



# Olimpia

## Ciberseguridad en Colombia:

# Protege a tu empresa de las amenazas digitales

La **ciberseguridad** es un tema cada vez más relevante en Colombia, especialmente para las empresas que buscan proteger sus activos más valiosos. En **Olimpia**, **te ayudamos a blindar lo más importante**: la continuidad de tu operación, la seguridad de tus datos y confiAnza de tus clientes ante las crecientes amenazas digitales.

# 5

## Consejos prácticos para cuidar la información de tu empresa

# 1 Convierte a tu equipo en la primera **línea de defensa**

Tu equipo puede ser el eslabón más débil o el más fuerte en la cadena de seguridad cibernética. ¡Todo depende de las acciones que tomes! Muchos ataques comienzan con tácticas de ingeniería social, **como correos electrónicos falsos que parecen reales (phishing) o llamadas solicitando información confidencial.**



En muchos casos, el desconocimiento hace que los colaboradores **entreguen datos clave o caigan en trampas** que parecen inofensivas.

**Desde OlimplA, te recomendamos:**



Capacitar a todo tu equipo, incluyendo al área administrativa, operativa y directivos, **para reconocer ataques comunes como correos falsos o mensajes engañosos.**



**Realizar simulacros de phishing y medir qué tan preparados están los empleados**, no para señalar errores, sino educarlos en ciberprotección.



**Implementar prácticas de seguridad** como el uso de contraseñas seguras y autenticación multifactor (MFA) para acceder a sistemas críticos.

## Por ejemplo

Un cliente **evitó un robo masivo de información** gracias a un entrenamiento efectivo. Un empleado detectó un correo sospechoso que solicitaba datos de acceso y tomó las medidas adecuadas.

**¡La educación es la mejor defensa contra las amenazas!**



# 2

## Mantén tu tecnología siempre **actualizada**

Un sistema desactualizado es como dejar las puertas de tu empresa abiertas. Muchos ciberdelincuentes aprovechan las **vulnerabilidades del software** antiguo o sin parches de seguridad para infiltrarse. No actualizar tus sistemas pone en riesgo tu operación y afecta el rendimiento de las operaciones.



### Aquí te dejamos algunos consejos clave:



Configura actualizaciones críticas automáticas en tus equipos y aplicaciones esenciales. Esto reduce el **margen de error humano**.



Si usas **software especializado**, asegúrate de contar con soporte técnico constante y verifica que los parches más recientes estén instalados.



**Realiza auditorías técnicas periódicas** para identificar y resolver vulnerabilidades en tu infraestructura digital.



Una empresa puede sufrir un ataque al utilizar un software obsoleto. **La solución es simple: actualizarlo.** A veces, lo básico es lo que más te protege. En **Olimpia**, sabemos que mantener tus sistemas actualizados es sinónimo de **proteger y optimizar tu negocio.**

# 3

## **Protege tu red** como si fuera la puerta principal

**Tu infraestructura empresarial es el eje que conecta datos, sistemas y colaboradores.** Si alguien no autorizado accede a ella, podría comprometer todo tu negocio. Mantenerla segura es como cerrar bien la puerta principal y asegurarte de que solo las personas indicadas puedan entrar.



## Desde Olimpia te recomendamos:



**Configura redes seguras** y cambia las contraseñas de Wi-Fi periódicamente. Asegúrate de que las credenciales de acceso a la red no sean fáciles como: "1234".



**Utiliza redes privadas virtuales (VPN)** para proteger las conexiones remotas y cifrar la información sensible.



**Monitorea el tráfico de la red** con firewalls avanzados y herramientas de detección de intrusiones para identificar actividades sospechosas.

## Te puede interesar

[La Inteligencia Artificial como herramienta transformadora de la ciberseguridad](#)



# 4

## Haz del respaldo de datos un

### **hábito constante**

Imagina perder toda la información de tus clientes, contratos y operaciones en un instante. Los ciberataques, errores humanos y fallos técnicos pueden ocurrir en cualquier momento. **Tener un respaldo de datos te permite recuperarte rápido y minimizar las pérdidas.**

### **Por eso, te sugerimos:**



**Realiza copias de seguridad diarias o semanales,** dependiendo de la criticidad de tu información.



**Almacena los respaldos en varios lugares seguros,** como dispositivos externos y soluciones en la nube.



**Prueba periódicamente tus copias de seguridad** para asegurarte de que la recuperación sea exitosa, en caso de que llegue a ocurrir algún incidente.

Recuerda la **estrategia**  
de **backup 3-2-1**  
como una **técnica para**  
**proteger los datos** que consiste en:

Tener al menos  
**3 copias** de  
los datos

Almacenar las  
copias en **2 tipos**  
de **medios**  
diferente

Guardar una copia  
fuera del sitio, en  
una **ubicación**  
**remota**

Esta **estrategia** es una de  
las más **recomendadas**  
para garantizar la  
recuperación y resiliencia  
de los datos.



# 5 Monitorea la ciberseguridad **en tiempo real** para anticiparte

**La ciberseguridad no es un esfuerzo de una sola vez, es un proceso continuo.** Las amenazas evolucionan rápidamente, por lo que monitorear tu infraestructura en tiempo real es clave para anticiparte a los riesgos.

¡No te olvides de la **seguridad de tus clientes!**



**Monitorea 24/7** las redes, aplicaciones y dispositivos para detectar comportamientos sospechosos.



**Crea respuestas rápidas y automatizadas** ante incidentes críticos para evitar daños mayores.



**Realiza un análisis continuo** para identificar vulnerabilidades y mejorar la seguridad de tu infraestructura.



# Nuestras soluciones

## para proteger a tu empresa

En **Olimpia**, contamos con productos y servicios especializados que se adaptan a las necesidades de tu empresa:



### **SOC 24/7 (Centro de Operaciones de Seguridad):**

Monitoreo constante para detener amenazas en tiempo real.



### **Gestión de vulnerabilidades y pruebas de penetración (Pentesting):**

Identificamos y resolvemos fallas de seguridad antes de que se conviertan en problemas.



### **Protección de redes y dispositivos:**

Implementamos firewalls avanzados y soluciones como Endpoint Detection and Response (EDR).



### **Respuesta a incidentes CSIRT:**

Contenemos, mitigamos e investigamos ciberataques para evitar que vuelvan a ocurrir.

# Proteger tu empresa es construir

## ConflAnza Digital

Sabemos que la **ciberseguridad no solo se trata de proteger sistemas**, sino de asegurar que las operaciones de tu empresa se realicen sin interrupciones, lo que fortalece la credibilidad y confianza de tus clientes.

Trabajemos juntos en la estrategia de ciberseguridad de tu empresa, comienza aquí.

