Soluciones Tecnológicas e Informáticas

Innovamos, conectamos y protegemos tu entorno digital

Evolución de la Tecnología y la Seguridad Informática

80s–90s

Primeros Virus y la Era del PC
Avance Tecnológico: Nacimiento de las computadoras personales (IBM PC, 1981). Expansión del uso de MS-DOS y Windows 95.
Seguridad: Surgen los primeros virus (Brain, Michelangelo) y los primeros antivirus comerciales (McAfee, Norton)

2000

Internet y la Seguridad Perimetral
Avance Tecnológico: Masificación de Internet, llegada del Wi-Fi y el auge de los servidores empresariales.
Seguridad: Implementación de firewalls y sistemas de detección de intrusos (IDS/IPS) para proteger redes corporativas.

2010

Movilidad, Nube y Amenazas Avanzadas
Avance Tecnológico: Boom de los smartphones, servicios en la nube y el IoT (Internet de las Cosas).
Seguridad: Crecen los ciberataques (WannaCry, 2017), el ransomware y la IA comienza a usarse en ciberseguridad.

2020

Actualidad: Transformación Digital y Seguridad Integrada

Avance Tecnológico: Expansión de la inteligencia artificial, redes 5G y digitalización empresarial acelerada.

Seguridad: Se adopta el modelo **Zero Trust**, protección en la nube, ciberseguridad en OT (tecnología operativa)

20?

?

Somos el resultado de mas de 18 años de experiencia en el sector tecnológico.

Soluciones personalizadas y a la medida de las necesidades de nuestros clientes.

Enfoque en pequeña y mediana empresa con una selección estratégica de soluciones y herramientas.

Nuestra Visión:

Convertirnos en el mejor aliado estratégicos de las PYMEs en su transformación digital.

Nuestra Misión:

Brindar soluciones tecnológicas confiables y accesibles para impulsar el crecimiento de nuestros clientes.

Característica de una PYME (en latinoamerica)

1. Infraestructura Tecnológica:

•Hardware:

- Pequeña empresa: Suelen tener menos de **10 a 20 computadoras** y **servidores limitados** o basados en la nube.
- Mediana empresa: Pueden contar con más de **20 a 100 computadoras**, **servidores locales** y mayor capacidad de almacenamiento.

•Red y Conectividad:

- Pequeña empresa: Conexiones de banda ancha estándar, routers simples y menos redundancia.
- Mediana empresa: Redes más robustas con balanceo de carga, seguridad avanzada y redundancia en internet.

2. Uso de Software y Sistemas:

•Sistemas de Gestión:

- Pequeña empresa: Pueden usar herramientas básicas como **Excel**, software de contabilidad simple o **ERP** limitados.
- Mediana empresa: Implementan **ERP**, **CRM** y software de gestión más sofisticado.

•Automatización y Digitalización:

- Pequeña empresa: Baja automatización; procesos manuales.
- Mediana empresa: Mayor automatización en ventas, atención al cliente y finanzas.

Característica de una PYME (en latinoamerica)

3. Ciberseguridad:

•**Pequeña empresa:** Seguridad básica o limitada (antivirus y firewall simple).

•**Mediana empresa:** Medidas más robustas, incluyendo **firewalls avanzados**, **gestión de identidades**, y **copias de seguridad automatizadas**.

4. Presupuesto y Gastos en TI:

•**Pequeña empresa:** Menos del **5% del presupuesto anual** se destina a TI.

•**Mediana empresa:** Entre **5% y 15% del presupuesto anual** se destina a TI, con mayor inversión en innovación y mantenimiento.

El Desafío de las PYMEs

•Falta de recursos especializados en TI ni hablar de Seguridad.
•Falta de presupuestos adecuados o muy limitados.
•Amenazas de ciberseguridad en aumento.
•Necesidad de equipos y soluciones confiables para operar y crecer
•Las PYMEs enfrentan los mismos riesgos que las grandes empresas, pero con menos recursos y personal.

Debería mi PYME adoptar algún estandar de seguridad?

¡Definitivamente sí! Aunque las PYMEs suelen tener **menos presupuesto** para tecnología y seguridad informática, **sí deberían basarse en estándares de seguridad**, aunque sea de manera gradual y adaptada a sus recursos. No solo **vale la pena**, sino que es **fundamental** para proteger sus datos, evitar pérdidas financieras.

¿Por qué una PYME debería seguir estándares de seguridad?

- **Ciberataques son una amenaza real:** El 43% de los ciberataques a nivel mundial están dirigidos a PYMEs.
- **Costos de recuperación altos:** Es más caro recuperarse de un ataque que prevenirlo.
- **Confianza de clientes y socios:** Cumplir con estándares mejora la reputación y facilita alianzas comerciales.
- **Regulaciones y cumplimiento legal:** Dependiendo del país y sector, pueden enfrentar multas por no proteger datos.

Estándares Recomendados para PYMEs:

No es necesario implementar los estándares de manera completa desde el inicio; pueden adoptarse **de forma gradual** según prioridades y recursos.

Estándar de Seguridad	¿Por qué es adecuado para PYMEs?	Qué cubre
ISO 27001 (Sistema de Gestión de Seguridad de la Información)	Adaptable y escalable según el tamaño de la empresa.	Políticas de seguridad, gestión de accesos y continuidad del negocio.
NIST Cybersecurity Framework (CSF)	Es flexible y prioriza los riesgos más críticos.	Identificación, protección, detección y recuperación ante incidentes.
CIS Controls (Center for Internet Security)	Proporciona controles básicos y avanzados según el nivel de madurez.	Contraseñas seguras, parches, monitoreo y seguridad en la nube.
PCI DSS (Payment Card Industry Data Security Standard)	Relevante si aceptan pagos con tarjetas de crédito.	Protección de datos de transacciones y cifrado.

¿Cómo Implementar Seguridad en PYMEs con Presupuesto Limitado?

1.Iniciar con lo básico (CIS Controls):

1. Actualización y parches regulares.
2. Autenticación multifactor (MFA).
3. Respaldo de datos automatizado.

2.Priorizar los datos más críticos:

1. Protege primero datos financieros y de clientes.
2. Cifra datos sensibles y usa copias de seguridad en la nube.

3.Apoyarse en la nube y servicios gestionados:

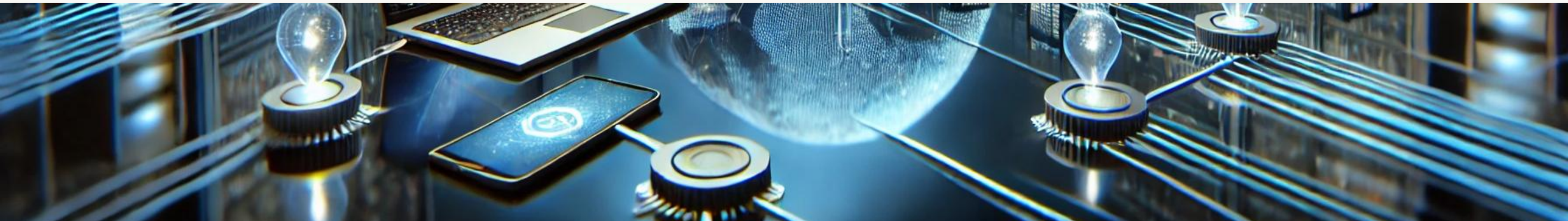
1. Los servicios en la nube (AWS, Azure, Google Cloud) ofrecen seguridad integrada.
2. Los proveedores de seguridad gestionada (MSSP) son más accesibles que un equipo interno.

4.Capacitar a los empleados:

1. El 85% de los ciberataques se deben a **errores humanos**.
2. Capacitación básica en **phishing**, contraseñas y uso de redes públicas.

Roadmap de Seguridad para PYMEs Basado en Estándares

Objetivo:
Implementar seguridad en fases progresivas para cumplir con estándares clave y proteger activos críticos.



Tiempo: 1 - 3 meses

Objetivo: Proteger contra las amenazas más comunes y asegurar la continuidad operativa.

Solución	Estándar Cubierto	Beneficio Clave
ESET NOD32 (Protección de Endpoints)	- **CIS Control 8** (Malware Defense) - **NIST CSF (Protect - PR.DS)**	Prevención de malware, virus y ransomware.
Horney Security (Anti-Spam y Cifrado de Correo)	- **ISO 27001 A.13** (Seguridad en las comunicaciones) - **GDPR (Privacidad de datos)**	Bloqueo de spam y phishing; cifrado de datos.
Atera (Gestión de TI y Parches)	- **CIS Control 3** (Continuous Vulnerability Management) - **ISO 27001 A.12** (Operaciones Seguras)	Automatización de parches y gestión de vulnerabilidades.
PhishingBox (Simulación de Phishing y Concienciación)	- **NIST CSF (Protect - PR.AT)** - **ISO 27001 A.7.2** (Capacitación en Seguridad)	Fortalece la conciencia de seguridad del personal.
Backup Automatizado (Ej. Atera/ManageEngine)	- **ISO 27001 A.12.3** (Backup) - **CIS Control 10** (Data Recovery Capability)	Recuperación rápida ante incidentes.

Fase 2: Seguridad Intermedia – Protección y Detección Proactiva

Tiempo: 4 - 6 meses

Objetivo: Detectar y responder a amenazas más avanzadas con monitoreo continuo.

Solución	Estándar Cubierto	Beneficio Clave
Horney Security (Advanced Threat Protection - ATP)	- **NIST CSF (Detect - DE.CM)** - **ISO 27001 A.12.4** (Monitoreo de Eventos)	Detección de amenazas sofisticadas (fraude CEO, ransomware).
Quest Foglight (Monitoreo de Bases de Datos)	- **CIS Control 6** (Maintenance, Monitoring, and Analysis) - **ISO 27001 A.12.4**	Visibilidad del rendimiento y seguridad de datos.
ManageEngine (Monitoreo de Infraestructura)	- **NIST CSF (Detect - DE.CM)** - **ISO 27001 A.12.6** (Gestión de Incidentes)	Monitoreo en tiempo real y alertas de anomalías.
PhishingBox (Evaluaciones Periódicas)	- **CIS Control 17** (Security Awareness Training)	Reforzamiento continuo de la conciencia de seguridad.

Fase 3: Seguridad Avanzada – Gestión de Accesos y Resiliencia
Tiempo: 7 - 12 meses
Objetivo: Implementar controles avanzados de acceso y resiliencia para la continuidad del negocio.

Solución	Estándar Cubierto	Beneficio Clave
Quest PAM (Privileged Access Management)	- **ISO 27001 A.9** (Control de Accesos) - **CIS Control 4** (Controlled Use of Admin Privileges	Control y auditoría de accesos privilegiados.
Quest Active Directory Security	**ISO 27001 A.11** (Control de Accesos Físicos y Lógicos) - **NIST CSF (Protect - PR.AC)**	Protección de identidades y accesos en AD y Entra ID.
Atera (Automatización y Continuidad de Negocio)	- **ISO 27001 A.17** (Continuidad del Negocio)	Automatización y respuesta ante fallos de sistema.
Horney Security (Archivado y Cifrado GDPR)	-- **GDPR (Art. 32)** - **ISO 27001 A.18.1.3** (Protección	Cifrado y archivado para cumplimiento regulatorio

Resumen del Roadmap:

Fase	Duración Estimada	Prioridad	Resultado Clave
🏁 **Fase 1**(Fundamentos)	1 - 3 meses	Alta (Imprescindible)	Protección básica contra malware y pérdida de datos.
🏃 **Fase 2** (Intermedia)	4 - 6 meses	Media-Alta	Monitoreo continuo y detección proactiva.
🚀 **Fase 3** (Avanzada)	7 - 12 meses	Media-Baja (Pero necesaria)	Gestión de accesos y resiliencia ante incidentes.

Beneficios de Seguir este Roadmap:
•**Escalabilidad:** Se adapta al crecimiento y presupuesto de la PYME.
•**Cumplimiento de Estándares:** Alineado con **ISO 27001**, **NIST CSF** y **CIS Controls**.
•**Reducción de Riesgos:** Minimiza el impacto de ciberataques y errores humanos.
•**Mejora de la Resiliencia:** Garantiza continuidad del negocio.

Beneficios de seguir el Roadmap:

- **Escalabilidad:** Se adapta al crecimiento y presupuesto de la PYME.
- **Cumplimiento de Estándares:** Alineado con **ISO 27001**, **NIST CSF** y **CIS Controls**.
- **Reducción de Riesgos:** Minimiza el impacto de ciberataques y errores humanos.
- **Mejora de la Resiliencia:** Garantiza continuidad del negocio.

Soluciones de Seguridad

Trustifi

Quest

phishing box

ATERA

ManageEngine

ESET