GUÍA

Los 3 Pilares para Fortalecer tu Red y Evitar el Downtime Inesperado

Por SISA Consultores – Expertos en Redes, TI y Ciberseguridad.

SISA
consultoría para TI

www.sisaconsultores.mx

Introducción para el Gerente de TI.

En el ecosistema empresarial actual, la red es el sistema nervioso central. Un fallo no es solo una molestia; es una pérdida de ingresos, reputación y productividad.

Como Gerente de TI o Ciberseguridad, tu desafío es construir una infraestructura que no solo funcione, sino que resista y se adapte.

Esta guía condensa nuestra experiencia en los tres pilares fundamentales que todo líder de TI debe monitorear y fortalecer para garantizar la continuidad del negocio y la visibilidad total.

PILAR 1: Visibilidad de Capa 2 y Endpoints (El Riesgo Invisible)

La mayoría de los ataques exitosos no entran por el firewall, sino por la capa de acceso y la negligencia de los dispositivos finales (endpoints).

Acción Crítica: Blindar el Acceso a la Red.

Desafío común	Solución SISA	Checklist de Implementación
DHCP Spoofing: Ataques Man-in-the-Middle y agotamiento de IPs.	DHCP Snooping & Inspección ARP: Activación y configuración obligatoria en todos los switches de acceso.	[ ] ¿Todos los switches tienen un puerto troncal confiable (trusted)?
Falta de Detección en Endpoints: Antivirusque no detecta amenazas avanzadas (Zero Day).	Implementación de EDR (Endpoint Detection & Response): Sustitución del AV tradicional por una solución que detecte, investigue y responda automáticamente.	[ ] ¿Hemos evaluado el costo-beneficio de una solución EDR gestionada?
Dispositivos Desconocidos: PCs o móviles no autorizados en la red.	NAC (Network Access Control): Solución que permite o deniega el acceso a la red según la identidad y el estado de seguridad del dispositivo.	[ ] ¿Existe una política automatizada para aislar dispositivos no conformes?

SISA
consultoría para TI

www.sisaconsultores.mx

PILAR 2: La Higiene y Arquitectura de la Red (La Base de la Continuidad)

La eficiencia operativa depende de una red que evite la congestión y mantenga el servicio crítico.

Acción Crítica: Optimización y Redundancia.

Desafío común	Solución SISA	Checklist de Implementación
Punto Único de Falla: Dependencia de un solo equipo (firewall, router, servidor).	Redundancia y Alta Disponibilidad (HA): Configuración de clusters de equipos para conmutación por error instantánea (Failover).	[ ] ¿Se realiza un simulacro de failover al por semestre?
Cuellos de Botella: La red se vuelve lenta en horarios pico.	Segmentación VLAN y QoS: Clasificación del tráfico crítico (VoIP, ERP) y asignación de prioridades para garantizar el rendimiento.	[ ] ¿El 80% del tráfico crítico está clasificado y priorizado correctamente y uso de link aggregation asi como velocidades adecuadas de puertos troncales?
Obsolescencia: Equipos de red antiguos sin soporte ni parches.	Plan de Vida Útil (Lifecycle Management): Auditoría anual de hardware y software para planificar reemplazos antes de que expiren las garantías y soporte.	[ ] ¿Existe un inventario actualizado de equipos con fecha de fin de vida (EoL)?

PILAR 3: Respuesta, Políticas y Usuario (El Factor Humano)

El error humano sigue siendo el vector de ataque más común.
La ciberseguridad es una mezcla de tecnología y cultura.

Acción Crítica: Entrenar y Automatizar la Respuesta.

Desafío común	Solución SISA	Checklist de Implementación
Phishing y BEC (Business Email Compromise): Correos falsos que engañan a los empleados.	Simulacros de Phishing y KAPA 8: Entrenamiento continuo y evaluación de la cultura de seguridad de los empleados.	[ ] ¿Se realizan pruebas de phishing no anunciadas mensualmente?
Tiempos de Respuesta Lentos: Demorar horas en identificar y contener un ataque.	Planes de Respuesta a Incidentes (IRP) y SOC/MDR: Tener procedimientos claros y/o un servicio gestionado que contenga la amenaza en minutos.	[ ] ¿El tiempo medio de detección y respuesta (MTTD/MTTR) es menor a 60 minutos?
Falta de Políticas Claras: Empleados que usan contraseñas débiles o software no autorizado.	Políticas de Acceso Cero (Zero Trust): Nunca confiar, siempre verificar. Implementar autenticación multifactor (MFA) obligatoria en todos los puntos de acceso.	[ ] ¿Hemos implementado MFA para todos los servicios críticos (VPN, Email, ERP)?

Conclusión:
El Aliado de tu Continuidad

Tu red es tu mayor activo y tu mayor responsabilidad. En SISA Consultores, combinamos la experiencia técnica en Redes e Infraestructura con una visión de Ciberseguridad proactiva.

Si al revisar este checklist encuentras 3 o más elementos sin implementar o verificar, es momento de una conversación estratégica.

Contáctanos hoy para un diagnóstico sin costo de tu infraestructura crítica.

33-3072-4235

info@sisaconsultores.mx

SISA
consultoría para TI