TECNOKLI

GUÍA DE SEGURIDAD DE TU INFORMACIÓN

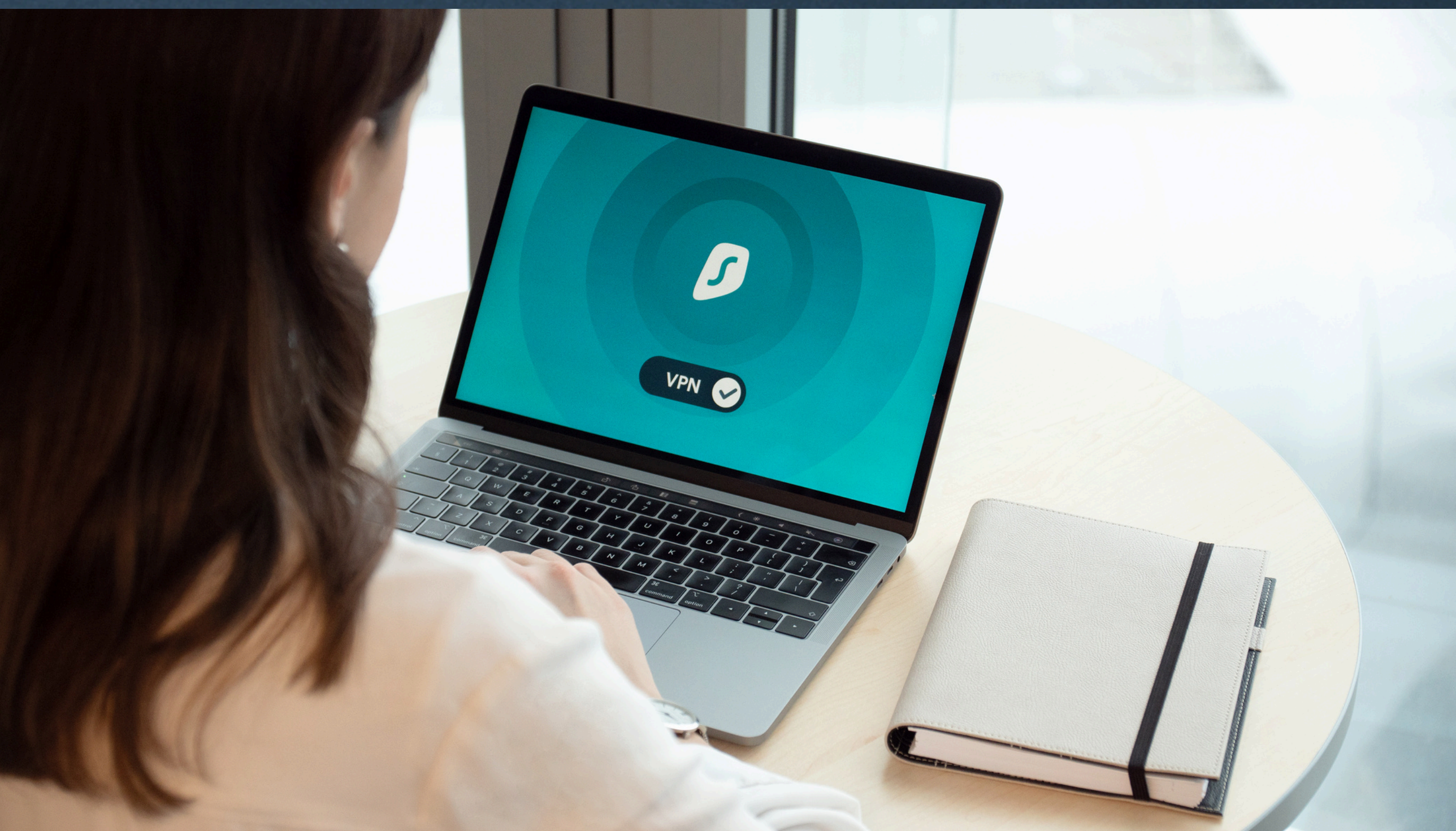
Estrategias para cuidar la información de tu negocio

tecnokli.com

TECNOKLI

INTRODUCCIÓN

En un mundo cada vez más digital, la ciberseguridad se ha convertido en una necesidad crítica para las empresas de todos los tamaños. En Colombia, las micro, pequeñas y medianas empresas (Mipymes) representan más del 90% del tejido empresarial, y muchas de ellas están en riesgo por no contar con medidas de protección adecuadas frente a amenazas informáticas.



TECNOKLI

CAPÍTULO 1: ⚠ PANORAMA ACTUAL DEL CIBERCRIMEN EN COLOMBIA

Según datos del Centro Cibernético de la Policía Nacional, los delitos informáticos en Colombia aumentaron en un 32% durante el último año. Entre los más comunes se encuentran el robo de información, el secuestro de datos (ransomware), fraudes financieros y suplantación de identidad. Las Mipymes son objetivos frecuentes debido a su bajo nivel de protección y desconocimiento de los riesgos.

🔒 **Incremento de ataques de ransomware**
Se ha registrado un aumento de más del 40% en ataques con secuestro de datos.

👥 **Suplantación de identidad**
Las estafas a través de correos electrónicos falsos se han duplicado.

💰 **Pérdidas económicas**
Se estima que una Mipyme puede perder entre $10 y $50 millones de pesos por un solo incidente cibernético

TECNOKLI

CAPÍTULO 2: 🔓 PRINCIPALES RIESGOS PARA LAS MIPYMES

Según datos del Centro Cibernético de la Policía Nacional, los delitos informáticos en Colombia aumentaron en un 32% durante el último año. Entre los más comunes se encuentran el robo de información, el secuestro de datos (ransomware), fraudes financieros y suplantación de identidad. Las Mipymes son objetivos frecuentes debido a su bajo nivel de protección y desconocimiento de los riesgos.

Falta de formación del personal
El desconocimiento de prácticas seguras como la gestión de contraseñas o el manejo de correos electrónicos puede abrir la puerta a los ciberdelincuentes.

Uso de software no actualizado o sin licencias
Las vulnerabilidades en software desactualizado son uno de los principales puntos de entrada para ataques.

Ausencia de políticas de seguridad
Muchas empresas no cuentan con lineamientos internos sobre seguridad digital.

Respaldo de información deficiente
No tener copias de seguridad actualizadas puede ser devastador en caso de un ataque.

TECNOKLI

CAPÍTULO 3: 🔐 RECOMENDACIONES CLAVE PARA PROTEGER TU EMPRESA

Capacitación constante del personal

- Educa a tus empleados sobre amenazas comunes como phishing, ingeniería social y malware.
- Organiza talleres y charlas con expertos en seguridad.
- Utiliza pruebas internas para medir el nivel de conciencia cibernética.

Implementar políticas de contraseñas seguras

- Obliga el uso de contraseñas complejas que incluyan letras, números y símbolos.
- Cambia las contraseñas con regularidad y evita repetirlas en diferentes plataformas.
- Implementa la autenticación en dos pasos (2FA) para accesos críticos.

Mantener software y sistemas actualizados

- Asegúrate de que todos los sistemas operativos, navegadores, antivirus y programas estén al día.
- Automatiza las actualizaciones cuando sea posible para reducir errores humanos.

Utilizar soluciones de seguridad confiables

- Instala antivirus y antimalware reconocidos.
- Utiliza firewalls para proteger el perímetro de tu red.
- Configura herramientas de monitoreo para detectar comportamientos sospechosos en tiempo real.

TECNOKLI

Realizar respaldos frecuentes

- Establece una política de copias de seguridad diaria o semanal, dependiendo del volumen de datos.
- Guarda las copias en diferentes ubicaciones (local y nube) y verifica su integridad regularmente.
- Asegúrate de que las copias estén cifradas y protegidas con contraseñas.

Limitar el acceso a la información sensible

- Define roles de usuario con permisos diferenciados.
- Controla los accesos a carpetas, bases de datos y documentos críticos.
- Monitorea el uso de la información para detectar accesos indebidos.

Evaluar proveedores y terceros

- Exige a tus proveedores cumplir con estándares básicos de ciberseguridad.
- Firma acuerdos de confidencialidad y políticas de tratamiento de datos.
- Realiza auditorías o revisiones periódicas de sus prácticas de seguridad.

Desarrollar un plan de respuesta ante incidentes

- Ten un protocolo claro sobre qué hacer en caso de un ataque.
- Designa responsables de gestión de crisis cibernéticas.
- Documenta los incidentes para aprender de ellos y fortalecer tus defensas.

TECNOKLI

CAPÍTULO 4: 🔐🛡️ CIBERSEGURIDAD PERSONAL:

PROTEGE TU VIDA DIGITAL

La ciberseguridad no es solo un tema empresarial. Cualquier persona con un celular, acceso a internet o redes sociales puede ser blanco de ataques. Desde el robo de tu cuenta de WhatsApp hasta fraudes bancarios, los riesgos están más cerca de lo que parece. En este capítulo encontrarás medidas prácticas y fáciles de aplicar para proteger tu vida digital.

🔐 **Contraseñas fuertes y únicas**

No uses la misma contraseña en varias plataformas. Crea claves de al menos 12 caracteres, combinando letras, números y símbolos. Evita fechas de nacimiento o nombres conocidos.

🟦 **Gestores de contraseñas**

Utiliza herramientas como Bitwarden, LastPass o 1Password para generar y guardar tus claves de forma segura. Así no tendrás que memorizarlas todas.

🔑 **Autenticación en dos pasos (2FA)**

Activa el doble factor de verificación en todas las cuentas que lo permitan: correo, redes sociales, banca móvil, plataformas de trabajo y más. Esto añade una capa adicional de protección.

🚫 **Cuidado con lo que compartes**

Evita publicar información personal como tu número de teléfono, dirección, fechas de viaje o rutinas diarias. Los ciberdelincuentes pueden usar estos datos para suplantarte o chantajearte.

TECNOKLI

🕵️ **Revisa tu configuración de privacidad**
Limita quién puede ver tus publicaciones, historias y lista de amigos. Desactiva la opción de ser etiquetado sin aprobación previa.

🔗 **Evita enlaces sospechosos**
Nunca hagas clic en enlaces de sorteos, promociones o premios que no esperabas. Verifica siempre el dominio web y, si tienes dudas, no abras el enlace.

💻 **Conéctate solo desde dispositivos seguros**
No realices pagos o transferencias desde equipos públicos o redes Wi-Fi abiertas. Si es urgente, usa una red privada virtual (VPN) como ProtonVPN

🛍️ **Compra en sitios confiables**
Asegúrate de que el sitio web tenga un candado 🔒 en la barra de direcciones (https://) y una política de privacidad visible.

📩 **Desconfía de mensajes urgentes**
Los bancos nunca piden datos por correo o WhatsApp. Si recibes un mensaje sospechoso, contacta directamente a la entidad desde sus canales oficiales.

📱 **Actualiza el sistema operativo y las apps**
Las actualizaciones no son solo mejoras visuales, también corrigen fallos de seguridad.

📲 **Instala apps solo desde tiendas oficiales**
Evita descargar archivos APK o apps de sitios desconocidos. Pueden contener malware que roba tu información.

TECNOKLI

🔍 **Controla los permisos de cada app**
Muchas apps solicitan acceso innecesario a cámara, micrófono o contactos. Revisa y ajusta estos permisos desde la configuración.

🔒 **Bloqueo de pantalla seguro**
Usa PIN, patrón, huella digital o reconocimiento facial para proteger el acceso a tu dispositivo.

🧯 **Configura un sistema de borrado remoto**
Activa opciones como “Buscar mi dispositivo” para localizar tu teléfono en caso de pérdida o robo, y borrar los datos si es necesario.

La ciberseguridad personal comienza con pequeños hábitos. Cada medida que implementes reduce significativamente el riesgo de ser víctima. Recuerda: no necesitas ser experto en tecnología para proteger tu información, solo necesitas estar informado y ser precavido.

TECNOKLI

☑ CHECKLIST DE IMPLEMENTACIÓN EN CIBERSEGURIDAD PARA MIPYMES

- [ ] Todo el personal ha recibido formación básica en ciberseguridad.
- [ ] Se aplican políticas de contraseñas seguras y se usa autenticación en dos pasos.
- [ ] Todos los sistemas operativos y programas están actualizados.
- [ ] Se cuenta con antivirus, antimalware y firewall activos y actualizados.
- [ ] Se realizan respaldos periódicos y seguros de la información crítica.
- [ ] El acceso a datos sensibles está limitado según roles de usuario.

TECNOKLI

- [ ] Los proveedores externos cumplen con estándares mínimos de seguridad.
- [ ] Existe un plan de respuesta ante incidentes documentado y probado.
- [ ] Las políticas internas de seguridad están escritas y divulgadas a todo el equipo.
- [ ] Se realizan auditorías internas o externas de seguridad al menos una vez al año.

TECNOKLI

IMPLEMENTA SEGURIDAD

Proteger tu empresa no tiene que ser costoso ni complejo. Kaspersky ofrece soluciones diseñadas especialmente para Mipymes, con herramientas avanzadas que permiten:

- Protección contra malware, ransomware y spyware.
- Control de accesos y navegación segura.
- Administración centralizada de la seguridad de todos los dispositivos.
- Soporte técnico especializado en español.

Beneficios de Kaspersky para tu negocio:

- Prevención de pérdidas económicas por ataques cibernéticos.
- Mayor confianza por parte de tus clientes y proveedores.
- Cumplimiento de normativas de protección de datos.
- Tranquilidad para enfocarte en el crecimiento de tu empresa.

302 413 5832

TECNOKLI.COM