

CLARO EMPRESAS · SCITUM

CIBERSEGURIDAD PARA EMPRESAS

Protegiendo la continuidad del negocio en un mundo cada vez más expuesto.

Arturo Riveros · Ejecutivo de Soluciones Corporativas — Claro Empresas

WhatsApp +595 994 384 508



Ya no se trata de si ocurrirá sino de cuándo



La digitalización aceleró los negocios.

También aceleró los riesgos.



Cualquier empresa puede ser objetivo.

No importa su tamaño ni su rubro.



Ataques dirigidos todos los días.

A empresas, gobiernos y personas.

Paraguay **no está exento**



7,4 millones de registros de ciudadanos paraguayos filtrados en la dark web

Filtración masiva de datos — Resecurity / Security Affairs, 2025



Ciberspionaje atribuido a China (grupo Flax Typhoon) infiltró sistemas del Estado

Comunicado EE.UU.—Paraguay; Fiscalía abrió causa penal — ABC Color / Infobae, jul. 2026



El Banco Central alertó por fraudes: “no otorga préstamos ni pide contraseñas ni datos”

Alertas de phishing del BCP — RDN / Última Hora, 2026



“Crecen los ataques cibernéticos en Paraguay”; el robo de credenciales, principal vía contra empresas

Paraguay.com / Kaspersky, 2026

¿Qué ocurre si una empresa es víctima de un ataque?



Pérdida de dinero



Interrupción de operaciones



Robo de información sensible



Secuestro de datos
(ransomware)



Impacto reputacional



Pérdida de confianza de
clientes



Sanciones regulatorias



En la mayoría de los casos, **el costo de recuperación es muy superior al costo de prevención.**

ENFOQUE

La ciberseguridad es parte de la continuidad del negocio

No hablamos solamente de tecnología.
Hablamos de proteger lo que sostiene a la organización.



Personas



Información



Operaciones



Clientes



Ingresos



Reputación

LA ALIANZA

Claro Empresas + Scitum

Una alianza para proteger organizaciones. Scitum es una de las empresas líderes de ciberseguridad en América Latina.

24/7

Centro de Operaciones de Seguridad (SOC) monitoreando de forma continua, todos los días del año.



SOC 24x7



Monitoreo continuo



Prevención de amenazas



Detección y respuesta



Servicios administrados de seguridad



Protección de infraestructura crítica

Un modelo de madurez en tres etapas

01



IDENTIFICAR

AVN

Análisis de Vulnerabilidades

02



PROTEGER

SPA

Seguridad Perimetral Administrada

03



DETECTAR Y RESPONDER

SOC + EPDR

Operación y respuesta 24x7

Conocer → Blindar → Vigilar y responder. Cada etapa eleva la madurez de seguridad de la organización.

IDENTIFICAR

AVN

Análisis de Vulnerabilidades

Identifica, clasifica y prioriza las vulnerabilidades de la infraestructura tecnológica antes de que un atacante las aproveche.



“No se puede proteger lo que no se conoce.”

BENEFICIOS



Detectar riesgos antes de que sean explotados



Identificar los puntos débiles de la organización



Priorizar las acciones correctivas



Mejorar la postura de seguridad



Validar las tareas de remediación

MODALIDADES

Externo

Interno

Con credenciales

Sin credenciales

PROTEGER

SPA

Seguridad Perimetral Administrada

Servicio administrado que protege el perímetro de la red corporativa: controla la información que entra y sale de la organización.



Su primera línea de defensa ante amenazas externas.

ADMINISTRACIÓN Y OPERACIÓN



Administración especializada y SOC dedicado



Monitoreo 24x7 y alertamiento de eventos



Cambios administrados y atención remota

INCLUYE

Firewall NG

VPN

IPS

Web Filter

Antivirus

Antispam

SD-WAN

DETECTAR Y RESPONDER

SOC + EPDR

Centro de Operaciones de Seguridad. Servicio administrado que protege servidores, notebooks, PCs y dispositivos corporativos.



24x7x365

Operación permanente: prevención, detección, monitoreo, respuesta y contención de amenazas.

FUNCIONES



Prevención



Detección



Monitoreo



Respuesta



Contención



Análisis de amenazas

Protección contra malware y ransomware · visibilidad total de eventos · respuesta especializada.

¿Qué obtiene su empresa?



Reducción de riesgos



Mayor continuidad operativa



Protección de datos



Menor exposición a ataques



Monitoreo permanente



Especialistas trabajando para su organización

CLARO + SCITUM



PROTECCIÓN



CONTINUIDAD DEL NEGOCIO

Tecnología y experiencia de nivel enterprise, sin necesidad de grandes inversiones internas.

EL COSTO DE NO ACTUAR

El costo de prevenir siempre es menor que el costo de recuperarse.

Una hora de indisponibilidad puede representar:



Pérdida de ingresos



Clientes insatisfechos



Daño reputacional



Costos operativos



Tiempo de recuperación

La ciberseguridad dejó de ser un tema tecnológico. **Es un tema de negocio.**



Agendemos la reunión técnica

Arturo Riveros · Claro Empresas

WhatsApp +595 994 384 508