



REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR PARA LA
EDUCACIÓN UNIVERSITARIA,
CIENCIA Y TECNOLOGÍA
INSTITUTO UNIVERSITARIO POLITÉCNICO
“SANTIAGO MARIÑO”
EXTENSIÓN CABIMAS

**"Auditoria Informática al Departamento de
Infraestructura de Red y Comunicaciones de la
Empresa TeleNET Solutions C.A"**

Autores:

Fiorella David Cl: 30.278.024

Juan Marcano Cl: 30.423.647

María Yoris Cl: 29.519.479

Victor Ysea Cl: 31.283.152

Auditoria y Evaluación de Sistemas Sección “A”

Cabimas, Febrero 2026

INDICE

	Pág.
DESARROLLO	1
CONTEXTOUALIZACIÓN DE LA EMPRESA	1
Descripción de la Empresa.....	1
Misión.....	1
Visión.....	1
Área a Auditar	2
FASE I: ESTUDIO INICIAL DEL ENTORNO AUDITABLE	2
Organización y Organigrama.....	2
Departamentos y Funciones.....	3
Relaciones Jerárquicas y Funcionales	3
Flujos de Información	4
Puestos de Trabajo	5
Situación Geográfica de los Sistemas.....	5
Arquitectura y Configuración de Hardware y Software	6
Inventario de Hardware y Software	7
Comunicación y Redes de Comunicación.....	8
Aplicaciones, Bases de Datos y Ficheros.....	8
FASE II: ALCANCES Y OBJETIVOS DE LA AUDITORÍA.....	9
Alcance de la Auditoría	9
Objetivos de la Auditoría	10
FASE III: PLAN Y PROGRAMAS DE TRABAJO	10
Tipo de Auditoría	10

Calendario de Actividades.....	11
Prioridades de Materias Auditables	11
Asignación de Tareas por Integrante del Equipo Auditor	12
Programación Detallada de Actividades.....	13
FASE IV: DETERMINACIÓN DE RECURSOS NECESARIOS	13
Recursos Humanos	13
Recursos Financieros.....	14
Recursos Tecnológicos	15
Recursos Materiales y Logísticos.....	15

DESARROLLO

CONTEXTUALIZACIÓN DE LA EMPRESA

Descripción de la Empresa

TeleNET Solutions C.A. es una empresa venezolana de telecomunicaciones fundada en 2010, dedicada a proveer servicios de conectividad, internet corporativo, telefonía IP y soluciones de redes empresariales. La empresa atiende a más de 500 clientes corporativos en todo el territorio nacional, incluyendo entidades bancarias, empresas de retail, instituciones educativas y organismos gubernamentales. La sede principal ubicada en Caracas cuenta con una plantilla de 65 empleados y alberga el Data Center principal de la organización, desde donde se gestionan todos los servicios críticos de la empresa.

Misión

Proveer soluciones integrales de telecomunicaciones con los más altos estándares de calidad, garantizando la conectividad y continuidad operativa de nuestros clientes mediante tecnología de vanguardia y un equipo humano altamente capacitado.

Visión

Ser la empresa líder en soluciones de telecomunicaciones en Venezuela para el año 2028, reconocida por la excelencia en el servicio, la innovación tecnológica y el compromiso con la satisfacción del cliente.

Área a Auditar

La presente auditoría se enfocará en el Departamento de Infraestructura de Red y Comunicaciones de la sede principal de Caracas, el cual es responsable de la administración, mantenimiento y operación de toda la infraestructura de red de la empresa, incluyendo el Data Center principal, los equipos de networking, los enlaces de comunicación y los sistemas de monitoreo. Este departamento cuenta con 12 empleados y gestiona más de 200 equipos de red activos, siendo un área crítica para la continuidad operativa de la empresa y la prestación de servicios a los clientes.

FASE I: ESTUDIO INICIAL DEL ENTORNO AUDITABLE

Organización y Organigrama

TeleNET Solutions C.A. presenta una estructura organizacional de tipo jerárquico-funcional, encabezada por la Gerencia General y distribuida en lo que serían un total de cinco gerencias principales. A continuación, se presenta el organigrama oficial de la organización:



Departamentos y Funciones

A continuación, se describen las funciones de cada departamento que conforma la Gerencia de Infraestructura (área auditada):

DEPARTAMENTO	FUNCIONES PRINCIPALES
Administración de Red	<ul style="list-style-type: none">• Configuración y mantenimiento de equipos de red (routers, switches, firewalls)• Gestión de direccionamiento IP• Administración de VLANs y segmentación de red• Implementación de políticas de QoS• Documentación de topología de red
Data Center	<ul style="list-style-type: none">• Administración de servidores físicos y virtuales• Gestión de almacenamiento y respaldos• Mantenimiento de sistemas de climatización• Control de acceso físico al Data Center• Monitoreo de disponibilidad de servicios
Seguridad de Red	<ul style="list-style-type: none">• Administración de firewalls y sistemas IDS/IPS• Gestión de VPNs corporativas• Monitoreo de amenazas y vulnerabilidades• Implementación de políticas de seguridad• Respuesta a incidentes de seguridad

Relaciones Jerárquicas y Funcionales

El equipo auditor verificó las relaciones jerárquicas dentro del área de Infraestructura de Red y Comunicaciones:

CARGO	REPORTA A	SUPERVISA A
Gerente de Infraestructura	Gerente General	Coordinadores de área
Coord. Administración de Red	Gerente de Infraestructura	Técnicos de Red (3)

Coord. Data Center	Gerente de Infraestructura	Técnicos de Data Center (2)
Coord. Seguridad de Red	Gerente de Infraestructura	Analistas de Seguridad (2)

Flujos de Información

Se identificaron los siguientes flujos de información dentro del departamento a auditar:

Flujo Vertical Descendente: Las políticas, procedimientos y directrices se comunican desde la Gerencia de Infraestructura hacia los coordinadores y técnicos mediante correo electrónico institucional y reuniones semanales.

Flujo Vertical Ascendente: Los reportes de incidentes, métricas de rendimiento y solicitudes de recursos se elevan desde los técnicos hacia la gerencia mediante el sistema de tickets ServiceDesk y reportes mensuales.

Flujo Horizontal: Existe comunicación constante entre los tres departamentos del área para coordinar cambios en la red, ventanas de mantenimiento y respuesta a incidentes. Se utiliza un grupo de Microsoft Teams para comunicación inmediata.

Hallazgo: La documentación de cambios en la infraestructura no sigue un flujo formalizado. Los cambios menores se realizan sin registro previo en el sistema de gestión de cambios.

Puestos de Trabajo

El área de Infraestructura de Red cuenta con los siguientes puestos de trabajo:

PUESTO	N° DE PERSONAS	FUNCIONES REALES	OBSERVACIONES
Gerente de Infraestructura	1	Dirección estratégica del área	Conforme
Coord. Administración de Red	1	Supervisión de red y equipos	Conforme
Coord. Data Center	1	Gestión del centro de datos	Conforme
Coord. Seguridad de Red	1	Gestión de seguridad perimetral	Conforme
Técnico de Red Senior	2	Config. y mantenimiento de red	Funciones duplicadas
Técnico de Red Junior	3	Soporte de red nivel 1 y 2	Conforme
Analista de Seguridad	3	Monitoreo y respuesta a incidentes	1 vacante sin cubrir

Total de personal en el área: 12 empleados (11 activos + 1 vacante)

Situación Geográfica de los Sistemas

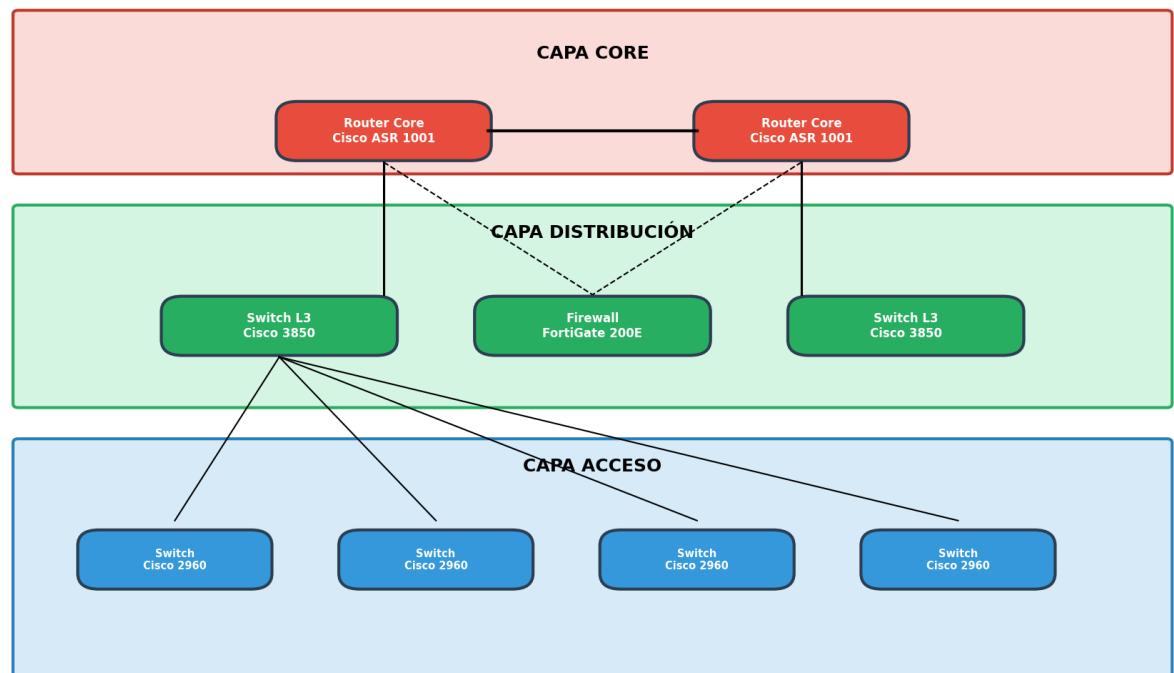
La presente auditoría se centra exclusivamente en la sede principal de Caracas, donde se encuentra el Data Center principal de la organización:

UBICACIÓN	TIPO	RESPONSABLE	ESTÁNDARES
Caracas (Sede Principal)	Data Center Principal	Coord. Data Center	ISO 27001 (parcial)

A su vez, el centro de datos se encuentra ubicado estratégicamente en el piso 12 de la Torre Empresarial Delta, contando con una superficie operativa de 80 m² de espacio técnico diseñada para albergar una infraestructura de seis racks de 42U. Para garantizar la continuidad operativa y la integridad del hardware, las instalaciones disponen de un sistema de climatización compuesto por dos unidades de aire de precisión, respaldadas por un esquema energético de alta disponibilidad que integra UPS redundantes y una planta eléctrica propia. Finalmente, la seguridad física del recinto está gestionada mediante un riguroso control de acceso multicapa que combina tecnología biométrica y tarjetas de proximidad.

Arquitectura y Configuración de Hardware y Software

La arquitectura de red de TeleNET Solutions está diseñada en un modelo de tres capas (Core, Distribución y Acceso) con los siguientes componentes principales:



Inventario de Hardware y Software

Inventario de Hardware

EQUIPO	MARCA/MODELO	CANTIDAD	UBICACIÓN	ESTADO
Router Core	Cisco ASR 1001-X	2	Data Center	Operativo
Switch L3	Cisco Catalyst 3850	4	Data Center	Operativo
Switch L2	Cisco Catalyst 2960-X	18	Data Center / Pisos	2 con fallas
Firewall	FortiGate 200E	2	Data Center	Operativo
Servidor Rack	Dell PowerEdge R740	8	Data Center	Operativo
Servidor Rack	HP ProLiant DL380	4	Data Center	2 obsoletos
Storage SAN	Dell EMC Unity 300	1	Data Center	Operativo
UPS	APC Smart-UPS 10kVA	2	Data Center	1 sin mantenimiento
Access Point	Cisco Aironet 2800	12	Pisos oficina	Operativo
Patch Panel	Panduit 48 puertos	8	Data Center	Operativo
Rack 42U	APC NetShelter	6	Data Center	Operativo

Inventario de Software

SOFTWARE	VERSIÓN	LICENCIAS	TIPO	ESTADO
Windows Server	2019 Datacenter	8	Sistema Operativo	Vigente
VMware vSphere	7.0 U3	1 (Enterprise)	Virtualización	Vigente
Veeam Backup	11.0	1	Respaldo	Vigente
FortiAnalyzer	7.0	1	Monitoreo Seguridad	Vigente
PRTG Network Monitor	22.1	500 sensores	Monitoreo Red	Vigente
Cisco IOS	15.2(4)	N/A	Firmware	Desactualizado
Microsoft 365	Business Premium	65	Productividad	Vigente
ServiceDesk Plus	11.0	25 técnicos	Mesa de Ayuda	Vigente

Nessus Professional	10.0	1	Escaneo Vuln.	Vencido (3 meses)
---------------------	------	---	---------------	-------------------

Comunicación y Redes de Comunicación

La sede principal cuenta con la siguiente infraestructura de comunicaciones:

TIPO DE ENLACE	PROVEEDOR	CAPACIDAD	REDUNDANCIA
Internet Principal	CANTV Empresas	100 Mbps	No
Internet Backup	Movistar	50 Mbps	Sí (manual)
Enlace Dedicado Clientes	Propio (fibra)	1 Gbps	Parcial

Redes Locales (LAN):

VLAN	PROPÓSITO	RANGO IP
VLAN 10	Administración	10.0.10.0/24
VLAN 20	Servidores	10.0.20.0/24
VLAN 30	Usuarios	10.0.30.0/24
VLAN 100	Invitados	192.168.100.0/24

Aplicaciones, Bases de Datos y Ficheros

Sistemas y aplicaciones críticas del área de Infraestructura:

APLICACIÓN	FUNCIÓN	BASE DE DATOS	DOCUMENTACIÓN
PRTG Network Monitor	Monitoreo de infraestructura	SQL Server 2019	Parcial
ServiceDesk Plus	Gestión de tickets e incidentes	PostgreSQL 13	Completa
FortiAnalyzer	Ánalisis de logs de seguridad	Propietaria	Manuales fabricante
Veeam B&R	Respaldos y recuperación	SQL Server 2019	Parcial
Sistema Inventario (propio)	Control de activos TI	MySQL 5.7	Sin documentación

Frecuencia de respaldos:

TIPO DE DATOS	FRECUENCIA	RETENCIÓN
Bases de datos críticas	Diario (incremental)	30 días
Configuraciones de red	Semanal	90 días
Máquinas virtuales	Diario (incremental)	14 días

FASE II: ALCANCES Y OBJETIVOS DE LA AUDITORÍA

Alcance de la Auditoría

La presente auditoría informática tiene como alcance la evaluación del Departamento de Infraestructura de Red y Comunicaciones de TeleNET Solutions C.A. en su sede principal de Caracas, abarcando las siguientes áreas:

ÁREA DE ALCANCE	ELEMENTOS A EVALUAR
Seguridad de la Información	<ul style="list-style-type: none">• Controles de acceso lógico• Configuración de firewalls• Políticas de contraseñas
Infraestructura Tecnológica	<ul style="list-style-type: none">• Estado de equipos de red• Sistema de respaldos• Redundancia y alta disponibilidad
Controles Internos	<ul style="list-style-type: none">• Políticas y procedimientos documentados• Gestión de cambios• Control de acceso al Data Center
Cumplimiento Normativo	<ul style="list-style-type: none">• Licenciamiento de software• Contratos con proveedores• Políticas de retención de datos
Eficiencia Operativa	<ul style="list-style-type: none">• Métricas de disponibilidad (uptime)• Tiempos de respuesta a incidentes• Procesos de monitoreo

El alcance de la presente auditoría se circumscribe exclusivamente a la sede principal de Caracas, limitando la evaluación operativa al periodo comprendido por los últimos doce meses. Es importante precisar que, con el fin de salvaguardar la integridad de los servicios críticos, el ejercicio excluye la ejecución de pruebas de penetración activas sobre los sistemas en

producción, centrándose estrictamente en el análisis de cumplimiento y seguridad dentro de los parámetros establecidos.

Objetivos de la Auditoría

Objetivo General

Verificar que los recursos informáticos del área de Infraestructura de Red y Comunicaciones de TeleNET Solutions C.A. son adecuadamente utilizados, coordinados y vigilados, evaluando la eficiencia de los controles internos, la seguridad de la información y el cumplimiento de las políticas establecidas.

Objetivos Específicos

Resguardar la información: Evaluar los mecanismos de protección de datos, identificando brechas de seguridad y vulnerabilidades.

Verificar integridad de datos: Comprobar que los controles de integridad previenen alteraciones no autorizadas en configuraciones y datos.

Evaluar disponibilidad: Analizar los procedimientos de respaldo y la capacidad de mantener continuidad operativa.

Medir eficiencia: Identificar ineficiencias en el rendimiento, evaluando métricas de disponibilidad y tiempos de respuesta.

FASE III: PLAN Y PROGRAMAS DE TRABAJO

Tipo de Auditoría

Tipo según alcance:	Auditoría por área específica (Infraestructura de Red)
Tipo según profundidad:	Auditoría parcial (sede principal Caracas)

Calendario de Actividades

La auditoría se ejecutará en un período de 5 días hábiles, del lunes 03 al viernes 07 de febrero de 2026:

DÍA	FECHA	ACTIVIDADES
Día 1 (Lunes)	03/02/2026	<ul style="list-style-type: none">• Reunión de apertura• Recopilación de documentación• Entrevistas iniciales
Día 2 (Martes)	04/02/2026	<ul style="list-style-type: none">• Inspección física Data Center• Revisión de inventarios• Verificación de configuraciones
Día 3 (Miércoles)	05/02/2026	<ul style="list-style-type: none">• Análisis de seguridad• Revisión de respaldos• Pruebas de controles
Día 4 (Jueves)	06/02/2026	<ul style="list-style-type: none">• Análisis de hallazgos• Elaboración recomendaciones• Redacción informe borrador
Día 5 (Viernes)	07/02/2026	<ul style="list-style-type: none">• Revisión final• Reunión de cierre• Entrega informe final

Prioridades de Materias Auditables

PRIORIDAD	MATERIA AUDITABLE	JUSTIFICACIÓN
1 - Crítica	Seguridad perimetral (Firewall)	Primera línea de defensa
2 - Crítica	Sistema de respaldos	Recuperación ante desastres
3 - Alta	Configuración de equipos de red	Disponibilidad de servicios

4 - Alta	Control de acceso Data Center	Protección física de activos
5 - Media	Documentación y procedimientos	Continuidad operativa
6 - Media	Licenciamiento de software	Cumplimiento legal
7 - Baja	Capacitación del personal	Mejora continua

Asignación de Tareas por Integrante del Equipo Auditor

AUDITOR	ROL	RESPONSABILIDADES	ÁREAS ASIGNADAS
Víctor Ysea	Líder de Auditoría	<ul style="list-style-type: none"> • Coordinación general • Entrevistas con gerencia • Consolidación informe final 	<ul style="list-style-type: none"> • Arquitectura de red • Seguridad perimetral
María Yoris	Auditor Senior	<ul style="list-style-type: none"> • Evaluación controles internos • Revisión de documentación • Verificación cumplimiento 	<ul style="list-style-type: none"> • Políticas y procedimientos • Licenciamiento
Fiorella David	Auditor Senior	<ul style="list-style-type: none"> • Inspección física • Levantamiento inventarios • Revisión de respaldos 	<ul style="list-style-type: none"> • Inventario HW/SW • Sistema de respaldos
Juan Marcano	Auditor Junior	<ul style="list-style-type: none"> • Análisis de configuraciones • Pruebas técnicas • Documentación de evidencias 	<ul style="list-style-type: none"> • Configuración equipos • Control de acceso

Programación Detallada de Actividades

Actividades	Dia 1	Dia 2	Dia 3	Dia 4	Dia 5
Reunión de apertura	Equipo				
Recopilación de documentación	Maria	Maria			
Entrevistas iniciales		Victor			
Inspección física data center		Fiorella			
Revisión de inventarios		Fiorella			
Verificación de configuraciones		Maria	Victor		
Análisis de seguridad			Maria		
Revisión de respaldos			Fiorella		
Pruebas de controles				Victor	
Análisis de hallazgos					Equipo
Elaboración de recomendaciones				Victor	
Redacción de borrador de informe				Equipo	
Revisión final					Victor
Reunión de cierre					Equipo
Entrega informe final					Equipo

Leyenda: Equipo Victor Maria Fiorella Juan

FASE IV: DETERMINACIÓN DE RECURSOS NECESARIOS

Recursos Humanos

Equipo auditor:

NOMBRE	ROL	DEDICACIÓN	CONTACTO
Víctor Ysea	Líder de Auditoría	100% (5 días)	victor.ysea@auditor.com
María Yoris	Auditor Senior	100% (5 días)	maria@auditor.com
Fiorella David	Auditor Senior	100% (5 días)	fiorella@auditor.com

Juan Marcano	Auditor Junior	100% (5 días)	juan@auditor.com
--------------	----------------	---------------	------------------

Personal a auditar (disponibilidad requerida):

NOMBRE Y APELLIDO	CARGO	DEPARTAMENTO	DISPONIBILIDAD
Carlos Mendoza	Gerente de Infraestructura	Infraestructura de Red	Día 1, 4 y 5
Roberto Fernández	Coord. Administración de Red	Administración de Red	Día 1, 2 y 3
Ana Martínez	Coord. Data Center	Data Center	Día 2 y 3
Luis Pérez	Coord. Seguridad de Red	Seguridad de Red	Día 2 y 3
José García	Técnico de Red Senior	Administración de Red	Día 2
María López	Técnico de Red Senior	Administración de Red	Día 2
Pedro Rodríguez	Técnico de Data Center	Data Center	Día 2
Carmen Díaz	Analista de Seguridad	Seguridad de Red	Día 3

Recursos Financieros

Presupuesto estimado de la auditoría:

CONCEPTO	DETALLE	MONTO (USD)
Honorarios Equipo Auditor	4 auditores x 5 días x \$150/día	\$3,000.00
Software de Auditoría	Licencias temporales	\$200.00
Gastos de Transporte	Traslados diarios (5 días)	\$200.00
Viáticos y Alimentación	4 personas x 5 días x \$20/día	\$400.00
Materiales de Oficina	Papelería, impresiones	\$50.00
Comunicaciones	Telefonía e internet	\$30.00
Imprevistos (10%)	Reserva para contingencias	\$388.00
TOTAL		\$4,268.00

Recursos Tecnológicos

RECURSO	DESCRIPCIÓN	PROPÓSITO
Laptops	4 equipos con herramientas	Trabajo de campo
Software de escaneo	NMAP, Nessus (trial)	Ánálisis de vulnerabilidades
Analizador de red	Wireshark	Captura de tráfico
Herramientas documentación	Microsoft Office 365	Elaboración de informes
Acceso a sistemas	Credenciales de solo lectura	Revisión configuraciones
Cámara fotográfica	Documentación evidencias	Registro de hallazgos

Recursos Materiales y Logísticos

Documentación requerida:

- Organigrama actualizado del área de Infraestructura
- Políticas de seguridad de la información
- Procedimientos operativos (gestión de cambios, incidentes, respaldos)
- Inventario de hardware y software
- Diagramas de topología de red
- Contratos con proveedores de telecomunicaciones
- Licencias de software vigentes
- Reportes de incidentes de los últimos 12 meses

Herramientas de recolección de datos:

HERRAMIENTA	APLICACIÓN
Cuestionarios	Recopilación inicial de información
Guías de entrevista	Entrevistas estructuradas
Checklists	Verificación de cumplimiento
Plantillas de observación	Registro de hallazgos físicos

Instalaciones requeridas:

- Sala de reuniones para entrevistas
- Acceso físico al Data Center (acompañado)
- Espacio de trabajo temporal para el equipo auditor
- Acceso a la red WiFi corporativa