





MEJORES PRÁCTICAS PARA LA SEGURIDAD EN SOPORTE TI

El soporte TI (Tecnologías de la Información) se refiere a la asistencia técnica que se proporciona a usuarios y organizaciones para resolver problemas relacionados con sistemas informáticos, software, hardware, redes y otros recursos tecnológicos. Este soporte es fundamental para garantizar el funcionamiento óptimo de las operaciones empresariales y la productividad de los empleados, también involucra resolución de problemas, gestión de incidentes, configuración y mantenimiento, seguridad informática, atención al usuario, gestión de activos, monitorización y mantenimiento y recuperación de datos.

El soporte técnico de TI es uno de los pilares fundamentales en cualquier organización moderna. Sin embargo, también representa un punto crítico de riesgo de seguridad, ya que los técnicos tienen acceso privilegiado a sistemas, datos sensibles y redes internas. Por ello, implementar prácticas de seguridad en el soporte de TI no es opcional: es esencial para proteger la integridad, confidencialidad y disponibilidad de la información.

El soporte de TI no es solo una función técnica, sino también una responsabilidad de seguridad. Implementar controles, formar al personal, y seguir buenas prácticas ayuda a:

-  Prevenir accesos no autorizados
-  Proteger la información de la empresa y los clientes
-  Cumplir con normativas legales
-  Garantizar la operatividad del negocios

En una empresa de desarrollo de software, como Netguard Solutions, el área de **Soporte Técnico en TI** cumple una función crítica no sólo para mantener los sistemas funcionando, sino también para **proteger los activos digitales más valiosos**: el código fuente, los datos de los clientes, los entornos de desarrollo, pruebas y producción.

¿Cómo llevar a cabo buenas prácticas de seguridad en soporte TI?

Control de Acceso

- Usa el principio de mínimos privilegios: solo acceso necesario para cada tarea.
- Implementa autenticación multifactor (MFA) en sistemas críticos.
- Evita compartir credenciales entre técnicos.

Gestión de Contraseñas

- Usa contraseñas seguras y únicas.
- Emplea un gestor de contraseñas aprobado.
- Cambia contraseñas predeterminadas en dispositivos o sistemas nuevos.

Actualizaciones y Parches

- Mantén sistemas operativos y software actualizados.

- Aplica parches de seguridad tan pronto como estén disponibles.
- Usa herramientas de administración remota con funciones de actualización centralizada.

✓ Uso Seguro de Herramientas de Soporte Remoto

- Usa conexiones cifradas (ej. RDP con VPN, TeamViewer con verificación).
- Solicita autorización explícita del usuario antes de conectarte.
- Finaliza la sesión correctamente y cierra accesos remotos cuando no estén en uso.

✓ Respaldo y Recuperación

- Verifica que existan copias de seguridad automáticas y regulares.
- Prueba los procesos de restauración periódicamente.
- Asegura que los backups estén cifrados y almacenados fuera del entorno productivo.

✓ Monitoreo y Registro

- Habilita logs de acceso y actividades en servidores, estaciones y herramientas de soporte.
- Monitorea eventos sospechosos o accesos no autorizados.
- Usa SIEM o herramientas de análisis si es posible.

✓ Seguridad Física

- Controla el acceso físico a los servidores, redes y estaciones de trabajo.
- Usa cerraduras, cámaras o tarjetas de identificación según el entorno.

✓ Educación y Concientización

- Capacita al personal técnico y a los usuarios finales sobre phishing, ingeniería social y políticas de seguridad.
- Documenta los procedimientos seguros para tareas comunes (instalaciones, soporte remoto, etc.).

✓ Políticas y Procedimientos

- Establece políticas claras de soporte (horarios, límites de acceso, tiempos de respuesta).
- Documenta cada incidente o intervención técnica.
- Ten procedimientos definidos para responder a incidentes de seguridad.

✓ Seguridad en el Correo Electrónico y Navegación

- Evita abrir archivos adjuntos o enlaces sospechosos.
- Usa filtros antispam y antivirus actualizados.
- Configura políticas de uso seguro de internet y correo corporativo.

La **seguridad en el soporte TI** es un elemento estratégico en empresas de software. Va más allá de resolver incidencias: implica proteger activos críticos, mantener la continuidad del desarrollo y asegurar que los entornos estén blindados frente a errores humanos, ataques y malas prácticas.

