

8. SISTEMAS A INTEGRARSE.

8.1. General

Los sistemas actualmente instalados, **Monitoreo de Línea de Molinetes** y **CCTV Cocheras y Talleres** deben ser integrados a este sistema.

8.2. Sistema “Monitoreo de Línea de Molinetes”.

Corresponde al sistema que visualiza los molinetes de las líneas.

Se trata de un sistema compuesto por cámaras fijas color IP con resolución HD administrada por MilestoneXprotect Enterprise, para un total de 300 cámaras.

El Centro de Monitoreo se encuentra ubicado en el PCO sito en la calle Bernardo de Irigoyen 235 CABA y está compuesto por cinco (5) puestos de monitoreo.

Los servidores se encuentran ubicados en la Sala Técnica de la estación Independencia.

8.3. Sistema “CCTV Cocheras y Talleres”

Corresponde al sistema que visualiza, controla accesos y posee sensores de alarmas para alerta temprana de intrusiones y vandalismo en cocheras y talleres y otros sitios donde pernoctan formaciones.

Se trata de un sistema con monitoreo y grabación local en cada uno de los sitios, administrado por MilestoneXprotect Professional con Cámaras Bosch “Flexidome HD 720p - High Definition NIN-733-14IPS y Domos Bosch “Autodome 7000 IP”

Posee, a su vez, monitoreo de cámaras, acceso y alarmas, con siete (7) puestos de monitoreo en cada uno de ellos, en:

- Dirección General de Custodia y Seguridad de Bienes del GCBA, Corrientes 5300 CABA.
- Administración de SBASE, Agüero 48 CABA.

La cantidad de cámaras, controles de acceso y sensores se indican en el ANEXO 9.

Estas Cámaras están incluidas en la planilla del ANEXO 7 – Video Cámaras por Línea y Estación.

9. SEGURIDAD EN CENTROS DE MONITOREO PARA SUBTERRÁNEOS.

9.1. General.

En ambos C.M.S. se proveerán Sistemas, independientes del "Sistema de Seguridad Electrónica para Líneas Subterráneas y Pre Metro" (Sistema Principal), para Detección de Incendios, para Control de Accesos y Circuito Cerrado de Televisión de Seguridad (C.C.TV.). Las Unidades Principales de cada Sistema se instalarán en el mismo ámbito que los equipos propios del Sistema Principal (Sala de Servidores). Todos los dispositivos de estos sistemas deberán estar conectados a la U.P.S. del C.M.S.

9.2. Subsistema de Detección de Incendio del C.M.S.

Cada ambiente del C.M.S. deberá estar protegido por una Central de Alarmas de Incendio en función de lo determinado en el punto 6.3 del PET Generales. Responderá técnicamente a las normas IRAM que en el orden Nacional se hayan aprobado y se complementarán con las normas NFPA 72 (National Fire Protection Association 72: National Fire Alarm Code - Asociación). Además deberá respetar el Anexo I - Documento Complementario del Código de la Edificación N° VI (se deberá tener en cuenta la modificación del Art. 4.12.1.2 y del Art. 4.12.2.3 del 11 de mayo del año 2000). La Central de Alarmas de Incendio deberá ser del tipo Analógica Direccionable. Según el ambiente donde se deban colocar los detectores, estos serán para la detección de: humo (iónicos/ópticos), térmicos, llamas, gas, según corresponda; además deberá considerarse al menos 3 avisadores manuales con llave para fácil restablecimiento, uno dentro de la Sala de Monitoreo y el resto en pasillos de acuerdo a norma; las sirenas serán del tipo combinada (con luces electroboscópicas). Todos los dispositivos deberán estar certificados por las normas UL, ULC, NFPA. El cable a utilizar será el certificado color rojo, apantallado, no propagador del fuego y libre de halógenos. En la oferta se debe especificar la propuesta y en cada ítem de ésta hacer referencia de la norma aplicada, quedando a criterio de SBASE, o quién éste disponga, su modificación basándose en la normativa vigente. Deberán considerarse dispositivos de señalización (aviso) para personas de capacidades diferentes.

9.3. Subsistema de C.C.TV. del C.M.S.

Todo el sistema debe responder a tecnología digital IP. Las cámaras deberán ser del tipo día-noche. La cámara tipo domo (PTZ) deberá tener un zoom óptico mínimo de 11X y para su manejo deberá proveerse con un joystick (este dispositivo deberá ser instalado en la Oficina del 2do. Jefe del Centro de Monitoreo para Subterráneos. El Oferente en su propuesta deberá colocar la ubicación de los dispositivos propuestos y sus características, quedando a criterio de SBASE, o quién éste disponga, su modificación en cuanto a la ubicación física de los dispositivos. El sistema de grabación deberá ser del tipo "stand alone" con capacidad de almacenamiento de 60 (SESENTA) días corridos de grabación a 25 cuadros por segundo, resolución mínima D1 (720 x 568 pixels), mejor calidad de muestreo y con detección de movimiento. Debe permitir agenda de grabación y acceso mediante INTERNET con acreditación por "Usuario" y "Contraseña". Deberá poseer un sistema de firma electrónica para garantizar que las filmaciones que se extraen de él no sean adulteradas y sirvan de prueba a la justicia.

9.4. Subsistema de Control de Accesos del C.M.S.

Cada Oficina deberá poseer su debido sistema de acreditación mediante lectoras de tarjetas de proximidad (compatibles con protocolo Wiegand, tecnología Rfid: identificación por radiofrecuencia), según se detalla en el ítem 6.3 del PET Generales y unidos en red. En el caso de proponer cerraduras electromagnéticas para las puertas de acceso, éstas no deberán ser inferiores a 600 libras/270kgs de fuerza. En el caso de utilizar cerraduras electromagnéticas, se deberá considerar para los ambientes que fueran detallados como de "sólo control de entrada", un pulsador del lado interior de la habitación para facilitar la salida de personas. Para los ambientes que deberán tener control de "entrada-salida", en el interior de la habitación se colocará una lectora de proximidad. Se utilizarán controladoras para dos puertas o control de una puerta "entrada-salida", en el caso de proveerse controladoras con mayor poder de control, deberá tenerse en cuenta las distancias. De ser necesario, se utilizará cableado RS 485/EIA485 para Control de Accesos, y deberá cablearse la salida de la Central de Alarmas de Incendio para que interactúe con el Sistema de Control de Accesos liberando todos los accesos. Todas las Controladoras deberán poseer una batería de respaldo. Si la propuesta considerara cerraduras eléctricas, para el caso de ambientes con doble control ("entrada-salida"), del lado interno se utilizará una lectora de proximidad y para los ambientes de "sólo control de ingreso", deberá dejarse del lado interno colocado el picaporte de la puerta. No se podrá usar cerraduras eléctricas (pestaño eléctrico) en puertas dobles. El software de control de accesos deberá poder administrar usuarios y contraseñas, reportes en tiempo real de transacciones, expansión automática de tarjetas y dispositivos, monitoreo de alarmas y eventos, control de período de tiempo en la apertura de puertas. El Oferente en su propuesta deberá colocar la ubicación de los dispositivos propuestos y sus características, quedando a criterio de SBASE, o quién éste disponga, su modificación en cuanto a la ubicación física de los dispositivos.

10. RED DE ENLACE Y TRANSPORTE

10.1. Características generales de la red.

La red sobre la que se instalará el sistema de video vigilancia para la red de subterráneos, estará compuesta por equipos que soporten y cumplan con las funcionalidades descriptas a continuación.

1. Los equipos que la conformen deberán soportar tecnologías Ethernet, Fast Ethernet, Gigabit Ethernet, 10 G Ethernet.
2. Deberá poseer funcionalidades para la segmentación de dominios de broadcast a través de redes LAN virtuales (VLANs).
3. Al tratar de una red que soportara grandes cargas de tráfico con información de video, deberá poseer funcionalidades avanzadas para servicios Multicast.
4. Poseer funcionalidades avanzadas para el manejo de la calidad de servicio y priorización para la información de video.
5. Dado lo extenso de la red, los equipos deberán poseer funcionalidades avanzadas para integrarse con una herramienta de gestión que permita monitorear, configurar, detectar y corregir problemas de forma centralizada y con un alto grado de seguridad en los procedimientos para cumplir con estos requisitos.
6. Deberá constituirse como una red de tipo self-healing, de tal manera que se reconfigure en forma automática ante cualquier corte en la Fibra Óptica (dispuesta en forma de anillos según se describe en 10.2)

Esquemáticamente se planificó una topología que describirá un anillo por línea o ramal, haciendo un total de 7 anillos incluyendo el Pre Metro. Estos anillos a su vez estarán interconectados entre ellos a través de equipos de core ubicados en 3 sitios en donde funcionarán las centrales de monitoreo y se alojaran servidores y electrónica de red necesaria.

Nota Importante: SBASE suministrará el tendido de Fibra Óptica.

10.2. Solicitud infraestructura de red y soporte.

Se deberá contemplar para la implementación un esquema de anillo para cada una de las líneas de subterráneos. Asimismo estos anillos estarán interconectados con 3 sitios, los cuales estarán a su vez interconectados entre sí.

Todo esto conforme la topología descripta en los esquemas Anexos y la información resultante de la visita de obra.

En los sitios se deberán contemplar los sistemas de energía ininterrumpida para el correcto funcionamiento de los dispositivos propuestos por al menos 1 hora.

10.3. Estaciones o puntos de anillo

Cada estación o nodo del anillo de cada línea deberá contar con el equipamiento de red que como mínimo cumpla con las siguientes necesidades:

Switches de acceso y de enlace del anillo.

SUBTERRÁNEOS DE BUENOS AIRES S.E.

1. Deberá soportar tecnologías Ethernet, Fast Ethernet, Gigabit Ethernet, 10 G Ethernet.
2. Interfaces:
 - a. Como mínimo con 2 slots para módulos transceptores SPF 10 Gbps.
 - b. Como mínimo deberá estar equipado con 2 módulos transceptores SPF de 10 Gbps para fibra monomodo de las características mencionadas en el cuerpo del presente pliego y soportar la comunicación para las distancias existentes entre cada punto del anillo. Con conector LC-SC APC.
 - c. Contar con un mínimo de 24 interfaces Gigabit Ethernet 10/100/1000 Base-T RJ45 independientes que soporte auto-negociación de velocidad y dúplex. POE. Cada una de estas interfaces debe proporcionar POE o POE plus
 - d. Contar al menos con un puerto Ethernet 10/100 Base-T para la administración fuera de banda.
 - e. Deberá contar con una interfaz USB para realizar copias de respaldo y actualizaciones de firmware.
3. Manejo de protocolos y funcionalidades:
 - a. Apilamiento o Staking:
 - i. Debe poseer funcionalidades para realizar apilado o staking entre equipos, conformando un chasis que se pueda administrar de forma unificada como si fuera un único dispositivo.
 - ii. Deberá soportar Staking de los equipos, utilizando una interconexión dedicada utilizando un backplane o una alternativa (indicarla).
 - iii. Deberá soportar el staking de switches (indicar cantidad mínima y máxima).
 - iv. Deberá manejar un mínimo 50 gbps de uplink para las conexiones de staking.
 - v. Cada equipo deberá estar provisto del los correspondientes cable para el staking por backplane o alternativo.
 - b. Soportará funcionalidades de multicast. Deberá soportar IGMP Snooping versiones 1, 2 y 3. Para IPv6. Con capacidad de full querier.
 - c. Deberá soportar el protocolo Link Agregación Control Protocol (LACP) conforme especificación IEEE 3ad. Y cada grupo podrá confirmarse como mínimo con 6 puertos de cualquiera de los miembros del stack.
 - d. Cada chasis o conjunto de equipos apilados, deberán soportar al menos 10 grupos de link aggregation.
 - e. Debe poseer funcionalidades de control de broadcast, multicast y unicast con supresión para cada puerto.
 - f. Deberá soportar el manejo de Jumbo Frames.
 - g. Deberá soportar el manejo de VLANs según especificación IEEE 802.1Q.
 - h. Deberá soportar SNMP en sus versiones v2 y v3.
 - i. Deberá soportar el protocolo LLDP, para identificación de dispositivos de VOIP. Según especificación IEEE 802.1AB.
 - j. Deberá soportar los protocolos NTP y SNTP.
 - k. Soporte IPv6.
 - l. Soportará la definición de dominios de broadcast en VLANs (Virtual LANs) en todos sus puertos según especificación IEEE 802.1Q.
 - m. Deberá poseer funcionalidades de administración jerárquica de VLANs y pudiendo crear, renombrar o borrar las mismas evitando realizar estas tareas en cada nodo de comunicaciones.
 - n. Soportará ARP proxy.
 - o. Calidad de servicio:

SUBTERRÁNEOS DE BUENOS AIRES S.E.

- i. Deberá permitir implementar colas de prioridades permitiendo priorizar tráfico según especificación IEEE 802.1P CoS.
 - ii. Soportará QoS en grupos de link aggregation.
- p. SpanningTree:
- i. Manejo de protocolo SpanningTree.
 - ii. Manejo de protocolo Rapid SpanningTree según especificación IEEE 802.1.w.
 - iii. Deberá tener funciones que permitan inhabilitar de forma automática una interface que esté identificada como puerto de acceso, cuando reciba un frame BPDU.
 - iv. También deberá tener funcionalidades que permitan configurar la interface para que al detectar la intención de introducir un frame BPDU filtre este tráfico pero permita que el resto del tráfico.
- q. Seguridad:
- i. Deberá soportar DHCP Snooping.
 - ii. Los equipos deberán poseer funcionalidades para asegurar la infraestructura y evitar que en la red operen servidores de DHCP no autorizados.
 - iii. Deberá tener la funcionalidad de identificar los intentos de consumir el o los scopes de direcciones administradas por el o los servidores de DHCP autorizados. Esta funcionalidad deberá utilizar el campo CHADDR del protocolo DHCP y no solamente la dirección MAC o origen de la solicitud.
 - iv. Deberá poseer funcionalidades para evitar ataques de ARP Poisoning.
 - v. Los equipos deberán poseer funcionalidades para limitar el número de direcciones físicas (MAC address) asociadas a una misma interfaz.
 - vi. El equipo deberá tener las funcionalidades para identificar la dirección física y habilitar una determinada configuración para el puerto al que se conecte.
 - vii. Deberá soportar autenticación según especificación 802.1x.
 - viii. Deberá permitir al utilizar autenticación según 802.1x, asignar una VLAN específica a la interface según las credenciales del usuario.
 - ix. Deberá soportar trafficmirroring por puerto o por VLAN. Replicando el tráfico en una interfaz dentro del mismo switch o chasis de staking, o bien, otro switch o chasis remoto.
 - x. Deberá soportar autenticación RADIUS y/o TACACS+.
 - xi. Deberá soportar conexiones SSH v2, para administración.
 - xii. Deberá soportar el bypass de la autenticación basada en direcciones MAC.
 - xiii. Deberá soportar la limitación de tráfico por ACL aplicada en puertos o en VLAN:
 - 1. Por direcciones MAC de origen o destino.
 - 2. Direcciones IP de origen o destino.
 - 3. Número de puerto TCP/UDP.
 - 4. Soportará como mínimo 1000 ACL en el chasis o stack.
4. Todos los equipos deberán incluir todos los elementos para el montaje en un rack de 19 pulgadas.
5. Fuentes de alimentación:
- a. Las fuentes deberán ser alimentados con 220 V – 50Hz, monofásico con toma Tipo I.
 - b. No se aceptaran transformadores de 220 VCA a 110 VCA agregados a la fuente.

SUBTERRÁNEOS DE BUENOS AIRES S.E.

- c. La fuente del equipo deberá aceptar directamente 220 VCA a 50 Hz. Tampoco se aceptaran fuentes externas.
- 6. Administración:
 - a. Deberá soportar la administración y configuración por línea de comandos de consola y soportar conexiones seguras SSH v2.
 - b. Deberá poseer agente de SNMP para ser administrado dentro de banda utilizando el protocolo SNMP v3.
 - c. Deberá permitir monitorear el estado y tráfico de los componentes de la red según estructura MIB-II.
 - d. La administración poder realizarse en todas las interfaces simultáneamente.
 - e. Deberá soportar los grupos de RMON 1 eventos, históricos, estadísticas y alarmas.
 - f. Deberá proveer mecanismos que permitan configurar sensores de tráfico para detectar retardos entre equipos utilizando MIBs según RFC 2925.
 - g. Deberá poseer capacidades para implementaciones de Syslog.
 - h. Deberá poseer la capacidad de configurar alarmas ante el mal funcionamiento de alguno componente de los equipos que conformen los nodos, esto deberá configurarse de forma centralizada y administrarse de la misma forma. Por ejemplo alerta de temperatura o falla en la actualización del sistema operativo.
 - i. Deberá soportar la actualización del sistema operativo de forma remota a través de la red.
 - j. La actualización de los sistemas operativos de los equipos deberá se gestionada desde una consola central la cual servirá de autentificadora para los mismos, evitando y detectando cargas de software no firmado.
 - k. Deberá soportar tecnologías TDR (Time Domain Reflectometry), para la detección y señalización de cableado o conectores.
 - l. El rango de direccionamiento IP adoptado para la Administración del Sistema será establecido por SBASE., o quién este disponga.
- 7. Accesorios:
 - a. Equipado con software y todas las licencias necesarias para su operación con las funcionalidades solicitadas sin límite de tiempo.
 - b. Incluir un juego de manuales en dos idiomas, español e inglés.

Nota Importante: En el caso que, en los anillos de cada una de las líneas (7 anillos secundarios) se requieran equipamientos para manejar un flujo de información menor de 10 Gbps Ethernet, el Oferente podrá ofrecerlos como alternativa, justificándolo plenamente mediante el cálculo correspondiente, todo ello sin perder las características restantes

10.3.1. Sitios o nodos concentradores

Cada sitio o nodo concentrador deberá contar con el equipamiento de red como mínimo con las siguientes características:

10.3.2. Switches de core o concentradores.

1. Deberá soportar tecnologías Ethernet, Fast Ethernet, Gigabit Ethernet, 10 G Ethernet.
2. Capacidades de conmutación mínima de 800 Gbps.
3. Interfaces:
 - a. Como mínimo deberá contar con 16 slots para módulos transceptores SPF 10 Gbps.

- b. Como mínimo deberá estar equipado con 16 módulos transceptores SPF de 10 Gbps para fibra monomodo de las características mencionadas en el cuerpo del presente pliego y soportar la comunicación para las distancias existentes entre cada punto del anillo. Con conector LC.
 - c. Contar al menos con un puerto Ethernet 10/100BaseT para la administración fuera de banda.
4. Manejo de protocolos y funcionalidades:
- a. Deberá tener capacidad de manejo de los equipos en modalidad cluster, comportándose los dos equipos lógicamente como uno solo, tanto desde el punto de vista de administración como el de tráfico.
 - b. Deberá poder realizarse conexiones agregadas (Link Aggregation), hacia las dos unidades del cluster, teniendo todas las conexiones activas en todo momento.
 - c. Soportará funcionalidades de multicast:
 - i. Deberá soportar IGMP Snooping versiones 1, 2 y 3. Para IPv4 e IPv6. Con capacidad de full querier.
 - d. Deberá soportar el protocolo Link Agregación Control Protocol (LACP) conforme especificación IEEE 3ad. Y cada grupo podrá confirmarse como mínimo con 6 puertos de cualquiera de los miembros del stack.
 - e. Cada chasis o conjunto de equipos apilados, deberán soportar al menos 10 grupos de link aggregation.
 - f. Debe poseer funcionalidades de control de boadcast, multicast y unicast con supresión para cada puerto.
 - g. Deberá soportar el manejo de Jumbo Frames.
 - h. Deberá soportar el manejo de más de más de 4000 VLANs según especificación IEEE 802.1Q.
 - i. Deberá soportar SNMP en sus versiones v2 y v3.
 - j. Deberá soportar el protocolo LLDP, para identificación de dispositivos de VOIP. Según especificación IEEE 802.1AB.
 - k. Deberá soportar los protocolos NTP y SNTP.
 - l. Soporte IPv6.
 - m. Soportará la definición de dominios de broadcast en VLANs (Virtual LANs) en todos sus puertos según especificación IEEE 802.1Q.
 - n. Deberá poseer funcionalidades de administración jerárquica de VLANs y pudiendo crear, renombrar o borrar las mismas evitando realizar estas tareas en cada nodo de comunicaciones.
 - o. Soportará DHCP relay DHCP helper.
 - p. Soportará ARP proxy.
 - q. Calidad de servicio:
 - i. Deberá permitir implementar colas de prioridades permitiendo priorizar tráfico según especificación IEEE 802.1P CoS.
 - ii. Soportará QoS en grupos de link aggregation.
 - iii. Manejo de 8 colas de calidad de servicio por puerto.
 - iv. Soportará QoS por puerto o por VLAN, o bien, por puerto por VLAN.
 - v.
 - r. SpanningTree:
 - i. Manejo de protocolo SpanningTree.
 - ii. Manejo de protocolo Rapid SpanningTree según especificación IEEE 802.1.w.

SUBTERRÁNEOS DE BUENOS AIRES S.E.

- iii. Deberá tener funciones que permitan inhabilitar de forma automática una interface que esté identificada como puerto de acceso, cuando reciba un frame BPDU.
- iv. También deberá tener funcionalidades que permitan configurar la interface para que al detectar la intención de introducir un frame BPDU filtre este tráfico pero permita que el resto del tráfico.
- s. Seguridad:
 - i. Deberá soportar DHCP Snooping.
 - ii. Los equipos deberán poseer funcionalidades para asegurar la infraestructura y evitar que en la red operen servidores de DHCP no autorizados.
 - iii. Deberá tener la funcionalidad de identificar los intentos de consumir el o los scopes de direcciones administradas por el o los servidores de DHCP autorizados. Esta funcionalidad deberá utilizar el campo CHADDR del protocolo DHCP y no solamente la dirección MAC o origen de la solicitud.
 - iv. Deberá poseer funcionalidades para evitar ataques de ARP Poisoning.
 - v. Los equipos deberán poseer funcionalidades para limitar el número de direcciones físicas (MAC address) asociadas a una misma interfaz.
 - vi. El equipo deberá tener las funcionalidades para identificar la dirección física y habilitar una determinada configuración para el puerto al que se conecte.
 - vii. Soportar funcionalidades de control de tormentas de broadcast y multicast.
 - viii. Deberá soportar autenticación según especificación 802.1x.
 - ix. Deberá permitir al utilizar autenticación según 802.1x, asignar una VLAN específica a la interface según las credenciales del usuario.
 - x. Deberá soportar trafficmirroring por puerto o por VLAN. Replicando el tráfico en una interfaz dentro del mismo switch o chasis de staking, o bien, otro switch o chasis remoto.
 - xi. Deberá soportar autenticación RADIUS y/o TACACS+.
 - xii. Deberá soportar conexiones SSH v2, para administración.
 - xiii. Deberá soportar el bypass de la autenticación basada en direcciones MAC.
 - xiv. Deberá soportar la limitación de tráfico por ACL aplicada en puertos o en VLAN:
 - 1. Por direcciones MAC de origen o destino.
 - 2. Direcciones IP de origen o destino.
 - 3. Número de puerto TCP/UDP.
 - 4. Soportará como mínimo 1000 ACL en el chasis o stack.
- 5. Todos los equipos deberán incluir todos los elementos para el montaje en un rack de 19 pulgadas.
- 6. Fuentes de alimentación:
 - a. Las fuentes deberán ser alimentados con 220 V – 50Hz, monofásico con toma Tipo I.
 - b. Poseerá fuentes de alimentación redundantes con forzadores redundantes y todas estas funcionalidades deberán ser hot-swap.
 - c. No se aceptaran transformadores de 220 VCA a 110 VCA agregados a la fuente.

- d. La fuente del equipo deberá aceptar directamente 220 VCA a 50 Hz. Tampoco se aceptaran fuentes externas.

7. Administración:

- a. Deberá soportar la administración y configuración por línea de comandos de consola y soportar conexiones seguras SSH v2.
- b. Deberá poseer agente de SNMP para ser administrado dentro de banda utilizando el protocolo SNMP v3.
- c. Deberá permitir monitorear el estado y tráfico de los componentes de la red según estructura MIB-II.
- d. La administración poder realizarse en todas las interfaces simultáneamente.
- e. Deberá soportar todos los grupos de RMON 1 y todos los grupos de RMON 2.
- f. Deberá proveer mecanismos que permitan configurar sensores de tráfico para detectar retardos entre equipos utilizando MIBs según RFC 2925.
- g. Deberá poseer capacidades para implementaciones de Syslog.
- h. Deberá contar con herramientas integradas que permitan diagnosticar y medir SLA de sesiones de audio, video y datos. Como también capacidades para simplificar y monitorear el QoS de video. Además deberá ser capaz de simular sesiones de video para verificar la capacidad de la red.
- i. Deberá poseer la capacidad de configurar alarmas ante el mal funcionamiento de alguno componente de los equipos que conformen los nodos, esto deberá configurarse de forma centralizada y administrarse de la misma forma. Por ejemplo alerta de temperatura o falla en la actualización del sistema operativo.
- j. Deberá soportar la actualización del sistema operativo de forma remota a través de la red.
- k. La actualización de los sistemas operativos de los equipos deberá ser gestionada desde una consola central la cual servirá de autentificadora para los mismos, evitando y detectando cargas de software no firmado.

8. Accesorios:

- a. Equipado con software y todas las licencias necesarias para su operación con las funcionalidades solicitadas sin límite de tiempo.
- b. Incluir un juego de manuales en dos idiomas, español e inglés.

Todos los equipos propuestos deben ser compatibles 100% con la herramienta de administración centralizada propuesta que se solicita a continuación, tanto equipos de distribución como equipos de core.

10.4. Software de Administración de Red LAN

Solución de Administración de Red de extremo a extremo Monitoreo de servicios y tecnologías críticas para el negocio en todo el ciclo de vida de la Red que cumpla con las siguientes funcionalidades:

1. Monitoreo y solución de Problemas

- a. Deberá contar con un Navegador Centralizado de eventos y fallas (consolidación de syslog, traps, eventos y alarmas)
- b. Deberá permitir la Navegación rápida para identificar aéreas con problemas
- c. Deberá contar con Flujos de Trabajo embebidos para solución de problemas, para poder aislarlos de manera rápida y remediarlos

SUBTERRÁNEOS DE BUENOS AIRES S.E.

- d. Deberá soportar el uso del protocolo SNMP (Simple Network Management Protocol) para poder identificar problemas de disponibilidad y rendimiento.
 - e. Deberá manejar IPSLAs para las operaciones de video lo cual ayuda a identificar si la red está lista para aplicaciones de video y multimedia
 - f. Deberá permitir la Interacción Inteligente para la creación de un requerimiento de servicio y/o búsquedas inteligentes en comunidades para solución de problemas.
 - g. Deberá poseer capacidades para detectar equipos de video y que pueda hacer una evaluación de la red para que cumpla con mejores prácticas para la transmisión de video y multimedia.
2. Administración de Configuraciones
- a. Deberá permitir el respaldo de configuraciones
 - b. Deberá permitir la administración de Versiones de firmwares con los que corren los diferentes dispositivos
 - c. Deberá permitir el control de cambios para mantenimiento y actualización de Dispositivos
 - d. Deberá permitir la Actualización de Librerías de Configuración directamente de una página web.
3. Inventario
- a. Deberá permitir llevar un inventario de Chasis, Módulos e Interfaces entre otros.
 - b. Deberá proveer un menú para ver el estado del avance del descubrimiento en curso de la red
 - c. Deberá soportar más de 200 tipos de dispositivos.
4. Reportes
- a. Deberá contar con un menú para que la navegación a través de esta funcionalidad (reporteo) sea sencilla y se pueda acceder a reportes detallados.
 - b. Deberá permitir generar reportes como inventario, equipos con anuncio de fin de vida o de soporte, alertas sobre bugs de seguridad.
 - c. Deberá permitir que los reportes se pueden agendar para que corran diario, o semanalmente o mensualmente, y pueden ser consultados en línea o exportados a un archivo tipo csv.
5. Centros de Trabajo
- a. Deberá contar con flujos de trabajo (workflows) que permitan que la configuración de dispositivos de distintas tecnologías sea simple.
 - b. Que contenga Indicadores gráficos (dashboards) que den una actualización del estado de configuración de los dispositivos, inventario y monitoreo para poder solucionar problemas.
6. Administración
- a. Deberá ser centralizada y de acceso sencillo y seguro, si es posible con soporte para dispositivos móviles como tabletas o teléfonos inteligentes.
7. Deberá proporcionar una cobertura completa de los dispositivos:
- a. Para poder administrar una red con eficacia, la cobertura del dispositivo es esencial, no importa donde se encuentre el dispositivo.

SUBTERRÁNEOS DE BUENOS AIRES S.E.

- b. Deberá cubrir el ciclo completo de administración de la red. El mantenimiento y la gestión de los servicios que se asocian con una red requiere una buena base para hacer frente a la infraestructura de red básica y las tareas del día a día asociadas con la gestión de ciclo de vida , esta herramienta proporciona la funcionalidad necesaria para realizar las tareas del día a día, incluyendo el descubrimiento, el monitoreo y solución de problemas, configuración y gestión de cambios, corrección automática e inventario así como informes para estar dentro de estándares.
8. Funcionalidades generales:
 - a. Deberá permitir el monitoreo en tiempo real.
 - b. Deberá poseer la capacidad de un asistente o guía para solucionar problemas.
 - c. Que tenga la Capacidad de instalarse en una plataforma Virtualizada.

10.5. Equipos IPS- VPN- FireWall, Antispam, Antispyware

Cada sitio o nodo concentrador deberá con el equipamiento de seguridad que como mínimo cumpla con las siguientes necesidades:

1. Ser capaz de procesar al menos 8 Gbps de tráfico (con paquetes grandes) y 12.000.000 paquetes por segundo (con paquetes de 64Bytes).
2. Funcional en ALTA DISPONIBILIDAD y luego de esta interconexión, Poseer al menos 6 Interfaces 10/100/1000 Ethernet físicas libres.
3. Contar con un mínimo de OCHO (8) interfaces Gigabit Ethernet10/100/1000Base-T RJ45 independientes que soporte auto-negociación de velocidad y dúplex.
4. Contar con al menos UNA (1) interface Fast Ethernet 10/100Base-T RJ45, para su administración fuera de banda.
5. Todas las interfaces se podrán utilizar independientemente en modo L3 o L2, es decir se podrán agrupar para formar un dominio de Broadcast (L2) representadas por una interfase L3 virtual o cada interfase física o lógica podrá configurarse con una dirección IP independiente (L3)
6. La totalidad de las VLANS podrán ser configuradas en un único puerto físico destinado a conexiones internas.
7. No deberá tener un límite de concurrencia de usuarios impuesto por el hardware ni por el software o licencias.
8. Soporte de múltiples zonas de seguridad. Se entiende zona de seguridad a la agrupación de una o más interfaces (físicas o lógicas) sobre las que se aplicaran políticas de seguridad.
9. El equipo deberá poder configurarse en modo Layer 3 (L3) o en modo Layer 2 (L2 - Modo Transparente) que permita integrarse a una topología existente sin cambiar el direccionamiento IP de los equipos instalados previamente.
10. El mecanismo de control de filtrado utilizado por el sistema operativo del equipo deberá estar basado en técnicas "statefullinspection" que crean conexiones virtuales, incluso para los protocolos connection-less como UDP y RPC.

SUBTERRÁNEOS DE BUENOS AIRES S.E.

11. Las reglas del de tráfico serán configuradas por objetos que representen a las redes o estaciones de trabajo, servicios etc. Las estaciones de trabajo, servicios o redes se podrán agrupar para crear un único objeto y facilitar la configuración de dichas reglas.
12. Redes privadas virtuales (IPSec VPN):
 - a. Deberá soportar VPNs mediante IPSec soportando, como mínimo, 4.5Gbps. de tráfico encriptado con AES, 3DES de 168-bits, hash MD5 y SHA-1.
 - b. Permitir la generación VPN de tipo Site-to-Site y Client-to-Site.
 - c. Mecanismo de intercambio de llaves para VPN de tipo Diffie-Hellman Grupo 1,2 y 5.
 - d. Mecanismos de autenticación de VPN mediante certificados digitales y clave precompartida (pre-shared).
 - e. Enrutamiento dinámico de VPN: deberá soportar la configuración de protocolos de ruteo dinámicos como RIP OSPF sobre los túneles IPSEC para permitir el manejo de túneles redundantes.
13. El equipo debe contar con un mecanismo automático de creación de túneles entre los equipos remotos para ser usado con tráfico de voz para la comunicación entre dependencias.
14. Funciones de Routing:
 - a. Soporte de protocolo de enrutamiento RIP.
 - b. Soporte de protocolo de enrutamiento OSPF.
 - c. Soporte de protocolo de enrutamiento BGPv4.
 - d. Soporte de PolicyBasedRouting donde la decisión de ruteo sea basada en campos del paquete (MATCH) como IP-Source/Puerto (TCP o UDP) IP-Destino/Puerto (TCP o UDP) y/o Qos (priority). La decisión de ruteo debe tomar la acción de seleccionar la interface a utilizar para enviar el paquete (Next-interface) o seleccionar el gateway a utilizar (next-hop).
 - e. Soporte de múltiples dominios de ruteo mínimo 3, donde cada dominio tendrá su propia tabla de ruteo y las interfaces físicas o lógicas pertenecientes a cada dominio podrán solapar su direccionamiento IP.
 - f. Las rutas pertenecientes a cada dominio de ruteo se podrán exportar entre los dominios utilizando listas de acceso para seleccionar las mismas.
15. Manejo de Tráfico y ataques:
 - a. Deberá poseer capacidad de manejo de apertura de puertos dinámicos en base a protocolos de uso común (FTP, H323, SIP, SCCP, MGCP) y posibilidad de crear sesiones personalizadas que manejen dicho comportamiento.
 - b. La solución deberá soportar la configuración de parámetros referidos a timeout en la tabla de estados de conexiones sobre cualquier servicio TCP en forma individual y global y sobre los servicios configurados por el administrador.
 - c. La solución deberá soportar la activación y desactivación de técnicas de detección y evasión de ataques de DOS (Denegación de servicio) y portScanning.

- d. La solución deberá soportar la activación y desactivación de técnicas de protección de ataques de generación masiva de conexiones (SYN attack) permitiendo su configuración para una dirección IP en particular como origen o destino del ataque.
 - e. El dispositivo debe tener la capacidad de configurar límites máximos de conexiones concurrentes recibidas por una dirección IP o hacia un mismo destino.
 - f. La solución deberá soportar la activación y desactivación de técnicas de anti-spoofing sobre cada zona de seguridad.
 - g. La solución deberá soportar técnicas de mitigación de spoofing en todas las interfaces.
 - h. El dispositivo debe poseer técnicas que mitiguen los ataques conocidos como: Ping Of Death ,TearDropAttack y WinNuke.
 - i. Las reglas que permitan o denieguen el trafico que atraviesa el dispositivo de seguridad deberán poder definirse, diferenciando protocolo, IP destino / IP origen, puerto destino / puerto origen, zona de seguridad y horario.
16. Administración:
- a. Deberá permitir monitoreo remoto mediante SNMP v2 permitiendo los queries de SNMP a través de la definición de direcciones IP autorizadas para realizar las consultas.
 - b. Autenticación de usuarios en forma local, por RADIUS, LDAP, SecureIDclient y TACACS+.
 - c. Las reglas deben permanecer en medios físicos, no volátiles.
17. Autenticación de usuarios de red:
- a. El equipo tendrá un mecanismo de autenticación que permitirá validar los usuarios para acceder a los recursos con 2 tipos de mecanismos simultáneos configurables por administrador para cada caso:
 - i. Con el equipo interceptando trafico FTP, Telnet o http para solicitar credenciales
 - ii. Con un portal Web HTTPS donde el usuario ingresa sus credenciales.
18. Calidad de Servicio:
- a. El equipo deberá permitir la configuración por políticas de Calidad de Servicio bajo todas a cada una de las siguientes:
 - i. Configuración por protocolo y por regla.
 - ii. Configuración de Ancho de banda garantizado.
 - iii. Configuración de Ancho de banda mínimo.
 - iv. Priorización en la utilización de Ancho de banda.
 - v. Clasificación y marcado de trafico por DiffServ.
 - vi. Aplicación de QOS a túneles IPSEC.
 - vii. Reserva de Ancho de banda para túneles IPSEC.
 - viii. El dispositivo debe permitir crear políticas de traffic-shaping en el tráfico saliente para las interfaces virtuales como subinterfaces o interfaces túneles.
19. Procesamiento de Contenidos (Funcionalidad General):

- a. El equipo deberá tener la potencialidad de incorporación de las siguientes funcionalidades de procesamiento de contenidos:
 - i. Antivirus para los siguientes protocolos: SMTP, POP3, Webmail, FTP, IMAP, http tanto en tráfico entrante como saliente.
 - ii. Detección y prevención de intrusos para los siguientes protocolos: SMTP, POP3, Webmail, FTP, IMAP, http tanto en tráfico entrante como saliente.
 - iii. ANTI-SPAM basado en base de datos de direcciones IP que permiten el acceso, marcado o eliminación de e-mail según la procedencia del correo.
 - iv. Filtro de contenidos para tráfico Web con creación de perfiles y políticas.

20. Licenciamiento:

- a. Deberá incluir una licencia por un plazo de tres (3) años para antivirus, prevención de intrusión, filtrado web, antispam, gestión de vulnerabilidad, control de aplicaciones y servicios de base de datos de seguridad.

10.6. Características de la Fibra Óptica

Los cables de Fibra Óptica responden a las Recomendaciones UIT-T G-652 D, para tráfico de voz, datos e imágenes con distribución entre los edificios.

El tipo de fibra es Monomodo La longitud de onda de dispersión nula 1310 +/- 10 nm

11. TECNOLOGÍA DE ALMACENAMIENTO

11.1. General.

Preferiblemente el almacenamiento deberá ser del tipo Scale-Out de Alta Capacidad Performance de tipo NAS u otra topología que favorezca la satisfactoria implementación de la solución del Software V.M.S. a implementar como repositorio de la información de video.

11.2. Aclaraciones

El texto siguiente hará referencia al término "solución". Para entendimiento de los requerimientos técnicos, se define el término "solución" como un "Clúster de alta capacidad para almacenamiento de datos que utilice la tecnología de Scale-Out NAS (Network Attached Storage) u otra topología que favorezca la implementación de la solución de la plataforma, sin dejar de considerar las definiciones antes mencionadas para disponibilidad del espacio de almacenamiento de datos de aplicaciones, usuarios finales, servidores y otros componentes del Sistema de Seguridad Electrónica de la Red de Subterráneos (Líneas A, B, C, D, E, H y Pre Metro). El término de "Cluster" se refiere a la agrupación de las unidades de procesamiento en un modo de trabajo tal que permita la continuidad del servicio que la solución brinda, aún ante la falla de alguna de las mismas, sin pérdida de datos y de modo transparente para los usuarios y/o aplicaciones que estén haciendo uso de la solución. El término Scale-Out se refiere a que el crecimiento no está limitado a la capacidad de la caja, sino al crecimiento del Clúster permitiendo la agregación de componentes que se visualicen como una única solución. Por último, la solución debe permitir que por medio de agregado de controladoras se pueda comenzar por una solución orientada a la capacidad, y permita la potencial incorporación de controladoras y/o discos que permitan también escalar el performance. Asimismo se considera que una solución NAS de almacenamiento no es una opción basada en servidores con sistemas operativos de propósitos múltiples (tales como Windows). En lo sucesivo el término "incluir" hará referencia a que la solución provista contenga de la capacidad o función descripta. Mientras que "disponer" hará referencia a los casos en que la solución provista no contenga la capacidad descripta, pero se podrá adicionar en un futuro y bajo las condiciones que se detallan en la descripción. Se entiende como "componente" a cualquier ítem que conforme la solución, pudiendo ser discos, placas de red, memoria, CPUs, chasis, interconexión de red, fuente de alimentación, entre otros. Global NameSpace, es una federación de sistemas de archivos a partir de cualquier cantidad de dispositivos de almacenamiento o servidores de archivos; es un mecanismo estándar para el manejo distribuido de volúmenes de almacenamiento de datos, permitiendo el acceso a los datos independientemente de su ubicación física. Podrá ser también aceptado que los datos de los sistemas de archivos puedan ser manejados en forma nativa y autónoma por el sistema de VMS, incluyendo los mecanismos de failover de la solución, todo esto manteniendo los estándares de seguridad y funcionalidades de la plataforma ofertada. El término provisionar hace referencia al término de lengua inglesa. "provisioning" utilizado para reservar espacio en unidades lógicas de almacenamiento y asignarlas a

un servidor o recurso. Considérese "Cuota" al espacio fijo en disco asignado para la guarda, sobre un volumen de disco compartido.

11.3. Especificaciones.

La propuesta deberá cumplir con las siguientes características:

- a) Deberá cumplir con un espacio mínimo disponible como para permitir el almacenamiento de la información con la calidad y espacio de tiempo requerida (estimación de 5-CINCO Petabytes- el Oferente hará el cálculo exacto y lo justificará), con un nivel de protección de disco mínimo de (Raid 6, DP o superior), como así también alta disponibilidad, entendiéndose esto como que tenga la capacidad de tolerar la falla de uno o más componentes que conforman la solución sin pérdida de datos ni de servicio. Una vez reparado el elemento dañado, la solución deberá recomponer el nivel de protección para toda la información existente antes de la falla y realizarlo en forma automática.
Deberá demostrar el cálculo realizado para el almacenamiento de la información
- b) La arquitectura de la solución deberá ser un único files system, o suplirlo con la inclusión e implementación de un único Global NameSpace, o utilizar la organización de archivos provista en forma nativa por el Software a implementar, manteniendo los estándares de Seguridad y funcionalidades de lo solicitado anteriormente.
- c) Deberá disponer la capacidad de crecer en tamaño desde la capacidad de almacenamiento calculada a 20 (VEINTE) Petabytes, o mayor en un solo Filesystem y/o NameSpace o en la organización de archivos provista en forma nativa por el sistema de V.M.S ofertado., en modo no disruptivo para las aplicaciones y/o usuarios y sin ser requeridos cambios configurativos en los clientes (usuarios y/o aplicaciones) de la solución. Esto implica que la solución provista deberá contar con todo lo necesario para cumplir el crecimiento formulado y garantizar la no interrupción del servicio durante la adición de componentes a la misma. Durante el proceso de adición de componentes la solución deberá disponer de la capacidad de seguir manteniendo el nivel de protección definido en cada paso.
- d) Deberá incluir discos de tecnología NLSAS/SATA de 2, 3 o 4TB, de modo tal de cumplir con la capacidad de almacenamiento ofertada (disponibles) y el nivel de protección Raid 6, DP o superior requerido
- e) Ante el incremento en la cantidad de discos por la adición de componentes, la solución deberá disponer la capacidad de redistribuir la información existente en modo automática y transparente para el usuario y sin modificar el NameSpace o la organización de archivos provista en forma nativa por el sistema de V.M.S. de la solución. Todo esto manteniendo los estándares de seguridad y funcionalidades de lo solicitado anteriormente. Caso de no realizarse, el proveedor deberá incluir un servicio para la redistribución de los datos SIN afección del servicio brindado por el almacenamiento. El mismo deberá incluirse junto a los costos de crecimiento futuro para 10 (DIEZ) Peta bytes con las tareas y tiempos requeridos para el balanceo del contenido entre todos los discos de todas las controladoras.

- f) Deberá incluir la capacidad de actualizar el sistema operacional de modo transparente, de forma tal de garantizar que el impacto sobre los "clientes" conectados al cluster sea el menor posible y preferentemente transparente. El Oferente deberá explicar en detalle el proceso de "upgrade" de versiones.
- g) Deberá estar soportada por un mínimo de 24 (veinticuatro) controladoras redundantes nativas NAS.
- h) Deberá incluir una "Cache" no menor a 512GB. Como Cache no se considera las expansiones complementarias sobre placas de memoria o sobre discos SSD
- i) Deberá contar con la cantidad de puertos FC, ISCSI y/o IP tanto en el Front-End como en los Back-End necesarios para garantizar la mejor performance posible para la solución.
- j) Deberá implementar e incluir, como mínimo, los siguientes protocolos, que dispondrán las áreas de almacenamiento de red: NFSV1, NFSV2, NFSV3, NFSV4, CIFS (SMBV1 e SMBV2), FTP, HTTP, HTTPS.
- k) Deberá incluir el gerenciamento centralizado vía Web, integrado en su propio sistema operativo, con capacidades de creación de niveles de acceso de usuario (Súper usuario, Administrador, Operador, etc).
- l) Deberá incluir acceso vía SSH para la administración remota mediante línea de comandos.
- m) Deberá incluir el soporte de protocolo NDMP para realizar backup vía NDMP mediante protocolo FiberChannel, permitiendo la interconexión directa a la SAN, permitiendo el tráfico de Backup se realice entre la solución y los dispositivos de Backup (Tape Libraries) sin necesidad de uso en las CPUs del servidor de Backup.
- n) Deberá disponer de soporte para la provisión dinámica de espacio de almacenamiento para usuario, servidores y aplicaciones, sin requerir cambios de configuración en los clientes de la solución.
- o) Deberá incluir soporte de los Sistemas Operativos: Windows 2000, Windows 2003, Windows 2008, Windows XP, Windows 7, IBM AIX, HP-UX, Solaris, VMWareESX, vSphere, Red Hat Linux Enterprise y SuSE Enterprise Linux.
- p) Deberá disponer de la capacidad de implementar replicación remota de datos de forma asíncrona. Deberá permitir políticas de recuperación rápida en caso de desastre y la tecnología de Snapshot.
- q) Deberá incluir soporte de IPv4 e IPv6.
- r) Deberá disponer de un monitoreo de sus componentes con almacenamiento de datos históricos, de forma que las informaciones puedan ser analizadas y utilizadas para provisión de futuros upgrades.

12. CABLEADO.

12.1. General.

Según la normativa EIA/TIA 942, 606-A, 568-B, 569-B, 607. Se realizará el Cableado UTP interior, el que debe cumplir con las pruebas de rendimiento y desempeño de la EIA/TIA 568B.2-1 y ISO/ IEC 11801 Categoría 6 o superior. El cable tendrá aislante de Polietileno de alta densidad y la cubierta del cable UTP debe ser de PVC, tipo Plenum. Los puntos de red serán centralizados e identificados debidamente, tanto en los puestos de trabajo como en el Rack principal. Se proveerá de un punto de red por cada puesto de trabajo. Estos puntos estarán centralizados e identificados debidamente tanto en los puestos de trabajo como el rack de reparto principal. Debido a las pruebas de calidad que se realizarán, todo el equipamiento aquí propuesto deberá pasar por un proceso de certificación de todas las líneas de UTP conforme a las normativas EIA / TIA que define los criterios de desempeño, con los cuales se podrán medir con uniformidad todos los componentes de la red.

12.2. Normativas aplicables al Cableado.

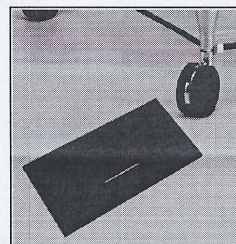
- EIA/TIA 942 Norma de estándares de instalaciones en centros de datos.
- ANSI/TIA/EIA-568-B Cableado de Telecomunicaciones.
- TIA/EIA 568-B1 Requerimientos generales.
- TIA/EIA 568-B2 Componentes de cableado mediante par trenzado balanceado.
- TIA/EIA 568-B3 Componentes de cableado, Fibra óptica.
- ANSI/TIA/EIA-569-A Normas de Recorridos y Espacios de Telecomunicaciones en Edificios Comerciales (Cómo enrutar el cableado).
- ANSI/TIA/EIA-570-A Normas de Infraestructura Residencial de Telecomunicaciones
- ANSI/TIA/EIA-606-A Normas de Documentación y Administración de Infraestructura de Telecomunicaciones en Edificios Comerciales.
- ANSI/TIA/EIA-607 Requerimientos para instalaciones de sistemas de puesta a tierra de Telecomunicaciones en Edificios Comerciales, siempre que no se contrapongan a las disposiciones de la A.E.A. (Asociación Electrónica Argentina). Ver Pliego de Especificaciones Técnicas Generales.
- ANSI/TIA/EIA-758 Norma Cliente-Propietario de cableado de Planta Externa de Telecomunicaciones.

12.3. Distribución y Terminales.

La Red de Datos y de Telefonía que deba realizarse por sistema de "piso ducto" terminará en tapas al ras de piso similares a la que se muestra en la figura:

Dentro de la Misma, y en el caso de Cajas Rectangulares de Pared u otra Disposición, se deberá instalar como mínimo, por cada puesto:

- 2 Bocas de UTP RJ-45 (Una Datos / Una Telefonía)



- 2 Tomas 220V, NO ESTABILIZADA
- 2 Tomas 220V, ESTABILIZADA

12.4. Organización de Racks y Cableado interno.

Se utilizará el criterio de diseño denominado "Middle of Row" para la distribución de Racks. El Rack Central dentro de la Sala según Esquema Adjunto, será el que contendrá la Electrónica de Red (Switch's) y los Patch-Panel Necesarios para el Cableado Estructurado de todo el Edificio; también tendrán 7 Patch-Panel de 24 Bocas cada uno, destinados a la interconexión de Racks. Se contemplara en el mismo Rack espacio destinado a los equipos provistos por los proveedores de Acceso. Si no fuese suficiente un Rack, se utilizara el Rack contiguo, Equilibrando la carga de los mismos. (SW, Patch-Panel's, Espacio para Proveedores). En cada Rack instalado en la Sala, se colocara en la parte superior un Patch-Panel de 24 bocas destinado a la interconexión con el Rack Central de DISTRIBUCION.

13. SALA DE SERVIDORES

13.1. General.

Se deberá tener en cuenta como referencia que con la totalidad del equipamiento instalado, los equipos de aire acondicionado deben poder brindar una temperatura en la Sala de Servidores constante entre 20 a 25 °C , con una Humedad del 40 % al 55% (Relativa). Todas las perforaciones que se realicen en las paredes de la Sala de Servidores para entrada o salida de ductos, bandejas porta cables, deberán estar selladas por un material con clasificación de contención de fuego de 1 hora, que cumple con los requerimientos de ASTM E 814: Standard Method of Fire Tests of Through-Penetration Fire Stops. Desde el Tablero Seccionador, debe realizarse por las bandejas portacables de tensión (bajo el piso técnico) el cableado hasta sobre cada una de las posiciones de los racks como se detalla en plano; quedando un total de 2 Mts. de excedente a fin de dar conexión eléctrica dentro de dichos Racks. Cada servicio contará con llaves térmicas dedicadas conectadas al sistema de U.P.S.. Como terminal se proveerá de Conectores Industriales con puesta a tierra 20A. Cada Línea de Alimentación de Rack debe poseer un Filtro/Protector de Red Eléctrica de la Potencia adecuada, a fin de proteger el equipamiento ante variaciones bruscas de alimentación/eliminación de ruidos y distorsiones que pudieren ocasionar fallas en el correcto funcionamiento. Todas las bandejas que se instalen dentro de los pisos técnicos y que transporten cables eléctricos deben poseer conductividad de Puesta a Tierra (Ver Pliego de Especificaciones Técnicas Generales) y estar a una distancia de 30 cm. de la Bandeja de Datos. Toda la información de los trabajos propuestos deberá estar presentada en la Oferta, junto con los planos de distribución: eléctricos, dispositivos de red y de almacenamiento, entre otros.

13.2. Racks.

Los Racks deben ser de una altura Máxima de 45 RU, con capacidad para alojar equipos de hasta 19" de ancho. Debe ser capaz de manejar un enfriamiento y un flujo de aire tal que elimine la necesidad de ventiladores adicionales; además debe tener una puerta en la parte delantera y otra en la parte trasera la cual pueda ser abierta ya sea hacia la izquierda o hacia la derecha, y que sea fácilmente desmontable. Estas deben ser del tipo micro perforadas para que el racks mantenga sus propiedades de flujo de aire. Debe contar con organizadores Verticales de cableado a sus ambos lados de un mínimo de 8".

13.3. Bandejas porta cables.

Se dispondrá en el piso técnico y por debajo de la Columna de Racks, las bandejas necesarias para el tendido de cableado eléctrico, cableado de red y Cableado de Fibra Óptica; todas bandejas independientes instaladas debajo del piso técnico a una distancia de Bandeja a Bandeja no menor de 30 cm. La disposición será la siguiente:

- Las bandejas más cercanas a los Racks serán para el Cableado de datos, preferentemente debajo del pasillo caliente.
- La bandeja de Cableado de Energía se colocará preferentemente debajo del pasillo caliente.

13.4. Piso Técnico.

Se dispondrá en la sala de datos correspondiente a cada C.M.S., un Piso Técnico Completo, tipo acero cemento, con pedestales para regulación de altura de 38 cm NPT (regulación +/- 2 cm.). Los pedestales podrán ser cortados por su colocador para conseguir la altura deseada. Descripción de las placas: Placas de piso técnico formadas por doble capa de chapa de acero protegidas con pintura epoxi en las cuatro caras, conformada estructuralmente por estampa, soldadas entre sí, y rellenas con mortero cementicio liviano de alta resistencia, con revestimiento laminado plástico de 1,6 mm de espesor, para alto tránsito. Deberá responder a las siguientes características:

DIMENSIONES	610 x 610 x 35
mm	
PESO MÍNIMO DEL PANEL	15 Kg/unidad
PESO MÁXIMO DEL SISTEMA	45 kg/m ²
TOLERANCIA DIMENSIONAL	+/- 0,2 mm

CARACTERÍSTICAS MINIMAS DE PERFORMANCE

Carga concentrada en el centro	445 Kg
Deformación máxima admisible	0.02 mm
Carga puntual de rotura	1.100 kg.
Carga distribuida equivalente	1.500 Kg/m ²
Conductividad Eléctrica cumple norma ASTM E84-86 y NFPA	Clase 1
Desarrollo de humo	< 10
Frecuencia	500 ciclos/seg.
Aislación acústica cumple norma ASTM E36-77 / E413-77	
Carga axil de compresión que soporta cada pedestal	3.500 kg

Asimismo se proveerán 2 pares de ventosas aptas para la remoción de las placas instaladas sobre los pedestales.

13.5. Refrigeración.

Se deberá proveer e instalar un sistema de refrigeración de Precisión para la capacidad total de Carga Eléctrica y las dimensiones de la Sala de Equipos, no se aceptan equipos de aire acondicionado de confort. La unidad debe ser diseñada específicamente para acondicionar salas de cómputo y telecomunicaciones, debe cumplir con el control preciso de temperatura y humedad relativa, con ciclos de: enfriamiento, Calefacción, Humidificación, deshumidificación y Filtrado del aire. La unidad debe tener un Controlador basado en microprocesador con control automático de todas las funciones; tener un visualizador ("display") exhibiendo: Temperatura ambiente en °C, Humedad Relativa del Cuarto, Indicador de Modo de Operación, Alarmas. Las configuraciones y parámetros de operación del sistema deben permanecer almacenados en la memoria

en forma no volátil ante un corte de energía. El controlador debe tener por lo menos tres (3) niveles de seguridad para el acceso a la información y los parámetros de configuración. El controlador debe ser capaz de comunicarse mediante el protocolo SNMP para establecer una función de supervisión remota. Debe poseer un registro histórico de los últimos 50 acontecimientos, y un sistema de alarma audible ante desperfectos y variaciones de parámetros configurados.

13.6. Sistema de Energía Ininterrumpida (U.P.S.) para carga IT.

Se deberá proveer e instalar un sistema UPS para la Carga Eléctrica Total de la Sala de Equipos.- La autonomía mínima será de 15 Minutos. Será una U.P.S. tipo en línea ("on line") de doble conversión. El sistema estará Configurado en el Formato 2+1 (50% redundancia). El Sistema podrá funcionar en un Rango de Voltaje de 220 o 380 Volts.(+-20%). Poseerá unidad de Monitoreo y control con visualización (Display) del estado de la unidad, de todos sus parámetros básicos, alarmas; además de una alarmas audible ante eventos del tipo alarma, y debe ser capaz de comunicarse mediante el protocolo SNMP para establecer una función de supervisión remota. El tipo de baterías será selladas, libres de mantenimiento, y alojadas al exterior de la UPS en un gabinete adjunto.

14. SERVIDORES

Los servidores a proveer tendrán las características que permitan brindar todas las condiciones de funcionamiento del Sistema V.M.S. ofrecido y deberán responder a primeras marcas del mercado (HP, DELL, IBM).

15. PROVISION DE INSTRUMENTOS DE PRUEBA

Se proveerá el siguiente instrumental necesario para los análisis en las post instalaciones del sistema de video vigilancia:

- Medidor / Analizador de Inductores Capacitores y Resistores. UT612 o similar.
- Luxómetro Digital de 3 ½ dígitos Marca Tenmars o similar. Con Estuche.
- Multímetro de banco. UT 803 o similar.
- Pinza amperométrica, UT 204 o similar.
- Decibelímetro. UT 352 o similar.
- Generador de Funciones UTG9010C o similar
- Cámara termográfica modelo Flex cam T155 (FLUKE) o similar.
- Certificador de red FLUKE Serie DTX-1800 MSO o similar
- Network Time Machine CSN/NTM-PO2B-10PA o similar

16. ERGONOMETRÍA DE MOBILIARIO DE SALA DE MONITOREO DEL C.M.S.

Todos los puestos enumerados en los puntos 5.6; 5.7; 5.8 y 5.9 deberán equiparse respetando lo dispuesto en las normas IRAM 4174, ISO 11064-1; 9241; 9241-11 y 11064-7 que contempla el diseño ergonómico de centros de control, que sean de aplicación lo requerido.

16.1. Silla ergonómica para operadores de Centros de Monitoreo

Deberá poseer las siguientes características:

- Silla con base de cinco radios, con ruedas que permitan el desplazamiento con un mínimo de esfuerzo.
- Fabricada 100% en Nylon.
- El forro del asiento y respaldo debe de ser de color negro.
- Debe tener soporte ergonómico en la zona lumbar y mantener la curvatura natural del hueco que se produce en la espalda, para evitar fatiga.
- Debe tener articulación en el asiento. El borde delantero del asiento debe inclinarse suavemente hacia abajo y no debe presionar el muslo.
- Altura de asiento y respaldo ajustables con el fin de que sea suficientemente alta para que los muslos formen un ángulo de 90° con el piso.
- Respaldo largo
- Descansa brazos

17. CARACTERÍSTICAS DEL SERVICIO A BRINDAR POR EL ADJUDICATARIO.

17.1. General.

Durante el primer año de servicio y cursos de capacitación mediante, el personal técnico del adjudicatario deberá configurar el sistema para la entrega modalidad "llave en mano" y responder a los requerimientos de reconfiguración, agregado de mapas digitales interactivos, copias de resguardo y restauración, generación de "rondas", "vistas", configuración de zonas de alarma y/o control de accesos, soporte para bajada de imágenes y videos, y todo otro tipo de servicios propios de un sistema de esta envergadura; todos ellos sin costo adicional para SBASE

17.2. Servicio de Mantenimiento preventivo y correctivo.

El Servicio Ofrecido deberá:

- Brindar soporte de 24 horas, durante los 7 días de la semana, incluido feriados, durante el período de 36 meses, al momento de dar por aceptado la instalación de los equipos. El tiempo de respuesta para la asistencia en el sitio (onSite) para cualquier tipo de falla de hardware 24 horas corridas siguientes de abierto el caso.

18. PRUEBAS DE ACEPTACIÓN DEL SISTEMA**18.1. General**

El Oferente deberá entregar a la Comisión Técnica Evaluadora una versión completa del Software ofrecido y su documentación completa para su evaluación por el término de 30 días corridos, así como también una cámara de cada tipo de las requeridas en el PET Particulares con toda su documentación, sin perjuicio de la evaluación que se realizará a través de la siguiente Matriz de Evaluación Técnica:

18.2. Matriz de Evaluación Técnica.

RESUMEN	MAX
1. Plataforma del Sistema: Software de Gestión de Video (V.M.S.), Alarmas y Ctrol. de Accesos. Cumplimiento de los ítems 5 y 6 del PET Generales e ítems 4, 5, y 6 del PET Particulares, con exclusión de los ítems 5.7.4, 5.7.5, 5.7.6, 5.7.7 y 5.7.8 (Video Cámaras).	30
2. Hardware de Almacenamiento: Cumplimiento de los ítems 5.2. y 5.3. del PET Generales e ítem 9 del PET Particulares	10
3. Hardware de Red: Cumplimiento de los ítems 5.2. y 5.3. del PET Generales e ítem 8 del PET Particulares.	20
4. Dispositivos de Captura / Video Cámaras: Cumplimiento de los ítems 5.7.4, 5.7.5, 5.7.6, 5.7.7 y 5.7.8. del PET Particulares.	10
5. C.M.S.: Cumplimiento de los ítems 6 y 7 del PET Generales e ítems 7, 11, 12, 13, 14 y 16 del PET Particulares.	15
6. Del Oferente: Cumplimiento de los ítems 3, 4.11., 11, 12 y 13 del PET Generales e ítem 3 del PET Particulares.	15
TOTAL	100

1. PLATAFORMA DEL SISTEMA:	Evaluación
PET Generales ítems 5 y 6. PET Particulares ítems 4.1., 4.3., 4.4., 4.6., 4.7., 4.8., y 4.9.	No satisface: 0 Satisface: 4 Muy Satisfactorio: 5
PET Particulares ítems 4.2 y 4.5.	No satisface: 0 Satisface: 4 Muy Satisfactorio: 5
PET Particulares ítems 5.1., 5.2., 5.2.1, y 5.2.2.	No satisface: 0 Satisface: 4 Muy Satisfactorio: 5
PET Particulares ítems 5.2.3., 5.2.4., 5.2.5. y 5.3.	No satisface: 0 Satisface: 3 Muy Satisfactorio: 5

SUBTERRÁNEOS DE BUENOS AIRES S.E.

PET Particulares ítems 5.4., 5.5., 5.6. y 5.7.	No satisface: 0 Satisface: 3 Muy Satisfactorio: 5
PET Particulares ítem 6.	No satisface: 0 Satisface: 3 Muy Satisfactorio: 5

2. HARDWARE DE ALMACENAMIENTO	Evaluación
PET Particulares Ítem 9.3 Especificaciones	No satisface: 0 Satisface: 8 Muy Satisfactorio: 10

3. HARDWARE DE RED	Evaluación
PET Particulares Ítem 8.2.1. Estaciones o puntos de anillo	No satisface: 0 Satisface: 3 Muy Satisfactorio: 5
PET Particulares ítem 8.2.3. Switches de core o concentradores	No satisface: 0 Satisface: 3 Muy Satisfactorio: 5
PET Particulares Ítem 8.3. Software de Administración de Red LAN	No satisface: 0 Satisface: 5 Muy Satisfactorio: 7
PET Particulares ítem 8.4. Equipos IPS- VPN- FireWall, Antispam, Antispyware	No satisface: 0 Satisface: 2 Muy Satisfactorio: 3

4. PUNTOS DE CAPTURA/CÁMARAS.	Evaluación
PET Particulares ítem 5.7.4. Cámaras General	No satisface: 0 Satisface: 1 Muy Satisfactorio: 2
PET Particulares Ítem 5.7.5. Cámaras fijas Color	No satisface: 0 Satisface: 1 Muy Satisfactorio: 2
PET Particulares Ítem 5.7.6. Cámaras HD Color	No satisface: 0 Satisface: 2 Muy Satisfactorio: 3
PET Particulares Ítem 5.7.7. Cámaras Domo Color	No satisface: 0 Satisface: 2 Muy Satisfactorio: 3

5. C.M.S.	Evaluación
-----------	------------

PET Particulares Ítems 7.1. y 7.2.	No satisface: 0 Satisface: 3 Muy Satisfactorio: 4
PET Particulares Ítem 7.3.	No satisface: 0 Satisface: 3 Muy Satisfactorio: 4
PET Particulares Ítem 7.4.	No satisface: 0 Satisface: 1 Muy Satisfactorio: 2
PET Particulares Ítems 11, 12, 13, 14 y 16.	No satisface: 0 Satisface: 4 Muy Satisfactorio: 5

6. DEL OFERENTE	Evaluación
PET Generales Ítems 3.2., 3.3., 3.4., 4.8., 4.9., 4.10., 4.11., y 4.12.	No satisface: 0 Satisface: 3 Muy Satisfactorio: 5
PET Generales Ítems 11, 12, 13 y del PET Particulares Ítem 3	No satisface: 0 Satisface: 8 Muy Satisfactorio: 10

Cuando en la tabla figura el ítem principal y no se detallan los subítems, se los debe considerar en su totalidad. No se considerarán Ofertas que no cumplan con alguno de los ítems de la matriz. Aquellas ofertas que alcancen un mínimo de 70 puntos en la Matriz de Evaluación Técnica (PET), pasarán a ser evaluadas en su faz económica.

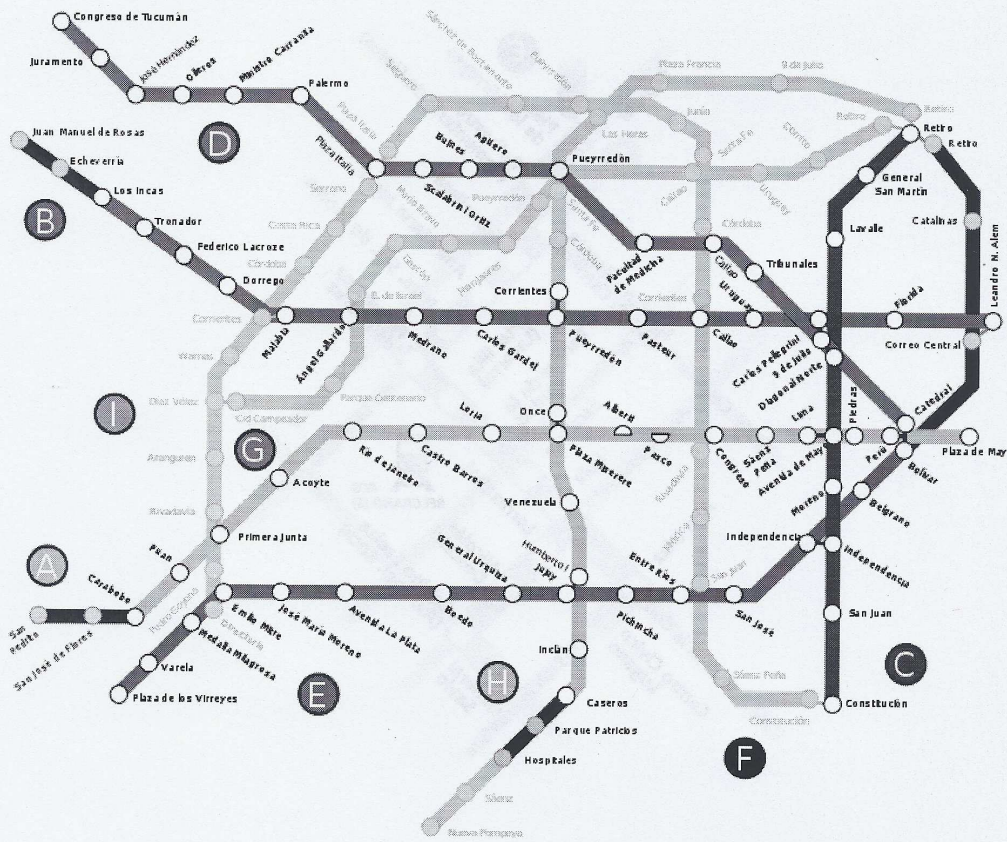
19. GARANTÍA

El equipamiento y software deberá poseer una garantía de 3 años con 24hs de tiempo de respuesta 12x5 de 9 a 19hs, días hábiles.

Subestación 1	Muy Satisfactorio
Subestación 2	Muy Satisfactorio
Subestación 3	Muy Satisfactorio
Subestación 4	Muy Satisfactorio
Subestación 5	Muy Satisfactorio
Subestación 6	Muy Satisfactorio
Subestación 7	Muy Satisfactorio
Subestación 8	Muy Satisfactorio
Subestación 9	Muy Satisfactorio
Subestación 10	Muy Satisfactorio
Subestación 11	Muy Satisfactorio
Subestación 12	Muy Satisfactorio
Subestación 13	Muy Satisfactorio
Subestación 14	Muy Satisfactorio
Subestación 15	Muy Satisfactorio
Subestación 16	Muy Satisfactorio
Subestación 17	Muy Satisfactorio
Subestación 18	Muy Satisfactorio
Subestación 19	Muy Satisfactorio
Subestación 20	Muy Satisfactorio

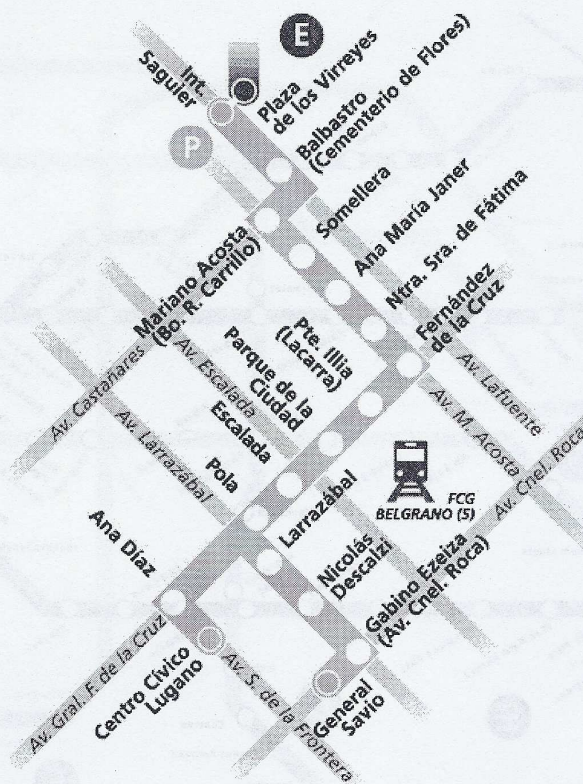
Cuando en la tabla figura el ítem "Satisfactorio" y no se detallan los subítems, se los debe considerar en su totalidad. No se consideran "Defectos" los subítems que no cumplen con alguno de los ítems de la matriz, aquellos datos que difieren en un máximo de 10 puntos en la Matriz de Evaluación Técnica (MET) poseen a ser evaluados en su ítem correspondiente.

20. ANEXO 1 – Plano Red de Subterráneos de la Ciudad Autónoma de Buenos Aires



21. ANEXO 2 - Plano Red del Pre Metro de la Ciudad Autónoma de Buenos Aires

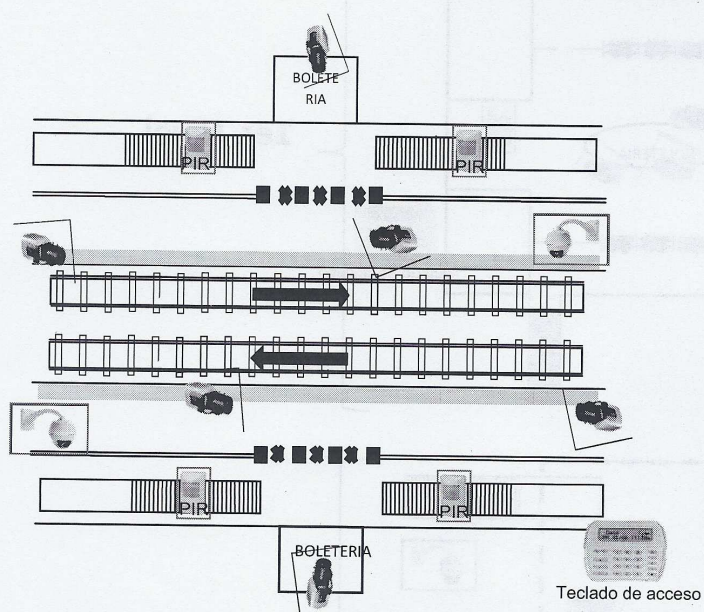
Recorrido y estaciones del Premetro



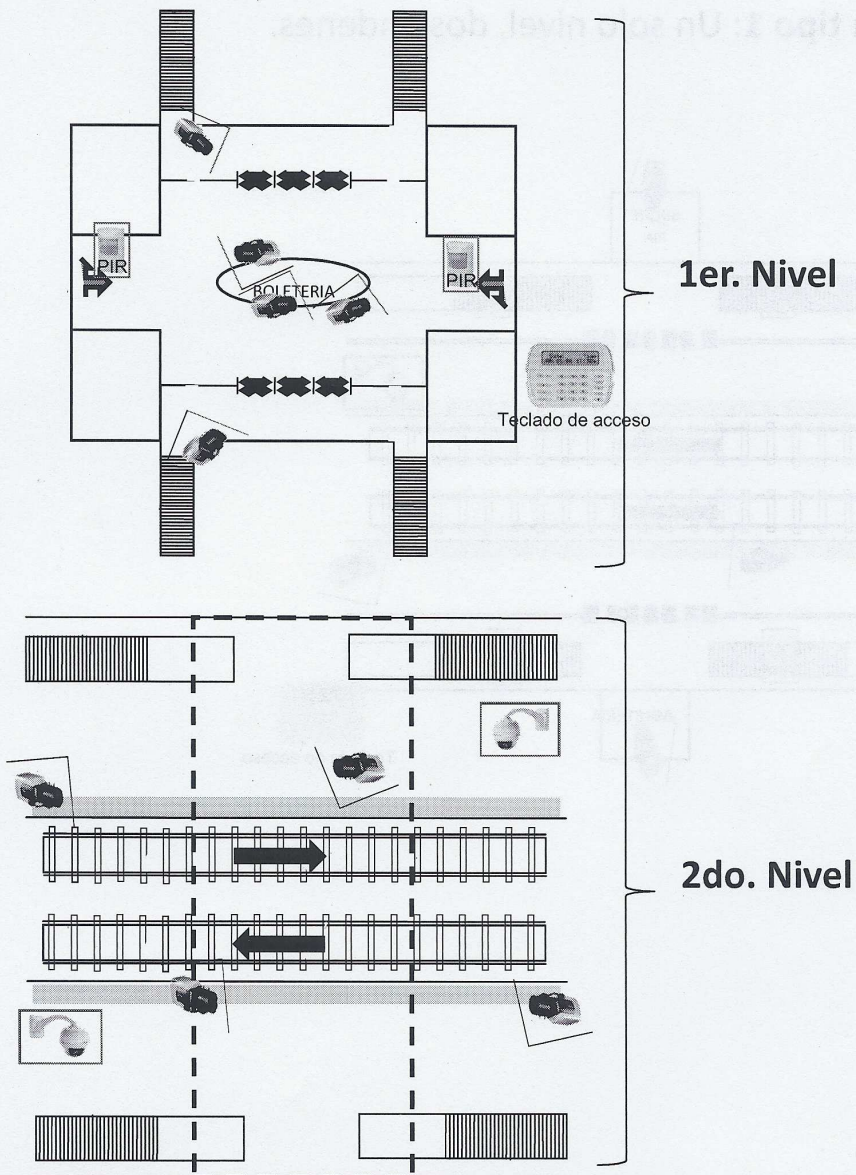
Tiene un total de 17 estaciones, tres de las cuales son terminales (Virreyes, Gral. Savio y Centro Cívico, en total suman 16 domos y cuatro cámaras fijas).

22. ANEXO 3 – Modelos tipo Estaciones de Subterráneo para colocación de dispositivos de captura de imagen.

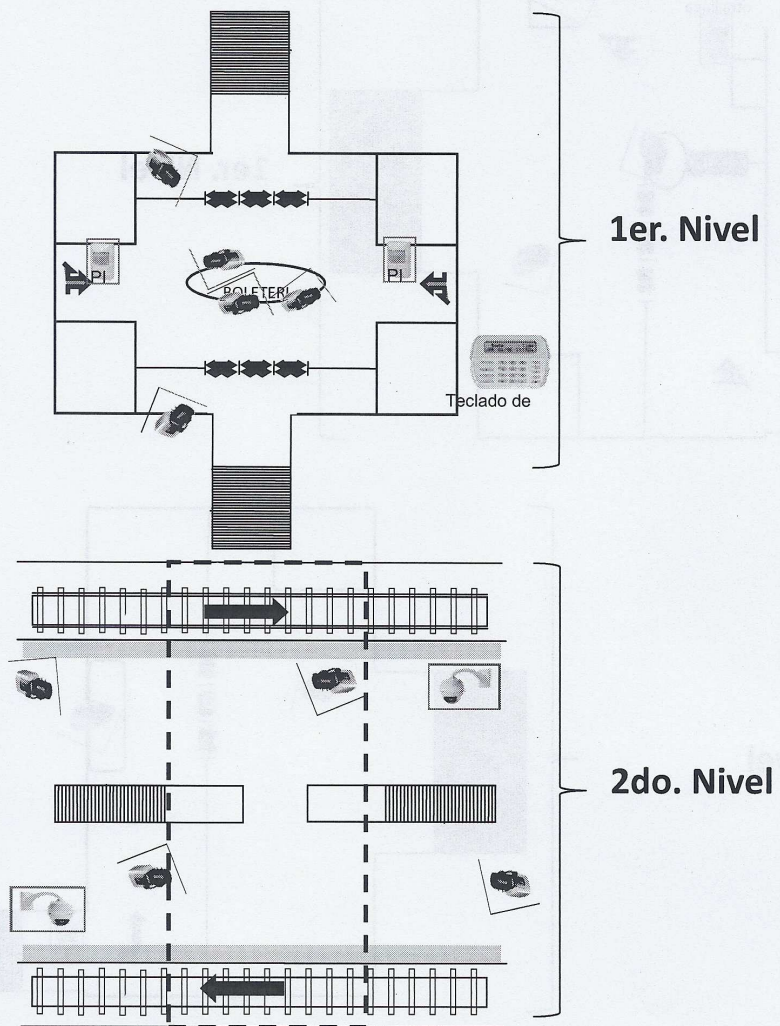
Planta tipo 1: Un solo nivel, dos andenes.



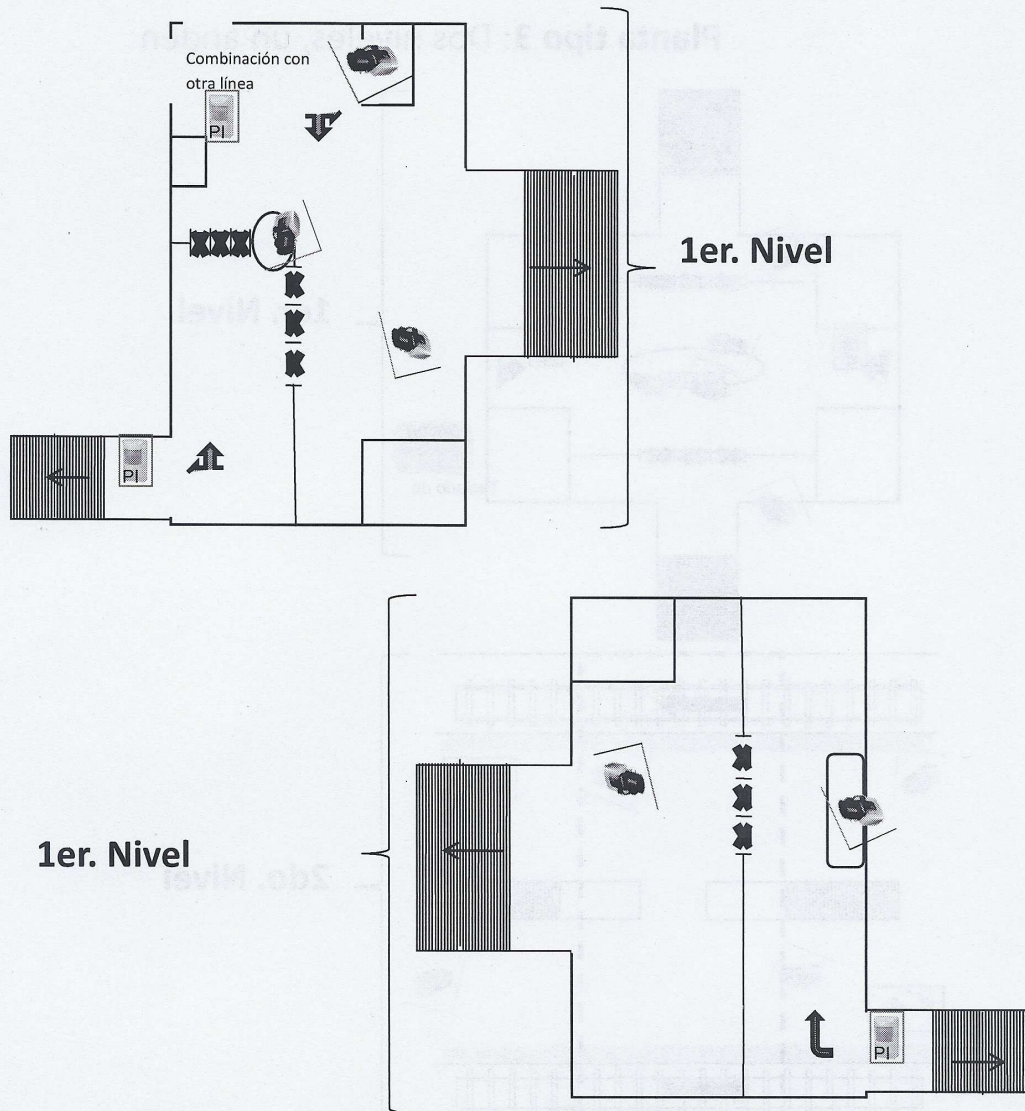
Planta tipo 2: Dos niveles, dos andenes.



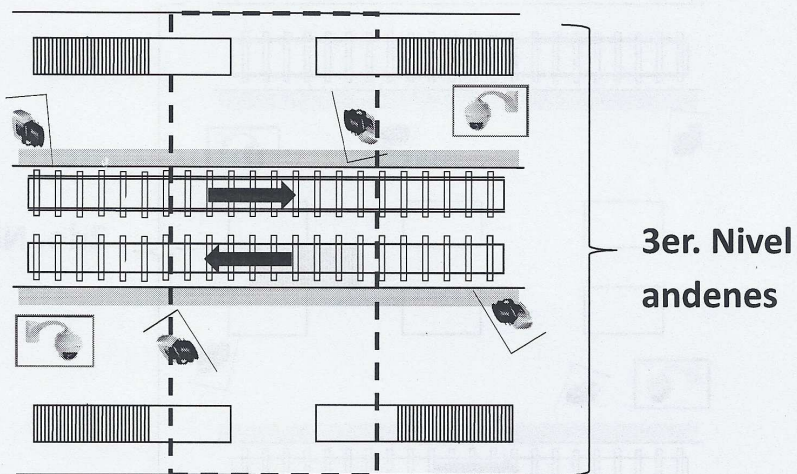
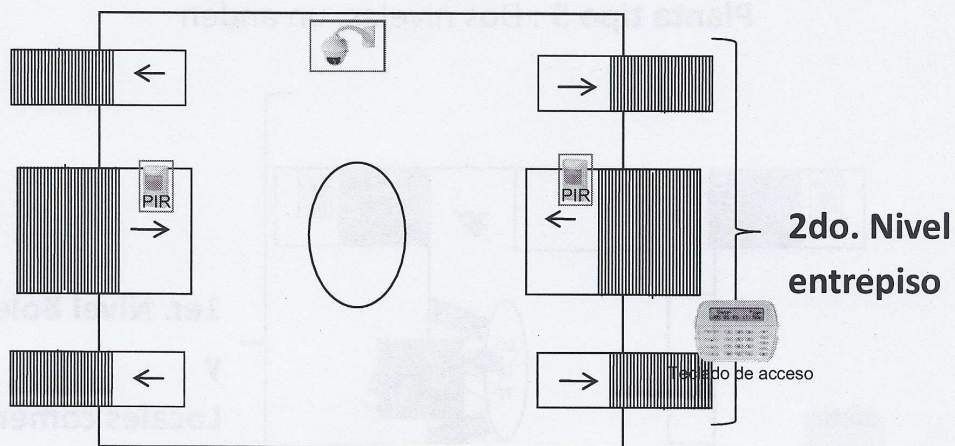
Planta tipo 3: Dos niveles, un andén



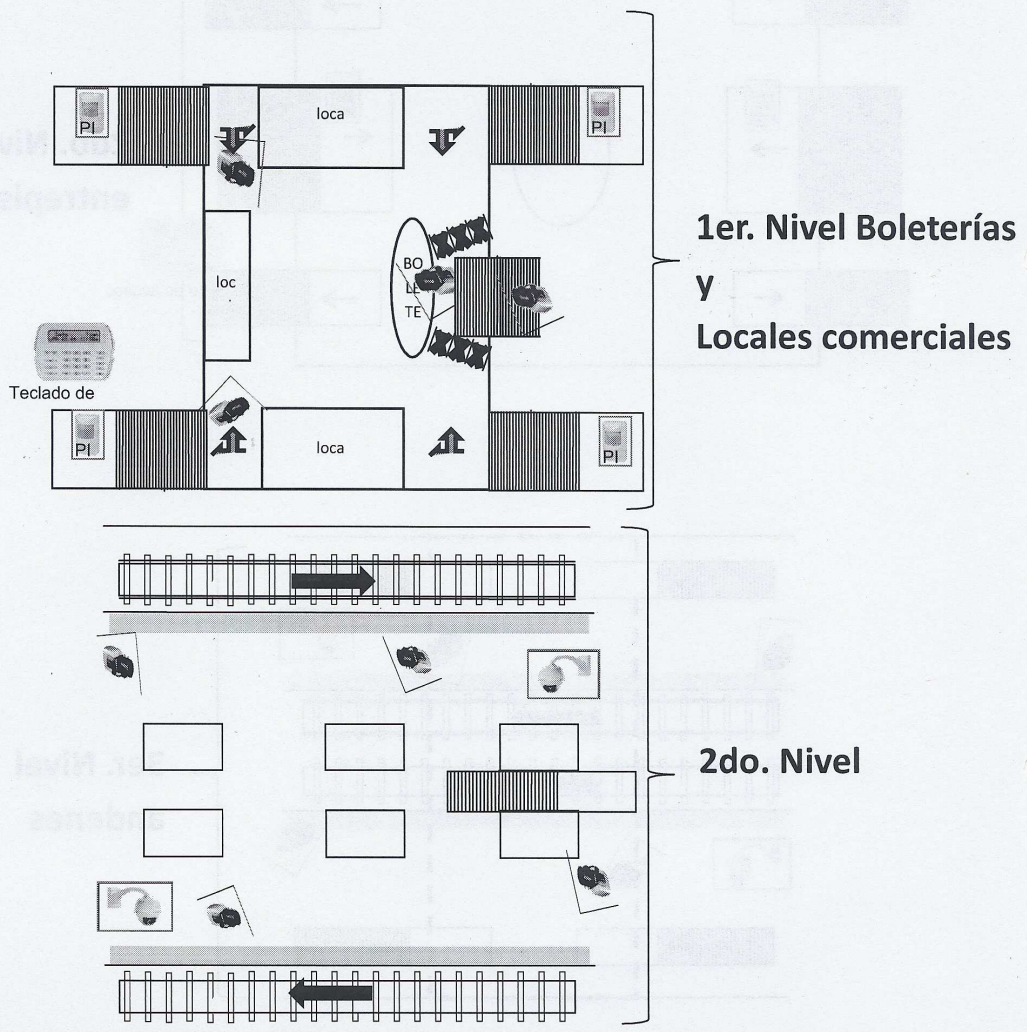
Planta tipo 4: Tres niveles, dos andenes, dos ingresos



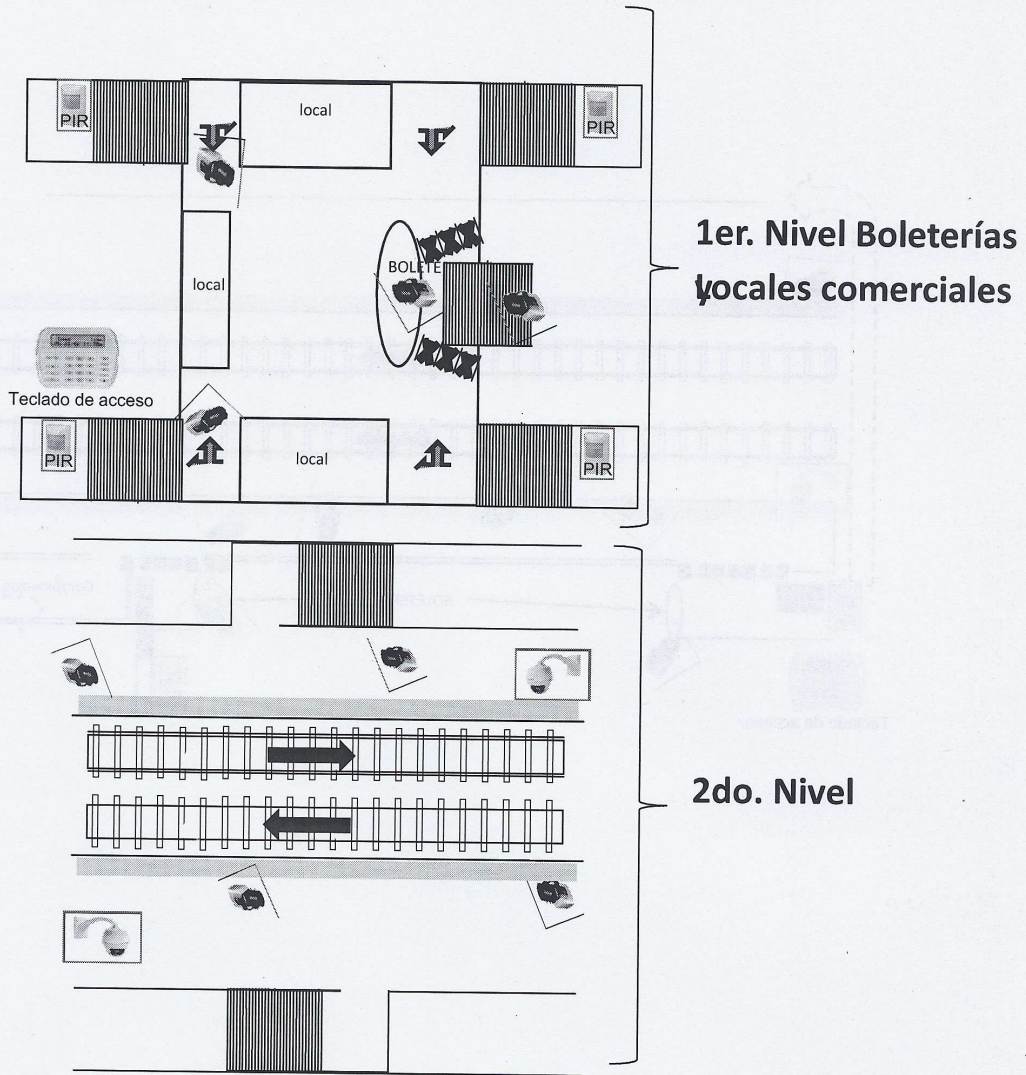
Planta tipo 4 : Tres niveles, dos andenes, dos ingresos



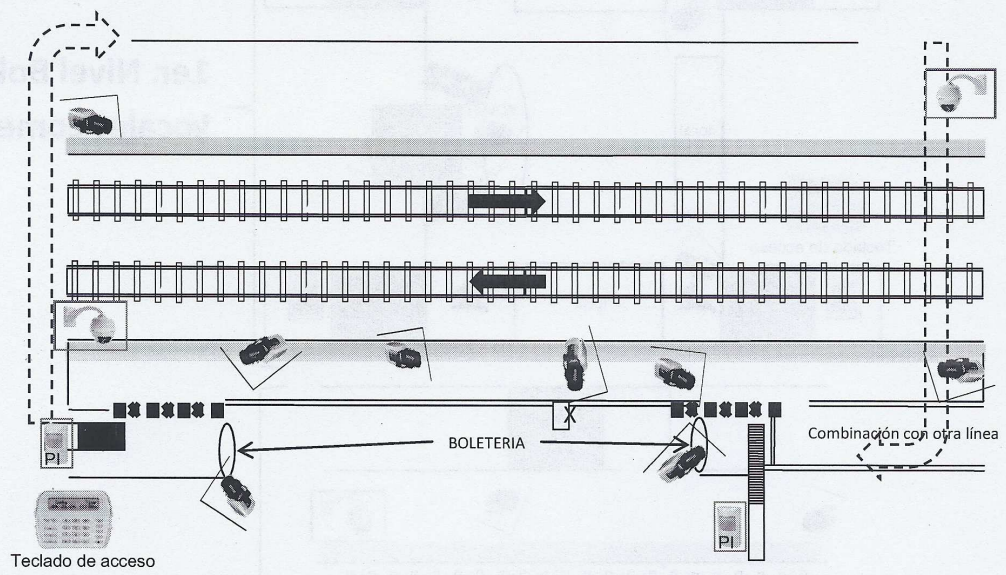
Planta tipo 5 : Dos niveles, un andén



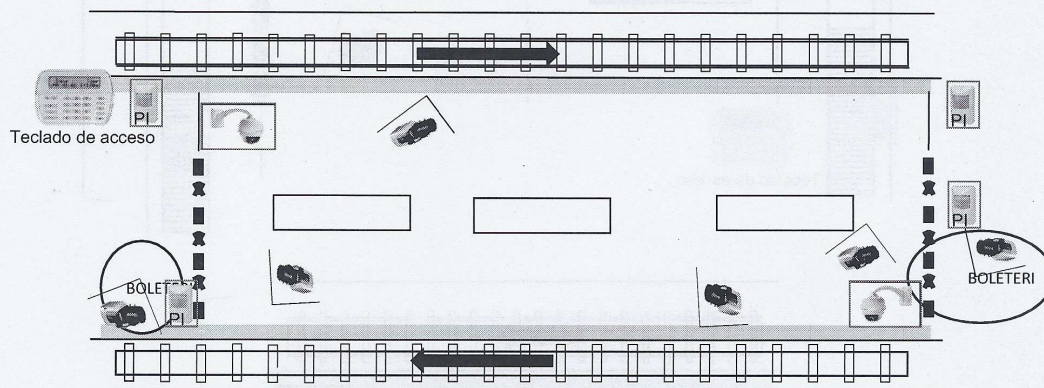
Planta tipo 6 : Dos niveles, dos andenes.



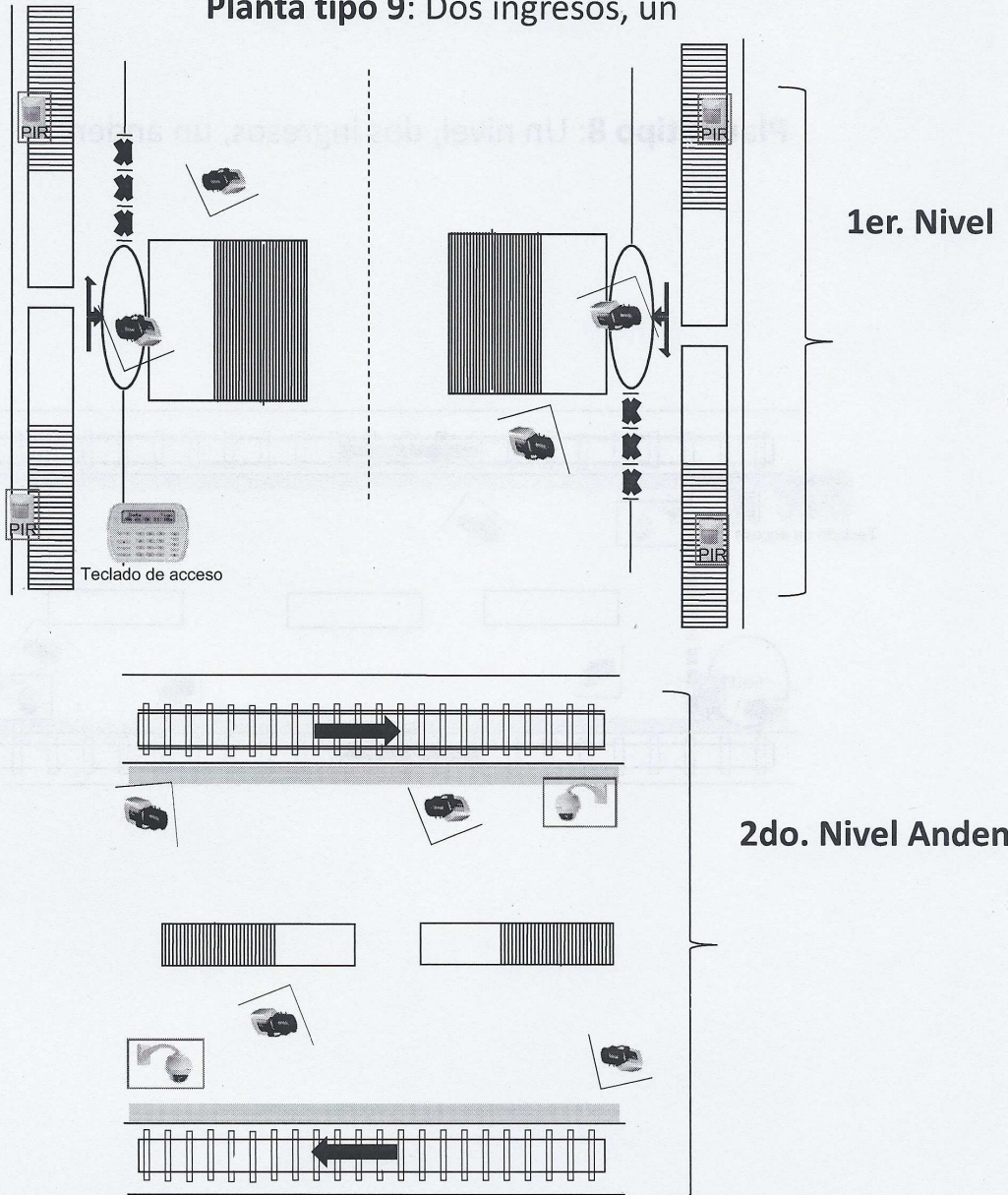
Planta tipo 7: Un nivel, dos ingresos, dos andenes.



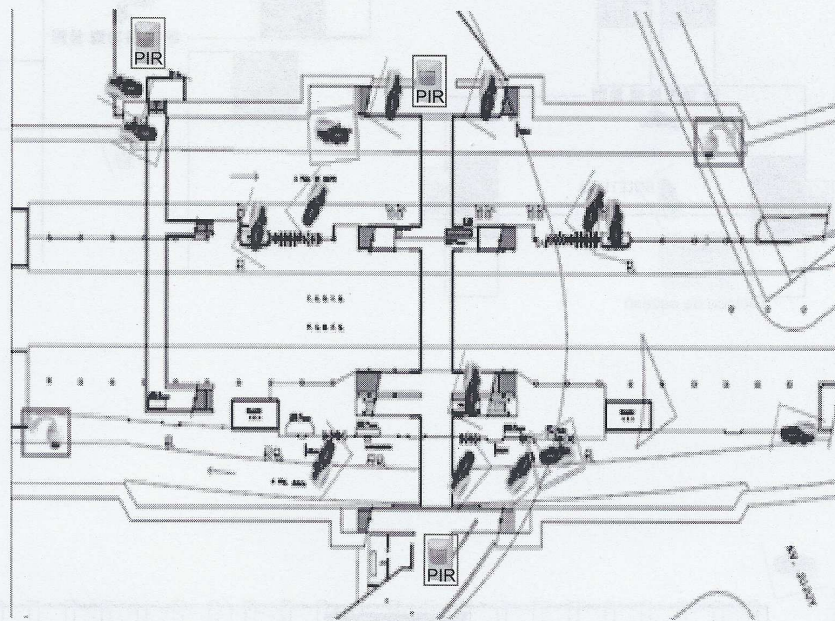
Planta tipo 8: Un nivel, dos ingresos, un andén



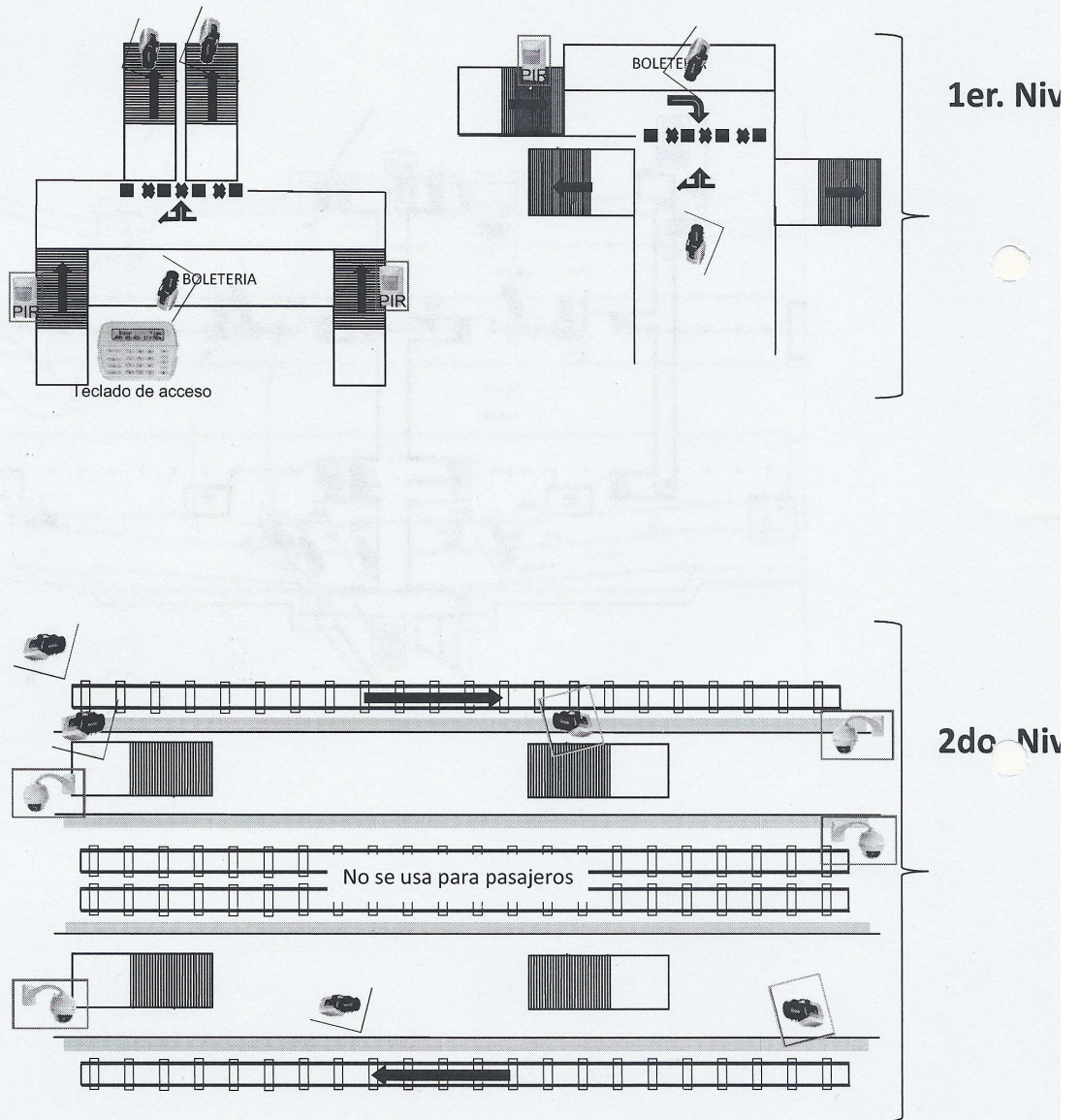
Planta tipo 9: Dos ingresos, un



Planta atípica 1: Un nivel, varios ingresos, dos andenes.

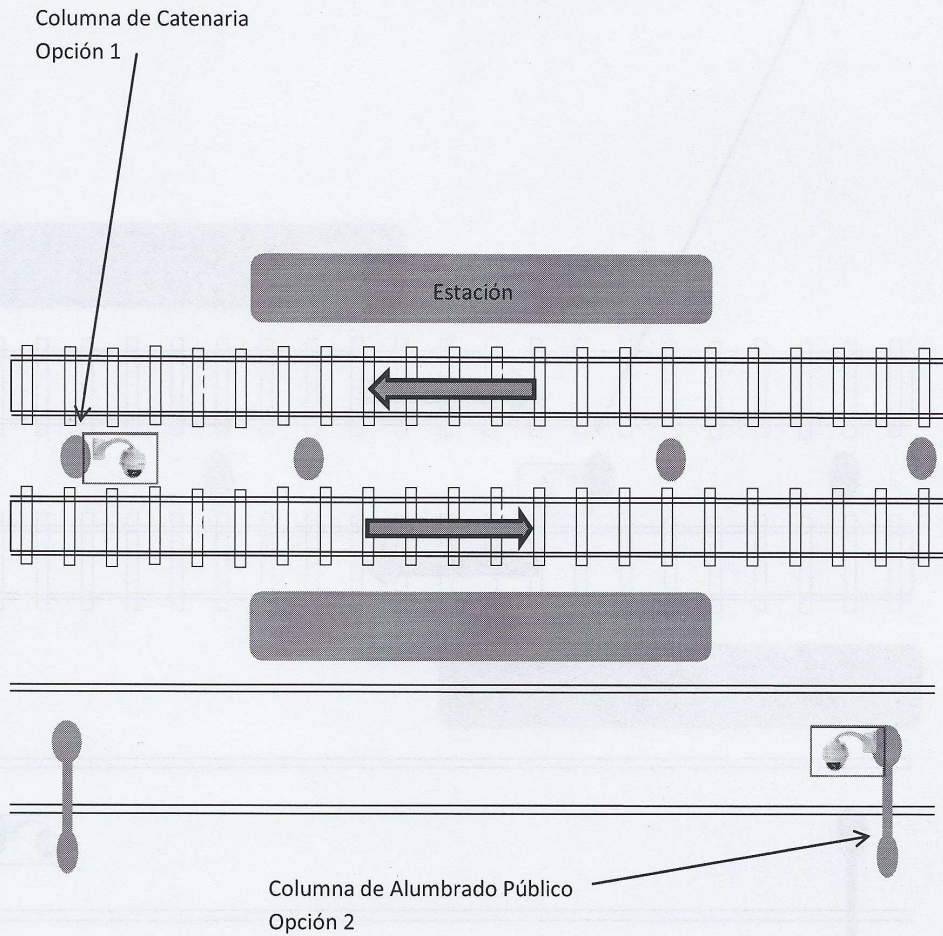


Planta atípica 2: Dos niveles, dos ingresos, dos andenes.

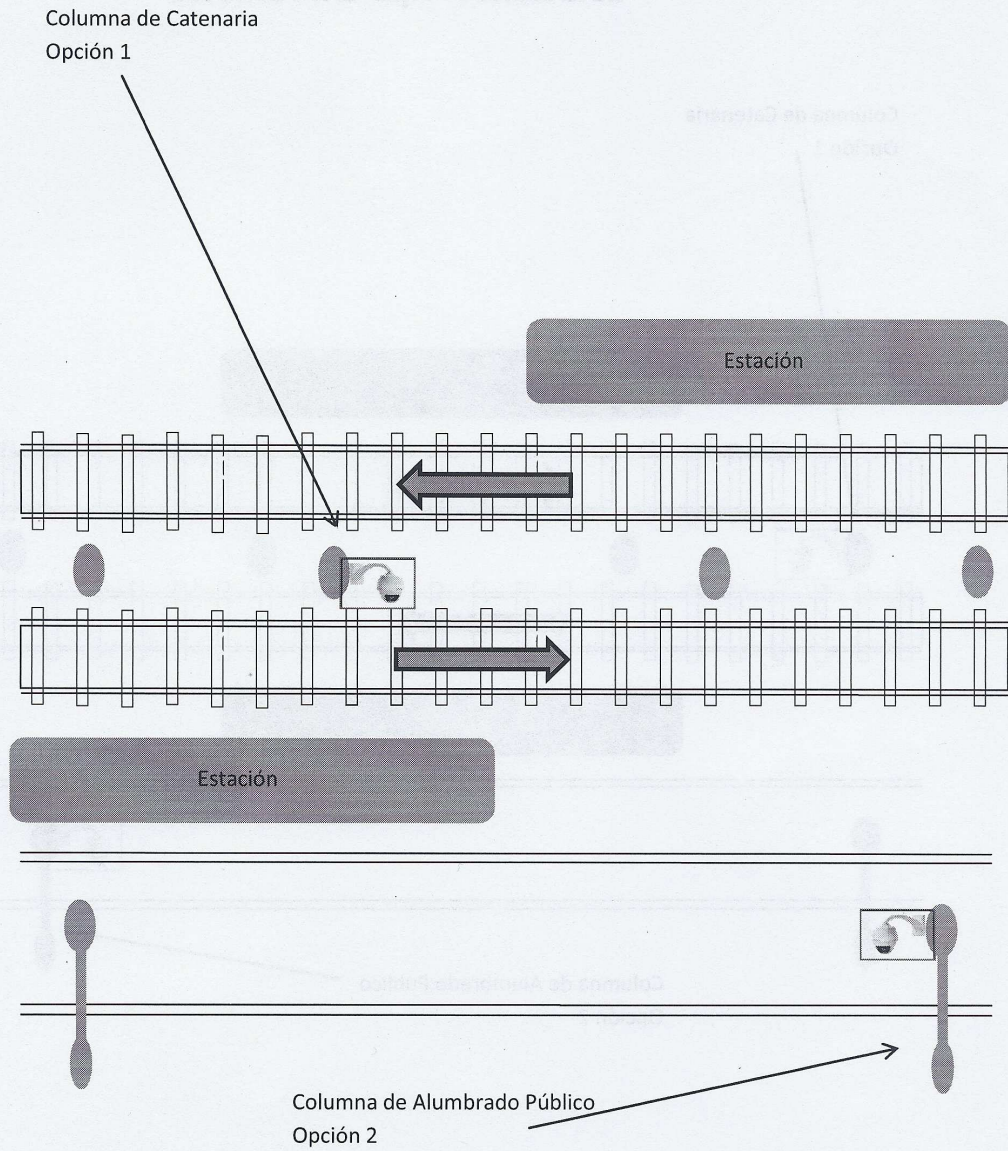


23. ANEXO 4 – Modelo tipo Estaciones Pre Metro para colocación de dispositivos de captura de imagen.

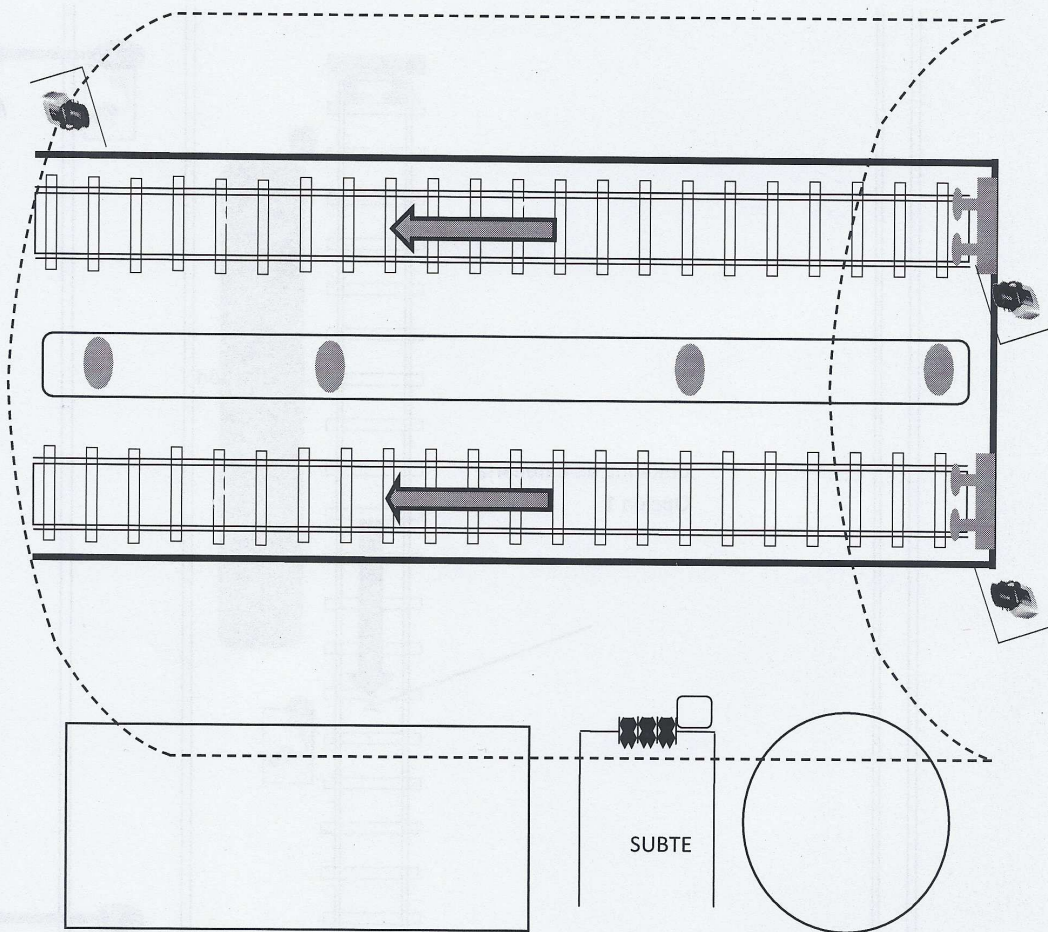
Estaciones Tipo 1 :Premetro



Estaciones Tipo 2: Premetro



Estación Terminal Tipo 1: Premetro



Estación Terminal Tipo 2: Premetro

