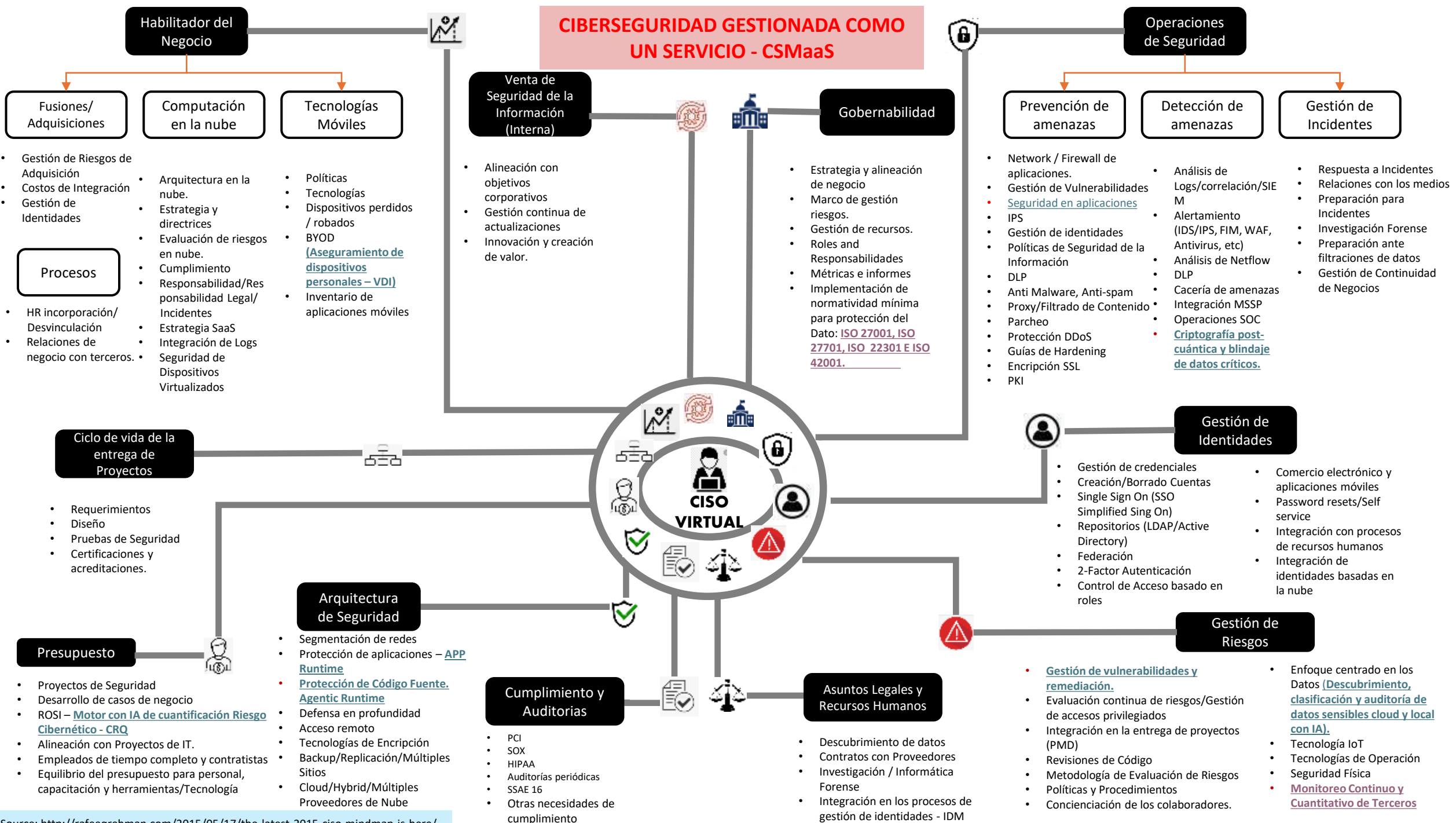


CIBERSEGURIDAD GESTIONADA COMO UN SERVICIO - CSMAaaS



CIBERRESILIENCIA COMO UN SERVICIO - CRaaS

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



BENEFICIOS

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

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 **CRaaS Oficial de Ciberresiliencia como un servicio.**

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.



LA TRIADA DE CERTIFICACIÓN CLAVE HOY EN DÍA PARA LA PROTECCIÓN DEL DATO

Privacidad de la información • Seguridad de la información • Confianza en la IA



**ISO
27701**

PRIVACIDAD DE LA INFORMACIÓN

Extiende ISO 27001 para la gestión de la privacidad de la información personal (PII) en todo su ciclo de vida.



**ISO
42001**

GESTIÓN DE LA IA RESPONSABLE

Establece un sistema de gestión para la IA que promueve un desarrollo y uso ético, transparente y confiable.



**ISO
27001**

SEGURIDAD DE LA INFORMACIÓN

Establece los requisitos para un sistema de gestión de seguridad de la información (SGSI) robusto y efectivo.



INTEGRADAS, SE COMPLEMENTAN. JUNTAS, PROTEGEN LO QUE MÁS IMPORTA:
LOS DATOS, LAS PERSONAS Y LA CONFIANZA.