MODELO DE ENTREGABLE. La empresa, la red, las mediciones y los hallazgos de este documento son ficticios. Se publica para mostrar la estructura y el nivel de detalle de un informe de evaluación de 3JC. No corresponde a un trabajo ejecutado para un cliente.

CORPORACIÓN 3JC, C.A.
3JC Telecommunications & Network Engineering
RIF J-50817370-8

3JC-TNE-INF-0000
Revisión 1
Estado: MODELO

Informe de evaluación de la red de comunicaciones operativas

Centro de control, Planta Compresora PC-1 y Estación de Flujo EF-2

Cliente	Operadora Modelo, S.A. (ficticia)
Solicitud	Evaluar si la red puede mantener la supervisión SCADA de PC-1 y EF-2 ante la falla de un enlace.
Trabajo de campo	9 al 13 de marzo de 2026
Fecha del informe	27 de marzo de 2026
Clasificación	Confidencial. Uso exclusivo del cliente.

Contenido

1. Resumen ejecutivo
2. Alcance
3. Red evaluada
4. Resumen de hallazgos
5. Hallazgos en detalle
6. Plan de corrección
7. Metodología y criterios
8. Limitaciones
9. Anexos
10. Control del documento

1. Resumen ejecutivo

Operadora Modelo solicitó verificar si la supervisión SCADA de la Planta Compresora PC-1 y de la Estación de Flujo EF-2 se mantiene cuando falla el enlace de fibra óptica entre el centro de control y PC-1.

No se mantiene. En la prueba de corte del 12 de marzo, la red pasó al enlace de respaldo en menos de un segundo y el ping a las RTU siguió respondiendo, pero el centro de control dejó de recibir datos de las dos instalaciones

durante los 6 minutos y 15 segundos que duró la prueba. El enlace del operador que sirve de respaldo filtra el segmento de red donde están las RTU (hallazgo H-01).

Además:

- La fibra CC–PC-1 perdió 4,7 dB de señal desde su puesta en servicio en 2021. El margen actual es de 2,1 dB; el criterio de diseño pide 3 dB. La causa más probable es una curvatura del cable cerca del km 21,3 (H-03).
- Las computadoras de oficina de PC-1 están en la misma red que los controladores de proceso, sin ningún filtro entre ellos (H-02).
- El radioenlace PC-1–EF-2 registró 47 cortes en 30 días. Nadie lo sabía, porque la red no tiene monitoreo (H-04, H-05).

Se recomienda corregir H-01 antes de cualquier otra cosa. Es un cambio de configuración en el equipo del operador y no requiere compra de equipos. Las acciones están ordenadas en la sección 6.

2. Alcance

Objetivo	Determinar si la red mantiene el transporte del tráfico SCADA ante la falla de un enlace, e identificar los riesgos que comprometen su disponibilidad.
Qué se evaluó	Enrutadores CR-CC y CR-PC1, conmutadores SW-PC1 y SW-EF2, enlace de fibra CC–PC-1, servicio L3VPN de respaldo (lado cliente), radioenlace PC-1–EF-2, alimentación eléctrica de los gabinetes de comunicaciones en PC-1.
Qué quedó fuera	Servidores y estaciones del sistema SCADA, configuración de las RTU y PLC, red interna del operador del servicio L3VPN, prueba de intrusión. La revisión de seguridad se limitó a la segmentación de la red.
Condiciones	Acceso de solo lectura a los equipos, salvo la prueba de corte, hecha en ventana de mantenimiento autorizada por el cliente con un operador de consola presente.

3. Red evaluada

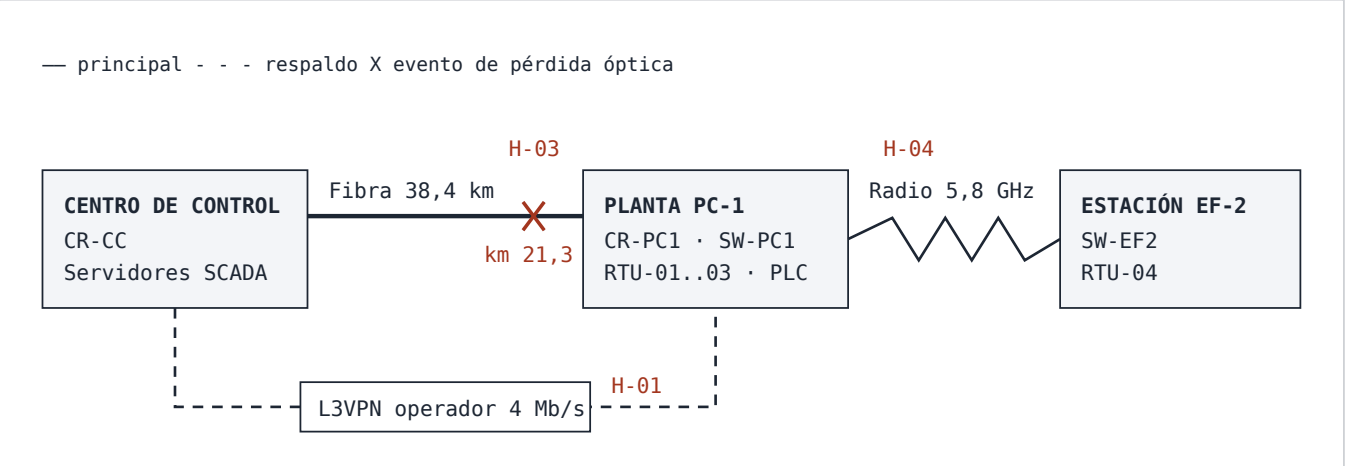

Figura 1. Esquema simplificado. Las marcas en rojo remiten a los hallazgos.

Enlace	Medio	Función	Enrutamiento
CC – PC-1	Fibra monomodo, 38,4 km, SFP 1550 nm	Principal	OSPF área 0
CC – PC-1	L3VPN de operador, 4 Mb/s	Respaldo	Ruta estática flotante (distancia administrativa 250)
PC-1 – EF-2	Radioenlace punto a punto, 5,8 GHz, 12,6 km	Único	Capa 2, VLAN extendida

4. Resumen de hallazgos

ID	Hallazgo	Criticidad	Activo
H-01	El enlace de respaldo no transporta el tráfico SCADA	CRÍTICA	L3VPN, CPE del operador
H-02	Equipos de oficina en la misma red que los controladores de proceso	ALTA	SW-PC1, VLAN 1
H-03	Margen óptico de 2,1 dB en la fibra CC–PC-1	ALTA	Fibra CC–PC-1
H-04	Radioenlace PC-1–EF-2 con nivel de recepción 13 dB por debajo del diseño	MEDIA	Radio PC-1 / EF-2
H-05	La red no tiene monitoreo ni registro centralizado de eventos	MEDIA	Todos los equipos
H-06	Autonomía eléctrica de 18 minutos en el gabinete de PC-1	MEDIA	UPS gabinete PC-1
H-07	Relojes de los equipos sin sincronizar	BAJA	CR-CC, CR-PC1, SW-EF2
H-08	Diagrama de red de 2019, sin tres equipos instalados después	BAJA	Documentación

> **Lo que funciona bien.** La configuración OSPF es coherente en los dos enrutadores y la conmutación al respaldo fue inmediata. Salvo el evento del km 21,3, la fibra mide dentro de los valores de diseño. Los gabinetes del centro de control están ordenados y etiquetados, y el personal de PC-1 conoce la red y colaboró en todas las pruebas.

5. Hallazgos en detalle

H-01 El enlace de respaldo no transporta el tráfico SCADA

CRÍTICA

Activo	Servicio L3VPN de respaldo, equipo terminal (CPE) del operador en el centro de control.
Descripción	El CPE del operador tiene una lista de acceso que solo permite el segmento administrativo 10.10.0.0/24. El segmento de operación 10.20.0.0/24, donde están las RTU y el PLC, se descarta. Al caer la fibra, el enrutamiento conmuta bien, pero los paquetes SCADA no llegan.
Por qué importa	Ante un corte de la fibra, el centro de control pierde la supervisión de PC-1 y EF-2 hasta que la fibra se repare. La prueba de ping no detecta el problema porque se hace desde el segmento administrativo.
Evidencia	Prueba de corte del 12/03/2026, 10:02:15 a 10:08:30. Detalle en el anexo A. • Ruta de respaldo instalada en menos de 1 s. • Ping de CR-CC a RTU-01: 0 % de pérdida. • Interrogaciones DNP3 (TCP 20000) del servidor SCADA: 0 respondidas de 412.
Recomendación	Solicitar al operador que agregue 10.20.0.0/24 a la lista de acceso del CPE, en ambos sentidos. Dejar la solicitud y la respuesta del operador por escrito.
Verificación	Repetir la prueba de corte en ventana de mantenimiento y confirmar que el servidor SCADA mantiene las interrogaciones a las cuatro RTU.

H-02 Equipos de oficina en la misma red que los controladores de proceso — ALTA

Activo	SW-PC1, VLAN 1.
Descripción	Nueve computadoras de oficina y una impresora de PC-1 están en la VLAN 1, la misma de RTU-01 a RTU-03 y del PLC de la planta. No hay ningún filtrado entre ellas.
Por qué importa	Un virus en una computadora de oficina, o un equipo mal configurado que sature la red, afecta directamente a los controladores. Las RTU aceptan comandos DNP3 de cualquier dirección del segmento.
Evidencia	Tabla de direcciones MAC de SW-PC1 y prueba de alcance: desde una computadora de oficina se abrió conexión al puerto 20000 de RTU-02.
Recomendación	Separar la red de operación y la administrativa en VLAN distintas y permitir entre ellas solo el tráfico necesario, con una lista de acceso en CR-PC1 o un cortafuegos. Tomar como referencia el modelo de zonas y conductos de la norma IEC 62443-3-2.
Verificación	Desde una computadora de oficina, intentar conectar a los puertos 20000 y 502 de las RTU: la conexión debe ser rechazada.

H-03 Margen óptico de 2,1 dB en la fibra CC–PC-1 — ALTA

Activo	Enlace de fibra CC–PC-1, hilos 1 y 2.
Descripción	La potencia recibida en CR-PC1 es de −20,9 dBm. La sensibilidad del módulo es de −23,0 dBm, lo que deja 2,1 dB de margen. En el acta de puesta en servicio de 2021 la potencia recibida era de −16,2 dBm.
Por qué importa	Con menos de 3 dB de margen, cualquier degradación adicional por suciedad en conectores, envejecimiento o una nueva curvatura puede dejar el enlace intermitente. Con H-01 sin corregir, eso equivale a perder la supervisión.
Evidencia	Trazas OTDR bidireccionales a 1310 y 1550 nm (anexo B). Hay un evento en el km 21,3 con 4,6 dB de pérdida a 1550 nm y 1,2 dB a 1310 nm. Que la pérdida sea mucho mayor en 1550 nm es típico de una curvatura del cable, no de un empalme defectuoso. Pérdida total medida a 1550 nm: 17,6 dB. Pérdida esperada según los valores de diseño: 12,8 dB.
Recomendación	Inspeccionar la tanquilla o el tramo aéreo más cercano al km 21,3 y corregir la curvatura. Limpiar e inspeccionar los conectores en ambos extremos.
Verificación	Nueva traza OTDR y medición de potencia. La pérdida del evento debe bajar de 0,3 dB y la potencia recibida debe quedar en −17 dBm o mejor.

H-04 Radioenlace PC-1–EF-2 con nivel de recepción 13 dB por debajo del diseño

MEDIA

Activo	Radios punto a punto en PC-1 y EF-2.
Descripción	El nivel de recepción es de −71 dBm en ambos extremos. El cálculo de diseño del enlace prevé −58 dBm. El registro interno de las radios muestra 47 cortes en los últimos 30 días, con 5 h 46 min fuera de servicio en total.
Por qué importa	Una disponibilidad de 99,2 % en 30 días deja a EF-2 sin supervisión unas 70 horas al año. Además, la banda de 5,8 GHz no es licenciada y puede recibir interferencias de otros equipos de la zona.
Evidencia	Lectura del nivel de recepción en la interfaz de gestión de cada radio. Inspección visual en EF-2: el soporte de la antena tiene un tornillo flojo y la antena está girada respecto a la marca de instalación.
Recomendación	Realinear y asegurar la antena de EF-2. Si después de alinear el nivel no supera −62 dBm, hacer un barrido de espectro en ambos extremos para descartar interferencia.
Verificación	Nivel de recepción de −60 dBm o mejor, y ningún corte en el registro de las radios durante 15 días.

H-05 La red no tiene monitoreo ni registro centralizado de eventos

MEDIA

Activo	Todos los equipos de red.
Descripción	SNMP está deshabilitado y los equipos guardan sus eventos solo en memoria. Las fallas se conocen cuando el operador de consola nota que una RTU dejó de reportar.
Por qué importa	Los problemas de H-03 y H-04 llevaban meses desarrollándose sin que nadie lo supiera. Con monitoreo se hubieran detectado al empezar.
Recomendación	Instalar un sistema de monitoreo en el centro de control y alertas por umbral para: estado de enlaces, potencia óptica recibida, nivel de recepción de las radios y uso de los enlaces. Enviar los eventos de todos los equipos a un servidor syslog.
Verificación	Desconectar un enlace de prueba y comprobar que la alerta llega al responsable designado.

H-06 Autonomía eléctrica de 18 minutos en el gabinete de PC-1 — MEDIA

Activo	UPS del gabinete de comunicaciones de PC-1.
Descripción	Con la carga actual, la autonomía medida de la UPS es de 18 minutos. La planta eléctrica de la instalación se arranca manualmente. CR-PC1 y SW-PC1 tienen una sola fuente de alimentación cada uno.
Por qué importa	Si el arranque de la planta eléctrica tarda más de 18 minutos, por ejemplo de noche, PC-1 queda incomunicada.
Recomendación	Ampliar el banco de baterías o conectar el gabinete a una transferencia automática. Definir la autonomía mínima con el área de operaciones.
Verificación	Prueba de descarga controlada con la carga real del gabinete.

H-07 Relojes de los equipos sin sincronizar — BAJA

Descripción	Ningún equipo usa NTP. Entre CR-CC y CR-PC1 hay 7 min 40 s de diferencia.
Por qué importa	Cuando se analiza una falla, los eventos de cada equipo no se pueden ordenar en el tiempo.
Recomendación	Configurar NTP en todos los equipos contra una misma fuente, preferiblemente la del sistema SCADA.

H-08 Diagrama de red de 2019, sin tres equipos instalados después — BAJA

Descripción	El último diagrama es de 2019. No incluye SW-EF2, la radio de EF-2 ni el CPE del servicio L3VPN.
Recomendación	El cliente recibe con este informe el diagrama actualizado y el inventario de equipos (anexo C). Se sugiere revisarlos después de cada cambio en la red.

6. Plan de corrección

El orden combina la criticidad con el esfuerzo. Las acciones 1 y 2 se pueden hacer en la primera semana y no requieren compras.

#	Hallazgo	Acción	Esfuerzo	Plazo sugerido
1	H-01	Corregir la lista de acceso del CPE y repetir la prueba de corte	Bajo	Inmediato

#	Hallazgo	Acción	Esfuerzo	Plazo sugerido
2	H-04	Realinear la antena de EF-2	Bajo	7 días
3	H-03	Ubicar y corregir la curvatura del km 21,3	Medio	30 días
4	H-02	Separar las redes de operación y administrativa	Medio	60 días
5	H-05, H-07	Monitoreo, syslog y NTP	Medio	60 días
6	H-06	Ampliar la autonomía eléctrica de PC-1	Alto	90 días
7	H-08	Mantener el diagrama y el inventario al día	Bajo	Permanente

7. Metodología y criterios

1. **Levantamiento.** Revisión de la documentación existente, entrevistas con el personal de operación y visita a las tres instalaciones.
2. **Revisión de configuración.** Configuración y tablas de enrutamiento, VLAN y direcciones MAC de los cuatro equipos, obtenidas con acceso de solo lectura.
3. **Mediciones.** OTDR bidireccional a 1310 y 1550 nm, potencia óptica con medidor calibrado, nivel de recepción de las radios, autonomía de la UPS.
4. **Prueba de corte.** Desconexión controlada de la fibra en ventana de mantenimiento, con medición del tráfico SCADA real y no solo del ping.

Valores de referencia para la fibra, tomados del proyecto original: 0,25 dB/km a 1550 nm, 0,1 dB por empalme, 0,5 dB por conector y 3 dB de margen mínimo.

Criticidad	Criterio	Qué implica
CRÍTICA	Puede dejar sin supervisión una instalación hoy, sin que concurra otra falla.	Corregir de inmediato.
ALTA	Puede dejar sin supervisión una instalación si se suma una falla probable.	Corregir en semanas.
MEDIA	Reduce la disponibilidad o retrasa la detección y la reparación de fallas.	Planificar en el trimestre.
BAJA	Dificulta la operación o el análisis, sin efecto directo en la disponibilidad.	Atender con las tareas de mantenimiento.

8. Limitaciones

Los resultados describen la red durante la semana del trabajo de campo. No se evaluó la red interna del operador del servicio L3VPN ni los equipos del sistema SCADA. La revisión de seguridad se limitó a la segmentación y no sustituye una prueba de intrusión. Las mediciones del radioenlace no incluyeron un barrido de espectro.

9. Anexos

Anexo A. Registro de la prueba de corte (extracto)

```
12/03/2026  Ventana autorizada 10:00–10:30   Testigo: operador de consola, turno A

10:02:15  CR-CC   Te0/1 desconectada (fibra hacia PC-1)
10:02:15  CR-CC   %OSPF-5-ADJCHG: Nbr 10.255.0.2 on Te0/1 from FULL to DOWN
10:02:15  CR-CC   Ruta 10.20.0.0/24 vía 172.31.4.1 (estática, AD 250) instalada
10:02:20  CR-CC   ping 10.20.0.11 (RTU-01) origen 10.10.0.1: 100/100 OK, prom. 48 ms
10:02:20  SCADA   Interrogación DNP3 RTU-01..RTU-04: sin respuesta
10:08:29  SCADA   Interrogaciones acumuladas sin respuesta: 412 de 412
10:08:30  CR-CC   Te0/1 reconectada; OSPF FULL a las 10:08:41
10:08:44  SCADA   RTU-01..RTU-04 en línea

Repetición del ping con origen 10.20.0.1: 0/100 OK. Lista de acceso del CPE
leída por el operador por teléfono: permit ip 10.10.0.0 0.0.0.255 any.
```

Anexo B. Resumen de las trazas OTDR, enlace CC–PC-1

Evento	Distancia (km)	Pérdida 1310 nm (dB)	Pérdida 1550 nm (dB)	Observación
Conector CC	0,00	0,42	0,38	Dentro de valor
Empalme 7	12,04	0,08	0,06	Dentro de valor
No reflectivo	**21,31**	**1,20**	**4,60**	**Curvatura probable**
Empalme 15	26,88	0,11	0,09	Dentro de valor
Conector PC-1	38,42	0,47	0,44	Dentro de valor
Total del enlace	38,42	16,9	17,6	Esperado a 1550 nm: 12,8

Se muestran solo los eventos relevantes. El anexo completo incluye las trazas de los 22 empalmes en ambos sentidos.

Anexo C. Diagrama actualizado e inventario de equipos

Se entregan como archivos aparte: diagrama en formato editable y PDF, e inventario en hoja de cálculo con modelo, número de serie, versión de software, ubicación y responsable de cada equipo.

10. Control del documento

Revisión	Fecha	Descripción
0	20/03/2026	Borrador para revisión del cliente
1	27/03/2026	Incorpora comentarios del cliente sobre H-06 y los plazos del plan

Elaborado por
Ingeniero de redes
Nombre, firma y n.º CIV

Revisado por
Ingeniero de redes
Nombre, firma y n.º CIV

Recibido por
Cliente
Nombre, cargo y firma