

REPORTE EJECUTIVO

Diagnóstico de infraestructura de telecomunicaciones y TI

Corporativo Demo S.A. de C.V. (datos ficticios)

Oficinas centrales, Ciudad de México

FECHA DEL LEVANTAMIENTO

14 de octubre de 2026

FOLIO

TV-2026-DEMO

DIRIGIDO A

Laura Méndez, Gerente de TI

PREPARADO POR

Gustavo Sánchez Bonilla, TelecomVerse

ÁREAS EVALUADAS

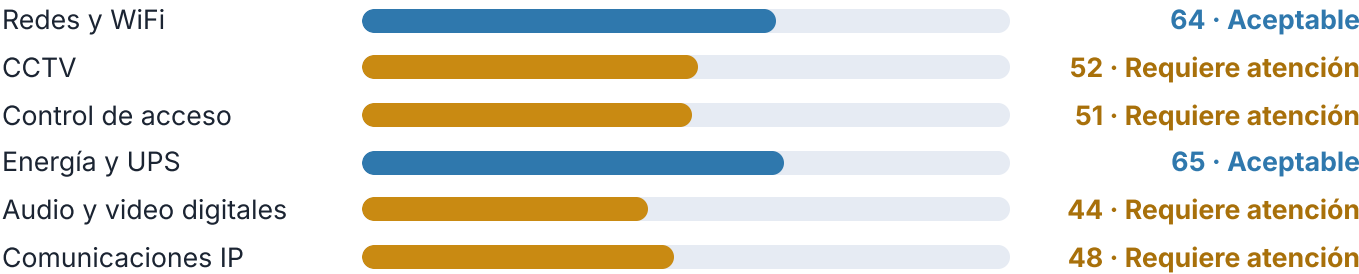
Redes y WiFi, CCTV, Control de acceso,
Energía y UPS, Audio y video digitales,
Comunicaciones IP

Documento confidencial para uso exclusivo del cliente. Diagnóstico antes que inversión.

Estado general de la infraestructura



Resultado por área



Lectura ejecutiva

Se realizó un levantamiento en sitio en Oficinas centrales, Ciudad de México con alcance en Redes y WiFi, CCTV, Control de acceso, Energía y UPS, Audio y video digitales y Comunicaciones IP. El índice general de madurez de la infraestructura es 54 de 100 (requiere atención).

El área mejor resuelta es Energía y UPS (65/100). La que requiere atención primero es Audio y video digitales (44/100).

Se identificaron 51 hallazgos: 5 críticos, 6 altos, 23 medios y 17 bajos. Los críticos y altos deben atenderse en los próximos 30 días porque comprometen la continuidad o la seguridad de la operación.

Cinco prioridades

SEVERIDAD	ÁREA	HALLAZGO
CRÍTICO	CCTV	El NVR está publicado en internet con redirección de puertos 80 y 8000.
CRÍTICO	Control de acceso	Las credenciales son clonables o usan llaves por defecto: se pueden copiar en segundos con equipo de bajo costo.
CRÍTICO	Comunicaciones IP	Las troncales SIP operan sin SBC ni control en el firewall: expuestas a fraude y ataques.
CRÍTICO	Comunicaciones IP	Hay contraseñas débiles o SIP expuesto a internet: riesgo de fraude telefónico con costos elevados.
CRÍTICO	CCTV	El NVR está publicado en internet con redirección de puertos: expuesto a escaneos y ataques automatizados.

Redes y WiFi

Alineado a: Network Health Assessment



Acceptable

Riesgo evaluado en sitio: Medio
Cobertura de datos: 100%

2
ENLACES DE INTERNET

9
SWITCHES

14
ACCESS POINTS

260
DISPOSITIVOS EN WIFI

Fortinet 60E
FIREWALL

Lo que funciona

- ✓ Firewall con licencias y soporte vigentes
- ✓ Segmentación por VLAN
- ✓ Cableado ordenado y etiquetado
- ✓ Monitoreo con alertas
- ✓ Contraseñas de administración cambiadas

Brechas y recomendaciones

SEVERIDAD	HALLAZGO	RECOMENDACIÓN
MEDIO	Hay más de un enlace, pero no hay conmutación automática: la recuperación depende de una persona.	Contratar un segundo enlace de otro proveedor y configurar failover automático en el firewall o router.
MEDIO	No existe diagrama de red ni inventario actualizado: el conocimiento depende de personas.	Levantar y mantener diagrama lógico y físico, e inventario con modelo, serie, firmware y garantía.
MEDIO	No se respaldan las configuraciones: ante una falla de equipo, la recuperación toma horas o días.	Programar respaldos automáticos de configuración y guardarlos fuera del equipo.
MEDIO	El firmware de los equipos está desactualizado y expone vulnerabilidades conocidas.	Definir un calendario de actualización de firmware con ventana de mantenimiento y plan de reversa.
BAJO	La topología es mixta o no está documentada, lo que complica el diagnóstico y el crecimiento.	Rediseñar hacia estrella o core + acceso, con enlaces redundantes en los puntos críticos.
BAJO	El presupuesto PoE tiene poco margen o no se ha verificado; un equipo nuevo puede saturarlo.	Calcular el consumo real contra el presupuesto de cada switch y redistribuir o ampliar la capacidad.
BAJO	Se reportan problemas puntuales de WiFi que conviene medir y corregir.	Realizar un sitio survey WiFi con la ocupación real y rediseñar cobertura, canales y densidad de APs.

SEVERIDAD	HALLAZGO	RECOMENDACIÓN
BAJO	Algunos equipos del inventario están en mal estado o fuera de línea.	Reparar o reemplazar los equipos en mal estado y programar su renovación por ciclo de vida.

Inventario

25 equipos o elementos 14 buenos 10 regulares 1 en mal estado o fuera de línea

EQUIPO	MARCA Y MODELO	UBICACIÓN	CANT.	ESTADO	NOTAS
Switch	D-Link DGS-1210	Bodega	1	Fuera de línea	Sin energía

Observaciones del consultor

La red creció por fases sin diseño y no cuenta con diagrama actualizado. Hay un solo proveedor de internet efectivo, porque el segundo enlace no conmuta solo.



Requiere atención
Riesgo evaluado en sitio: Alto
Cobertura de datos: 100%

42
CÁMARAS

3
FUERA DE LÍNEA

26 / 30 días
RETENCIÓN REAL / REQUERIDA

24 TB
ALMACENAMIENTO

Hikvision
SISTEMA

Lo que funciona

- ✓ Discos con redundancia
- ✓ NVR y switches PoE con respaldo de energía
- ✓ Contraseñas de fábrica cambiadas

Brechas y recomendaciones

SEVERIDAD	HALLAZGO	RECOMENDACIÓN
CRÍTICO	El NVR está publicado en internet con redirección de puertos: expuesto a escaneos y ataques automatizados.	Cerrar los puertos y acceder por VPN o por la nube del fabricante con autenticación reforzada.
MEDIO	Hay cámaras sin imagen o fuera de línea que reducen la cobertura.	Restablecer las cámaras fuera de servicio y activar alertas de pérdida de video.
MEDIO	La retención real está ligeramente por debajo del objetivo.	Recalcular el almacenamiento (resolución, códec, modo de grabación) y ampliar discos o ajustar la grabación.
MEDIO	No se ha verificado el estado de los discos.	Reemplazar discos con alertas, usar discos para videovigilancia y verificar SMART periódicamente.
MEDIO	Se identificaron puntos ciegos en áreas relevantes.	Revisar el plano de cobertura y reubicar o agregar cámaras en accesos, perímetro y áreas críticas.
MEDIO	No hay procedimiento para exportar y resguardar evidencia.	Definir un procedimiento de exportación, custodia y entrega de evidencia con responsables.
MEDIO	Las cámaras comparten red con los usuarios: una cámara vulnerada da acceso a la red interna.	Aislar las cámaras en una VLAN con acceso restringido al NVR.
MEDIO	Una parte relevante de los equipos inventariados está en mal estado o fuera de línea.	Reparar o reemplazar los equipos en mal estado y programar su renovación por ciclo de vida.
BAJO	Se usa un códec poco eficiente que consume más almacenamiento y ancho de banda.	Habilitar H.265 o H.265+ donde NVR y cámaras lo soporten.

SEVERIDAD	HALLAZGO	RECOMENDACIÓN
BAJO	La imagen nocturna es mala: el video no sirve para identificar personas ni placas.	Ajustar iluminación, IR y configuración de exposición; sustituir cámaras con baja sensibilidad.

Hallazgos adicionales en sitio

SEVERIDAD	HALLAZGO	RECOMENDACIÓN
CRÍTICO	El NVR está publicado en internet con redirección de puertos 80 y 8000.	Cerrar los puertos de inmediato y acceder únicamente por VPN.

Inventario

43 equipos o elementos 30 buenos 1 regulares 12 en mal estado o fuera de línea

EQUIPO	MARCA Y MODELO	UBICACIÓN	CANT.	ESTADO	NOTAS
Cámaras bala 4 MP	Hikvision	Perímetro	6	Malo	Sin imagen
Cámaras bala 4 MP	Hikvision	Estacionamiento	6	Fuera de línea	

Observaciones del consultor

El NVR está accesible desde internet. Se recomienda cerrar puertos de inmediato.

Control de acceso

Alineado a: Security Gap Analysis



Requiere atención
Riesgo evaluado en sitio: Alto
Cobertura de datos: 100%

24
PUNTOS CONTROLADOS

2
FUERA DE SERVICIO

210
CREDENCIALES ACTIVAS

ZKTeco ZKBio
PLATAFORMA

EM4100 (125 kHz)
CREDENCIAL

Lo que funciona

- ✓ Doble factor en áreas críticas
- ✓ Cifrado entre controladora, servidor y clientes
- ✓ Liberación de puertas con la alarma contra incendio
- ✓ Respaldo de base de datos y configuración
- ✓ Controladoras y lectores IP en VLAN separada
- ✓ Contraseñas de fábrica cambiadas

Brechas y recomendaciones

SEVERIDAD	HALLAZGO	RECOMENDACIÓN
CRÍTICO	Las credenciales son clonables o usan llaves por defecto: se pueden copiar en segundos con equipo de bajo costo.	Migrar a credenciales DESFire EV2 o EV3 con llaves propias, empezando por accesos críticos.
ALTO	Los lectores usan Wiegand u otro protocolo sin cifrado: la señal puede interceptarse o suplantarse.	Migrar a OSDP v2 con Secure Channel (o lectores IP) en accesos críticos y planear el resto por fases.
ALTO	Las credenciales no se dan de baja al salir un colaborador: personal ex colaborador conserva acceso.	Conectar altas y bajas con Recursos Humanos y auditar credenciales activas cada mes.
MEDIO	La comunicación entre lector y controladora no está cifrada.	Activar OSDP Secure Channel o reemplazar los lectores que no lo soporten.
MEDIO	Se usan las llaves del fabricante: cualquiera con el mismo modelo de lector puede leer y emitir credenciales.	Generar llaves propias, respaldarlas y custodiarlas con un responsable definido.
MEDIO	Controladoras y cerraduras no tienen respaldo: un apagón deja puertas abiertas o bloqueadas según el tipo de cerradura.	Respaldar controladoras y fuentes con UPS o batería y definir el comportamiento fail-safe o fail-secure por puerta.
MEDIO	No se prueba periódicamente la apertura de emergencia.	Programar pruebas trimestrales y registrar resultados.

SEVERIDAD	HALLAZGO	RECOMENDACIÓN
BAJO	Una parte importante de los puntos de acceso está fuera de servicio o sin lector.	Reparar o reponer lectores y cerraduras, y priorizar accesos críticos.
BAJO	No se pudo confirmar el estado del firmware.	Actualizar firmware con plan de pruebas y respaldo de configuración previo.
BAJO	Algunos equipos del inventario están en mal estado o fuera de línea.	Reparar o reemplazar los equipos en mal estado y programar su renovación por ciclo de vida.
BAJO	Los biométricos presentan fallas o rechazos frecuentes.	Revisar ubicación, iluminación y mantenimiento, o evaluar otra modalidad biométrica.

Inventario

30 equipos o elementos 6 buenos 22 regulares 2 en mal estado o fuera de línea

EQUIPO	MARCA Y MODELO	UBICACIÓN	CANT.	ESTADO	NOTAS
Lectores	ZKTeco	Torniquete	2	Malo	

Observaciones del consultor

Las credenciales de proximidad se pueden clonar. Se identificaron 14 tarjetas activas de personal que ya no labora.

Energía y UPS

Alineado a: UPS Critical Infrastructure Review



Acceptable
Riesgo evaluado en sitio: Alto
Cobertura de datos: 100%

2
UPS INSTALADAS

12 min
AUTONOMÍA

78 %
CARGA

Más de 4 años
BATERÍAS

APC Smart-UPS 3 kVA
EQUIPO

Lo que funciona

- ✓ Estado visible de baterías
- ✓ Voltaje fase a neutro en rango
- ✓ Tablero y circuitos del cuarto
- ✓ Temperatura del cuarto
- ✓ Protección del cuarto
- ✓ Equipos del inventario en buen estado

Brechas y recomendaciones

SEVERIDAD	HALLAZGO	RECOMENDACIÓN
ALTO	Las baterías superan 4 años: es probable que no entreguen la autonomía esperada ni resistan una falla real.	Programar cambio de baterías y validar autonomía con prueba de descarga.
MEDIO	La autonomía es justa (10 a 14 minutos).	Recalcular autonomía con la carga real y ampliar baterías o capacidad de UPS.
MEDIO	Existe tierra física pero no se ha medido.	Medir la resistencia de la tierra física y corregir o instalar sistema de tierras conforme a norma.
MEDIO	El voltaje neutro a tierra está entre 1 y 2 V: vigilar.	Revisar neutro y tierra del tablero y las cargas, y corregir antes de ampliar equipos.
MEDIO	No hay mantenimiento preventivo documentado.	Contratar un programa de mantenimiento preventivo semestral con prueba de descarga.
BAJO	La UPS opera entre 70% y 80% de carga, con poco margen de crecimiento.	Redistribuir cargas, retirar cargas no críticas o aumentar capacidad.
BAJO	El aire es compartido: puede dejar de operar cuando el edificio lo apaga.	Instalar aire acondicionado dedicado con control de temperatura y alertas.
BAJO	Sin planta de emergencia la autonomía depende solo de las baterías.	Evaluar planta con transferencia automática si la operación exige continuidad prolongada.

Hallazgos adicionales en sitio

SEVERIDAD	HALLAZGO	RECOMENDACIÓN
MEDIO	El cuarto de equipos comparte aire acondicionado con la oficina y se apaga por las noches.	Instalar aire dedicado con alarma de temperatura.

Inventario

2 equipos o elementos 0 buenos 2 regulares 0 en mal estado o fuera de línea

Observaciones del consultor

Las dos UPS tienen más de 5 años con las baterías originales.

8

ESPACIOS AV

Teams, Zoom

PLATAFORMAS

Controles individuales

CONTROL

Lo que funciona

- ✓ Transporte de señal ordenado

Brechas y recomendaciones

SEVERIDAD	HALLAZGO	RECOMENDACIÓN
ALTO	Los usuarios no pueden iniciar una reunión sin ayuda de TI: pérdida de tiempo y mala percepción del servicio.	Estandarizar el arranque de reunión de un toque y el método de compartir pantalla en todas las salas.
MEDIO	Se reportan problemas frecuentes en las salas que conviene corregir.	Atender primero audio y conexión; son lo que más pesa en la experiencia de una reunión.
MEDIO	Las salas presentan varios problemas de entorno (eco, ruido, luz o ubicación de pantallas).	Aplicar tratamiento acústico, control de luz y reubicar pantallas según la regla de visión 4-6-8.
MEDIO	Una parte relevante de los equipos inventariados está en mal estado o fuera de línea.	Reparar o reemplazar los equipos en mal estado y programar su renovación por ciclo de vida.
BAJO	Los controles son individuales: la experiencia cambia de sala a sala.	Unificar el control de salas con una plataforma estándar y plantillas por tipo de sala.

Inventario

6 equipos o elementos 4 buenos 1 regulares 1 en mal estado o fuera de línea

EQUIPO	MARCA Y MODELO	UBICACIÓN	CANT.	ESTADO	NOTAS
Pantalla 65"	Samsung	Sala 5	1	Malo	

Observaciones del consultor

Las salas de juntas del piso 2 tienen eco marcado y requieren tratamiento acústico.

Comunicaciones IP

Alineado a: IP Communications Assessment



Requiere atención
Riesgo evaluado en sitio: Alto
Cobertura de datos: 100%

160
EXTENSIONES

12
CANALES SIP

PBX local
PLATAFORMA

Asterisk 16 (FreePBX)
PBX

SIP
TRONCALES

Lo que funciona

- ✓ QoS y VLAN de voz
- ✓ Equipos del inventario en buen estado

Brechas y recomendaciones

SEVERIDAD	HALLAZGO	RECOMENDACIÓN
CRÍTICO	Las troncales SIP operan sin SBC ni control en el firewall: expuestas a fraude y ataques.	Colocar un SBC o configurar el firewall con listas de IP del proveedor y límites de llamadas.
CRÍTICO	Hay contraseñas débiles o SIP expuesto a internet: riesgo de fraude telefónico con costos elevados.	Cerrar el puerto SIP al público, usar contraseñas robustas y límites de llamadas internacionales.
ALTO	No hay respaldo ante la caída del internet o del PBX: la empresa pierde comunicación externa.	Implementar respaldo (segundo enlace, troncal alterna, desvío automático o PBX en alta disponibilidad).
BAJO	No hay soporte formal del PBX o no se pudo confirmar su vigencia.	Renovar soporte o planear migración si la versión ya no tiene soporte.
BAJO	Se reporta un problema de calidad de voz que conviene medir.	Medir jitter, pérdida y latencia, y corregir QoS, códecs y enlace.
BAJO	Los canales contratados parecen pocos para el número de extensiones: validar con la calculadora de troncales SIP (Erlang B).	Validar con la calculadora de troncales SIP (Erlang B) contra tu tráfico en hora pico.

Hallazgos adicionales en sitio

SEVERIDAD	HALLAZGO	RECOMENDACIÓN
ALTO	Intentos de registro SIP desde direcciones del exterior en la bitácora de Asterisk.	Restringir SIP al proveedor, instalar fail2ban y limitar llamadas internacionales.

Inventario

161 equipos o elementos 160 buenos 1 regulares 0 en mal estado o fuera de línea

Observaciones del consultor

El puerto SIP está abierto a internet. Se detectaron intentos de registro desde el exterior.

Plan de acción priorizado

Las acciones se ordenan por severidad. Las fechas se definen con el cliente en la sesión de revisión.

Primeros 30 días críticos y altos

1. **CCTV:** Cerrar los puertos de inmediato y acceder únicamente por VPN.
2. **Control de acceso:** Migrar a credenciales DESFire EV2 o EV3 con llaves propias, empezando por accesos críticos.
3. **Comunicaciones IP:** Colocar un SBC o configurar el firewall con listas de IP del proveedor y límites de llamadas.
4. **Comunicaciones IP:** Cerrar el puerto SIP al público, usar contraseñas robustas y límites de llamadas internacionales.
5. **CCTV:** Cerrar los puertos y acceder por VPN o por la nube del fabricante con autenticación reforzada.
6. **Comunicaciones IP:** Restringir SIP al proveedor, instalar fail2ban y limitar llamadas internacionales.
7. **Control de acceso:** Migrar a OSDP v2 con Secure Channel (o lectores IP) en accesos críticos y planear el resto por fases.
8. **Control de acceso:** Conectar altas y bajas con Recursos Humanos y auditar credenciales activas cada mes.
9. **Energía y UPS:** Programar cambio de baterías y validar autonomía con prueba de descarga.
10. **Audio y video digitales:** Estandarizar el arranque de reunión de un toque y el método de compartir pantalla en todas las salas.
11. **Comunicaciones IP:** Implementar respaldo (segundo enlace, troncal alterna, desvío automático o PBX en alta disponibilidad).

1. **Energía y UPS:** Instalar aire dedicado con alarma de temperatura.
2. **Redes y WiFi:** Contratar un segundo enlace de otro proveedor y configurar failover automático en el firewall o router.
3. **CCTV:** Restablecer las cámaras fuera de servicio y activar alertas de pérdida de video.
4. **CCTV:** Recalcular el almacenamiento (resolución, códec, modo de grabación) y ampliar discos o ajustar la grabación.
5. **CCTV:** Reemplazar discos con alertas, usar discos para videovigilancia y verificar SMART periódicamente.
6. **Energía y UPS:** Recalcular autonomía con la carga real y ampliar baterías o capacidad de UPS.
7. **Energía y UPS:** Medir la resistencia de la tierra física y corregir o instalar sistema de tierras conforme a norma.
8. **Energía y UPS:** Revisar neutro y tierra del tablero y las cargas, y corregir antes de ampliar equipos.
9. **Audio y video digitales:** Atender primero audio y conexión; son lo que más pesa en la experiencia de una reunión.
10. **Redes y WiFi:** Levantar y mantener diagrama lógico y físico, e inventario con modelo, serie, firmware y garantía.
11. **Redes y WiFi:** Programar respaldos automáticos de configuración y guardarlos fuera del equipo.
12. **Redes y WiFi:** Definir un calendario de actualización de firmware con ventana de mantenimiento y plan de reversa.

y 11 acciones más en los capítulos.

3 a 6 meses severidad baja y optimización

1. **Redes y WiFi:** Rediseñar hacia estrella o core + acceso, con enlaces redundantes en los puntos críticos.
2. **Redes y WiFi:** Calcular el consumo real contra el presupuesto de cada switch y redistribuir o ampliar la capacidad.
3. **Redes y WiFi:** Realizar un sitio survey WiFi con la ocupación real y rediseñar cobertura, canales y densidad de APs.
4. **Redes y WiFi:** Reparar o reemplazar los equipos en mal estado y programar su renovación por ciclo de vida.
5. **Control de acceso:** Reparar o reponer lectores y cerraduras, y priorizar accesos críticos.
6. **Control de acceso:** Actualizar firmware con plan de pruebas y respaldo de configuración previo.
7. **Control de acceso:** Reparar o reemplazar los equipos en mal estado y programar su renovación por ciclo de vida.
8. **Energía y UPS:** Redistribuir cargas, retirar cargas no críticas o aumentar capacidad.
9. **Energía y UPS:** Instalar aire acondicionado dedicado con control de temperatura y alertas.
10. **Audio y video digitales:** Unificar el control de salas con una plataforma estándar y plantillas por tipo de sala.
11. **Comunicaciones IP:** Renovar soporte o planear migración si la versión ya no tiene soporte.
12. **Comunicaciones IP:** Medir jitter, pérdida y latencia, y corregir QoS, códecs y enlace.

y 5 acciones más en los capítulos.

Cómo leer este reporte

Nivel de madurez

80 a 100 · Sólido Controles en buen estado.	60 a 79 · Aceptable Funciona, con brechas puntuales.	40 a 59 · Requiere atención Riesgo de falla o incidente.	0 a 39 · Crítico Operación comprometida.
---	--	--	--

Metodología

El puntaje de cada área es el cumplimiento ponderado de los controles verificados en sitio (88 controles en las áreas de este reporte): cumple suma 1, cumple parcialmente suma 0.5 y no cumple suma 0. Los controles que afectan la continuidad o la seguridad pesan más. Los controles sin información no se promedian y se reportan como cobertura de datos. El índice general es el promedio simple de las áreas evaluadas.

Limitaciones

El levantamiento es no intrusivo y se basa en observación visual, mediciones puntuales y lo declarado por el personal del cliente el día de la visita. No incluye pruebas de penetración, mediciones de laboratorio ni validación de cada punto de red o de cada equipo. Los hallazgos reflejan la condición del sitio en esa fecha. Este reporte no sustituye un diseño de ingeniería de detalle ni constituye una certificación.

Siguientes pasos

1. Sesión de revisión de este reporte con TI y dirección (60 minutos).
2. Validar prioridades y alcance de la remediación.
3. Plan de implementación por fases, con responsables y fechas.
4. Reevaluación a los 90 días para medir el avance del índice.

Hablemos de tu plan de acción

Agenda la sesión de revisión de este reporte con TelecomVerse.

Gustavo Sánchez Bonilla · contacto@telecomverse.net · 55 6200 5855

calendly.com/diagnostico-telecomverse