ANEXO - FORMULARIO UNICO Y OFICIAL DE OFERTA

Cotizar en esta planilla en letra de imprenta y en pesos con IVA incluido:
La cotización debe presentarse únicamente en la presente Planilla de Cotización

Nº RENG	CANT.	DETALLE	PRECIO MENSUAL
1	12 meses	• **Servicio de Soporte de Tercer Nivel e Ingeniería de Redes y Servidores,** según Anexo - Especificaciones Técnicas y Anexo – Planos (39 - treinta y nueve)	
		TOTAL GENERAL ANUAL DE LA OFERTA:	

(Solo se aceptarán precios unitarios expresados con hasta 2 (dos) decimales. En caso de cotizar con más decimales de los indicados, solo se tomarán los dos primeros.)

*Son pesos (IVA INCLUIDO):(Importe en letras)*_____

Aceptamos la competencia de los Tribunales Federales en lo Contencioso Administrativo con Asiento en la Ciudad Autónoma de Buenos Aires y hacemos expresa renuncia a otro fuero o jurisdicción.

Esta Propuesta, junto con la aceptación por escrito del Adjudicatario, constituirá un vínculo contractual entre ambas partes una vez integrada la Garantía de Fiel Cumplimiento de contrato y emitida la Orden de Compra. Entendemos que la Universidad no está obligada a aceptar ni la oferta más baja ni ninguna otra que puedan recibir.

Confirmamos por la presente que esta Oferta cumple con el período de validez y con la Garantía de Oferta, en caso de ser requerida en los Documentos de la presente contratación. Asimismo, con carácter de Declaración Jurada, el oferente manifiesta no estar incurso en ninguna de las causales de inhabilidad ni inelegibilidad contempladas en la normativa aplicable, conforme Art. 18, Inc. i) apartado 5, del Pliego Único de Bases y Condiciones Generales aprobado por Disposición ONC Nº 63/16.

La sola presentación de la propuesta en el marco del presente proceso significará de parte del proponente el pleno conocimiento y aceptación de las cláusulas que rigen el llamado, por lo que no será necesario presentar junto con la propuesta ningún ejemplar de los pliegos.

Firma Autorizada del Oferente:	
Nombre y Cargo del Firmante:	
Razón Social de la Empresa:	
CUIT Nº:	
Dirección, Localidad, Código Postal:	
Teléfono y Fax aptos para notificaciones:	
Correo electrónico apto para notificaciones:	

ANEXO – ESPECIFICACIONES TÉCNICAS

Objeto de la contratación

El presente tiene por objeto la contratación de un servicio especializado de soporte técnico de tercer nivel, ingeniería de networking avanzada y asesoramiento estratégico, destinado a garantizar la continuidad operativa, disponibilidad, seguridad y evolución tecnológica de la infraestructura de redes, telecomunicaciones, centros de datos y plataformas de servicios de la Universidad.

La prestación requerida se desarrollará sobre un entorno tecnológico de alta criticidad operativa, conformado por múltiples plataformas y fabricantes, con infraestructura distribuida geográficamente, coexistencia de tecnologías legacy y modernas, y dependencia directa de los servicios tecnológicos institucionales para el normal funcionamiento de actividades académicas, administrativas y de gestión.

El servicio comprenderá tanto la resolución de incidentes complejos y contingencias operativas como la participación activa en tareas de diagnóstico, análisis de performance, optimización de infraestructura, rediseño arquitectónico, planificación tecnológica, implementación de mejoras y acompañamiento técnico en procesos de evolución y modernización de plataformas existentes.

La infraestructura objeto del presente servicio opera en esquemas de alta disponibilidad e integración transversal entre servicios de networking, seguridad perimetral, virtualización, storage, telefonía IP, conectividad inalámbrica, monitoreo y plataformas de infraestructura crítica, requiriendo capacidades avanzadas de análisis, troubleshooting y operación sobre entornos enterprise de elevada complejidad técnica.

Asimismo, el adjudicatario deberá integrarse operativamente con los equipos técnicos de la Dirección de Informática, colaborando en tareas de soporte N3, ingeniería, planificación y transferencia de conocimiento, priorizando la continuidad operativa de los servicios institucionales y minimizando riesgos asociados a intervenciones sobre entornos productivos.

La Universidad prevé además avanzar progresivamente en procesos de modernización tecnológica vinculados a automatización, observabilidad avanzada, integración de servicios híbridos y adopción gradual de nuevas arquitecturas tecnológicas, por lo que se requerirá capacidad de acompañamiento técnico y consultoría especializada en dichos escenarios evolutivos.

La prestación del servicio se desarrollará bajo esquema de asistencia técnica especializada a demanda, conforme a la criticidad, complejidad y requerimientos operativos definidos por la Dirección de Informática, pudiendo comprender intervenciones remotas, presenciales, tareas de ingeniería, troubleshooting avanzado, consultoría técnica y acompañamiento sobre procesos de evolución tecnológica.

Caracterización general de la Infraestructura

La infraestructura tecnológica institucional se encuentra distribuida sobre un total de treinta y un (31) edificios interconectados, de los cuales veintisiete (27) poseen vinculación mediante enlaces de fibra óptica monomodo y multimodo, mientras que los restantes cuatro (4) se encuentran integrados mediante infraestructura de cableado estructurado UTP.

La arquitectura tecnológica responde a un esquema distribuido de múltiples centros de datos interconectados, operando de manera integrada para brindar soporte a los distintos servicios académicos, administrativos y de gestión de la Universidad. Se adjuntan planos, diagramas y esquemas de interconexión al final del documento.

La infraestructura tecnológica institucional brinda soporte a un entorno compuesto por equipamiento de networking, servidores físicos y virtuales, plataformas de telefonía IP, dispositivos

de impresión, servicios de infraestructura y aproximadamente cuatro mil (4000) conexiones inalámbricas concurrentes promedio diarias, totalizando un ecosistema operativo del orden de cuatro mil quinientos (5500) dispositivos, servicios y sesiones activas distribuidas sobre la totalidad del campus universitario.

La arquitectura de red se sustenta en una segmentación lógica de alta granularidad, compuesta por ciento trece (113) VLANs operativas. El entorno exige una gestión avanzada de políticas de aislamiento, control de acceso y filtrado de tráfico basada en una matriz de criticidad institucional, asegurando la compartimentación funcional y la protección integral de los servicios críticos.

Asimismo, la operación de la infraestructura contempla múltiples instancias de spanning-tree, coexistencia de equipamiento multivendor, integración entre servicios de networking, seguridad, virtualización y telefonía IP, y administración de dependencias cruzadas entre plataformas críticas de producción.

La coexistencia de distintas generaciones tecnológicas, fabricantes y arquitecturas operativas configura un entorno de variada complejidad técnica, donde las tareas de soporte, troubleshooting y evolución tecnológica requieren experiencia comprobable en interoperabilidad, análisis de impacto y administración de entornos enterprise no homogéneos.

La continuidad operativa de la infraestructura tecnológica institucional resulta crítica para el normal funcionamiento de los servicios académicos, administrativos y de comunicación de la Universidad, por lo que cualquier intervención técnica deberá contemplar mecanismos de minimización de impacto, coordinación operativa y resguardo de disponibilidad de servicios.

Arquitectura de red y topología operativa

La infraestructura de red institucional se encuentra organizada bajo un esquema jerárquico de core, distribución y acceso, interconectando edificios, centros de datos y plataformas tecnológicas críticas mediante enlaces redundantes de alta capacidad.

Los centros de datos principales operan sobre plataformas Cisco Catalyst 4507R+E, interconectadas mediante enlaces de fibra óptica monomodo de 10 Gbps configurados bajo esquemas de agregación LACP, constituyendo el backbone principal de comunicaciones de la Universidad.

La arquitectura implementada contempla mecanismos de redundancia y alta disponibilidad entre datacenters, segmentación lógica distribuida por servicios y edificios, dominios de falla identificados y dependencias operativas entre plataformas de networking, seguridad, virtualización, storage y telefonía IP.

Sobre esta infraestructura operan servicios críticos institucionales que requieren disponibilidad permanente, como plataformas académicas, administrativas, sistemas de autenticación, conectividad institucional, telefonía IP, servicios de virtualización y plataformas de monitoreo.

La topología de red actualmente implementada contempla coexistencia de tecnologías legacy y modernas, integración entre múltiples fabricantes y administración de tráfico sobre distintos niveles de criticidad operativa, requiriendo capacidad avanzada de análisis sobre convergencia, redundancia, interoperabilidad y comportamiento de tráfico en escenarios complejos.

El adjudicatario deberá poseer experiencia comprobable en administración y troubleshooting de topologías enterprise distribuidas, con identificación de puntos únicos de falla, análisis de impacto operativo, troubleshooting avanzado sobre entornos productivos y capacidad de intervención sobre infraestructuras activas minimizando riesgos de indisponibilidad o degradación de servicios.

Asimismo, deberá contar con capacidad técnica para participar en tareas de optimización, rediseño y evolución de la arquitectura existente, colaborando en procesos de expansión, modernización tecnológica y fortalecimiento de los esquemas de continuidad operativa institucional.

Infraestructura de Networking

La infraestructura de networking institucional se encuentra conformada por un ecosistema multivendor compuesto por aproximadamente ciento cincuenta y ocho (158) equipos activos de switching y distribución, desplegados sobre una arquitectura jerárquica de core, distribución y acceso, interconectando la totalidad de los edificios y centros de datos de la Universidad.

La plataforma combina equipamiento de distintas generaciones tecnológicas y múltiples fabricantes, coexistiendo entornos legacy con infraestructura de última generación actualmente en producción. Esta condición requiere capacidades avanzadas de interoperabilidad, troubleshooting y diagnóstico transversal sobre escenarios no homogéneos.

La infraestructura actualmente comprende equipamiento Cisco Catalyst, Huawei CloudEngine y TP-Link Omada, entre otros, los modelos son:

Cisco Catalyst:

- C9200L-24P-4X, C9200L-48T-4G, WS-C2960X-48FPS-L, WS-C2960X-24PS-L, WS-C2960G-48TC-L, WS-C2960S-48FPS-L, WS-C2960S-48LPS-L, WS-C2960S-24PS-L, WS-C2960-8PC-L

Huawei CloudEngine:

- S6730-H24X6C, S5731-S24P4X-A, S5735-L24P4S-A1, S5735-L24P4S-A-V2

TP-Link Omada:

- SX3206HPP

Sobre dicha infraestructura se implementan mecanismos avanzados de switching y segmentación lógica, con VLANs distribuidas, múltiples instancias de spanning-tree, agregación de enlaces mediante LACP, políticas QoS y priorización de tráfico para servicios críticos como telefonía IP, virtualización y aplicaciones institucionales.

La operación cotidiana del entorno exige capacidad de análisis sobre eventos de degradación de red, loops de capa 2, broadcast storms, inconsistencias de spanning-tree, saturación de enlaces, problemas de interoperabilidad entre fabricantes y fallas asociadas a convergencia o segmentación lógica.

El adjudicatario deberá acreditar experiencia comprobable en entornos de switching L2/L3 de características equivalentes, así como capacidad de intervención sobre infraestructuras activas en producción, minimizando riesgos operativos y tiempos de indisponibilidad durante tareas de mantenimiento, troubleshooting o implementación de cambios.

Firewalling

La infraestructura de seguridad perimetral de la Universidad se encuentra basada en plataformas Fortinet de última generación operando en esquemas de alta disponibilidad (HA), constituyendo el núcleo de protección y segmentación de los servicios institucionales expuestos tanto hacia Internet como hacia redes internas críticas.

El entorno se encuentra conformado principalmente por clusters FortiGate 200F desplegados en los centros de datos principales y equipos FortiGate 100F instalados en sedes remotas, integrados mediante túneles VPN site-to-site y políticas centralizadas de seguridad.

Sobre esta plataforma se implementan políticas avanzadas de seguridad de capa 3 a capa 7, inspección profunda de tráfico, control de aplicaciones, filtrado web, prevención de intrusiones (IPS), antivirus, segmentación de zonas de seguridad, acceso remoto mediante SSL-VPN e integración con servicios de autenticación institucionales.

La infraestructura mantiene dependencias directas con servicios críticos de conectividad, virtualización, acceso remoto, telefonía IP y servicios académicos y administrativos, por lo que cualquier intervención sobre la plataforma requiere capacidades avanzadas de análisis, diagnóstico y mitigación de impacto operativo.

El adjudicatario deberá acreditar experiencia comprobable sobre plataformas Fortinet y equivalentes, incluyendo administración y optimización de políticas de seguridad, troubleshooting avanzado de conectividad, análisis de tráfico mediante herramientas de diagnóstico nativas (debug flow, packet capture, session table), resolución de incidentes de seguridad, administración de entornos HA y diagnóstico de túneles VPN site-to-site y SSL-VPN.

Dado el grado de complejidad operativa de esta infraestructura, no se admitirán oferentes sin experiencia verificable en plataformas Fortinet de características equivalentes a las actualmente implementadas.

Routing y Conectividad

La Universidad opera una arquitectura de conectividad redundante y distribuida basada en múltiples proveedores de tránsito y peering. Los enlaces son provistos por Claro, RIU y CABASE, sobre los cuales se implementa enrutamiento dinámico mediante protocolo BGP.

La infraestructura de borde se encuentra soportada principalmente por routers Mikrotik CCR1072-1G-8S+, operando en un entorno de multihoming con ASN propio y direccionamiento IPv4/IPv6 asignado por LACNIC, permitiendo la administración autónoma de políticas de ruteo, balanceo de tráfico y contingencia ante fallas de conectividad.

La conectividad principal provista por Claro se encuentra enlazada sobre infraestructura de fibra óptica dedicada hacia equipamiento Huawei serie S3900 administrado por el proveedor, coexistiendo además enlaces LAN to LAN utilizados para integración con CABASE y servicios de peering académico e institucional.

La operación de esta infraestructura contempla escenarios de redundancia activa, manipulación de rutas, priorización de tráfico, failover automático y administración de sesiones BGP con múltiples upstream providers, requiriendo conocimientos avanzados en routing dinámico y análisis de convergencia.

El adjudicatario deberá poseer experiencia comprobable en administración de entornos con ASN propio, mantenimiento de sesiones BGP, diseño y aplicación de políticas de ruteo, filtrado de prefijos, balanceo de tráfico, troubleshooting avanzado de flapping, pérdida de alcance, inestabilidad de sesiones y análisis de tablas de ruteo IPv4 e IPv6.

Asimismo, deberá contar con capacidad de diagnóstico sobre incidentes de conectividad complejos que involucren interacción entre routing, seguridad perimetral, servicios críticos y enlaces de telecomunicaciones.

La Dirección de Informática podrá requerir asistencia sobre herramientas y tecnologías vinculadas a automatización de infraestructura, APIs de administración, scripting operativo, automatización de

configuraciones de networking y plataformas Infrastructure as Code (IaC), tecnologías como Ansible, Terraform o equivalentes.

Dado el carácter crítico de la conectividad institucional y su impacto directo sobre los servicios académicos y administrativos, no se admitirán oferentes sin experiencia verificable en operación de infraestructura BGP sobre entornos productivos equivalentes.

Infraestructura Wireless

La infraestructura wireless institucional se encuentra actualmente compuesta por aproximadamente ochenta y cinco (85) access points en producción, distribuidos entre edificios académicos, administrativos y áreas comunes, operando sobre un ecosistema multivendor integrado por tecnologías Cisco, Ubiquiti UniFi y TP-Link Omada. En el marco del proceso de modernización tecnológica y ampliación de cobertura institucional, se prevé la incorporación progresiva de nuevo equipamiento inalámbrico, proyectando una infraestructura superior a ciento veinte (120) access points operativos.

La plataforma Cisco opera mediante controladoras AIR-CT5520-K9 configuradas en cluster, administrando actualmente cincuenta y dos (52) access points Cisco Aironet modelos AIR-CAP3802E-A-K9, AIR-CAP3702E-A-K9, AIR-SAP1602I-A-K9, AIR-AP1042N-A-K9 y WAP4410N. Complementariamente, la Universidad dispone de doce (12) access points Ubiquiti U6-LR administrados mediante plataforma UniFi y veintiún (21) equipos TP-Link Omada EAP690E HD gestionados mediante Omada Controller. Asimismo, se prevé la incorporación progresiva de nuevos access points Cisco AIR-CAP3800 Series, Ubiquiti U6 Series y TP-Link Omada Series como parte del proceso de modernización de la infraestructura inalámbrica institucional.

La infraestructura inalámbrica brinda cobertura a servicios académicos, administrativos y de conectividad general, coexistiendo múltiples SSIDs, segmentaciones lógicas, políticas de autenticación y perfiles de tráfico diferenciados según el tipo de usuario y servicio.

La operación del entorno requiere experiencia en planificación y optimización RF, análisis de cobertura, diagnóstico de interferencias, administración de roaming y handoff entre celdas inalámbricas, ajuste de potencias y canales, y resolución de problemas de desempeño asociados a densidad de clientes, saturación de espectro o coexistencia entre fabricantes.

El adjudicatario deberá acreditar experiencia comprobable en administración y troubleshooting de entornos wireless empresariales multivendor, plataformas centralizadas de gestión, diagnóstico de degradación de servicio y optimización operativa en escenarios de alta concurrencia y distribución geográfica.

Infraestructura de Telefonía IP

La infraestructura de telefonía IP institucional brinda servicio a aproximadamente quinientos sesenta (560) internos IP distribuidos sobre la totalidad de los edificios y dependencias de la Universidad, integrándose operativamente con la infraestructura de networking, seguridad y virtualización institucional.

La plataforma de comunicaciones se encuentra basada en dos centrales físicas HIPERPBX CP3000 operando en cluster y alta disponibilidad, permitiendo continuidad operativa ante contingencias y administración centralizada de servicios de voz institucionales.

La infraestructura de terminales IP se encuentra conformada principalmente por teléfonos Grandstream modelos GXP1450 y GXP1628, coexistiendo además dispositivos Grandstream HT502, terminales inalámbricas DP752 y equipos Siemens C430 y Siemens A580 homologados por el fabricante de la central.

La operación del entorno requiere capacidades avanzadas de troubleshooting sobre señalización SIP, tráfico RTP, aprovisionamiento automático de terminales, integración con VLANs de voz, políticas QoS y diagnóstico de problemas asociados a latencia, jitter, pérdida de paquetes o degradación de calidad de audio.

El adjudicatario deberá acreditar experiencia comprobable en plataformas HIPERPBX y entornos de telefonía IP empresariales equivalentes, con administración de clusters en alta disponibilidad, análisis de tráfico SIP/RTP, integración con plataformas de networking multivendor y resolución de incidentes sobre servicios críticos de comunicación institucional.

Infraestructura de Servidores, Storage y Virtualización

La infraestructura de servidores y virtualización de la Universidad se encuentra desplegada sobre un entorno híbrido compuesto por plataformas físicas, virtuales y sistemas de almacenamiento enterprise, brindando soporte a servicios académicos, administrativos, bases de datos, aplicaciones institucionales y servicios de infraestructura críticos.

La plataforma de servidores se conforma de clusters con equipamiento HP ProLiant DL380 G9, Lenovo ThinkSystem SR630 V3/V4, actualmente en producción como infraestructura principal de cómputo sobre los centros de datos institucionales, coexistiendo con infraestructura legacy compuesta por servidores HP ProLiant DL380 G5, DL380 G6, DL380 G7 y DL380p G8, así como plataformas Dell PowerEdge R210, Dell PowerVault NX3100, IBM x3650, configurando un entorno heterogéneo de distintas generaciones tecnológicas.

La infraestructura de almacenamiento centralizado se encuentra soportada por plataformas EMC VNX 3200, DELL-EMC Unity 300 y Lenovo ThinkSystem DE6400, utilizadas para almacenamiento de máquinas virtuales, servicios institucionales y repositorios de backup.

El entorno de virtualización opera sobre tecnologías VMware ESXi versión 6 y Proxmox VE versión 9.1, totalizando aproximadamente trescientas veinte (320) máquinas virtuales actualmente en producción, con servicios críticos de autenticación, bases de datos, monitoreo, aplicaciones institucionales y servicios de infraestructura.

La estrategia de backup y recuperación se encuentra basada en Veeam Backup & Replication y almacenamiento DELL-EMC Data Domain DD2200, contemplando tareas de respaldo, replicación, restauración y recuperación ante contingencias operativas. Se ha comenzado con la implementación de Proxmox Backup Server.

La operación de esta infraestructura requiere capacidades avanzadas de troubleshooting sobre servidores físicos, virtualización, storage y networking asociado, análisis de hardware, firmware y plataformas de administración, análisis de performance, capacity planning, diagnóstico de latencia de almacenamiento, optimización de recursos, recuperación ante fallas y administración de entornos híbridos coexistentes.

El adjudicatario deberá acreditar experiencia comprobable en plataformas VMware, Proxmox, storage enterprise y soluciones de backup de características equivalentes, así como capacidad de intervención sobre infraestructuras activas de alta criticidad minimizando riesgos operativos y tiempos de indisponibilidad.

Infraestructura Eléctrica DataCenter

Los centros de datos institucionales cuentan con infraestructura eléctrica redundante orientada a garantizar la continuidad operativa de los servicios críticos de la Universidad ante contingencias energéticas o interrupciones del suministro eléctrico.

La plataforma se encuentra compuesta por sistemas UPS APC SURT 10000 XLI con bancos de baterías externos, brindando autonomía aproximada de treinta (30) minutos sobre la infraestructura, así como grupos electrógenos a gas instalados en los datacenters principales para garantizar continuidad prolongada de operación.

La infraestructura eléctrica mantiene relación directa con la operación de plataformas de networking, virtualización, storage, telefonía IP y seguridad perimetral, requiriendo capacidad de correlación entre eventos eléctricos e incidentes de infraestructura tecnológica.

El adjudicatario deberá brindar asistencia técnica especializada en diagnóstico de incidentes vinculados a continuidad eléctrica, comportamiento de UPS, eventos de transferencia, impacto sobre servicios tecnológicos y recomendaciones orientadas a fortalecer la resiliencia y disponibilidad operativa de los centros de datos institucionales.

Monitoreo y Observabilidad

La Universidad dispone actualmente de una plataforma de monitoreo compuesta por herramientas Nagios, Check_MK y Veeam ONE, utilizadas para supervisión de infraestructura de networking, servidores, virtualización, servicios críticos y plataformas de almacenamiento.

El entorno de monitoreo permite la visualización operativa de eventos, generación de alertas, seguimiento de disponibilidad y análisis básico de performance sobre distintos componentes de la infraestructura institucional.

No obstante, debido al crecimiento sostenido de la infraestructura tecnológica y a la creciente complejidad operativa del entorno, la Universidad prevé evolucionar progresivamente hacia un modelo de observabilidad moderna que permita correlacionar métricas, eventos y registros provenientes de múltiples plataformas tecnológicas.

En este contexto, el adjudicatario deberá brindar soporte y optimización sobre las plataformas existentes, ajuste de métricas, umbrales, alertas y tableros operativos, así como participar en procesos de evolución tecnológica orientados a incorporar herramientas de observabilidad, centralización de logs, métricas y visualización, tales como Prometheus, Grafana o tecnologías equivalentes.

Asimismo, deberá poseer capacidades para asistir en la correlación de eventos de infraestructura, análisis de performance, identificación temprana de degradaciones operativas y construcción de tableros integrados de visibilidad tecnológica sobre entornos híbridos y multivendor.

Automatización y Evolución Tecnológica

La Universidad se encuentra en un proceso continuo de modernización y evolución de su infraestructura tecnológica, orientado a mejorar los niveles de disponibilidad, estandarización operativa, escalabilidad y capacidad de respuesta ante el crecimiento sostenido de los servicios institucionales.

En este contexto, el adjudicatario deberá asistir técnicamente en la incorporación progresiva de prácticas de automatización, estandarización de configuraciones e infraestructura como código, orientadas a reducir el error operativo, optimizar tiempos de implementación y fortalecer la trazabilidad de cambios sobre plataformas críticas.

Asimismo, deberá brindar capacidades de consultoría e ingeniería para la evaluación de nuevas arquitecturas tecnológicas como esquemas híbridos on-premise/cloud, integración con servicios en la nube, evolución de plataformas de virtualización y contenedorización, modernización de herramientas de monitoreo y observabilidad, automatización de despliegues y adopción gradual de tecnologías emergentes compatibles con la estrategia tecnológica institucional.

La Universidad podrá avanzar progresivamente hacia esquemas de infraestructura híbrida y adopción parcial de servicios cloud, por lo que el adjudicatario deberá contar con capacidades técnicas y experiencia comprobable en integración de entornos on-premise con plataformas de nube pública, incluyendo arquitecturas basadas en Amazon Web Services (AWS), Microsoft Azure o tecnologías equivalentes. Dichas capacidades podrán comprender conectividad híbrida, segmentación y seguridad de entornos cloud, integración de servicios de identidad, estrategias de backup y recuperación, monitoreo unificado, virtual networking, automatización de despliegues y evaluación de arquitecturas orientadas a alta disponibilidad y continuidad operativa.

Las tareas podrán comprender análisis de factibilidad técnica, recomendaciones de arquitectura, evaluación de impacto operativo, definición de buenas prácticas y acompañamiento técnico en procesos de migración o implementación progresiva de nuevas soluciones.

La Universidad podrá requerir asistencia sobre tecnologías vinculadas a automatización de configuraciones, gestión centralizada, observabilidad avanzada, integración de servicios híbridos, consolidación de plataformas y optimización de infraestructura existente, debiendo el adjudicatario contar con capacidades técnicas acordes a dichos escenarios evolutivos.

Provisión de Equipamiento

Con el objeto de minimizar el impacto operativo ante fallas críticas de infraestructura y garantizar la continuidad de los servicios institucionales, el adjudicatario deberá disponer de capacidad de provisión temporal de equipamiento de reemplazo para dispositivos de networking de acceso, distribución, core o borde cuya reposición no pueda realizarse en forma inmediata o que no cuenten con soporte vigente del fabricante.

Dicha provisión deberá contemplar equipamiento de la misma marca o de características técnicas equivalentes o superiores, compatible con la arquitectura actualmente implementada y apto para integrarse operativamente, sin generar degradación de los servicios o incurrir en nuevas configuraciones que afecten la disponibilidad del equipo técnico de la Dirección de Informática.

La capacidad de reemplazo podrá comprender equipamiento de switching de acceso, distribución o core perteneciente a líneas Cisco Catalyst series 2900, 9200 y 4500, así como Huawei CloudEngine series S5700 y S6700, TP-Link Omada SX3206HPP o tecnologías equivalentes de nivel enterprise, compatible con la arquitectura actualmente implementada y apto para integrarse operativamente sin afectar la continuidad de los servicios institucionales.

El equipamiento provisto deberá entregarse dentro de plazos compatibles con la criticidad del incidente, permanecer operativo durante el tiempo necesario para la reposición definitiva y permitir la continuidad de los servicios institucionales bajo condiciones operativas normales.

Alcance Operativo y Niveles de Servicio

El adjudicatario deberá garantizar capacidad de atención técnica remota inmediata ante incidentes críticos que afecten la operación de la infraestructura tecnológica institucional, incluyendo plataformas de core networking, seguridad perimetral, conectividad BGP, virtualización, storage y telefonía IP.

Asimismo, deberá contar con disponibilidad para intervención presencial (on-site) en los centros de datos o dependencias de la Universidad cuando la criticidad del incidente o la naturaleza técnica de la intervención así lo requieran.

Para incidentes que afecten infraestructura crítica, tales como core de red, firewalls, servicios de telefonía IP o plataformas centrales de virtualización, el tiempo máximo de presencia on-site no podrá superar las seis (6) horas desde la notificación formal del incidente.

Para incidentes asociados a infraestructura de acceso, switching secundario o servicios no críticos, el tiempo máximo de intervención presencial será de hasta doce (12) horas.

El adjudicatario deberá poseer capacidad operativa para coordinar tareas de troubleshooting, diagnóstico avanzado, recuperación de servicios y ejecución de cambios sobre entornos productivos activos, minimizando riesgos operativos e impacto sobre usuarios finales.

Toda tarea que implique afectación potencial sobre servicios en producción deberá ejecutarse en ventanas programadas y coordinadas previamente con la Dirección de Informática, priorizando su realización en horarios de baja utilización comprendidos entre las 20:00 hs y las 08:00 hs, y asegurando mecanismos de rollback ante contingencias operativas.

Asimismo, el adjudicatario deberá mantener canales de comunicación técnica permanentes con el personal de la Dirección de Informática, garantizando seguimiento operativo, escalamiento adecuado y transferencia de información sobre incidentes, cambios o tareas ejecutadas.

La intervención técnica podrá ser requerida en forma remota o presencial bajo esquema a demanda, conforme a criticidad, impacto operativo y necesidad técnica o requerimiento de ingeniería determinado por la Dirección de Informática.

Servicio a Contratar

El adjudicatario deberá prestar, bajo modalidad de asistencia técnica especializada a demanda, servicios de soporte técnico de tercer nivel sobre la totalidad de la infraestructura tecnológica descripta en el presente pliego, mediante modalidades remota, telefónica y presencial (on-site), conforme a los requerimientos operativos definidos por la Dirección de Informática de la Universidad. La prestación podrá requerirse en forma variable conforme a la criticidad de los incidentes, necesidades operativas, contingencias, requerimientos de ingeniería y procesos de evolución tecnológica de la infraestructura institucional.

El servicio comprenderá asistencia técnica avanzada sobre plataformas de networking, seguridad perimetral, wireless, routing, telefonía IP, servidores, virtualización, storage, monitoreo y servicios de infraestructura asociados.

Asimismo, el adjudicatario deberá brindar soporte especializado sobre plataformas Mikrotik CCR, herramientas Nagios, NagVis, Check_MK y Veeam ONE, troubleshooting avanzado, optimización operativa, asistencia ante contingencias e integración con el resto de la infraestructura institucional.

Las tareas podrán incluir diagnóstico y resolución de incidentes complejos, ejecución de configuraciones avanzadas, troubleshooting sobre infraestructura crítica, asistencia ante emergencias operativas, implementación de mejoras tecnológicas y acompañamiento técnico en procesos de migración o evolución de plataformas existentes.

En materia de networking y seguridad, el adjudicatario deberá brindar soporte sobre infraestructura multivendor, para switching L2/L3, VLANs, spanning-tree, routing dinámico, plataformas Fortinet, túneles VPN, políticas de seguridad, análisis de tráfico y troubleshooting avanzado de conectividad.

Respecto de la infraestructura de telefonía IP, el servicio deberá contemplar soporte sobre centrales HIPERPBX CP3000 en alta disponibilidad, terminales Grandstream y Siemens homologados, diagnóstico de señalización SIP y tráfico RTP, integración con infraestructura de red y mecanismos de aprovisionamiento automático de terminales IP distribuidos sobre distintos segmentos institucionales.

En relación con la infraestructura de servidores y virtualización, el adjudicatario deberá brindar soporte sobre plataformas VMware y Proxmox, administración de entornos híbridos,

troubleshooting de storage, optimización de performance, capacity planning y asistencia sobre plataformas de backup y recuperación basadas en Veeam y EMC Data Domain.

Asimismo, deberá brindar soporte técnico sobre servidores Windows y Linux y servicios de infraestructura asociados, tales como Active Directory, DNS, DHCP, NTP, LDAP, Syslog, plataformas de correo electrónico institucional y mecanismos de integración con plataformas de seguridad y autenticación institucional

El servicio también comprenderá asistencia sobre plataformas de monitoreo y observabilidad, ajuste de métricas, alertas, dashboards operativos y correlación de eventos sobre infraestructura.

El adjudicatario participará conjuntamente con el personal técnico de la Dirección de Informática en proyectos de ingeniería, rediseño, migración, expansión e implementación de nuevas tecnologías, colaborando en tareas de análisis, planificación, validación e implementación operativa.

Toda intervención sobre infraestructura crítica deberá ejecutarse bajo coordinación con la Dirección de Informática, priorizando la continuidad operativa de los servicios institucionales y minimizando el impacto sobre los entornos productivos.

Requisitos del Oferente

El oferente deberá acreditar capacidad técnica, operativa y experiencia comprobable en la prestación de servicios especializados de soporte técnico de tercer nivel sobre infraestructuras tecnológicas de características equivalentes o superiores a las descriptas en el presente pliego.

A tal efecto, deberá demostrar experiencia comprobable no inferior a cinco 5 años en administración, soporte y operación de entornos tecnológicos complejos, distribuidos geográficamente y conformados por infraestructura multivendor de networking, seguridad, virtualización y servicios críticos.

El oferente deberá presentar antecedentes verificables de servicios prestados en organismos públicos, universidades, empresas o instituciones que posean múltiples sedes interconectadas, infraestructura distribuida o entornos tecnológicos de alta criticidad operativa, incluyendo referencias técnicas que permitan validar la experiencia declarada.

Se valorará especialmente la experiencia previa en entornos donde coexistan tecnologías legacy y plataformas modernas en producción simultánea, así como experiencia específica en procesos de continuidad operativa, contingencia, migración tecnológica y soporte sobre servicios críticos institucionales.

El oferente deberá acreditar experiencia y capacidades técnicas comprobables sobre plataformas Cisco, Huawei, Mikrotik, Ubiquiti UniFi, Omada, HIPERPBX, Grandstream, Siemens, Fortinet, VMware, Proxmox, EMC, Dell-EMC, Dell, HP, IBM, Lenovo, Veeam, Nagios, Check_MK, NagVis y tecnologías equivalentes actualmente implementadas en la Universidad.

Asimismo, deberá acreditar experiencia en administración de plataformas BGP con ASN propio, entornos multihoming, plataformas de seguridad Fortinet en alta disponibilidad, infraestructura wireless empresarial, entornos de virtualización híbridos , storage enterprise y herramientas de monitoreo y observabilidad.

El oferente deberá poseer experiencia comprobable en integración y administración de entornos híbridos on-premise/cloud, plataformas Amazon Web Services (AWS), Microsoft Azure o tecnologías equivalentes, así como capacidades técnicas orientadas a interoperabilidad entre infraestructuras, conectividad segura, automatización y operación de servicios distribuidos. Se considerarán especialmente antecedentes técnicos y certificaciones oficiales vigentes vinculadas a

arquitecturas cloud, infraestructura híbrida, networking y seguridad sobre entornos de nube pública.

El oferente deberá disponer de un equipo técnico especializado en networking, seguridad, virtualización y sistemas, con capacidad de intervención sobre incidentes críticos y disponibilidad operativa compatible con los niveles de servicio requeridos.

Asimismo, deberá identificar al responsable técnico del servicio y al personal asignado, detallando perfiles técnicos, experiencia y grado de especialización en las tecnologías involucradas.

Se valorará especialmente el conocimiento previo del entorno tecnológico institucional, la capacidad de integración operativa con los equipos técnicos existentes y la adopción de metodologías de trabajo alineadas a buenas prácticas de gestión de servicios ITSM, automatización y observabilidad moderna.

Confidencialidad

El adjudicatario deberá garantizar absoluta confidencialidad respecto de toda información técnica, administrativa u operativa a la que acceda durante la prestación del servicio, incluyendo configuraciones de infraestructura, topologías de red, credenciales, políticas de seguridad, direccionamiento IP, documentación técnica, información de usuarios y cualquier otro dato vinculado a la operación tecnológica institucional.

Toda intervención técnica deberá realizarse exclusivamente bajo autorización y coordinación de la Dirección de Informática, no pudiendo el adjudicatario efectuar modificaciones sobre infraestructura crítica, configuraciones operativas o políticas de seguridad sin aprobación expresa del personal autorizado por la Dirección de Informática.

El adjudicatario deberá adoptar las medidas técnicas y organizativas necesarias para garantizar la protección de la información institucional, evitando divulgación, copia, utilización indebida o acceso no autorizado a los sistemas y plataformas de la Universidad.

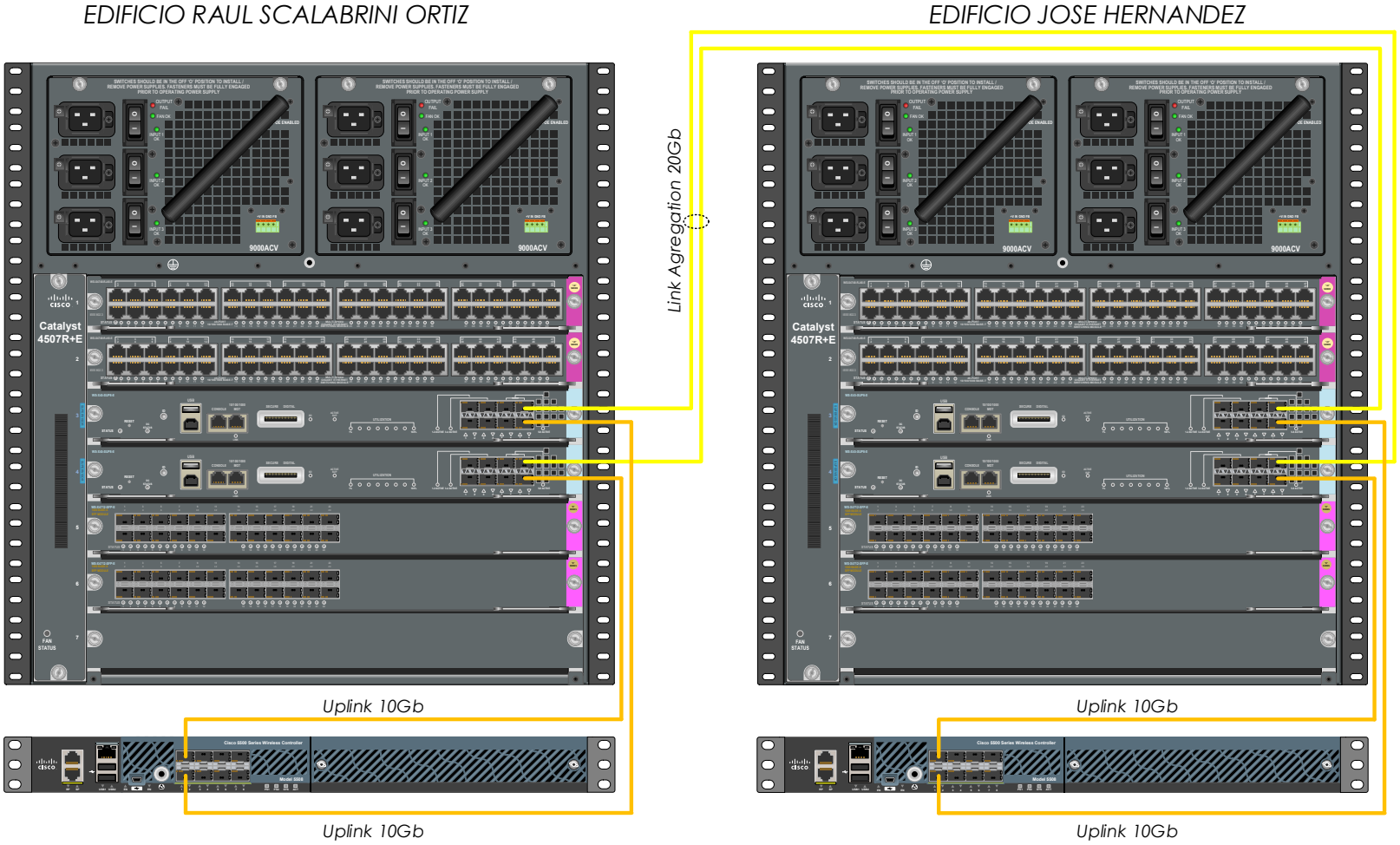
Asimismo, deberá garantizar que el personal afectado al servicio mantenga estricta reserva sobre la información a la que acceda durante la ejecución contractual, incluso con posterioridad a la finalización del vínculo entre las partes.

La Universidad podrá requerir la firma de acuerdos específicos de confidencialidad y resguardo de información para el personal técnico asignado al servicio, así como establecer procedimientos de auditoría, trazabilidad y control sobre accesos administrativos o intervenciones realizadas sobre la infraestructura tecnológica institucional.

…….
Firma y aclaración.

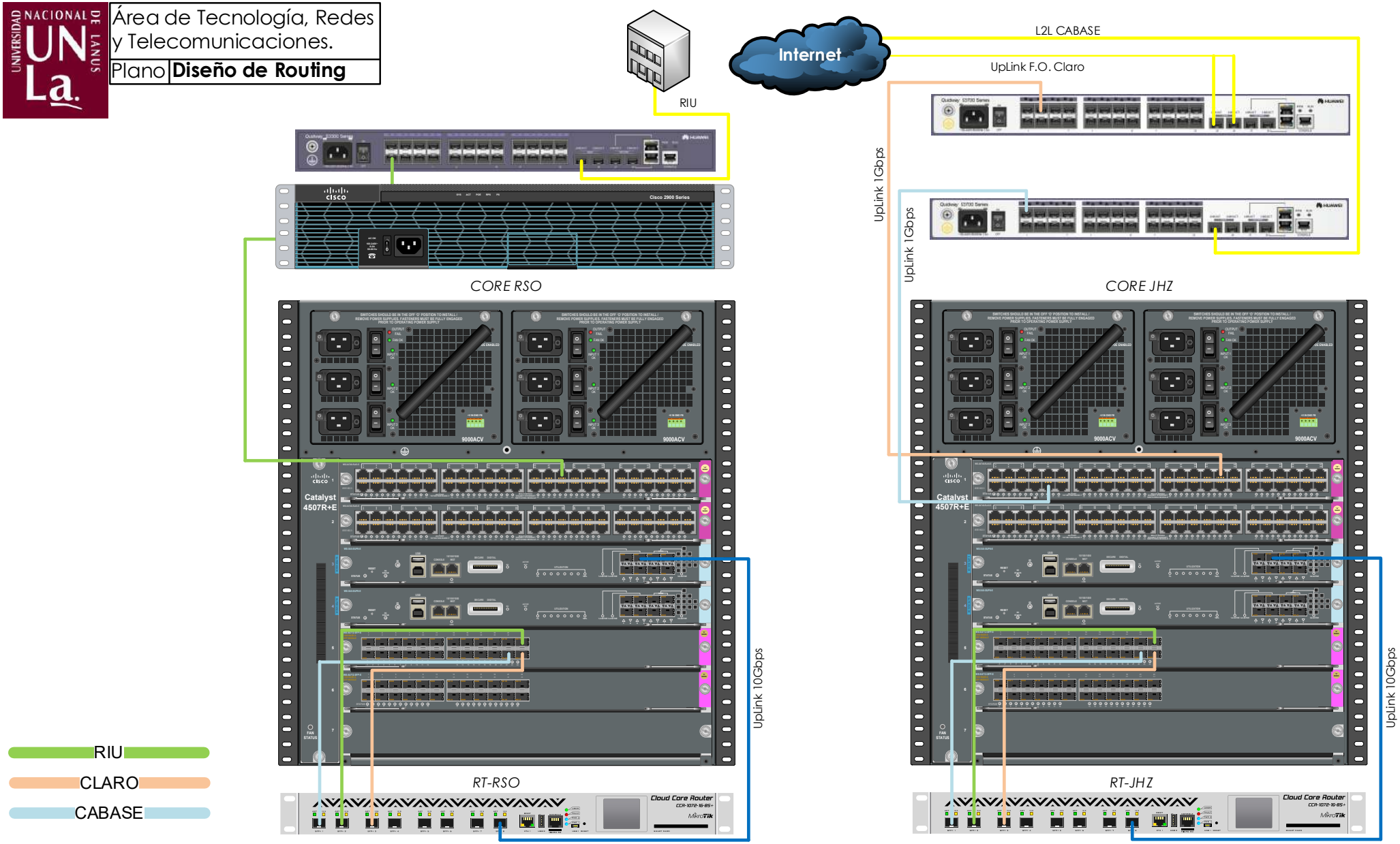
ANEXO – PLANOS

UNIVERSIDAD NACIONAL DE LANUS UNLa.	Área de Tecnología, Redes y Telecomunicaciones.
	Plano **Diagrama de Core's y WLC**



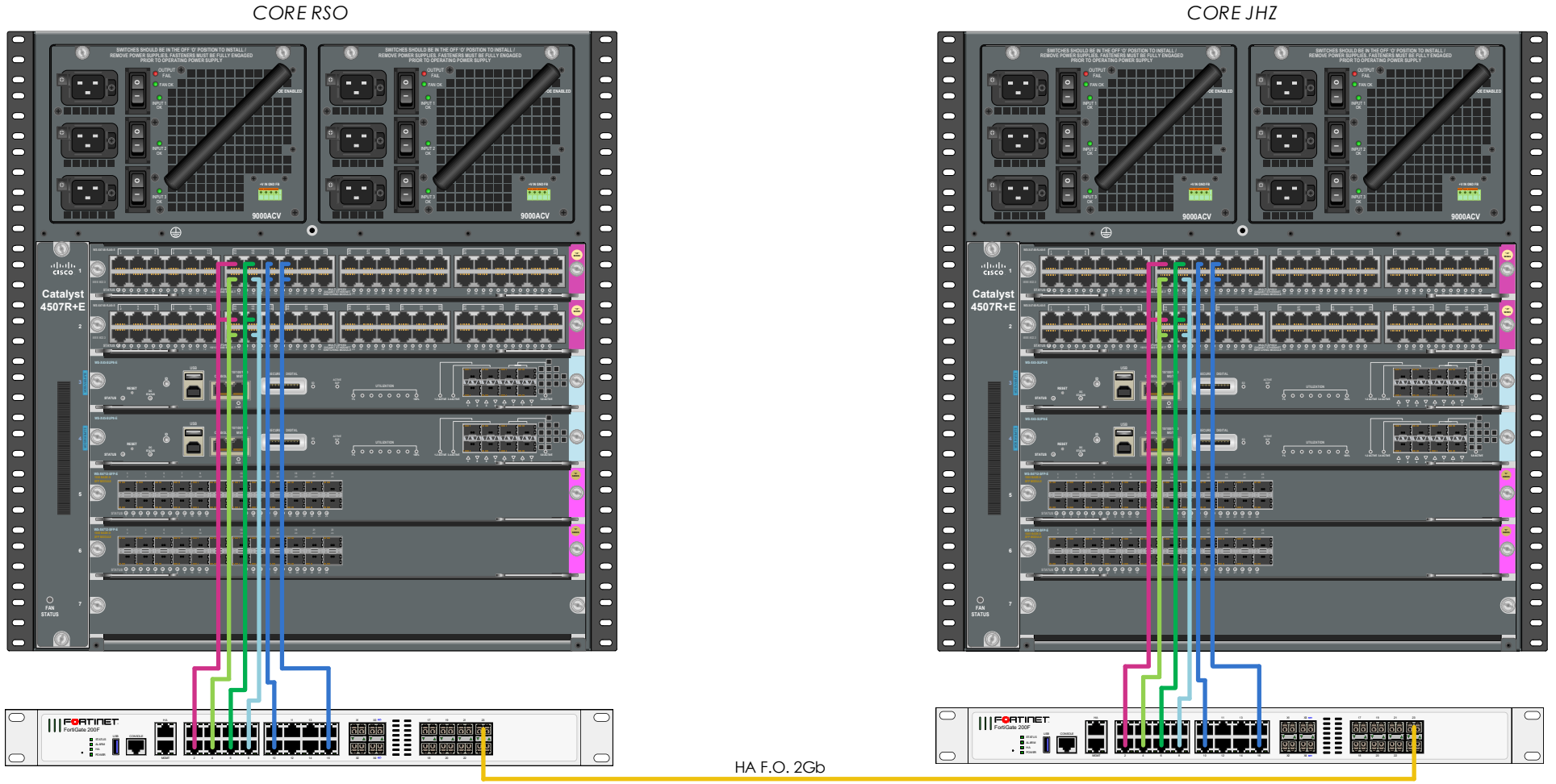
Área de Tecnología, Redes y Telecomunicaciones.

Plano **Diseño de Routing**



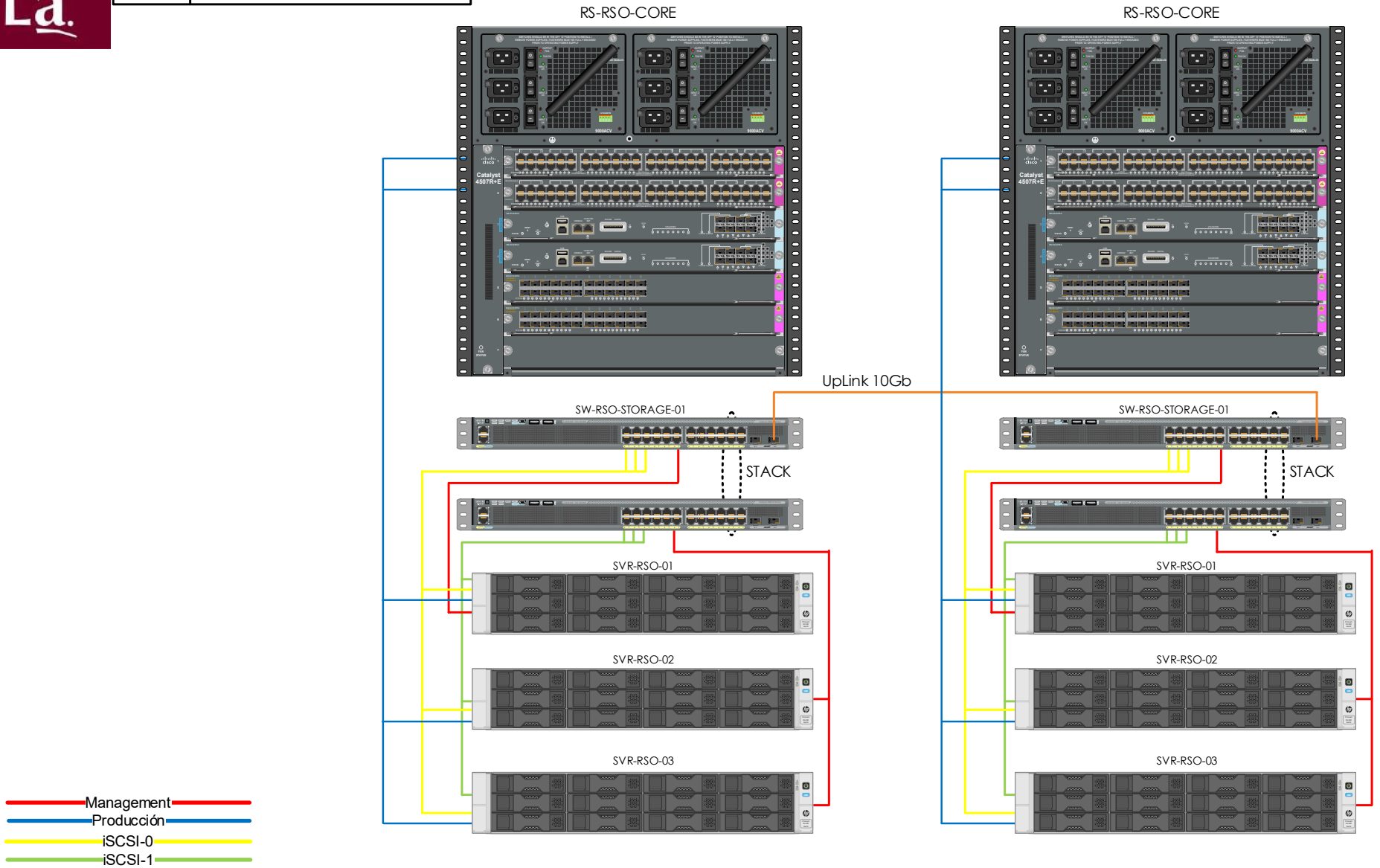
Área de Tecnología, Redes y Telecomunicaciones.

Plano **Diseño de Firewalling**



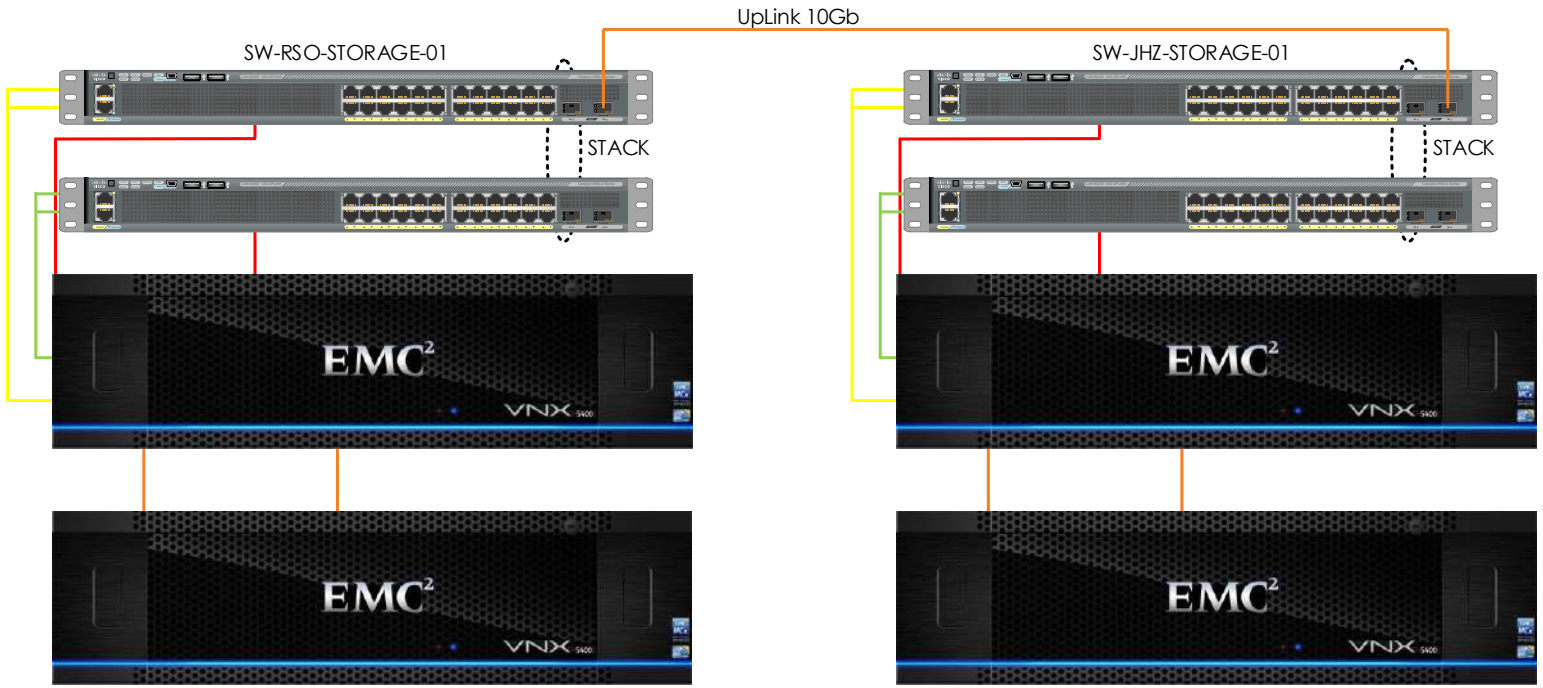
Área de Tecnología, Redes y Telecomunicaciones.

Plano **Diseño de Servidores**



Área de Tecnología, Redes y Telecomunicaciones.

Plano **Diseño de Storage**



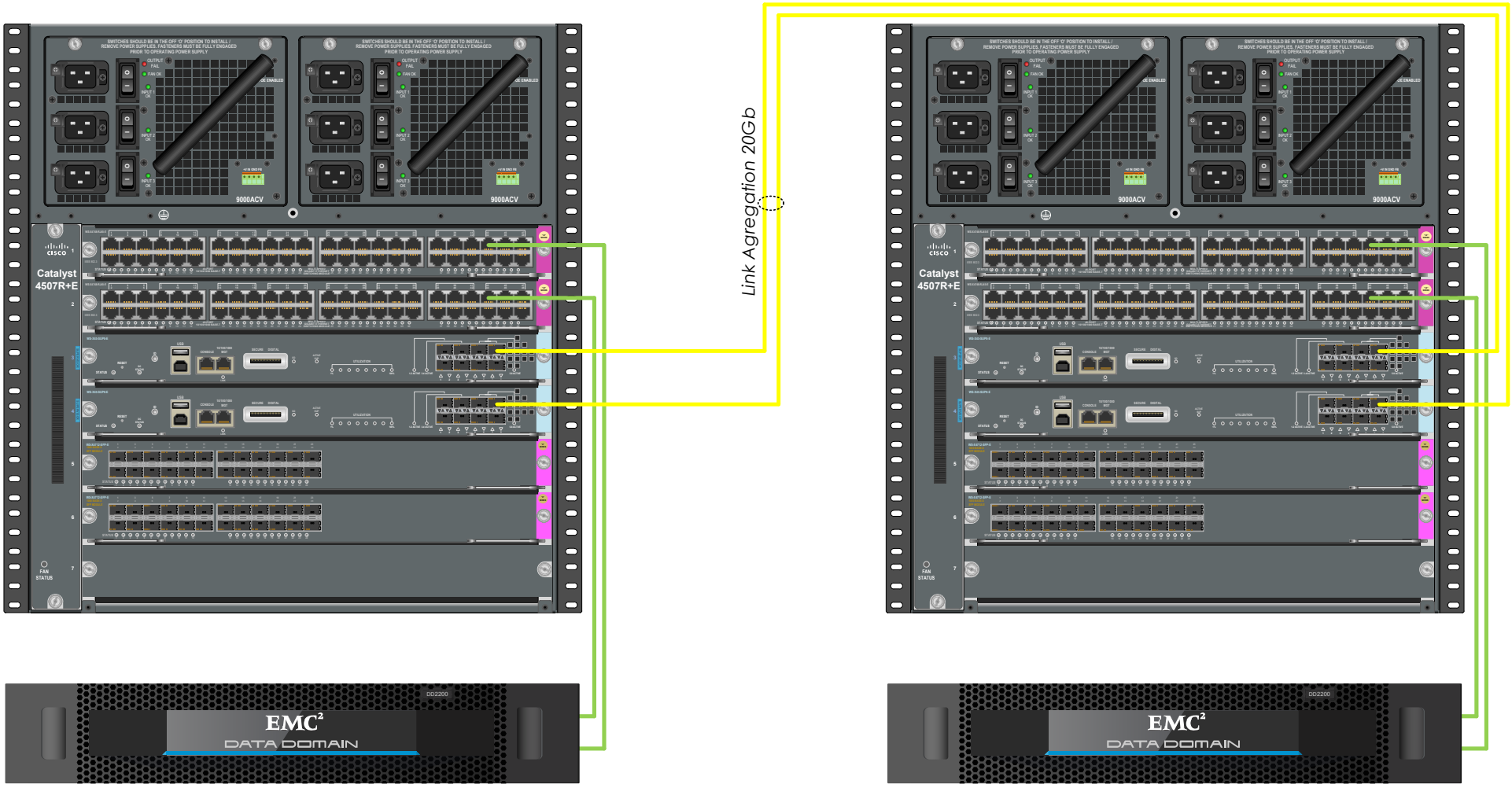
Management
iSCSI-0
iSCSI-1

Área de Tecnología, Redes y Telecomunicaciones.

Plano **Diseño de DataDomain**

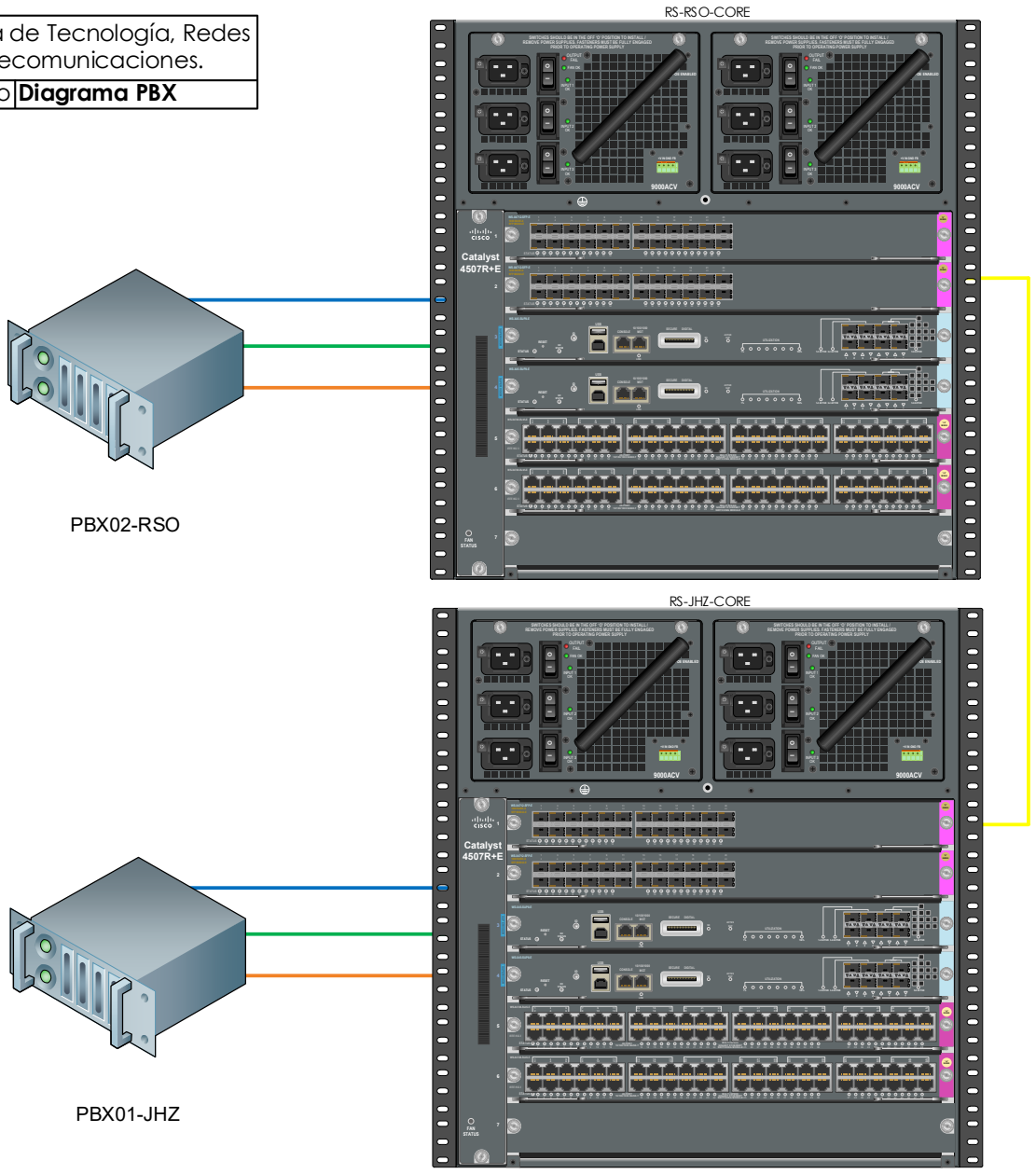
EDIFICIO RAUL SCALABRINI ORTIZ

EDIFICIO JOSE HERNANDEZ



Área de Tecnología, Redes y Telecomunicaciones.

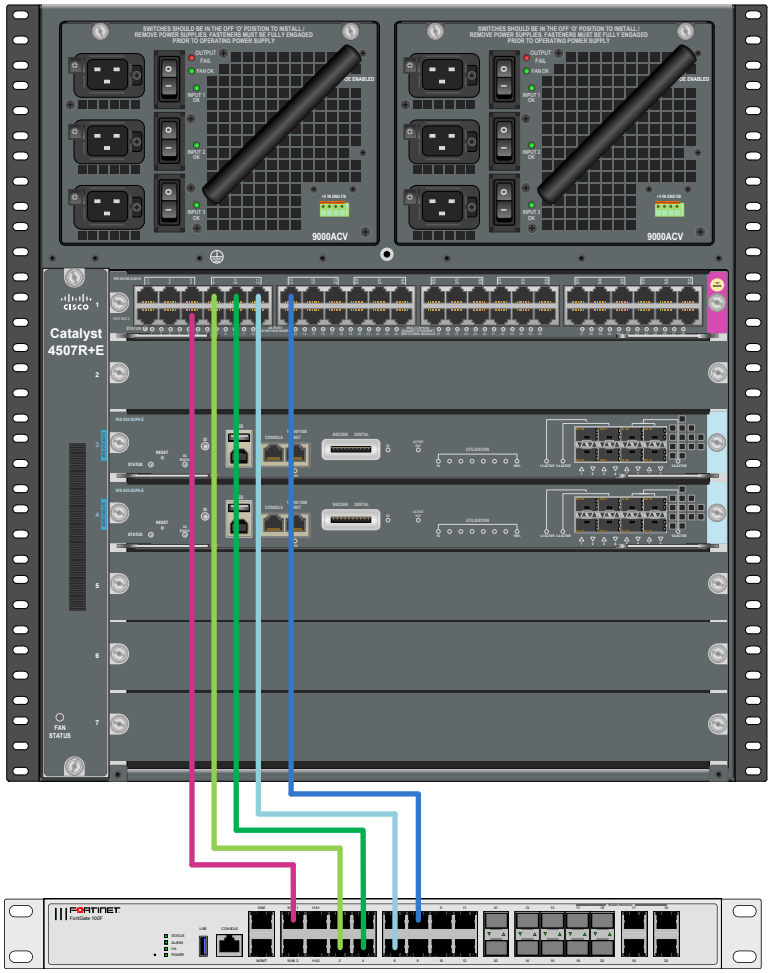
Plano **Diagrama PBX**



Área de Tecnología, Redes
y Telecomunicaciones.

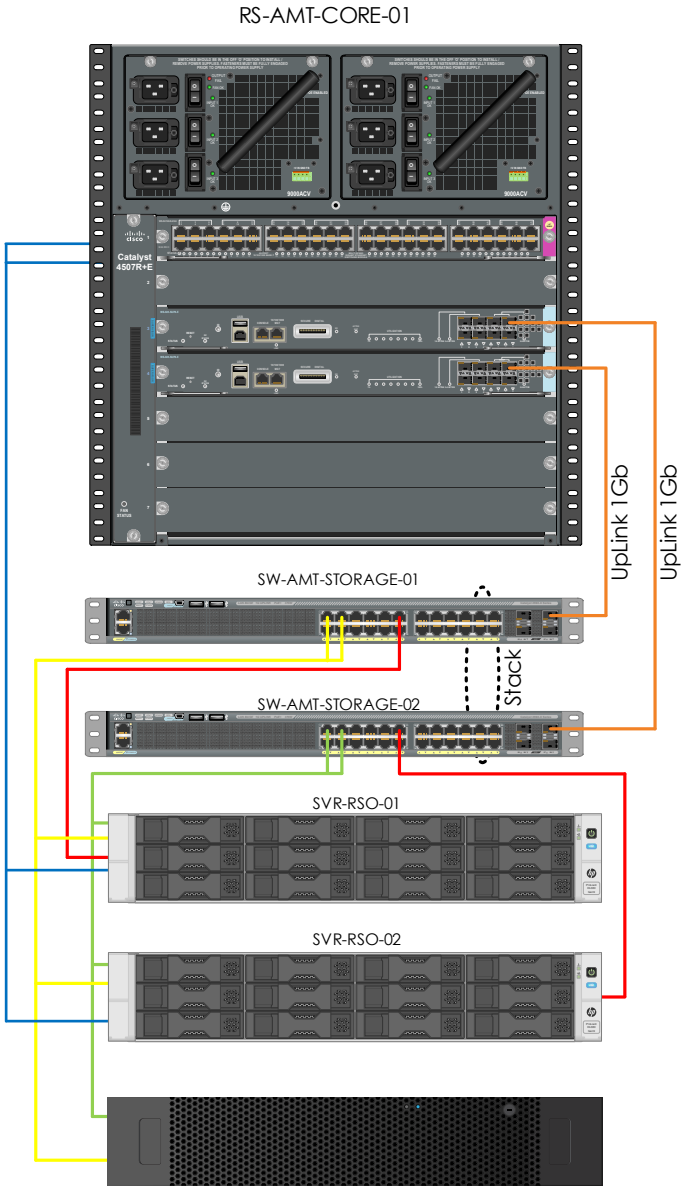
Plano **Diseño de Firewalling Abremate**

CORE AMT



Área de Tecnología, Redes y Telecomunicaciones.

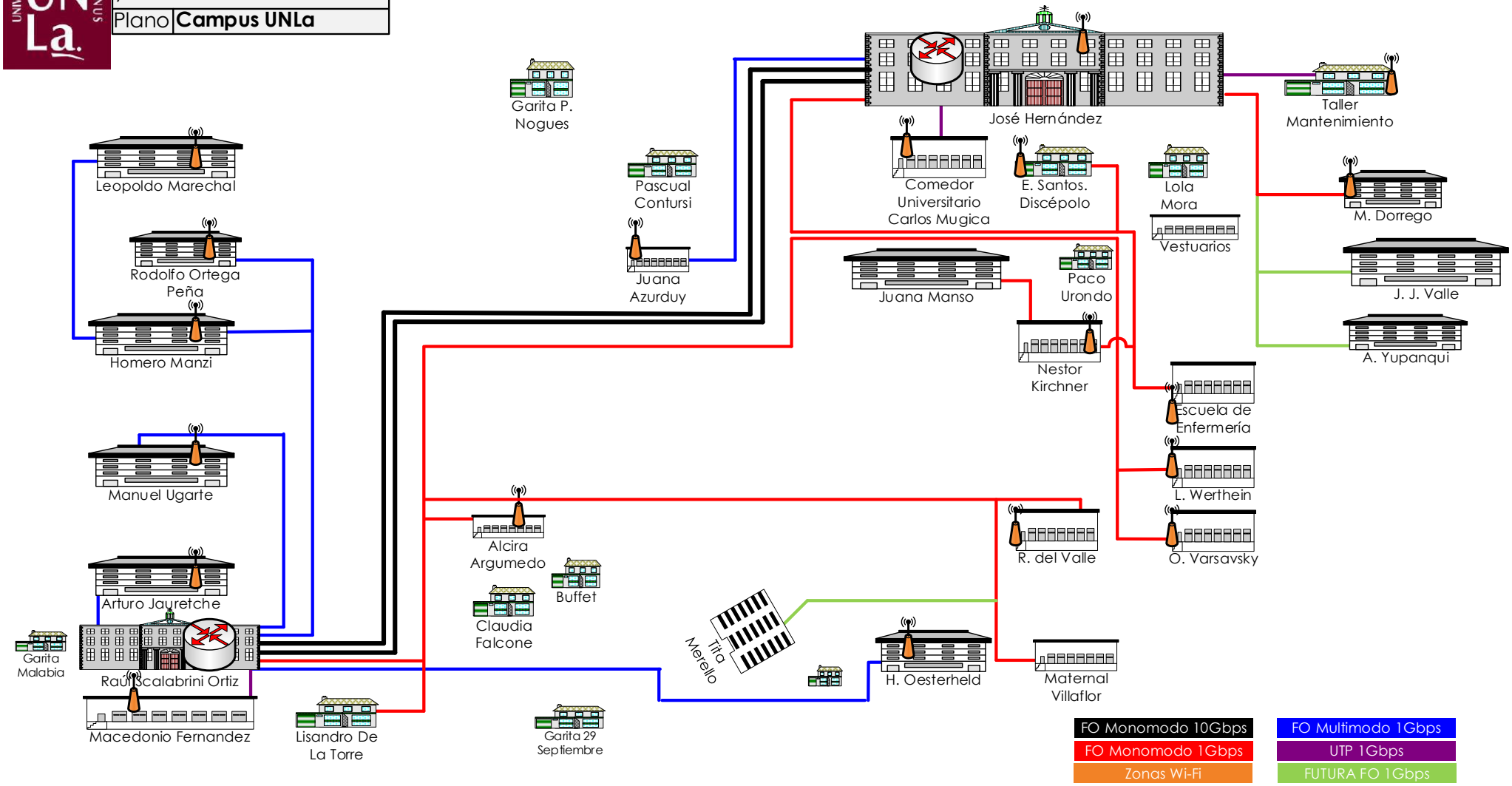
Plano **Core Abremate**



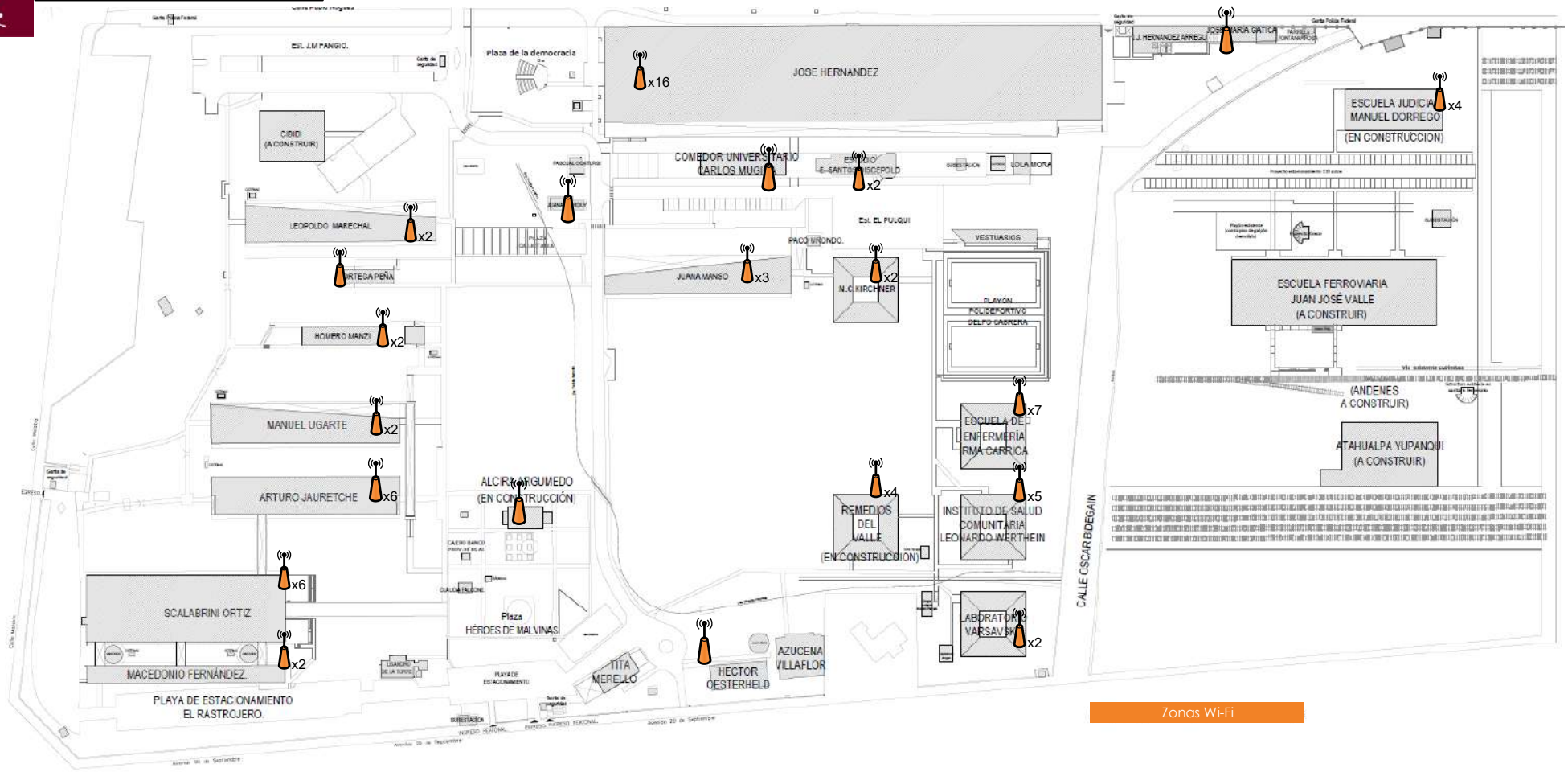
Management
Producción
iSCSI-0
iSCSI-1

Área de Tecnología, Redes y Telecomunicaciones.

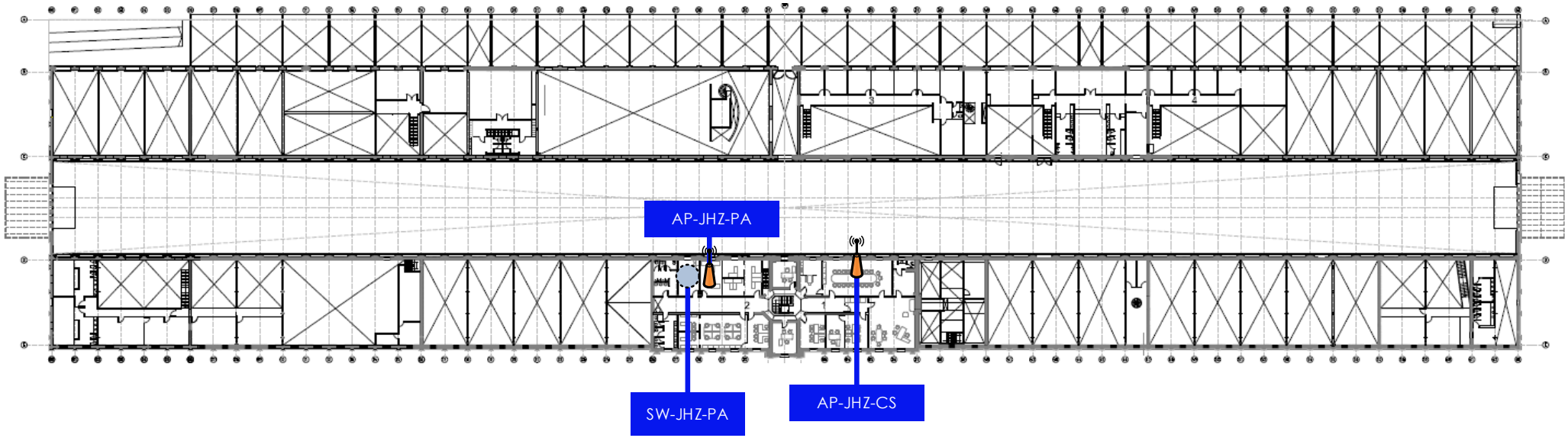
Plano **Campus UNLa**



Área de Tecnología, Redes y Telecomunicaciones.	
Plano	**Zonas WiFi UNLa**

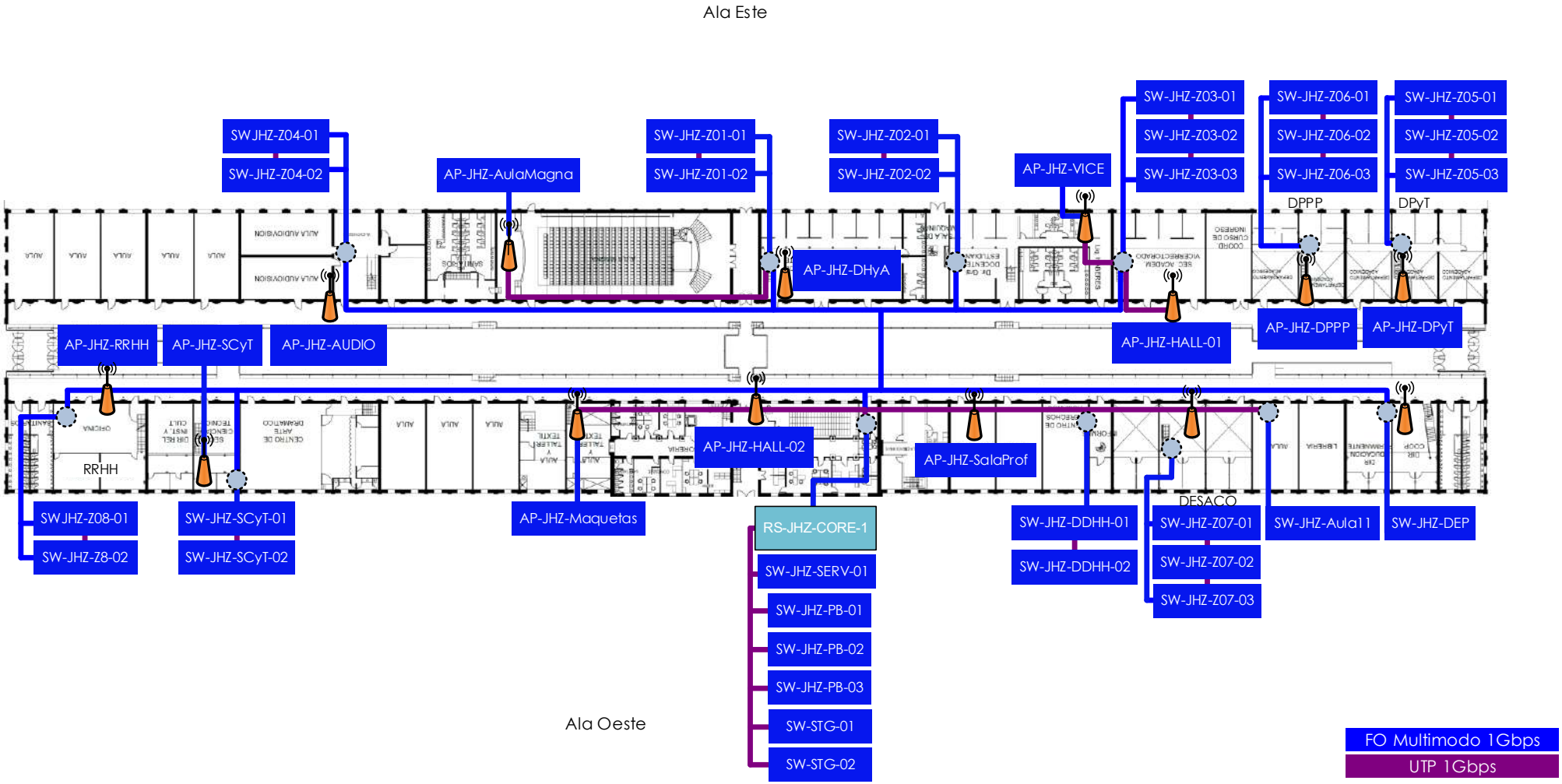


Área de Tecnología, Redes y Telecomunicaciones.	
Plano	Edificio **J. Hernandez PA**



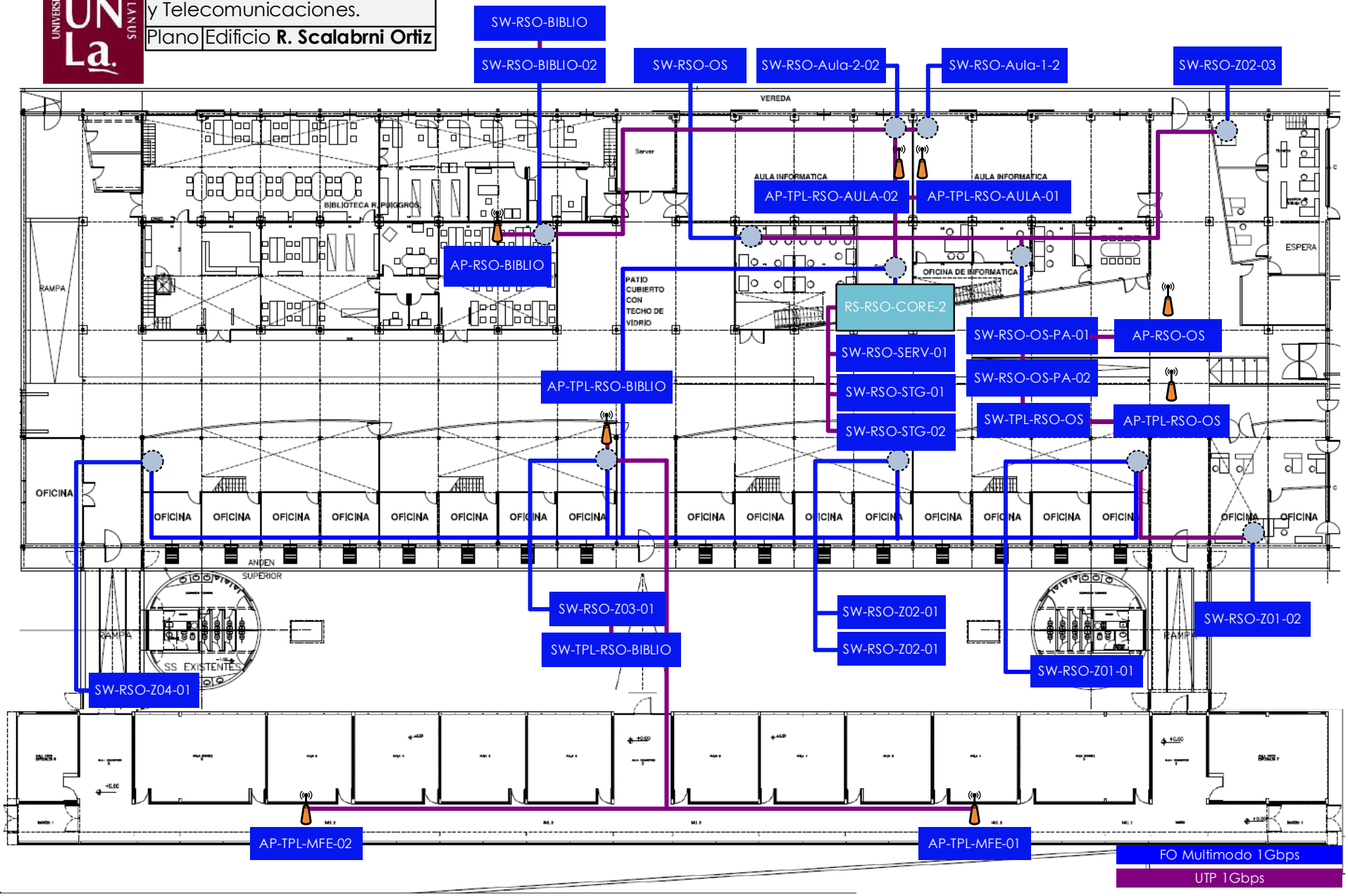
Área de Tecnología, Redes y Telecomunicaciones.

Plano | Edificio **J. Hernandez PB**



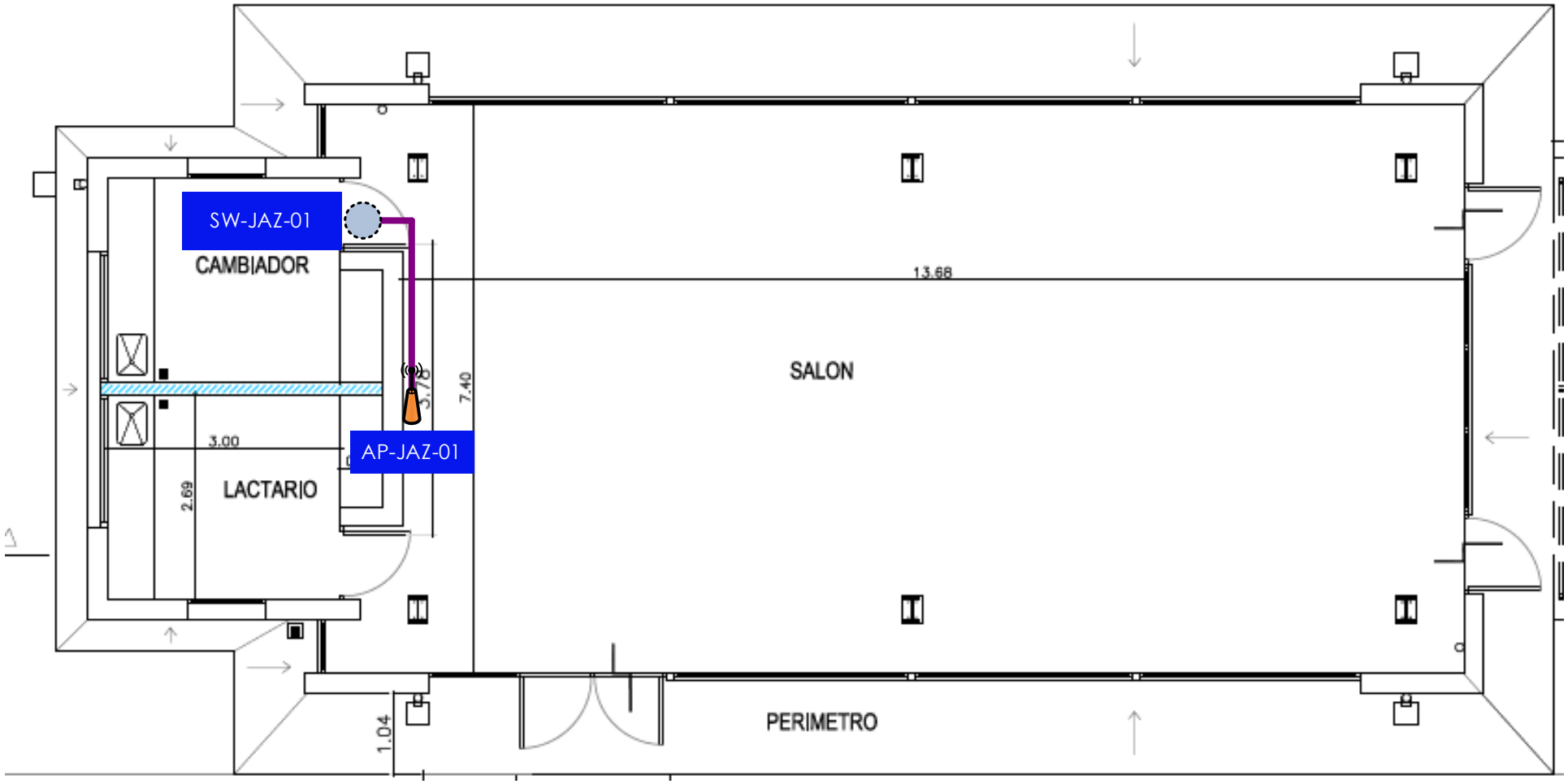
Área de Tecnología, Redes y Telecomunicaciones.

Plano | Edificio **R. Scalabrni Ortiz**



Área de Tecnología, Redes y Telecomunicaciones.

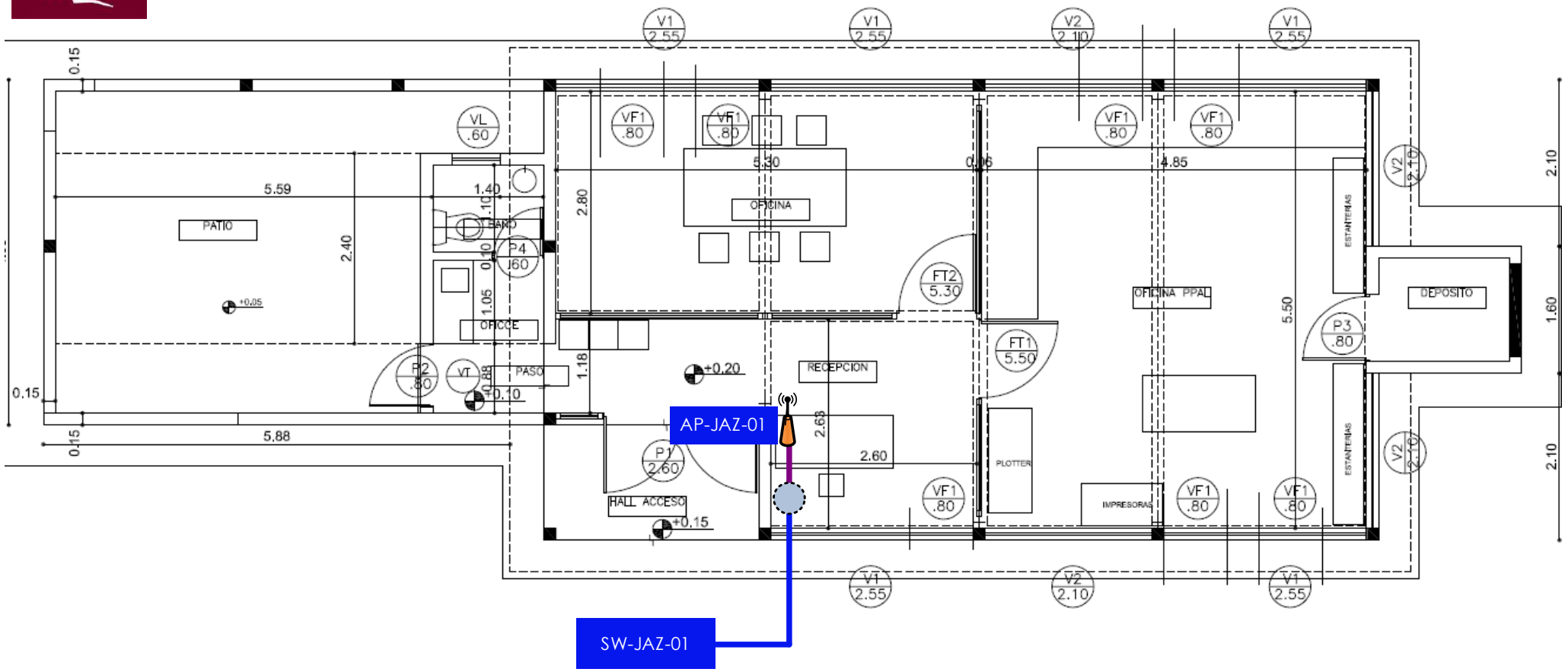
Plano | Edificio **A. Argumedo**



UTP 1Gbps

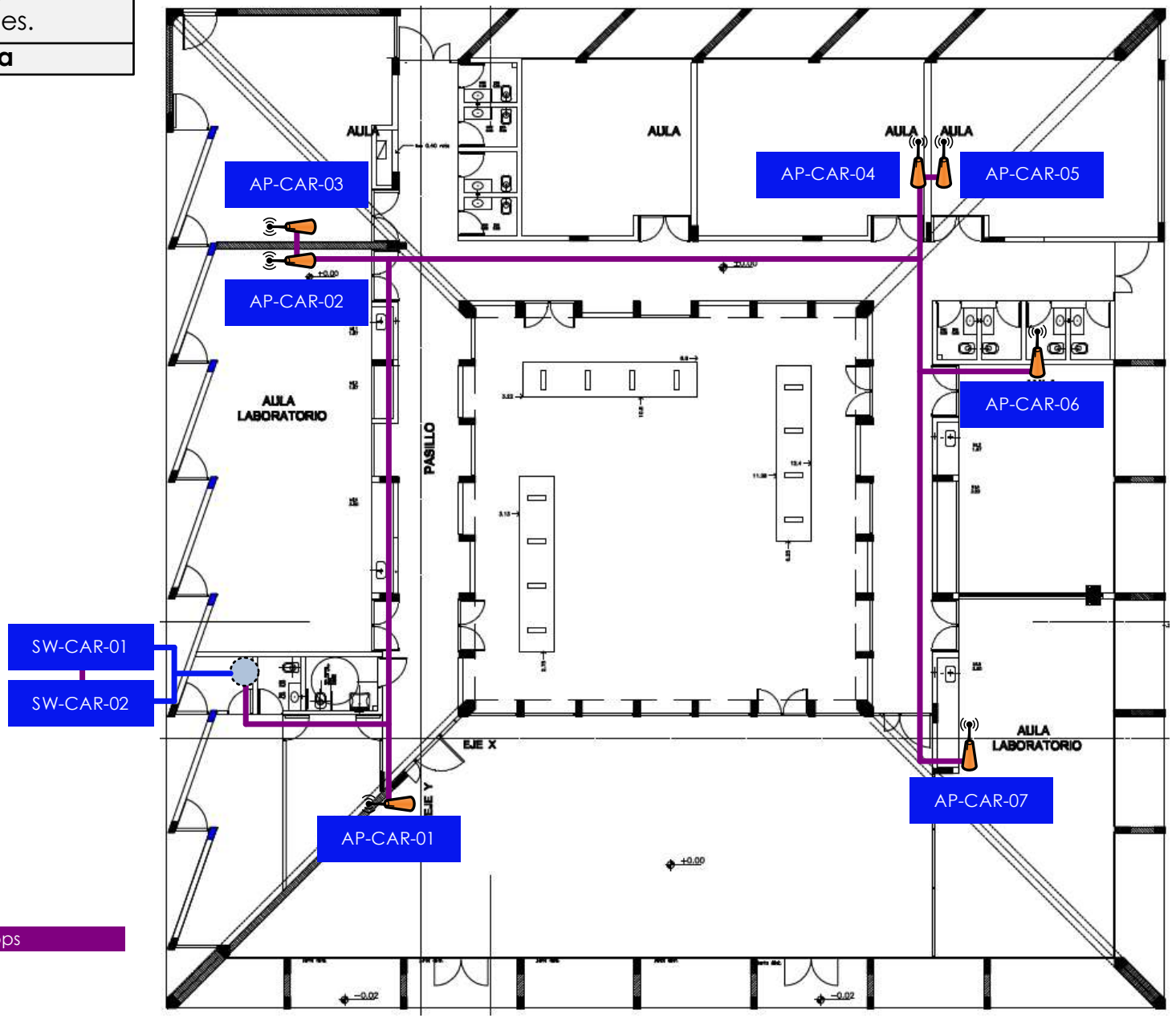
Área de Tecnología, Redes y Telecomunicaciones.

Plano | Edificio **J. Azurduy**



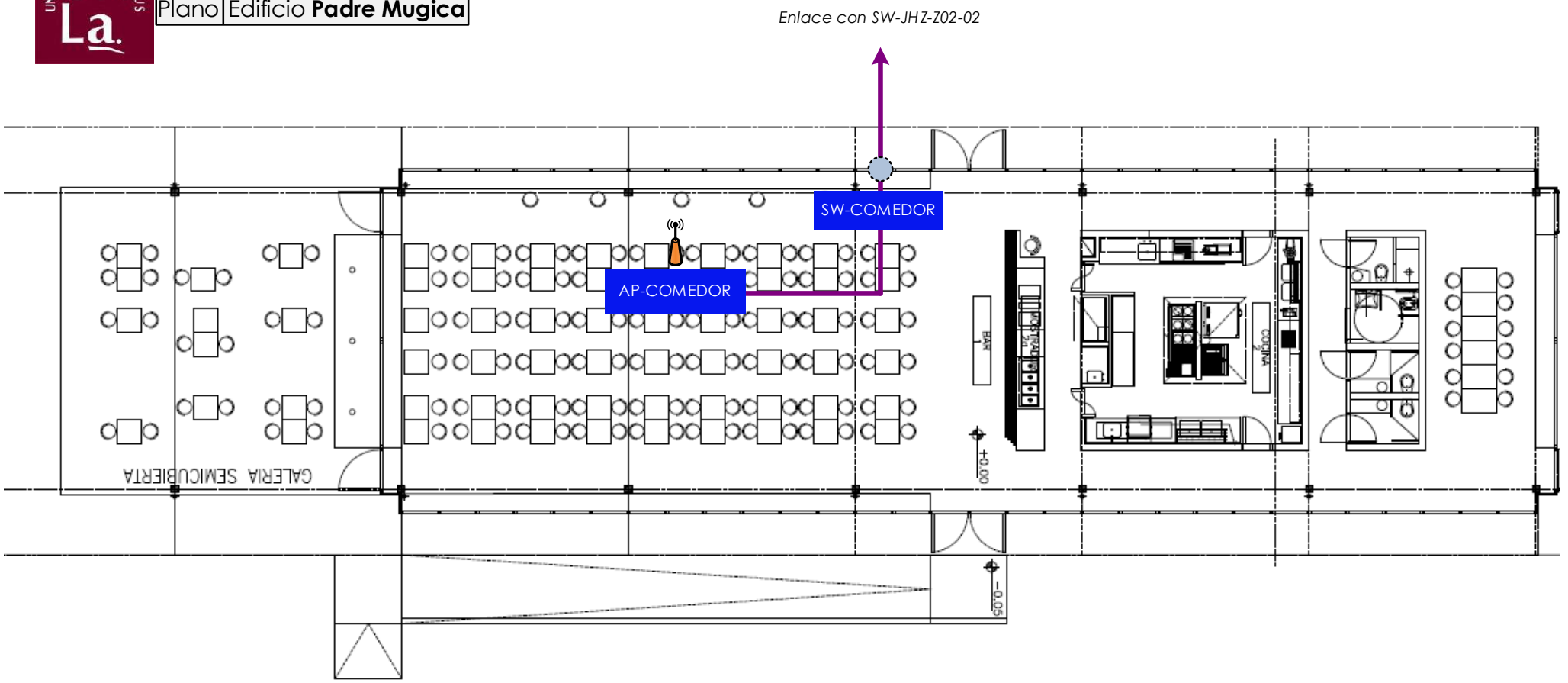
UTP 1Gbps

Área de Tecnología, Redes y Telecomunicaciones.	
Plano	Edificio **Carrica**



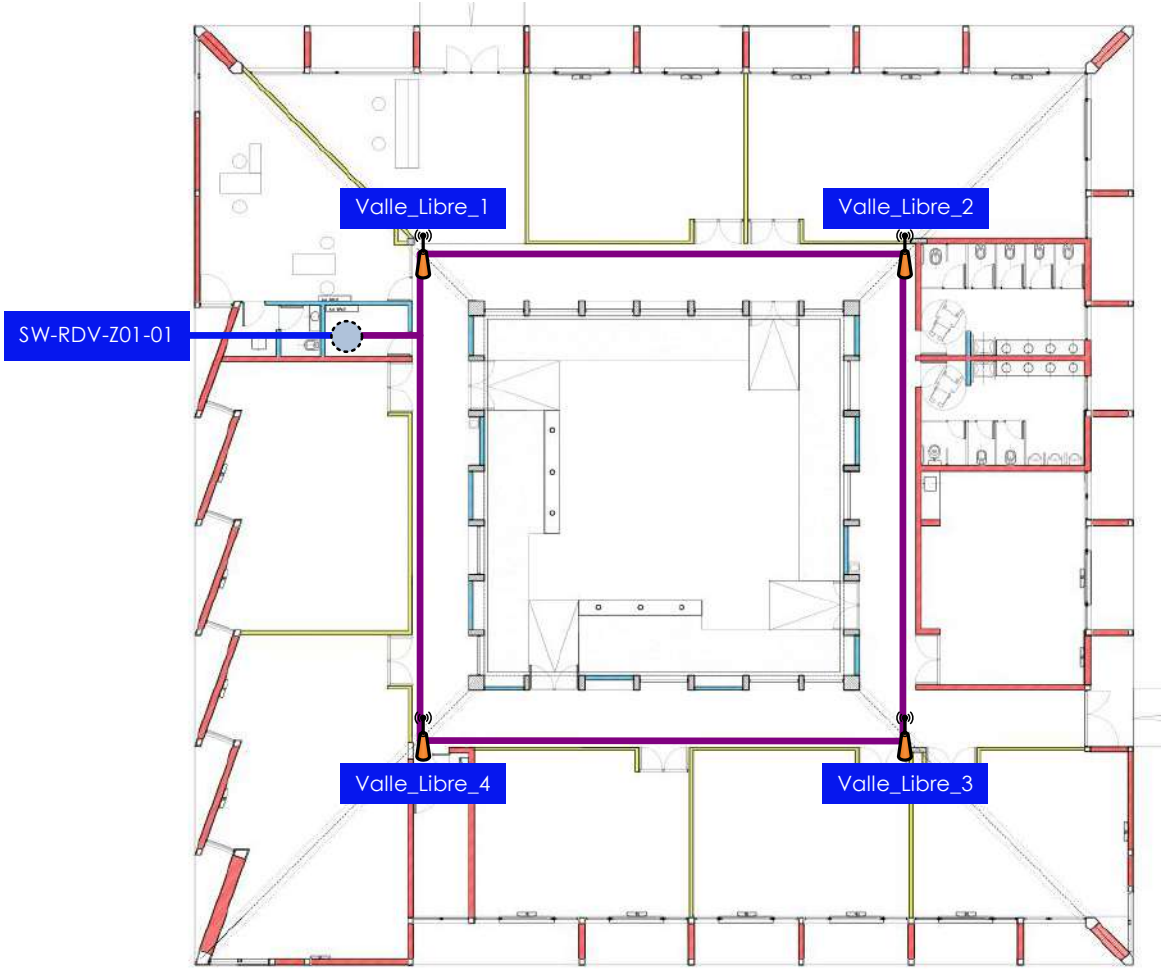
Área de Tecnología, Redes y Telecomunicaciones.

Plano | Edificio **Padre Mugica**



UTP 1Gbps

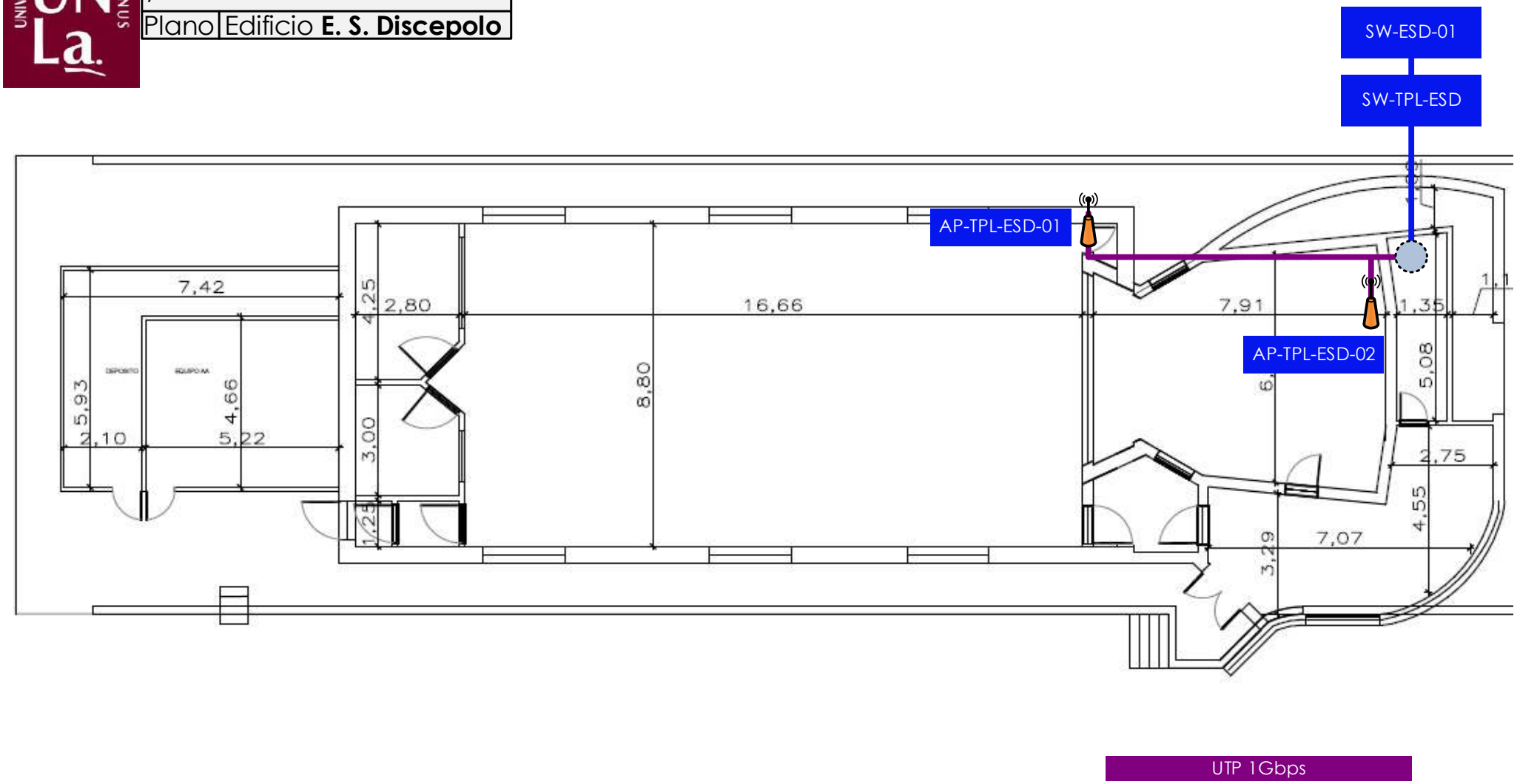
Área de Tecnología, Redes y Telecomunicaciones.	
Plano	Edificio **R. Del Valle**



UTP 1Gbps

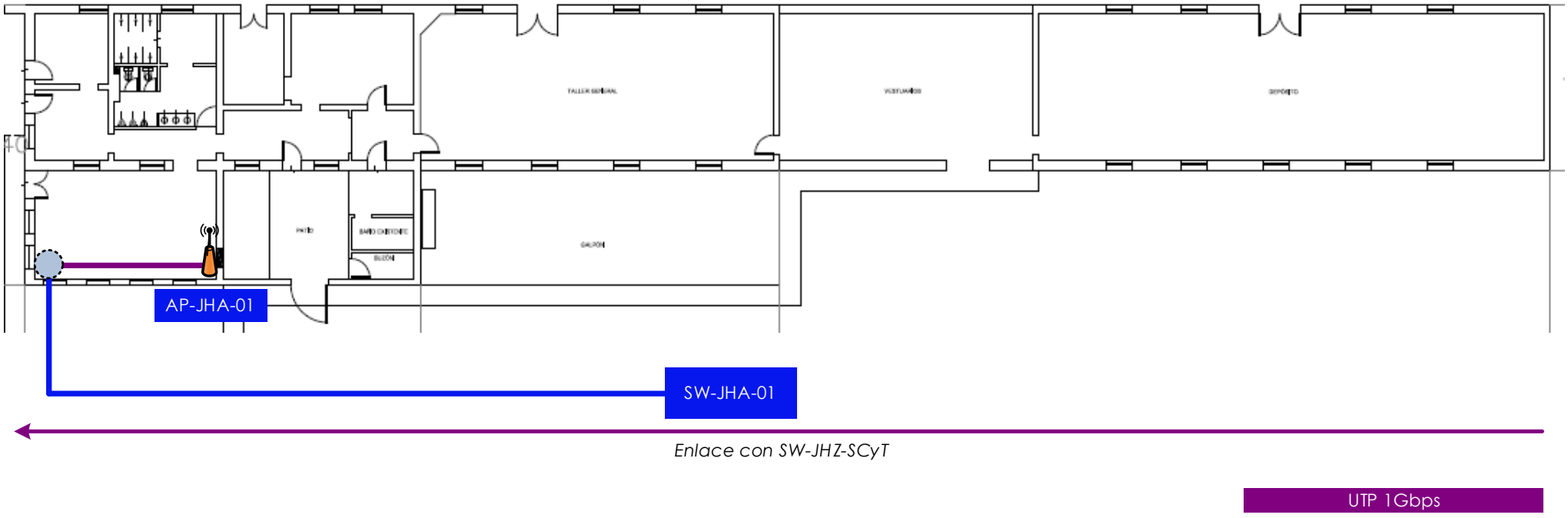
Área de Tecnología, Redes y Telecomunicaciones.

Plano | Edificio **E. S. Discepolo**

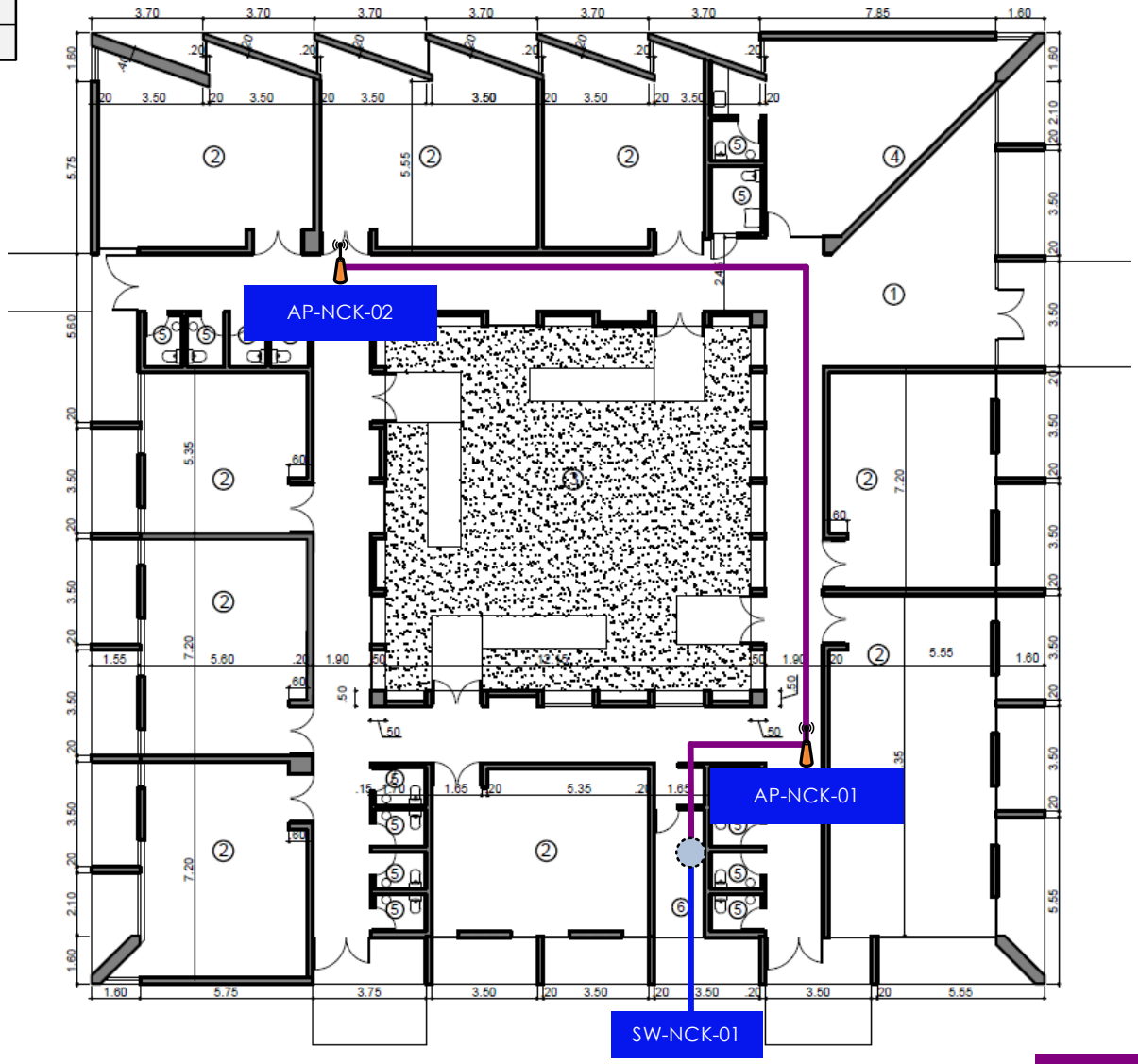


Área de Tecnología, Redes y Telecomunicaciones.

Plano | Edificio **H. Arregui**

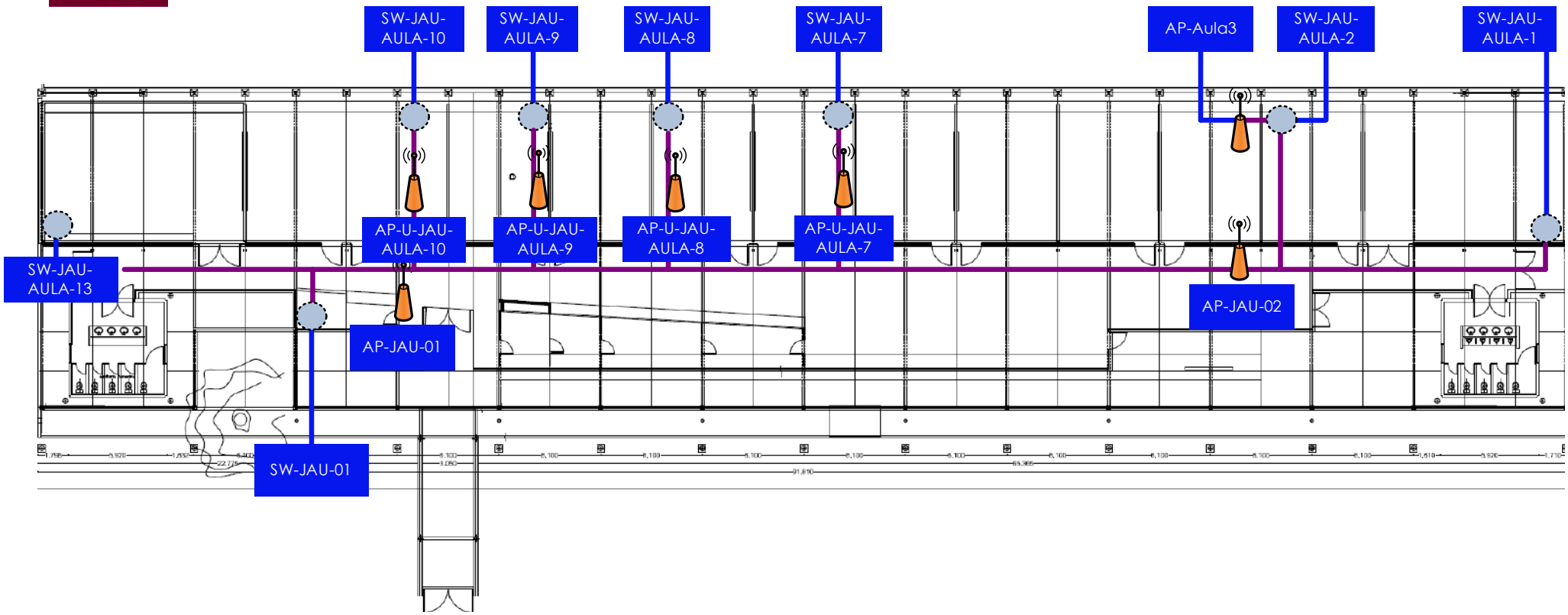


Área de Tecnología, Redes y Telecomunicaciones.	
Plano	Edificio **N. Kirchner**



Área de Tecnología, Redes y Telecomunicaciones.

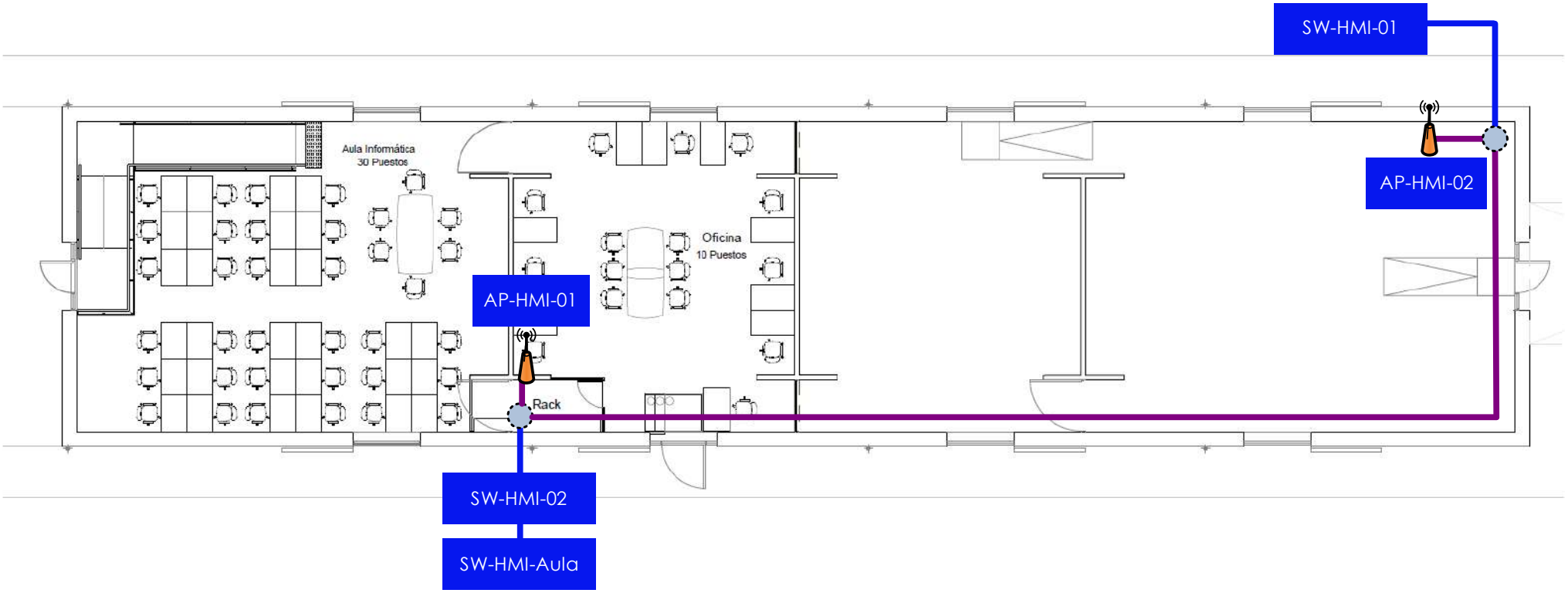
Plano | Edificio **A. Jauretche**



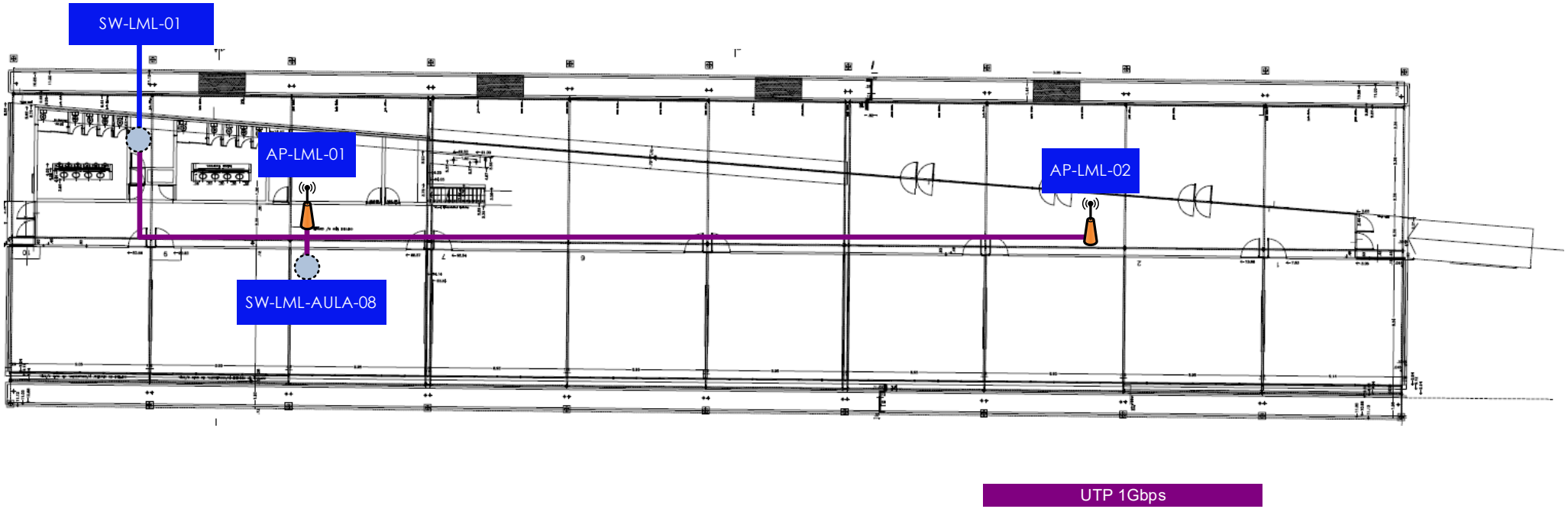
UTP 1Gbps

Área de Tecnología, Redes y Telecomunicaciones.

Plano | Edificio **H. Manzi**

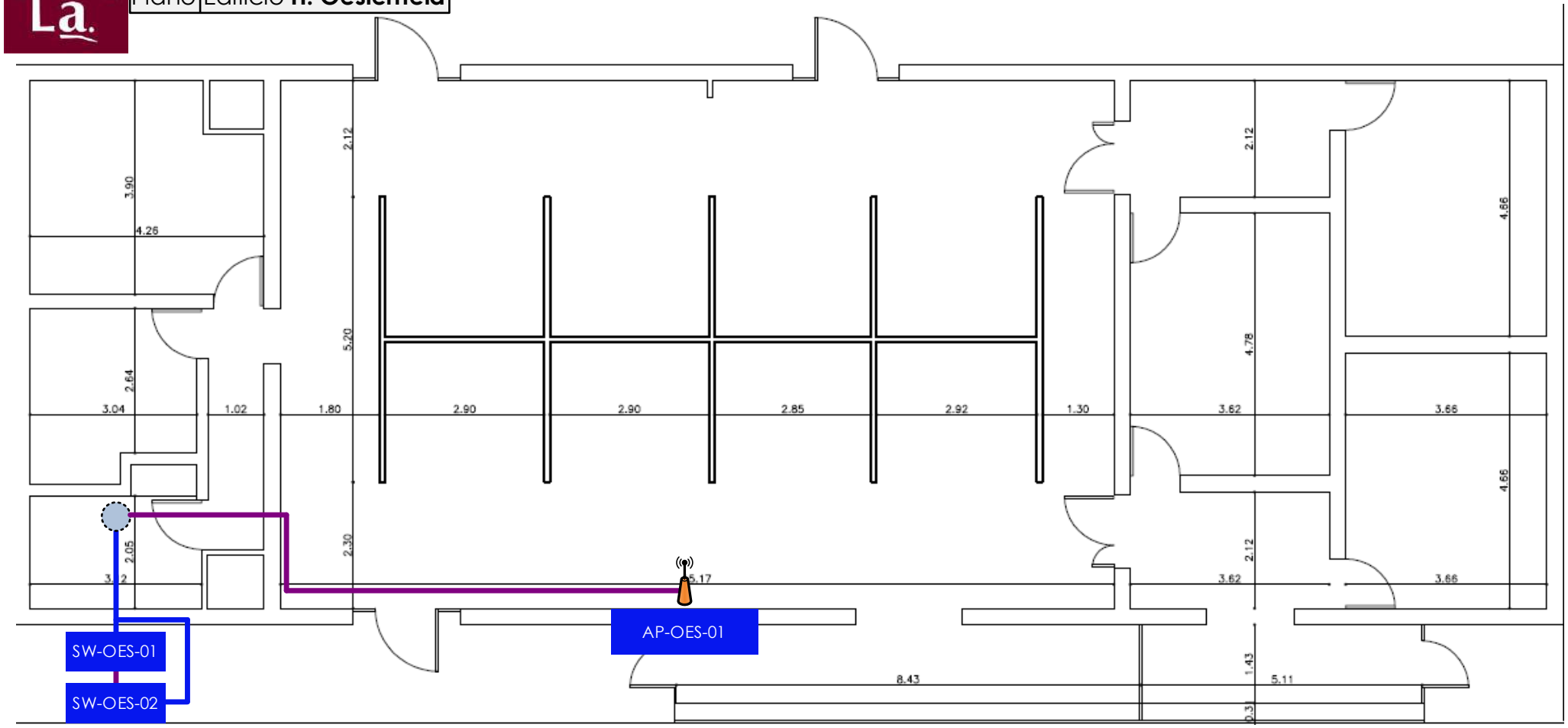


Área de Tecnología, Redes y Telecomunicaciones.	
Plano	Edificio **L. Marechal**

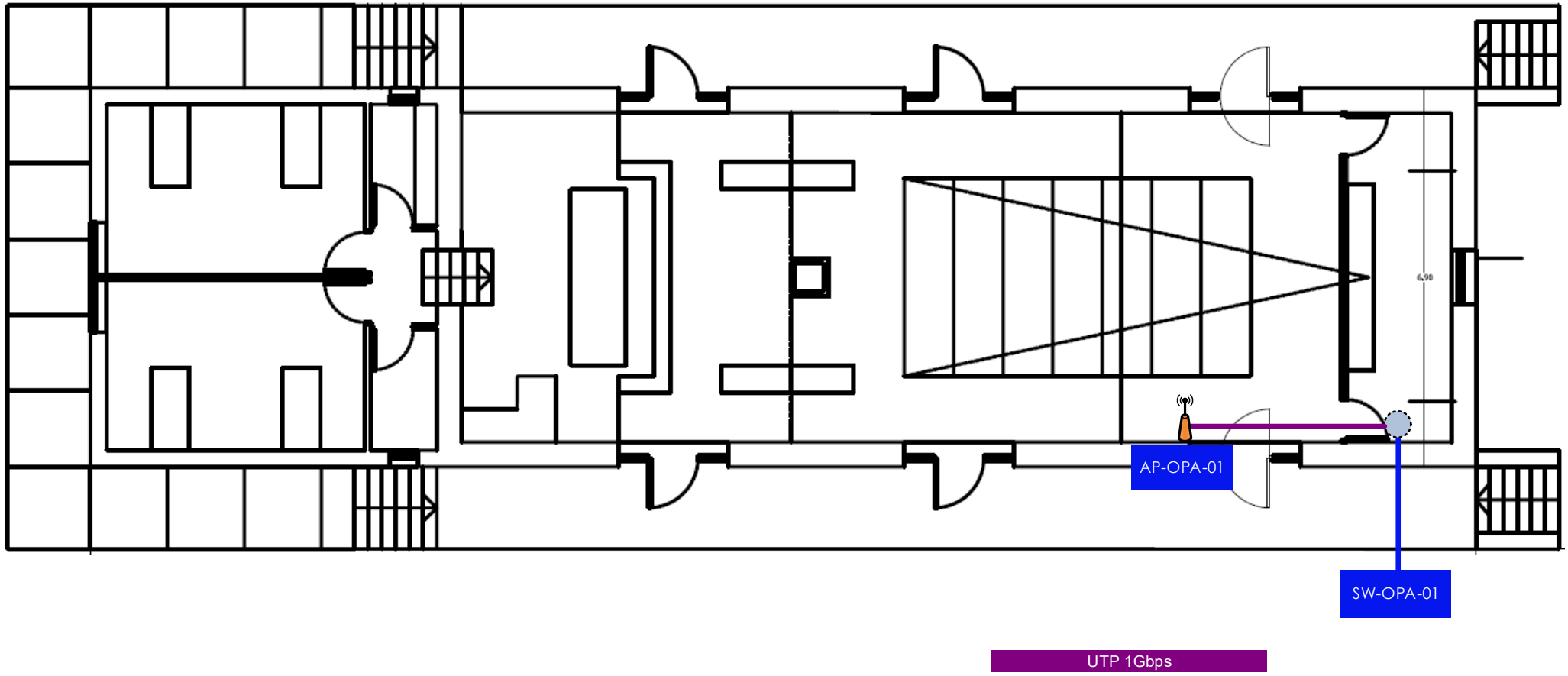


Área de Tecnología, Redes y Telecomunicaciones.

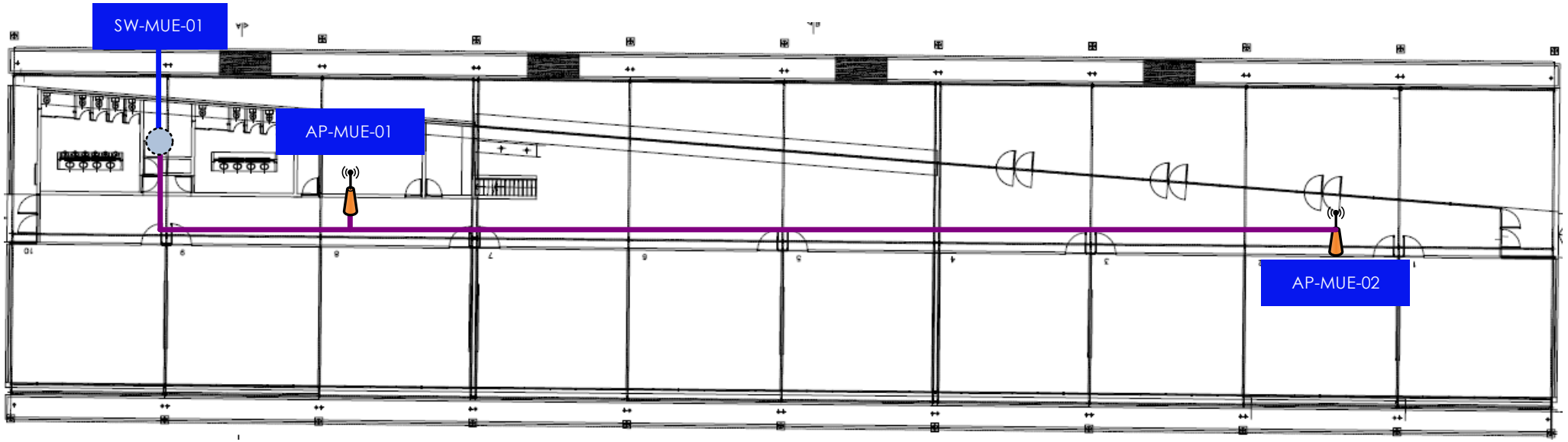
Plano | Edificio **H. Oesterheld**



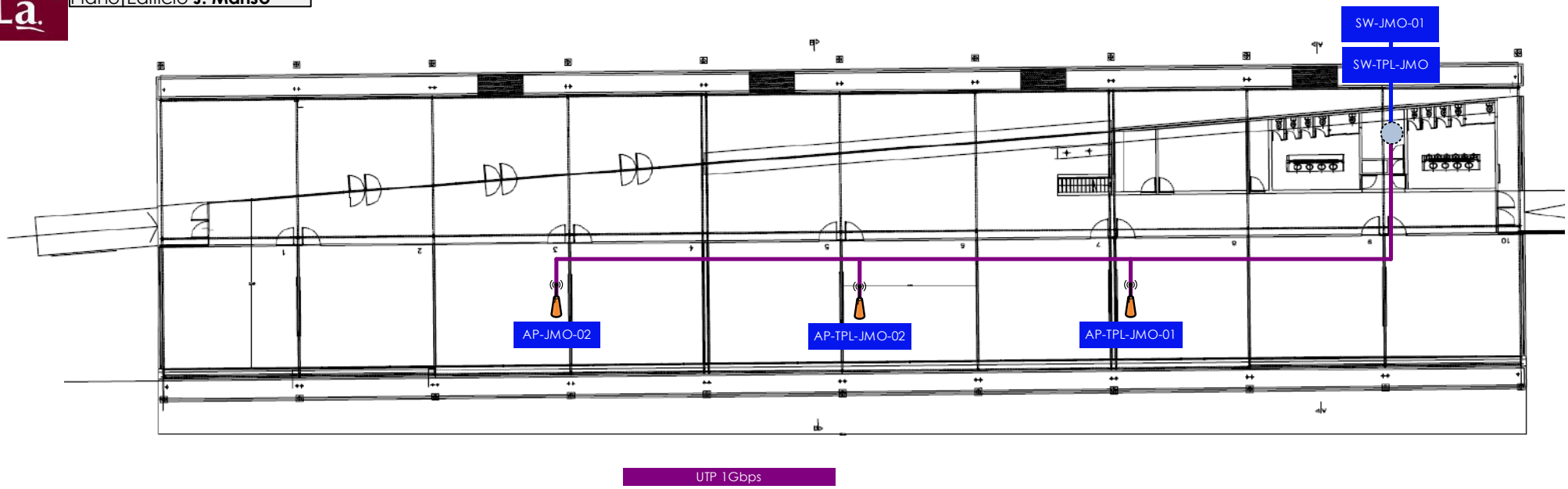
Área de Tecnología, Redes y Telecomunicaciones.	
Plano	Edificio **O. Peña**



UNIVERSIDAD NACIONAL DE LANUS UNLa.	Área de Tecnología, Redes y Telecomunicaciones.
Plano	Edificio **M. Ugarte**

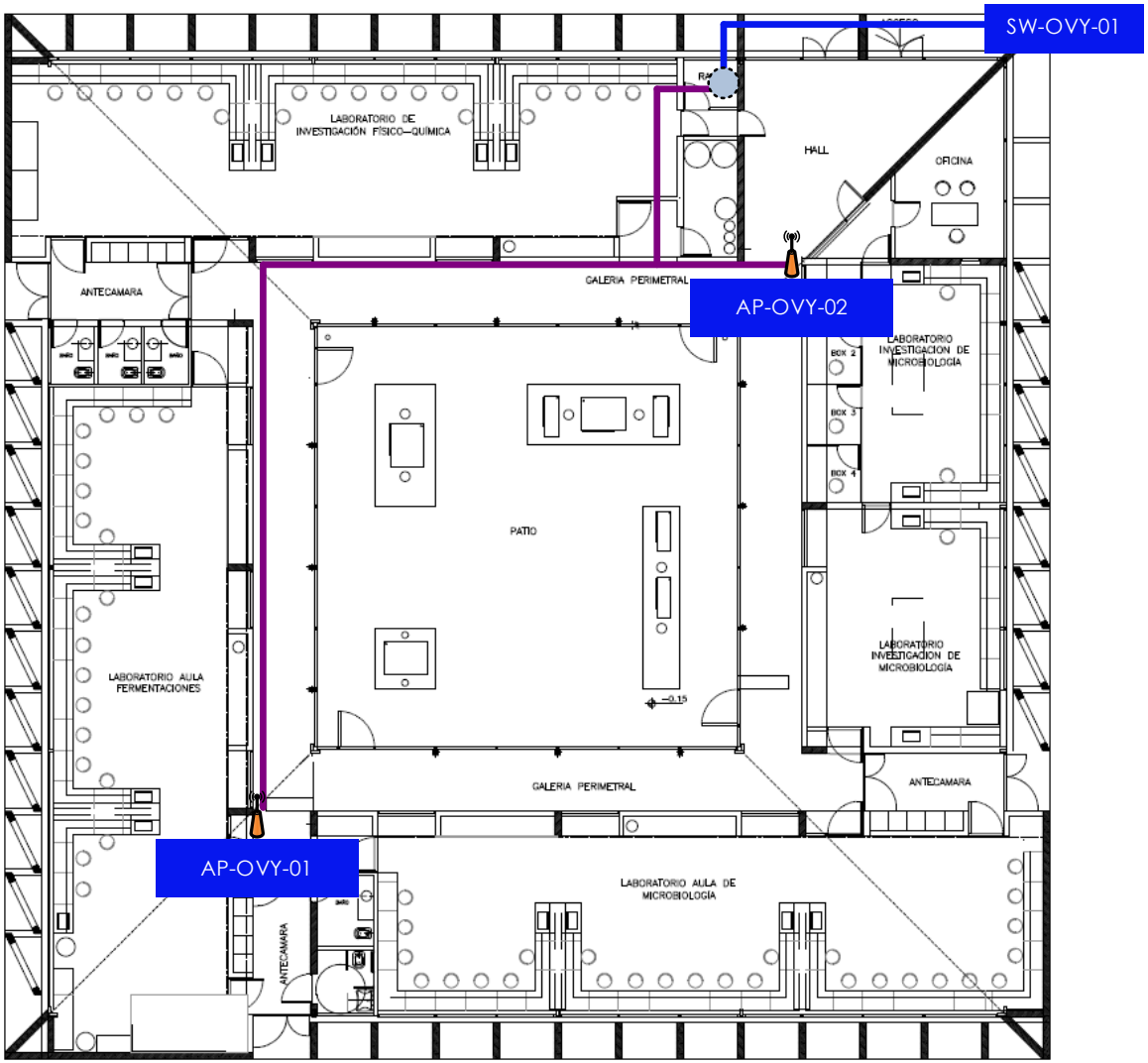


Área de Tecnología, Redes y Telecomunicaciones.
Plano|Edificio **J. Manso**



Área de Tecnología, Redes y Telecomunicaciones.

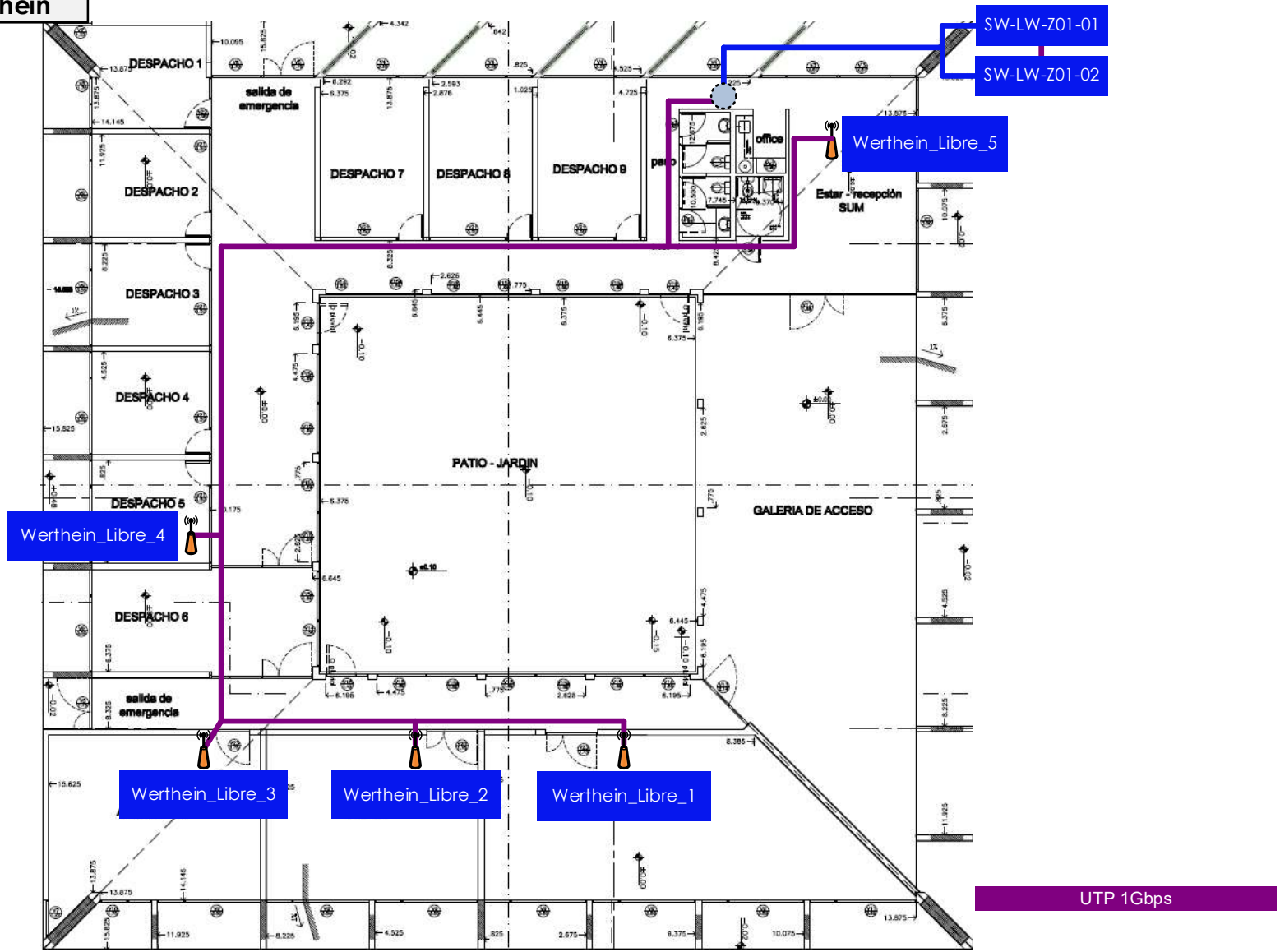
Plano | Edificio **O. Varsavsky**



UTP 1Gbps

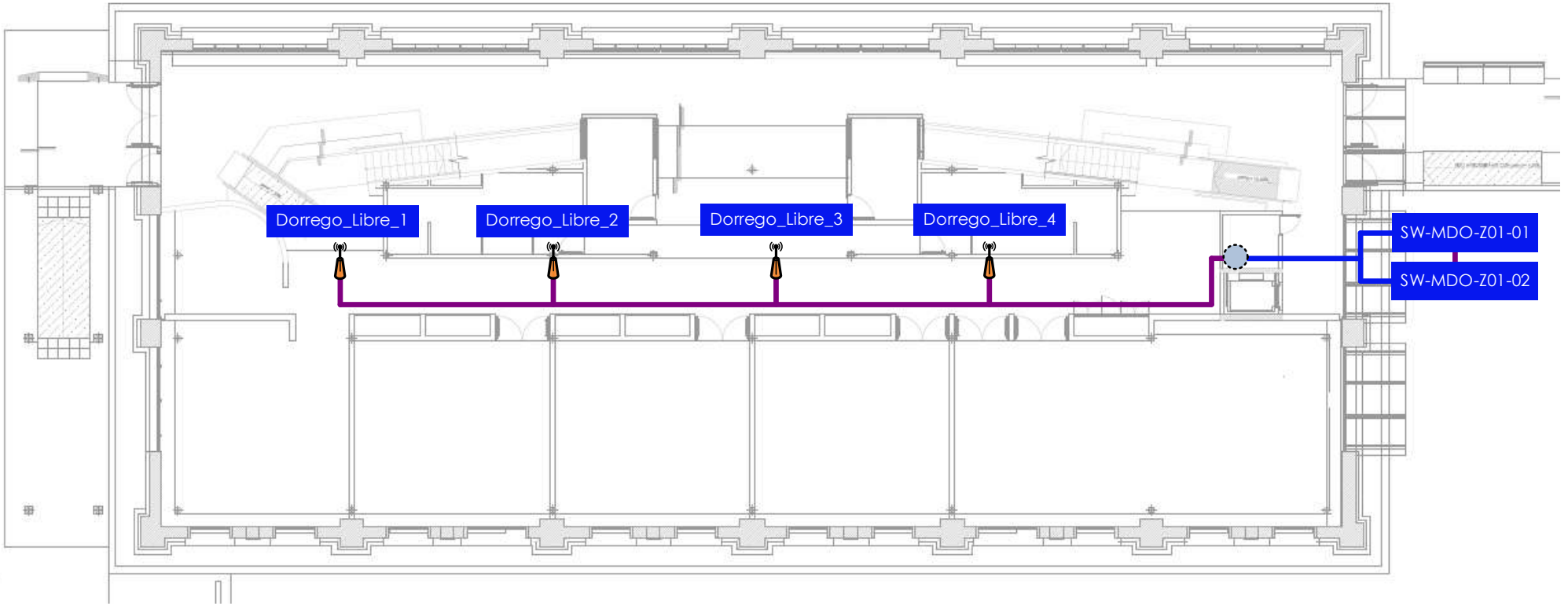
Área de Tecnología, Redes y Telecomunicaciones.

Plano | Edificio **L. Werthein**

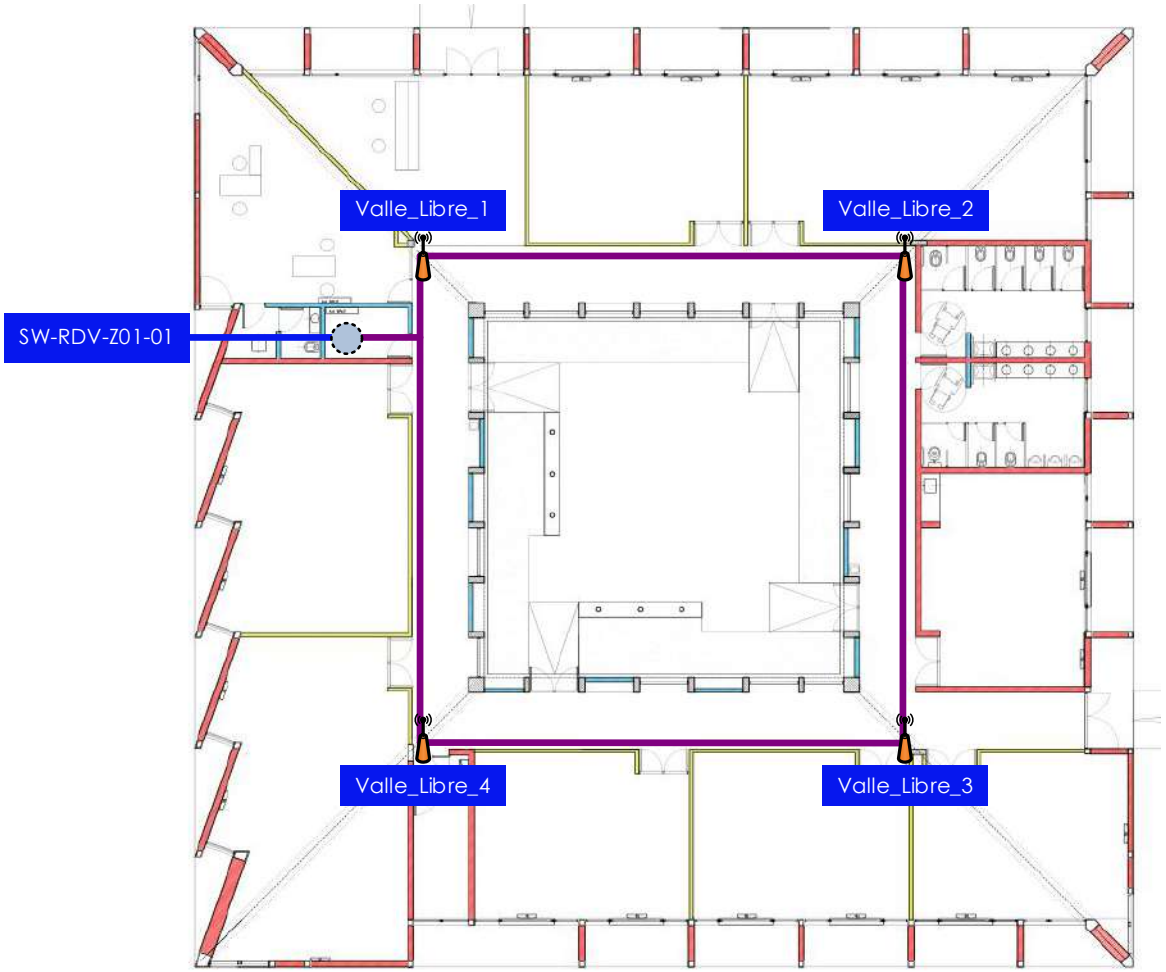


Área de Tecnología, Redes y Telecomunicaciones.

Plano | Edificio **M. Dorrego**

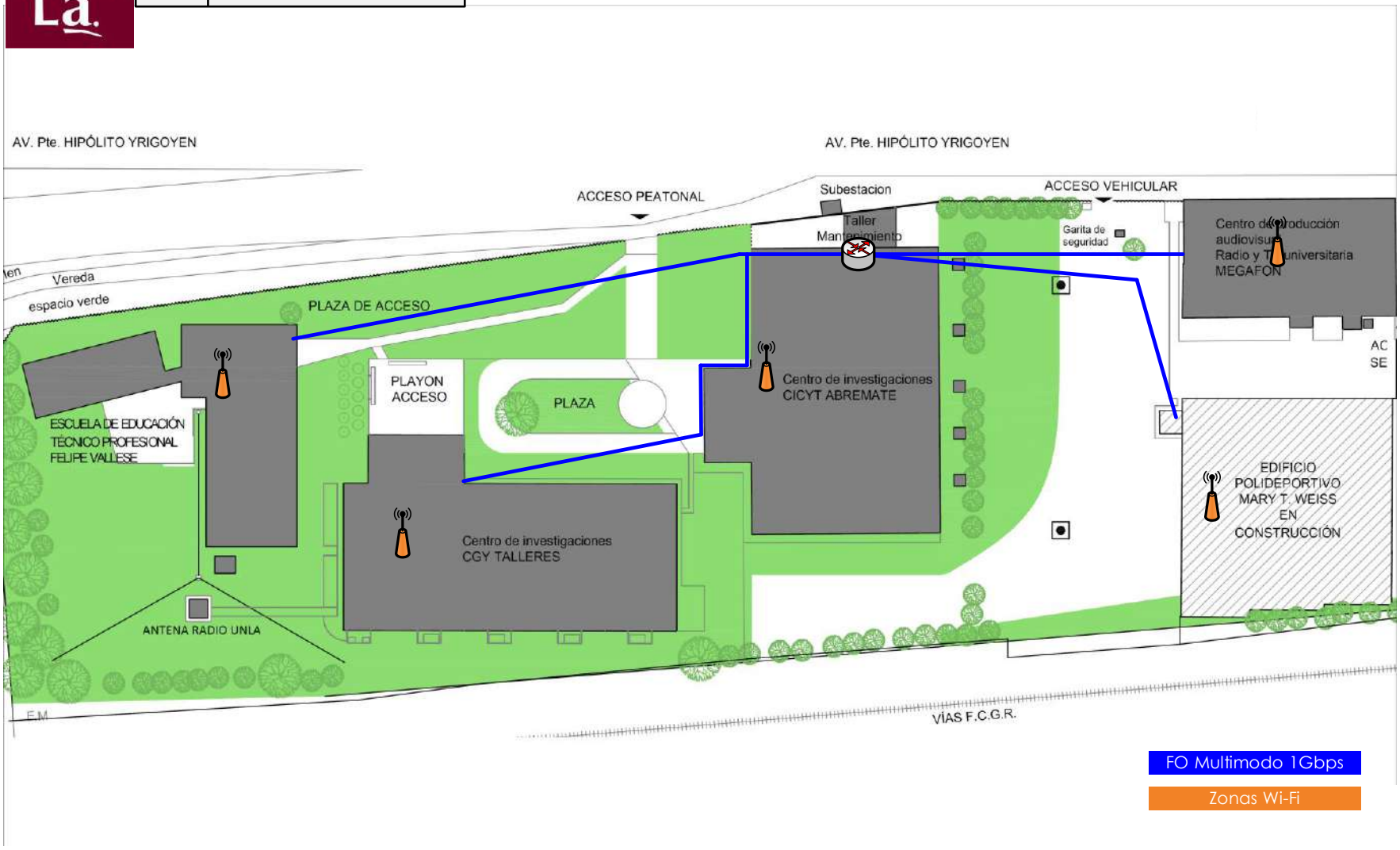


Área de Tecnología, Redes y Telecomunicaciones.	
Plano	Edificio **R. Del Valle**



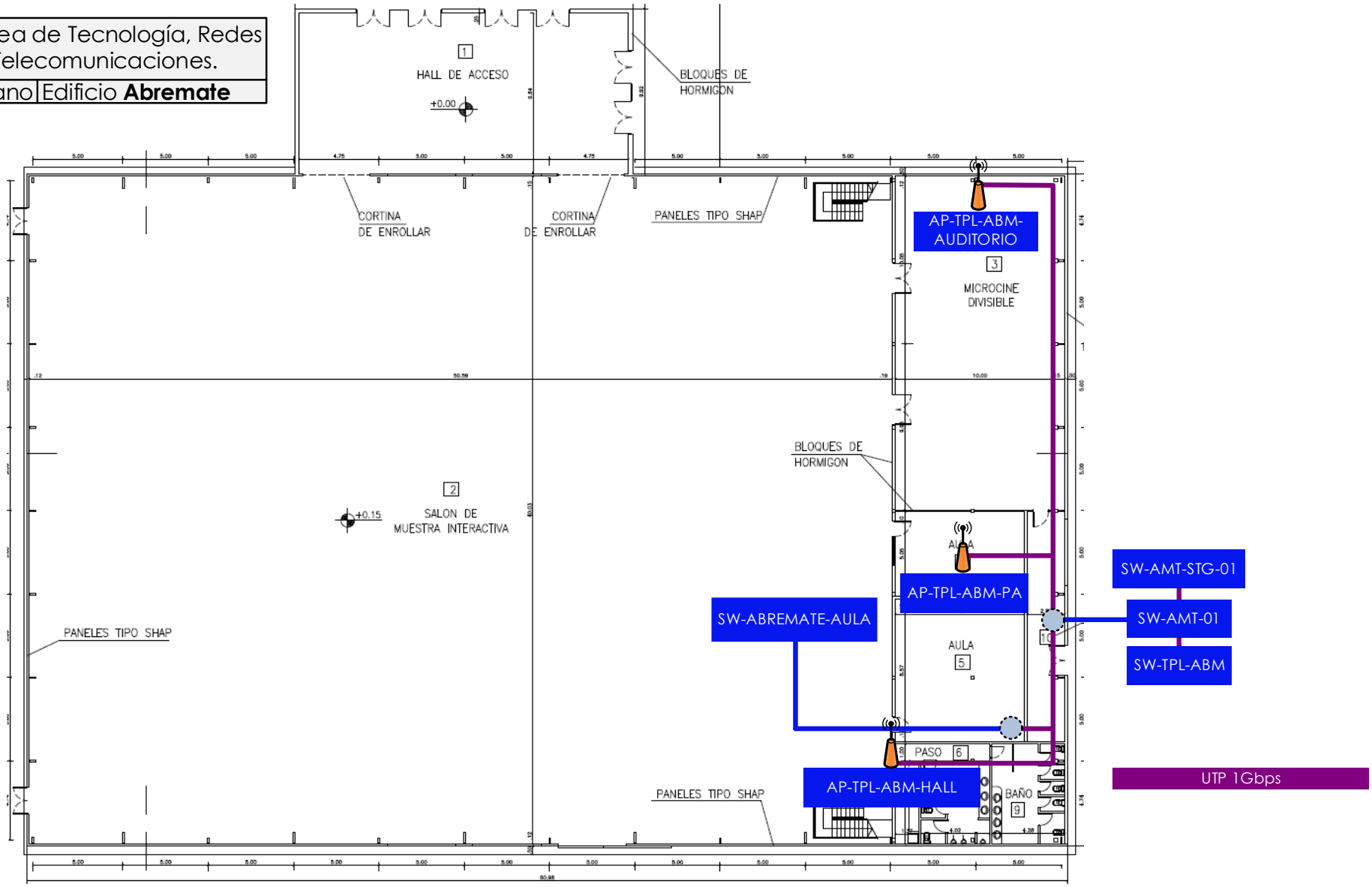
UTP 1Gbps

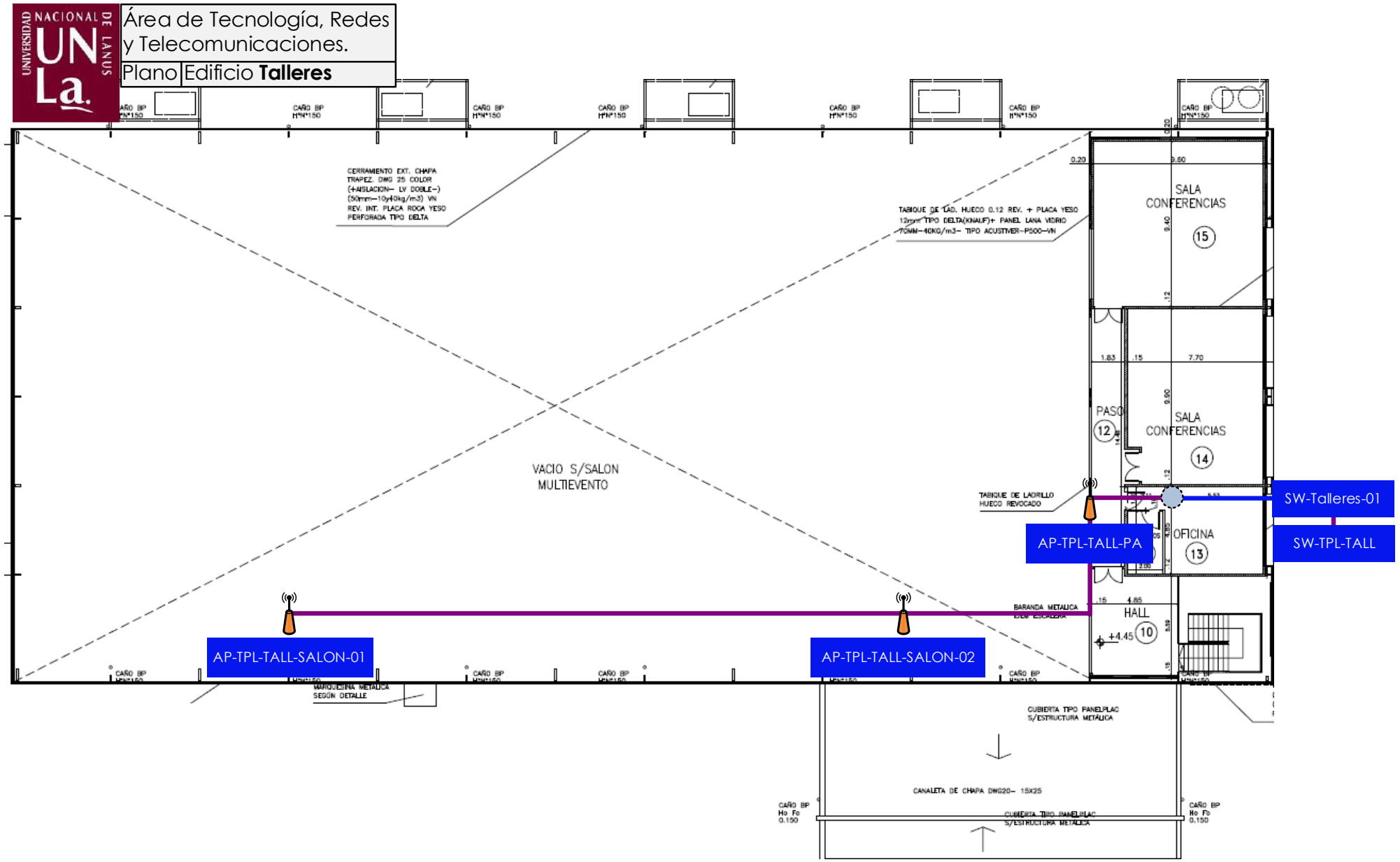
Área de Tecnología, Redes y Telecomunicaciones.	
Plano	**Predio Abremate**



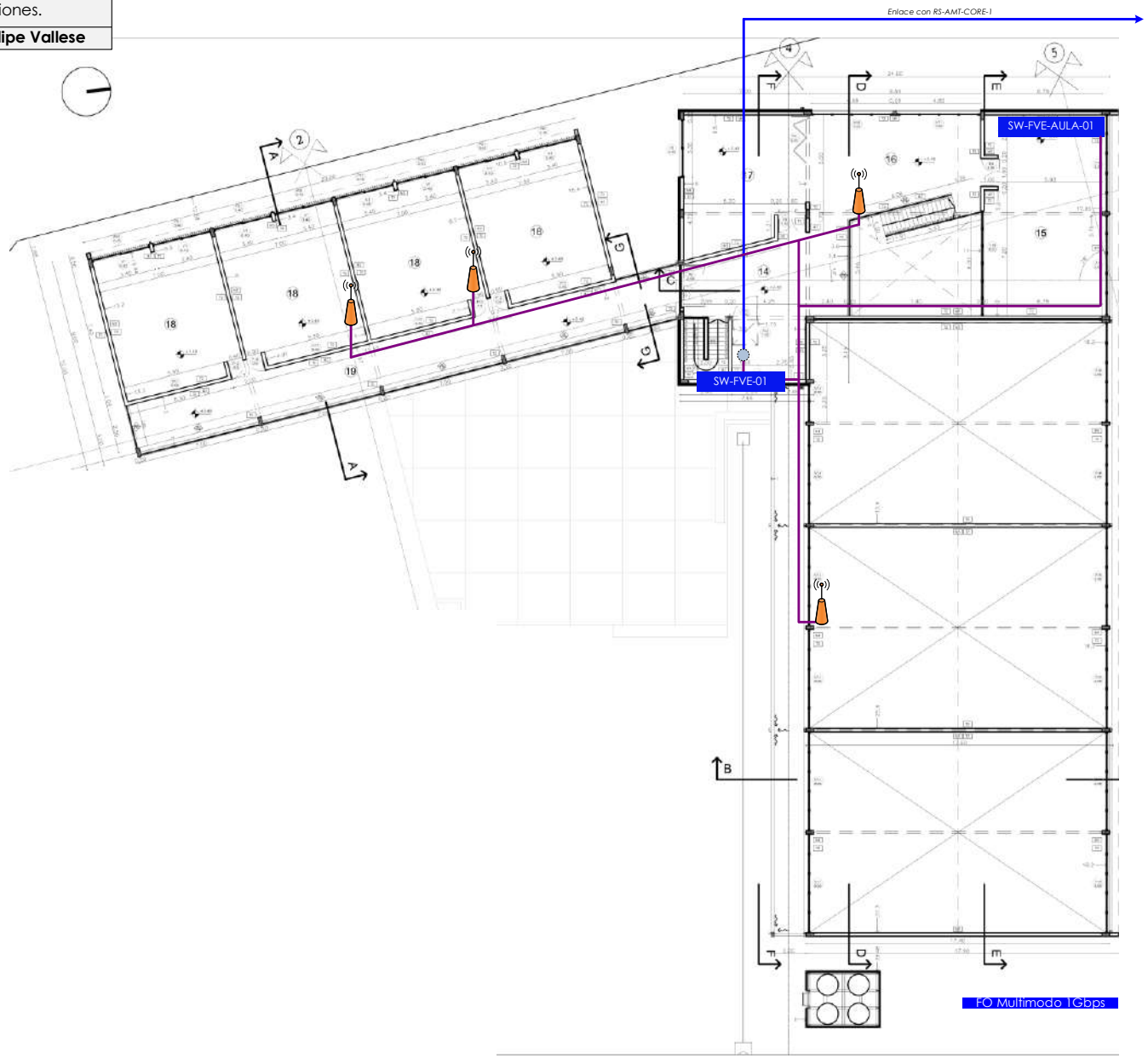
Área de Tecnología, Redes y Telecomunicaciones.

Plano | Edificio **Abremate**



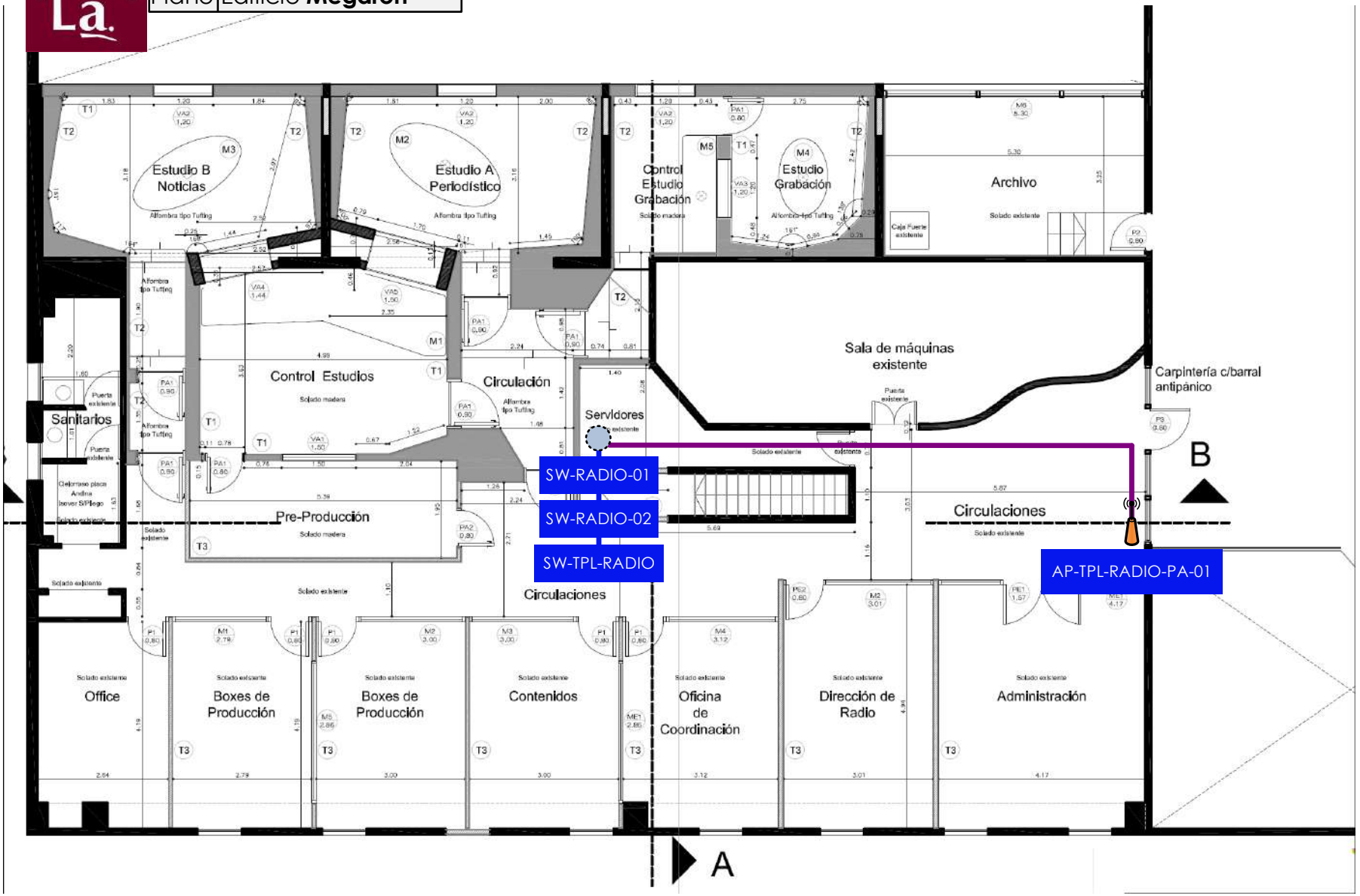

Área de Tecnología, Redes y Telecomunicaciones.
Plano Edificio **Talleres**
CERRAMIENTO EXT. CHAPA TRAPEZ. DMG 25 COLOR (+AISLACION– LV DOBLE–) (50mm–10y40kg/m3) VN REV. INT. PLACA ROCA YESO PERFORADA TIPO DELTA
TABIQUE DE LAD. HUECO 0.12 REV. + PLACA YESO 12mm TIPO DELTA(KNAUF)+ PANEL LANA VIDRIO 70MM–40KG/m3– TIPO ACUSTIVER–P500–VN
SALA CONFERENCIAS
15
PASO
12
SALA CONFERENCIAS
14
OFICINA
13
HALL
+4.45
10
VACIO S/SALON MULTIEVENTO
TABIQUE DE LADRILLO HUECO REVOCADO
BARANDA METALICA
SW-Talleres-01
SW-TPL-TALL
AP-TPL-TALL-PA
AP-TPL-TALL-SALON-01
AP-TPL-TALL-SALON-02
CUBIERTA TIPO PANELPLAC S/ESTRUCTURA METALICA
CANALETA DE CHAPA DMG20– 15X25
CUBIERTA TIPO PANELPLAC S/ESTRUCTURA METALICA
CAÑO BP H°N°150

Área de Tecnología, Redes y Telecomunicaciones.	
Plano	Edificio **Felipe Vallese**

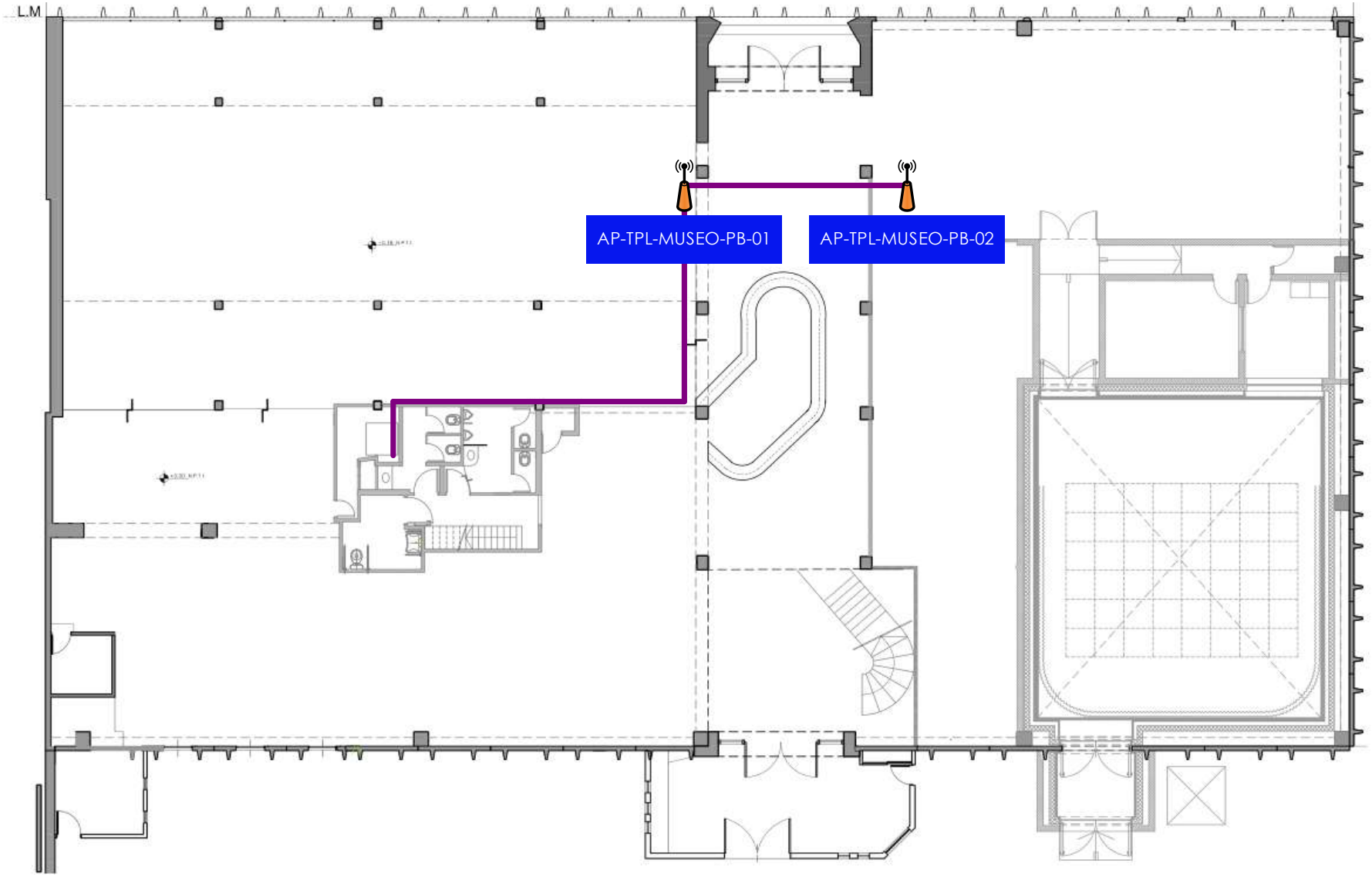


Área de Tecnología, Redes y Telecomunicaciones.

Plano | Edificio **Megafon**



Área de Tecnología, Redes y Telecomunicaciones.	
Plano	Edificio **MUD**



ANEXO - DECLARACIÓN JURADA DE PARENTESCO Y/O VINCULOS COMERCIALES (R.R. Nº 140/15)

Lugar y Fecha,.....

Razón Social:…….

Nº CUIT:…….

EL QUE SUSCRIBE (CON PODER SUFICIENTE PARA ESTE ACTO) DECLARA BAJO JURAMENTO, QUE LA PERSONA CUYOS DATOS SE DETALLAN PRECEDENTEMENTE, SUS SOCIOS DIRECTOS Y/O REPRESENTANTES LEGALES **SI / NO** **(tachar lo que no corresponda)** MANTIENEN RELACIÓN DE PARENTESCO Y/O RELACIONES COMERCIALES CON TRABAJADORES Y/O FUNCIONARIOS DE LA UNIVERSIDAD NACIONAL DE LANÚS.

Si declara "SI", Completar:	
FUNCIONARIO	**GRADO DE PARENTESCO / RELACIÓN COMERCIAL**

FIRMA: .....

ACLARACIÓN DE FIRMA: .....

CARÁCTER EN EL QUE REPRESENTO A LA EMPRESA: .....

DOMICILIO ESPECIAL:.....

TELEFONO DE CONTACTO: .....

CORREO ELECTRONICO APTO PARA NOTIFICACIONES: .....

ANEXO - DECLARACIÓN JURADA DE INTERESES DEL DECRETO 202/17

Lugar y Fecha,.....

Razón Social:…….

Nº CUIT:…….

¿La persona declarante tiene vinculación con los funcionarios enunciados en los artículos 1° y 2° del Decreto N° 202/17? *(Marque con una X donde corresponda)*

SI		NO	
Complete los campos "Funcionario con quien la persona declarante posee un vínculo" y "Tipo de vínculo". **En caso de que hubiere más vínculos con los funcionarios enunciados en los artículos 1º y 2º del Decreto 202/17 debe completar tantos formularios como vínculos hubiere**.		La opción elegida implica la declaración expresa de la inexistencia de vinculaciones en los términos del Decreto N° 202/17. No se exige más información. Firme al pie del formulario la Declaración Jurada de Intereses.	

Funcionario con quien la persona declarante posee un vínculo ¿Con cuál de los siguientes funcionarios? *(Marque con una X donde corresponda)*

Presidente	
Vicepresidente	
Jefe de Gabinete de Ministros	
Ministro	
Autoridad con rango de ministro en el Poder Ejecutivo Nacional	
Autoridad con rango inferior a Ministro con capacidad para decidir	

En caso de haber marcado "Ministro", "Autoridad con rango de ministro en el Poder Ejecutivo Nacional" o "Autoridad con rango inferior a Ministro con capacidad para decidir" complete los siguientes campos:

Nombres	
Apellidos	
Cargo	
Jurisdicción	

Tipo de vínculo *(Marque con una X donde corresponda y brinde la información adicional requerida para el tipo de vínculo elegido)*

Sociedad o comunidad		En información adicional detalle "Razón Social" y "CUIT".
Parentesco por consanguinidad dentro del cuarto grado y segundo de afinidad		En información adicional detalle qué parentesco existe concretamente.
Pleito pendiente		En información adicional detalle "carátula", "nº de expediente", "fuero", "jurisdicción", "juzgado" y "secretaría".
Ser deudor		En información adicional detalle "motivo de deuda" y "monto".
Ser acreedor		En información adicional detalle "motivo de acreencia" y "monto".
Haber otorgado al funcionario beneficio/s de importancia		En información adicional detalle "tipo de beneficio" y "monto estimado".
Amistad pública que se manifieste por gran familiaridad y frecuencia en el trato		No se exige información adicional

Información adicional

Declaro bajo juramento que:

- Estoy en conocimiento de que la falsedad en la información consignada en este formulario será considerada una falta de máxima gravedad a los efectos que correspondan en los regímenes sancionatorios aplicables.
- Estoy en conocimiento de que la declaración negativa de vinculaciones con los funcionarios/as mencionados en los artículos 1º y 2º del Decreto 202/17, implica la declaración expresa de la inexistencia de tales vinculaciones.
- Todos los datos consignados son verdaderos y cuando declaro información de terceros he realizado las debidas diligencias para constatar su veracidad.

(https://www.argentina.gob.ar/anticorrupcion/prevencion/decretos-intereses/202-17/ddjj)

…….

Firma y aclaración.

ANEXO - DECLARACIÓN JURADA DE INCORPORACIÓN DE PERSONAS CON DISCAPACIDAD

Lugar y Fecha,.....

Razón Social:…….

Nº CUIT:…….

De conformidad con lo previsto en Ley 22.431, Art. 7° del Decreto N° 312/10 y Art. 18, Inc. i) apartado 4, del Pliego Único de Bases y Condiciones Generales aprobado por Disposición ONC Nº 63/16), declaro bajo juramento que, de resultar adjudicatario, me obligo a ocupar a personas con discapacidad en una proporción no inferior al CUATRO POR CIENTO (4%) de la totalidad del personal afectado a la prestación del servicio licitado. El porcentaje aludido se computará sobre la totalidad del personal afectado a la prestación del servicio licitado y resultara exigible cuando sea posible cuantitativamente cumplir con el mismo, o sea, que tal porcentaje represente al menos UNA (1) persona.

…….
Firma y aclaración.

De conformidad con lo previsto en Ley 22.431, Art. 7° del Decreto N° 312/10 y Art. 18, Inc. i) apartado 4, del Pliego Único de Bases y Condiciones Generales aprobado por Disposición ONC Nº 63/16), declaro que, por las particularidades del servicio no resulta posible contar con personas con discapacidad que reúnan las condiciones de idoneidad para cumplir con la prestación. A continuación, se detallan las particularidades del servicio que imposibilitan contar con personas con discapacidad en el porcentaje requerido por la ley:
……
……
……

…….
Firma y aclaración.