Evaluación y Rediseño de Infraestructura de Red en TecnoPlast S.A.

Objetivo
Diseñar una arquitectura de red inteligente para la planta de TecnoPlast S.A., integrando automatización, M2M, IoT, redes 5G y plataformas en la nube, garantizando visibilidad en tiempo real, seguridad y escalabilidad.

1 Diagnóstico de la infraestructura actual

La red existente se compone de equipos industriales aislados, una única VLAN sin segmentación, una red Wi-Fi básica sin cifrado ni autenticación avanzada y reportes de producción elaborados manualmente. El mantenimiento es correctivo, lo que genera paradas inesperadas y elevados costos operativos. La visibilidad en tiempo real es nula, impidiendo decisiones oportunas. La falta de segmentación expone a toda la planta a riesgos de ciberataques y provoca cuellos de botella en el tráfico.

2 Propuesta de nueva arquitectura

La solución adopta una topología híbrida estrella-malla local por áreas funcionales, segmentada en VLAN dedicadas y conectada a una nube privada para almacenamiento y análisis de datos.

2.1 Segmentación por VLAN y QoS

Se definen cinco VLAN:

- **Administración (VLAN 10)**: PCs de gestión, servidores de aplicaciones y base de datos.
- **Producción (VLAN 20)**: PLCs, HMIs y servidores SCADA.
- **IoT / M2M (VLAN 30)**: Sensores, gateways IoT y dispositivos M2M.
- **Wi-Fi (VLAN 40)**: Puntos de acceso con WPA2-Enterprise respaldados por RADIUS.
- **DMZ (VLAN 50)**: Plataforma de nube local, repositorio de datos y accesos externos.

El tráfico de planta se jerarquiza mediante colas de calidad de servicio (QoS) en routers y switches de capa 3, priorizando control real-time (SCADA) sobre otros flujos no críticos.

2.2 Conectividad y redundancia

La interconexión entre switches de cada área utiliza enlaces troncales 802.1Q con agregación LACP para aumentar ancho de banda y tolerancia a fallos. Entre zonas críticas se establecen enlaces redundantes en anillo gestionados por STP optimizado. El core de red se implementa con routers industriales Cisco ISR 4331, conectados a un firewall ASA 5506-X que gestiona políticas de acceso y VPN site-to-site hacia la nube.

2.3 Integración 5G y nube

Se simula un enlace 5G privado en la VLAN 30, ofreciendo baja latencia (<10 ms) para AGVs y robots móviles. El gateway IoT envía datos a un clúster de análisis en la nube privada (VLAN 50) mediante túnel VPN cifrado con TLS 1.2.

3 Caso de uso: Mantenimiento predictivo

Sensores de vibración y temperatura instalados en motores de inyección envían lecturas cada dos segundos al gateway IoT. Un algoritmo de IA alojado en la nube analiza tendencias y detecta anomalías antes de que ocurra una falla. Al identificar un patrón de vibración excesiva, el sistema genera automáticamente una orden de trabajo en el sistema de gestión de mantenimiento (CMMS) y notifica al equipo de ingeniería. Esto reduce paradas no planificadas y extiende la vida útil del equipamiento.

4 Consideraciones de ciberseguridad

La seguridad se basa en estándares ISA/IEC 62443 y NIST SP 800-82. Se aplican los siguientes controles:

- **Autenticación y autorización**: 802.1X con RADIUS para acceso de usuarios y dispositivos, políticas RBAC para segmentos críticos.
- **Cifrado**: TLS 1.2/1.3 en comunicaciones SCADA, VPN IPSec para conexiones a nube y entre sedes.
- **Segmentación**: ACL en routers y switches capa 3 para restringir tráfico inter-VLAN sólo a servicios autorizados.
- **Monitoreo**: SIEM centralizado recoge registros de firewall, switches y servidores; IDS/IPS virtuales en VLAN 20 y 30.
- **Gestión de vulnerabilidades**: escaneos periódicos automatizados y actualizaciones programadas de firmware.

5 Ventajas esperadas

La nueva arquitectura proporcionará:

- **Eficiencia**: datos en tiempo real para optimizar procesos y reducir tiempos de ciclo.
- **Costos**: disminución de paradas por mantenimiento predictivo y reducción de intervenciones manuales.
- **Seguridad**: aislamiento de riesgos, autenticación robusta y cifrado de extremo a extremo.
- **Escalabilidad**: reserva de VLAN y capacidad de procesamiento en la nube para integrar futuras aplicaciones de Industria 4.0.
- **Resiliencia**: redundancia en enlaces y dispositivos críticos, mantenimiento de operación ante fallos individuales.

6 Conclusión

La propuesta de red inteligente transforma la planta de TecnoPlast S.A. en un ecosistema interconectado y seguro, alineado con prácticas de ciberseguridad industrial y tecnologías de Industria 4.0. La segmentación, el uso de 5G y la integración en la nube permiten a la organización anticipar fallas, mejorar la productividad y mantener la integridad de sus operaciones ante amenazas cibernéticas.