SEGOB
SECRETARÍA DE GOBERNACIÓN

SECRETARIADO EJECUTIVO
DEL SISTEMA NACIONAL
DE SEGURIDAD PÚBLICA

Anexo 1
Manual Técnico

para homologar características, tecnología, infraestructura y sistemas de los Centros de Control, Comando, Cómputo y Comunicaciones a nivel nacional

CONTENIDO

0 INTRODUCCIÓN

Las normas técnicas cumplen una función primordial para la política de seguridad pública porque contribuyen a que los proyectos tecnológicos sean construidos bajo un fundamento técnico sólido, garantizando su eficacia y sostenibilidad, apoyando así al uso racional de los fondos y subsidios que el Gobierno de la República destina a su financiamiento y sentando las bases para los procesos de certificación y mejora continua.

El Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP) es la instancia encargada de establecer normas y lineamientos técnicos orientados a homologar la operación y fortalecer las instituciones de seguridad pública y justicia en los tres órdenes de gobierno.

En cumplimiento de esta función, a través del Centro Nacional de Información (CNI), el SESNSP ha elaborado un conjunto de normas para estandarizar la tecnología empleada en la seguridad pública, con la finalidad de establecer parámetros técnicos que sirvan de base para la definición de proyectos en las instancias del Sistema Nacional de Seguridad Pública.

La más reciente, es la Norma para homologar características, tecnología, infraestructura y sistemas de los Centros de Control, Comando, Cómputo y Comunicaciones (conocidos como C4 o C5 cuando se incorpora en su nombre un quinto elemento de “Coordinación” por ejemplo). Dicho instrumento forma parte de un conjunto de normas que en los últimos tres años el SESNSP ha desarrollado para fortalecer la operación de las instituciones de seguridad pública en materia de centros de atención de llamadas de emergencia, sistemas de videovigilancia, así como la presente dedicada a los complejos de seguridad, término acuñado durante su elaboración para facilitar su manejo conceptual.

Con este nuevo instrumento se completa el paquete de normas que el CNI desarrolló para establecer un referente técnico en los programas de prioridad nacional de su competencia.

En este caso, la norma establece requerimientos técnicos mínimos para conseguir la interconexión de los complejos de seguridad, el suministro e intercambio seguro de información para apoyar las tareas de reacción e inteligencia, la integración de tecnologías emergentes a los procesos y servicios sustantivos de los complejos, así como nuevos sistemas de seguridad ciudadana susceptibles de integrarse a los sistemas estatales a través de los complejos, entro otros temas.

En ese sentido, esta norma plantea un nuevo paradigma para el uso de la información de seguridad pública, estableciendo esquemas de intercambio que requieren que los complejos compartan tecnología y procesos para potenciar sus capacidades y, con ello, garantizar mejores resultados.

El Consejo Nacional de Seguridad Pública, en su Cuadragésima Tercera Sesión Ordinaria, aprobó la norma e instruyó al SESNSP a realizar las gestiones necesarias para que se convierta en una Norma Oficial Mexicana (NOM) y a diseñar el modelo y marco institucional para que los complejos de seguridad lleven a cabo la certificación de su cumplimiento.

En forma previa a su publicación, la norma ha sido socializada y comentada por los responsables técnicos de los complejos de seguridad a nivel nacional, de quienes se recibieron aportaciones que fueron analizadas e incorporadas al instrumento.

El presente documento es el Manual técnico de la norma, el cual sirve como referencia para la elaboración de proyectos de nuevos complejos o bien para mejorar los existentes, fortaleciendo sus capacidades tecnológicas, con miras a lograr su interconexión en una red nacional para el intercambio de información, bajo un nuevo paradigma que permita poner al alcance de las instituciones, en forma oportuna y

segura, la información necesaria para apoyar su desempeño en beneficio de la ciudadanía.

Este documento forma parte de una trilogía compuesta por la Norma técnica, el Manual de Gestión y el presente Manual Técnico, los cuales están en proceso de ser dictaminados por la Dirección General de Normas (DGN) de la Secretaría de Economía para conformar una NOM.

El Proyecto de NOM presentado por el SESNSP establece los requisitos y las directrices para gestionar la operación de los complejos de seguridad, incluyendo la planeación estratégica, la gestión de recursos, la gestión de la operación, la gestión técnica y el análisis y mejora. Dicho proyecto fue incluido en el Programa Nacional de Normalización 2018 que expide la Secretaría de Economía, a través de la Dirección General de Normas (DGN) y que fue publicado en el Diario Oficial de la Federación el 12 de marzo de 2018.

La transformación en una NOM permitirá llevar a cabo los procesos de certificación de los complejos con base en la Ley Federal de Metrología y Normalización, lo cual tendrá un impacto positivo en el mercado de tecnología al establecer, con su publicación, requisitos y parámetros mínimos de cumplimiento obligatorio para los proveedores de tecnología de los complejos de seguridad, quienes a su vez habrán de procurar la calidad de los bienes y servicios contratados.

En tanto que ese proceso concluye ante la DGN, el SESNSP pone a disposición el presente anexo técnico para su consulta, con la finalidad de apoyar la definición e implementación de los proyectos tecnológicos que involucran a los complejos de seguridad en México.

Nota metodológica.

Este Manual se relaciona con las necesidades técnicas en el ámbito de las telecomunicaciones y de la información electrónica para los Complejos de Seguridad

(CS) que se encuentran en las diferentes entidades de la República Mexicana. Se cuida el vocablo y términos apegándose a los que se usan en normas internacionales y nacionales para evitar confusiones en el contexto. Se ha dividido este documento en capítulos; la estructura y redacción siguen las recomendaciones de la norma NMX-Z-013-SCFI-2015.Este documento es de orden superior en relación con las Normas ya existentes, es decir, Norma Técnica para Estandarizar las Características Técnicas y de Interoperabilidad de los Sistemas de Video Vigilancia para la Seguridad Pública y la Norma Técnica para la Estandarización de los Servicios de Llamadas de Emergencia a través del Número Único Armonizado 9-1-1 (Nueve, Uno, Uno); existen algunas modificaciones sobre la mismas que aparecen aquí y por tanto deben ser atendidas.

Con base en el diagrama a bloques mostrado en la figura 1, se definen los alcances de este Manual; se contemplan las partes técnicas más importantes que existen o pudieran existir en los Complejos de Seguridad (CS). El alcance del Manual es el desarrollo de los bloques de color gris, el bloque con puntos es un bloque nuevo que se considera necesario crear. Aunque los bloques con líneas diagonales están presentes en los CS no son parte de los mencionados alcances.

1 OBJETIVO Y CAMPO DE APLICACIÓN

1.1 Objetivo

El objetivo de este manual es establecer las especificaciones y los lineamientos de carácter técnico en el ámbito de los sistemas de telecomunicaciones, servidores, dispositivos de almacenamiento y bases de datos que deben satisfacer las instalaciones de todo Complejo de Seguridad, para proveer sus servicios a la población y a las entidades de gobierno con las que se vincula.

1.2 Campo de aplicación

Este manual aplica a los Complejos de Seguridad, conocidos como C4 y C5, en los aspectos técnicos necesarios para ofrecer principalmente a la población los servicios de:

1. Procesamiento y distribución de la información necesaria para la atención de un incidente de emergencia en materia de seguridad, protección civil y salud.
2. Denuncia anónima 089.
3. Monitoreo de la Seguridad Pública a través de los Sistemas de Video Vigilancia.
4. Gestión de infraestructura en telecomunicaciones (voz, datos y radiocomunicaciones).
5. Gestión de bases de datos.
6. Monitoreo de redes y análisis delictivo.

Este manual no aplica a Complejos de Seguridad diferentes de los C4 y C5, como son las corporaciones policiacas, de auxilio vial, protección civil, de bomberos, entre otras.

2 REFERENCIAS NORMATIVAS

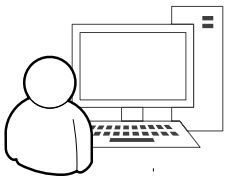
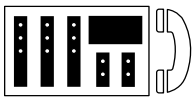
1. NOM-001-SEDE 250-32:2012 Puesta a Tierra y Unión – Edificios o estructuras alimentadas por alimentadores o por circuitos derivados (NOM-001-SEDE: 2012, MOD).
2. NOM-001-SEDE 250-43:1999 Puesta a Tierra - Equipo fijo o conectado de forma permanente (NOM-001-SEDE 250-43:1999, MOD).
3. NOM-001-SEDE 250-44:1999 Puesta a Tierra - Equipo no-eléctrico. (NOM-001-SEDE 250-44:1999, MOD).
4. NOM-001-SEDE 770-49:1999 Cables de Fibra Óptica y sus Canalizaciones - Cables en el interior de edificios- Resistencia al fuego de cables de fibra óptica. (NOM-001-SEDE 770-49:1999, MOD).
5. NOM-001-SEDE 770-50:1999 Cables de Fibra Óptica y sus Canalizaciones - Cables en el interior de edificios - Aprobación, marcado e instalación de cables de fibra óptica. (NOM-001-SEDE 770-50:1999, MOD).
6. NOM-001-SEDE 770-51:1999 Cables de Fibra Óptica y sus Canalizaciones - Cables en el interior de edificios - Requerimientos de aprobación para cables de fibra óptica y sus canalizaciones. (NOM-001-SEDE 770-50:1999, MOD).
7. NOM-001-SEDE 770-53:1999 Cables de Fibra Óptica y sus Canalizaciones - Cables en el interior de edificios - Aplicaciones de los cables de fibra óptica y sus canalizaciones. (NOM-001-SEDE 770-53:1999, MOD).
8. NOM-001-SEDE 800-49:1999 Sistemas de comunicación –Circuitos de comunicación- Resistencia al fuego de cables y alambres de comunicación. (NOM-001-SEDE 800-49:1999, MOD).
9. NOM-001-SEDE 800-50:1999 Sistemas de comunicación –Circuitos de comunicación–Métodos de puesta a tierra (NOM-001-SEDE 800-50:1999, MOD).
10. NOM-001-SEDE 800-50:2012Sistemas de comunicación –Circuitos de comunicación– Circuitos que necesitan protectores primarios (NOM-001-SEDE 800-50:2012, MOD).
11. NOM-001-SEDE 800-51:1999 Sistemas de comunicación –Circuitos de comunicación– Requerimientos de aprobación. (NOM-001-SEDE 800-51:1999, MOD).
12. NOM-001-SEDE 800-52:1999 Sistemas de comunicación –Circuitos de comunicación– Instalación de cables, alambres y equipos de comunicación. (NOM-001-SEDE 800-51:1999, MOD).
13. NOM-227-SCFI-2017, Estandarización de los Servicios de Llamadas de Emergencia a través del Número Único Armonizado 9-1-1 (Nueve, Uno, Uno).

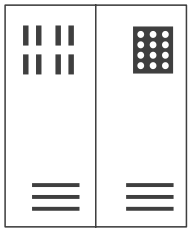
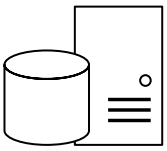
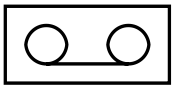
Tabla 2.1 Tabla de concordancia

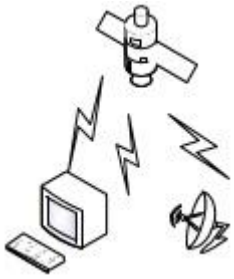
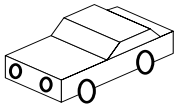
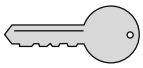
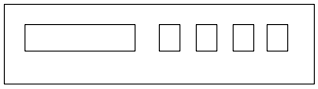
Norma Internacional	Norma Mexicana	Concordancia
ANSI/EIA/TIA 568-B.1:2001Cableado horizontal. (ANSI/EIA/TIA 568-B.1:2001. MOD).	Norma Técnica Para Homologar Características, Tecnología, Infraestructura Y Sistemas De Los Centros De Control, Comando, Cómputo Y Comunicaciones A Nivel Nacional, Que Permita Definir Un Estándar Mínimo Estructural Para La Interconexión Entre Los Centros A Cargo De Los Beneficiarios Del Subsidio Para El Fortalecimiento Del Desempeño En Materia De Seguridad Pública A Los Municipios Y Demarcaciones Territoriales De La Ciudad De México Y En Su Caso, A Las Entidades Federativas Que Ejerzan De Manera Directa O Coordinada La Función De Seguridad Pública En El Ámbito Municipal (Fortaseg) Y Los Estatales Y Federales	MOD
ANSI/EIA/TIA 568-B.1:2001 Cableado de *backbone*. (ANSI/EIA/TIA 568-B.1:2001).		MOD
ANSI/EIA/TIA 568-B.1:2001 Área de trabajo. (ANSI/EIA/TIA 568-B.1:2001).		MOD
ANSI/EIA/TIA 568-B.2:2001 Cableado Horizontal. (ANSI/EIA/TIA 568-B.2:2001).		MOD
ANSI/EIA/TIA 568-B.2:2001 Cables de par trenzado balanceados - Transmisión. (ANSI/EIA/TIA 568-B.2:2001).		MOD
ANSI/EIA/TIA 568-B.2:2001 Cables de par trenzado balanceados - Diafonía en el extremo cercano. (ANSI/EIA/TIA 568-B.2:2001).		IDT
ANSI/EIA/TIA 568-B.2:2001 Cables de par trenzado balanceados – Potencia de diafonía en el extremo cercano. (ANSI/EIA/TIA 568-B.2:2001).	Norma Técnica Para Homologar Características, Tecnología, Infraestructura Y Sistemas De Los Centros De Control, Comando, Cómputo Y Comunicaciones A Nivel Nacional, Que Permita Definir Un Estándar Mínimo Estructural Para La Interconexión Entre Los Centros A Cargo De Los Beneficiarios Del Subsidio Para El Fortalecimiento Del Desempeño En Materia De Seguridad Pública A Los Municipios Y Demarcaciones Territoriales De La Ciudad De México Y En Su Caso, A Las Entidades Federativas Que Ejerzan De Manera Directa O Coordinada La Función De Seguridad Pública En El Ámbito	IDT
ANSI/EIA/TIA 568-B.2:2001 Cables de par trenzado balanceados – Balance de diafonía en el extremo lejano (ANSI/EIA/TIA 568-B.2:2001).		IDT
ANSI/EIA/TIA 568-B.2:2001 Cables de par trenzado balanceados - Potencia de diafonía en el extremo lejano (ANSI/EIA/TIA 568-B.2:2001).		IDT
ANSI/EIA/TIA 568-B.2:2001 Cables de par trenzado		MOD

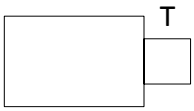
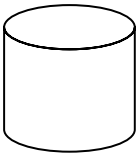
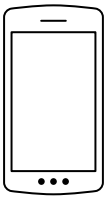
Norma Internacional	Norma Mexicana	Concordancia
balanceados - Mecánico (ANSI/EIA/TIA 568-B.2:2001).	Municipal (Fortaseg) Y Los Estatales Y Federales	
ANSI/EIA/TIA 568-B.2:2001 Cables de par trenzado balanceados –Pérdida en el extremo cercano. (ANSI/EIA/TIA 568-B.2:200).	Norma Técnica Para Homologar Características, Tecnología, Infraestructura Y Sistemas De Los Centros De Control, Comando, Cómputo Y Comunicaciones A Nivel Nacional, Que Permita Definir Un Estándar Mínimo Estructural Para La Interconexión Entre Los Centros A Cargo De Los Beneficiarios Del Subsidio Para El Fortalecimiento Del Desempeño En Materia De Seguridad Pública A Los Municipios Y Demarcaciones Territoriales De La Ciudad De México Y En Su Caso, A Las Entidades Federativas Que Ejerzan De Manera Directa O Coordinada La Función De Seguridad Pública En El Ámbito Municipal (Fortaseg) Y Los Estatales Y Federales	IDT
ANSI/EIA/TIA 568-B.2:2001 Cables de par trenzado balanceados - PSNEXT loss. (ANSI/EIA/TIA 568-B.2:2001).		IDT
ANSI/EIA/TIA 568-B.2:2001 Cables de par trenzado balanceados - ELFEXT. (ANSI/EIA/TIA 568-B.2:2001).		IDT
ANSI/EIA/TIA 568-B.2:2001 Cables de par trenzado balanceados - PSELFEXT. (ANSI/EIA/TIA 568-B.2:2001).		IDT
ANSI/EIA/TIA 568-B.3:2000 *Optical fibre cables*. (ANSI/EIA/TIA 568-B.3:2000).		MOD
ANSI/EIA/TIA 568-B.2:2001 *Balanced twisted pair cables* - Transmission. (ANSI/EIA/TIA 568-B.2:2001).		MOD

2.2 Simbología

	**Monitorista**
	**Despachador**
	**Operador telefónico del 9-1-1/089**
	**Conmutador**
	**Estación base**

	**Sitio Maestro**
	**Servidor de Almacenamiento**
	**Grabadora**
	**Radio**

	**Posicionamiento**
	**Patrullas**
	**Dispositivos de banda ancha**
	**Cifrado**
	**Enrutador**
	**Controlador de Videowall (NVR)**

	**Cámara**
	**Videowall**
	**Base de Datos**
	**Teléfono Inteligente**
	**Botón de Emergencias**

	**Sensores**
	**Punto de Acceso**

3 TÉRMINOS Y DEFINICIONES

3.1 Abonado

Persona asociada a una terminal del sistema, que tiene acceso a todos o parte de los servicios ofrecidos por la red.

3.2 ACD, por sus siglas en inglés

Distribuidor Automático de Llamada, (*Automatic Call Distributor*).

3.3 Acuerdo de Nivel Operacional

(OLA por sus siglas en inglés: *Operational Level Agreement*), acuerdo entre un proveedor de servicios TI y otra parte de la misma organización; gobierna la prestación de un servicio de apoyo.

3.4 Acuerdos de los Niveles de Servicio

(SLA por sus siglas en inglés *Service Level Agreement*), es un contrato que describe el nivel de servicio que un cliente espera de su proveedor.

3.5 Administrador de base de datos

Es el profesional con perfil técnico que recibe las especificaciones del equipo de Análisis y Diseño para su implementación en un Sistema de Gestión de Base de Datos, como por ejemplo Oracle, SQL, Server, DB2, entre otros.

3.6 Afectación

Es sinónimo de falla en el servicio.

3.7 Altimetría

Parte de la topografía que se ocupa de la medición de alturas.

3.8 Android

Sistema operativo para dispositivos móviles.

3.9 ANI, por sus siglas en inglés

Identificación automática de número, (*Automatic Number Identification)*.

3.10 API, por sus siglas en inglés

Interfaz de programación de aplicaciones, *(Application Programming Interface).*

3.11 Aplicación Cliente

Aplicación usada por un usuario en equipo de cómputo para consultar datos que normalmente proporciona una aplicación tipo servidor.

3.12 Aplicación Servidor

Aplicación en red que provee de información a las peticiones que hace una aplicación cliente.

3.13 APP, por sus siglas en inglés

Aplicación, (*Application*).

3.14 ATM. por sus siglas en inglés

Modo de Transferencia, (*Asynchronous Transfer Mode*). Modo de Transferencia. Modo de transmisión en el que la información está organizada en celdas; es asíncrono en el sentido de que la recurrencia de las células de un usuario individual no es necesariamente periódica.

3.15 Autenticación PAP

Autenticación a través del Protocolo de Contraseña, (Password Authentication Protocol).

3.16 AVL, por sus siglas en inglés

Localización Automática de Vehículos, (*Automatic Vehicle Location).*

3.17 AWG, por sus siglas en inglés

Calibre de alambre estadounidense, (*Arrayed Waveguide Grating).*

3.18 *Backplane*

Tarjeta pasiva que interconecta las tarjetas que se le puedan insertar a un chasis de un equipo de comunicaciones.

3.19 Base de datos

Conjunto de datos estructurados y definidos a través de un proceso específico, que busca evitar la redundancia, y que se almacena en algún medio de almacenamiento masivo, como un disco.

3.20 Bastidor

Soporte metálico usado para montar equipos de telecomunicaciones en los cuartos de telecomunicaciones. Comercialmente existen de 88 cm y 2.04 cm de alto, y 58 cm aproximadamente de ancho.

3.21 BCE

Bastidor de Cableado de Edificio.

3.22 BCP

Bastidor de Cables de Piso.

3.23 BD, por sus siglas en inglés

Base de Datos (Data Base).

3.24 BGP, por sus siglas en inglés

Protocolo de Borde de Puerta de Enlace, *(Border Gateway Protocol).*

3.25 CAD, por sus siglas en inglés

Despacho Asistido por Computadora, (*Computer Aided Dispatch*).

3.26 CALLE

Centro de Atención de Llamadas de Emergencia.

3.27 Cámara PTZ

3.28 Cámara que hace paneo o movimientos horizontales, inclinaciones verticales y acercamientos.

3.29 Canal de control

Canal radio usado para la transmisión de la señalización y de los datos.

3.30 Canal de tráfico

Canal radio usado para la transmisión de la voz y de datos.

3.31 Canal

Porción especificada del espectro radioeléctrico que transporta una señal radiofrecuencia específica.

3.32 Canaletas

La canaleta es un ducto diseñado para alojar cables de telecomunicaciones y proporcionarles una mayor protección en contra de perturbaciones, que generalmente se instala en las áreas de trabajo.

3.33 Canalización horizontal

El esquema de canalización horizontal especifica las facilidades proporcionadas para la instalación de cables de red hacia los cuartos de telecomunicaciones, y proporciona los espacios, rutas, así como los soportes necesarios para los cables de telecomunicaciones que parten desde el bastidor de piso (BCP) hasta las salidas de telecomunicaciones instaladas dentro de las áreas de trabajo.

3.34 Canalización

Sistema de tuberías que permite la protección y conducción de cableado eléctrico y de telecomunicaciones que pueden estar fabricadas de compuestos de metal, fibra de vidrio o materiales plásticos rígidos o con un grado de flexibilidad.

3.35 CCTV, por sus siglas en inglés

Circuito Cerrado de Televisión (*Closed Circuit Television).*

3.36 Central Telefónica

Equipo de primer contacto y principal plataforma de operación del Centro de Atención de Llamadas de Emergencia (CALLE) a través del número único armonizado 9-1-1 (Nueve-Uno-Uno), que debe estar integrado por los siguientes dispositivos: conmutador, *Gateway* y módulos de integración.

3.37 CHAP, por sus siglas en inglés

Protocolo de autenticación por desafío mutuo. (*Challenge Handshake Authentication Protocol).*

3.38 CNI

Centro Nacional de Información.

3.39 Cobertura

Área que cubren las transmisiones de un teléfono, una célula de radio o la señal de un radar.

3.40 Compatibilidad

Grado de transparencia suficiente para soportar una calidad de servicio aceptable en la conexión entre entidades de sistemas. La plena compatibilidad implica la transparencia total.

3.41 Componente

Elemento de un sistema capaz de operar independientemente, pero diseñado, construido y operado como parte integral del mismo.

3.42 Conexiones concurrentes

Varios usuarios o conexiones TCP/IP conectados al mismo tiempo sobre un aplicativo o sistema operativo.

3.43 Conexiones simultáneas

Varios usuarios o conexiones TCP/IP conectados en diferente tiempo sobre un aplicativo o sistema operativo.

3.44 Confidencialidad.

Propiedad por la que la información no está disponible y no es revelada a individuos, entidades o procesos sin autorización.

3.45 Conmutador de datos

Equipo de comunicaciones de capa 2 del modelo OSI. Si este equipo es el que interconecta a todos los demás como nodo raíz en una topología estrella, se le conoce como Conmutador de Datos Principal.

3.46 *Conmute*

Cambiar una cosa o por otra.

3.47 Construcción de Servicios *Web*

(WSDL por sus siglas en inglés *Web Services Description Language*), es el lenguaje usado para la definición de los *Web Services*, WSDL es un lenguaje basado en XML y que tiene una especificación dentro de los estándares de W3C, el documento de definición del WSDL es "*Web Services Description Language* (WSDL) Versión 1.1" o superior.

3.48 Control de Acceso al Sistema

Metodología por la cual un radio subscriptor solicita servicios de un sistema troncalizado y les son otorgados o denegados tales servicios.

3.49 Convencional

Sistema de Radio que permite a los subscriptores de radio controlar ellos mismos el acceso a los canales de radiofrecuencia.

3.50 Coordenadas Geográficas

Sistema de coordenadas que permite que cada ubicación en la Tierra sea especificada por un conjunto de números, letras o símbolos.

3.51 Coordenadas UTM

Es un sistema basado en la proyección cartográfica de Mercator, sus unidades son los metros a nivel del mar, que es la base del sistema de referencia.

3.52 Coordenadas WGS 84

Es un sistema de coordenadas geográficas mundial que permite localizar cualquier punto de la Tierra por medio de tres unidades dadas. WGS84 son las siglas en inglés de *World Geodetic System 84* (Sistema Geodésico Mundial 1984).

3.53 Cortafuegos (*Firewall*)

Programa informático que controla el acceso de una computadora a la red y de elementos de la red a la computadora, por motivos de seguridad.

***3.54* CPU, por sus siglas en inglés**

Unidad de procesamiento central (*Central Processing Unit).*

3.55 CRM, por sus siglas en inglés

Gestión de las relaciones con clientes *(Customer Relationship Management).*

3.56 CS

Complejo de Seguridad.

3.57 CT

Cuarto de Telecomunicaciones.

3.58 DAS, por sus siglas en inglés

Almacenamiento de conexión directa, *Direct Attached Storage* (DAS), es el método tradicional de almacenamiento y el más sencillo.

3.59 Datos personales

Información concerniente a una persona física identificada o identificable, que puede estar expresada en forma numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo.

3.60 DCE, por sus siglas en inglés

Equipo de Comunicaciones de Datos (*Data Communications Equipment).*

3.61 DHCP, por sus siglas en inglés

Protocolo de control de configuración de host dinámico. (*Dynamic Host Configuration Protocol*).

3.62 Direcciones MAC

Direcciones definidas por la capa 2 del modelo OSI que se usan principalmente para identificar a la tarjeta de red de equipos de cómputo.

3.63 Disponibilidad

Indica el tiempo, expresado en términos porcentuales, en el que el sistema está en operación, en un determinado intervalo de evaluación.

$$\frac{HMD - HIP - HINP}{HMD - HIP} x100\%$$

Donde:

HMD = Tiempo, en horas o minutos, máximo disponible en

el período acordado de medición.

HIP = Tiempo, en horas o minutos, con interrupción programada del servicio para actualizar, dar mantenimiento, o cualquier otro evento requerido para mantener el sistema en condiciones óptimas de funcionamiento.

HINP = Tiempo, en horas o minutos, con interrupciones no programadas del servicio, relacionados con fallas en algún componente que impide el otorgamiento del servicio.

3.64 Distribuidor Automático de Llamada

Dispositivo capaz de distribuir las llamadas entrantes a un cierto grupo de terminales.

3.65 DMZ, por sus siglas en inglés

Zona desmilitarizada (*Demilitarized Zone).*

3.66 DNS, por sus siglas en inglés

Sistema de Nombres de Dominio (Domain Name System).

3.67 DNIS, por sus siglas en inglés

Servicio de Identificación de Números Marcados. (*Dialed Number Identification Service*).Servicio de Identificación de Números Marcados. Esta característica se utiliza en un centro de llamadas que tiene varios números de teléfono, para distinguir el número específico al que llamó el llamante.

3.68 Dominio

Conjunto de valores que integran una base de datos.

3.69 *Down-Hole*

El método *Down-Hole* consiste en generar ondas sísmicas en la superficie, mediantes golpes verticales y horizontales en una placa ubicada a una

distancia de 1 a 3 metros aprox., registrándose los tiempos de llegada de las ondas de compresión y cizalle.

3.70 DRP, por sus siglas en inglés

Plan de Recuperación ante Desastres (*Disaster Recovery Plan).*

3.71 DSCP, por sus siglas en inglés

Punto de código de servicios diferenciados. (*Differentiated Services Code Point).*

3.72 DTE, por sus siglas en inglés

Equipo de Terminación de Datos (*Data Terminal Equipment).*

***3.73* DVMRP, por sus siglas en inglés**

Protocolo de Ruteo Multicast de Vector de Distancia. *(Distance Vector Multicast Routing Protocol).*

3.74 EF

Entrada de Facilidades.

3.75 EMI, por sus siglas en inglés

Interferencia Electromagnética (*Electromagnetic Interference).*

3.76 Enrutador

Equipo de telecomunicaciones que realiza la función de dirigir los paquetes IP a su destino a través de redes IP.

3.77 Equipo de comunicaciones

Transmisores y receptores de datos de tipo digital o analógico para sistemas de redes de área local o redes de área amplia, diseñados para la interconexión con la red pública.

3.78 Escalabilidad horizontal

Varios servidores (conocidos como Nodos) trabajando como un todo, con facilidad de agregar más nodos.

3.79 Escalabilidad vertical

Escalabilidad vertical o hacia arriba, siendo la más simple, pues significa crecer el *hardware* de uno de los nodos.

3.80 Escalerilla

Es una estructura rígida mecánica usada para el transporte de cable en el cableado estructurado. Sus bandejas están formadas por peldaños y son usadas normalmente en techos.

3.81 Espectro radioeléctrico

Porción del espectro electromagnético en el que es posible la propagación de ondas electromagnéticas sin guía artificial, cuyas bandas de frecuencia se fijan convencionalmente por debajo de los 3000 GHz.

3.82 Esquema XML

XML *Schema*. Describe la estructura de un documento XML.

3.83 Estándar

Que es el más común o el más usual; que está ampliamente extendido, por lo que constituye un modelo o una norma.

3.84 Estándares. Documentos que contienen las especificaciones y procedimientos destinados a la generación de productos, servicios y sistemas confiables. Estos establecen un lenguaje común, el cual define los criterios de calidad y seguridad, son documentos prácticos que fijan metas alcanzables, son sujetos a revisión constante para permitir el avance conforme a las tecnologías. Los estándares pueden incluir referencia a otros estándares internacionales, códigos, especificaciones o manuales, entre otros.

3.85 Estudios Geofísicos

Técnicas desarrolladas a partir de métodos físicos que ayudan a revelar la presencia o ausencia de cuerpos y estructuras dentro del subsuelo que no pueden verse a simple vista.

3.86 Estudios Geológicos

Características geológicas del terreno afectado por la construcción, distinguiendo entre el terreno como cimiento de la vía y sus estructuras y

el terreno como material a emplear en la construcción, así como información sobre las condiciones hidrológicas y de drenaje.

3.87 Extraer, transformar y cargar

(ETL por sus siglas en inglés *Extract, Transform and Load*), organizar datos de múltiples fuentes.

3.88 Falla en el Servicio

Significa que un componente de la plataforma tecnológica para la interoperabilidad no cumple con los Estándares de Servicios y/o de Disponibilidad.

3.89 *FastEthernet*

Tecnología de la familia *Ethernet* para redes de área local de capa 2 del modelo OSI. Usada en cables UTP categoría 5, fibra óptica y conmutadores de datos de dicha tecnología para conectar los equipos de red en la red de área local.

3.90 FC-AL, por sus siglas en inglés

Protocolo *Fibre Channel Arbitrated Loop*, usado en *hubs* SAN.

3.91 FCoE, por sus siglas en inglés

Es una tecnología de red de computadoras que encapsula las tramas de canal de fibra a través de redes *Ethernet*.

3.92 FC-SW, por sus siglas en inglés

Protocolo *Fibre Channel Switched*, usado en *switches*, en este caso varias comunicaciones pueden ocurrir simultáneamente.

3.93 FEXT, por sus siglas en inglés

Ruido Extremo Lejano (*Far End Crosstalk).*

3.94 FHD, por sus siglas en inglés

Alta definición plena. Imagen en formato 16:9 o 9:16, 1080p, 30 fps (*Full High Definition).*

3.95 *Fibre channel*

El canal de fibra (del inglés *fibre channel*) es una tecnología de red utilizada principalmente para redes de almacenamiento.

3.96 FPS, por sus siglas en inglés}

Tramas por segundo *(Frames Per Second).*

3.97 FTP, por sus siglas en inglés

Protocolo de transferencia de Archivos. (*File Transfer Protocol*).

3.98 FW, por sus siglas en inglés

Cortafuegos (*Firmware).*

3.99 G.711

Estándar de compresión de audio utilizado para teléfonos digitales. G.711 usa un ancho de banda de 64 Kbps.

3.100 G.723.1

Técnica de compresión que se utiliza para teléfonos digitales. Produce audio digital a 6.4 o 5.3 Kbps.

3.101 G.729

El algoritmo de voz estándar de la ITU-T con una tasa de codificación de la voz a 8 Kbps.

3.102 Gabinete

Armazón que contiene equipos de comunicaciones o equipo de cómputo, tiene un marco exterior y un bastidor interior con una o varias puertas.

3.103 *Gateway*

Puerta de Enlace.

3.104 Geolocalización

Capacidad para obtener la ubicación geográfica real de un objeto.

3.105 Georreferencia

Se refiere a la localización de un objeto espacial (representado mediante punto, vector, área, volumen), en un sistema de coordenadas y *datum* determinado.

3.106 Gestión del Rendimiento

(CPM por sus siglas en inglés *Corporate Performance Management*), herramientas informáticas para gestionar el rendimiento de una empresa basándose en metodologías, métricas, procesos y sistemas necesarios para monitorear.

3.107 *GigaEthernet*

Tecnología de la familia *Ethernet* para redes de área local de capa 2 del modelo OSI. Usada en cables UTP categoría 5e o 6, fibra óptica y conmutadores de datos de dicha tecnología para conectar los equipos de red en la red de área local.

3.108 GIS, por sus siglas en inglés

Sistema de Información Geográfica. (*Geographic Information System*).

3.109 H.264

Codificador/decodificador para video de la ITU.

3.110 H.323

Recomendación ITU-T que se basa en protocolos para la transmisión de voz y video a través de PSTN, ISDN y ATM.

3.111 *Hardware*

Se refiere a los dispositivos físicos que componen una red de datos.

3.112 HC, por sus siglas en inglés

Conexión Cruzada Horizontal (*Horizontal Cross-Connect).*

3.113 HD, por sus siglas en inglés

Alta definición. Imagen en formato 16:9 ó 9:16, 720p, 30 fps *(High Definition).*

3.114 Hot Swap

Tecnología que permite cambiar partes de un equipo de comunicaciones sin necesidad de apagarlo.

3.115 HTTP, por sus siglas en inglés

Protocolo de Transferencia de Hiper Texto (*HyperText Transport Protocol).*

3.116 HTTPS, por sus siglas en inglés

Protocolo de transferencia de hipertexto seguro. (*Hypertext Transport Protocol Secure*).

3.117 Hypervisores

Monitor de máquina virtual que permite aplicar diversas técnicas de control de virtualización para utilizar, al mismo tiempo, diferentes sistemas operativos.

3.118 IAX, por sus siglas en inglés

(*Inter Asterisk Exchange Protocol*). Protocolo utilizado para manejar conexiones VoIP entre servidores Asterisk, y entre servidores y clientes que utilizan el protocolo IAX.

3.119 IAX2, por sus siglas en inglés

(*Inter Asterisk Exchange Protocol* versión 2).

3.120 IC

Conexión Intermedia.

3.121 IDS, por sus siglas en inglés

Sistema Detector de Intrusos (*Intrusion Detection System).*

3.122 IEEE 802.11

El estándar define el uso de los dos niveles inferiores de la arquitectura o modelo OSI (capa física y capa de enlace de datos), especificando las normas de funcionamiento de una red de área local inalámbrica.

3.123 IEEE, por sus siglas en inglés

Instituto de Ingenieros Eléctricos y Electrónicos. (*Institute of Electrical and Electronics Engineers).*

3.124 IFT

Instituto Federal de Telecomunicaciones.

3.125 IGMP, por sus siglas en inglés

Protocolo de administración de grupos de Internet. (*Internet Group Management Protocol*).

3.126 Indicador Clave de Rendimiento

(KPI por sus siglas en inglés *Key Performance Indicator*), medida del nivel del desempeño de un proceso.

3.127 Infiltración No Autorizada a la Plataforma Tecnológica

Acceso registrado en el sistema mediante el cual la información o los componentes del sistema pudieron ser consultados, leídos o copiados por un individuo o sistema que no está autorizado para hacerlo.

3.128 Instancia

Dependencia municipal, estatal o federal con alguna base de datos que comparte información.

3.129 Integridad

Propiedad de la información que se refiere a que dicha información contenida en sistemas para la prestación de servicios digitales permanece completa e inalterada y, en su caso, que sólo ha sido modificada por la fuente de confianza correspondiente.

3.130 Interfaz de intercambio de información

Conjunto de protocolos, estándares y componentes que sirven para intercambiar datos entre sistemas, con independencia del lenguaje de programación o plataforma en la que fueron desarrollados y operan.

3.131 Interfaz

Frontera común entre dos sistemas asociados, en la cual se establecen las características necesarias para que los sistemas se puedan comunicar de una forma particular.

3.132 Interoperabilidad

Sistemas o programas capaces de intercambiar información y operar juntos de manera efectiva.

3.133 IOPS, por sus siglas en inglés

(*Input/Output Operations Per Second*) u Operaciones de entrada/salida por segundo.

3.134 iOS

Sistema operativo desarrollado por la compañía *Apple*.

3.135 IP, por sus siglas en inglés

Protocolo de Internet. (*Internet Protocol*).

3.136 IPS, por sus siglas en inglés

Sistema Preventor de Intrusos (*Intrusion Prevention System*).

3.137 IRC, por sus siglas en inglés

Repetidor de conversaciones por internet (*International Record Carrier*).

3.138 iSCSI

Abreviatura de Internet SCSI, es un estándar que permite el uso del protocolo SCSI sobre redes TCP/IP.

3.139 ISDN, por sus siglas en inglés

Red Digital de Servicios Integrados. (*Integrated Services Digital Network*).Una red digital conmutada que admite la transmisión de voz, datos e imágenes, a través de líneas telefónicas convencionales.

3.140 IS-IS, por sus siglas en inglés

Sistema intermediario a sistema intermediario. *(Intermediate system to intermediate system).*

3.141 ITU-T

Sector de Telecomunicaciones de la Unión Internacional de Telecomunicaciones.

3.142 IVR, por sus siglas en inglés

Interactive Voice Response. Respuesta de Voz Interactiva. (*Interactive Voice Response*).

3.143 Kerberos

Protocolo de autenticación de redes de ordenador.

3.144 KPI, por sus siglas en inglés

Indicador clave o medidor de desempeño (*Key Performance Indicators).*

3.145 LAN, por sus siglas en inglés

Red de Área Local. (*Local Area Network*). Una red de computadoras que abarca un área relativamente pequeña. La mayoría de las LAN están confinadas a un sólo edificio o grupo de edificios. Sin embargo, una LAN puede conectarse a otras LAN a cualquier distancia a través de líneas telefónicas y ondas de radio.

3.146 LED, por sus siglas en inglés

Diodo emisor de luz (*Light Emitting Diode).*

3.147 Legislación de Protección de Datos

Se refiere a la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, y toda otra legislación y reglamentación aplicables relativas al procesamiento de datos personales y privacidad.

3.148 Lenguaje de Ejecución de Proceso de Negocio con Servicios Web

(WS-BPEL por sus siglas en inglés *Web Services Business Process Execution Language Version*), lenguaje estandarizado por OASIS (*Organization for the Advancement of Structured Information Standards*) para la composición de Servicios *Web*.

3.149 LFPDPPP

Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

3.150 LFTAIPG

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

3.151 Llamada en espera

Servicio suplementario o característica de servicio que ofrece la posibilidad de notificar a un usuario móvil la entrada de una llamada mientras la terminación se encuentra ocupada. Posteriormente, el abonado podrá contestar, rechazar o ignorar la llamada entrante.

3.152 Llamada

Utilización, efectiva o posible, de una o varias conexiones establecidas entre dos o más usuarios y/o servicios.

3.153 LOG

Archivo de registros de eventos. Estos registros los genera un dispositivo de red y los guarda en dicho archivo, que puede estar en el mismo dispositivo o en otro.

3.154 Lun, por sus siglas en inglés

(*Logical Unit Number)* una partición virtual (o volumen) dentro de un conjunto RAID.

3.155 m

Metros.

3.156 MAC, por sus siglas en inglés

Control de acceso al medio, (*Medium Access Control).*

3.157 MAN, por sus siglas en inglés

Red de área metropolitana, *(Metropolitan Area Network).*

3.158 MC, por sus siglas en inglés

Cuarto Principal, (*Main Cross-Connect).*

3.159 MDF, por sus siglas en inglés

Servicio de Distribución Principal (Main Distribute Facilite).

3.160 MIB, por sus siglas en inglés

Base de información de administración, (*Management Information Base*).

3.161 mm

Milímetros.

3.162 Modelo OSI

Modelo de referencia para las comunicaciones electrónicas realizado por la organización de normalización ISO.

3.163 MPI, por sus siglas en inglés

Interfaz de Paso de Mensajes (*Message Passing Interface*).

3.164 MSTP, por sus siglas en inglés

Protocolo de *Spanning Tree* Múltiple. *(Multiple Spanning Tree Protocol).*

3.165 MTBF, por sus siglas en inglés

Tiempo medio entre fallos, *(Mean Time Between Failures).*

3.166 MTTF, por sus siglas en inglés

Tiempo medio para un fallo, *(Mean Time to Failure).*

3.167 MTTR, por sus siglas en inglés

Tiempo medio para recuperarse. *(Mean Time to Repair).*

3.168 MTTT, por sus siglas en inglés

Tiempo medio para la transición.

3.169 MUTO

Salida Multiusuario.

3.170 NAS, por sus siglas en inglés

Almacenamiento conectado a la red. (*Network Attached Storage*).

3.171 Negación de Servicio (DOS)

Se produce cuando se genera una gran cantidad de tráfico desde varios puntos de conexión a un sólo destino**.**

3.172 NEXT, por sus siglas en inglés

Ruido Extremo Cercano (*Near End Crosstalk).*

3.173 NOC, por sus siglas en inglés

Centro de Monitoreo de la Red (*Network Operation Center*).

3.174 NOM

Norma Oficial Mexicana.

3.175 Normalización de bases de datos

Técnica eficaz para el diseño de bases de datos, que puede aplicarse tanto a sistemas relacionales como a otros modelos.

3.176 NTP, por sus siglas en inglés

Protocolo de tiempo de red (*Network Time Protocol).*

3.177 NVR, por sus siglas en inglés

Grabador de video en red (*Network Video Recorder).*

3.178 *Offline*

Sin conexión (apagado).

3.179 OLA, por sus siglas en inglés

Acuerdo del Nivel Operacional (Operating Level Agreement).

3.180 *Online*

Con conexión (encendido).

3.181 Orografía

Parte de la geografía física que se encarga del estudio, descripción y representación del relieve terrestre.

3.182 OSPF, por sus siglas en inglés

Primera ruta más corta, abierto. *(Open Shortest Path First).*

3.183 Panel

Placa, moldura, cuadro o compartimiento prefabricado.

3.184 PAP, por sus siglas en inglés

Protocolo de Autenticación de Contraseña. (*Password Authentication Protocol*).

3.185 PBX, por sus siglas en inglés

(*Private Branch Exchange*). Centralita privada de telefonía que se utiliza dentro de una empresa para conectar redes telefónicas públicas y privadas.

3.186 Pérdida de Información

Información que una vez que ha persistido en los sistemas de almacenamiento de la plataforma no pueda ser recuperada inmediatamente, ni restaurada a partir de un respaldo de seguridad de la misma.

3.187 Perfil de Referencias Cruzadas (PRC)

Soporta las referencias cruzadas de los expedientes.

3.188 Petición

Mensaje electrónico de solicitud que hace un sistema cliente a una Plataforma determinada y que debe de ser contestado por ella ya sea en sentido positivo, negativo o con la información solicitada.

3.189 Planimetría

Parte de la topografía que trata la medición y representación de una porción de la superficie terrestre sobre una superficie plana.

3.190 Plataforma Tecnológica para la Integración de Información (PTII)

Sistema para compartir datos del Complejo de Seguridad (CS) en tiempo real, permite el conocimiento y la actualización para brindar un servicio con mayor eficiencia y calidad.

3.191 Plataforma Tecnológica

Conjunto de elementos de *hardware*, *software*, desarrollos, protocolos y telecomunicaciones que operan para la provisión del servicio.

3.192 PMI

3.193 Punto de Monitoreo Inteligente.

3.194 PO

Puesto de Operador.

3.195 POE, por sus siglas en inglés

Corriente eléctrica sobre *Ethernet* (*Power Over Ethernet).*

3.196 Pool

Combinación de varios discos duros en una sola unidad virtual.

3.197 POP 3, por sus siglas en inglés

Protocolo de Oficina de Correo (*Post Office Protocol).*

3.198 PPP, por sus siglas en inglés

Protocolo Punto a Punto. (*Point to Point Protocol*).

3.199 PRC

Perfil de Referencias Cruzadas.

3.200 Programador de aplicaciones

Genera las aplicaciones necesarias en el sistema, con el lenguaje de programación que se requiere y conoce, para la obtención de las entradas de datos que alimentarán la base de datos y, también, para lograr las salidas, como las pantallas de resultados o reportes, que se plantearon en la respuesta de solución.

3.201 Protocolo de Iniciación de Sesión

Protocolo de comunicación en tiempo real para voz sobre el protocolo IP.

3.202 Protocolo de Internet para sincronizar relojes

(NTP por sus siglas en inglés *Network Time Protocol*), acción que sirve para sincronizar los relojes de los sistemas informáticos a través de enrutamiento de paquetes en redes con latencia variable.

3.203 Protocolo

Conjunto formal de procedimientos adoptados para garantizar la comunicación entre dos o más funciones, dentro de la misma capa jerárquica de funciones.

3.204 PSTN, por sus siglas en inglés

Red Telefónica Pública Conmutada, *(Public Switched Telephone Network).*

3.205 PTII

Plataforma Tecnológica para la Integración de Información.

3.206 PTT, por sus siglas en inglés

Pulsa y Habla (*Push-To-Talk*).

3.207 Puerta de enlace

Dirección que usan equipos de cómputo o equipos de comunicaciones cuando requieren comunicarse a otra subred IP.

3.208 Puesto a tierra

Conexión a tierra por medio de un elemento conductor para dirigir eventuales desvíos de corriente hacia la tierra.

3.209 Pulling

Frecuencia y extracción de datos.

3.210 Punto de acometida

Punto de interconexión entre las instalaciones del proveedor y las del usuario.

3.211 PVC, por sus siglas en inglés

Policloruro de Vinilo (*Polyvinyl Chloride*).

3.212 QoS, por sus siglas en inglés

Calidad de servicio (Quality Of Service).

3.213 Radiocomunicación

Comunicación o transmisión a distancia de mensajes hablados, sonidos, imágenes o señales convencionales a través del espacio, mediante ondas electromagnéticas de longitud superior a las del calor radiante.

3.214 RAID, por sus siglas en inglés

Arreglo redundante de discos independientes. *(redundant array of independent disks).*

3.215 RAM, por sus siglas en inglés

Memoria de Acceso Aleatorio. (*Random Access Memory*).

3.216 Red

Conjunto de nodos y enlaces que proporciona conexiones entre dos o más puntos definidos para facilitar la telecomunicación entre ellos.

3.217 Reenvío de llamadas

Servicio suplementario o características de servicio que permiten al usuario dirigir sus llamadas entrantes a otros números.

3.218 RIP, por sus siglas en inglés

Protocolo de Información de ruteo. *(Routing Information Protocol).*

3.219 RJ45

Jack registrado 45.

3.220 RJDQ

Consulta Demográfica del Registro Judicial

3.221 RSTP, por sus siglas en inglés

Protocolo de *Spanning Tree* rápido. *(Rapid Spanning Tree Protocol).*

3.222 RTCP, por sus siglas en inglés

Protocolo con control RTP (*Real Time Transport Control Protocol).*

3.223 RTP, por sus siglas en inglés

Protocolo de transporte en tiempo real. *(Real-time Transport Protocol).*

3.224 s

Segundos.

3.225 SAN, por sus siglas en inglés

Red de área de almacenamiento (*Storage Area Network).*

***3.226* SCE, por sus siglas en inglés**

Sistema de Cableado Estructurado *(Structured Cabling System).*

3.227 Seguridad

Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad son también consideradas.

3.228 Servicio de localización

Servicio de movilidad particular en el que se puede proporcionar a los usuarios autorizados o a las autoridades pertinentes información sobre la posición, en caso de llamadas de emergencia o para gestionar el tránsito de vehículos.

3.229 Servidor

(1) Computadora principal en una red que envía información almacenada en respuesta a solicitudes o consultas. (2) El término servidor también se utiliza para referirse al *software* que hace posible el proceso de publicación de información.

3.230 Servidor de filtro web

Servidor o equipo de seguridad que se utiliza para filtrar contenidos no necesarios y riesgosos a la red interna o externa.

3.231 Servidor Identificador de intrusos (IDS)

Programa que detecta accesos no autorizados a una computadora, a un servidor o a una red.

3.232 Servidor Preventor de Intrusos (IPS)

Servidor protector que examina el tráfico de red para detectar y prevenir ataques a vulnerabilidades que afectan diversos servicios.

3.233 Servidor Secundario

Es una réplica del servidor primario o un servidor a respaldar en su sistema operativo, aplicativos y servicios.

3.234 Sesiones múltiples

Varias sesiones remotas de forma simultánea en un mismo entorno de trabajo de un sistema operativo.

3.235 SFTP, por sus siglas en inglés

Protocolo de transferencia de archivo SSH. (*SSH File Transfer Protocol*).

3.236 SGSI

Sistema de Gestión de Seguridad de la Información

3.237 SIP, por sus siglas en inglés

Protocolo de Inicio de Sesión. (*Session Initial Protocol*).Es un protocolo de control de capa de aplicación (señalización) para crear, modificar y terminar sesiones con uno o más participantes. Estas sesiones incluyen llamadas telefónicas por Internet, distribución multimedia y conferencia multimedia.

3.238 Sistema de gestión de cámaras

Aplicación usada para la captura de video desde las cámaras y su visualización por los monitoristas, por lo que requiere que la aplicación se divida en dos, la aplicación cliente para el monitorista y la aplicación servidor que reside en un computador tipo servidor o en un NVR.

3.239 Sistema de Gestión de Incidentes

Software de despacho de una emergencia que debe de presentar funcionalidades mínimas que permitan un óptimo funcionamiento del sistema Nueve-Uno-Uno (9-1-1) en los tiempos de respuesta para la atención de una llamada de emergencia.

3.240 Sistema de Grabación de Audio

Sistema destinado a grabar todas y cada una de las conversaciones recibidas en el sistema Nueve-Uno-Uno (9-1-1) y del Sistema de Denuncia Anónima 089.

3.241 Sistema de información

Conjunto de elementos que permiten procesar y almacenar información con el apoyo de equipos de cómputo.

3.242 Sistema Manejador de Base de Datos (SMBD)

Módulo de programa que constituye la interfaz entre los datos de bajo nivel almacenados en la base de datos y los programas de aplicaciones y las consultas hechas al sistema.

3.243 Sistema

Sinónimo de Plataforma Tecnológica.

3.244 SITE

Cuarto de telecomunicaciones.

3.245 SLA, por sus siglas en inglés

Acuerdo de Nivel de Servicio (*Sistem Level Agreement*)

3.246 SLIP, por sus siglas en inglés

Protocolo de Interface de Línea Serial. (*Serial Line Internet Protocol*).

3.247 SM

Salida Multiusuario.

3.248 SMS. por sus siglas en inglés

Servicio de Mensajes Cortos. *(Short Message Service)*. Es un servicio que proporciona al usuario servido la capacidad de enviar y recibir mensajes

cortos. Los mensajes cortos se intercambian entre el usuario que envía y el que recibe a través de un Centro de servicio de mensajes cortos. El SMS se proporciona independientemente de una llamada.

3.249 SMTP, por sus siglas en inglés

Protocolo Para la Transferencia Simple de Correo (*Simple Mail Transfer Protocol).*

3.250 SNMP, por sus siglas en inglés

Protocolo de administración de red simple. (*Simple Network Management Protocol*).

3.251 SNTP, por sus siglas en inglés

Protocolo Simple de Hora de Red (*Simple Network Time Protocol).*

3.252 SOA, por sus siglas en inglés

Arquitectura Orientada a Servicios (*Service Oriented Architecture*).

3.253 *Sockets*

Es el zócalo o conexión de la placa base donde se instala el procesador.

3.254 *Softphone*

Aplicación que permite usar una PC de escritorio para controlar y recibir llamadas telefónicas de *software* y para controlar un teléfono IP. También permite la colaboración de audio, video y escritorio con múltiples partes de una llamada.

3.255 *Spanning Tree*, Múltiple

Protocolo que se usa para evitar que las tramas giren sin fin en enlaces físicos redundantes y que pueda trabajar conjuntamente con VLAN.

3.256 *Spanning Tree*, protocolo

Protocolo que se usa para evitar que las tramas giren sin fin en enlaces físicos redundantes.

3.257 SSH, por sus siglas en inglés

Intérprete de órdenes seguro (*Secure Shell).*

3.258 ST

Salida de Telecomunicaciones.

3.259 STP

Ensayo de penetración estándar o SPT (del inglés *Standard Penetration Test*), es un tipo de prueba de penetración dinámica, empleada para ensayar terrenos en los que se quiere realizar un reconocimiento geotécnico.

3.260 Subsistema de Radiofrecuencia

Infraestructura de Radiofrecuencia que es la columna vertebral de los sistemas troncalizados y convencionales.

3.261 SVV

Sistema de Video Vigilancia.

3.262 *Syslog*

Syslog es un estándar de facto para el envío de mensajes de registro en una red informática IP.

3.263 TCP, por sus siglas en inglés

Protocolo de control de transmisión. (*Transmission Control Protocolo*).

3.264 TCP/IP, por sus siglas en inglés

Nombre de la familia de protocolos de Internet basados en IP.

3.265 Telefonía IP

Término genérico para el transporte parcial o total de voz, fax y servicios relacionados, sobre redes basadas en paquetes IP.

3.266 *TengigaEthernet*

Tecnología de la familia *Ethernet* para redes de área local de capa 2 del modelo OSI. Usada en cables UTP categoría 6e, fibra óptica y conmutadores de datos de dicha tecnología para conectar los equipos de red en la red de área local.

3.267 TFTP, por sus siglas en inglés

Protocolo de transferencia de archivos trivial. (*Trivial file transfer Protocol*).

3.268 TI

Tecnologías de la Información.

3.269 Tiempo de atención a Fallas en el Servicio

Tiempo que transcurre desde la recepción de una solicitud de soporte, hasta el momento en que el personal del Proveedor inicia las actividades de soporte.

3.270 Tiempo de espera, tiempo de cola

En el modo de operación con espera, intervalo de tiempo transcurrido entre la tentativa de toma de un órgano y su toma.

3.271 Tiempo de ocupación

Tiempo transcurrido entre la toma de un órgano y su liberación.

3.272 Tiempo de respuesta

El tiempo que transcurre desde el inicio de una interrupción en el servicio, hasta el momento en que el servicio afectado es restablecido.

3.273 Topografía

Técnica que consiste en describir y representar en un plano la superficie o el relieve de un terreno.

3.274 Topología

Se refiere a la forma física en que están conectados los equipos de comunicaciones y equipos finales de usuario.

3.275 TOS, por sus siglas en inglés

Tipo de servicio (*Type of Service).*

3.276 TR

Cuarto de Telecomunicaciones.

3.277 Transacción exitosa

Información desplegada en el monitor en donde se solicitó la consulta por el usuario, o bien, el mensaje de confirmación en el monitor del usuario de que la transacción de alta, baja o actualización de la información solicitada se realizó exitosamente.

3.278 Transacción no exitosa

Transacción recibida por el Sistema pero que no puede ser procesada para convertirse en una transacción exitosa.

3.279 Transacción recibida

Solicitud al Sistema por parte de un usuario para el alta, baja, actualización y/o consulta de la información contenida en el registro electrónico alojado en las bases de datos que corresponda.

3.280 Transacción

El alta, baja, actualización y/o consulta de la información contenida en el registro electrónico alojado en las bases de datos que corresponda.

3.281 Transferencia de llamada

Servicio suplementario o característica de servicio que permite al usuario móvil atendido transferir una comunicación establecida (llamada entrante o saliente) a un tercero usuario.

3.282 Transformaciones XSL

(XSLT por sus siglas en inglés *Extensible Styles Heet Language Transformations*), estilo de Lenguaje para XML.

3.283 Transmisión multibanda

Modo de operación en el que se transmite en varias bandas de frecuencia simultáneamente.

3.284 Troncalizado

Sistema de Radio que permite compartir un número finito de canales de radiofrecuencia entre una población de subscriptores de Radio a través de un acceso controlado mediante un canal de control.

3.285 Tubería

La tubería metálica es uno de varios tipos canalización metálica, de sección circular, que ha sido aprobada para la instalación de conductores eléctricos y de telecomunicaciones, es un buen conductor de puesta a tierra de equipo cuando se instala con sus accesorios y acoplamientos aprobados.

3.286 UDDI, por sus siglas en inglés

(Universal Description, Discovery and Integration). Es un catálogo de negocios de internet.

3.287 USB, por sus siglas en inglés

Bus Serie Universal. (*Universal Serial Bus*).

3.288 Usuario

Persona que cuenta con permisos para acceder a los recursos y servicios que ofrece un sistema.

3.289 Usuarios de base de datos

Administrador de la bases de datos, programador de aplicaciones y usuario final.

3.290 UTC, por sus siglas en inglés

Tiempo Universal Coordinado (*Universal Time Coordinated).*

3.291 UTP, por sus siglas en inglés

Par trenzado sin blindaje. *(Unshielded Twisted Pair).*

3.292 *Video Wall*

Panel de Video.

3.293 VLAN, por sus siglas en inglés

Red de área local virtual (*Virtual Local Area Network).*

3.294 VoIP, por sus siglas en inglés

Voz sobre Protocolo de Internet. (*Voice Over Internet Protocol*).

3.295 VPN, por sus siglas en inglés

Red Privada Virtual. (*Virtual Private Network*).

3.296 VRRP, por sus siglas en inglés

Protocolo de redundancia de enrutador virtual. *(Virtual Router Redundancy Protocol).*

3.297 W3C, por sus siglas en inglés

World Wide Web Consortium. Se refieren a un consorcio internacional que desarrolla recomendaciones y estándares que aseguren el crecimiento de la Red Informática Mundial.

3.298 WAN, por sus siglas en inglés

Red de Área Amplia. (*Wide Area Network*).

3.299 Web Service Description Language (WSDL)

Es un formato utilizado para describir los servicios web.

3.300 WC

Servicios sanitarios.

3.301 WLAN, por sus siglas en inglés

Red de Área Local Inalámbrica. (*Wireless Local Area Network*).Una red inalámbrica mediante la cual un usuario puede conectarse a una red de área local (LAN) a través de una conexión inalámbrica (radio), como alternativa a una red de área local con cable.

3.302 WS-BPEL,por sus siglas en inglés

Lenguaje de Ejecución de Procesos de Negocio (Business Process Execution Language).

4 PRINCIPIOS FUNDAMENTALES

En este Manual se establecen tres niveles para los Complejos de Seguridad, en función de sus actividades y competencias. El Nivel más completo es el 1 y el nivel básico es el 3. El listado que sigue describe los elementos de cada uno, de acuerdo a la Figura 1. El Nivel 3 cuenta con lo mínimo necesario para cumplir con sus actividades y está conformado por los siguientes elementos:

1. Red Estatal de Transporte de Datos, Red Nacional de Telecomunicaciones, (voz, datos y radiocomunicación), cámaras. Se contemplan enlaces de fibra ópticas, microondas y servicios de telecomunicaciones arrendados.
2. Personal de Sistemas y Telecomunicaciones. Actualmente esta área no existe. En esta norma se establece lo necesario para su implementación.
3. Sistema de Respaldo de Energía (UPS y Subestación). Independientemente del tamaño, capacidades operativas y de infraestructura, todos los complejos deben tener un sistema de respaldo de energía que les permita operar en situaciones de contingencia.
4. Red LAN. Todos los complejos deben contar con una red LAN que les permita interconectar los diferentes sistemas informáticos existentes en el CS así como contemplar su interconexión hacia el exterior.
5. Red Estatal de Radiocomunicación. Se refiere a la infraestructura de comunicaciones básica que utiliza el despachador (medio de transporte con tecnología TDM e IP, torres y radios) así como la disponibilidad de los servicios utilizados por los usuarios.
6. Aire Acondicionado. Todas las secciones deben contar con aire acondicionado en las instalaciones del CS y se debe monitorear los parámetros de temperatura y humedad.
7. Sistema de Video Vigilancia. (Norma Técnica para Estandarizar las Características Técnicas y de Interoperabilidad de los Sistemas de Video Vigilancia para la Seguridad Pública). Todas las secciones deben contar con un Sistema de Video Vigilancia (incluyendo los sistemas remotos).
8. Servicio de Atención de Llamadas de Emergencia 9-1-1. (Norma Técnica para Estandarizar los Servicios de Llamadas de Emergencia a través del Número Único Armonizado 9-1-1 (Nueve, Uno, Uno).
9. Sistema de Acceso. Sistema de control de acceso al CS (Biométricos, electrónicos) y sus procesos asociados.

10. Circuito Cerrado de Televisión (CCTV) en área internas y periferia del inmueble.

El Nivel 2 incluye lo que existe en el Nivel 3, más lo siguiente:

11. Sistemas Administrativos.
12. Análisis y Estadística.
13. Ciberseguridad.

El Nivel 1 es el más completo e incluye lo existente en los Niveles 3 y 2 y además:

14. Registro de Personal (Cámara Ecoica, Registro de huellas digitales, Cuarto fotográfico, instalaciones para desarrollo de pruebas de ADN, cuando se estime necesaria por parte de la Alta dirección).
15. Servicio de Atención de Llamadas de Denuncia Anónima (089).
16. Sistema de Alta Disponibilidad TIER III (ANSI/TIA-942).
17. Área de Inteligencia.
18. Sistemas de Desarrolladores.
19. Sistema de Reconocimiento de Placas.
20. Sistemas de Recuperación contra Desastres.
21. Administración y Reparación, que se refiere a la creación de grupos de radio, asignación de perfiles y de reparación de radios, etc.

Todos los Niveles están directamente relacionados con:

22. Base de datos
23. Áreas requeridas por cuestiones de operación, atribuciones legales y/o innovación tecnológica.

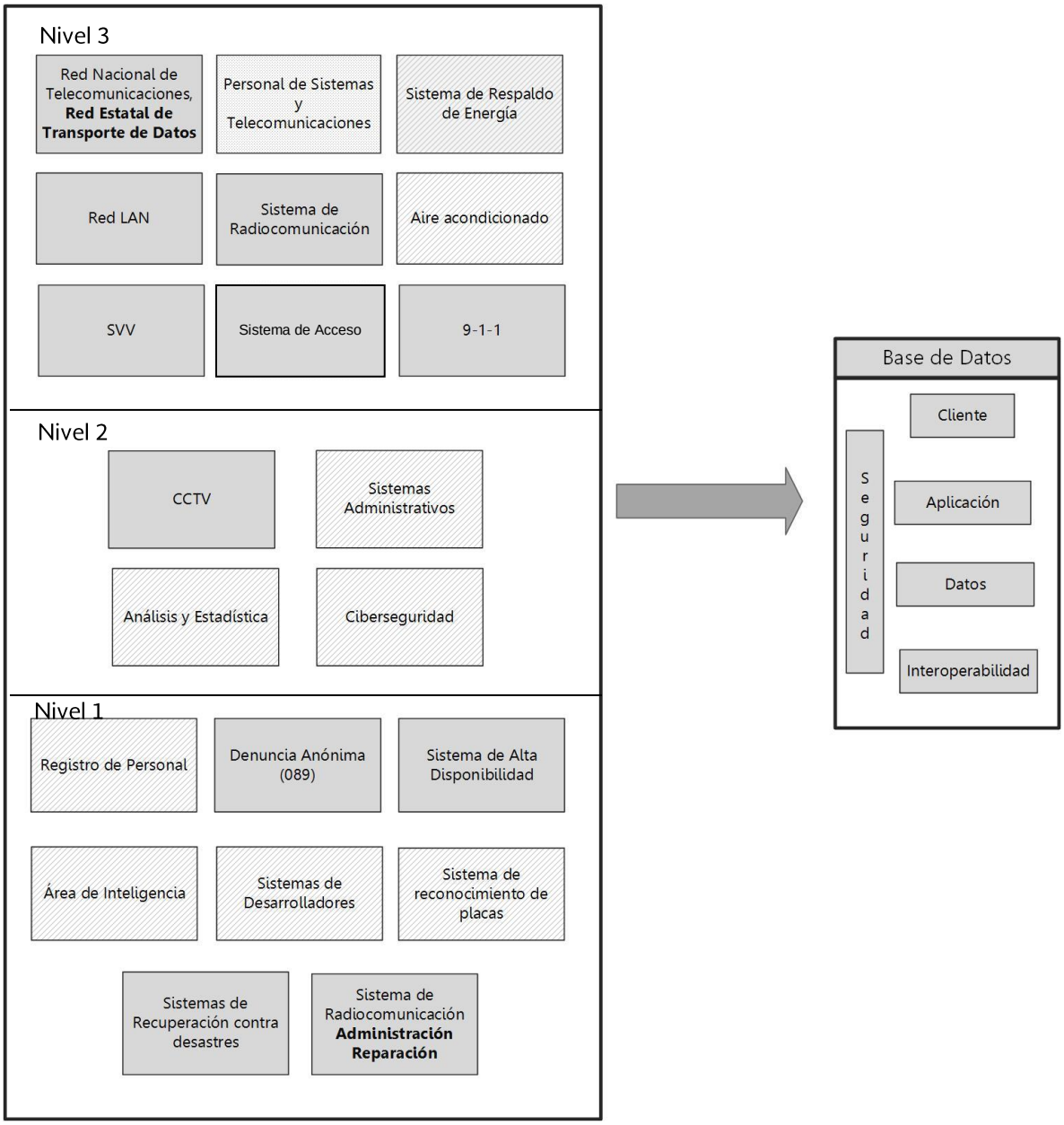


Figura. 1 Diagrama a bloques del Complejo de Seguridad

Desde un punto de vista técnico, los Complejos de Seguridad se subdividen en varios sistemas que cuentan con diferentes áreas, de tal forma que en su totalidad permiten la realización de las funciones del Complejo y de la misión para la cual fue creado. En la figura 2 se muestra el diagrama general de los diferentes sistemas que componen a un CS:

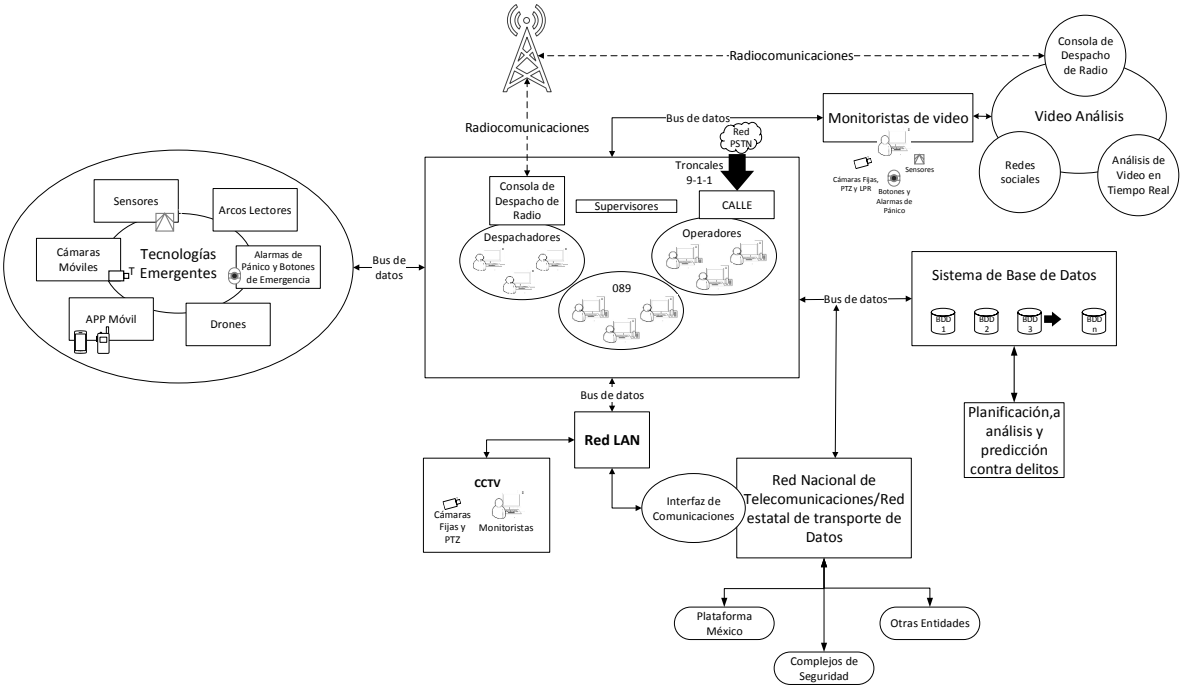


Figura. 2 Esquema de un Complejo de Seguridad

Los sistemas que debe tener necesariamente un Complejo de Seguridad son:

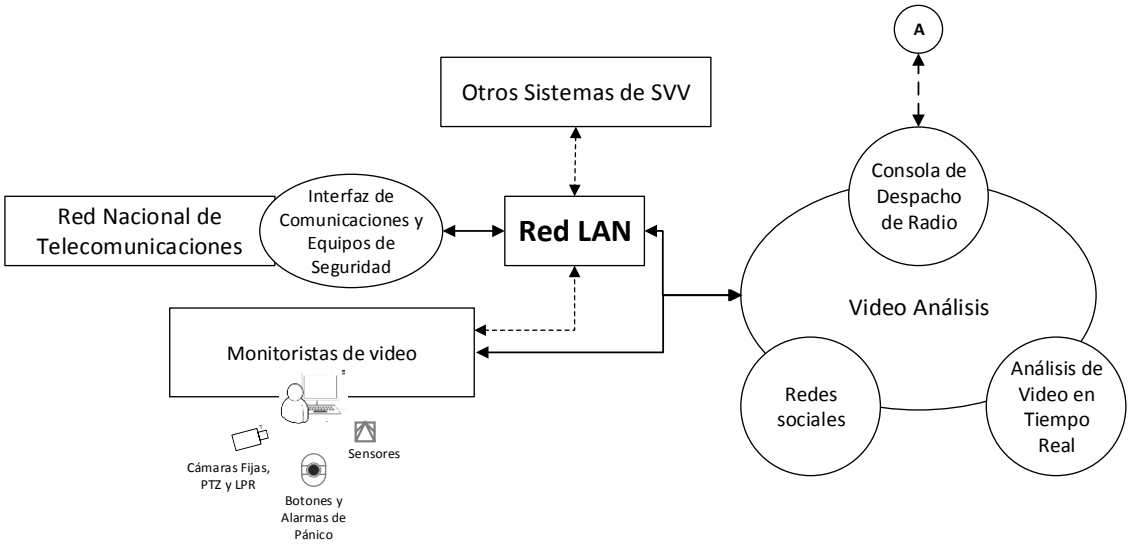
- Video análisis.
- Tecnologías Emergentes.
- Despacho Asistido por Computadora (CAD).
- Sistema de Base de Datos.
- Red Nacional de Telecomunicaciones/Red estatal de transporte de Datos.
- Red LAN.

Como se muestra en la figura 2, la interconexión entre los sistemas se realiza mediante el bus de datos indicado por las flechas continuas mientras que las comunicaciones de radio se identifican con las flechas punteadas.

Los dos primeros sistemas deben ser contemplados para los nuevos Complejos de Seguridad. Este documento no define las características técnicas de ambos sistemas, pero se mencionan sus fines en esta introducción. Cada uno de estos sistemas tiene una función que se explica a continuación en lo general:

Video Análisis

Como se observa en la figura 3 la señal de video que proviene de las cámaras fijas, PTZ y LPR, será consultada por el área de Video Análisis. A diferencia de los monitoristas, que tienen asignadas varias cámaras, en esta área se observarán sólo cámaras especificas definidas por el Complejo de Seguridad. Los puntos de interés podrán ser bancos, cajeros automáticos, centros comerciales, eventos masivos, entre otros, donde se realizará el análisis de video en tiempo real. Puede observarse que el área de Video Análisis tiene conexión a Plataforma México, para realizar consultas a sus bases de datos. Se propone que se realice reconocimiento de rostros y/o placas en tiempo real en los videos de las cámaras de vigilancia utilizando software especializado, el CS definirá cual es el software que más convenga con base en su infraestructura. Las líneas punteadas indican que podrán considerarse los videos de otros sistemas SVV (como Bancos, tiendas de conveniencia, entre otros) y videos proporcionados por monitoristas de video remotos. La letra A encerrada en el círculo indica la comunicación con radio.



1. Figura. 3 Diagrama del área de Monitoreo de redes y análisis delictivo.

En el área de Video Análisis se realizan, entre otras, las siguientes funciones:

- Análisis de video en redes sociales. Se analizarán los videos de las diferentes redes sociales. El Complejo de Seguridad definirá las redes sociales de su interés.
- Análisis de video en tiempo real. Debe contar con aplicativos que permitan vigilar en bancos, centros comerciales, cajeros automáticos, etc., para identificar rostros y/o placas de automóviles. El reconocimiento de rostros y/o placas se debe realizar en tiempo real y debe compararse con la base de datos correspondiente

en Plataforma México; en caso de detectar alguna alerta se dará aviso a la consola de despacho de radio.

El Área de Monitoreo de redes y análisis delictivo debe contar con conexión al Área de Despacho, que se encargará de comunicarse con las diferentes dependencias para atender las alertas que se presenten.

Tecnologías Emergentes

La posibilidad de integrar tecnologías emergentes para apoyar las funciones del Complejo de Seguridad se muestra en la figura 4. No está contemplada toda la variedad de tecnologías emergentes posibles que contribuyen a los Complejos de Seguridad, pero se mencionan algunas, y la forma en que proporcionan apoyo al complejo. Estas tecnologías emergentes deben utilizar los medios de comunicación tales como redes cableadas o inalámbricas que pueden ser comerciales o arrendadas, como las redes celulares y redes privadas. La transmisión de información se debe llevar a cabo, cuando sea conveniente, utilizando VPN desde y hacia el Complejo de Seguridad, a todas las tecnologías emergentes. Se debe pasar por la zona desmilitarizada para alcanzar la granja de servidores. De esta forma la información podrá ser enviada por una red de datos no segura o pública.

Los arcos lectores, cámaras, sensores, botones de pánico, drones y los dispositivos portables deben utilizar redes cableadas o inalámbricas que pueden ser comerciales o arrendadas para transmitir los datos de la aplicación, apegándose a la implementación de VPN del Complejo de Seguridad.

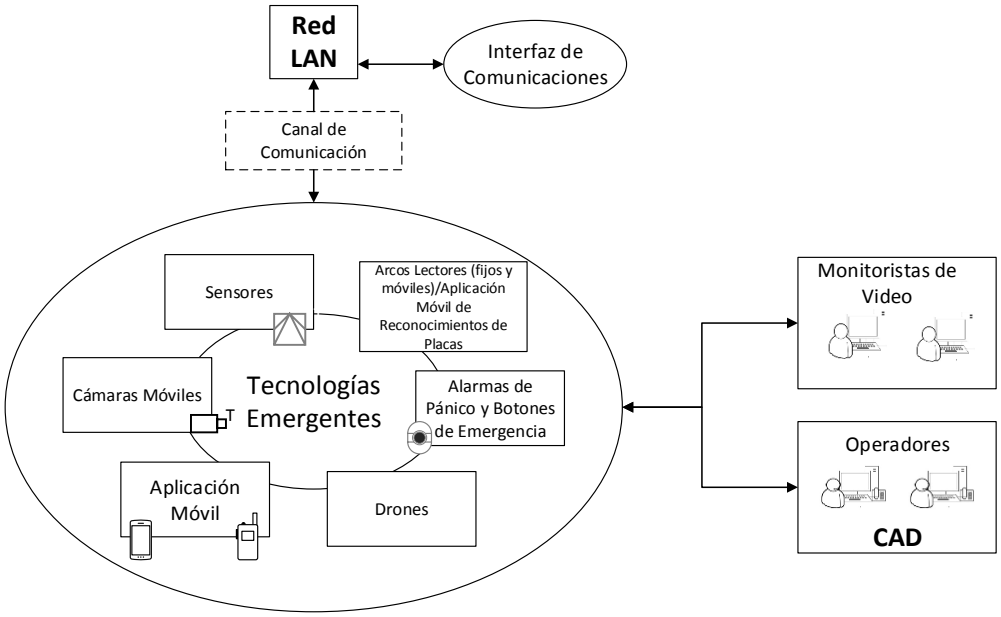


Figura. 4 Diagrama de Tecnologías Emergentes.

Este apartado se describen brevemente algunas de las tecnologías emergentes con las que puede contar el Complejo de Seguridad:

a) **Arcos lectores fijos y móviles/aplicación móvil de reconocimiento de placas.** Debe instalarse arcos lectores de placa en puntos estratégicos que serán definidos por el Complejo de Seguridad. Los lectores podrán ser fijos y/o utilizar lectores móviles. La aplicación móvil de reconocimiento de placas se instalará en dispositivos portables que el Complejo de Seguridad defina (tales como tabletas, teléfonos inteligentes, computadoras móviles) para sistemas operativos Android, iOS, Windows o Linux. Los arcos lectores y la aplicación móvil realizarán consultas a las Bases de Datos Criminalísticas y de Personal del Sistema Nacional de Seguridad Pública (BDCPSNSP) correspondientes en tiempo real. Cuando los arcos o la aplicación móvil detecten una placa con reporte en la BDCPSNSP se debe emitir una alerta a los operadores del CAD. En el caso de los arcos lectores podrán conectarse al Complejo de Seguridad por redes cableadas o inalámbricas (o cualquier otro medio de comunicación que cumpla con el ancho de banda requerido), y la información debe ser cifrada. El Complejo de Seguridad definirá los aplicativos y los procesos para realizar esta actividad.

b) **Cámaras Móviles.** Las cámaras móviles se podrán instalar en los vehículos de seguridad y ser portados por elementos de seguridad. Deben utilizar de ser posible redes cableadas o inalámbricas o cualquier otro medio de comunicación

que cumpla con el ancho de banda requerido, y la información debe ser cifrada para comunicarse al Complejo de Seguridad con el fin de transmitir videos de placas y rostros. Las imágenes de placas y rostros deben compararse con las bases de datos respectivas en la BDCPSNSP. El Complejo de Seguridad definirá los aplicativos y los procesos para realizar esta actividad.

c) **Aplicaciones Móviles.** Las aplicaciones móviles se instalarán en dispositivos portables que el Complejo de Seguridad defina (tales como tabletas, teléfonos inteligentes, computadoras móviles, de uso rudo) para sistemas operativos Android o iOS. Deben desarrollarse aplicaciones que coadyuven a las labores y actividades del CS. Podrán utilizar redes cableadas o inalámbricas o cualquier otro medio de comunicación que cumpla con el ancho de banda requerido, y la información debe ser cifrada para comunicarse al Complejo de Seguridad.

d) **Sensores/Alarmas de Pánico y Botones de Emergencia.** Se instalarán sensores en instalaciones y áreas estratégicas definidas por el Complejo de Seguridad (tales como sensores de movimiento, cámaras térmicas, apertura de puertas, entre otros). Los sensores podrán conectarse al Complejo de Seguridad utilizando redes cableadas o inalámbricas o cualquier otro medio de comunicación que cumpla con el ancho de banda requerido, y la información debe ser cifrada. Se recomienda que se instalen botones de emergencia en el mismo lugar donde se encuentren las cámaras de video vigilancia. Se propone que las Alarmas de Pánico sean utilizadas por establecimientos comerciales, tiendas de conveniencia, entre otros. El Complejo de Seguridad definirá los aplicativos y los procesos para realizar estas actividades observando las políticas de seguridad correspondientes.

e) **Drones.** Se recomienda el uso de drones para realizar video vigilancia en áreas de alto riesgo, de difícil acceso o donde lo defina el Complejo de Seguridad. El video debe ser grabado de forma local y de ser posible transmitido por las redes inalámbricas existentes para comunicarse al Complejo de Seguridad. El Complejo de Seguridad definirá los aplicativos y los procesos para realizar estas actividades, en conjunto con la Dirección General de Aeronáutica Civil en el área que le corresponda.

Despacho asistido por computadora (*Computer Aided Dispatch*, CAD)

El Centro de Atención de Llamadas (CALLE), a través del sistema de atención de llamadas de emergencia 9-1-1, atiende, registra y asigna al sistema correspondiente las diferentes emergencias recibidas por parte de la ciudadanía. Por lo cual se requiere de un elemento que le permita al operador del sistema 9-1-1 hacer la captura de toda la información y dar seguimiento a cada una de ellas. El Despacho Asistido por Computadora (CAD) es el sistema mediante el cual se hace la captura de la

información en el momento de atender un llamado de emergencia. Los datos básicos de captura con los que debe contar son:

- Geo-localización del lugar desde donde se reporta la emergencia (debe de ser automática y segura).
- Datos generales del ciudadano que reporta la emergencia.
- Número telefónico desde donde se reporta la emergencia (debe de ser automático).
- Tipo de emergencia (dependiendo de la emergencia que se reporte (Médica, Seguridad y/o Protección Civil), el CAD debe contener los campos necesarios para almacenar la información de cada una de ellas).

Sin embargo, el CAD no es únicamente el elemento de registro de información, sino que también es el medio por el cual el Sistema de Video Vigilancia (SVV) y el Área de Operadores se deben comunicar. Cada uno de ellos debe tener el mismo CAD, con los elementos necesarios para su operación, de acuerdo al área que pertenezcan. De esta forma, cuando se reciba una emergencia el primer contacto que se tendrá es con el operador del sistema 9-1-1 y de requerirse atención por parte del SVV se podrá notificar a dicha área por medio del CAD. Finalmente, toda llamada procedente debe canalizarse al área de despacho, haciéndolo de la misma forma, a través del CAD.

En la figura 5 se muestra la interconexión de los sistemas 9-1-1, SVV, área de operadores y despachadores a través del CAD.

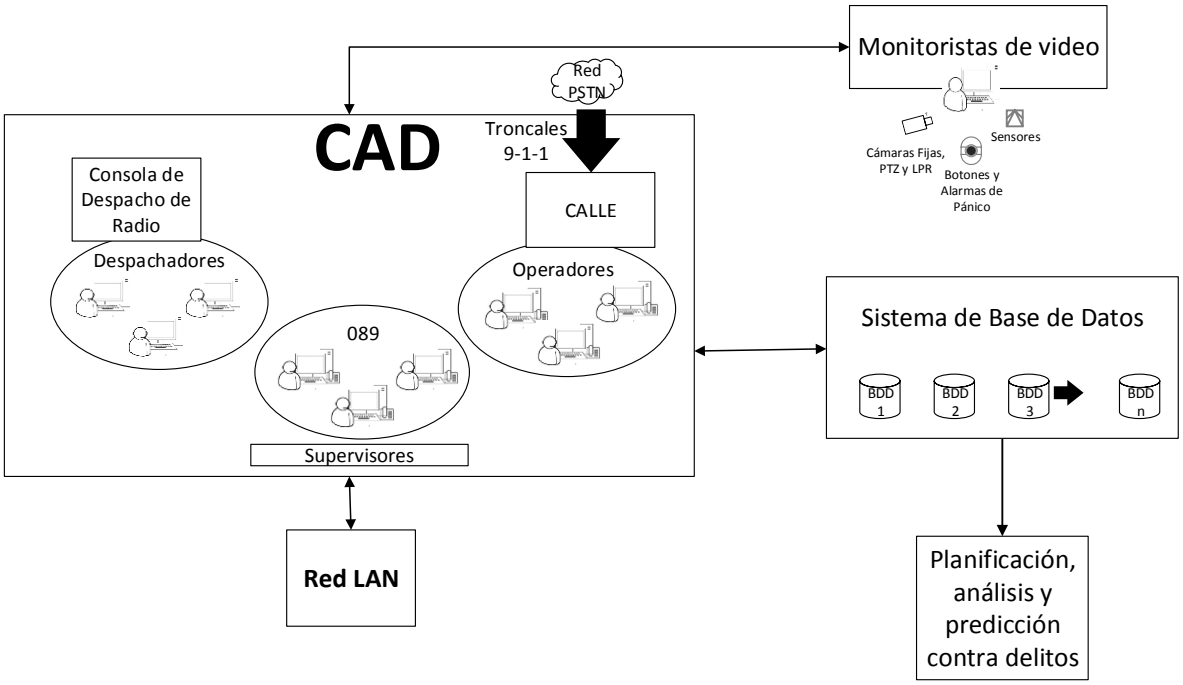


Figura. 5 Despacho Asistido por Computadora CAD

Los sistemas 9-1-1, SVV, área de Operadores y Despachadores, deben compartir un aplicativo a través del CAD para que cada uno atienda la emergencia que le corresponde. Los eventos serán registrados en la base de datos correspondiente. La interconexión de los sistemas se realizará a través de la Red LAN.

Sistema de Base de Datos

Este sistema define los protocolos de comunicación y el diseño de la red de datos para el funcionamiento del Complejo de Seguridad en su interoperabilidad interna y externa, de modo que se contribuya a una mejora en la calidad de los procesos de comunicación: mayor eficiencia, reducción de errores, eliminación de duplicidad de datos, entre otros.

Lo anterior, para el cumplimiento de los objetivos en materia de operación policial, emergencias, comunicaciones de seguridad pública, así como con fines de consulta y explotación de las bases de datos siguientes: 1. Informe Policial Homologado, 2. Licencias de Conducir, 3. Mandamientos Judiciales, 4. Registro Nacional de Armamento y Equipos, 5. Registro Nacional de Información Penitenciaria, 6. Registro Nacional de Personal de Seguridad Pública, 7. Registro de Vehículos Robados y Recuperados, 8. Registro Público Vehicular, 9. Incidencia Delictiva y 10. Sistema de Atención de Llamadas de Emergencia 9-1-1 y de denuncia anónima 089.

Como se muestra en la figura 6, en el Sistema de Base de Datos se propone contar con un aplicativo que realice las funciones de planificación, análisis y predicción contra delitos. Con base en la explotación de las bases de datos correspondientes se podrá realizar la planificación de acciones que permitan disminuir las actividades delictivas.

Por otro lado, se podrá hacer análisis de la información histórica de inicidencia delictiva para predecir eventos y contribuir a inhibir la delincuencia. El CS definirá cual es el software que más le convenga con base en su infraestructura. Por ejemplo, se podrán realizar análisis sobre robo de autos, identificando zonas, horarios, tipos de vehículos, para reforzar la vigilancia en las zonas y horarios identificados y de esa manera planificar acciones que ayuden a prevenir el delito. Este análisis se podría aplicar a delitos como secuestro, robo a casa habitación, robo con violencia, extorsión, entre otros.

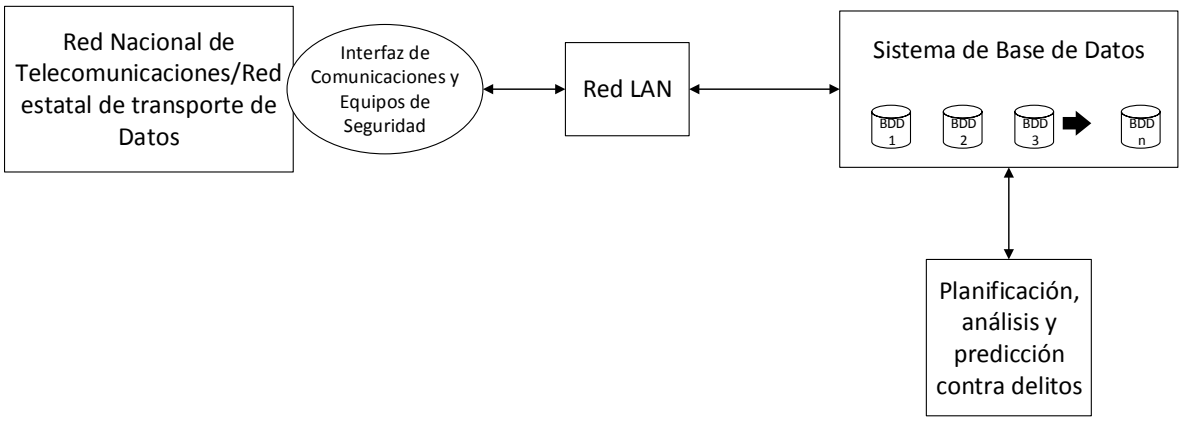


Figura. 6 Diagrama general del Sistema de Base de Datos

En la sección X de esta norma se explica en detalle el funcionamiento del sistema de base de datos.

En el CS se propone implementar un sistema gestor de base de datos que, con base en el software adecuado y definido por cada CS, permita el almacenamiento, modificación y extracción de la información en las base de datos. Además de contar con herramientas para añadir, borrar, modificar y analizar los datos. Los usuarios definidos por los CS podrán acceder a la información usando las herramientas específicas de consulta y de generación de informes.

La administración de las bases de datos debe contar con métodos para mantener la integridad de los datos, administrar el acceso de usuarios a las bases de datos y

recuperar la información si el sistema se corrompe. Se recomienda incluir un módulo gráfico que permita presentar la información con gráficos y tablas.

En la figura 7 se muestra la arquitectura de la Plataforma Tecnológica para la Integración de Información.

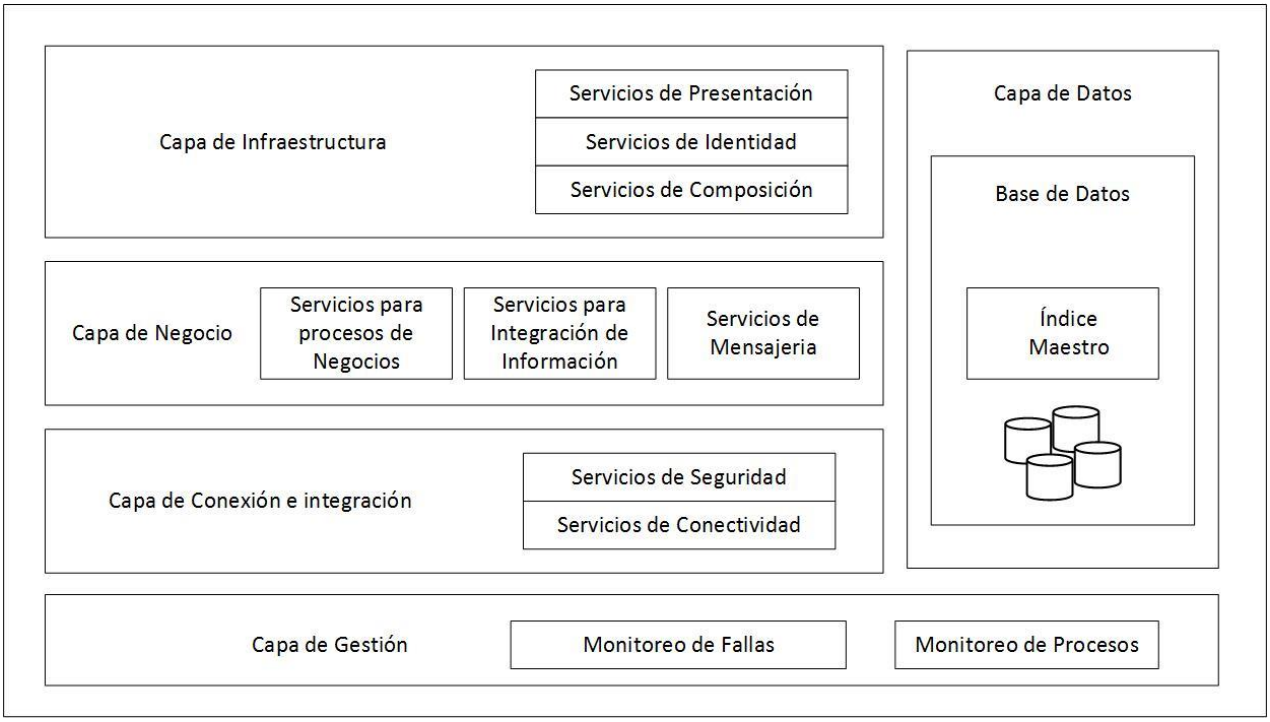


Figura. 7 Arquitectura de la Plataforma Tecnológica para la Integración de Información (PTII)

Red Nacional de Telecomunicaciones/Red Estatal de Transporte de Datos

Como se muestra en la figura 8, el Complejo de Seguridad debe tener conexión a través de la Red LAN/ WAN, utilizando una Interfaz de Comunicaciones con Plataforma México y una red WAN con otros Complejos de Seguridad y con otras instancias de gobierno o aquéllas vinculadas a la seguridad de la población. Se podrá utilizar la Red MPLS, fibra óptica, microondas o cualquier otro medio de comunicación que cumpla con el ancho de banda requerido.

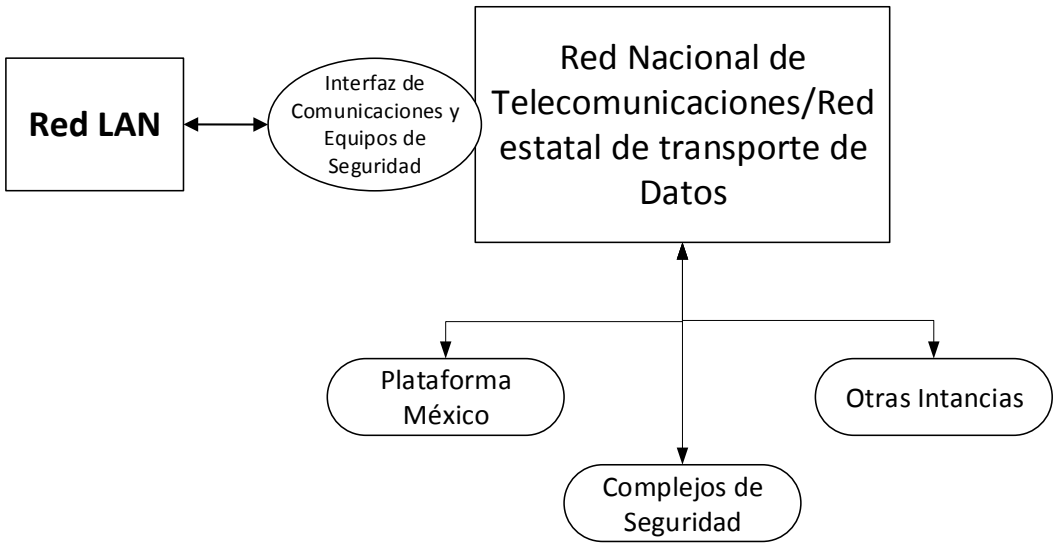


Figura. 8 Diagrama de la Red Nacional de Telecomunicaciones

Red LAN

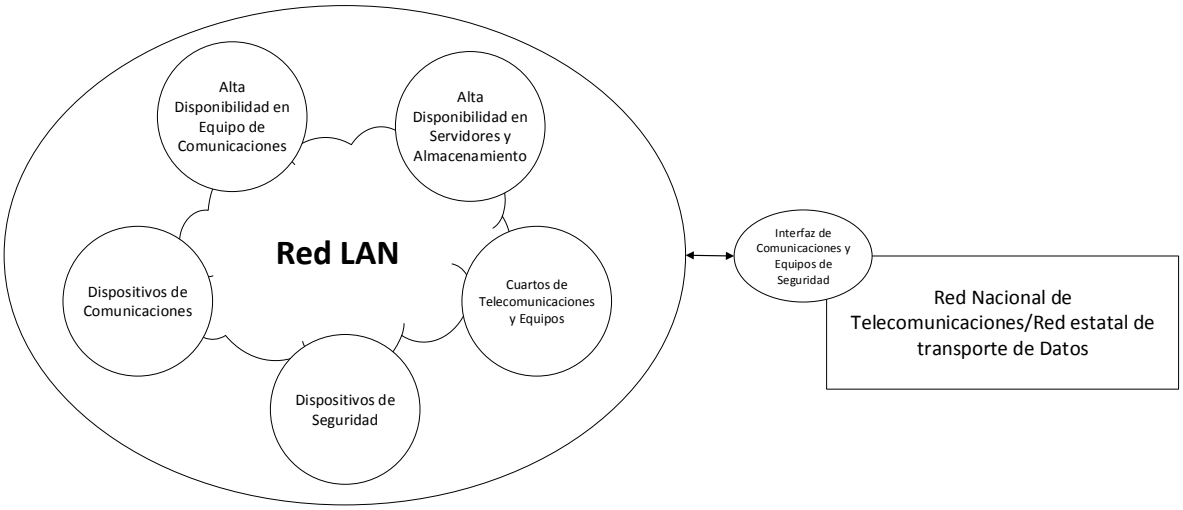


Figura. 9 Diagrama de la Red LAN del Complejo de Seguridad

La Red LAN debe estar preparada para soportar el Sistema de Video Vigilancia, el sistema 9-1-1, el sistema 089 y demás servicios que proveen beneficio a la sociedad. También la Red LAN debe soportar las operaciones internas del Complejo de Seguridad que coadyuvan al servicio de seguridad de la población. Por ello se consideran los siguientes sistemas dentro de la Red LAN:

Cableado estructurado: donde se dan lineamientos que debe cumplir el cableado estructurado, así como los correspondientes para los cuartos de telecomunicaciones

y de equipos. Se hace énfasis en que los cuartos de telecomunicaciones y de equipos estén debidamente preparados y ambientados para albergar los dispositivos de telecomunicaciones, granjas de servidores y los sistemas de almacenamiento, las 24 horas del día, los 365 días del año.

Equipos de comunicaciones (conmutador de datos y enrutadores): donde se definen los protocolos de comunicaciones válidos para diferentes casos de implantaciones. Cuando no se define un protocolo de comunicaciones para un caso específico se debe recurrir a protocolos generados por organismos nacionales o internacionales. Se dan lineamientos para seleccionar equipos de telecomunicaciones con el fin de proveer un servicio continuo por parte de estos equipos y prever el crecimiento de la Red LAN.

Equipos de seguridad: la implementación de equipos de seguridad es obligatoria para los Complejos de Seguridad. Las granjas de servidores y el almacenamiento deben tener como piedra angular para su protección el corta fuego y un IDS/IPS, de tal forma que se asegure que no serán violados los servicios y la integridad de las bases de datos. En cuanto a la salida para la Internet, también es obligatorio protegerla, teniendo como elemento extra para su protección -además de los elementos ya mencionados- un filtro *web*, implementado en las políticas de filtrado *WEB* que el Complejo de Seguridad defina. Además es importante considerar otras áreas que por la delicadeza de la información que manejan o generan deben también ser apropiadamente protegidas.

Alta disponibilidad en equipos de comunicaciones: el servicio prestado a la sociedad por un Complejo de Seguridad es crítico, por lo que para proveer alta disponibilidad se debe considerar redundancia en diferentes sistemas. Se contempla un apartado dedicado a esquemas de alta disponibilidad aplicados a los equipos de comunicaciones, y se definen equipos de respaldo para el conmutador de datos principal y para las salidas de comunicaciones del Complejo de Seguridad.

Alta disponibilidad para servidores y almacenamiento de información: este sistema, titulado en este documento como Arquitectura de Servidores y Sistemas de Almacenamiento, aborda los lineamientos que se deben cumplir en servidores para mantener sus servicios en alta disponibilidad, es decir, tolerantes a fallos. De igual forma, se plantean arquitecturas para sistemas de almacenamiento que aseguren mantener su servicio disponible y la recuperación de información en caso de fallo de discos. Todas las arquitecturas permiten el escalamiento a partir de una arquitectura simple, a otra con mayores prestaciones y rendimiento.

4.1 Lineamientos para la aplicación de las especificaciones en sistemas de telecomunicaciones, servidores, sistemas de almacenamiento y sistema de bases de datos para la complejos de seguridad

4.1.1 Objetivo

El objetivo de estas especificaciones es precisar las disposiciones de carácter técnico que deben cumplir los sistemas de telecomunicaciones, servidores, sistemas de almacenamiento y bases de datos en un Complejo de Seguridad.

Las disposiciones establecidas en esta norma no deben considerarse como guía de diseño de instalaciones ni como un manual de instrucciones para personas no calificadas. Se considera que, para hacer un uso apropiado de estas especificaciones, es necesario recibir capacitación y tener experiencia suficiente en las tecnologías de telecomunicaciones y de información.

4.1.2 Características de las especificaciones de la Norma

Las especificaciones de esta Norma se dividen como se indica en el apartado 5.

4.1.3 Disposiciones obligatorias y notas aclaratorias

Las disposiciones de carácter obligatorio indicadas en esta norma, son aquéllas que identifican acciones exigidas o prohibidas específicamente y se caracterizan por el uso del término “debe” o “no debe”, o por el tiempo gramatical en futuro.

Las notas no son disposiciones obligatorias, a menos que se indique otra cosa en esta norma, sólo intentan aclarar conceptos o proporcionar información adicional que permita comprender lo indicado en la disposición que les antecede, o bien proporcionan referencias a otras disposiciones.

5 ESPECIFICACIONES

5.1 Red Nacional de Telecomunicaciones, Red Estatal de Transporte de Datos

5.1.1 Objetivo

Interconectar a las diferentes dependencias que interoperan con el Complejo de Seguridad, y proporcionar algunas de las características técnicas que deben cumplir los enlaces de comunicaciones.

5.1.2 Alcance

Las características y especificaciones definidas en este apartado aplican a la infraestructura de telecomunicaciones de los Complejos de Seguridad, no es una guía de diseño y debe ser leído por personal capacitado en tecnología de telecomunicaciones.

5.1.3 Campo de aplicación

Complejos de Seguridad.

5.1.4 Descripción

Como se muestra en la figura I.1 el Complejo de Seguridad debe tener conexión a través de la Red LAN, utilizando una interfaz de comunicaciones con Plataforma México, con otros Complejos de Seguridad y otras Instancias.

El Complejo de Seguridad definirá los requisitos de comunicaciones correspondientes para conectarse a la Red LAN a través de la interfaz de comunicaciones. El Complejo de Seguridad definirá el medio de comunicación adecuado para conectarse con Plataforma México, otros CS y otras Instancias que se consideren pertinentes. La conexión entre los CS debe cumplir con las políticas de seguridad y lineamientos correspondientes.

La interconexión entre CS y Plataforma México debe realizarse en tiempo real para garantizar los requerimientos de información del Nuevo Sistema de Justicia Penal Acusatorio y el intercambio de información que favorezca la coordinación efectiva

entre las corporaciones de seguridad pública para coadyuvar las labores de inteligencia entre los CS. Los CS deben utilizar redes cableadas o inalámbricas que pueden ser comerciales o arrendadas para transmitir la información, apegándose a la implementación de una o varias VPN del Complejo de Seguridad.

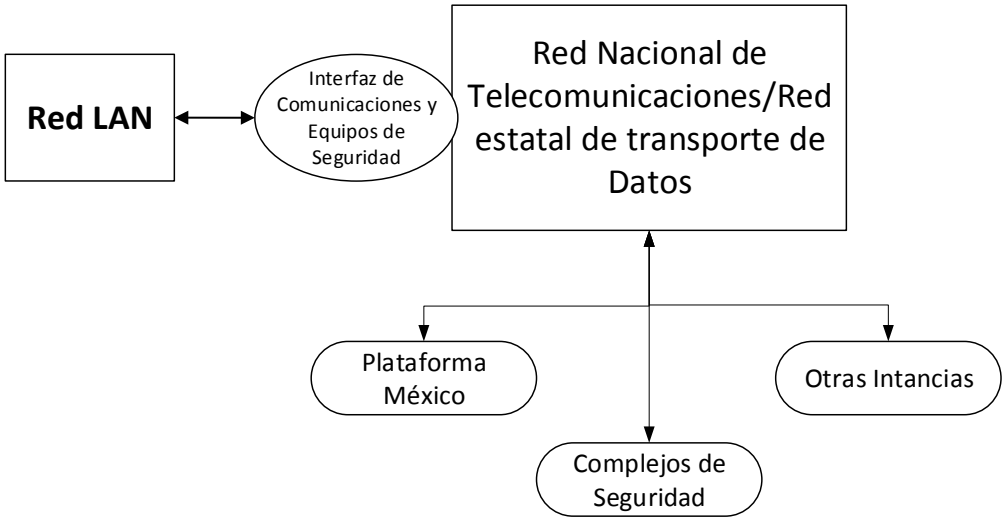


Figura I. 1 Conexión del Complejo de Seguridad con otros Complejos de Seguridad y otras instancias

Se debe utilizar los medios de comunicación tales como redes cableadas o inalámbricas que pueden ser comerciales o arrendadas, como pueden ser las redes celulares y redes privadas. La transmisión de información se debe llevar a cabo, cuando sea conveniente, utilizando una o varias VPN desde y hacia todos los Complejos de Seguridad. De esta forma la información podrá ser enviada por una red de datos no segura o pública, como se muestra en la figura I.2.

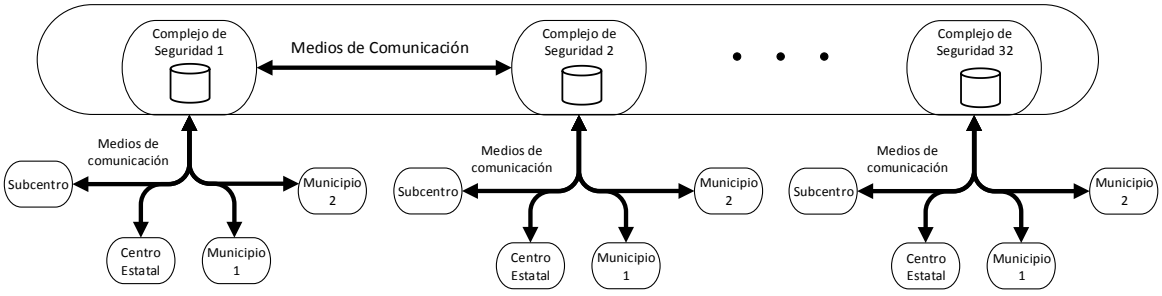


Figura I. 2 Conexión del Complejo de Seguridad con otros Complejos de Seguridad y otras instancias

5.1.5 Requerimientos Generales del Complejo de Seguridad para conectarse con una Red de Microondas y Redes de Fibra Óptica.

5.1.5.1 Requerimientos de diseño para los enlaces inalámbricos y de fibra óptica de la red estatal.

A continuación se describen los requerimientos generales previos a cubrir para la selección del equipo, protocolos de comunicación y demás dispositivos o elementos que se utilizarán en la puesta de la red estatal:

a) Determinación de los anchos de banda a usar en los enlaces.

b) Tipo de medio, topología y equipos a usar.

c) Para los enlaces de microondas (PTP, PMP, suscriptor) se debe realizar el estudio del enlace de microondas correspondiente, especificando al menos los siguientes parámetros:

I. Potencia de salida utilizada en el cálculo de enlace (no sólo la potencia máxima que pueda utilizar la estación radioeléctrica).
II. Potencia Isotrópica Radiada Efectiva (PIRE, por sus siglas en inglés) (limitada por las disposiciones nacionales e internacionales).
III. Tipo de antena:
    i. PTP, PMP (sectorial/haz amplio).
    ii. Incluyendo las características del reflector (tipo, tamaño, etc.).
    iii. Tipo de polarización.
    iv. Frecuencias de operación de transmisión y recepción en la banda de 4.9 GHz.
    v. Ancho del haz de media potencia, Horizontal.
    vi. Ancho del haz de media potencia, Vertical.
    vii. Relación frente a espalda (F/B).
    viii. Ganancia a baja frecuencia.
    ix. Ganancia a media frecuencia.
    x. Ganancia a alta frecuencia.
    xi. Patrón de radiación.

d) En caso de ser medio de fibra óptica, a partir de los requerimientos del sistema y de la información de parte del fabricante del equipo óptico elegido, se requiere realizar el diseño del enlace óptico a través de cálculos o especificaciones del fabricante, para determinar, como mínimo:

I. Trayectorias, así como sus longitudes, número de empalmes, protección del empalme, conectores, acopladores, herrajes, así como aditamentos necesarios para asegurar físicamente la fibra óptica.
II. Tipo de fibra óptica: MMF (Fibra Óptica Multimodo) o SMF (Fibra Óptica Monomodo).
III. Recubrimiento de la fibra óptica de acuerdo al medio donde se instale: instalación subterránea, aérea, en ductos, etc.
IV. Número de fibras a instalar.
V. Longitud de onda a usar en el enlace: 850 nm, 1300 nm, 1550 nm, etc.
VI. Ancho de banda del enlace, el cual debe satisfacer los requerimientos del sistema.
VII. Pérdida o atenuación total del enlace debido a la fibra óptica, empalmes y conectores; la cual debe estar de acuerdo con las especificaciones del fabricante del equipo óptico.
VIII. Si se requieren, atenuadores.

e) Previo a cualquier instalación se debe contar con un sistema de energía eléctrica, tierra física, pararrayos y respaldo de energía.

f) Para los enlaces inalámbricos, las frecuencias deben ser asignadas por el Instituto Federal de Telecomunicaciones (IFT) para uso exclusivo de seguridad pública en los tres órdenes de gobierno. No se permite el uso de frecuencias libres o de otro tipo de asignaciones.

g) Definir índice de protección para exteriores en los equipos de comunicaciones.

h) Definición de pruebas de los enlaces y equipos de comunicaciones.

i) Los dispositivos instalados en otras dependencias siempre se conectarán a través de un elemento de red, para comunicarse con el Complejo de Seguridad. Los dispositivos instalados en el Complejo de Seguridad y en las otras dependencias deben ser compatibles con el elemento de red.

5.1.5.2 Lineamientos de diseño

a) Se deben usar protocolos abiertos de organizaciones de normalización internacionales para garantizar la interoperabilidad de los sistemas de voz, datos y video.

b) Se deben utilizar protocolos de comunicación para el monitoreo y administración que proporcionen seguridad al envío de la información.

c) Se debe solicitar pruebas de los enlaces.

d) La transmisión de datos debe realizarse utilizando un algoritmo de cifrado.

e) La estación radioeléctrica debe estar homologada ante el Instituto Federal de Telecomunicaciones.

f) Se debe configurar y gestionar los elementos de la red, local y remotamente.

5.1.5.3 Parámetros de Radiocomunicación

A continuación, se enlistan los parámetros técnicos de la estación radio eléctrica punto a punto, multipunto y la repetidora. Se presentan tomando como referencia el documento "Norma técnica para estandarizar las características técnicas y de interoperabilidad de los sistemas de video vigilancia para la Seguridad Pública". Se enlistan en dicho orden.

a) Estación radio eléctrica punto a punto suscriptor (usualmente el ancho de banda es de 10/25 Mbps).

I. En el enlace de microondas se puede utilizar LOS (*Line Of Sight*, por sus siglas en inglés) /OLOS (*Obstructed Line Of Sight,* por sus siglas en inglés)/NLOS (*Non Line of Sight*, por sus siglas en inglés) en terminal PTP y compatible con terminal PMP; se podrá escoger cualquier tipo, de acuerdo al estudio del enlace.
II. Frecuencias asignadas por el Instituto Federal de Telecomunicaciones (IFT) para uso exclusivo de seguridad pública en los tres órdenes de gobierno. No se permite el uso de frecuencias libres o de otro tipo de asignaciones.
III. Modulación dinámica: el equipo de radio frecuencia debe soportar como mínimo los siguientes tipos de modulación BPSK, QPSK, 16QAM, 64QAM.
IV. Ancho del canal: se podrá usar el ancho de canal que cumpla la regulación aplicable por usuario y a las frecuencias asignadas a la entidad.
V. Capacidad del sistema: el ancho de banda (AB) será determinado por los requerimientos del Complejo de Seguridad.Debe tener una disponibilidad de al menos 99.991% (que equivale a 47.304 minutos/año).
VI. Calidad del servicio: la estación radio eléctrica debe soportar las siguientes normas para proveer la calidad de servicio: IEEE 802.1p, IP ToS de acuerdo con RFC791 y DSCP de acuerdo con RFC2474. Con un manejo mínimo de cuatro colas de prioridad.
VII. Dependiendo del diseño de la red inalámbrica, se debe utilizar una VLAN (Red de Área Local Virtual, por sus siglas en inglés) que esté certificada por

un organismo internacional. Habrá VLAN para cada uno de los servicios (video, voz, administración, etc.).

VIII. Gestión: de acuerdo a las necesidades de gestión de la estación radio eléctrica, se podrá elegir uno o más de los siguientes protocolos orientados a conexión de gestión de los equipos: HTTPS/SSH/SNMP V2c o V3.

IX. No se permiten los protocolos TELNET y HTTP; en caso de que el equipo los soporte, serán deshabilitados.

X. La estación radio eléctrica se debe configurar y gestionar desde la radio base y remotamente, además de reportar los parámetros operativos más importantes como son RSSI, *throughput*, estado del enlace, como mínimo. Se debe permitir deshabilitar las funciones de configuración y gestión.

XI. Potencia de transmisión: ésta se definirá en el estudio previo de enlace.

XII. Actualización de *software*: las estaciones radio eléctricas deben tener la característica de actualización de *firmware* de manera local y remota de forma gratuita, a través de los protocolos TFTP/FTP.

XIII. Cifrado de datos: el video y los datos de las terminales finales serán cifrados usando alguno de los siguientes algoritmos DES, AES 128 bits y/o 256 bits.

XIV. Interfaz *GigaEthernet* o *Ten GigaEthernet*: opcional la capacidad de recibir corriente eléctrica (usando una norma certificada por un organismo internacional) (PoE) a través del puerto *Ethernet*.

XV. Debe contar con corrección de errores y mecanismo de retransmisión automática a nivel RF: *Forward Error Correction* (FEC).

XVI. Regulación: la estación radioeléctrica debe estar homologada ante el Instituto Federal de Telecomunicaciones (IFT).

XVII. Alimentación Eléctrica: 110 VCA – 120 VCA a 50 Hz - 60 Hz o vía puerto *Ethernet* (*Power over Ethernet* PoE) en cumplimiento con una norma certificada por un organismo internacional.

XVIII. Certificación de índice de protección para exteriores: de acuerdo a las condiciones ambientales de sitio, la estación radioeléctrica debe cumplir con alguno de los siguientes índices de protección: IP 65/66/67.

XIX. Debe incluir todos los accesorios necesarios para su correcta instalación.

XX. Posibilidad de crecimiento del sistema sin necesidad de licencias adicionales.

XXI. Alineación de la estación radio eléctrica: se recomienda contar con una herramienta de alineación entre las antenas, por ejemplo, tono audible.

XXII. Capacidad de enrutamiento: esto depende de los requerimientos de diseño.

XXIII. Protocolos de enrutamiento: dependiendo de los requerimientos de diseño, en caso de requerir un protocolo de ruteo dinámico abierto se puede usar RIPv2/OSPF o sus versiones superiores.

XXIV. Temperatura de operación: los equipos deben operar en un rango de temperatura de -35 °C a 60 °C. Este parámetro puede variar de acuerdo a la región de instalación.

XXV. Se recomienda la posibilidad de contar con sincronización de la antena vía GPS/SNTP.

XXVI. Humedad de operación: la aplicación de este parámetro depende de la zona geográfica en la que se instale el sistema.

b) Estación radio eléctrica PMP: la capacidad del enlace en Mbps dependerá del ancho de banda determinado por los requerimientos del Complejo de Seguridad (número de suscriptores y del ancho de banda que demanden de acuerdo a los requerimientos del Complejo de Seguridad).

I. En el enlace de microondas se puede utilizar LOS/OLOS/NLOS (Línea de Vista /Línea de Vista Obstruida/ Sin Línea de Vista) en terminal PTP (Punto a Punto) y compatible con terminal PMP (Punto Multi Punto). Se podrá escoger cualquier tipo, de acuerdo al estudio de enlace.

II. Frecuencias asignadas por el Instituto Federal de Telecomunicaciones (IFT) para uso exclusivo de seguridad pública en los tres órdenes de gobierno. No se permite el uso de frecuencias libres o de otro tipo de asignaciones.

III. Tipo de antena: sectorial/haz amplio.

IV. Método de multiplexaje: TDM/OFDM (dependiendo de las necesidades del usuario se podrá utilizar MIMO). El método de multiplexaje debe ser el mismo en todos los elementos del enlace de microondas (PTP y suscriptores).

V. Esquema de duplexaje: TDD/FDD. El esquema de duplexaje debe ser el mismo en todos los elementos del enlace de microondas (PTP y suscriptores).

VI. Modulación adaptativa: el equipo de radio frecuencia debe soportar como mínimo los siguientes tipos de modulación BPSK, QPSK, 16QAM, 64QAM.

VII. Ancho del canal: se podrá usar cualquier ancho de canal cumpliendo la regulación aplicable por usuario y a las frecuencias asignadas a la entidad.

VIII. Capacidad del sistema: el ancho de banda (AB) será determinado por los requerimientos del Complejo de Seguridad.

IX. Enlace inalámbrico PTP: en este caso debe ser de alta capacidad y debe tener una disponibilidad de al menos el 99.991% (que equivale a 47.304 minutos/año).

X. Calidad del servicio: la estación radio eléctrica debe ser regida por normas certificadas por organismos internacionales para proveer la calidad de servicio y utilizar frecuencias asignadas a seguridad pública y/o concesionadas al Estado.

XI. Dependiendo del diseño de la red inalámbrica, en caso de requerir el uso de VLAN debe estar certificada por un organismo internacional. Habrá VLAN para cada uno de los servicios (video, voz, administración, etc.).

XII. Gestión: de acuerdo a las necesidades de gestión de la estación radio eléctrica se podrá elegir uno o más de los siguientes protocolos orientados a conexión de gestión de los equipos: HTTPS/SSH/SNMP V2c o V3. No se permiten los protocolos TELNET y HTTP, en caso de que el equipo los soporte, serán deshabilitados.

XIII. La estación radio eléctrica del enlace PTP de alta capacidad se debe configurar y gestionar desde la radio base y remotamente, además de reportar los parámetros operativos más importantes como son RSSI, *throughput*, estado del enlace como mínimo. Se debe permitir deshabilitar las funciones de configurar y gestionar.

XIV. Potencia de transmisión: ésta se definirá en el estudio previo de cálculo de enlace.

XV. Actualización de *software*: las estaciones radio eléctricas deben tener la característica de actualización de *firmware* de manera local y remota de forma gratuita, a través de los protocolos TFTP/FTP.

XVI. Cifrado de datos: el video y los datos de las terminales finales del PMI serán cifrados usando alguno de los siguientes algoritmos DES, AES 128 bits y/o 256 bits.

XVII. Interfaz *Giga Ethernet* o *Ten Giga Ethernet*. Opcional la capacidad de recibir corriente eléctrica (usando una norma certificada por un organismo internacional) a través del puerto *Ethernet*.

XVIII. Debe contar con corrección de errores y mecanismo de retransmisión automática a nivel RF: *Forward Error Correction* (FEC).

XIX. Regulación: la estación radioeléctrica debe estar homologada ante el Instituto Federal de Telecomunicaciones (IFT).

XX. Certificación de índice de protección para exteriores: de acuerdo a las condiciones ambientales de sitio, la estación radioeléctrica debe cumplir con alguno de los siguientes índices de protección: IP 65/66/67.

XXI. Debe incluir todos los accesorios necesarios para su correcta instalación.

XXII. Posibilidad de crecimiento del sistema sin necesidad de licencias adicionales.

XXIII. Alineación de la estación radio eléctrica: se recomienda contar con una herramienta de alineación entre las antenas, por ejemplo, tono audible.

XXIV. Capacidad de enrutamiento: esto depende de los requerimientos de diseño.

XXV. Protocolos de enrutamiento: dependiendo de los requerimientos de diseño, en caso de requerir un protocolo de ruteo dinámico abierto se puede usar RIPv2/OSPF o sus versiones superiores.

XXVI. Temperatura de operación: los equipos deben operar en un rango de temperatura de -35 °C a 60 °C. Este parámetro puede variar de acuerdo a la región de instalación.

XXVII. Se recomienda la posibilidad de tener sincronización de la antena vía GPS/SNTP.

XXVIII. Humedad de operación: la aplicación de este parámetro depende de la zona geográfica en la que se instale el sistema.

c) Estación radio eléctrica PTP de alta capacidad, la capacidad del enlace en Mbps dependerá del ancho de banda calculado a partir de los puntos de agregación (se definirá el ancho de banda de acuerdo a los requerimientos del Complejo de Seguridad).

I. Líneas de vista LOS/OLOS/NLOS en terminal PTP (Punto a Punto) y compatible con terminal PMP (Punto Multi Punto). Se podrá escoger cualquier tipo, de acuerdo al estudio de enlace.

II. Frecuencias asignadas por el Instituto Federal de Telecomunicaciones (IFT) para uso exclusivo de seguridad pública en los tres órdenes de gobierno. No se permite el uso de frecuencias libres o de otro tipo de asignaciones.

III. Método de multiplexaje: TDM/OFDM.

IV. Modulación adaptativa: el equipo de radio frecuencia debe soportar como mínimo los siguientes tipos de modulación BPSK, QPSK, 16QAM, 64QAM.

V. Ancho del canal: se podrá usar cualquier ancho de canal cumpliendo la regulación aplicable por usuario y a las frecuencias asignadas a la entidad.

VI. Capacidad del sistema: el ancho de banda (AB) será determinado por los requerimientos del Complejo de Seguridad.

VII. Enlace inalámbrico punto-punto: en este caso debe ser de alta capacidad y debe tener una disponibilidad de al menos del 99.991% (que equivale a 47.304 minutos/año).

VIII. Calidad del servicio: la estación radio eléctrica debe soportar normas certificadas por organismos internacionales para proveer la calidad de servicio.

IX. Dependiendo del diseño de la red inalámbrica, en caso de requerir el uso de VLAN (Red de Área Local Virtual, por sus siglas en inglés) debe estar

certificado por un organismo internacional. Habrá VLAN para cada uno de los servicios (video, voz, administración, etc.)

X. Gestión: de acuerdo a las necesidades de gestión de la estación radio eléctrica se podrá elegir uno o más de los siguientes protocolos orientados a conexión de gestión de los equipos: HTTPS/SSH/SNMP V2c o V3. No se permiten los protocolos TELNET y HTTP, en caso de que el equipo los soporte, serán deshabilitados.

XI. La estación radio eléctrica del enlace punto a punto de alta capacidad se debe configurar y gestionar desde la radio base y remotamente, además de reportar los parámetros operativos más importantes como son RSSI, *throughput*, estado del enlace como mínimo. Se debe permitir deshabilitar las funciones de configurar y gestionar.

XII. Potencia de transmisión: ésta se definirá en el estudio de enlace.

XIII. Actualización de *software*: las estaciones radio eléctricas deben tener la característica de actualización de *firmware* de manera local y remota de forma gratuita, a través de los protocolos TFTP/FTP.

XIV. Cifrado de datos: el video y los datos de las terminales finales del PMI serán cifrados usando alguno de los siguientes algoritmos DES, AES 128 bits y/o 256 bits.

XV. Interfaz *Giga Ethernet* o *Ten Giga Ethernet*. Opcional la capacidad de recibir corriente eléctrica (usando una norma certificada por un organismo internacional) a través del puerto *Ethernet*.

XVI. Debe contar con corrección de errores y mecanismo de retransmisión automática a nivel RF: *Forward Error Correction* (FEC).

XVII. Regulación: la estación radioeléctrica debe estar homologada ante el Instituto Federal de Telecomunicaciones (IFT).

XVIII. Alimentación Eléctrica: 110 VCA – 120 VCA, 50 Hz - 60 Hz o vía puerto *Ethernet* en cumplimiento con una norma certificada por un organismo internacional.

XIX. Alimentación Eléctrica: 110 VCA – 120 VCA, 50 Hz - 60 Hz o vía puerto *Ethernet* en cumplimiento con una norma certificada por un organismo internacional.

XX. Certificación de índice de protección para exteriores: de acuerdo a las condiciones ambientales del sitio, la estación radioeléctrica debe cumplir con alguno de los siguientes índices de protección: IP 65/66/67.

XXI. Debe incluir todos los accesorios necesarios para su correcta instalación.

XXII. Posibilidad de crecimiento del sistema sin necesidad de licencias adicionales.

XXIII. Alineación de la estación radio eléctrica: se recomienda contar con una herramienta de alineación entre las antenas, por ejemplo, tono audible.

XXIV. Capacidad de enrutamiento: esto depende de los requerimientos de diseño.

XXV. Protocolos de enrutamiento: dependiendo de los requerimientos de diseño, en caso de requerir un protocolo de ruteo dinámico abierto se pueden usar RIPv2/OSPF o sus versiones superiores.

XXVI. Temperatura de operación: los equipos deben operar en un rango de temperatura de-35 °C a 60 °C. Este parámetro puede variar de acuerdo a la región de instalación.

XXVII. Se recomienda la posibilidad de tener sincronización de la antena vía GPS/SNTP.

XXVIII. Humedad de operación: la aplicación de este parámetro depende de la zona geográfica en la que se instale el sistema.

d) Enrutador y Conmutador de Datos del Complejo de Seguridad y de otras entidades para conectarse a la red estatal.

De requerirse el conmutador de datos en las otras instancias podrá ser un equipo no administrable o administrable, dependiendo de los requerimientos del diseño. El conmutador de datos y el enrutador deben cumplir, en caso de que sean administrables, con protocolos y normas establecidos por la IEEE y la IETF.

Para el enrutador y de acuerdo a los requerimientos del diseño, se escogerán los protocolos que apliquen.

I. Puertos o interfaces de tecnología *Giga Ethernet* o *Ten Giga Ethernet*.

II. Los enrutadores podrán soportar MPLS de acuerdo al RFC 6178, RFC 6790 o *Frame Relay* certificado por un organismo internacional, dependiendo de los requerimientos del sistema.

III. Soporte a protocolos IPv4 e IPv6: debe cumplir con los RFC 791, 1349 y 6864 para IPv4 y para el caso de IPv6 se deben cumplir los RFC 2460 y RFC 5722.

IV. Direcciones primarias y/o secundarias por interfaz o VLAN (debe estar certificado por un organismo internacional): los equipos con capacidades de enrutamiento deben poder soportar el uso de direcciones IP en sus interfaces o en VLAN por puerto. Es opcional que además de poder asignar una primera dirección IP, se puedan asignar direcciones IP secundarias extra, esto depende del diseño o requerimientos.

V. Rutas estáticas: los equipos con capacidades de enrutamiento deben tener la posibilidad de configurar manualmente rutas para llenar su tabla de enrutamiento.

VI. Protocolo de ruteo dinámico RIPv2 y OSPF para IPv4 e IPv6: el protocolo de ruteo dinámico RIP debe cumplir con lo especificado en el RFC 2453 y el RFC 2080 y es recomendable para redes pequeñas cuando subredes están a no más de 15 enrutadores de separación. Para el caso de OSPF debe cumplir con el RFC 2328 y el RFC 5340 y se recomienda cuando el número de subredes supera a las limitantes de RIP v2.

VII. DHCP: debe cumplir con el RFC 2131 y el RFC 3046. Un equipo con capacidades de enrutamiento puede ser un servidor DHCP, cliente DHCP y/o DHCP de reenvío. El servidor DHCP permite asignar direcciones IP de *host* a los clientes DHCP. El cliente DHCP en un enrutador permite que a sus interfaces se les asigne una dirección IP por medio de un servidor DHCP. El DHCP de reenvío manda las peticiones de clientes DHCP al servidor DHCP. El servidor DHCP debe poder asignar direcciones fijas por MAC y configurar el tiempo de renta de parámetro IP.

VIII. IGMP: debe cumplir con el RFC 2236. Este protocolo permite que todos los grupos *multicast* sean anunciados a los protocolos de ruteo *multicast*.

IX. PIM-SM: debe cumplir con el RFC 7761. Permite el ruteo *multicast*.

X. DVMRP: debe cumplir con los RFC 1075 y 2715. Permite el enrutamiento con direcciones IP *multicast*.

XI. SNTP: debe cumplir con el RFC 4330. Usado cuando se requiere que los equipos sincronicen su reloj tomándolo de un servidor de tiempo.

XII. QoS DSCP/Precedencia IP: protocolo que utiliza el marcado de paquetes IP en el campo TOS del encabezado que permite darle un tratamiento para priorizar tramas.

XIII. Soporte a VLAN a través de una norma certificada por un organismo internacional, que describa el funcionamiento, formatos de paquetes y parámetros de las VLAN.

XIV. Soporte a mecanismos de control de flujo, para así evitar congestionamientos a través de un protocolo certificado por un organismo internacional.

XV. SNMPv2c/v3: protocolo que permite el monitoreo de dispositivos de red.

XVI. SSHv2: protocolo que permite el acceso remoto a un equipo de red de forma segura vía línea de comandos.

XVII. FTP/TFTP Cliente: protocolos que permiten la transferencia de archivos. Usuales para actualizar *firmware* o archivos de configuraciones, o para respaldarlos.

XVIII. *Syslog*: protocolo que permite el almacenamiento de mensajes de eventos en servidores remotos.

XIX. RMON: protocolo que da un conjunto de variables o MIB para el monitoreo de red, así como un protocolo para la consulta de estos MIB.
XX. HTTPS: protocolo basado en hipertexto para el monitoreo de un dispositivo de red de forma segura. A diferencia de HTTP la transmisión de datos viaja de forma cifrada gracias a la implementación de los protocolos SSL y TLS.
XXI. No se permite el uso de Telnet y HTTP, en caso de que el equipo tenga implementados estos protocolos, deben ser deshabilitados. Las aplicaciones aquí recomendadas son para fines de administración y actualización de equipo.
XXII. El equipo debe soportar actualizaciones de *firmware* vía remota y local.

Para el conmutador de datos y de acuerdo a los requerimientos del diseño, se escogerán los protocolos que apliquen.

I. Puertos o interfaces de tecnología *Giga Ethernet* o *Ten Giga Ethernet*.
II. Soporte a protocolos IPv4 e IPv6: debe cumplir con los RFC 791, 1349 y 6864 para IPv4 y para el caso de IPv6 se deben cumplir los RFC 2460 y RFC 5722.
III. Direcciones primarias y/o secundarias por interfaz o VLAN (debe estar certificado por un organismo internacional): los equipos con capacidades de enrutamiento deben poder soportar el uso de direcciones IP en sus interfaces o en VLAN por puerto. Es opcional que, además de poder asignar una primera dirección IP, se puedan asignar direcciones IP secundarias extra, lo que depende del diseño o requerimientos.
IV. IGMP: debe cumplir con el RFC 2236. Este protocolo permite que todos los grupos *multicast* sean anunciados e identifiquen sus miembros en los puertos de un conmutador de datos.
V. SNTP: debe cumplir con el RFC 4330. Usado cuando se requiere que los equipos sincronicen su reloj tomándolo de un servidor de tiempo.
VI. QoS DSCP/Precedencia IP: protocolo que utiliza el marcado de paquetes IP en el campo TOS del encabezado que permite darle un tratamiento para priorizar tramas.
VII. Soporte a VLAN a través de una norma certificada por un organismo internacional, que describa el funcionamiento, formatos de paquetes y parámetros de las VLAN.
VIII. Soporte a mecanismos de control de flujo para así evitar congestionamientos a través de un protocolo certificado por un organismo internacional.
IX. Se permite utilizar un método de capa dos del modelo OSI para marcar y dar tratamiento a tramas para fines de calidad de servicio, certificado por un organismo internacional.

X. Se permite utilizar un mecanismo para suministrar energía eléctrica a través de los puertos de *Ethernet*; este mecanismo debe estar certificado por un organismo internacional.
XI. Se permite utilizar mecanismos que regulen el ahorro de energía; este mecanismo debe estar certificado por un organismo internacional.
XII. Soporte a mecanismos de control de flujo para así evitar congestionamientos a través de un protocolo certificado por un organismo internacional.
XIII. SNMPv2c/v3: protocolo que permite el monitoreo de dispositivos de red.
XIV. SSHv2: protocolo que permite el acceso remoto a un equipo de red de forma segura vía línea de comandos.
XV. FTP/TFTP Cliente: protocolos que permiten la transferencia de archivos. Usuales para actualizar *firmware* o archivos de configuraciones, o para respaldarlos.
XVI. Syslog: protocolo que permite el almacenamiento de mensajes de eventos en servidores remotos.
XVII. RMON: protocolo que da un conjunto de variables o MIB para el monitoreo de red así como un protocolo para la consulta de estos MIB.
XVIII. HTTPS: Protocolo basado en hipertexto para el monitoreo de un dispositivo de red de forma segura. A diferencia de HTTP la transmisión de datos viaja de forma cifrada gracias a la implementación de los protocolos SSL y TLS.
XIX. No se permite el uso de Telnet y HTTP, en caso de que el equipo tenga implementado estos protocolos, deben ser deshabilitados. Las aplicaciones aquí recomendadas son para fines de administración y actualización de equipo.
XX. El equipo debe soportar actualizaciones de *firmware* vía remota y local.

5.1.5.4 Parámetros de los Dispositivos de la Red de Fibra Óptica

El conmutador de datos de los Complejo de Seguridad y los de otras instancias conectadas a la red estatal deben ser administrables. El conmutador de datos y el enrutador deben cumplir con protocolos y normas establecidos por la IEEE y la IETF. A continuación, se enlistan los protocolos más usuales. De acuerdo a los requerimientos del diseño, se escogerán los que apliquen.

a) Puertos o interfaces de tecnología *Giga Ethernet* o *Ten Giga Ethernet*.
b) Puertos SFP para realización de enlaces con otros dispositivos de comunicaciones que no estén en las otras dependencias. Deben hacer referencia de la distancia de cada tipo de SFP.

c) Soporte a protocolos IPv4 e IPv6: debe cumplir con los RFC 791, 1349 y 6864 para IPv4; y para el caso de IPv6 se deben cumplir los RFC 2460 y RFC 5722.
d) Direcciones primarias y/o secundarias por interfaz o VLAN (debe estar certificado por un organismo internacional): los equipos con capacidades de enrutamiento deben poder soportar el uso de direcciones IP en sus interfaces o en VLAN por puerto. Es opcional que además de poder asignar una primera dirección IP, se pueda asignar direcciones IP secundarias extra, esto depende del diseño o requerimientos.
e) Rutas estáticas: los equipos con capacidades de enrutamiento deben tener la posibilidad de configurar manualmente rutas para llenar su tabla de enrutamiento.
f) Protocolo de ruteo dinámico RIPv2 y OSPF para IPv4 e IPv6. El protocolo de ruteo dinámico RIP debe cumplir con lo especificado en el RFC 2453 y el RFC 2080 y es recomendable para redes pequeñas cuando subredes están a no más de 15 enrutadores de separación. Para el caso de OSPF debe cumplir con el RFC 2328 y el RFC 5340 y se recomienda cuando el número de subredes supera a las limitantes de RIP v2.
g) DHCP: debe cumplir con el RFC 2131 y el RFC 3046. Un equipo con capacidades de enrutamiento puede ser un servidor DHCP, cliente DHCP y/o DHCP de reenvío. El servidor
   DHCP permite asignar direcciones IP de *host* a los clientes DHCP. El cliente DHCP en un enrutador permite que a sus interfaces se le asigne una dirección IP por medio de un servidor DHCP. El DHCP de reenvío manda las peticiones de clientes DHCP al servidor DHCP.
h) IGMP: debe cumplir con el RFC 2236. Este protocolo permite que todos los grupos *multicast* sean anunciados a los protocolos de ruteo *multicast*, en el caso de los enrutadores, o sean identificados sus miembros en los puertos de un conmutador de datos.
i) PIM-SM: debe cumplir con el RFC 7761. Permite el ruteo *multicast*.
j) DVMRP: debe cumplir con los RFC 1075 y 2715. Permite el enrutamiento con direcciones IP *multicast*.
k) SNTP: debe cumplir con el RFC 4330. Usado cuando se requiere que los equipos sincronicen su reloj tomándolo de un servidor de tiempo.
l) QoS DSCP/Precedencia IP: protocolo que utiliza el marcado de paquetes IP en el campo ToS del encabezado, que permite darle un tratamiento para priorizar tramas.

m) Soporte a VLAN a través de una norma certificada por un organismo internacional, que describa el funcionamiento, formatos de paquetes y parámetros de las VLAN.
n) Soporte a mecanismos de control de flujo para evitar congestionamientos a través de un protocolo certificado por un organismo internacional.
o) Se permite utilizar un método de capa dos del modelo OSI para marcar y dar tratamiento a tramas con fines de calidad de servicio, certificado por un organismo internacional.
p) Se permite utilizar un mecanismo para suministrar energía eléctrica a través de los puertos de *Ethernet*; este mecanismo debe estar certificado por un organismo internacional.
q) Se permite utilizar mecanismos que regulen el ahorro de energía; este mecanismo debe estar certificado por un organismo internacional.
r) SNMPv2c/v3: protocolo que permite el monitoreo de dispositivos de red.
s) SSHv2: protocolo que permite el acceso remoto a un equipo de red de forma segura vía línea de comandos.
t) FTP/TFTP Cliente: protocolos que permiten la transferencia de archivos. Usuales para actualizar *firmware* o archivos de configuraciones, o para respaldarlos.
u) *Syslog*: protocolo que permite el almacenamiento de mensajes de eventos en servidores remotos.
v) RMON: protocolo que da un conjunto de variables o MIB para el monitoreo de red, así como un protocolo para la consulta de estos MIB.
w) HTTPS: protocolo basado en hipertexto para el monitoreo de un dispositivo de red.
x) No se permite el uso de Telnet y HTTP; en caso de que el equipo tenga implementados estos protocolos, deben ser deshabilitados. Las aplicaciones aquí recomendadas son para fines de administración y actualización de equipo.
y) La alimentación de energía eléctrica debe de ser de 110 V a 120 V, a la frecuencia de 50 Hz a 60 Hz.

5.1.5.5 Redes privadas virtuales de las (VPN)

5.1.5.5.1 Uso de las VPN

Las VPN deben usarse para el envío de información desde un Complejo de Seguridad a otro con base en las políticas de seguridad del CS.

5.1.5.5.2 Topologías

Los topologías permitidas para conectarse:

a) **Punto a punto:** un equipo de comunicaciones o seguridad forma la VPN con otro equipo de comunicaciones o seguridad, y los usuarios autorizados y conectados también a los equipos de comunicaciones envían su información a través de la VPN creada.
b) **Multipunto-punto:** un equipo de comunicaciones o seguridad es un servidor de VPN y sus clientes VPN son otros equipos de comunicaciones o seguridad que establecen su propia VPN con el servidor VPN. Los usuarios conectados a estos equipos y autorizados mandan su información a través de la VPN formada.
c) **Remoto:** un equipo de comunicaciones, seguridad o equipo de cómputo tipo servidor son servidores VPN, y los clientes son terminales de usuario final con un cliente VPN. Cada cliente forma su VPN con el servidor VPN. Los usuarios de las terminales finales pueden enviar su información a través de la VPN que crearon.
d) **Multipunto-punto y remoto:** el servidor VPN, que puede ser un equipo de comunicaciones, seguridad o un equipo de cómputo tipo servidor, puede crear una VPN con equipos de comunicaciones, seguridad o terminales de usuario final con software cliente VPN.

5.1.5.5.3 Protocolos

Los protocolos permitidos para la realización de la VPN son los enlistados enseguida, los cuales se pueden usar de manera individual o combinados:

a) IPSec definido por la IETF.
b) L2TP/IPSec definido por la IETF.
c) GRE definido por la IETF.

5.1.5.5.4 Autenticación

Los métodos para la autenticación al momento de establecer una VPN son los enlistados enseguida, los cuales se pueden usar de manera individual o combinados:

a) **Usuario y contraseña:** los cuales se administrarán de acuerdo a las políticas de seguridad del Complejo de Seguridad.

b) **Certificados:** los cuales se administraran de acuerdo a las políticas de seguridad del Complejo de seguridad.
c) **Certificados con contraseña:** Los cuales se administrarán de acuerdo a las políticas de seguridad del Complejo de seguridad.
d) **Por MAC y contraseña:** Los cuales se administraran de acuerdo a las políticas de seguridad del Complejo de Seguridad.
e) **Uso de servidores de autentificación:** se permite el uso de servidores de autentificación RADIUS, TACACS Y TACACS+.
f) **Tarjeta inteligente**.
g) **EAP** en sus diferentes variantes, excepto EAP-MS-CHAP y PAP en sus diferentes versiones.

5.2 Red de Área Local

5.2.1 Objetivo

Definir un marco normativo con los lineamientos necesarios para la correcta planeación, diseño, construcción, puesta en marcha, administración, soporte y mantenimiento de las redes de cableado estructurado de telecomunicaciones para las instalaciones del Complejo de Seguridad, empleando las normas nacionales e internacionales vigentes que garanticen la adecuada operación de la infraestructura de equipos y servicios de voz, video y datos.
Definir características y especificaciones que deben cumplir los equipos de comunicaciones, direccionamiento IP, equipos de seguridad, así como políticas de seguridad para la Red LAN.

5.2.2 Alcance

Las características y especificaciones definidas en este apartado aplican a la infraestructura de telecomunicaciones del Complejo de Seguridad, no es una guía de diseño y debe ser leído por personal capacitado en tecnología de telecomunicaciones.

5.2.3 Campo de aplicación

Complejos de Seguridad.

5.2.4 Descripción de cableado estructurado para equipos de telecomunicaciones

5.2.4.1 Cableado estructurado

5.2.4.1.1 Elementos de un sistema de cableado estructurado

Son considerados elementos de cableado estructurado (SCE) los que a continuación se citan:

a) Bastidor de cableado de edificio (BCE).
b) Cableado vertical o principal.
c) Bastidor de cables de piso (BCP).
d) Cableado horizontal.
e) Área de trabajo.

5.2.4.1.2 Elementos que conecta el cableado vertical o principal

Conecta la conexión principal (CP), la conexión intermedia (CI) y la conexión cruzada (HC) de los cuartos de equipo y de telecomunicaciones de entrada (ver figura II.1); los CI incluirán los distribuidores principales de cables en el edificio, mientras que los HC contemplarán los distribuidores secundarios de cables de piso. El cableado principal debe incluir:

a) Cables principales
b) Conexiones cruzadas intermedias
c) Terminaciones mecánicas, cordones de parcheo usados para conexión cruzada

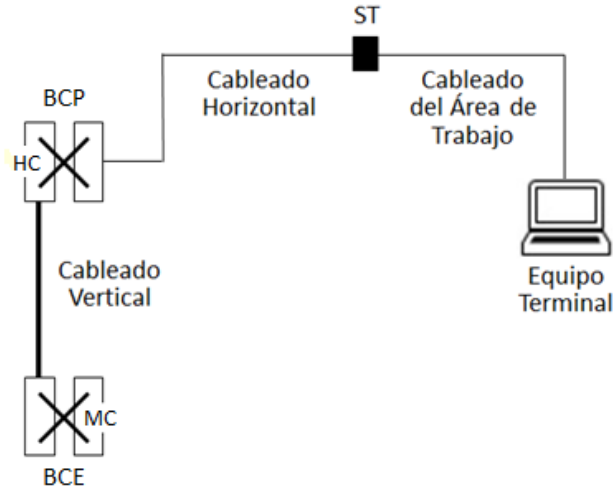


Figura II. 1 Subsistemas de cableado estructurado

5.2.4.1.3 Cableado horizontal

Cableado que se instala desde los distribuidores de cables de piso hasta las salidas de telecomunicaciones (ST) (Ver figura II.1).

5.2.4.1.4 Topología permitida del cableado

El cableado estructurado en edificio del Complejo de Seguridad debe tener una topología en estrella jerárquica y la cantidad, así como el tipo, de subsistemas de

cableado que están incluidos dentro del diseño, dependerán de la ubicación y dimensión de estos, así como de las necesidades del usuario. Ver figura II.2.

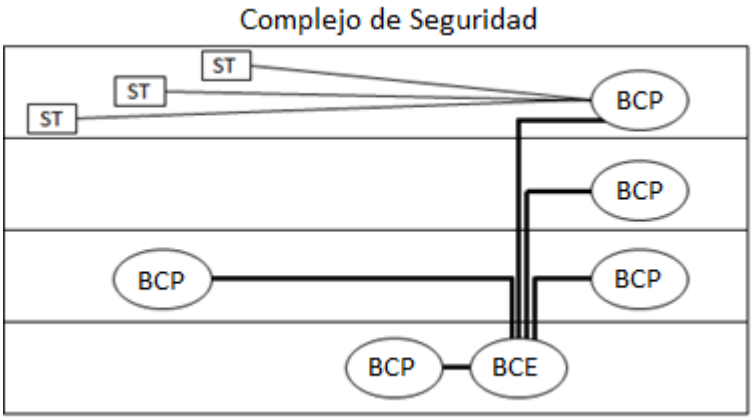


Figura II. 2 Red de cableado estructurado

5.2.4.2 Cableado horizontal

5.2.4.2.1 Distribución horizontal

Debe ser punto a punto iniciando desde el distribuidor de cables de piso, rematando hasta la salida de telecomunicaciones. El área de trabajo debe de ser servida por un cuarto de telecomunicaciones localizado en el mismo piso. Los puentes y empalmes no son permitidos como parte del cableado horizontal de cobre.

5.2.4.2.2 Distancias Horizontales

La distancia permitida en el cable de cobre es de 90metros como máximo y para el caso de fibra óptica, la distancia permitida entre el distribuidor de cables de piso y la salida/conector de telecomunicaciones, debe ser de 150 metros como máximo. Ver figura II.3.

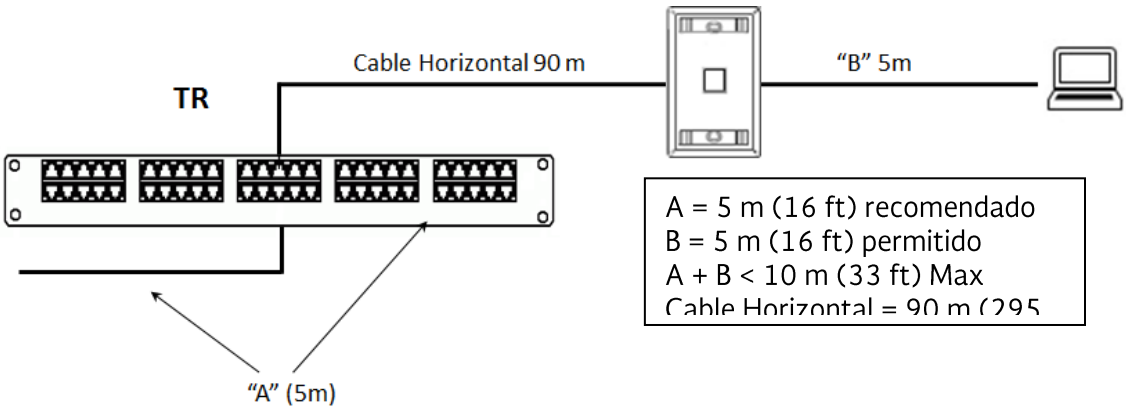


Figura II. 3 Límites de distancias horizontales para cable de cobre UTP

5.2.4.2.3 Cables permitidos para cableado horizontal

El cable de cobre permitido en el cableado de cobre horizontal debe ser categoría 6 o superior y en el caso de la fibra óptica debe ser multimodo. A continuación, se dan características del cable de cobre y fibra óptica permitidos:

a) UTP de 4-pares de 100 Ω (sin blindaje)
b) Blindado de 4-pares de 100 Ω(ScTP)
c) STP-A de 2-pares de 150 Ω (blindado)
d) Fibra óptica de 62.5/125 µm
e) Fibra óptica de 50/125 µm

Los cables de cobre aceptados deben ser resistentes al fuego, contar con retardante de flama para instalaciones eléctricas y poseer forro con propiedades de bajas emisiones de humo, halógenos o equivalente para uso en cuartos con aire acondicionado y cableado principal de edificio u otros espacios.

Los cables de fibra óptica instalados dentro de edificios deben ser resistentes al fuego y deben ser rotulados e instalados con base en lo indicado en los artículos 800-50, 800-51, 800-52, 800-53de la Norma NOM-001-SEDE-1999, poseer forro con propiedades de bajas emisiones de humo, halógenos en cuartos con aire acondicionado y cableado principal de edificio u otros espacios.

Todos los cables de comunicaciones se deben instalar de acuerdo a lo indicado en el artículo 770-53de la Norma Oficial Mexicana NOM-001-SEDE-1999.

5.2.4.2.4 Conectores

5.2.4.2.4.1 Salidas de datos: para salidas de datos el conector debe ser RJ-45 hembra de 4 pares trenzados con una impedancia de 100 Ω categoría 6 o superior y en el caso de fibra óptica multimodo se podrá instalar conectores 568 SC o ST o LC de 50/125 o 62.5/125.

5.2.4.2.4.2 Salidas de voz: para salidas de voz el conector debe ser RJ-45 hembra rematado a cables de cuatro pares de par trenzado de 100 Ω, categoría 6 mejorada y en el caso de fibra óptica multimodo se podrá instalar conectores 568 SC o ST o LC de 50/125 o 62.5/125.

5.2.4.2.5 Cuartos intermedios (uso de áreas individuales en cableado horizontal)

Todas las áreas con instalaciones de cableado horizontal que excedan los límites en distancia máxima permitida deben ser fragmentadas en áreas individuales; cualquier área individual debe ser atendida solamente por un cableado horizontal, y para el cableado principal de servicios de voz debe utilizarse cable multipar categoría 6 o superior.

5.2.4.2.6 Colocación de los bastidores

Los bastidores de cableado horizontal deben instalarse dentro de los cuartos de telecomunicaciones o en el cuarto de equipos, y deben estar aterrizados, al igual que la acometida de servicios externos. Ver figura II.4.

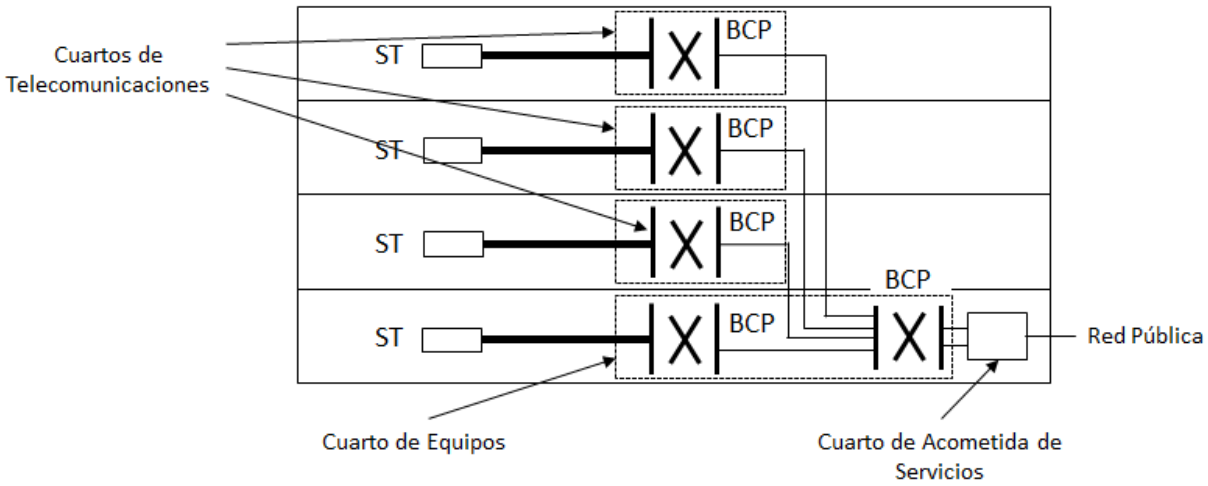


Figura II. 4 Ubicación de los bastidores

5.2.4.2.7 Elementos de interconexión

Para los servicios de voz y datos en el bastidor de cables de piso se recomienda utilizar paneles de parcheo con puertos modulares y con conectores hembra RJ-45 para cable de cobre categoría 6 o superior de 8 posiciones, con capacidad de 12, 24, 32 o 48 puertos, configuración TIA/EIA 568 A o B.
Para llevar a cabo el remate de los cables de fibra óptica que se conectan a un bastidor de cables de piso, se deben utilizar unidades de interfaz de luz, con montaje universal de 48.26cm (19"), con charola integrada con adaptadores SC, ST, LC, MPO.

5.2.4.2.8 Armarios de telecomunicaciones

En caso de existir el espacio necesario para su instalación, se recomienda utilizar armarios de telecomunicaciones con las siguientes características, sin limitar otras que los requerimientos del Complejo de Seguridad especifiquen:

a) Armario de piso
b) Puerta frontal con marco metálico y cristal
c) Puerta posterior con cerradura de seguridad
d) Techo con adaptación para entrada de cables y ventiladores
e) Abertura para ranuras de ventilación en la parte inferior
f) Soportes de nivelación
g) Barra de contactos eléctricos con terminal de conexión a tierra física
h) Juego de barras universales para fijación de equipos frontal y posterior
i) Superficie con acabado resistente a la corrosión
j) Módulo de ventiladores
k) Barra de cobre para puesta a tierra
l) Cuando no exista espacio suficiente para la instalación de un gabinete de piso se recomienda utilizar bastidores de pared o de techo con los siguientes elementos, sin limitar otros que los requerimientos del Complejo de Seguridad especifiquen:
   i. Puerta frontal con marco metálico y cristal
   ii. Techo con adaptación para entrada de cables instalación y ventiladores
   iii. Barra de cobre de puesta a tierra
   iv. Superficie con acabado resistente a la corrosión
   v. Barra de contactos eléctricos con terminal de conexión a tierra física

5.2.4.3 Cableado principal o vertical

5.2.4.3.1 Topología

El cableado principal debe utilizar una topología en forma estrella jerárquica y debe tener como máximo 2 niveles jerárquicos de interconexión, como muestra la figura II.5, con el propósito de evitar la degradación de la señal producida por elementos pasivos y para simplificar la administración de la red de cableado.

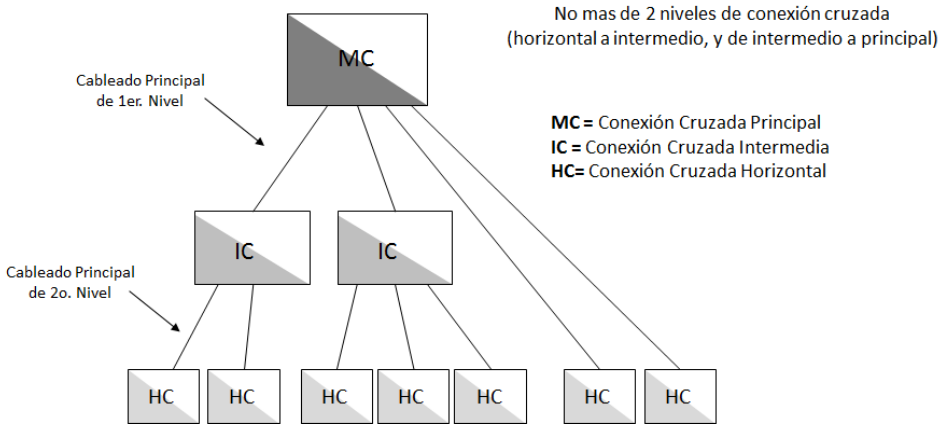


Figura II. 5 Topología de cableado principal

5.2.4.3.2 Redundancia

En caso de que se requiera de alta disponibilidad para poder asegurar la persistencia del servicio, se permitirá instalar el cableado directo entre los bastidores de cables por medio de una trayectoria diferente.

5.2.4.3.3 Cables reconocidos en el cableado principal

El cable de cobre permitido en el cableado horizontal debe ser categoría 6 o superior de acuerdo a los requerimientos del Complejo de Seguridad, y en el caso de la fibra óptica debe ser multimodo o monomodo. Los nuevos Complejos de Seguridad deben usar fibra óptica.

a) UTP 4-pares de 100 Ω calibre 24 AWG para salidas de voz, datos y video(sin blindaje)
b) Blindado 4-pares de 100 Ω para salidas de voz, datos y video (ScTP)
c) STP-A de 2-pares de 150 Ω para salidas de voz, datos y video (blindado)
d) Fibra óptica multimodo de 62.5/125 µm para voz, video y datos
e) Fibra óptica multimodo de 50/125 µm para voz, video y datos
f) Fibra óptica mono-modo 8-10/125 µm

5.2.4.3.4 Características contra el medio de los cables en cableado principal

Los cables de cobre aceptados deben ser resistentes al fuego, contar con retardantes de flama, deben ser rotulados, poseer forro con propiedades de bajas emisiones de humo, halógenos en cuartos con aire acondicionado y cableado principal de edificio u otros espacios.

Todos los cables de comunicaciones se deben instalar de acuerdo a lo indicado en el artículo 770-53 de la Norma Oficial Mexicana NOM-001-SEDE-1999.

En caso de cables instalados bajo tierra se debe incluir:

a) Protección contra humedad y agua
b) Protección contra roedores
c) Protección contra tensión durante la instalación

5.2.4.3.5 Distancias máximas del cableado principal

La tabla II.1 muestra las distancias máximas para fibra óptica en el cableado principal y la figura II.6 muestra que el cableado principal es el segmento que conecta el MC y el IC (letra B) y el segmento que conecta el IC y el HC (letra C). El uso del IC depende de si las distancias a cubrir exceden las mostradas en la tabla II.1.

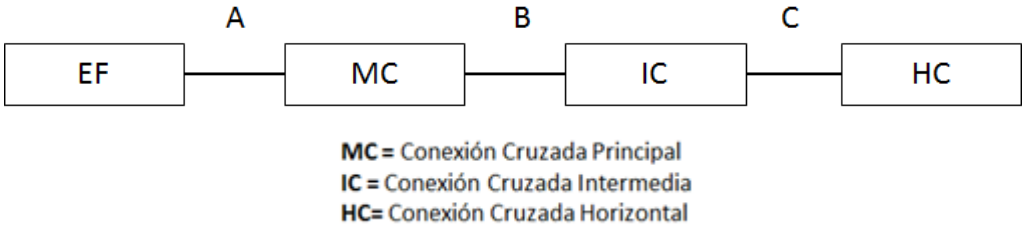


Figura II. 6 Distancias máximas permitidas

Tabla II. 1 Distancias máximas de cableado principal

SFP	Tipo de Fibra Óptica/Longitud de onda	Medida de la Fibra Óptica	Ancho de banda por km (MHz-km)	Distancia máxima de operación
100BaseFx	MMF/1310nm	50	500	5 km
		62.5		2 km
100BaseSx	MMF/850	50	500	550 m
		62.5	200	300 m
100BaseLX	SMF			10km
100BaseEX	SMF			40km
100BaseZX	SMF			80km
1000BaseSX	MMF/850	62.5	160	220 m
			200	275 m
		50	400	500 m
			500	550 m
			2000	1 km
1000BaseLX/ LH	SMF/1310			10km a 20 km

1000BaseEX	SMF/1310			20km a 40km
1000BaseZX	SMF/1550			80 km
10GBaseSR	MMF/850	62.5	160	26 m
			200	33 m
		50	400	66 m
			500	82 m
			2000	300 m
10GBaseLR	SMF/1310			10km
10GBaseER	SMF/1550			40km

5.2.4.3.6 Sistema de tierra de equipos

Las partes metálicas expuestas y no conductoras de corriente eléctrica del equipo fijo que no estén destinadas a transportar corriente, se deben aterrizar con base en lo mencionado en el artículo 250-42, 250-95 NOM-001-SEDE-1999, y las cubiertas metálicas de los cables de comunicación que entren a los edificios deben ser puestas a tierra tan cerca como sea posible del punto de entrada o interrumpirse tan cerca del punto de entrada como sea practicable, por una junta aislada o por un dispositivo equivalente, con base en lo indicado en los artículos 800-33 y 800-40 de la norma anterior.

5.2.4.4 Requerimientos de cables de cobre

5.2.4.4.1 Requerimientos eléctricos

Las características eléctricas del cable deben estar certificadas de acuerdo a una norma internacional.

5.2.4.4.2 Requerimientos de instalación

a) El *hardware* de conexión debe ser de la misma categoría (o mejor) que el cable instalado.
b) Los cables de equipo y cables de parcheo del área de trabajo en el Conector Cruzado Horizontal están limitados a un total de 10m (33 ft).
c) Planear las rutas del cableado para limitar las tiradas horizontales a 90m (295 ft) o menos.
d) Evitar todas las fuentes de EMI (Interferencia Electromagnética) copiadoras o impresoras láser.
e) Si los cables de telecomunicaciones y electricidad van juntos en una vía de acceso deben ser separados por una barrera física.
f) Evitar fuentes de calor, como ductos de calefacción y tuberías de agua caliente.

g) Usar métodos de soporte apropiados cuando se instale cableado suspendido en el techo.
h) La terminación de conectores hembra y macho, así como de paneles de parcheo, debe ser tal que la fuerza no maltrate los cables; no pelar demasiado la cubierta del cable; no permitir que se destrencen los cables, sobre todo para categoría 6 o superior, para evitar las pérdidas por retorno.
i) No jalar el cable con fuerza excesiva debido a que esto podría alterar el aislamiento de los cables y las propiedades de transmisión.
j) No permitir que el cable se doble o enrede cuando se jale de la caja o bobina, la deformación del trenzado de los pares puede alterar el desempeño del cable.
k) Mantener un radio de doblaje mínimo de 4 veces el diámetro del cable UTP y mantener un radio de doblaje mínimo de 8 veces el diámetro del cable STP.
l) Usar los sujetadores de cable holgadamente a intervalos aleatorios y no apretar en exceso los sujetadores de cables, en especial en donde se haga visible el punto de aplastado o deformado.

5.2.4.4.3 Mapa de colores

El código de colores para un cable de 4 pares, debe ser como se muestra en la tabla II.2. Para cables de más de 4 pares, se debe aplicar el código de colores de la norma NMX-I-236-NYCE. La distribución de los cables en el conector hembra es la mostrada en la figura II.7.

Tabla II. 2 Mapa de colores

Número de Par	Mapa de colores	Abreviación
Par1	Blanco-Azul Azul	(B-A) (A)
Par2	Blanco-Naranja Naranja	(B-N) (N)
Par3	Blanco-Verde Verde	(B-V) (V)
Par4	Blanco-Café Café	(B-C) (C)

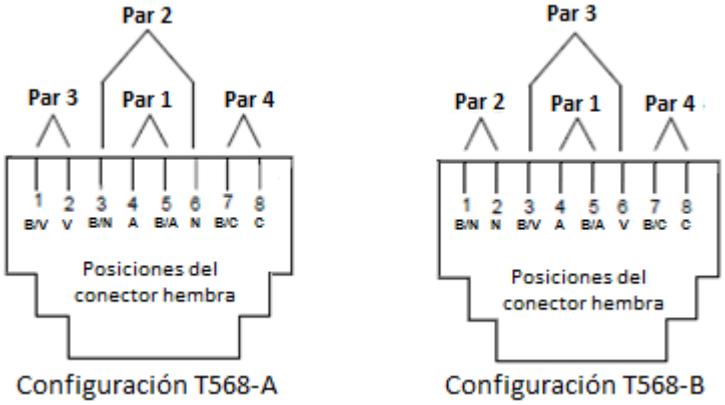


Figura II. 7 Mapas de colores EIA 568-A y 568-B

5.2.4.4.4 Pérdida de paradiafonía (NEXT)

Para cable UTP categoría 6, todas las frecuencias de 0.772 MHz a 100 MHz y todas las pérdidas de paradiafonía del cable, deben cumplir con los valores determinados a partir de la ecuación II.1, o deben tener estos valores certificados por una norma internacional. En caso de cable de categoría superior, estos valores se deben verificar con base en la ecuación que aplica a dicha categoría, o deben estar certificados por una norma internacional.

$$NEXT\ (f) = 47.3 - 15\ \log_{10}(f\ /100)db/100 \qquad (II.1)$$

5.2.4.4.5 Pérdida de paradiafonía por suma de potencia (PSNEXT)

Para cable UTP categoría 6, todas las frecuencias de 0.772 a 100 MHz y todas las pérdidas de paradiafonía por suma de potencia del cable, deben cumplir con los valores determinados a partir de la ecuación II.2, o deben estar certificados estos valores por una norma internacional. En caso de cable de categoría superior, estos valores se deben verificar con base en la ecuación que aplica a dicha categoría o deben estar certificados por una norma internacional.

$$PSNEXT\ (\ f\ )dB\ m_{\ cable} \geq 64 - 15\log / 0.772\ /100 \qquad (II.2)$$

5.2.4.4.6 Atenuación

Para todas las frecuencias de 0.772 a 100 MHz la atenuación será igual o menor a la indicada en la ecuación II.3, la cual aplica para el cable categoría 6, o bien estos

valores deben estar certificados por una norma internacional. Para otra categoría, verificar la fórmula que aplica o estos valores deben estar certificados por una norma internacional.

$$Atenuación_{cable,100m} \leq \left(1.808\sqrt{f}\right) + 0.0017f + \frac{0.2}{\sqrt{f}}(db/100m) \qquad \text{(II.3)}$$

5.2.4.5 Canalización del cableado estructurado

5.2.4.5.1 Elementos fundamentales

En la figura II.8 se ilustra la relación entre las canalizaciones más importantes y los elementos de espacio dentro de un edificio, los cuales se mencionan a continuación.

a)Canalización horizontal.
b)Canalización principal de edificio.
c)Cuarto de Telecomunicaciones.
d)Cuarto de equipos.
e)Área de trabajo.
f) Espacio o cuarto de acometida para servicios externos.
g)Canalización principal para servicios externos.
h)Canalización alterna para servicios externos.

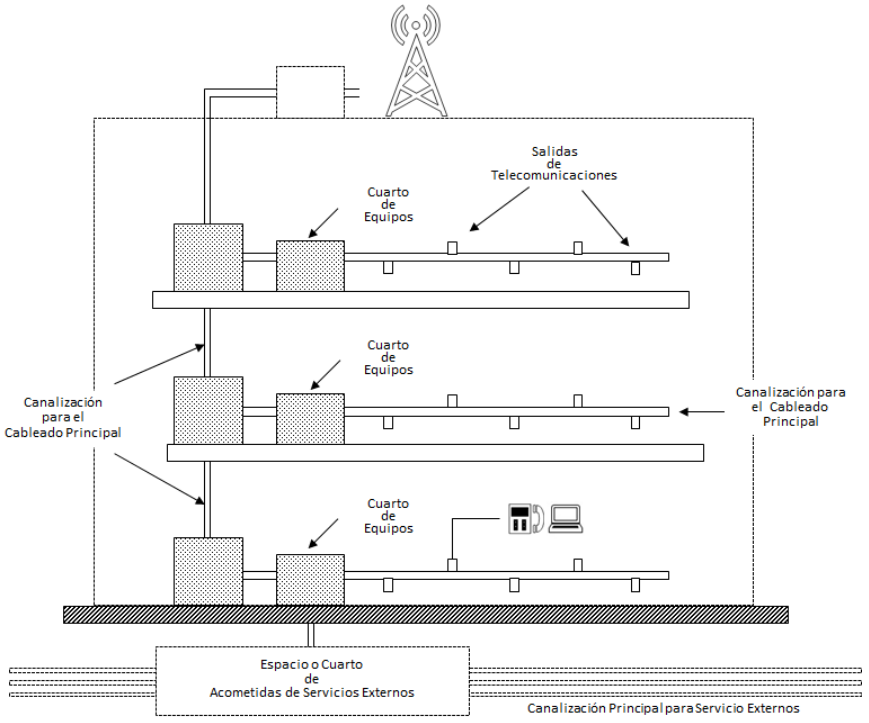


Figura II. 8 Canalizaciones en un edificio

5.2.4.5.2 Canalización horizontal

Las canalizaciones deben estar integradas por varios componentes, como charolas tipo escalerilla, soportes portacables, ductos para cables, tubería de pared delgada, piso celular, ductos bajo el piso, canaleta de piso o perimetral.

a) Canalizaciones bajo piso (ductos bajo piso, piso celular). De uno o dos niveles, los cableados de electricidad y comunicaciones deben de ser distribuidos en ductos o celdas separados.

b) Piso de acceso/elevado. Cuando se utilice el piso de distribución, se debe establecer rutas dedicadas para la distribución del cableado de comunicaciones.

Las canalizaciones o trayectorias horizontales que se encuentran dentro de los edificios deben de ser instaladas en localidades secas para que se proteja a los cables de los niveles de humedad que están más allá del rango de operación previsto y no deben localizarse en el interior de los ductos para los elevadores del edificio.

Las canalizaciones en áreas con demasiado mobiliario y equipo de cómputo, deben ser metálicas y completamente cerradas, con el fin de evitar la fuga de humo, en caso de incendio del cableado.

5.2.4.5.3 Canalización por techos

La canalización horizontal instalada por arriba de los plafones de las áreas de trabajo debe ser montada utilizando cualquiera de los siguientes materiales: escalerilla portacable, tubería de pared delgada, cajas de lámina de acero galvanizado, ducto cuadrado empotrable y canaletas perimetrales de pared o de piso; además debe atender las especificaciones siguientes:

a) Un mínimo de 7.5 cm de separación entre el cable y los paneles techo o plafón.
b) El cableado no debe ser puesto directamente en los paneles del techo o los rieles.
c) Los soportes del cable deben ser localizados en centros de 1220-1525mm.
d) Deben ser establecidas trayectorias dedicadas para la distribución de cableados de telecomunicaciones.
e) Los rieles tipo T del techo podrán ser utilizados para montar apropiadamente los sujetadores de cable, cargados con cables hasta un peso total de 0.7 kg/m, lo cual es equivalente a un grupo de 16 cables UTP de 4-pares categoría 6.

5.2.4.5.4 Tubería

La instalación de la tubería debe ser realizada de acuerdo a la figura II.9.Los tipos de tubería permitidos para la canalización horizontal colocada arriba del plafón de las áreas de trabajo de los Complejos de Seguridad serán los que a continuación se citan:

a) Tubería (tipo *conduit*) de acero galvanizado de pared gruesa o pared delgada.
b) Tubería (tipo *conduit*) de aluminio sin cobre de pared gruesa exterior.

I.- Ninguna sección de tubo conduit debe ser mayor a 30m ni debe contener más de dos curvas de 90° entre puntos o cajas de registro.
II.- El radio de curvatura interno para un *conduit* de 5cm o menos debe ser al menos de 6 veces el diámetro interno.
III.- El tubo *conduit* que tenga fibra óptica instalada en él, debe tener un radio de curvatura mínimo de 10 veces su diámetro interno.
IV.- En tubo *conduit* el porcentaje de llenado debe ser como máximo de 40%.
V.- Los tubos de conduit flexibles no se recomiendan, y si se usan deben ser de no más de 6m por corrida.
VI.- Los tubos de *conduit* que penetren el piso del cuarto de telecomunicaciones deben ser terminados de 1 a 3 pulgadas por encima del piso.

c) Se debe utilizar tubería rígida o flexible de aluminio o policloruro de vinilo (PVC) adherida a las paredes o muros por medio de herrajes, algún tipo de abrazadera o tira de pegamento para derivar de la parte superior del techo, o plafones a las salidas con conectores de telecomunicaciones.

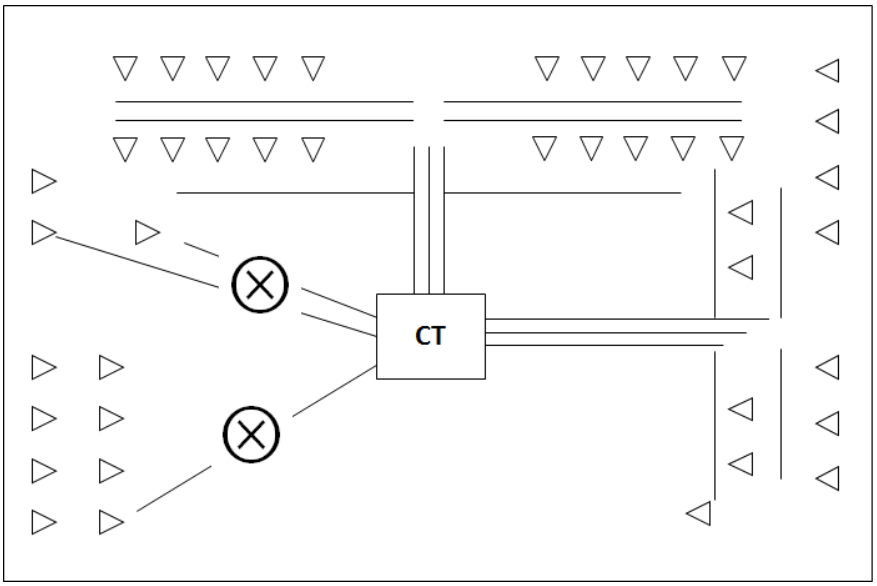


Figura II. 9 Distribución en pisos de acceso elevado

5.2.4.5.4.1 Elementos de instalación

a) **Soportes:** el tubo *conduit* metálico evitará tensiones mecánicas sobre los cables, por lo que debe instalarse y sujetarse como un sistema completo con firmeza, como mínimo cada 3m; además el tubo debe sujetarse a no más de 1m de cada caja de salida, caja de terminales o terminación cualquiera; en caso de que no se permita a 1m se podrá hasta un máximo de 1.5m.

En sitios húmedos, todos los accesorios como pernos, abrazaderas, tornillos, etc., deben ser de un material resistente a la corrosión o estar protegidos por materiales resistentes contra ella.

Todos los extremos cortados del tubo *conduit* se deben acabar de forma apropiada para dejarlos lisos, y cuando el tubo *conduit* se rosque durante su instalación, se debe utilizar una tarraja normal con conicidad.

b) **Salidas de telecomunicaciones entradas del edificio:** se debe reservar espacio suficiente para alojar los cables junto con sus pares de entrada de los proveedores a las salidas de telecomunicaciones, por medio de regletas 110, que estarán formadas por tantos pares de remates como pares constituyan la red de distribución del Complejo de Seguridad. Ver figura II.10.

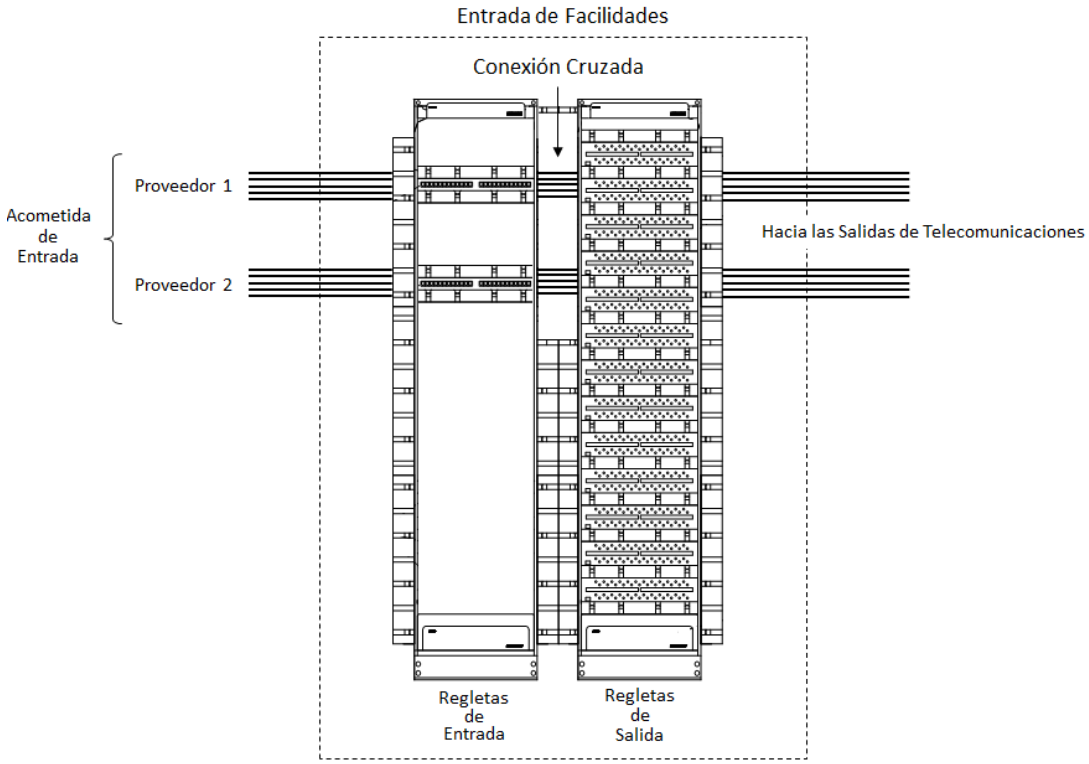


Figura II. 10 Remate de la entrada a salidas de telecomunicaciones

c) **Número de cables por tubo.**

El número máximo de cables que puede albergar un tubo *conduit* es mostrado en la tabla II.3

Tabla II. 3 Número de cables por tubo

Diámetro Comercial (pulgadas)	Número de Cables									
	Diámetro Exterior del Cable (mm)									
	3.3	4.6	5.6	6.1	7.4	7.9	9.4	13.5	15.8	17.8
¾	6	5	4	3	2	2	1	0	0	0
1	8	8	7	6	3	3	2	1	0	0
1 1/4	16	14	12	10	6	4	3	1	1	1
1 1/2	20	18	16	15	7	6	4	2	1	1
2	30	26	22	20	14	12	7	4	3	2
2 1/2	45	40	36	30	17	14	12	6	3	3
3	70	60	50	40	20	20	17	7	6	6
3 1/2	-	-	-	-	-	-	22	12	7	6
4	-	-	-	-	-	-	30	14	12	7

5.2.4.5.4.2 Herrajes para tubo

a) **Coples:** permite unir dos segmentos de tubería y permite que los tubos unidos resistan tanto las fuerzas internas como externas, y las vibraciones.

b) **Codos:** los codos deben estar fabricados del mismo material que el tubo conduit y su radio interno de curvatura debe ser de al menos 6 veces el diámetro interno de la tubería.

c) **Contratuercas:** las uniones entre las cajas de registro y cajas de salida de telecomunicaciones se fijarán con una contratuerca de seguridad para fijar ambos elementos. Ver figura II.11.

d) **Cajas de lámina galvanizada:** se debe usar cajas de registro galvanizadas con perforaciones en las aristas y en la cara posterior.Ver figura II.11.

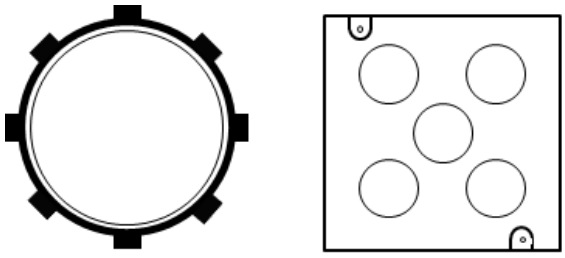


Figura II. 11 Contratuercas y cajas galvanizadas

e) **Cajas para salidas de telecomunicaciones:** se debe usar cajas galvanizadas con perforaciones en las aristas y en la cara posterior.

5.2.4.5.4.3 Escalerillas

Este concepto está orientado a una sencilla instalación debido a que proporciona flexibilidad, seguridad, ventilación, limpieza, economía, así como ganancia en tiempo, sin piezas especiales de derivación. Ver figura II.12.

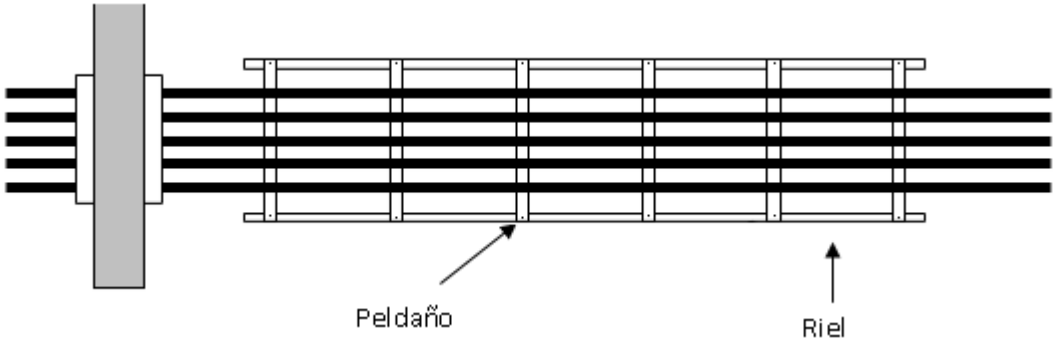


Figura II. 12 Escalerilla para cableado estructurado

a) **Características:** la longitud por cada tramo es de 3.66m, con altura de pared de borde de 8.0cm, capacidad de carga de 80 kg, bordes lisos para evitar las rasgaduras del forro de los cables, con rieles laterales para fijación; sus soportes deben colocarse a una distancia de1.80m, con tramos rectos y en curva para su unión por medio de tornillos, tuercas y rondanas planas.

En ambientes sin filtros de aire se debe contemplar una cubierta para disminuir la electricidad estática y se permitirá extender la escalerilla de forma transversal a través de muros, mamparas o paredes, y en forma vertical a través de losas, pisos o plafones, sellando las aberturas por medio de un material que sea retardante al fuego.

El espaciamiento entre una losa y la escalerilla, al igual que entre escalerillas, debe ser al menos de 50cm y se deben formar grupos de cables abrazados firmemente a los peldaños por medio de cintillos de plástico y velcro, que ayuden a formar los buses de cables que en conjunto no deben superar el 50% del área interior de la escalerilla, además se debe contemplar un sistema de puesta tierra.

Nota: Se podrá permitir un 5% de tolerancia de las dimensiones especificadas.

b) **Materiales de fabricación:** deben ser fabricadas de acero galvanizado y acero inoxidable contra la corrosión, aluminio o plástico, en función del sitio en donde se van a colocar.

5.2.4.5.4.4 Ductos con tapa abatible

El ducto cuadrado es un sistema de soporte con tapa rígida metálica, diseñado para soportar y proteger cables de telecomunicaciones en su interior, fabricado con lámina de acero con acabado de pintura electrostática.

a) **Características:** longitud por tramo mínima de 2m a 3.05m, altura de pared de borde de 8.0cm, capacidad de carga de 80 kg, bordes lisos para evitar las rasgaduras del forro de los cables, con rieles laterales para fijación; sus soportes deben colocarse cada 1.50m de distancia, con tramos rectos y en curva para su unión por medio de tornillos, tuercas y rondanas planas. Ver tabla II.4.

   Se permitirá extender de forma transversal a través de muros, mamparas o paredes y en forma vertical a través de pisos o plafones, sellando las aberturas por medio de un material retardante de fuego.

   El espaciamiento entre una losa y el ducto, al igual que entre ductos, debe ser al menos de 50cm, y se deben formar grupos de cables abrazados por medio de cintillos de velcro que puedan deslizarse aún atados a una distancia aleatoria, y que ayuden a formar los buses de cables cuya suma transversal en conjunto no debe superar el 50% del área interior del ducto; se debe asegurar que otros componentes de un edificio, como ductos eléctricos o ductos de aire acondicionado, no restrinjan el acceso al ducto, y se debe contemplar un sistema de puesta tierra.

Nota: Se podrá permitir un 5% de tolerancia en las dimensiones especificadas.

Tabla II. 4 Longitud máxima del tramo de un ducto

Ancho X Altura (mm)	Longitud máxima del tramo(m)
100 x 100	Entre 2 y 3.05
150 x 150	
200 X 200	
250 X 100	
300 X 150	

5.2.4.5.4.5 Canaletas

Dependiendo de los requerimientos del Complejo de Seguridad se permite usar la canaleta para la canalización horizontal, y su uso debe ser en caso de que no se pueda instalar otro tipo de medio de transporte del cableado horizontal. Ver figura II.13.

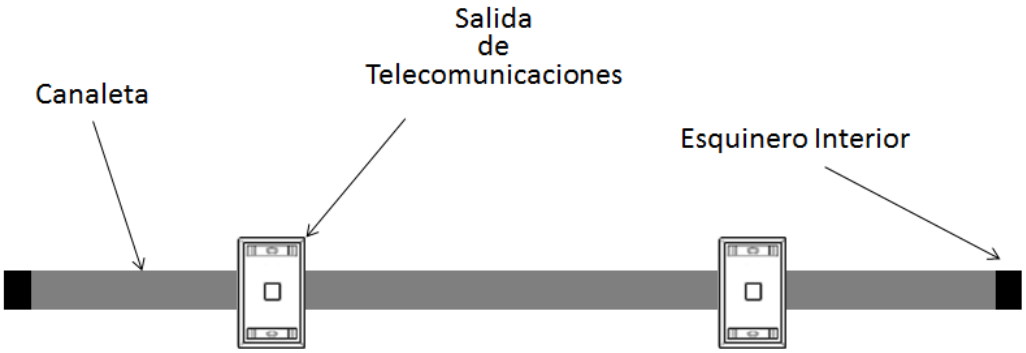


Figura II. 13 Canaleta para cables de telecomunicaciones

a) **Características:** los materiales de las canaletas que se podrán instalar en el Complejo de Seguridad podrán ser policloruro de vinilo (PVC)rígido o flexible, acero galvanizado resistente a la corrosión o aluminio galvanizado, con tramos de 2 a 3 metros de longitud y sección transversal de 2 a 8 pulgadas, bordes lisos para evitar las rasgaduras del forro de los cables, y deben tener accesorios de conexión u otros elementos apropiados, como esquineros exteriores e interiores, tapa final, coples para unión tipo codo plano, derivaciones "T" y "X", en caso de que se requieran. El soporte de las canaletas será por medios mecánicos, como pijas galvanizadas con o sin taquetes.

   Se permitirá extender de forma transversal a través de muros, mamparas o paredes, y en forma vertical a través de pisos o plafones, sellando las aberturas por medio de un material retardante de fuego.

   En conjunto, el cableado en suma transversal no debe superar el 40% del área interior de la canaleta.

5.2.4.5.4.6 Postes para servicios de telecomunicaciones

Los postes de servicio son usados típicamente en ambientes de oficinas abiertas para llevar cables de comunicaciones y eléctricos del techo a las estaciones de trabajo. Ver figura II.14.

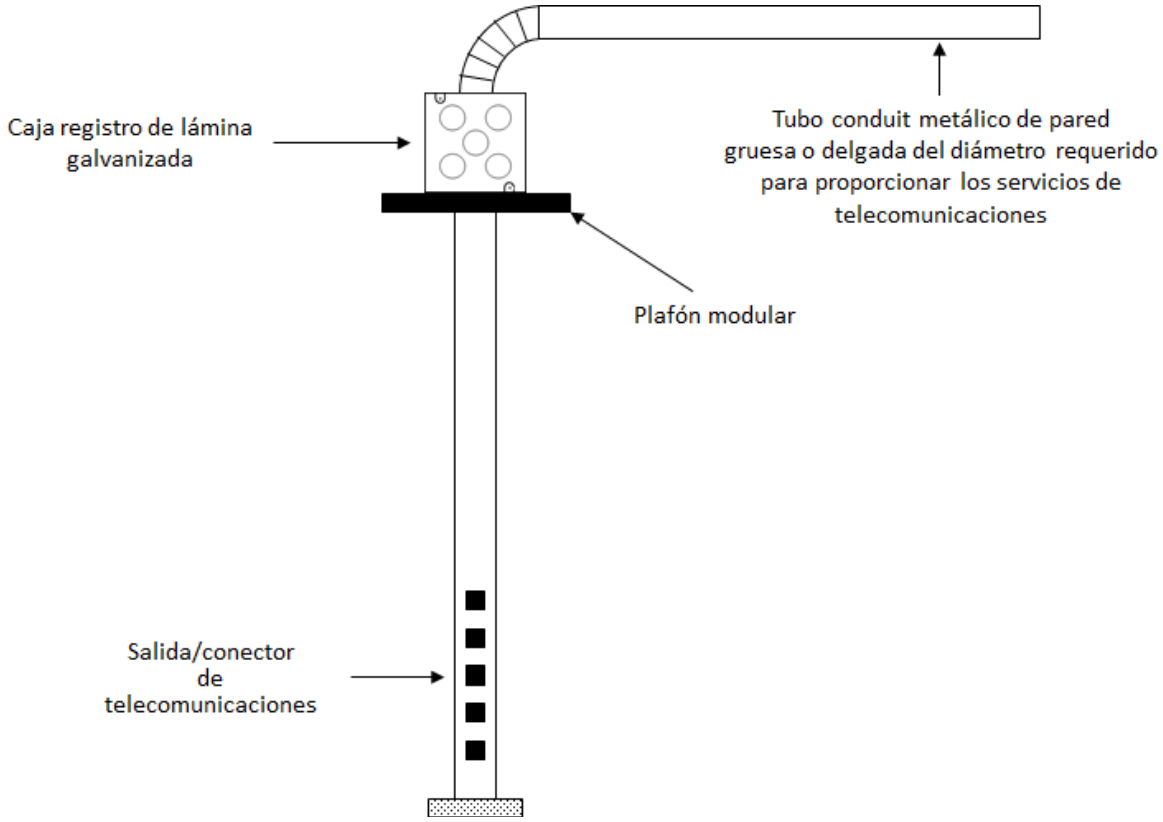


Figura II. 14 Postes de servicio

a) **Características:** los materiales de los postes de servicio podrán ser policloruro de vinilo (PVC) rígido o aluminio anodizado, deben fijarse a la losa o plafón, así como al piso, con el fin de evitar tensiones mecánicas.

5.2.4.5.4.7 Infraestructura de soporte para cableado estructurado

Se deben emplear estructuras rígidas prefabricadas para la protección y soporte de cables o conductores que tendrán los siguientes tipos:

a) Escalerilla
b) Charola de fondo ventilado
c) Charola de fondo sólido
d) Charola de un sólo riel
e) Canastilla
f) Malla para soportar cable.

5.2.4.6 Espacios para equipo y distribución de cableado

5.2.4.6.1 Generalidades

Todos los equipos y elementos de terminación de cableado estructurado, así como los bastidores, se deben instalar en áreas con acceso restringido de un edificio, nombrados cuarto de equipos o cuarto de telecomunicaciones. Su diseño debe considerar voz, video y datos, así como la incorporación de CCTV, alarmas de seguridad y otros sistemas críticos, por lo que un Complejo de Seguridad debe contener al menos un cuarto de equipos o un cuarto de telecomunicaciones.

Dependiendo del tamaño del Complejo de Seguridad, así como de la cantidad y distribución de los servicios de comunicación podrán existir al menos un MDF y varios centros de distribución IDF.

5.2.4.6.2 Cuarto de Telecomunicaciones

El cuarto de telecomunicaciones debe ser un área cerrada dentro del Complejo de Seguridad con un sólo acceso y restringido sólo a personal autorizado, designada para uso exclusivo de equipos asociados con el sistema de bastidores de interconexión asociado y con los sistemas auxiliares requeridos para la operación de equipos.

El cuarto de telecomunicaciones de un Complejo de Seguridad debe proporcionar todas las condiciones necesarias, como son una apropiada ventilación, temperatura interior adecuada, energía eléctrica regulada bajo normas aplicables para el correcto funcionamiento de equipos, así como para el buen desempeño de los elementos pasivos instalados en su interior.

Nota: Cada cuarto de telecomunicaciones debe tener acceso directo a la canalización principal (vertical) del edificio y a la canalización horizontal de las oficinas.

5.2.4.6.2.1 Diseño

Se deben considerar las tomas eléctricas dobles o simples dedicadas a los equipos de telecomunicaciones en la cantidad suficiente que satisfaga los requerimientos del equipo a instalar, cada una en un circuito derivado por separado. Por ningún motivo deben ser compartidas con otras instalaciones eléctricas diferentes a las destinadas al uso de los equipos, y en su caso adicionalmente se deben colocar tomas auxiliares distanciadas 1.8m alrededor del perímetro del cuarto y a una altura apropiada al sitio de instalación.

Las tomas eléctricas dobles podrán colocarse a una altura de 150mm puesto que el cuarto de telecomunicaciones no se considera un espacio público; dicha altura

permitirá además que se pueda aprovechar mejor el espacio al colocar el hardware de conexión a partir de los 300mm por encima del piso terminado, medidos desde el borde inferior del equipo de conexión.

5.2.4.6.2.2 Dimensionamiento

La tabla II.5 muestra los tamaños mínimos del cuarto de telecomunicaciones con base en el número de usuarios. Si se requiere albergar equipos, se debe consultar con el fabricante el tamaño de estos y los requerimientos para su instalación en el cuarto de telecomunicaciones, con el fin de dimensionarlo correctamente.

Tabla II. 5 Dimensiones del Cuarto de Telecomunicaciones

Número de usuarios	Tamaño del cuarto vertical
Hasta 100	$14m^2$
De 101 a 400	$37m^2$
De 401 a 800	$74m^2$
De 801 a 1200	$111m^2$

5.2.4.6.2.3 Interconexión de los cuartos de telecomunicaciones

Cuando existan 2 o más cuartos de telecomunicaciones en un mismo piso de un Complejo de Seguridad, estos pueden ser intercomunicados a través de tuberías *conduit* con un diámetro mínimo de 50mm o por medio de escaleras portacables o ductos cuadrados. Ver figura II.15.

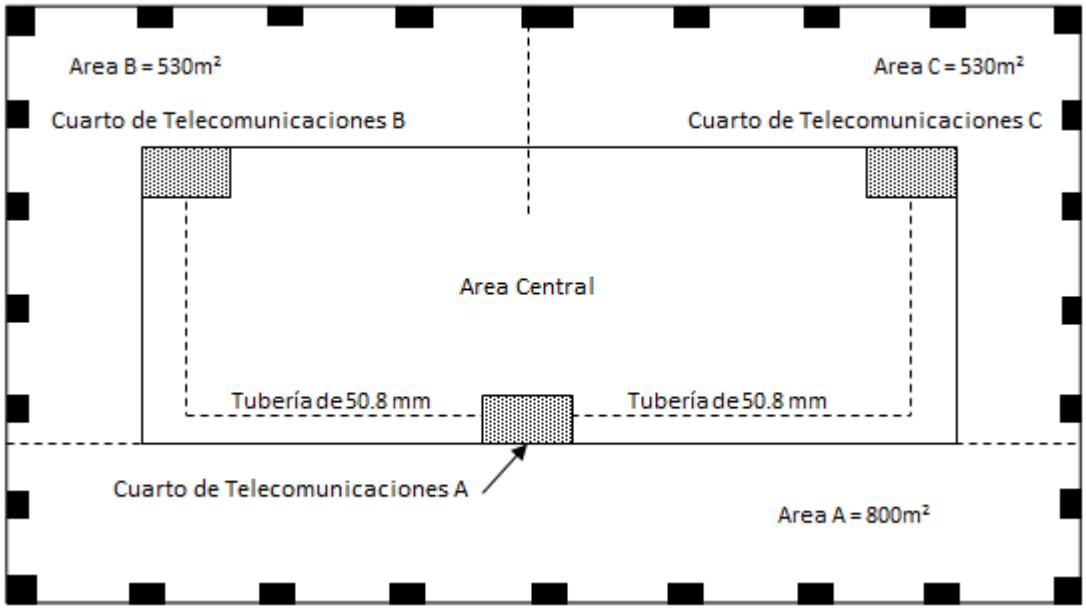


Figura II. 15 Interconexión de cuartos de telecomunicaciones

5.2.4.6.2.4 Sistema de tierra

Las instalaciones de puesta a tierra cumplirán con los reglamentos y normas aplicables, esto también aplica para el cuarto de equipos y la acometida. En el cuarto de telecomunicaciones al menos debe existir una barra de cobre para poner a tierra los equipos, gabinetes o accesorios metálicos de los bastidores de cableado y las canalizaciones metálicas como es la tubería conduit, escalera portacables y los ductos, entre otros. El sistema de tierra debe tener un valor de impedancia en cualquiera de sus puntos de conexión menor de 5 Ω, y cuando se tenga equipo electrónico sofisticado que requiera una resistencia a tierra inferior a 2 Ω, el encargado debe solicitar al proveedor o prestador del servicio que indique el valor de impedancia requerido en los cuartos de telecomunicaciones, donde sea indispensable.

5.2.4.6.2.5 Acondicionamiento

a) Con el fin de facilitar el enrutamiento de los cables horizontales, los cuartos de telecomunicaciones no deben tener techos falsos; esto también aplica para el cuarto de equipos y la acometida.
b) Al menos 3 paredes del cuarto de telecomunicaciones deben estar preparadas para permitir la instalación de equipo sobrepuesto.

c) Se recomienda que la iluminación interior del cuarto de telecomunicaciones sea la necesaria para llevar a cabo la realización de trabajos de instalación y mantenimiento de los sistemas de telecomunicaciones.
d) Se recomienda que los interruptores de luz sean fácilmente accesibles a la entrada del cuarto, esto también aplica para el cuarto de equipos y el cuarto donde está instalada la acometida.
e) La iluminación adecuada es necesaria para instalar y mantener las terminaciones de cable, y las lámparas de iluminación deben montarse en el techo estructural, puesto que no se recomiendan los techos falsos en los cuartos de telecomunicaciones.
f) La puerta debe tener un mínimo de 0.9m de ancho y 2.4m de alto, sin umbral, con bisagras que permitan abrirla hacia afuera, o deslizable hacia ambos lados, y estar provista de una cerradura de seguridad; esto también aplica para el cuarto de equipos y el cuarto donde esté instalada la acometida.
g) Los pisos, paredes y techos deben sellarse para eliminar el polvo, los acabados deben ser de colores claros para mejorar la iluminación del cuarto y esto también aplica para el cuarto de equipos y el cuarto donde esté instalada la acometida.
h) Los muros deben ser anti-inflamables, esto también aplica para el cuarto de equipos y el cuarto donde esté instalada la acometida.
i) El cuarto de telecomunicaciones debe estar conectado a un sistema de corriente eléctrica regulada y a un sistema de respaldo de energía para asegurar el suministro las 24 horas del día los 365 días del año.
j) Al cuarto de telecomunicaciones se le deben asegurar una temperatura y humedad relativa de acuerdo a las especificaciones de los equipos instalados, y en caso de una falla del sistema de temperatura y de humedad relativa se debe conmutar a un sistema de respaldo, para asegurar las condiciones mencionadas las 24 horas día, los 365 días del año.
k) El cuarto de telecomunicaciones debe estar provisto con equipo o un sistema en contra de incendios.

5.2.4.6.2.6 Penetraciones de los cuartos de telecomunicaciones

Las penetraciones al cuarto de telecomunicaciones son necesarias para acceder tanto a las canalizaciones del cableado principal como al horizontal y deben estar selladas de manera adecuada con materiales para evitar el paso de humo y fuego, en caso de un siniestro o incendio.

Para intercomunicar los cuartos de telecomunicaciones que se encuentran alineados uno arriba de otro como se recomienda, se deben utilizar 3 tubos de 100mm como mínimo.

5.2.4.7 Cuarto de equipos

5.2.4.7.1 Generalidades

El cuarto de equipos puede albergar los equipos de telecomunicaciones y contener terminaciones de cable, conexiones cruzadas, equipos de cómputo y de almacenamiento, que se podrán considerar como unidades que deben atender a todo un Complejo de Seguridad, mientras que los cuartos de telecomunicaciones deben atender sólo pisos individuales.

5.2.4.7.2 Diseño

El espacio dedicado al cuarto de equipos debe ser un espacio que no se encuentre limitado por componentes de construcción fijos que impidan su crecimiento a futuro, por lo que es importante considerar para su ubicación evitar cercanía con elevadores, paredes exteriores del Complejo de Seguridad, muros de carga, paredes fijas de soporte y otras áreas mecánicas.
El cuarto de equipos debe tener accesos amplios que permitan la entrada y salida de equipos de grandes dimensiones.

5.2.4.7.3 Acondicionamiento del Cuarto de Equipos

a) Los acabados interiores como paredes, pisos y techo, deben estar sellados para reducir la acumulación de polvo, y se utilizarán colores claros para una mejor iluminación al interior del cuarto de equipos, y para el piso se deben seleccionar materiales con propiedades antiestáticas.

b) La iluminación debe tener un valor mínimo de 500 lux medida a 1 metro arriba de la losa superior, a la mitad de todos los pasillos y entre gabinetes de equipos. La iluminación debe ser controlada mediante uno o más interruptores, localizados cerca de la puerta de entrada al cuarto de equipos.

c) Los interruptores de luz deben estar ubicados de tal forma que sean fácilmente accesibles a la entrada. Las instalaciones de iluminación, así como las instalaciones eléctricas para el cuarto de equipos, deben utilizar tableros eléctricos separados.

d) El cuarto de equipos se debe ubicar por encima del nivel de inundación y estar protegido contra infiltraciones de tuberías de agua y drenaje; un sistema de achique sería de gran utilidad si existe riesgo de ingreso de agua.

e) El cuarto de equipo debe estar conectado a un sistema de corriente eléctrica regulada y a un sistema de respaldo de energía, para asegurar el suministro las 24 horas del día los 365 días del año.

f) Al cuarto de equipos se le deben asegurar su temperatura y humedad relativa de acuerdo a las especificaciones de los equipos instalados, y en caso de una falla del sistema de temperatura y de humedad relativa se debe conmutar a un sistema de respaldo para asegurar las condiciones mencionadas las 24 horas día, los 365 días del año.
g) El cuarto de equipos debe estar provisto con equipo o un sistema en contra de incendios.

5.2.4.7.4 Sistema de tierra

Las instalaciones de puesta a tierra cumplirán con los reglamentos y normas aplicables, esto también aplica para el cuarto de equipos y el cuarto donde está instalada la acometida. En el cuarto de telecomunicaciones al menos debe existir una barra de cobre para poner a tierra los equipos, gabinetes o accesorios metálicos de los bastidores de cableado y las canalizaciones metálicas como es la tubería *conduit*, escalera portacables y los ductos, entre otros. El sistema de tierra debe cumplir con normas internacionales y el valor de impedancia del sistema de tierra en cualquiera de sus puntos de conexión debe ser menor que 5 Ω, y cuando se tenga equipo electrónico sofisticado debe ser inferior a 2 Ω. El encargado debe solicitar al proveedor o prestador del servicio, que indique el valor de impedancia requerida en los cuartos de telecomunicaciones, donde sea indispensable.

5.2.4.7.5 Sistema de aire acondicionado

La temperatura, así como la humedad en el interior del cuarto de equipos deben ser controladas para proporcionar rangos de operación continua de 18° C a 24° C con 30% a 55% de humedad relativa. Se debe tener un sistema alterno de control de temperatura y humedad para garantizar estos parámetros las 24 horas del día, los 365 días del año.

Dependiendo de las condiciones ambientales locales del sitio, se puede requerir que el sistema de aire acondicionado tenga la facilidad de humidificación y deshumidificación del ambiente con un intercambio de aire de $3m^3$ por hora.

La temperatura ambiente y humedad deben medirse a una distancia de 1.5 metros sobre el nivel del piso, en cualquier punto a todo lo largo de un pasillo entre los equipos, y después de que el equipo esté en operación.

Si se utilizan baterías para respaldo de la alimentación eléctrica de los equipos, en caso de una falla de la energía eléctrica primaria, se debe tener una adecuada ventilación en el interior del cuarto de equipos, de tal forma que impida la concentración de gases tóxicos.

5.2.4.7.6 EMI

El cuarto de equipos debe estar separado de fuentes de interferencia electromagnética, y por ningún motivo el cuarto de equipos debe quedar cerca de transformadores eléctricos, motores y generadores de corriente alterna, equipo de rayos "X", transmisores de radar o radio, u otros equipos que generen alta inducción.

5.2.4.7.7 Vibración

La vibración mecánica acoplada a los equipos o a la infraestructura del cableado estructurado puede ocasionar fallas en los servicios de comunicación, tales como falsos contactos, por lo que el cuarto de equipos debe ubicarse lejos de fuentes de vibración.

5.2.4.7.8 Dimensiones

El cuarto de equipos debe tener las dimensiones suficientes para satisfacer los requerimientos de instalación de los equipos, a partir de las especificaciones de los fabricantes de los mismos, y se sugiere una altura mínima de 2.44m, sin obstrucciones de ningún tipo.

5.2.4.7.9 Acceso

Las dimensiones de la puerta de acceso deben tener como medidas mínimas 0.91m de ancho y 2m de altura, además ésta debe estar equipada con una cerradura de alta seguridad.

Si se tiene contemplado para un futuro la instalación de equipo más grande, se recomienda utilizar una puerta doble de 1.82m de ancho por 2.28m de altura.

5.2.4.8 Esquema de administración para la red de cableado estructurado

Los requerimientos de etiquetado son mostrados en la figura II.16 y listados a continuación:

a) Etiquetas a ambos extremos de todos los cables.
b) Etiquetas *Hardware* de Conexión.
c) Etiquetas a las posiciones de terminación de *hardware* de Conexión.
d) Etiquetas a los cuartos de telecomunicaciones y cuartos de equipos.
e) Etiquetas a las vías de acceso (tubo *conduit*, canaletas, escalerillas, bastidores, etc.).

f) Se deben identificar las canalizaciones del cableado de telecomunicaciones y sistemas de tierra.
g) Se deben elaborar y entregar los registros de datos para cada uno de los elementos que conforman las canalizaciones y el cableado de telecomunicaciones de acuerdo a lo especificado, en atención a lo solicitado por el responsable del Complejo de Seguridad.
h) Elaborar planos y diagramas de ruta de las canalizaciones, cableado de telecomunicaciones y sistemas de tierra, de acuerdo a lo especificado por el responsable del Complejo de Seguridad.

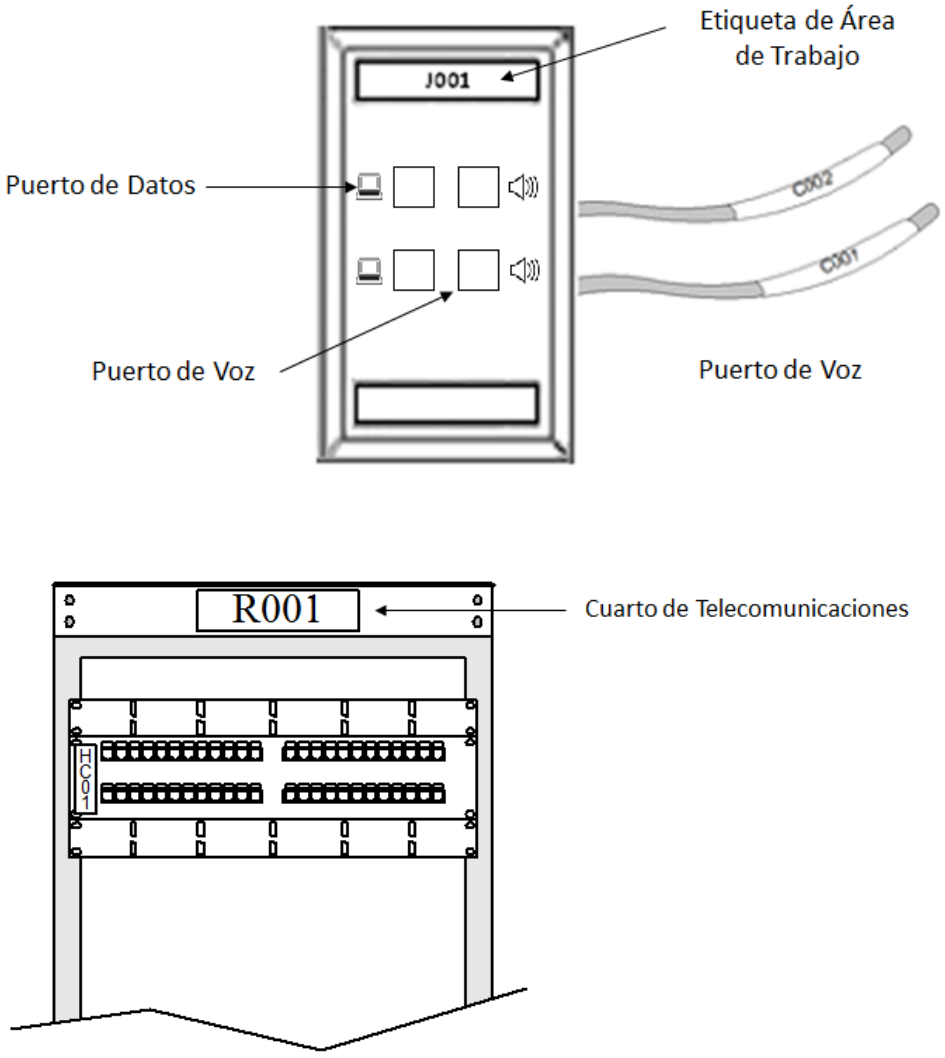


Figura II. 16 Interconexión de cuartos de telecomunicaciones

5.2.4.9 Pruebas para la aceptación de cableado estructurado

5.2.4.9.1 Prueba de integridad de la señal en cable UTP

Los valores que a continuación se enlistan deben estar de acuerdo a la norma internacional que se aplique al tipo de cable de cobre UTP a probar:

a) Mapa de cableado
b) Longitud
c) Atenuación
d) Paradiafonía (NEXT)
e) PSNEXT
f) *FarEnd Cross Talk* (FEXT o Telediafonía)
g) *EqualLevel* FEXT (ELFEXT)
h) Pérdida de Retorno
i) Retraso de Propagación y Diferencia del Retraso

Nota: Atenuación, *Cross-Talk* y Pérdida de Retorno son los puntos más susceptibles a errores por la instalación.

5.2.4.9.2 Pruebas de mapa de cableado

Los valores de que a continuación se enlistan deben estar de acuerdo a la norma internacional que se aplique al tipo de cable de cobre UTP a probar:

a) Continuidad
b) Pares Cruzados o directos
c) Pares Reversos
d) Pares Abiertos

5.2.4.9.3 Pruebas de Longitud Física

a) Puede ser determinada por las marcas de longitud en el cable
b) Puede ser estimada de la longitud eléctrica
c) Derivada del retardo de propagación de las señales
d) La calibración de la Velocidad de Propagación Nominal(NVP) es crítica para mayor exactitud en la distancia
e) Basada en el par con el retardo eléctrico más corto
f) Las diferencias de trenzado muestran diferentes longitudes

5.2.4.9.4 Atenuación

Referida a la pérdida de señal, entre menor sea el valor, mejores serán los enlaces.

5.2.4.9.5 Ruido

Los valores que a continuación se enlistan deben estar de acuerdo a la norma internacional que se aplique al tipo de cable de cobre UTP a probar:

a) ***NEXT*:** el ruido acoplado de un par a otro en el Extremo Cercano (Transmisor), y entre mayor sea su valor medido entre pares de cables es mejor.
b) ***Power Sum Next*:** El ruido acoplado de tres pares energizados hacia el 4o. par en el extremo cercano.
c) ***Farend Cross Talk*:** el FEXT es la medida de señal no deseada acoplada desde un transmisor hacia el extremo lejano dentro depares vecinos, medida en el extremo cercano.
d) ***PSELFEXT*:** FEXT acoplado de tres pares ante el 4o. par, cada uno es compensado por la atenuación para compensar la longitud.
e) **Pérdida de Retorno:** es la medida de la energía reflejada, causada por las diferencias de impedancia en el sistema de cableado.
f) **Retraso de Propagación:** mide la cantidad de tiempo que una señal toma en atravesar el enlace.

5.2.4.9.6 Prueba de integridad de la señal en cable de fibra óptica

Para realizar la prueba de atenuación deben seguirse los siguientes lineamientos:

a) seleccione la longitud de onda correcta en ambos extremos;
b) cada fibra en los enlaces debe ser probada usando el método de pérdida de inserción;
c) enlaces <90m probados a 850nm o 1300nmdeben ser probados en una sola dirección o en la dirección anticipada o prevista de transmisión;
d) cada fibra en el enlace será probada usando el método de pérdida de inserción, generalmente >90m y <300m;debe ser probada a 850nm o 1300nm en una sola dirección o en la dirección de transmisión anticipada;
e) probados en ambas longitudes de onda de operación 850 y 1300nm para multimodo, 1310 y 1550nm para mono-modo;
f) los valores de aceptación están calculados usando la ecuación 2.4 de atenuación de enlace:

$$Atenuacion\ Máxima\ \ del\ enlace = atenuacion\ del\ conector + atenuacion\ máxima\ del\ cable + atenuacion\ m + máxima\ del\ enlace \quad \text{(II.4)}$$

5.2.5 Direccionamiento IP y equipos de comunicaciones en la Red LAN

5.2.5.1 Direccionamiento IP

Requerimientos generales

a) La red de telecomunicaciones debe estar basada en direccionamiento IPv4. Los conmutadores de datos y enrutadores deben estar preparados para poder soportar IPv6 para instalaciones futuras.
b) Se debe garantizar un correcto orden y documentación del espacio de direcciones IPv4 o IPv6 del Complejo de Seguridad, mediante el seguimiento permanente y adecuado sobre los cambios que se produzcan en cada segmento de red, asegurando su crecimiento para hacer frente a nuevas necesidades.
c) Entre Complejos de Seguridad se debe generar una estructura de direccionamiento jerárquico para generar la sumarización de las rutas.
d) La Red LAN del Complejo debe tener un plan de direccionamiento IP cuyo diseño contemple separar las diferentes áreas y servicios en segmentos IP diferentes. Un área con más 130 *host* debe ser dividida en diferentes segmentos IP.
e) Dentro del Complejo de Seguridad se permite el uso de subredes de máscara variable y fija.
f) Se debe tener un esquema de direccionamiento escalable, flexible y simple.
g) Se debe de tener facilidad de asignación de direcciones futuras a segmentos IP si crece el número de terminales.
h) Se debe mantener un esquema de direccionamiento que evite el crecimiento incontrolado de las tablas de enrutamiento de los equipos locales.
i) Se debe asignar un esquema de direccionamiento privado hacia el interior del Complejo de Seguridad, debido a que por motivos de seguridad no es deseable que los trabajadores tengan mucho acceso a Internet. Las direcciones privadas permitidas son:
    i. De clase A: se usará direccionamiento de la red principal 10.0.0.0/8.
    ii. De clase B: se usará direccionamiento del rango de redes principales 172.16.0.0/16 a 172.31.255.0/16.
    iii. De clase C: se usará direccionamiento del rango de redes principales 192.168.0.0/24 a 192.168.255.0/24.
j) Para el direccionamiento IPv6, se utilizarán Direcciones Locales Únicas (ULA *Unique Local Address*). Las Direcciones IPv6 Locales Únicas son de uso local, como las direcciones IP v4 privadas. Si se trata de una dirección IPv6 de 128 bits se sigue el siguiente formato:
    i. Empiezan con el valor FC00::/7.
    ii. El octavo bit vale siempre 1.

iii. Los siguientes 40 bits son un identificador global que será único para cada Complejo de Seguridad, que se asignará de manera aleatoria.
iv. Los siguientes 16 bits forman el número de subred, el cual puede ser dado de forma secuencial o con cualquier otro método.
v. Los últimos 64 bits están formados por la dirección MAC de la interfaz en formato EUI-64.

k) Los esquemas de direccionamiento público serán responsabilidad del proveedor de servicios.
l) Se debe definir una instancia que coordine la asignación de direcciones en el estado.
m) Direccionamiento a VLAN: cada segmento IP en el Complejo de Seguridad debe implementarse con el uso de una norma internacional para redes de área local virtuales (VLAN), que permita la segmentación de *broadcast* y aislé tráfico basado en los puertos de los conmutadores de datos. El tráfico aislado es de grupos de terminales de cómputo, teléfonos u otro dispositivo que se conecte a la Red LAN; además se debe utilizar una VLAN diferente para cada uno de los servicios (video, voz, administración, etc.).

5.2.5.2 Conmutadores de datos

5.2.5.2.1 Selección de conmutadores de datos

Se presentan requerimientos para seleccionar los conmutadores de datos, que también aplican para enrutadores y equipo de seguridad para la red LAN.

a) Definir cantidad número de puertos que requiere el Complejo de Seguridad. Para ello se debe definir el número de nodos del Complejo de Seguridad y se debe contemplar un 30% de nodos extra para el crecimiento a corto plazo.
b) Sólo se permiten conmutadores de datos con puertos 10/100/1000 de tecnología *Ethernet*, que puedan suministrar corriente eléctrica a través del cableado de tecnología tipo *Ethernet*, y para ello se debe cumplir con una norma internacional y con los requerimientos de demanda eléctrica, y se debe poder regular el voltaje que se requiera (cámara, teléfono, etc.).
c) Debe soportar VLAN a través de método certificado por una norma internacional IEEE 802.1q, para la segmentación de *broadcast* y aislé tráfico basado en los puertos de los conmutadores de datos.
d) Definir los protocolos de comunicación que se deben usar.
e) Definir los protocolos de calidad de servicios a usar y de alta disponibilidad, dependiendo del diseño de los sistemas.
f) Definir las políticas de administración y monitoreo de equipo.

g) Definir segmentos IP y VLAN del Complejo de Seguridad.
h) Definir políticas de seguridad de acuerdo a los requerimientos del Complejo de Seguridad.
i) Los conmutadores de datos deben contar con interfaces SFP para módulos de fibra óptica y el tipo de conector SFP dependiendo de la distancia en que se conecten los equipos; la cantidad depende de los requerimientos del diseño del Complejo de Seguridad.
j) Los conmutadores de datos opcionalmente pueden soportar interfaces para apilarse con otros conmutadores de datos, con un máximo de 8 conmutadores de datos en una pila dentro de un mismo cuarto de comunicaciones, esto depende de los requerimientos del Complejo de Seguridad.
k) Los conmutadores de datos opcionalmente pueden ser de capa 3 cuando sean principales y sea necesario intercomunicar las VLAN, esto depende de los requerimientos del Complejo de Seguridad.

5.2.5.2.2 Protocolos de conmutadores de datos

A continuación, se enlistan las funcionalidades que los conmutadores deben soportar, dependiendo de los requerimientos del diseño de la red LAN del Complejo de Seguridad. Estas funcionalidades deben ser implementadas a través de un protocolo o método certificado por una norma internacional. El listado es enunciativo, pero no limitado a las funcionalidades que enlista. Si existiera un requerimiento que no resuelven las funcionalidades listadas, se debe buscar un protocolo abierto certificado por un organismo internacional.

a) Se permite que el conmutador de datos participe en el proceso de autentificación en apoyo a servidores RADIUS o TACACS o TACACS+ usando protocolos de autentificación.
b) Debe soportar VLAN para la segmentación de *broadcast* y aisle tráfico basado en los puertos de los conmutadores de datos.
c) Se permite el uso de GVRP para el descubrimiento de VLAN en forma dinámica.
d) Se permite que el conmutador de datos defina un método para marcar y dar tratamiento a tramas para fines de calidad de servicio, a través de las etiquetas que usan las VLAN usando IEEE 802.1p.
e) Se permite el uso del Algoritmo de la norma IEEE 802.1w, para dar redundancia al cableado en una red de área local (haciendo conexiones redundantes entre conmutadores de datos).

f) Se permite el uso del Algoritmo de la norma IEEE 802.1s, para dar redundancia al cableado en una red de área local (haciendo conexiones redundantes entre conmutadores de datos) considerando las VLAN para resolver la topología de redundancia.
g) Se permite el uso de un protocolo para realizar adición de puertos, es decir, se puede crear un grupo de puertos físicos con el fin de sumar anchos de banda. a través de la norma IEEE 802.3ad. Este grupo de puertos físicos se conecta del conmutador de datos a otro conmutador de datos, o del conmutador de datos a un servidor, para aumentar la velocidad de transmisión de información.
h) Se permite el uso de un protocolo que establezca mecanismos de control de flujo para evitar congestionamientos.
i) Se permite el uso de un método para proporcionar energía eléctrica por el conmutador de datos a través de sus puertos con velocidades 10/100/1000 Mbps tipo *Ethernet* a las terminales que se conectan a éste. El conmutador de datos debe tener la suficiente potencia para soportar los dispositivos a alimentar.
j) Se permite el uso de una norma de regulación de corriente eléctrica para el conmutador de datos.

Nota: Si el conmutador de datos es de capa 3, los protocolos permitidos están listados en la sección 5.2.5.3.2.

5.2.5.2.3 Conmutador de datos principal

Se debe tener un conmutador de datos principal que cumpla con el aparatado 5.8.4.1 y5.8.4.2.

5.2.5.3 Enrutadores

5.2.5.3.1 Requerimientos generales

a) La cantidad de puertos del enrutador debe satisfacer los requerimientos del Complejo de Seguridad, tomando en cuenta que, para la Red LAN, los puertos deben ser *GigaEthernet* o *TenGigaEthernet* u otra tecnología de la familia *Ethernet* de mayor velocidad, y para la WAN o MAN dependerán de la tecnología que pueda satisfacer los requerimientos del Complejo de Seguridad.
b) El enrutador ya puesto en servicio no debe tener su procesador y memoria a más del 70% de uso.

c) En caso de que se tengan varios proveedores de Internet o varias salidas a la misma red WAN o MAN, se debe proveer la arquitectura propuesta en el apartado 5.8.6.1.1.

5.2.5.3.2 Protocolos soportados

La siguiente lista indica los protocolos que se podrán soportar por los enrutadores. El listado es enunciativo, pero no limitado a las funcionalidades que enlista. Si existiera un requerimiento que no resuelven las funcionalidades listadas, se debe buscar un protocolo abierto certificado por un organismo internacional. En caso de requerir que el enrutador soporte protocolos de capa 2 del modelo OSI, consultar el apartado5.2.4.2.

a) Protocolo IPv4 e IPv6. Debe cumplir con los RFC 791, 1349 y 6864 para IPv4; y para el caso de IPv6 se deben cumplir los RFC 2460 y RFC 5722. Es obligatorio que los enrutadores para el Complejo de Seguridad tengan capacidades de enrutamiento sobre el protocolo IP.
b) Direcciones primarias y/o secundarias por interfaz o VLAN: los equipos con capacidades de enrutamiento deben poder soportar el uso de direcciones IP en sus interfaces o en VLAN por puerto. La VLAN debe permitir segmentar tráfico de *broadcast* y aislé tráfico de terminales finales de usuarios por puerto.
c) Rutas estáticas: deben tener la posibilidad de configurar manualmente rutas estáticas para llenar su tabla de enrutamiento.
d) VRRP: debe cumplir con el RFC 5798; este protocolo da la posibilidad de respaldar las puertas de enlace de una red o subred IP, a través de la implementación de un segundo enrutador. Ver el apartado VIII.8.1.1.
e) NAT: el enrutador debe soportar NAT Estático (RFC 2663), NAT-PAT (RFC 3022), NAT-PMP (NATcon protocolo de mapeo de puertos, RFC 6886), dependiendo de los requerimientos del Complejo de Seguridad.
f) Protocolo de calidad de servicio: los enrutadores deben soportar todas o algunas de las siguientes normas para proveer la calidad de servicio: IP ToS, CoS, DiffServe Code Point (DSCP) y IEEE 802.1p que usan la etiqueta de la VLAN (IEEE 802.1Q). Además, el enrutador debe tener cuatro o más colas de prioridad o de porcentaje de ancho de banda para encolar las tramas que requieran que se les de tratamiento de QoS.
g) Gestión: dependiendo de los requerimientos de diseño, se podrá elegir uno o más de los siguientes protocolos: HTTPS/SSH/SNMP V2c o V3.

h) Protocolos de enrutamiento: dependiendo de los requerimientos de diseño, se podrá elegir entre los siguientes protocolos de enrutamiento: RIP (RFC 2453 y RFC 2080), OSPF (RFC 2328 y RFC 5340), BGP (RFC 1163), IGMP (RFC 3376), PIM-SM (RFC 7761), EIGRP (RFC 7868) y DVMRP (RFC 1057), y para el caso de enrutamiento con IPv6 se podrá elegir entre RIPng, OSPFv3 y BGP-4 de la IETF.
i) DHCP: debe cumplir con el RFC 2131 y el RFC 3046. El enrutador debe tener capacidades de ser un servidor DHCP, cliente DHCP y DHCP de reenvío (DHCP *relay*).
j) SNTP o NTP: dependiendo de los requerimientos de diseño, se usará SNTP o NTP (RFC 5905 y RFC 7822) en el caso de que se requiera sincronización de relojes.
k) Conexiones VPN: se podrán utilizar los protocolos VPN IPSEC y/o VPN GRE, dependiendo de los requerimientos del Complejo de Seguridad.

5.2.5.4 Seguridad y monitoreo en conmutadores de datos y enrutadores

5.2.5.4.1 Seguridad de la infraestructura de telecomunicaciones

a) Se deben deshabilitar las cuentas que vienen pre-configuradas por defecto en los equipos de comunicaciones y crear cuentas de usuario con los mismos privilegios.
b) La administración de cada componente debe hacerse únicamente a través de las cuentas de diferentes perfiles para cada componente.
c) La contraseña de cada cuenta para la administración del equipo debe apegarse a la política de contraseñas.
d) Todos los equipos deben tener contraseñas diferentes.
e) Se debe establecer una política de creación de contraseñas por los administradores de la red que defina longitud de la contraseña, caracteres válidos y periodo de cambio de la misma.
f) Los servicios para la conexión y administración de los componentes que no cifren los canales de comunicación se deben deshabilitar, por considerarse inseguros ante un ataque tipo *Sniffer* en la red.
g) Se debe tener una VLAN para la administración.
h) Se debe restringir el acceso a los equipos de comunicaciones. Sólo determinado número de direcciones IP y/o segmentos de red podrán acceder a los equipos de comunicaciones para su administración.
i) Se debe establecer un control de cambios de las contraseñas.

j) Se debe establecer un control de cambios para la aplicación de las actualizaciones de los *firmware* de los equipos que sean aprobadas por el personal responsable del Área de las TIC, el cual debe considerar como mínimo lo siguiente:
    i. Justificación de la instalación
    ii. Resultado de la evaluación de la actualización realizada en ambientes de pruebas
    iii. Plan para la aplicación de la actualización
    iv. Fecha de la actualización
    v. Respaldo de las configuraciones
    vi. Procedimiento de regreso en caso de que la actualización genere problemas en el ambiente productivo
    vii. Autorización del cambio por la dirección responsable
k) Se debe desactivar protocolos que no se usen.
l) Contar con diagramas de la ubicación física de los equipos de comunicaciones del Complejo de Seguridad y tenerlos etiquetados para su fácil identificación.
m) Contar con un inventario actualizado donde se identifiquen las conexiones entre los conmutadores de datos y los restantes equipos de red.

5.2.5.4.2 Monitoreo de equipo de comunicaciones y equipos de seguridad

Con el fin de garantizar la continuidad del servicio provisto por los conmutadores de datos y enrutadores, se deben instalar aplicaciones que monitoreen su estado, desempeño y carga. Esto además da al administrador la posibilidad de conocer el comportamiento normal de la red con base en registros y gráficas. Se debe administrar y analizar tráfico comprometido y en exceso, así como tráfico en demanda y su exceso.

a) El ambiente de monitoreo debe estar restringido al personal a cargo de los conmutadores de datos y enrutadores a través de un software.
b) El ambiente de monitoreo debe tener seguridad para no comprometer los conmutadores de datos y enrutadores.
c) Se debe manejar notificaciones SNMP o *traps* SNMP en el caso de que el equipo monitoreado presente algún incidente.
d) Los aplicativos usados en el ambiente de monitoreo deben generar mensajes o avisos al administrador de la red, como correos electrónicos y mensajes, entre otros.
e) Los aplicativos usados en el ambiente de monitoreo no deben tener límite de números de dispositivos que se pueden monitorear.
f) Los aplicativos deben estar restringidos por usuario y contraseña y por perfil.
g) Los aplicativos deben verificar los equipos de comunicaciones cada 5 minutos o menos, dependiendo de los requerimientos del Complejo de Seguridad.

h) Actualización de *software*: se debe tener la característica de actualización de *firmware* de manera local y remota de forma gratuita, a través de los protocolos TFTP/FTP.
i) Se deben monitorear los equipos de enrutamiento usando https, SNMP v2c o SNMP v3 y SSH.
j) Se debe poder enviar registros de eventos tipo *syslog* a servidores de *log* remotos.
k) El monitoreo de equipo de comunicaciones se debe hacer con un aplicativo que soporte SNMPv2c o v3.
l) El enrutador debe soportar las MIB I y MIB II y opcionalmente RMON, dependiendo de los requerimientos del Complejo de Seguridad.
m) El porcentaje de uso de CPU, memoria y ancho de banda en los puertos de los equipos de comunicaciones y seguridad deben considerar una holgura de uso para crecimientos futuros, dependiendo de las proyecciones y recomendaciones del fabricante.
n) La temperatura y humedad ambiente a monitorear a la que deben estar los equipos de comunicaciones son de acuerdo al promedio del rango que recomienda el fabricante.

5.2.6 Seguridad y Monitoreo en equipo de cómputo

5.2.6.1 Seguridad física en los cuartos de telecomunicaciones

a) En todos los dispositivos tecnológicos instalados en el cuarto de telecomunicaciones que dispongan de algún medio físico para lectura de dispositivos de almacenamiento personal tales como: puertos USB, SD, micro SD, infrarrojo, lector CDROM y otros, deben ser deshabilitadas todas las opciones de lectura y arranque de *software* automático, así como el arranque de equipo por algún medio externo, esto con el fin de evitar instalación de *software* malicioso, espionaje y robo de información.
b) En el centro de cómputo se debe tener jaulas separadas de los servicios de telecomunicaciones, cómputo, bases de datos, radiocomunicaciones , almacenamiento de bases de datos, almacenamiento de video etc.
c) Se debe contar con cámaras con detección de movimiento, para monitorear los accesos y actividades al interior de la granja de servidores.
d) Se debe tener preferentemente un sólo acceso al cuarto de telecomunicaciones.
e) Se debe tener acceso restringido al cuarto de telecomunicaciones, mediante uno de los siguientes sistemas o una combinación de ellos:
    i. Contraseña

ii. Un dispositivo de acceso (tal como una tarjeta con chip, banda magnética o una llave, etcétera)
iii. Mediante un lector biométrico (retina, voz, huella digital, etcétera)

f) Si hay gabinetes, se debe tener puertas de acceso con llaves y al igual en los bastidores en el caso de que también se les haya adaptado una puerta.
g) El cuarto que contenga la granja de servidores debe tener las temperaturas óptimas para el buen funcionamiento de los equipos, considerando los manuales de operación. Para ello es necesario que cuente con un sistema de aire acondicionado, así como con un sistema de control de humedad.
h) La granja de servidores debe contar con un sistema de alimentación ininterrumpida (UPS) de respaldo contra caídas de tensión o interrupciones en el suministro de energía eléctrica. Adicionalmente debe contar con una planta de energía capaz de soportar la carga requerida por el cuarto hasta por 24 horas.
i) Se debe asegurar que las protecciones y cableado eléctrico sean del calibre adecuado, y realizar pruebas de funcionamiento óptimo.

5.2.6.2 Seguridad de acceso a servidores

a) Prohibir todo acceso a un equipo de cómputo, a menos que sea estrictamente necesario y se utilice con el fin específico para el que se asignó, con un horario claramente determinado.
b) Verificar periódicamente el equipo para evitar *software* malicioso, *software* no autorizado, o bien que estén activado micrófono y/o cámara del equipo de cómputo, o cualquier dispositivo que comprometa la integridad o secrecía de la información sensible en cualquier caso, a menos que así se haya decidido por mutuo acuerdo con el responsable del Complejo de Seguridad.
c) En todos los dispositivos que se encuentren en la granja de servidores y que dispongan de algún medio físico para lectura de dispositivos de almacenamiento tales como: puertos USB, SD, micro SD, infrarrojo, lector CDROM entre otros, deben ser deshabilitadas todas las opciones de lectura y arranque de software automático, así como el arranque de equipo de algún medio externo, esto con el fin de evitar instalación de *software* malicioso, espionaje y robo de información. Tendrá acceso a estos puertos sólo personal autorizado.
d) Los servidores deben tener deshabilitados los usuarios y contraseñas que traen de fábrica o instalación, y los usuarios y contraseñas activas deben estar protegidos mediante el cambio a una contraseña diferente de la que el fabricante o programador da por omisión.
e) Las contraseñas deben ser cambiadas cada determinado tiempo y asignadas a cada equipo con un criterio que será determinado por el área responsable.

5.2.6.3 Seguridad de acceso a equipo de cómputo de escritorio y móvil

5.2.6.3.1 Medidas que deben seguir los trabajadores del Complejo de Seguridad

a) El equipo de cómputo debe ser utilizado sólo para los fines a los que fue asignado. Debe tener un perfil de usuario administrado por el supervisor.
b) Utilizar el equipo en base a los roles clasificados y asignados por el área competente.
c) El uso de Internet debe estar restringido, a menos que el jefe inmediato lo autorice; será para uso exclusivo de las actividades encomendadas al trabajador del Complejo de Seguridad.
d) Los puertos de almacenamiento externo del equipo del trabajador del Complejo de Seguridad deben estar deshabilitados(a menos que el rol requiera el uso indispensable de estos), con el fin de evitar la instalación de *software* de terceros no indispensable para las actividades del usuario, de *software* malicioso, o bien el robo o filtrado de información.

5.2.6.3.2 Uso de dispositivos móviles de personal interno

Se prohíbe el uso de dispositivos y teléfonos móviles personales dentro del área de trabajo del Complejo de Seguridad, a menos que el jefe inmediato del trabajador así lo autorice y sólo para fines estrictamente relacionados con las actividades del trabajo realizado.

5.2.6.4 Entrega y uso de equipo

Se le asignará al personal un equipo o varios equipos de cómputo para desempeñar las actividades propias de su trabajo; es responsabilidad de los usuarios mantener el equipo en óptimas condiciones en cuanto a su *software* y *hardware* dándole el uso para el que fue asignado.

5.2.6.4.1 Gestión de aplicativos

a) Actualización de sistemas operativos
   El sistema operativo debe tener instaladas las últimas versiones de los parches correspondientes a la seguridad para evitar posibles vulnerabilidades por versiones obsoletas, por lo que debe existir un encargado de revisar las actualizaciones correspondientes, así como la estabilidad de las mismas.
b) Actualización de software aplicativo
   Los aplicativos del sistema deben contar también con las últimas actualizaciones de seguridad, con el fin de evitar posibles ataques detectados en las versiones anteriores y obsoletas.
c) Antivirus

i. Todos los equipos para usuarios personales deben tener un antivirus.
ii. Los antivirus se deben mantener actualizados de manera automática.
iii. Se deben programar escaneos periódicos.

d) Para la gestión de los aplicativos que estén en el equipo de cómputo se debe:
   i. Actualizar los aplicativos cuando se deba corregir errores.
   ii. Desinstalar los aplicativos obsoletos y que no se utilicen.
   iii. Designar un responsable de verificar periódicamente el buen funcionamiento de los aplicativos.
   iv. Si están activadas las actualizaciones automáticas, verificar periódicamente que se estén instalando.
   v. Verificar que no existen aplicativos obsoletos que pudieran vulnerar la seguridad del equipo o aplicativos que el personal utiliza.
e) Bitácora de mantenimiento periódico de aplicativos
   Se deja al departamento encargado de dar mantenimiento preventivo o correctivo el formato con la información que se requiera con base en el sistema operativo y de los aplicativos, para indicar convenientemente las fechas en las que se ha realizado la verificación de cada equipo respecto a sus actualizaciones, tanto de sistema operativo, escaneo y actualización del antivirus, como de las revisiones de versiones de los aplicativos con sus respectivos parches de seguridad.
f) Es necesario tener manuales técnicos operativos para la configuración de equipos, con instrucciones de los distintos aplicativos que se utilizan en el Complejo de Seguridad, así como el mecanismo para resolver los problemas más frecuentes con estos aplicativos.

5.2.6.5 Monitoreo de red de datos

a) Se debe sincronizar los relojes de todos los equipos del Complejo de Seguridad, por medio del protocolo NTP que utiliza UDP como su capa de transporte, sin necesidad de tener internet o de algún otro certificado por normas internacionales, que permita la correcta sincronización de los relojes de los equipos del Complejo de Seguridad, con el fin de tener congruencia al momento de generar las distintas bitácoras de incidentes.
b) Tanto en los servidores como en los aplicativos se debe tener activas las bitácoras tanto del sistema operativo como de los aplicativos con las alertas críticas (falla por error de contraseña, ataques de negación de servicio, o los que se consideren convenientes basados en el análisis de riesgos informáticos llevado por el área responsable); con el fin de monitorear actividad sospechosa, estas bitácoras deben estar almacenadas en otro dispositivo ajeno al servidor que se está monitoreando para evitar pérdidas de información y permitir, en caso de ser necesario, realizar una investigación al presentarse algún incidente.

c) De ser posible, se requerirá almacenar las alertas críticas para enrutadores, conmutadores de datos o dispositivos de comunicación que sean considerados vitales para el funcionamiento del Complejo de Seguridad.
d) Si se utiliza el protocolo SNMP será necesario utilizar el protocolo SNMP v2c o SNMPV3 para garantizar la seguridad en el manejo, administración y monitoreo de red, además de detectar errores, planificar su crecimiento y conocer su comportamiento.
e) El aplicativo de monitoreo debe estar protegido para su acceso por usuario y contraseña. En caso de que existan varios administradores, deben darse de alta en el aplicativo con su usuario correspondiente y un perfil definido.
f) El Complejo de Seguridad debe tener al menos un Identificador de Intrusos (IDS) que permita monitorear el tráfico y detectar posibles ataques a los diferentes servicios que brindan los servidores del Complejo de Seguridad.
g) Si se requiere agregar seguridad en el monitoreo del tráfico de red para prevenir diversos ataques se puede implementar un IPS (*Intrusion Prevention System*).

5.2.6.6 Equipo de seguridad

5.2.6.6.1 Cortafuegos

a) Se debe utilizar un cortafuegos (*firewall*) ya sea físico o lógico, para controlar los accesos a la red, previniendo ataques y accesos no autorizados y monitoreando las posibles actividades maliciosas, para actuar en consecuencia. Ver figura II.17.

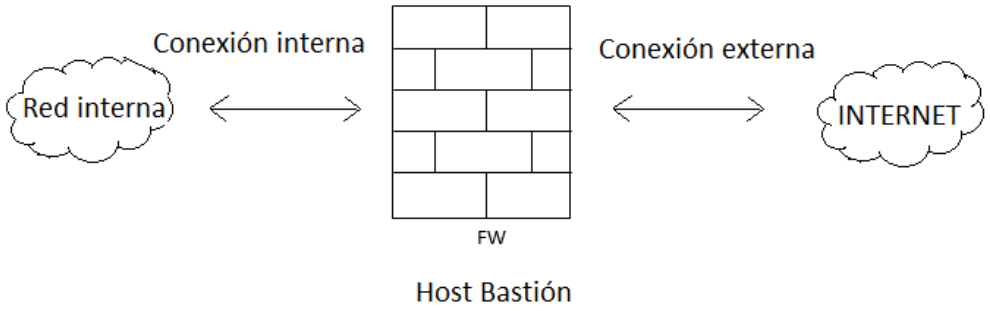


Figura II. 17 Integración de un cortafuegos

b) Se recomienda que el acceso remoto al cortafuegos se realice mediante el uso de una VPN, para incrementar la seguridad de acceso.
c) La siguiente lista indica los elementos que se deben proteger, sin restringir la protección de otros elementos, dependiendo de los requerimientos del Complejo de Seguridad:
    i. Salidas de Internet

ii. Granja de servidores
iii. Arreglo de discos, si aplica
iv. Acceso a conmutador de datos y voz principal

d) El *firewall* debe contar con los filtros para proteger la red que se enlistan a continuación, como filtros mínimos que deben tener los *firewall*, sin restringir otros tipos susceptibles de utilizarse, dependiendo de los requerimientos del Complejo de Seguridad.
   i. Listas de control de acceso por el protocolo IP.
ii. Bloquear paquetes que incluyan direcciones de difusión, con el fin de evitar ataques de negación de servicios (DOS).
   iii. Bloquear paquetes de entrada con direcciones de segmentos catalogados como privados por la IANA (*Internet Assigned Numbers Authority*).
   iv. Bloquear paquetes de entrada con direcciones de la red interna, esto con el fin de evitar ataques de suplantación de identidad.
   v. Bloquear los paquetes de salida cuya dirección fuente corresponde a direcciones externas a la red.
   vi. Bloquear paquetes pertenecientes al protocolo de control ICMP que den información sensible a la red, tales como los otorgados en peticiones de un ping o el *traceroute*.
   vii. Bloquear paquetes de control ICMP "*Redirect*," ya que permiten modificar las tablas de enrutamiento.
   viii. Bloquear paquetes de tamaño inferior al mínimo permitido o que por su estructura puedan ser motivo de sospecha por los valores que presentan inválidos en su cabecera, pues pueden representar un posible riesgo de ataque de negación de servicio.
   ix. Inspección de estado: tener la capacidad de analizar conexiones y flujos de paquetes.
   x. *Proxies/gateways* de aplicación: capacidad de controlar acceso de aplicaciones.

e) En cuanto a puertos es conveniente bloquearen el *firewall* todos aquellos que no se usan, dependiendo de la logística del Complejo de Seguridad, e ir habilitando sólo los que las políticas del Complejo de Seguridad permitan. A continuación, se enlistan los puertos que debe considerarse bloquear, dependiendo de las políticas del Complejo de Seguridad:
   i. Servicios de puertos que permiten la conexión remota, tales como: FTP(21), SSH (22), telnet (23), rlogin (512/TCP,513/TCP,514/TCP).
   ii. En redes con sistemas operativos, los puertos de los protocolos que permiten la conexión a red de recursos compartidos, tales como impresoras, archivos, directorios o carpetas, entre otros.
   iii. Los puertos que permiten el uso de terminales gráficas remotas de los diferentes sistemas operativos.

iv. Los puertos para servicios de correo electrónico en equipos que no actúan como servidores de correo: SMTP (25/TCP), POP3 (109/TCP), (110/TCO), IMAP (143/TCP).
v. El servicio de *Finger* (79/TCP), ya que facilita información de los usuarios del sistema, *echo* (7/TCP) y *chargen* (19/TCP, UDP) que pueden ser utilizados para efectuar un ataque de negación de servicio.
vi. El protocolo de transferencia de archivos TPFTP (69/UDP), el cual transfiere archivos sin cifrado.
vii. Puertos para servicio de web en servidores o equipos que no ofrezcan el servicio, puertos HTTP (80/TCP), (8080/TCP), SSL (443/TCP), entre otros.
viii. Puertos que la junta directiva del Complejo de Seguridad considere pertinentes filtrar, por los riesgos que implique mantenerlos abiertos.

f) Capacidades de análisis. El corta fuegos debe tener herramientas integradas o separadas para realizar análisis del tráfico que fluye a través de él para realizar análisis de contenido, análisis de ataques avanzados y comportamiento de tráfico de la red.
g) Es importante utilizar siempre protocolos seguros, tanto en las comunicaciones entre servidores como en los servicios que se entregan a los equipos del personal del Centro de Seguridad, por lo que se debe utilizar por ejemplo:
   i. Si se va a utilizar un servicio, se preferirá el uso de servicio cifrado por el puerto 443 al servicio de la información en claro (sin cifrar) del puerto 80; será importante redireccionar una petición del puerto 80 al puerto 443 en este ejemplo.
   ii. En otro ejemplo, debe utilizarse el protocolo cifrado de SFTP en lugar del protocolo FTP para transferencia de archivos, o si se va a realizar una conexión remota a un servidor, utilizar el protocolo SSH del puerto 22.
   iii. En cada caso será necesario utilizar preferentemente los protocolos seguros para evitar intromisiones, intercepciones y robo de información que permitan ataques de distintos tipos, dependiendo del servicio atacado.

5.2.6.6.2 Detector de Intrusos

Las características del Servidor para la identificación de intrusos de red (IDS *Intrusion Detection System*) se describen a continuación:

a) El detector de intrusos debe estar diseñado para identificar diversas actividades en la red, tanto sospechosas como maliciosas; estas actividades ya deben estar clasificadas con base en un análisis que permita evitar en la medida de lo posible tanto falsos positivos como falsos negativos.
b) El detector de intrusos puede conectarse en modo puente (Figurall.18).

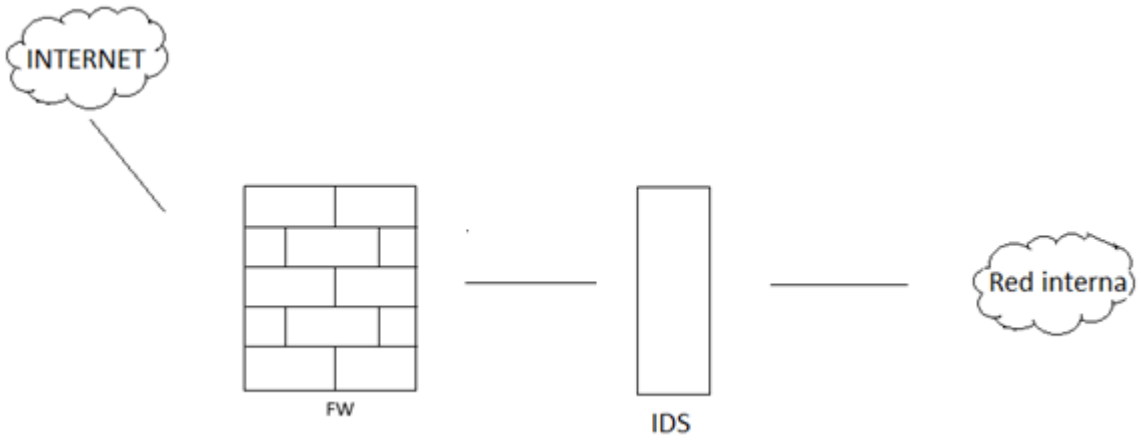


Figura II. 18 Detector de Intrusos en modo puente

c) El detector de intrusos se puede conectar en modo de sólo monitoreo (conectado a un puerto espejo), conexión que es más común utilizar en un detector de intrusos (Figura II.19).

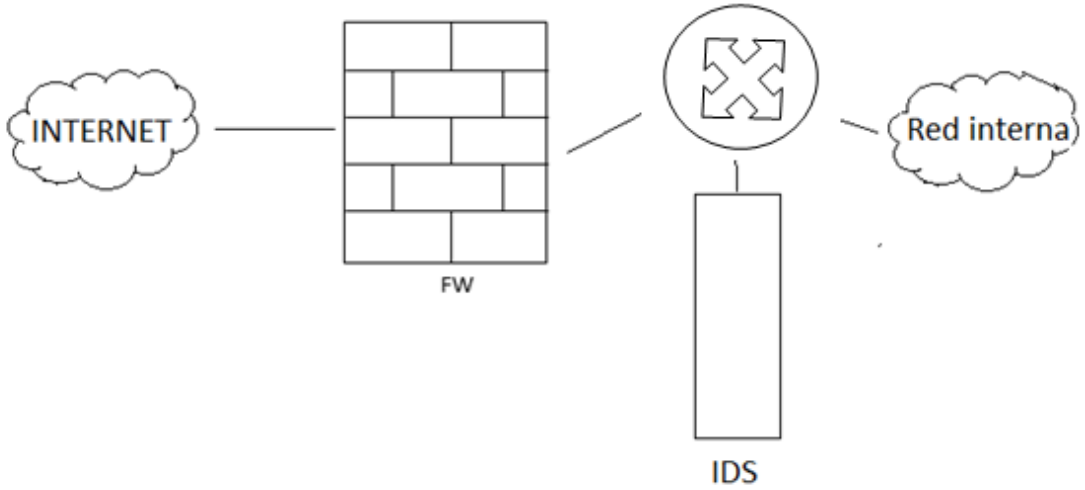


Figura II. 19 Conexión de IDS modo monitoreo

d) La selección de un modo de conexión del detector de intrusos será elegida por el analista asignado por el área de seguridad informática y podrá ser automática o manual, según los criterios de seguridad y operatividad del Complejo de Seguridad.
e) El diseño, monitoreo y análisis deben estar asignados a personal capacitado tanto para poder realizar la redacción de reglas, como para saber interpretar los resultados y actuar en consecuencia ante tráfico sospechoso y tráfico malicioso.

f) Se debe utilizar herramientas gráficas para poder analizar de una manera más eficiente todo el tráfico, tanto sospechoso como malicioso.
g) Para la clasificación de amenazas e incidentes se recomienda utilizar la clasificación del proyecto *Sguil* o alguna otra que cumpla con las normas nacionales o internacionales. La clasificación del proyecto *Sguil* es la siguiente:

i. Categoría 1: Accesos no autorizados a contraseñas de administrador.
ii. Categoría2: Accesos no autorizados de usuarios que no desempeñan tareas administrativas de servidores o sistemas.
iii. Categoría 3: Intentos de accesos no autorizados.
iv. Categoría 4: Ataque exitoso de negación de servicio.
v. Categoría 5: Malas prácticas de uso en cuanto a seguridad o violaciones a las políticas.
vi. Categoría 6: Uso de herramientas que permiten reconocer las características e infraestructura de red.
vii. Categoría 7: Infecciones por medio de gusanos o virus.

Nota: el Detector de Intrusos, puede estar en un dispositivo físico dedicado a éste o convivir con el *Firewall*, Filtro *Web* o Preventor de Intrusos en otro dispositivo físico, cuidando de no afectar el desempeño del mismo.

5.2.6.6.3 Preventor de Intrusos

Un sistema de prevención de intrusos (IPS) es un sistema preventivo que examina el tráfico de red para detectar y prevenir ataques a vulnerabilidades que afectan diversos servicios, que de ser exitosos se vería afectado el Complejo de Seguridad, por ejemplo con posibles accesos no autorizados a sus servidores, ataques de negación de servicios, entre otros posibles, por lo que en el Complejo de Seguridad será necesario el uso de estos servidores para aumentar la seguridad y prevenir este tipo de ataques.

Un sistema de prevención de intrusos es un sistema que trabaja en línea, que puede ser instalado en una o más redes que necesitan protección. Ver figura II.20.

La manera más común de conexión es antes de la entrada al cortafuegos (*firewall*) para complementar el análisis, lo que es una solución bastante aceptada para el resguardo de elementos sensibles de ataques, tales como servidores web, de correo, de bases de datos, entre muchos más.

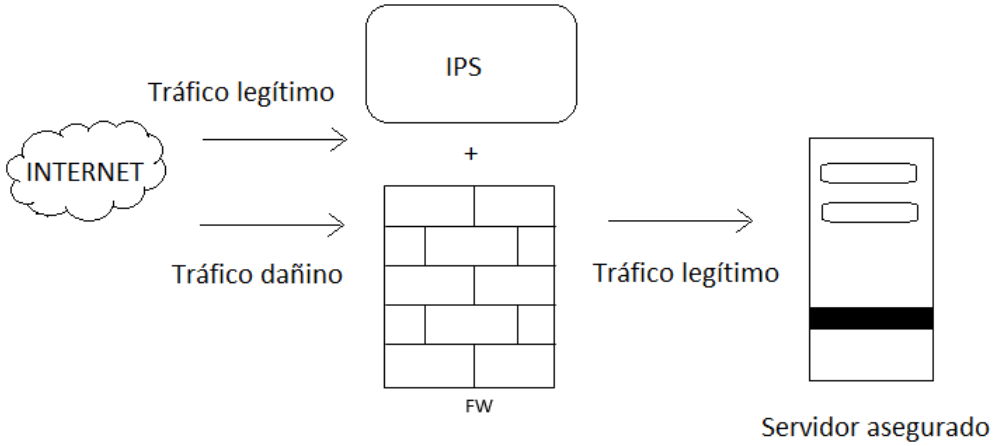


Figura II. 20 Conexión típica de un servidor para prevención de intrusos

a) Depende de las políticas del Complejo de Seguridad la forma en la que debe actuar en caso de que sea disparada una alerta:
   i. Envía una alarma al administrador (como el caso de un IDS).
   ii. Bloquea el tráfico de la fuente.
   iii. Desecha los paquetes maliciosos.
   iv. Reinicia la conexión.
b) El IPS debe trabajar de manera eficiente, pues debe evitarse la degradación del desempeño de la red.
c) El IPS debe detectar de manera precisa, para reducir los falsos positivos.
d) El IPS debe tener al menos dos mecanismos para la detección de tráfico malicioso:
   i. Detección basada en firmas.
   ii. Detección basada en estadísticas.

Nota: el Preventor de Intrusos puede estar en un dispositivo físico dedicado a éste o convivir con el Firewall, Filtro *Web* o Detector de Intrusos en otro dispositivo físico, cuidando de no afectar el desempeño del mismo.

5.2.6.6.4 Filtro Web

Se debe utilizar un filtro *web* para poder filtrar contenidos no necesarios y riesgosos por los posibles programas maliciosos que pudieran contener las páginas maliciosas (así como las descargas que contienen), reducir el flujo de tráfico(optimizando así los recursos de la red), así como evitar distracciones dentro del Complejo de Seguridad. Ver Figura II.21.

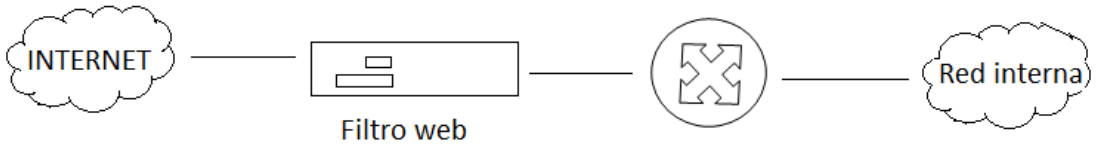


Figura II. 21 Conexión del Filtro web

El Servidor para filtrar el acceso a *la web* debe:

a) Soportar los protocolos HTTP y FTP.
b) Tener soporte para uso de caché, para acelerar la visita de páginas con mayor número de visitas.
c) Tener capacidades para configuraciones por medio de:
    i. Usuarios
    ii. Perfiles de grupo
    iii. Segmentos de red
d) Ser capaz de crear filtros basados en:
    i. Direcciones IP
    ii. Direcciones MAC
    iii. Horarios
    iv. Dominios
    v. URL específicos
    vi. Basado en distintos tipos de archivos
e) Debe tener la capacidad de generar listas negras para filtrar diferentes tipos de categorías, tales como:
    i. Chats basados en protocolo IRC o HTTP
    ii. Descargas ajenas a las necesidades laborales
    iii. Sitios de juegos en línea
    iv. Sitios de videos o música
    v. Sitios de pornografía
    vi. Transmisión de radio y TV vía *Web*
f) Implementación versátil de políticas que considere adecuadas el Complejo de Seguridad para el resguardo de la seguridad de la red.

Nota: el Filtrado *Web* puede estar en un dispositivo físico dedicado a éste o convivir con el *Firewall*, Detector de Intrusos o Preventor de Intrusos en otro dispositivo físico, cuidando de no afectar su desempeño.

5.2.6.7 Políticas para el personal externo

5.2.6.7.1 Restricciones en el uso de dispositivos portátiles

Debe restringirse el uso de dispositivos portátiles mediante:

a) Registro del equipo al entrar y salir del Complejo de Seguridad.
b) De preferencia pegar un distintivo en un lugar vistoso.
c) Debe ingresarse estrictamente para la actividad para la que se requirió el ingreso.
d) Evitar en lo posible el contacto con las zonas de mayor seguridad de red.
e) Monitorear su uso en caso de conectarse a alguna red que brinde servicio al Complejo de Seguridad.
f) Deben estar conectados a una red independiente de las redes que utiliza el Complejo de Seguridad para su labor diaria. Esta red debe tener las siguientes características:
    i. Debe estar en una red aislada del resto de las redes del Complejo de Seguridad.
    ii. No debe tener comunicación con las redes del Complejo de Seguridad.
    iii. Debe estar protegido a través de un sistema de filtrado de contenido Web.

5.2.6.7.2 Uso de dispositivos de almacenamiento personal de usuarios externos

El uso de dispositivos de almacenamiento, tales como memorias USB, discos duros tanto internos como externos, así como discos compactos, DVD, *blue ray* o cualquier tipo de memorias externas, debe ser mantenido bajo estricto control de vigilancia, ya que estos dispositivos pueden contener cualquier tipo de código malicioso o tener sistemas operativos en vivo (*Live* CD) o bien herramientas de auditorías de sistemas y red que pudieran ser utilizadas para vulnerar las medidas de seguridad existentes en cualquiera de los ámbitos tecnológicos, y que implican riesgos tales como instalación de *software*, escaneo de red, robo de información, entre otros, que pueden dañar la operación y funcionamiento del Complejo de Seguridad y/o entorpecer sus actividades prioritarias o secundarias.

5.3 Red Estatal de Radiocomunicación

5.3.1 Objetivo

Definir los requerimientos técnicos para conformar la Red Estatal de Radiocomunicación con conectividad IP que sea troncalizada, privada, cifrada de extremo a extremo y unificada en los Complejos de Seguridad para brindar servicios de voz y datos. Empleando el estándar y/o protocolos que permitan la interoperabilidad con las Redes Estatales de Radiocomunicación en los Estados, y que de esta forma mantengan la integración de la Red Nacional de Radiocomunicación (RNR), con el fin de garantizar la comunicación para la operación y coordinación de las autoridades federales, estatales y municipales en el país. Que permita el libre desplazamiento de los usuarios federales sin cambiar de dispositivo en la cobertura de la RNR.

Definir la infraestructura tecnológica para integrar las funciones de monitoreo y despacho, para visualizar los elementos de seguridad y patrullas. La interfaz de comunicación entre el CAD y los radios del sistema de radiocomunicaciones deben ser compatible en su integración.

5.3.2 Alcances

Las características y especificaciones definidas en este apartado aplican a la infraestructura de telecomunicaciones de los Complejos de Seguridad, no es una guía de diseño y debe ser leído por personal capacitado en tecnología de telecomunicaciones.

5.3.3 Campo de Aplicación

El campo de aplicación de la presente norma técnica establece los requerimientos técnicos necesarios de la Red Estatal de Radiocomunicación y del Área de Despacho de los Complejos de Seguridad.

5.3.4 Descripción

Este manual establece la infraestructura de la Red Estatal de Radiocomunicación que debe ser Digital, Troncalizada y Cifrada, y permitirá la comunicación de y hacia las patrullas, elementos de seguridad pública municipales, entidades estatales, así como usuarios federales que requieran el servicio de comunicaciones y estén administrados en el Complejo de Seguridad (CS).

Esta red debe ser compatible con la Red Nacional de Radiocomunicaciones. Debe permitir la comunicación con los dispositivos de radio, línea telefónica digital o analógica (independientemente de la central telefónica empleada), usados en Seguridad Pública, entre otros. La incorporación de todos estos recursos de telecomunicaciones debe ser totalmente transparente para el despachador.

Es importante resaltar que de acuerdo a la normatividad actual del Sistema Nacional de Seguridad Pública, las redes estatales que conforman la Red Nacional de Radiocomunicación deben ser compatibles con el protocolo que se establece en los Lineamientos de Sistemas de Radiocomunicación de Seguridad Pública. En caso de que el estado cuente con radios ajenos a la RNR, de manera transitoria y para operaciones especificas los puede interconectar a la red estatal de radiocomunicación mediante consolas de despacho. Debe hacerse con plena conciencia de que esta practica vulnera la seguridad de extremo a extremo de la RNR.

En la figura III.1 se observa un diagrama general de la operación de la Red de Radiocomunicación, en la cual se muestran los subsistemas de Radio, de Conmutación y de Gestión.

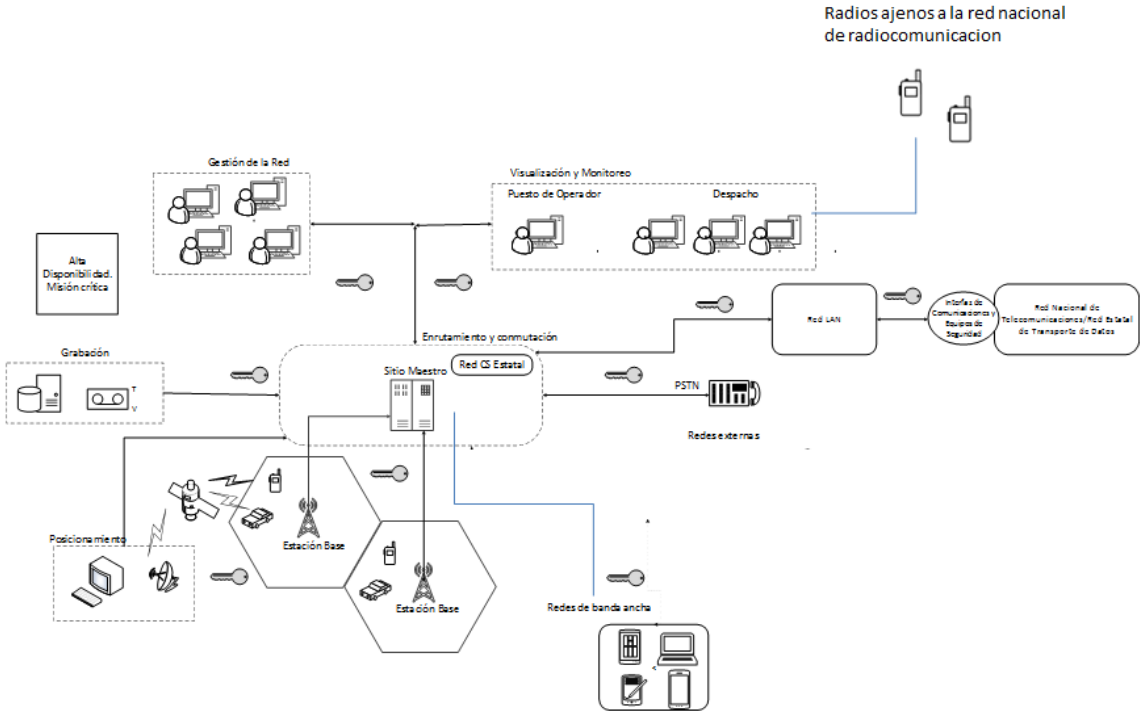


Figura III. 1 Diagrama general de la operación de la Red Estatal de Radiocomunicaciones con conexión a la Red Nacional de Radiocomunicación

El sistema debe cumplir las características técnicas siguientes:

- Mismo Cifrado de llamadas de extremo a extremo (*End to End)*
- Mantener el mismo protocolo entre repetidores y centrales y radios.
- Apegarse a una administración nacional de llaves (sincronización con todos los estados de la República).
- Permitir el roaming de los abonados en la Red Nacional de Radiocomunicación
- Proporcionar servicios de voz y datos:
    - Llamada privada cifrada
    - Llamadas de grupo cifradas y troncalizadas
    - Llamadas múltiples cifradas y troncalizadas
    - Comunicación cifrada de grupo local
    - Comunicación cifrada de grupo nacional
    - Creación y Cobertura multired
    - Llamadas privadas simultáneas
    - Envío de mensajes de radio a radio a sus RFSI correspondientes
    - Envío de mensajes de un operador a un terminal portátil al RFSI correspondiente
    - Administración de Bases de Datos
    - Extracción de reportes de alarmas y anomalías
    - Supervisión técnica y gráfica de la infraestructura de la red
    - Supervisión de la célula de radio
    - Emergencia geolocalizada
    - Direccionamiento funcional, para voz y datos, permitiendo que en los abonados se indique un ID de llamada de voz o datos pero vía Gestión Táctica se indica la dirección destino evitando la reprogramación de estos servicios en le terminal
    - Llamada implícita
    - Manejo de prioridades de servicios de voz y datos como una rutina, flash o emergencia
- Un Centro de Control para la administración de la Red de Radiocomunicación
- Comunicación con el nodo central de la RNR.
- Comunicación con la PSTN (Red Telefónica Pública Conmutada)
- Misión crítica y alta disponibilidad
- Puesto de Operador de Radio
- Área de despachadores de voz con señalización completa de la RNR
- Grabación de comunicaciones de grupo con señalización completa
- Gestión del sistema para las comunicaciones de voz y datos de las diferentes organizaciones usuarias, es decir, gestión de redes virtuales permitiendo una gestión independiente para cada organización.
- En particular en relación con la georreferenciación de equipos móviles y portátiles, el despachador debe visualizar la posición de los radios móviles y portátiles que envíen su posición. El despacho contará con un sistema de

geolocalización tanto de los equipos móviles como de los portátiles. Debe observar todos los radios móviles y portátiles de la red de radio en el CS.

- Contar con un sistema de grabación IP de audio. Con base en los requerimientos de cada CS se establecerá el almacenamiento de información. El sistema de grabación debe permitir grabar comunicaciones de todo el sistema de radiocomunicación. La grabación debe ser transparente para los usuarios de los sistemas de radio. El sistema de grabación debe contener elementos tales como grabadoras, base de datos y/o estaciones de operadores que realicen operaciones en las grabaciones, servidor de almacenamiento, a fin de volver a escuchar conversaciones grabadas de:
  - Llamada privada
  - Llamadas cifrada de grupo
  - Llamadas estatales de grupo cifrada y troncalizadas
  - Llamadas múltiples cifradas y troncalizadas
  - Comunicación cifrada de grupo en la Red Nacional de Radiocomunicación
  - Llamadas privadas simultáneas
  - Llamadas de Emergencia, reconocimiento de Alarma de Emergencia
  - Llamadas de Emergencia, alarma de emergencia desde Consola
  - La estación del operador puede buscar por diferentes campos las llamadas grabadas

5.3.5 Generalidades

El Complejo de Seguridad que requiera actualizar su Sistema de Radiocomunicación de misión crítica debe considerar los siguientes puntos:

- Debe estar orientado a la actualización del protocolo de transporte de la RNR.
- **Interoperabilidad**. Los sistemas de Radiocomunicación que pretendan tener interoperabilidad con la RNR deben cumplir con lo establecido en los Lineamientos de Sistemas de Radiocomunicación de Seguridad Pública y los protocolos establecidos en el Apéndice A.
- **Sistema digital**. La digitalización debe habilitar la mejora en la calidad de audio sobre los sistemas analógicos, promoviendo:
  - Comunicaciones de voz más claras sobre un intervalo mucho mayor de cobertura.
  - Rechazo de ruido.
- **Operación troncalizada**
  - Operación Troncalizada. Manejo de recursos de manera eficiente, comunicaciones de alta densidad de usuarios.
    - Provee a los usuarios de acceso compartido de un grupo de canales de radio.
    - Para operación independiente y/o área amplia.
- **Múltiples configuraciones**

  - Soportar **operación** en las bandas de frecuencia asignadas de 380 a 400 MHz, asignada para seguridad pública.
- **Servicios de Seguridad**.
  - Autenticación de los equipos subscriptores.
  - Servicio de administración de llaves.
  -
  - Manejo de claves de comunicación por aire
- **Eficiencia espectral**.
  - Debe poder operar sobre canales de 10 kHz.

Las características funcionales mínimas con las que deben cumplir los sistemas de radiocomunicación del Complejo de Seguridad son:

- Comunicaciones digitales.
- Comunicaciones troncalizadas locales y de área amplia.
- Comunicaciones cifradas.
- Comunicaciones de voz y datos.
- Comunicaciones grupales.
- Capacidad de migración cumpliendo el Apéndice A.
- Configuraciones de alta disponibilidad.
- Cobertura.
- Configuraciones de diversidad en recepción.
- El mismo alcance de cobertura para los servicios de voz y datos.
- Soporte de configuraciones modulares y escalables.
- *Roaming* automático entre sitios.
- *Roaming automático en toda la cobertura de la RNR.*
- Algoritmos de cifrado.
- Máxima prioridad para las llamadas de voz, incorporación automática a llamadas de voz estando en una llamada de datos.
- Portafolio de opciones de mantenimiento.
- Protección contra vulnerabilidades del sistema que puedan comprometer la seguridad de la red y la confidencialidad de la información.
- Compatibilidad entre *software* y versiones de los sistemas.
- Cifrado de extremo a extremo.
- Interfaces de Programación de Aplicaciones para: Administración del Sistema, Operaciones de Despacho y Aplicaciones de Datos.
- Configuraciones de redundancia.
- Soporte de la Guía de Implementación Técnica de Seguridad.
- Solución de despacho avanzado.
- Solución de grabación.
- Solución de administración.

Para la parte de despacho se deben considerar los siguientes requerimientos:

- Todos los reportes de incidentes de emergencias arriban y son manejados por los CS del Estado.
- Todos los radios portátiles y móviles deben estar funcionando y administrados desde el CS.
- El supervisor de radio será el responsable de validar la información acerca de los radios utilizados en los centros de emergencia.
- El despachador será el responsable de crear las llamadas y determinar si se desea acceder al radio.
- El CS debe proporcionar la comunicación y acceso a los radios.

5.3.6 Características de la Red de Radiocomunicaciones

5.3.6.1 Características de dimensionamiento

La Red de Radiocomunicación debe cumplir con el apéndice A.

- Debe operar en la banda de frecuencias 380-400 MHz.
- Establecer el máximo número de radio bases que soporta.
- Soportar las entidades (Policía Federal, Estatal y Municipal, bomberos, entre otros) que requiera el CS, brindandoles el servicio de roaming de voz y datos.
- En la Radio base se debe establecer:
    - El máximo número de conmutadores, incluyendo los conmutadores de gestión.
    - El máximo número de celdas de radio.
    - El máximo número de terminales locales y terminales de paso.
    - El máximo número de comunicaciones de grupo de manera simultánea.

El Sistema de Radiocomunicación debe operar en la banda de frecuencias asignada a seguridad pública a nivel nacional, de acuerdo al Cuadro Nacional de Atribuciones de Frecuencias del IFT (Instituto Federal de Telecomunicaciones) de 380 a 400 MHz.

5.3.6.2 Características de transmisión

La Red de Radiocomunicación debe presentar las siguientes características de transmisión:

- El sistema debe ser completamente digital con conectividad IP y TDM.
- Permitir múltiples modos de operación, troncalizados.
- La transmisión en el canal radio utilizará la modulación apropiada al sistema de comunicación.
- Las comunicaciones se deben realizar en modo *Push-To-Talk*.
- El sistema debe contar con mecanismos de identificación cifrado extremo a extremo en las comunicaciones y desactivación de los terminales a distancia.

5.3.6.3 Características de gestión

La Red de Radiocomunicación debe presentar las siguientes características de gestión:

La gestión de la red se divide en tres funciones: técnica, táctica y operacional.

- La gestión técnica debe realizar la configuración, el monitoreo, la gestión de las alarmas, la supervisión y el mantenimiento de la red. El conjunto de las organizaciones de la red se gestiona a través de uno o varios operadores técnicos.
- La gestión táctica debe realizar la gestión de las terminales y de los usuarios, la gestión de los grupos y de las comunicaciones.
- La gestión y atención operacional de las comunicaciones se debe realizar desde una sala de control a través de consolas de despacho.

5.3.7 Arquitectura

Las estaciones bases garantizan la cobertura de la red y son gestionadas por los conmutadores. Todos los equipos de la infraestructura deben estar conectados por IP entre ellos por medio de enlaces alámbricos o inalámbricos con una velocidad y latencia que garanticen calidad de servicio.

El conjunto compuesto por los conmutadores y enlaces forma la base de la red de conmutación y enrutamiento.

La arquitectura de la Red de Radiocomunicación debe contar con el subsistema de gestión, el subsistema de conmutación y el subsistema de radio, tal como se muestra en la Fig. III.2.

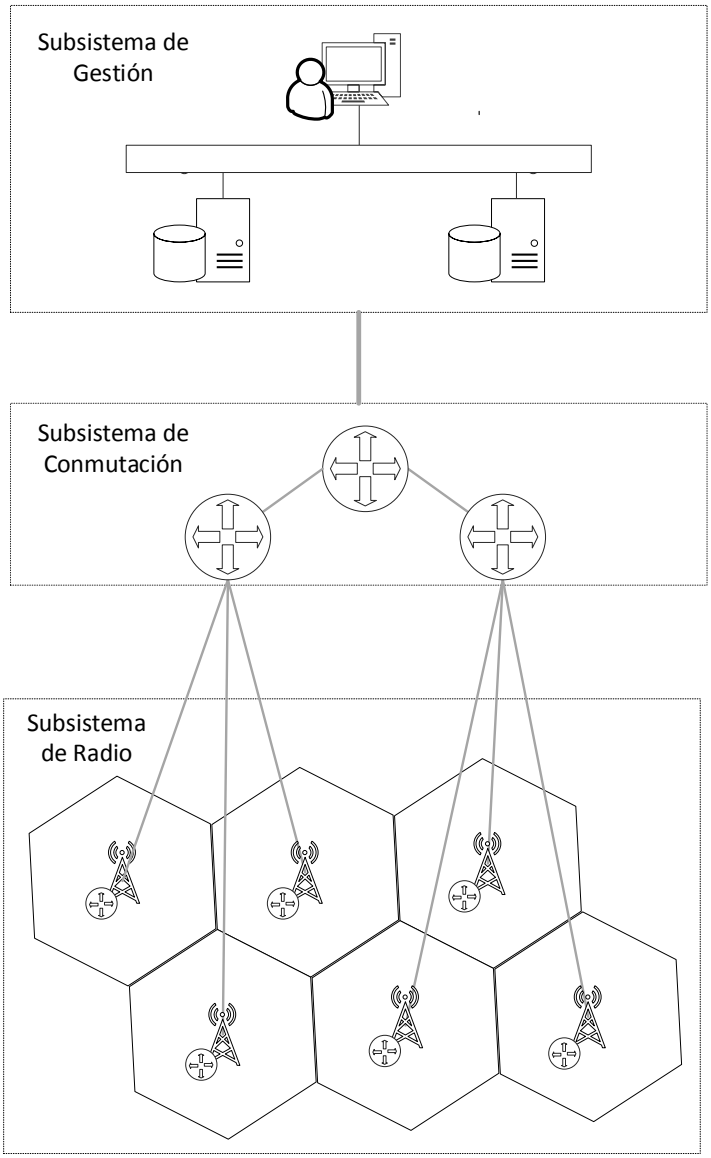


Figura III. 2 Subsistemas de la Red de Radio

5.3.7.1 Subsistema de Conmutación

El Subsistema de Conmutación se compone principalmente de los conmutadores de alta disponibilidad, sistemas de geolocalización mediante redundancia local o georedundancia y sistema de grabación, entre otros.

Se debe contar con conmutadores redundantes de gestión o primarios y conmutadores secundarios. Los conmutadores primarios se encargarán de la gestión

de la base de datos interna, gestión del cifrado, interconexión con la red *Ethernet* para las comunicaciones de datos, conexión con la RNR y con el subsistema de gestión, además de la centralización de información referente al tráfico de la red, alarmas y usuarios.

Los conmutadores secundarios se encargarán de la conmutación de circuitos para los servicios de voz, conmutación de paquetes para el servicio de datos, la señalización, gestión de dispositivos conectados como repetidores y puertas de enlaces.

Se pueden incluir repetidores alámbricos de radio que se conectan a través de enlaces físicos a terminales alámbricos. Los terminales alámbricos se recomiendan para el Puesto de Operador.

5.3.7.2 Subsistema de Radio

La cobertura de la Red de Radiocomunicación Estatal efectuada por estaciones base que cubren zonas denominadas como celdas.

Canales de radio

Cada estación base que realiza la cobertura de la red debe disponer de canales de radio de tráfico y al menos uno de control.

- Los canales de control se encargan del transporte de señalización y de los datos.
- Los canales de tráfico se encargan de la comunicación entre los usuarios, ya sea para el servicio de voz o datos.
- Los canales de datos dedicados tienen la funcionalidad de enviar mensajes cortos independientemente si la terminal se encuentra en un canal de voz o un canal de control permitiendo la transmisión de voz y datos de manera simultánea
- Los canales de control extendidos permiten gestionar una mayor capacidad de abonados bajo una célula para situaciones de emergencia o de operativos específicos

El operador técnico de la red debe definir del total de canales con que se cuente, de acuerdo a la evaluación de tráfico, cuántos canales de control, cuantos canales dedicados de datos y tráfico de voz se destinarán, de acuerdo a sus necesidades, así como a la asignación de estos canales para cada institución usuaria.

Se destinarán dos canales de frecuencias diferentes para una comunicación, uno para el enlace descendente (estación base a terminal) y el otro para el enlace ascendente (terminal a estación base), transmisión y recepción.

Equipos de radio

- El subsistema de radio se debe conformar, al menos, de los siguientes equipos.
- Estaciones base.

- Terminales de radio.

5.3.7.3 Subsistema de Gestión de infraestructura tecnológica

El subsistema de gestión se compondrá, al menos, de:

- Un servidor por red, conectado al conmutador de gestión.
- Uno o varios puestos de gestión técnica por red.
- Uno o varios puestos de gestión táctica por red.
- Uno o varios puestos operador por red, conectado al conmutador de gestión de red.

Servidor de la red de radiocomunicación

El servidor de la red de radiocomunicación debe soportar:

- La base de datos de la red con la información de la configuración y la gestión de la red; gestión de las terminales de las dependencias; de los grupos funcionales de abonados; y del sistema de comunicaciones.
- La base de datos que contiene los informes y las alarmas.
- Aplicativo dedicado a la configuración y gestión de la red.

Puesto de gestión técnica

El CS debe definir el número de puestos de gestión técnica que estarán conectados de manera local y, en caso de ser necesario, a distancia a través de una red *Ethernet* LAN (Red de Área Local) o WAN (Red de Área Amplia) al servidor de la red de radio, según se requiera.

Las principales funciones técnicas son:

- Visualizar el estado de los elementos de la red.
- Gestión técnica de las organizaciones.
- Gestión de las coberturas de la red.
- Gestión de las alarmas de los elementos de la red.
- Gestión de las funciones de explotación que permiten supervisar los distintos elementos de la red.
- Acceso a las funciones de gestión de la base de datos de aplicación, de gestión de la hora de la red de base, de modificación de los parámetros operacionales de las celdas y de los accesos alámbricos de las celdas.

Puesto de gestión táctica

El CS debe definir el número de puestos de gestión táctica que estarán conectados de manera local y en caso de ser necesario a distancia a través de una red *Ethernet* LAN (Red de Área Local) con IP o WAN (Red de Área Amplia) al servidor de la red de radio, según se requiera.

Las funciones tácticas son las encargadas de las tareas administrativas destinadas a proporcionar los servicios adecuados a los usuarios de la red en función de las misiones del CS.
Las principales funciones tácticas son:

- Identificación de las terminales móviles y portátiles.
- Programación de los servicios de las terminales móviles y portátiles.
- Formación de los grupos de comunicación.

Puesto de Operador de Radio (PO)

El PO principalmente se encargará de la gestión operacional de la red, podrá establecer comunicaciones, participar en las comunicaciones y monitoreo de los usuarios de la red.
El CS debe definir la prioridad del PO en las comunicaciones.

5.3.7.4 Interfaces que debe de contemplar el Complejo de Seguridad

Interfaces alámbricas

Para facilitar los servicios entre componentes principales de la infraestructura utilizados de forma alámbrica:

- Administración de Red (NOC externo al sistema de radiocomunicación).
- Interconexión Telefónica.

Interfaces para el despachador de radio
Interfaces físicas

El CS debe proveer un enlace físico y su respectiva configuración entre las estaciones de trabajo que utilizan el CAD y la Red de Radiocomunicaciones.

Interfaces lógicas

I. Funcionalidades

Evento	Descripción
1	Llamada a un grupo o radio específico con RFSI desde la pantalla de despacho del CAD
2	Selección de grupos desde el CAD
3	Ubicación geográfica de los radios por GPS
4	Mensaje de texto bidireccional con terminales.

5	Llamada de emergencia
6	Reconocimiento del RFSI de la terminal
7	Interconexión de llamada
8	Grabación de la conversación

II. Configuración de interfaces en cada CS

Modos operacionales de las interfaces de cada CS deben ser configurables:

- Fuera de línea, en este modo no existe ningún intercambio de datos entre los dispositivos.
- Modo de prueba, en este modo el supervisor de la red de radio se encarga de poder comunicar con los radios sin almacenar datos.
- Operación en tiempo real, en este modo el supervisor de la red de radio se encargará de administrar los incidentes y poder interactuar con los radios.

Considerando como mínimo las funcionalidades siguientes:

a) Botones de pánico.
b) Identificar perfiles de Usuarios.
c) Conocer el identificador del radio para llamada privada.
d) Activación de folio sólo para la grabación de llamada.
e) Conocer el identificador del grupo de habla
f) Grabador de conversaciones (relacionado sólo con la Emergencia)
g) Envío de Mensajes.
h) Gestión de unidades.
i) Gestión de llamada.
j) Geocerca con sistema de geolocalización de posición (GPS).
k) Configuración de grupos.
l) Licencia para usuarios.

Las cuatro áreas principales son:

1. Identificación, quién está comunicándose a través del radio

Identificar a un usuario específico con la función *Push to Talk* (PTT). La interfaz proporciona al despachador el nombre del usuario, el ID de la unidad, el ID de radio y el grupo de conversación asignado.

La experiencia práctica de esta función no es sólo identificar quién está hablando a través del PTT, sino que con mayor frecuencia se utiliza para identificar un incidente

de micrófono abierto. Los incidentes de micrófono abierto pueden ser intencionales y no intencionales. Los agentes a menudo involuntariamente activan sus botones PTT cuando se sientan en un vehículo y el equipo de su uniforme presiona el botón PTT en su radio portátil, o la ubicación del micrófono de la radio móvil causa un micrófono abierto.

Cuando el micrófono permanece abierto con los oficiales hablando en segundo plano, puede impedir que los oficiales de campo transmitan o reciban información el uno al otro. Debido a que las voces no están hablando directamente en un micrófono, puede ser difícil determinar la unidad por voz solamente. Esto puede tener consecuencias graves cuando existen situaciones de emergencia simultáneas, y es imperativo que estas situaciones de micrófono abierto se resuelvan rápidamente.

La interface puede resolver este problema. Los oficiales pueden presionar intencionalmente el botón PTT sin identificarse para transmitir una situación como cuando están luchando por controlar a un sospechoso. Otros oficiales pueden escuchar la situación y responder.

2. Emergencia, el uso de botones de alerta de emergencia

Los radios portátiles generalmente tienen dos o tres botones programables que controlan la iluminación de la pantalla, el cambio de canal o las funciones de emergencia. Cuando un botón está programado para la activación de emergencia, un oficial puede activar el botón discretamente para alertar a los despachadores de que tienen una situación de emergencia. La falta de comunicación de voz con la activación del botón de emergencia indicaría que son incapaces de hablar.

Un ejemplo: un oficial de policía de motocicleta en servicio que tuvo un accidente de motocicleta mientras trabajaba en que se cumplieran las leyes de tráfico. Incapaz de hablar debido a sus lesiones, el oficial podría usar la activación PTT o el botón de emergencia para indicar que había una emergencia. Sin la capacidad de localización del GPS, el despachador podría enviar oficiales a la última ubicación conocida del oficial para determinar el estado del oficial.

Hay casos en que los oficiales usan el botón para indicar una emergencia. Hay significativamente más instantes donde un oficial activa el botón por error. Es esencial que las agencias que usan la interfaz de radio desarrollen políticas antes de activarla, para definir cómo implementarán un protocolo escalonado para determinar la validez de la activación. Un protocolo puede ser pedir al despachador que intente obtener la verificación por voz de la emergencia desde la unidad. Si no hay respuesta, el

despachador enviaría otras unidades para ayudar. En las agencias donde se utilizó GPS los radios proporcionaban la latitud y longitud, y el despachador podía enviar unidades a la ubicación exacta. Si una agencia no utiliza GPS, el despachador enviará unidades a la última ubicación conocida.

3. Control, Despachador Radio Control

La interface de radio proporcionará al despachador la capacidad de organizar y cambiar grupos de conversación desde la línea de comandos del CAD o consola de administración de despacho del sistema de radio. Esto permite al despachador crear rápidamente grupos de conversación como fueran siendo necesarios para grupos con necesidades concurrentes específicas, tales como un grupo de narcóticos que sirve órdenes, una llamada de emergencia con un contenedor sospechoso ocurriendo en otra área al mismo tiempo, etcétera.

La interface permitirá al despachador cancelar grupos de la misma manera como fueron creados. La interface permitirá a los despachadores ejecutar una capacidad de reproducción a corto plazo de las últimas transmisiones de radio.

La reproducción será por un número limitado de segundos, pero que permita a los despachadores reproducir una transmisión que tal vez no hayan entendido o de la que no podían pedir verificación verbal debido a la emergencia o por el desarrollo de la situación emergente de los oficiales.

4. Análisis de archivo

El uso de la base de datos del registro de radio es para analizar el tiempo, la eficiencia, otros análisis y para responder a las preguntas operativas.

Análisis de archivo: los beneficios del archivo de registros de radio como parte de la interface de radio se derivan del uso de varias herramientas de análisis de bases de datos, en el CAD que había utilizado los registros de radio, para lograr objetivos operativos y administrativos.

El registro de radio documenta los eventos de PTT con una fecha y hora exactas de fracciones de segundos. Se puede reconstruir la llegada y las acciones de los oficiales en una situación de llamada de emergencia, haciendo referencia al identificador del grupo, al identificador del radio, a las fechas y horas que se observaron en los diversos sistemas utilizados en el Centro de Comunicaciones.

La activación del botón PTT para anunciar la llegada de los agentes a una llamada podría ingresar información del estado de este evento por medio de un despachador, en varios segundos.

Se puede evaluar las acciones de los oficiales basándose en los ingresos de registro en la interfaz de radio, en sus usos de la radio portátil o móvil. Al reconstruir incidentes, los oficiales posiblemente puedan identificar sus acciones, la línea de tiempo del incidente y si estaban dentro o fuera de su vehículo. Los identificadores de radio en el registro de interfaz de radio proporcionan pistas sobre esto.

Aunque los oficiales pueden utilizar sus radios portátiles en su vehículo, generalmente no lo hacen debido a un silenciamiento de retroalimentación que se produce debido a la proximidad de la radio portátil a la radio del vehículo.

5.3.8 Servicios

La Red de Radiocomunicación debe de ofrecer los servicios de voz y datos para los tres niveles de gobierno.

La terminal móvil o portátil podrá acceder a los servicios de la Red siempre que cumpla con:

- estar cargada, configurada y personalizada a través de la estación de programación de los terminales;
- dentro de la cobertura de la red;
- inscrita en la red.

5.3.8.1 Servicios de voz

Los derechos de acceso a los servicios se definen por los perfiles de usuario asignados a las terminales para las comunicaciones privadas y por la constitución de los grupos funcionales para las comunicaciones de grupo. Para cada terminal, la lista de los grupos funcionales a los que pertenece se actualiza dinámicamente por enlace de radio.

- **Comunicaciones privadas**. Se habilitan a petición de un usuario hacia otro o por varios llamados individuales, que reúnen: la llamada individual o la llamada múltiple.

- **Comunicaciones de grupo.** Las comunicaciones de grupo serán preestablecidas en una cobertura dada y destinadas a uno o varios grupos, que reúnen: llamada intra–grupo, conferencia, llamada general o llamada de

emergencia. Las comunicaciones de grupo podrán ser de tipo local o de tipo nacional.

- **Comunicaciones en modo directo.** Habilita la comunicación de radio a radio sin la necesidad de infraestructura de radiocomunicación.

- **Comunicaciones en modo repetidor independiente.** Servicio de comunicación fuera de red, con repetidor con un repetidor convencional, para extender el alcance del modo directo.

- **Conferencias inter-redes:** servicio de comunicación que permite establecer una comunicación de grupo que involucra a más de una red estatal de radiocomunicación.

5.3.8.2 Servicios de datos

El sistema de radiocomunicación debe ofrecer:

- Interfaces de datos cifrados. Para facilitar el intercambio de datos entre computadoras, redes de datos o fuentes de datos externos.
  - Interface con la red de datos. Específica en el contenido de los mensajes de datos.
  - Interface de datos con dispositivos periféricos. Permite la interconexión de subscriptores de radio móvil y portátil con computadoras portátiles, terminales de datos o unidades periféricas.
- Intercambio de mensajes entre servicios/aplicaciones específicas.
- Servicio de datos IP.
- Servicio de mensajes cortos (SMS).
- Servicio de mensajería.
- Servicio de reporte de ubicación.
- Distribución de llaves de cifrado.

5.3.8.3 Roaming nacional

El sistema de radiocomunicación debe contar con la capacidad de integrarse completamente con el nodo central de la red nacional de radiocomunicación a fin de permitir a los usuarios de la misma un libre desplazamiento en toda la cobertura nacional.

5.3.9 Seguridad

Como principal requerimiento el sistema de radiocomunicación debe apegarse a la Administración Nacional de Llaves y tendrá que sincronizarse con los estados de la República Mexicana. La comunicación debe ser cifrada de extremo a extremo en los

servicios de voz y datos. Se cuenta con un KMC a nivel nacional que se encarga de Administrar y generar las claves, la distribuye el KLU a la SPT, donde se cargan a las terminales. Debe considerar los siguientes puntos:

- Programación por interface Aire.
- Programación de llaves sobre la red *Ethernet*.
- Hombre caído.
- Activación de escucha de ambiente.
- Identificación del equipo.
- Cifrado de extremo a extremo. Se utilizará un protocolo de cifrado con llaves de 128 bps.
- Inhibir y habilitar equipo de radio.

5.3.10 Alta disponibilidad

El sistema de radiocomunicación debe contar con redundancia en:

- Redundancia de enlaces.
- Redundancia sitios principales.
- Redundancia sitio maestro.

5.3.11 Mejores prácticas

Solicitar a los fabricantes una lista de características de los productos que ofrecen, cuidando:

- Asegurar que las características requeridas son provistas por el producto.
- Preguntar si las características de los productos que ofrecen son desarrolladas en cumplimiento de esta norma.
- Asegurar que las características son diseñadas para ser interoperables con la norma.
- Preguntar si las características de los productos que ofrecen pasaron las pruebas aplicables.
- Asegurar que las características son verificadas para ser interoperables con la norma.

El Complejo de Seguridad debe contar con la documentación necesaria del Sistema de Radio como son:

- Manuales técnicos de los equipos
- Manuales de instalación
- Manuales de Mantenimiento
- Manuales de operación
- Protocolos de prueba
- Protocolos de aceptación (realizarlos)
- Memoria técnica
- Planes de mantenimiento
- Actualizaciones de *software*

El personal del Complejo de Seguridad debe tener capacitación relacionada a su perfil de puestos para que pueda operar, mantener, configurar y administrar el Sistema de Radiocomunicación.

5.4 Sistema de Video Vigilancia (SVV)

5.4.1 Objetivo

Definir arquitectura, protocolos y características que debe tener un sistema de video vigilancia y la Red LAN que lo soporta para el Complejo de Seguridad.

5.4.2 Alcance

Este capítulo indica las características técnicas que deben tener los elementos del Sistema de Video Vigilancia. Los apartados indican si son opcionales, obligatorios o si son condicionados a ciertos requerimientos. No se debe considerar como una guía de diseño. No se mencionan las características de las cámaras, puesto esta norma está dirigida a los sistemas que están instalados dentro del Complejo de Seguridad.

5.4.3 Campo de aplicación

Complejos de Seguridad.

5.4.4 Componentes de un sistema de video vigilancia para el Complejo de Seguridad

5.4.4.1 Arquitectura de un sistema de video vigilancia

5.4.4.1.1 Arquitectura basada en NVR y basada en Servidor

En los sistemas de video vigilancia se permitirán diferentes tipos de arquitecturas, clasificadas por la forma en que se administra el sistema, la manera en que ofrecen diferentes servicios y su almacenamiento.

Las arquitecturas se pueden resumir en las siguientes modalidades:

a) Distribuida o en el borde, definida así cuando su configuración de operación es autónoma y con ejecución de analíticas embebidas en el mismo dispositivo. Su almacenamiento principal, redundante o tolerante a fallas, se lleva a cabo de manera inicial al interior del mismo dispositivo y/o de manera alternativa o simultánea, en un sitio adicional, local o remoto.

b) Centralizada o basada servidores, donde se lleva la administración de usuarios, dispositivos, aplicaciones, bases de datos y reportes. Estos servidores pueden ser grabadores de video en red o NVRs, por sus siglas en inglés, servidores compartidos con otras aplicaciones o dedicados en un sitio determinado o

incluso en La Nube, sea ésta pública o privada, contratado como servicio de grabación primario, tolerante a fallas o redundante.

Como muestra la figura IV.1, el sistema de gestión de las cámaras está montado en un equipo dedicado, conectado a la red de datos, que a su vez ofrece comunicación con las cámaras IP de video digital. Un equipo dedicado ya está preparado para ofrecer servicio a cierta cantidad de clientes que se conecten a él, en el caso del NVR, los clientes serán cámaras y usuarios que visualizarán el video de las diferentes cámaras.

En la figura IV.2 se muestra que el sistema de gestión de cámaras está montado en un equipo de cómputo llamado Servidor. El Servidor debe ser dimensionado para ser eficiente y mantener un buen desempeño en el manejo de cámaras y almacenamiento de video, y atender las peticiones de usuarios que visualizan el video. En el dimensionamiento de un servidor se define:

i. Tipo de microprocesador a usar.

ii. Número de núcleos dedicados al software de gestión de video.

iii. Cantidad de memoria RAM y velocidad de su bus.

iv. Características de la tarjeta de red o de las tarjetas de red.

v. Características de discos duros.

Nota: Todas estas arquitecturas pueden satisfacer las necesidades del sistema de video vigilancia. Inclinarse por cualquiera de ellas, dependerá de factores técnicos, como ancho de banda disponible, capacidades de procesamiento en los servidores centrales, capacidad de almacenamiento, así como factores comerciales, como costos por servicios y licenciamiento.

c) Híbrida o mixta, cuando la solución, administración o reportes se encuentran parcialmente embebidos y parcialmente centralizados. Las ventajas de esta arquitectura se resumen un incremento considerable de la escalabilidad de cualquiera de las dos arquitecturas anteriores de manera aislada.

i. Permite almacenamiento redundante al grabar tanto en un servidor central como en su memoria interna, o bajo un modelo de tolerancia a fallos, donde en caso de que el sensor, dispositivo o periférico pierda comunicación con el servidor central o unidad de almacenamiento primario, tendrá la opción de

almacenar su información en otro dispositivo, interno o local, de manera temporal hasta el restablecimiento de la comunicación.

ii. El servidor central podrá administrar, además de usuarios, dispositivos, certificados y bases de datos, las diferentes funcionalidades disponibles, manejando los metadatos y relacionándolos directamente con distintas bases de datos, reduciendo la necesidad de grandes cantidades de ancho de banda y capacidades de procesamiento centralizado.

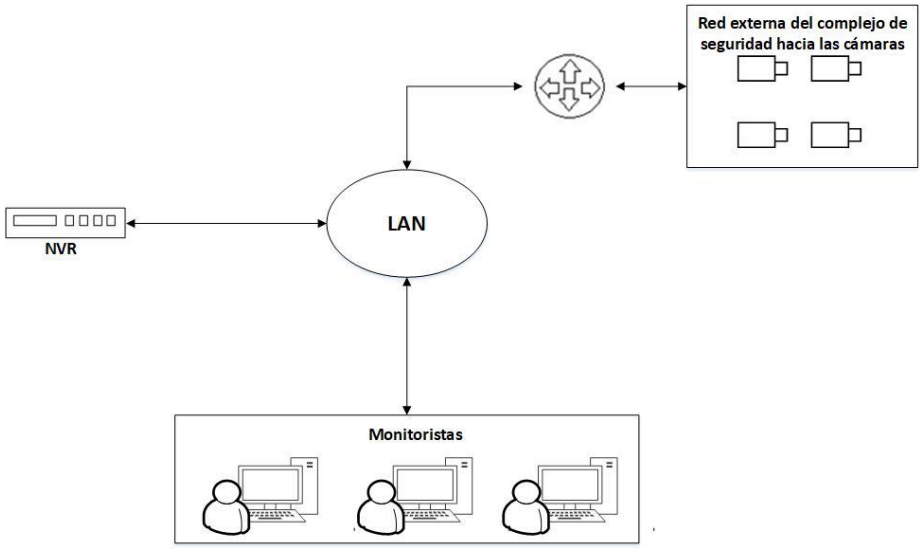


Figura IV. 1 Arquitectura de monitoreo basada en NVR

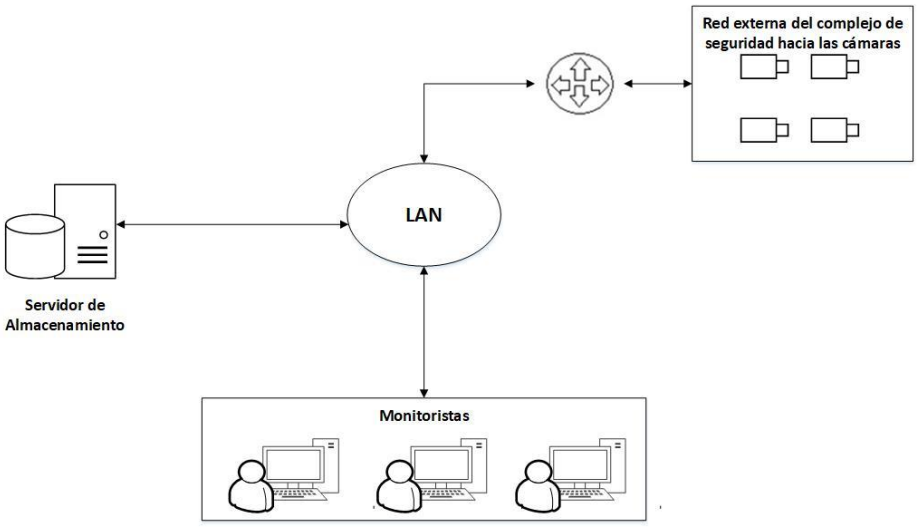


Figura IV. 2 Arquitectura de monitoreo basado en servidor

5.4.4.1.2 Arquitectura basada en sistemas de almacenamiento

Para los nuevos sistemas de video vigilancia se permiten los siguientes tipos de arquitecturas de almacenamiento:

a) Arquitectura basada en discos RAID tipo 1.

b) Arquitectura basada en almacenamiento NAS.

c) Arquitectura basada en un sistema de almacenamiento SAN.

d) Arquitectura basada en soluciones que puede combinar RAID con SAN.

e) Almacenamiento de conexión directa o DAS (Direct Attached Storage), conectado directamente al dispositivo y que puede funcionar como una memoria intermedia entre las arquitecturas mencionadas.

5.4.4.1.3 Requerimientos de las arquitecturas de almacenamiento

Los sistemas de almacenamiento para video vigilancia deben reunir los requisitos mencionados en el apartado 5.9.5, dependiendo de cuál arquitectura de almacenamiento se implementará.

5.4.5 El sistema de gestión de cámaras cliente y servidor

5.4.5.1 Del número de cámaras soportadas

El número de cámaras soportadas por el sistema de gestión de cámaras servidor no debe estar limitado por el mismo aplicativo. El número de cámaras soportado debe estar restringido por las licencias por cámara y por el hardware donde está montado el sistema de gestión de cámaras tipo servidor.

5.4.5.2 Protocolos de comunicación para la transferencia de video en el sistema de gestión de cámaras servidor

El sistema de gestión de cámaras servidor debe poder gestionar video proveniente de cámaras para su reproducción y almacenamiento. El sistema de gestión de video servidor debe trabajar con cámaras de diversas marcar o fabricantes, siempre bajo formatos y protocolos estándares. Los formatos de compresión que deberán ser utilizados, pueden ser cualquiera de los siguientes:

a) H.264

b) H.265

Los protocolos de comunicación para transmitir el flujo de video y para comunicarse entre dispositivos y servicios, deberán ser al menos:

c) RTP
d) RTPS
e) HTTPS
f) IGMP
g) FTP
h) SFTP
i) CIFS/SMB

a) Nota: los protocolos pueden trabajar de forma conjunta o individual y deberán contemplar medidas de seguridad adecuadas.

5.4.5.3 De los protocolos para administrar el NVR o el sistema de gestión de cámaras servidor

El NVR o el servidor donde está montado el sistema de gestión de cámaras servidor puede ser accesible para su administración sólo por uno o varios protocolos de la siguiente lista. No se permite un protocolo no seguro:

a. HTTPS
b. SSH
c. Puerto de consola
d. Interface iLO

Las contraseñas de acceso deben ser robustas.

5.4.5.4 Protocolos de comunicación entre el sistema de gestión de cámaras cliente y el sistema de gestión de cámaras servidor

El sistema de gestión de cámaras cliente debe proveer al personal que monitorea las cámaras, y a usuarios de administración del mismo sistema de video vigilancia una interfaz gráfica que se comunique con el sistema de gestión de cámaras servidor. Los protocolos y métodos de comunicación entre el sistema de gestión de cámaras cliente y el sistema de gestión de cámaras servidor son diferentes a los que se usan para transmitir el video. Para enviar video entre estos aplicativos pueden usarse los protocolos indicados en 5.4.5.2. Los protocolos de comunicación o métodos para comunicarse entre el sistema de gestión de cámaras cliente y el sistema de gestión de cámaras servidor pueden ser:

a) HTTPS: donde se usa un navegador de Internet para comunicarse con el gestor de cámaras.
b) SSH: donde la aplicación de gestión de cámaras cliente debe tener una interfaz gráfica.
c) Basadas en una API: puede ser una aplicación propietaria de un fabricante o desarrollada por el mismo Complejo de Seguridad, pero debe soportar los protocolos de comunicación para video mencionados en el apartado5.4.5.2.

5.4.5.5 Manejo de características de administración de video para su visualización o copiado en el sistema de gestión de cámaras cliente

Se enlistan características de administración de video para su visualización en el sistema de gestión de cámaras cliente. No se restringe el poder incluir otra característica que se considere relevante.

a) Se puede visualizar el video en directo y el del grabado, de forma eficiente y fácil para el personal de monitoreo y personal que administra el sistema de video vigilancia.
b) Debe permitir a múltiples usuarios visualizar el video de múltiples cámaras: no debe haber por parte del sistema de gestión de cámaras cliente o del servidor cámara, restricción del número de clientes que pueden estar conectados al sistema de gestión de cámaras servidor. La restricción en este sentido debe ser por el *hardware*.
c) Se debe poder poner diferentes tipos de vistas: en las vistas se visualiza el video de una o más cámaras. A continuación se enlistas los tipos de vistas principales:

    i. Vista completa: se ve el video de una cámara en toda el área de visualización del aplicativo.
    ii. Vista dividida: se ven varios videos de cámaras en el área de visualización del aplicativo. El número máximo de cámaras a visualizar dependerá de las necesidades específicas del Complejo de Seguridad.

d) Se deben hacer grupos de cámaras: los grupos de cámaras permiten ubicar y acceder fácilmente a una cámara identificada por alguna característica.
e) Se debe reproducir video almacenado.
f) Se debe poder escoger un video o parte de él y copiarlo a un destino especificado por el usuario, siempre que éste tenga los permisos para copiarlo.
g) Se debe poder hacer búsquedas de videos por diferentes criterios.
h) Se debe poder cambiar el formato de video al momento de copiarlo.
i) Se debe poder almacenar video en formato H.264 o H.265. Se permite uno de estos formatos si el otro no es requerido o soportado.

j) Se debe poder grabar en forma continua, por evento manual o programado, así como por resultado de alguna analítica activada.
k) Se debe poder escoger la resolución de grabación.

5.4.5.6 Características para administración de las cámaras desde el sistema de gestión de cámaras cliente

El sistema de gestión de cámaras cliente al estar conectado al sistema de gestión de cámaras servidor:

a) debe poder habilitar, deshabilitar y configurar SNMP v1,v2c,v3 de la cámara;
b) debe poder dar una dirección IP, máscara y puerta de enlace a la cámara;
c) debe poder actualizar el *firmware* de la cámara a través del protocolo FTP, TFTP o HTTPS: los protocolos mencionados para la actualización de *firmware* son los únicos admitidos;
d) configurar el protocolo NTP para tiempo si lo tiene disponible la cámara;
e) configurar asignación de direcciones IP manual o por el protocolo DHCP
f) configurar QoS si lo tiene disponible la cámara.

5.4.5.7 Características de acceso al sistema de gestión de cámaras cliente y al sistema de gestión de cámaras servidor

Para poder tener acceso al sistema de gestión de cámaras cliente o al sistema de gestión de cámaras servidor, se debe tener cuentas con diferente perfil de acceso. Debe haber 3 perfiles, sin restringir que el sistema pueda definir más. Los 3 perfiles deben tener las siguientes características:

a) Administrador general: tiene derecho a todas las opciones del sistema de gestión de cámaras cliente y servidor.
b) Operador: puede acceder a todas las opciones del sistema de gestión de cámaras cliente y del sistema de gestión de cámaras servidor, pero tiene restringido el crear, modificar o borrar usuarios de mayor nivel que él, además se le pueden restringir más opciones.
c) Acceso: sólo puede consultar el estado o servicios que ofrece el sistema de gestión de cámaras cliente y el sistema de gestión de cámaras servidor.

Nota: conjuntamente con estas características, se debe restringir las terminales que pueden acceder al sistema de gestión de cámaras servidor, implementando un mecanismo de autentificación a través del mismo sistema o en su defecto con un dispositivo de seguridad aparte. Para estos mecanismos de autentificación se pueden usar características de las terminales, sistemas operativos o de usuario, como pueden ser direcciones IP, direcciones de subred, direcciones MAC o nombres de host de las terminales, 802.1x, entre otras.

Las cámaras, grabadores y otros sensores y dispositivos conectados a la red y a los que se deba acceder con nombre de usuario y contraseña, bajo los niveles anteriormente mencionados, no deberán ofrecer acceso con clave de super usuario o contraseña definida por fábrica o terceros, ni procedimientos lógicos alternativos para acceder directamente a los equipos de manera anónima.

5.4.6 Equipo de cómputo de los monitoristas

5.4.6.1 Características de las computadoras personales

Las características de las computadoras personales que usan los monitoristas deben cumplir con las mencionadas en el apartado 5.5.5.3.1.1 en los incisos a) al d), y también cumplirán con los siguientes incisos enlistados:

a) contarán con dos salidas de video o más, de acuerdo a los requerimientos del Complejo de Seguridad;
b) la salida de video de la computadora personal permitirá una visualización adecuada de los videos presentados por el sistema de gestión de cámaras cliente.

5.4.6.2 Características de los monitores

El monitorista debe contar con un monitor en su escritorio, dedicado exclusivamente a la visualización de los videos de video vigilancia con el sistema de gestión de cámaras cliente. En caso de que el monitorista requiera usar otras aplicaciones, las visualizará con otro u otros monitores. Las características del monitor se enlistan a continuación.

a) El monitor debe contar con ajuste para su orientación e inclinación.
b) La imagen en la pantalla debe ser estable, sin destellos y reflejos.
c) El monitor debe tener la posibilidad de ajustar los niveles de intensidad luminosa, brillo y contraste, para adaptar la pantalla a las condiciones del entorno.
d) La resolución de los monitores debe permitir una visualización adecuada de la aplicación.
e) Las pantallas deben tener una relación de aspecto de al menos 16:9.

5.4.6.3 Características de los periféricos

a) Cada monitorista debe tener ratón ergonómico que cumpla con las características mencionadas en el apartado 5.5.5.3.1.3 inciso a).
b) Cada monitorista debe tener un teclado ergonómico que cumpla con las características mencionadas en el apartado5.5.5.3.1.3 inciso b).

5.4.6.4 Equipo Telefónico

El uso de un teléfono es opcional y su asignación depende de los requerimientos de trabajo del Complejo de Seguridad referentes al monitorista. En caso de ser requerido, debe cumplir con las características mencionadas en el apartado 5.5.5.3.2, incisos a) a f).

5.4.6.5 Del *joystick* o palanca de control para cámaras PTZ

El joystick que se debe usar por los operadores de video vigilancia, cuando se requiera, debe tener al menos las siguientes características:

a) el joystick debe ser con efecto de Hall de tres ejes: X/Y: para movimiento vertical y horizontal, Z: botón para el zoom.

b) Un teclado programable con funciones de acceso directo a aplicaciones definidas, para posicionar las cámaras a posiciones predeterminadas u otras herramientas para facilitar la navegación.

5.4.7 Videowall

5.4.7.1 Controlador del *videowall*

Para gestionar las pantallas del *videowall* se usará un dispositivo controlador de *videowall* que debe tener las características que se enlistan, lo cual no restringe el que tenga otras que sirvan para cubrir los requerimientos del *videowall* para el Complejo de Seguridad.

a) Uno o más puertos para conectarse a la Red LAN de tecnología *GigaEthernet*.
b) La conexión del controlador de *videowall* a las pantallas puede ser de una de las dos formas siguientes:
    i. a través de una red *fastEthernet* o *GigaEthernet*;
    ii. puertos de salida de video: en este caso se contará con los suficientes puertos de salida para el video, con el fin de conectar los monitores que se instalarán en el *videowall*, considerando puertos extras si se tiene proyectada una expansión a futuro del *videowall*.
c) Debe permitir ver un video en todas las pantallas del *videowall*, un video en cada pantalla del *videowall* y un video en más de una pantalla.
d) Debe poder soportar el envío de video con una resolución de HD, FHD o superior, de acuerdo a los requerimientos del proyecto del *videowall*.
e) El acceso al controlador del *videowall* para su administración y configuración y para la administración de los videos a visualizar en el *videowall,* debe realizarse a través de uno o varios de los siguientes protocolos o métodos listados. Si el equipo tiene protocolos no seguros, estos se deben activar:

i. HTTPS
ii. SSH
iii. Puerto de consola
iv. Interface iLO
v. Aplicación propietaria

f) Las contraseñas de acceso deben ser robustas.

5.4.7.2 Pantallas en el videowall

Se enlistan las características de las pantallas del *videowall,* sin restringir que se permitan otras, de acuerdo a los requerimientos del Complejo de Seguridad y de la Norma Técnica para Estandarizar las Características Técnicas y de Interoperabilidad de los Sistemas de Video Vigilancia para la Seguridad Pública.

a) La pantalla debe ser de una tecnología tipo LED o cualquier otra que evite la degradación de la imagen y dela definición de los colores.
b) Debe soportar HD, FHD o superior, de acuerdo a los requerimientos del sistema.
c) Las pantallas deben tener ángulos de visión de 170 grados o superior en la vertical y horizontal.
d) Las pantallas deben tener una relación de aspecto de al menos 16:9.

5.4.8 Características de la Red LAN para soportar el SVV

a) El equipo de comunicaciones debe poder identificar el tráfico de video basándose en diferentes criterios. Como ejemplo se mencionan direcciones de subred y *host* IP, direcciones Mac, puertos físicos y VLAN, entre otros, pero no se restringe el uso de uno que soporte en particular el equipo de comunicaciones.
b) El equipo de comunicaciones puede marcar las tramas o paquetes de video en los campos de la etiqueta de las VLAN o en el campo TOS/DSCP del encabezado del protocolo IP, para que los equipos de comunicación apliquen las políticas o los mecanismos de calidad de servicio a dichas tramas o paquetes IP.
c) Los equipos de comunicaciones del Complejo de Seguridad deben poder aplicar políticas o mecanismos de calidad de servicio al tráfico de video vigilancia.
d) La red de datos debe soportar el ancho de banda demandado por las cámaras del sistema de video vigilancia del Complejo de Seguridad, a través de los medios de conexión entre los equipos de comunicación, servidores, sistemas de almacenamiento y usuarios finales.
e) Se debe proveer el ancho de banda necesario, utilizando cualquier tecnología, protocolos, medio de comunicación con especificaciones o comportamiento certificado por un organismo internacional.

5.4.9 Dimensionamiento de servidores y almacenamiento

5.4.9.1 Dimensionamiento del servidor de video

El sistema donde se ubique la gestión de video debe poder soportar los flujos de video que le envían las cámaras que está administrando, almacenar dichos flujos y contestar a las peticiones que realicen los usuarios de monitoreo y administradores. Se debe considerar que las características de los flujos de video están dadas por:

a) Número de tramas por segundo (FPS) del video, estático o dinámico si estuviera disponible dicha opción. Si fuera distinto en diferentes cámaras, se debe considerar el promedio de FPS.

b) Tamaño promedio de la imagen: este valor depende de las siguientes variables:

i. Resolución del video
ii. Calidad de la imagen, nivel o porcentaje de compresión
iii. Compresión con H.264 o H.265
iv. Región de interés dinámico o porcentaje del área a monitorear
v. Estructura GOP dinámica

c) Número de cámaras.

d) 30 días de almacenamiento de los videos o más, de acuerdo con los requerimientos de diseño del Complejo de Seguridad.

e) Monitoreo continuo o por eventos.

5.4.9.2 Dimensionamiento de cantidad de almacenamiento para video

5.4.9.2.1 Requerimientos del sistema de almacenamiento

a) El sistema de almacenamiento debe poder mantener los videos de las cámaras durante 30 días o más, de acuerdo a los requerimientos del Complejo de Seguridad.
b) El sistema de almacenamiento debe proveer una arquitectura de alta disponibilidad en caso del daño de algún disco duro para recuperar información y que no se pierda la operación. Ver apartado 5.9.5.

5.4.9.2.2 Parámetros a considerar en el análisis del dimensionamiento del sistema de almacenamiento para el SVV

El análisis de dimensionamiento del sistema de almacenamiento debe considerar los siguientes parámetros:

a) Número de tramas por segundo (FPS) del video. En caso de que sea variable en diferentes cámaras, se debe considerar el promedio de FPS.

b) Tamaño promedio de la imagen. Este valor depende de las siguientes variables:
   i. Resolución del video
   ii. Calidad de la imagen
   iii. Compresión con H.264 o H.265
c) % de actividad del área a monitorear.
d) Número de cámaras.
e) 30 días de almacenamiento de los videos o más, de acuerdo a los requerimientos de diseño del Complejo de Seguridad.
f) Considerar un factor del 30% más de espacio de almacenamiento, adicional al calculado, para evitar que se saturen los dispositivos de almacenamiento.

5.4.10 Monitoreo y seguridad de los componentes del sistema de video vigilancia

5.4.10.1 Protocolos de monitoreo

El NVR o el servidor del sistema de gestión de cámaras y el controlador del *videowall*, si este último está considerado dentro del plan de monitoreo del Complejo de Seguridad, deben soportar los siguientes protocolos de monitoreo:

a) SNMP v2c y v3 de la familia de protocolos TCP/IP. Este protocolo permitirá generar consultas por el administrador del sistema de video vigilancia y mandar respuestas no solicitadas, si un dispositivo requiere avisar que sufre algún evento que deba atenderse por el personal a cargo.
b) MIB I y MIB II de la familia de protocolos TCP/IP, sin restringir el uso de otras MIB.
c) Registro de LOG: debe registrarse el acceso al equipo, interfaces caídas, apagado-encendido del dispositivo, así como modificaciones de configuración al sistema. No se restringe realizar el registro de otro tipo de eventos

5.4.10.2 Aplicativos de monitoreo con SNMP

El Complejo de Seguridad debe monitorear el estado del NVR o del servidor donde se instaló el sistema de gestión de cámaras servidor, así como a las cámaras mismas, a través de un aplicativo. Se pueden usar varios aplicativos en el caso de que uno sólo no pueda monitorear todos los aspectos de interés, o por facilidad de administración. Los aplicativos de monitoreo deben tener las siguientes características:

a) deben usar el protocolo SNMP v2c o SNMP v3 para realizar sus funciones de monitoreo y recepción de respuestas no solicitadas;
b) deben proveer un ambiente donde se pueda representar la topología a monitorear;
c) se debe restringir su uso a personal autorizado, con base en usuario y contraseña;

d) debe haber un aplicativo para poder recibir respuestas no autorizadas SNMP, en el caso de que el Complejo de Seguridad decidiera usar esta funcionalidad;
e) debe soportar la MIB I y MIB II de la familia de protocolos TCP/IP, sin restringir el poder soportar y usar MIB propietarias.

5.4.10.3 Variables a monitorear

Los aspectos a monitorear serán determinados por la persona encargada del Área de Telecomunicaciones, conjuntamente con el Área de TIC. Considerar cubrir los siguientes aspectos, sin restringir otros que determine el Área de TIC y el Administrador del Área de Telecomunicaciones:

a) estado del dispositivo a monitorear;
b) estado de tarjetas de red cuando se tiene más de una;
c) último reinicio o tiempo en que ha estado encendido el equipo;
d) cantidad de tráfico de entrada y salida;
e) uso de recursos de memoria y CPU.

5.4.10.4 Políticas de monitoreo del NVR o servidor del sistema de gestión de video vigilancia

a) Se debe monitorear el sistema de gestión de cámaras servidor para la detección y prevención de cualquier anomalía o falla.
b) Se debe tener reportes de eventos que puedan servir de evidencia en caso de presentarse un incidente de seguridad.
c) El monitoreo se debe realizar las 24 horas, los 365 días del año.
d) En caso de detectar un incidente, se debe corregir de forma inmediata.
e) Del monitoreo se debe poder generar información de forma estadística que permita conocer el comportamiento o desempeño del equipo a través del tiempo.
f) Se debe mantener una bitácora de cambios físicos y cambios de configuraciones.

5.4.10.5 Políticas de seguridad del NVR o servidor donde está montado el sistema de gestión de cámaras servidor

a) Protección contra ataques externos, colocando el sistema de almacenamiento, NVR o servidor en una VLAN para servidores y protegido en una Zona Desmilitarizada (DMZ).
b) En caso de que el sistema de gestión de cámaras servidor esté montado en un servidor, debe contar con un antivirus.
c) Las consolas o aplicativos de acceso al NVR, al servidor donde está montado el sistema de gestión de cámaras servidor y al sistema de almacenamiento, deben ser manejados por los administradores.

d) En caso de que el sistema de gestión de cámaras servidor esté montado en un servidor, se debe configurar las opciones de seguridad adicionales, de acuerdo al tipo de sistema operativo.
e) Tener activados protocolos de comunicación de acceso remoto seguros, como son HTTPS y Ssh, y desactivar protocolos de comunicación inseguros.
f) Para el caso de tener un servidor para el sistema de gestión de cámaras servidor, el servidor debe estar dedicado únicamente para el Sistema de Video Vigilancia.
g) Ya sea que el sistema esté basado en NVR, en un servidor central o cuente con una arquitectura distribuida, todos los equipos deberán mantenerse actualizados a la última versión de sistema operativo o firmware disponible.

5.4.10.6 Requerimientos sobre Cámaras Fijas

5.4.10.6.1 Uso de las cámaras fijas

Se deberán incluir cámaras fijas en el Sistema de Video Vigilancia. Las cámaras fijas ayudarán a detectar, con un sistema de análisis de video (analíticos) ya sea embebido, centralizado o distribuido, eventos que para el operador pueden pasar desapercibidos, además de que permiten mejorar el rendimiento y tiempo de respuesta ante posibles percances. De esta manera, las cámaras fijas auxilian a que el operador detecte vehículos o personas con comportamientos inusuales, conductas indebidas que, de acuerdo con un pronóstico, pudieran causar daños, infracciones o delitos. Además, de poder realizar reconocimiento facial y de manera automatizada, las matrículas vehiculares. Dependiendo del entorno ambiental, distancia de ésta al objetivo e intención de uso específico de la cámara, ésta deberá ofrecer las características de formato, tamaño, óptica y resistencia óptimas correspondientes.

Los analíticos usando cámaras fijas representan una ventaja dentro del Sistema de Video Vigilancia, adicionalmente a su capacidad de detección de movimiento, brinda al operador información en vivo y de vital importancia para la prevención, detección y despacho oportuno de eventos, así como para investigaciones de tipo forense en el futuro.

5.4.10.6.2 Características de video de las cámaras fijas

a) Deberá emplear la tecnología Digital IP.

b) La resolución mínima con la que debe contar la cámara debe ser de acuerdo al estándar HD, de 720p. o FHD 1080p o de mayor pixelaje, según la densidad de píxeles requerida por las analítica embebida, central o distribuida, así como para análisis a simple vista, según se requiera.

c) El lente puede ser fijo o varifocal y su distancia focal, dependerá de la relación del tamaño de sensor con la lente y el acercamiento requerido en el sitio a observar, así

como la distancia entre la cámara. su línea de enfoque y ángulo de visión mínimo requerido.

d) El sensor deberá ser preferentemente de tecnologías CCD o CMOS, pero serán aceptadas otras tecnologías que en el futuro, se conviertan en de uso mayoritario en la industria.

e) El zoom o acercamiento óptico y digital con el que debe contar la cámara, obedecerá a la intención de uso en cada zona a observar, la información que se desee obtener de ella (densidad de píxeles), relación de lente con el sensor de imagen y distancia entre la cámara y su línea de enfoque, así como al nivel de compresión digital, sin dejar de observar que la intención es obtener imágenes útiles o aprovechables.

f) La cámara deberá trabajar de acuerdo al estándar HD, FHD o superior, según se requiera y al menos, a la tasa de FPS que se ha definido para su grabación.

g) Los formatos de compresión con la que deberá trabajar la cámara, deberá ser consistente con lo especificado anteriormente en el presente documento.

h) La cámara empleada deberá permitir realizar ajuste de imagen en color, brillo, nitidez, balance de blancos, control de exposición y compensación de contraluz (autoiris).

i) La cámara debe contar con tecnología Día/Noche.

j) Si la cámara fuera a ser utilizada tanto en exteriores o interiores, pero con iluminación natural, deberá ofrecer la función de Rango Amplio Dinámico o WDR real.

k) Video inteligente: detección de movimiento por video o cualquier otra analítica embebida, podrá ser requerida dependiendo de las necesidades de cada sistema.

5.4.10.6.3 Características de red de las cámaras fijas

a) La cámara IP seleccionada debe ser compatible con los protocolos de comunicación descritos en el presente documento.

b) La seguridad deberá permitir uso de contraseña, filtro de dirección IP, cifrado HTTPS, control de acceso a red IEEE 802.1x y nuevos métodos de protección informática y de ciberseguridad.

c) Para permitir la actualización de la cámara, ésta deberá permitir la carga de nuevas versiones de firmware y/o de analíticas embebidas, utilizando al menos los protocolos descritos anteriormente, así como aquellos que demuestren su eficiencia y sea adoptados como estándares en la industria.

5.4.10.6.4 Características físicas de las cámaras fijas

a) La cámara fija a emplear, ya sea tipo caja, domo o bala entre otras variables disponibles en el mercado, dependerá de lo que más convenga para su uso en el ambiente donde vaya a ser instalada y al tipo de imágenes o datos que se esperan obtener, siendo criterios principales para la selección del formato, el tipo y tamaño de lente, la resistencia al medio ambiente y nivel de disuasión o discreción deseado.

b) La protección de la cámara contra el vandalismo deberá ser acorde al sitio de su ubicación y al riesgo principal existente, considerando al menos nivel IK08 para aquellas que no están al alcance normal de la gente, o de nivel superior en los casos donde se justifique. Deberá ofrecer grado de protección contra ingreso de líquidos y partículas, de acuerdo con lo definido en IP66 y deberá ofrecer resistencia a la corrosión, de acuerdo con el estándar NEMA 4X.

c) La cámara deberá contar con el herraje apropiado para su montaje.
d) El peso máximo de la cámara instalada, deberá ser de acuerdo con las condiciones físicas del sitio y accesorios de montaje, de acuerdo con la altura del poste (en su caso) y especificaciones de anclaje del mismo.

e) El intervalo de temperatura que deberá soportar la cámara para operar adecuadamente en la región donde vaya a ser instalada, debe encontrarse dentro de las temperaturas máximas y mínimas históricas registradas del sitio por el Servicio Meteorológico Nacional en la ubicación correspondiente.

f) La conexión de entrada de la cámara debe ser compatible con los conectores RJ-45 para redes 10BASE-T/100BASE-TX o 10BASE-T/100BASE-TX/1000BASE-T.

g) La alimentación debe ser compatible con PoE, PoE+ o High PoE, de acuerdo con la capacidad del switch o inyector a utilizar.

h) La memoria extraíble en las cámaras para guardar video localmente puede ser opcional u obligatoria, dependiendo de la arquitectura definida para el sistema, según lo descrito anteriormente (distribuida, centralizada o híbrida).

i) Podrá solicitarse soporte a audio, siempre que su uso esté contemplado en las particularidades del sistema, al igual que contactos de entrada y salida para conectar dispositivos externos.

j) La iluminación IR integrada, podrá ser necesaria en aquellos casos donde la iluminación ambiental sea insuficiente para ver a color con la cámara propuesta y su alcance, deberá ser suficiente para iluminar hasta la línea de enfoque. En casos necesarios, podrá ser complementada con iluminadores externos.

5.4.10.7 Sistemas de videovigilancia colaborativa.

Los sistemas de video colaborativo constituyen una tendencia mundial, competitivas y accesibles en costo-eficiencia. En su concepto estos sistemas facilitan el video alertamiento de la ciudadanía hacia el gobierno mediante sistemas basados en la nube. A continuación de presentan los principales atributos de estos sistemas, así como los elementos para su estandarización técnica mínima y su correcta implementación.

5.4.10.7.1 Atributos de funcionalidad.

a) La transmisión del flujo de video hacia la nube debe ser a través de internet.
b) Las cámaras que se integren al sistema deberán trasmitir a Internet sin necesidad de dispositivos adicionales, instalación de software o reenvío de puertos.
c) El monitoreo de video y búsqueda de archivos podrá realizarse desde un sistema central de monitoreo, vía web o vía aplicativo móvil (APP).
d) El sistema debe permitir el monitoreo de todos los sistemas de seguridad distribuidos en diferentes ubicaciones ya sea de forma individual, en grupo o en su totalidad.
e) Debe permitir opciones de conexión en línea desde un servidor físico a la nube, para visualización y acceso al video grabado o puede utilizar un servidor virtual en la nube sin necesidad de un hardware fisco.
f) Debe permitir la visualización de las cámaras desde el centro de monitoreo bajo demanda o mediante un sistema central de administración de las diferentes plataformas.
g) Debe permitir la visualización del flujo de video de las cámaras desde un dispositivo móvil bajo demanda.
h) Debe permitir que desde un dispositivo móvil se envíe flujo de video en tiempo real hacia la plataforma de monitoreo.
i) Debe considerar la integración de algún elemento detonador de eventos, este puede ser un sensor, un botón físico, un control de acceso o un detonador lógico como una aplicación para dispositivo móvil APP.
j) El video deberá estar correlacionado con los eventos del sistema tales como sensores, alarmas, control de acceso y eventos de intrusión, todo integrado en una misma plataforma operativa.
k) El sistema basado en la nube debe considerar integrarse a una plataforma operativa única que permita integralidad en el monitoreo, búsqueda y manejo de eventos vinculados en tiempo real, tales como la administración de alarmas, la generación de informes y la reproducción de eventos.

l) Tanto el sistema de nube como la plataforma operativa única, debe contar con mecanismos de seguridad tales como el uso de encriptación avanzada, certificados digitales o autenticación basada en notificaciones.

5.4.10.7.2 Especificaciones técnicas

a) Hospedaje basado en nube como VSaaS (Video Surveillance as a Service)
b) Debe permitir operar las configuraciones de la cámara de forma local o remota.
c) Uso de base de datos para almacenamiento de datos relacionados y almacenamiento de video local.
d) Deberá permitir que múltiples usuarios visualicen un video en múltiples ubicaciones de forma simultánea, utilizando el ancho de banda de cada segmento de red solo una vez por conexión a la red. para obtener acceso instantáneo a todas las cámaras con los privilegios correspondientes.
e) El sistema de nube debe integrarse a la plataforma operativa única, esta última debe ser abierta con opciones de integración mediante kits de herramientas de integración SDK, DDK de intrusión o arquitectura de complementos.
f) La plataforma debe ser compatible con los protocolos más comunes de video como H.265, H.264, MPEG-4, MJPEG, Wavelet y JPEG2000.
g) Debe ser compatible con tecnología de codificación SSL (capa de sockets seguros) de 128 bit y con HTTPS (protocolo seguro de transferencia de hipertexto) para proteger la comunicación con dispositivos periféricos.
h) Debe contemplar el monitoreo en tiempo real basado en mapas interactivos para ver y administrar los eventos, permitiendo importación en formato KML, interfaz de mapas interactivos, respuesta a alarmas activadas en mapa, e importación en formato de vectores.
i) El licenciamiento para grabación en nube por cámara deberá contemplar resoluciones desde 640x480 hasta 1920x1080p con grabación continua en la nube, debiendo considerar al menos 6 días de grabación con tasas de 10 y hasta 15 cuadros por segundo.
j) El sistema detonador de eventos deberá integrarse y operar sobre la plataforma operativa única de monitoreo permitiendo vincular el evento con el video en tiempo real, a fin de que el centro de monitoreo visualice las cámaras y datos mínimos como fecha, hora, georreferenciación sobre un mapa interactivo, datos generales del usuario vinculados al sistema.
k) El evento detonado, además de mostrarse en la plataforma operativa única, deberá tener la opción de visualizarse en línea a un dispositivo Smartphone o tableta, mostrando los datos generales con acceso al video en tiempo real.
l) La plataforma operativa única debe activar una alarma sonora y visual de manera en el centro de monitoreo así como en los dispositivos móviles asignados según sea el caso.
m) La instalación se recomienda en postes tipo cónico circular de entre 4.5 y 5.5 metros de altura, galvanizado por inmersión en caliente y construido en acero calibre 11, con soporte en tubo de 2" cedula 30 tipo rolado, con tapa abombada

desmontable en calibre 12, placa de asiento de 3/8" de 30 x 30 cm, 4 cartabones en placa de 1/4´´, soporte para 4 cámaras en tubo de 3´´ calibre 16, accesorios para soporte de cámaras, base cuadrada para instalar un botón de emergencia. base de concreto prefabricada de 62cmx62cmx70cm, con 45 cm de corona, con resistencia de 200kg/cm2, anclas galvanizadas de 3/4".

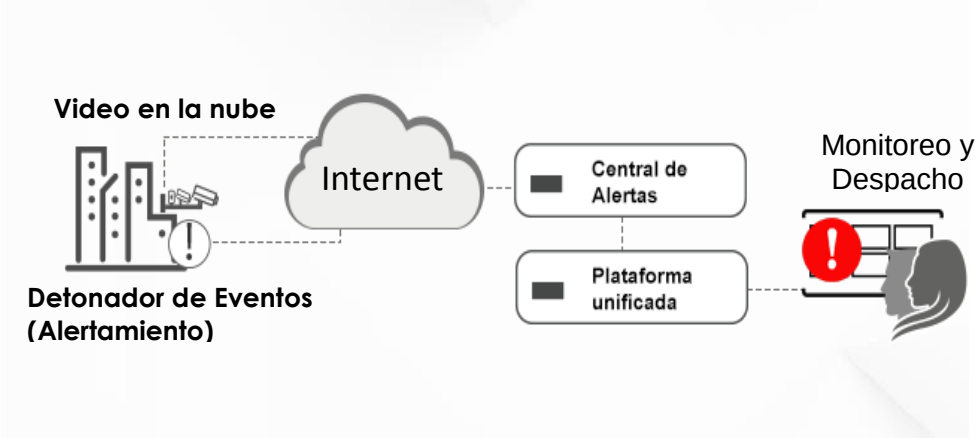


Figura IV. 3. Arquitectura de sistemas de video colaborativo en la nube.

5.4.10.7.8 Consideraciones para la instalación y puesta en operación de Sistemas de Video Vigilancia para poblaciones declaradas como "Pueblos mágicos" o para edificaciones catalogadas por el Instituto Nacional de Antropología e Historia

Para la instalación de cámaras para los Sistemas de Video Vigilancia se deberán tomar en cuenta las normas aplicables en la materia, a continuación se enumeran algunas:

- Ley Federal sobre monumentos y zonas arqueológicas, artísticos e históricos, así como su reglamento.
- Acuerdo por el que se establecen los Lineamientos generales para la incorporación y permanencia al Programa Pueblos Mágicos, publicado por la Secretaría de Turismo en el Diario Oficial de la Federación el 26 de septiembre de 2014.
- Reglamentos estatales o municipales sobre monumentos, zonas arqueológicas y/o patrimonio histórico- cultural.
- Norma Técnica para Estandarizar las Características Técnicas y de Interopersabilidad de los Sistemas de Video Vigilancia para la Seguridad Pública.

Para la instalación y puesta en operación de Sistemas de Video Vigilancia deben apegarse a los requerimientos de las autoridades correspondientes (por ejemplo el Instituto Nacional de Antropología e Historia y/o la Secretaría de Turismo), así como contar con el oficio o documentos suscrito (s) por la o las autoridades competente en el que se señale el aval o permiso para la colocación del Sistema de Video Vigilancia de conformidad con las necesidades de la edificación y/o comunidad.

5.5 Servicio del Centro de Atención de Llamadas de Emergencia 9-1-1 (Nueve Uno Uno)

5.5.1 Objetivo

Establecer y/o actualizar los requerimientos técnicos necesarios de los Centros de Atención de Llamadas de Emergencia a través del número único armonizado 9-1-1 (Nueve-Uno-Uno) del Complejo de Seguridad (CS) y su interacción con el Sistema de Video Vigilancia (SVV).

5.5.2 Alcances

Las características y especificaciones definidas en este apartado aplican a la infraestructura de telecomunicaciones de los Complejos de Seguridad, no es una guía de diseño y debe ser leído por personal capacitado en tecnología de telecomunicaciones.

5.5.3 Campo de Aplicación

El campo de aplicación de la presente Norma Técnica establece los requerimientos técnicos necesarios de los Centros de Atención de Llamadas de Emergencia a través del número único armonizado 9-1-1 (Nueve-Uno-Uno).

5.5.4 Descripción

El presente apartado tiene como finalidad plantear la estandarización del servicio del Centro de Atención de Llamadas de Emergencia (CALLE) a través del número único armonizado 9-1-1 (Nueve-Uno-Uno), tomando como referencia el documento “Norma Técnica para Estandarizar los Servicios de llamadas de Emergencia a través del número único armonizado 9-1-1 (Nueve, Uno, Uno)”. Asimismo, se definirán y/o actualizarán los aspectos tecnológicos indispensables para lograr su objetivo, asi como los aspectos tecnológicos indispensables para lograr la interoperabilidad del servicio de Atención de Llamadas de Emergencia a través del número único

armonizado 9-1-1 (Nueve-Uno-Uno) con el Sistema de Video Vigilancia (SVV) que se encuentra dentro del Complejo de Seguridad (CS).

El CS tiene como finalidad prestar un servicio de atención temprana y oportuna a los ciudadanos que se comuniquen para reportar una emergencia. Éstas pueden generarse a través de una llamada al Centro o a través de una aplicación móvil. Independientemente de la forma en que la emergencia sea reportada, el área de los operadores es el primer contacto con ella. Cada operador cuenta con un equipo específico para la captura de información que reporta el ciudadano. Dicha informacion es albergada en el CS, para darle seguimiento a todo el proceso que se sigue en la atención de la misma. Una vez que se ha registrado, la emergencia es canalizada al área de los despachadores, asignándola a la dependencia (de acuerdo al Catálogo Nacional de Incidentes de Emergencias), quienes asignan a los elementos para la atención.

La designación de los recursos en la atención de cada una de las emergencias, depende del tipo de emergencia y magnitud de la misma. Toda la información recabada de una emergencia se almacena en una base de datos propia del Centro de Atención de Llamadas de Emergencia.

Los aspectos técnicos que se considerarán en este apartado son:

a) Aplicativo "Despacho Asistido por Computadora" (*Computer Aided Dispatch* CAD)
b) Central Telefónica (Conmutador – *Gateway* y tarjetas de expansión)
c) Equipo y funcionalidades de los Equipos de los Operadores
d) Sistema de Información Geográfica (*Geographic Information System* GIS)
e) Tecnologías Emergentes

En la figura V.1 se presenta un diagrama general a bloques de los elementos que integran el CALLE: área de operadores (equipo de los operadores y aplicativo), Central Telefónica y su conexión a la red de área local (LAN) del CS.

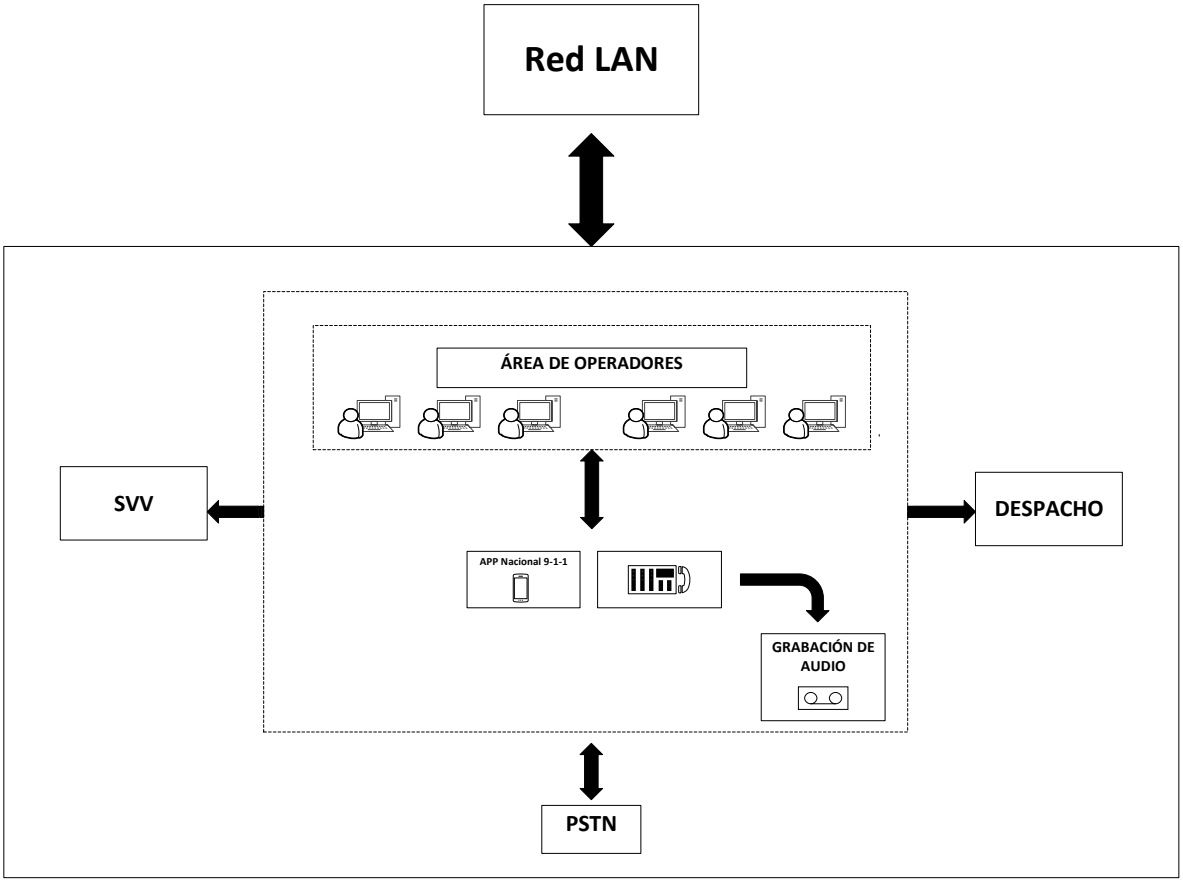


Figura V. 1 Diagrama General a Bloques de los elementos que integran el CALLE

El objetivo es lograr homogeneidad en la operación entre los CALLE que se encuentran ubicados en los CS, la cual es necesaria para lograr interoperabilidad entre los diferentes sistemas que integran el CS y entre los sistemas de otros CS.

Los requerimientos plasmados en este manual deben ser compatibles con los CS ya establecidos y así lograr interoperabilidad entre ellos.

Esta norma no incluye el diseño de sistema de tierras, aire acondicionado, respaldo de energía y en general acondicionamiento del área del CALLE.

5.5.5 Norma para el Servicio de Atención de Llamadas de Emergencia 9-1-1 (Nueve Uno Uno)

5.5.5.1 Despacho Asistido por Computadora (*Computer Aided Dispatch*, CAD)

Los requerimientos necesarios que debe cumplir el CAD para su implementación en el sistema 9-1-1 del CALLE, son los expuestos a continuación.

5.5.5.1.1 Especificaciones Técnicas y Funcionalidades del CAD

- Debe ser capaz de integrarse a cualquier sistema operativo.
- Debe estar alojado en los equipos de los operadores del 9-1-1 y ser capaz de integrarse a una red local.
- Debe vincularse o integrarse al sistema SVV y al área de despacho.
- Debe tener un servidor asociado en el cual se almacenen al menos los siguientes registros de las llamadas al 9-1-1:
    - Llamadas entrantes
    - Llamadas pérdidas
    - Llamadas en cola
    - Duración de llamada
    - Tiempo de llamada en cola
- Debe poder abrir registros y obtener sus actualizaciones en tiempo real.
- Debe poder consultar el historial de todos los registros de llamadas, además de poder consultar por tipo de incidente, por fecha entre otros criterios de búsqueda.
- Deben poder integrarse voz y datos para una comunicación óptima.
- Deben poder integrarse *N* corporaciones de emergencia estableciendo una comunicación eficiente, cumpliendo con los diferentes tipos de emergencias que se establecen en el Catálogo Nacional de Incidentes de Emergencias.
- Debe poder realizar una asignación eficiente de recursos para atender a las llamadas de emergencia, es decir, que la asignación de la emergencia del operador hacia el área de despacho correspondiente sea efectiva.
- Debe poder integrarse un *software* actualizado dedicado con el Sistema de Información Geográfica (GIS, por sus siglas en ingles).
- Debe mostrar la identificación del número que llama.
- Debe poder establecer una comunicación a nivel de red con la Central Telefónica.
- Las llamadas entrantes del 9-1-1 y registradas en el CAD se deben grabar en la Central Telefónica. El tiempo de registro de las llamadas debe ser de al menos 1 año. Dicho respaldo debe realizarse automáticamente, así como el borrado de la información.
- La información recibida de cada llamada de emergencia debe de almacenarse de forma automática en un sistema manejador de base de datos, generándose el "*Número de Identificación Automática* (*Automatic Number Identification*, ANI)", de tal forma que pueda distinguirse cada evento y se le pueda dar

seguimiento. Asimismo, este identificador debe de ser único y es mediante el cual cada uno de los sistemas ligados al 9-1-1 del CS pueden identificarlo.

- Debe contemplar la aceptación de ANI (*Automatic Number Identification*) y ALI (*Automatic Location Identification*).
- Los registros del CAD se deben almacenar en su servidor en formatos estándar.
- Se debe poder establecer una relación entre los registros del CAD y su correspondiente archivo de audio almacenado en la Central Telefónica.
- Debe poder registrar las incidencias atendidas por cada operador y se deben almacenar en su servidor correspondiente.
- Se debe dimensionar la Central Telefónica de acuerdo al análisis de dimensionamiento de llamadas del CS, considerando los siguientes lineamientos:

    a) Los equipos de central telefónica no deben superar el 80% de uso en recursos de físicos de cómputo.
    b) El equipo de central telefónica debe manejar alta concurrencias de llamadas de acuerdo al análisis de llamadas en hora pico.
    c) El ambiente de central telefónica debe tener la capacidad de configuración de agregar más equipos de centrales telefónicas.
    d) El ambiente de central telefónica debe tener la capacidad de balanceo de carga tanto en el ambiente local como en un ambiente de central telefónica remota.

- Se debe dimensionar el sistema de almacenamiento de llamadas de acuerdo al análisis de dimensionamiento de llamadas del CS. Se debe considerar los siguientes factores:
    - Número de llamadas al día
    - Número promedio de duración de llamadas
    - Tipo de codificador
    - Tiempo de almacenamiento de llamadas
    - Factor del 30% de espacio libre
- Debe contar con la detección de alertamiento de los botones de pánico, que a su vez deben estar ligados al Sistema de Video Vigilancia, con la intención de poder ubicar a través de las cámaras el evento que se reporte por este medio.
- Puede o no contar con la funcionalidad de detección de alertamiento de emergencias en bancos, autobuses urbanos, así como nuevas tecnologías que se desarrollen para promover la seguridad pública y ciudadana.
- Debe contar con la interfase de funcionalidad de detección de alertamiento de emergencias con la Aplicación Nacional 9-1-1.

5.5.5.1.2 Controles de Acceso del CAD

- El acceso al aplicativo CAD debe realizarse por medio de usuario y contraseña. Cada operador debe tener un nombre de usuario que lo identifique. Las contraseñas se deben actualizar de acuerdo a las políticas de seguridad del CS.

- A los usuarios que hagan uso del aplicativo CAD se les debe definir su nivel de acceso a través de perfiles. El perfil mínimo debe definir tres niveles de acceso, sin restringir que el aplicativo CAD pueda definir más. Los tres niveles de acceso en un perfil pueden ser:

  - Administrador General: tiene derecho a todas las opciones del aplicativo CAD.
  - Operador: puede tener acceso a todas las opciones del aplicativo CAD pero tiene restringido crear, modificar o borrar usuarios de mayor nivel que él como restricción básica, pudiendo restringírsele más opciones.
  - Acceso: sólo puede consultar el estado o servicios que ofrece el aplicativo CAD.

Nota: conjuntamente con estas características, se debe restringir las terminales que pueden acceder al aplicativo CAD implementando un mecanismo de autentificación a través del mismo aplicativo CAD o con un dispositivo de seguridad adicional.

5.5.5.2 Central Telefónica

La Central Telefónica estará integrada por: conmutador, *Gateway* y tarjetas de expansión.

Los requerimientos indispensables que debe cumplir la Central Telefónica para su implementación en el sistema 9-1-1 son los que se detallan a continuación.

5.5.5.2.1 Especificaciones Técnicas de la Central Telefónica

- Debe tener la capacidad de integrarse con los diferentes sistemas del Complejo de Seguridad mediante el uso de protocolos y/o estándares abiertos. De igual forma debe poder integrar cualquier aplicación necesaria para el correcto funcionamiento del Sistema de Atención de Llamadas de Emergencia a través de protocolos y/o estándares abiertos.
- Se debe contar con:
  - conmutador tipo PBX IP para los servicios de Telefonía

  - dispositivo Gateway de interconexión
  - El conmutador y el *Gateway* pueden o no estar integrados en un mismo dispositivo
- Debe contar con al menos TIER III.
- Debe poder conectarse a la Red Telefónica Pública Conmutada (PSTN, por sus siglas en inglés) a través de troncales digitales E1 o líneas telefónicas digitales de acuerdo a las necesidades del análisis de dimensionamiento de llamadas del CS.
- Las intercomunicaciones deben basarse en el protocolo de comunicación IP.
- Debe poder integrarse a la red de Sistema Global para las Comunicaciones Móviles (GSM, por sus siglas en inglés) para el Servicio de Mensajes Cortos (SMS, por sus siglas en inglés).
- Debe tener puertos de Red de Área Local (LAN, por sus siglas en inglés).
- Debe tener puertos de red para interconectarse a la Red de Área Amplia (WAN, por sus siglas en inglés) para intercomunicarse con otras centrales telefónicas.
- Debe tener puertos analógicos para teléfonos analógicos en caso de que se requieran.
- De acuerdo al análisis de dimensionamiento de llamadas, la central debe soportar el máximo número de llamadas en las horas pico más un 20%.
- Debe ser escalable a futuras necesidades del sistema Nueve-Uno-Uno (9-1-1). La Central Telefónica debe estar preparada para crecer por adición de nuevos módulos de conexión a la PSTN, integrarse con otra Central Telefónica de extensión y agregar más extensiones.
- La Central Telefónica debe estar bajo un esquema de alta disponibilidad con un conmutador redundante en el mismo CS.
- Debe soportar los siguientes codificadores: G.711, G.723.1 y/o G.729.
- Debe soportar el protocolo H.323, SIP y/o IAX2, dependiendo de los requerimientos del CS.
- Debe de tener la capacidad de grabar todas las conversaciones telefónicas recibidas a su disco local, en red SAN o NAS, dependiendo de los requerimientos del almacenamiento del CS.
- Debe soportar la adición de más extensiones telefónicas sin necesidad de adquirir licencias extras.
- Debe de tener contratado un servicio de mantenimiento con el proveedor o fabricante que incluya:
  - Servicio de soporte técnico vía telefónica de 24x7 todo el año.
  - Servicio de soporte técnico en sitio.
  - Servicio de cambio de partes dañadas.
  - Acceso a nuevos *firmwares* para la Central Telefónica.
  - Actualización de *firmware*.

- El proveedor en el momento de la entrega, instalación y puesta en marcha de la Central Telefónica, debe entregar:
  - Manual Técnico
  - Manual de Instalación
  - Manual de Mantenimiento
  - Manual de Operación
  - Protocolos de prueba
  - Pruebas de Aceptación
  - Memoria Técnica

5.5.5.2.2 Funcionalidades de la Central Telefónica

- Debe integrarse y/o incluir un tarificador de llamadas que registre al menos lo siguiente:
  - número de llamadas entrantes
  - duración de llamadas
  - número de llamadas perdidas
  - tiempo de cola de llamadas
  - número de llamadas en cola
- Debe poder generar estadísticas del traficador de llamadas.
- Debe contar con la aplicación de Distribución Automática de Llamadas (ACD, por sus siglas en inglés).
- Debe contar con la aplicación de Respuesta de Voz Interactiva (IVR, por sus siglas en inglés), dependiendo de los requerimientos del CS.
- Debe contar con un módulo para controlar las llamadas de broma.
- Debe contar con las siguientes funcionalidades, sin restringir otras que dependen de requerimientos específicos del 9-1-1:
  - desvío de llamadas
  - transferencia de llamada
  - llamada en espera
  - remarcación de último número para llamadas internas y externas
  - anuncio de llamada
  - grabación de voz automática o manual, dependiendo de los requerimientos del 9-1-1
  - discado abreviado
  - identificación de número llamado (DNIS, por sus siglas en inglés)
  - marcación automática para llamadas perdidas

5.5.5.2.3 Controles de Acceso a la Central Telefónica

Los controles de acceso deben cumplir los lineamientos de la sección II, Apartado II.7.2.1, y además los listados a continuación:

- El Servidor Telefónico Central debe estar colocado en el cuarto de telecomunicaciones o cuarto de equipo y de acceso restringido.
- Las personas que tengan acceso lógico y/o físico a la Central Telefónica deben ser autorizadas por el Director del sistema 9-1-1.
- El acceso a la Central Telefónica debe realizarse por medio de usuario y contraseña. Cada administrador de la Central Telefónica debe tener un nombre de usuario que lo identifique. Las contraseñas se deben actualizar de acuerdo a las políticas de seguridad del CS.
- A los usuarios que hagan uso de la Central Telefónica se les debe definir su nivel de acceso a través de perfiles. El perfil mínimo debe definir dos niveles de acceso, sin restringir que la Central Telefónica pueda definir más. Los dos niveles de acceso en un perfil pueden ser:
  - Administrador General: tiene derecho a todas las opciones de la Central Telefónica.
  - Acceso: sólo puede consultar el estado o servicios que ofrece la Central Telefónica.

Nota: conjuntamente con estas características, se debe restringir las terminales que pueden acceder a la Central Telefónica, implementando un mecanismo de autentificación con un dispositivo de seguridad por separado.

5.5.5.2.4 Alimentación Redundante a la Central Telefónica

Para alimentar la Central Telefónica se puede utilizar uno de los dos siguientes métodos:

- Fuentes de corriente redundantes residentes en la Central Telefónica
- Alimentación externa a través de un banco de baterías. El banco de baterías debe cumplir con los siguientes requerimientos:
  - La Central Telefónica debe contar con una red de baterías exclusiva para su respaldo;
  - La red de baterías de la Central Telefónica debe dar respaldo mínimamente de 30 minutos;
  - La planta de emergencia del CS debe ser capaz de respaldar o de alimentar al banco de baterías por 4 días o más.

5.5.5.2.5 Comunicación con otros CALLE

- La Central Telefónica debe brindar la facilidad del ruteo de llamadas.
- Para posibilitar el ruteo de una llamada hacia otro sistema Nueve-Uno-Uno (9-1-1) de un CS de una entidad federativa, así como la intervención en la línea en los procesos de supervisión y calidad, los conmutadores de voz deben estar interconectados.
- El ruteo de llamada selectivo hacia otro sistema Nueve-Uno-Uno (9-1-1) debe ser posible cuando un sistema Nueve-Uno-Uno (9-1-1) no tenga la disponibilidad de recibir llamadas, por cualquier motivo que sea (saturación, daños en la línea, mantenimiento, etc.). Este servicio debe ser proporcionado por el prestador de servicios y debe hacerse de forma inmediata.

5.5.5.2.6 Comunicación con el Sistema de Video Vigilancia (SVV)

La comunicación del Sistema Nueve-Uno-Uno (9-1-1) con el sistema SVV debe ser a través del aplicativo CAD, toda vez que éste alberga la información de cada una de las llamadas de emergencia recibidas, y es a través del ANI *"Número de Identificación de Evento"* (folio), que cada sistema interconectado con el sistema 9-1-1 da seguimiento a cada uno de ellos.

5.5.5.3 Equipo y Funcionalidades de los Equipos de los Operadores

5.5.5.3.1 Equipo de cómputo

5.5.5.3.1.1 Características de las computadoras personales

Cada operador debe contar con una Computadora Personal (PC) de escritorio que:

a) Tenga un procesador de última generación para computadoras personales de escritorio, con suficiente velocidad de procesamiento para ejecutar adecuadamente todas las aplicaciones y/o programas que se requieran.
b) Tenga la capacidad necesaria de almacenamiento para la instalación de aplicativos e información para su labor.
c) Cuente con suficiente memoria RAM para ejecutar adecuadamente todas las aplicaciones y/o programas que se requieran.
d) Cuente con los siguientes puertos: USB, puertos para audífono, micrófono, y entrada y salida de línea; conexión para red y puerto de salida a video.
e) Cuente con una tarjeta de video que permita una visualización adecuada de la aplicación del Sistema de Información Geográfica (GIS), así como una adecuada visualización en la captura de datos de cada una de las emergencias recibidas (CAD).

f) Debe contar con dos salidas de video o más, dependiendo de los requerimientos del CS.

5.5.5.3.1.2 Características de los monitores

Cada operador debe tener al menos dos monitores para la captura y visualización de la información.

a) Un monitor dedicado para la captura de datos requeridos en la atención de una llamada de emergencia en el CAD.
b) Un monitor para la visualización del GIS, ubicando el origen de la llamada de emergencia.
c) La resolución de los monitores debe permitir una visualización adecuada de la aplicación del Sistema de Información Geográfica (GIS), así como una adecuada visualización en la captura de datos de cada una de las emergencias recibidas (CAD).
d) El monitor debe facilitar la apertura de diferentes ventanas en pantalla.
e) El monitor debe contar con ajuste para su orientación e inclinación.
f) La imagen en la pantalla debe ser estable, sin destellos y reflejos.
g) El monitor debe tener la posibilidad de ajustar los niveles de intensidad luminosa, brillo y contraste para adaptar la pantalla a las condiciones del entorno.
h) Las pantallas deben tener una relación de aspecto de 16:9.

5.5.5.3.1.3 Características de los periféricos

a) Cada operador debe tener un ratón ergonómico:
   - para ser utilizado cómodamente tanto por personas diestras como zurdas.
   - alámbrico o inalámbrico.

b) Cada operador debe tener un teclado ergonómico:
   - alámbrico o inalámbrico.
   - con una superficie mate para evitar reflejos.
   - con teclas suficientemente legibles desde la posición normal de trabajo.

5.5.5.3.2 Equipo telefónico

Se puede usar indistintamente un teléfono físico con tecnología VoIP o una aplicación *softphone* para la computadora, que deben cumplir con las siguientes características:

a) transferencia de llamadas
b) conferencia
c) llamada en espera

d) registro de llamada
e) deben contar con teclas administrativas como:
   - llamada en espera
   - silencio
   - conferencia
   - transferencia
   - altavoz
   - subir/bajar volumen
   - menú
   - registro de llamadas
   - auriculares
f) Para teléfonos físicos:
   - debe contar con pantalla telefónica
   - debe tener puerto para *FastEthernet* o *GigaEthernet* para conectarse a la red LAN y puerto *FastEthernet* o *GigaEthernet* para conectarse a la PC
   - debe ser alimentado por *Ethernet* (PoE)
   - debe tener puerto y/o enchufe para auriculares
g) El operador debe contar con una diadema para lograr la comunicación con las personas que hacen las llamadas de emergencia con las siguientes características:
   - la diadema debe ser capaz de integrarse funcionalmente a un teléfono de escritorio (estándar)
   - debe tener micrófono, auricular y horquilla de alta calidad
   - debe tener micrófono anti ruido
   - debe tener cancelación de ruido

El proveedor debe entregar en el momento de la instalación y puesta en marcha de cada uno de los equipos:

- Manual Técnico
- Manual de Instalación
- Manual de Mantenimiento
- Manual de Operación
- Protocolos de prueba
- Pruebas de Aceptación
- Memoria Técnica

5.5.5.3.3 Controles de Acceso al Equipo del Operador

Debe cumplir los lineamientos de seguridad de la sección 5.2, Apartado 5.2.6.3.1.

Nota: Conjuntamente con estas características, se debe restringir las terminales que pueden acceder al equipo de cómputo.

5.5.5.4 Sistema de Información Geográfica (*Geographic Information System*, GIS)

5.5.5.4.1 Especificaciones Técnicas y Funcionalidades del GIS

Los requerimientos necesarios que debe cumplir el aplicativo GIS para su implementación en el sistema 9-1-1 son las siguientes:

- Podrá ser una aplicación comercial "libre" o una aplicación propietaria, pero debe contar con el licenciamiento correspondiente, así como su actualización constante. Asimismo, el CALLE debe contar con todas las licencias correspondientes para tener acceso total a las funcionalidades y actualizaciones del GIS.
- Debe ser capaz de integrarse a cualquier sistema operativo.
- Sin importar que sea un software propietario, éste debe permitir el desarrollo de aplicaciones que requiera el CALLE.
- Debe estar alojado en los equipos de los operadores del 9-1-1 y debe vincularse o integrarse al sistema del SVV y al área de despacho.
- Debe contar con un Sistema de Posicionamiento Global (GPS, por sus siglas en inglés).
- El GIS podrá ser de plataforma vectorial y/o por *web mapping* en tiempo real. Para el caso de *web mapping* los CALLE deben considerar el uso de una licencia completa y un enlace de Internet dedicado para este propósito a fin de garantizar la operación eficiente del GIS.
- Debe contener al menos las siguientes capas de información geográfica:
  - Entidad
  - Municipio
  - Colonia
  - Calle
- La integración del GIS con el CAD debe proporcionar a los operadores las siguientes funcionalidades para su implementación al 9-1-1:
  - Toma de decisiones de mando y control
  - Informe de densidad de delitos
  - Visualización de los límites territoriales para delimitar la responsabilidad jurisdiccional de los cuerpos de emergencia
  - Localización, identificación y mapeo del incidente con la menor incertidumbre posible
  - Utilización de geo datos en la coordinación del 9-1-1 y del SVV
  - Presentación en capas de mapas estratégicos
- Debe proporcionar información de cierre de calles, avenidas y carreteras en tiempo real para agilizar la atención de los cuerpos de emergencia.

- Debe poder determinar la ruta más corta o más rápida al incidente registrado, así como a las instalaciones de emergencia correspondientes.
- Los datos geoespaciales suministrados deben ser compatibles con los formatos estándar.

5.5.5.5 Tecnologías Emergentes

Debido a que las tecnologías emergentes son parte de la vida diaria de los ciudadanos, cada vez es más común integrarlas en la seguridad de los mismos, por lo que es necesaria la inclusión de estas tecnologías para la atención de todo tipo de emergencias en el CS.

5.5.5.5.1 Botones de Emergencia

Los botones de emergencia deben estar vinculados con el Centro de Atención de Llamadas de Emergencia (CALLE) y con el Sistema de Video Vigilancia (SVV), para permitir el reconocimiento de la zona en donde se genere la emergencia; esto debe apegarse a lo establecido en la Norma Técnica para estandarizar las características técnicas y de interoperabilidad de los Sistemas de Video Vigilancia para la Seguridad Pública.

Los botones de emergencia deben estar conectados al CS por cualquiera de los medios empleados para la transferencia de información (alámbrico e inalámbrico), considerando su ubicación respecto de la distribución de cámaras que se haga en la entidad federativa.

Cuando un ciudadano active un botón de emergencia, en el CAD del área de los operadores del sistema 9-1-1 se indicará dicho evento. El operador encargado de atenderla debe establecer comunicación con el ciudadano y la información recibida debe de almacenarse de forma automática en un sistema manejador de base de datos generándose el "Número de Identificación Automática" (*Automatic Number Identification*, ANI)", de tal forma que pueda distinguirse cada evento y se le pueda dar seguimiento. Asimismo, este identificador debe ser único y es mediante el cual cada uno de los sistemas ligados al 9-1-1 del CS pueden identificarlo.

5.5.5.5.2 Alarma de Pánico

Las alarmas de pánico deben estar vinculadas con el Centro de Atención de Llamadas de Emergencia (CALLE) y/o con el Sistema de Video Vigilancia y/o con el Área de Despacho del CS.

Los requerimientos necesarios que debe cumplir las alarmas son los siguientes:

- deben estar conectados al CS, a través de un medio alámbrico o inalámbrico.
- al igual que los botones de emergencia, cuando se active una alarma de pánico, el área responsable de atender el evento debe almacenar la información en un sistema manejador de base de datos generándose el "Número de Identificación Automática "(*Automatic Number Identification*, ANI)", de tal forma que pueda distinguirse cada evento y se le pueda dar seguimiento.

5.5.5.5.3 Sistema 9-1-1 Móvil

Los elementos policiacos podrán usar diferentes dispositivos de comunicación, tales como: teléfonos inteligentes o tabletas, para que sean notificados de las diferentes emergencias que deben atender.

Esta aplicación es independiente y diferente de la APP Nacional 9-1-1.

5.5.5.6 Pruebas de Desempeño del Centro de Atención de Llamadas de Emergencia

Deben realizarse pruebas de desempeño del CALLE en la atención de las emergencias reportadas por cualquiera de los medios indicados en esta norma:

a) Registro por la APP
b) Registro por llamada Telefónica
c) Registro por Botón de Emergencia
d) Estación de atención de Emergencia
e) Registro por Alerta de Pánico

En cualquiera de los casos anteriores se debe:

1. Verificar que se realiza el registro de la llamada.
2. Visualizar la geo localización de la emergencia.

3. Llenar la información de quien reporta la emergencia y tipo de emergencia en el CAD.
4. Verificar el registro de ANI.
5. Verificar la asignación de "*Número de Identificación de Evento*" (folio).

Asimismo, deben realizarse pruebas en la atención de llamadas para determinar el desempeño del sistema, tales como:

a) Prueba de llamadas simultáneas

Tomando en cuenta la cantidad de operadores del sistema 9-1-1 con que cuente el CS, se debe:

1. Realizar llamadas al CS, de tal forma que se supere a la cantidad de operadores del sistema 9-1-1 (doble de llamadas con respecto a la cantidad de los operadores)
2. Observar la asignación de turnos en el CAD ante esta situación
3. Registrar el tiempo de atención a cada una de las llamadas

b) Prueba en la recepción de llamadas de broma/falsas

1. Se deben realizar llamadas de broma y/o falsas hacia el sistema 9-1-1
2. Se debe verificar que el CAD registre la llamada, así como que el número de donde se está llamando se registre en la Central Telefónica
3. El protocolo que seguirá cada operador del sistema 9-1-1 para la atención de este tipo de llamadas, dependerá del proceso establecido en el CS
4. Se debe volver a marcar del mismo número para verificar si la Central Telefónica lo bloquea

c) Pruebas de falla en la prestación del servicio de Telefonía

Se debe simular falla en la prestación del servicio de las llamadas telefónicas (PSTN), para comprobar la funcionalidad de ruteo de llamadas.

5.6 Circuito Cerrado de Televisión

5.6.1 Objetivo

Definir arquitectura, protocolos y características que debe tener un sistema de circuito cerrado de televisión y la Red LAN que lo soporta para el Complejo de Seguridad.

5.6.2 Alcance

Este apartado indica las características técnicas que deben tener los elementos del circuito cerrado de televisión, se menciona si son opcionales, obligatorias o si son condicionadas a ciertos requerimientos. No se debe considerar como una guía de diseño.

5.6.3 Campo de aplicación

Complejos de seguridad.

5.6.4 Elementos que componen un sistema de circuito cerrado de televisión para el Complejo de Seguridad

5.6.4.1 Arquitectura de un circuito cerrado de televisión

5.6.4.1.1 Arquitectura basada en NVR y basada en Servidor

Para los sistemas de Circuito Cerrado de Televisión (CCTV) se permitirán dos tipos de arquitecturas, clasificadas por la forma en que está montado el sistema de gestión de las cámaras:

a) Arquitectura basada en **NVR** (Grabador de Video en Red). Como muestra la figura VI.1, el sistema de gestión de las cámaras servidor está montado en un equipo dedicado, conectado a la red de datos, que a su vez ofrece comunicación con las cámaras IP de video digital. Un equipo dedicado ya está preparado para ofrecer servicio a cierta cantidad de clientes que se conecten a él, en el caso del NVR, los clientes serán cámaras y usuarios que visualizarán el video de las diferentes cámaras.

b) Arquitectura basada en servidor. En la figura VI.2se muestra que el sistema de gestión de cámaras servidor está montado en un equipo de cómputo llamado **Servidor**. El Servidor debe ser dimensionado para ser eficiente en el manejo de cámaras, almacenamiento de video, y para atender las

peticiones de usuarios que visualizan el video, de tal forma que se debe definir:

i. Tipo de microprocesador a usar
ii. Número de núcleos dedicados al software de gestión de video
iii. Cantidad de memoria RAM y velocidad de su bus
iv. Características de la tarjeta de red o de las tarjetas de red
v. Características de discos duros

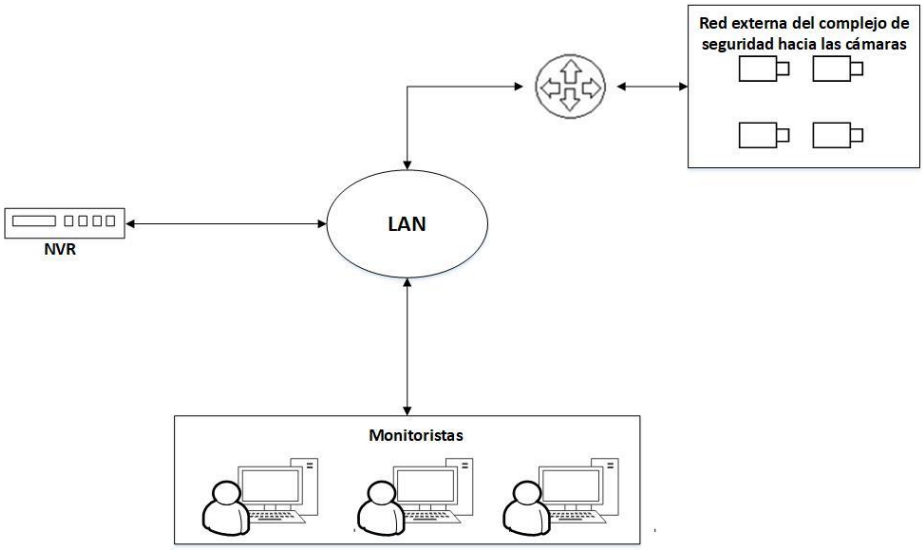


Figura VI. 1 Arquitectura de CCTV basado en NVR

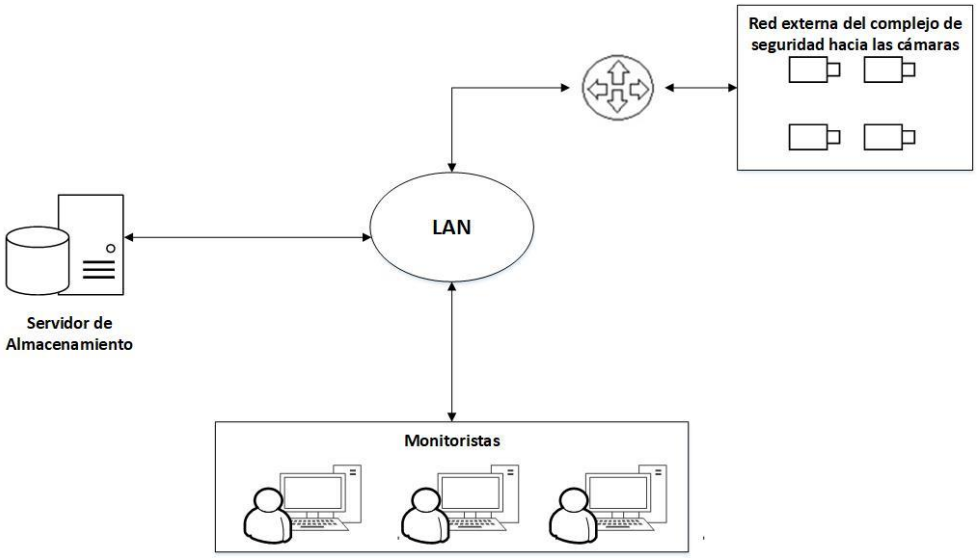


Figura VI. 2 Arquitectura de CCTV basado en Servidor

Nota: las dos arquitecturas pueden satisfacer las necesidades del sistema de CCTV. Inclinarse por cualquiera de las dos opciones dependerá de factores no técnicos.

5.6.4.1.2 Arquitectura basada en sistemas de almacenamiento

Para los nuevos sistemas de CCTV se permiten dos tipos de arquitecturas de almacenamiento:

a) Arquitectura basada en discos **RAID** tipo 1
b) Arquitectura basada en almacenamiento NAS

Nota: cualquier sistema de almacenamiento puede satisfacer las necesidades del sistema de video vigilancia. Inclinarse por cualquiera de ellas dependerá de los requerimientos del sistema CCTV.

5.6.4.1.3 Sistema de almacenamiento contra fallos

Los sistemas de almacenamiento deben proveer un sistema contra fallos, para ello se puede implementar cualquiera de las especificaciones de los apartados 5.9.5.1 y 5.9.5.2.

5.6.5 El sistema de gestión de cámaras cliente y servidor

5.6.5.1 Del número de cámaras soportadas

Debe cumplir con lo indicado en la sección 5.4.5.1

5.6.5.2 Protocolos de comunicación para la transferencia de video en el sistema de gestión de cámaras servidor

Deben cumplir con lo indicado en la sección 5.4.5.2 y sus incisos.

5.6.5.3 De los protocolos para administrar el NVR o el sistema de gestión de cámaras servidor

Deben cumplir con lo indicado en la sección 5.4.5.3 y sus incisos.

5.6.5.4 Protocolos de comunicación entre el sistema de gestión de cámaras cliente y servidor

Deben cumplir con lo indicado en la sección 5.4.5.4 y sus incisos.

5.6.5.5 Manejo de características de administración de video para su visualización en el sistema de gestión de cámaras cliente

Debe cumplir con lo indicado en la sección 5.4.5.5 y sus incisos.

5.6.5.6 Características para administración de las cámaras desde el sistema de gestión de cámaras cliente

Deben cumplir con los incisos de la sección 5.4.5.6.

5.6.5.7 Características de acceso al sistema de gestión de cámaras cliente y servidor

Deben cumplir con lo indicado en la sección 5.4.5.7 y sus incisos.

5.6.6 Equipo de cómputo de los monitoristas

5.6.6.1 Características de las computadoras personales

Deben cumplir con lo indicado en la sección 5.4.6.1 y sus incisos.

5.6.6.2 Características de los monitores

Deben cumplir con lo indicado en la sección 5.4.6.2 y sus incisos.

5.6.6.3 Características de los periféricos

Deben cumplir con lo indicado en la sección 5.4.6.3 y sus incisos.

5.6.6.4 Equipo Telefónico

Debe cumplir con lo indicado en la sección 5.4.6.4.

5.6.6.5 Del *joystick* o palanca de control para cámaras PTZ

Debe cumplir con lo indicado en la sección 5.4.6.5 y sus incisos.

5.6.7 *Videowall*

5.6.7.1 Controlador del *videowall*

El *videowall* para el CCTV es opcional, depende de los requerimientos del Complejo de Seguridad. En caso de requerir el *videowall* entonces debe cumplir con lo indicado en la sección 5.4.7.1 y sus incisos.

5.6.7.2 Pantallas en el *videowall*

Si el proyecto de CCTV contempla *videowall*, entonces las pantallas deben cumplir con lo indicado en la sección 5.4.7.2 en todos sus incisos.

5.6.8 Características de la Red LAN para soportar el CCTV

Deben cumplir con lo indicado en la sección 5.4.8 en todos sus incisos.

5.6.9 Dimensionamiento de servidores y almacenamiento

5.6.9.1 Dimensionamiento del servidor de video

Debe cumplir con lo indicado en la sección 5.4.9.1 en todos sus incisos.

5.6.9.2 Dimensionamiento de cantidad de almacenamiento para video

5.6.9.2.1 Requerimientos del sistema de almacenamiento

Deben cumplir con lo indicado en la sección 5.4.9.2.1 en todos sus incisos.

5.6.9.2.2 Parámetros a considerar en el análisis del dimensionamiento del sistema de almacenamiento para CCTV

Deben cumplir con lo indicado en la sección 5.4.9.2.2 y sus incisos.

5.6.10 Monitoreo y seguridad de los componentes del sistema de video vigilancia

5.6.10.1 Protocolos de monitoreo

Deben cumplir con lo indicado en la sección 5.4.10.1 y sus incisos.

5.6.10.2 Aplicativos de monitoreo con SNMP

Deben cumplir con lo indicado en la sección 5.4.10.2 y sus incisos.

5.6.10.3 Variables a monitorear

Deben cumplir con lo indicado en la sección 5.4.10.3 y sus incisos.

5.6.10.4 Políticas de monitoreo del NVR o servidor de la aplicación de gestión de video vigilancia

Deben cumplir con lo indicado en la sección 5.4.10.4 en todos sus incisos.

5.6.10.5 Políticas de seguridad del NVR o servidor donde está montada la aplicación de gestión de cámaras servidor

Deben cumplir con lo indicado en la sección 5.4.10.5 en todos sus incisos.

5.6.11 Cámaras del circuito cerrado de televisión

5.6.11.1 Características de las cámaras relacionadas a la calidad de la imagen

Las cámaras en un CCTV deben ser escogidas con el fin de poder identificar a una persona y de optimizar la transmisión de video; para ello deben tener las siguientes características, sin restringir que se adicionen más de acuerdo a los requerimientos del sistema.

a) Cámara de tecnología digital IP.
b) Resolución: la resolución de las cámaras debe ser HD o más alta, de tal forma que identifique a una persona a la distancia definida en el diseño del CCTV. Para cumplir este requisito se debe considerar la imagen de un rostro con una cantidad de 70 pixeles o más contados en sentido horizontal a la distancia máxima de cobertura la cámara.
c) Manejo de video a color.
d) Las cámaras deben contar con tecnología día y noche-día y noche.
e) Calidad de la imagen media a alta, dependiendo de si es suficiente para tener detalles del rostro que permitan identificar a una persona.
f) Debe poderse ajustar el número de tramas por segundo (FPS).
g) El *zoom* de las cámaras debe poder ver el rostro de la persona.
h) La compresión permitida es H.264 o H.265.
i) La cámara empleada debe permitir realizar ajuste de imagen en color, brillo, nitidez, balance de blancos, control de exposición y compensación de contraluz (auto-iris).

5.6.11.2 Protocolos de comunicación soportados para la trasmisión de video

Se enlistan los formatos de compresión y protocolos de comunicación permitidos para la transmisión de video. No es necesario que la cámara los soporte todos. Los protocolos pueden trabajar de forma individual o conjunta.

a) H.264
b) H.265
c) RTP
d) RTPS
e) HTTPS

f) IGMP
g) FTP
h) SFTP
i) CIFS/SMB

5.6.11.3 Protocolos para la administración soportados por la cámara

Para acceder a la cámara con el fin de poderla administrar, se podrá usar cualquiera de los protocolos a continuación listados, que se consideran como seguros. Se usará un usuario y contraseña para acceder a la cámara. Si hay un protocolo inseguro en la cámara que dé acceso a ésta, se debe deshabilitar.

a) HTTPS
b) SSH
c) Aplicación propietaria del fabricante: en este caso debe proveer una comunicación segura tal que autentifique al usuario y encripte la comunicación

5.6.11.4 Características de administración de red de las cámaras

La cámara debe soportar las siguientes características de administración:

a) Soportar protocolo IPv4 e IP v6 como opcional.
b) Debe poder habilitar, deshabilitar y configurar SNMP v2c y v3. Si tiene SNMP v1 deshabilitarlo.
c) Debe poder dar una dirección IP, máscara y puerta de enlace a la cámara.
d) Debe poder actualizar el *firmware* de la cámara a través del protocolo FTP, TFTP o HTTPS: los protocolos mencionados para la actualización de *firmware* son los únicos admitidos.
e) Protocolo NTP para actualizar tiempo.
f) Como opcional la cámara soportará QoS, dependiendo de los requerimientos de diseño del CCTV.
g) La cámara soportará asignación de direcciones por el protocolo DHCP.

5.6.11.5 Características físicas de las cámaras

a) En caso de ser una cámara PTZ tipo domo, debe permitir el movimiento horizontal de 360° y vertical de al menos 0° a 90°.

b) En caso de que la cámara se instale en el exterior, debe:

i. Contar con protección contra el vandalismo, misma que deberá ser acorde al sitio de su ubicación y al riesgo principal existente, considerando al menos nivel

IK08 para aquellas que no están al alcance normal de la gente, o superior en los casos donde se justifique. Deberá ofrecer grado de protección contra ingreso de líquidos y partículas, de acuerdo con lo definido en IP66 y deberá ofrecer resistencia a la corrosión, de acuerdo con el estándar NEMA 4X.

ii. Contar con el herraje apropiado para su montaje.

iii. El intervalo de temperatura que deberá soportar la cámara para operar adecuadamente en la región donde vaya a ser instalada, debe encontrarse dentro de las temperaturas máximas y mínimas históricas registradas del sitio por el Servicio Meteorológico Nacional en la ubicación correspondiente.

c) El puerto debe ser 100BASE-TX o 1000BASE-T o 1000BASE-TX con conector RJ45.

d) La alimentación debe ser compatible con cualquier clasificación PoE.

5.7 Sistema de Atención de Llamadas de Denuncia Anónima 089

5.7.1 Objetivo

Establecer y/o actualizar los requerimientos técnicos necesarios de los Centros de Atención de Llamadas de Denuncia Anónima 089 de un Complejo de Seguridad (CS).

5.7.2 Alcance.

Este capítulo indica las características técnicas que deben tener los elementos del Centro de Atención de Llamadas de Denuncia Anónima 089. No se debe considerar como una guía de diseño.

5.7.3 Campo de Aplicación

El campo de aplicación de la presente Norma Técnica establece los requerimientos técnicos necesarios de los Centros de Atención de Llamadas de Denuncia Anónima 089.

5.7.4 Descripción

El presente apartado tiene como finalidad indicar los aspectos tecnológicos indispensables para el Centro de Atención de Llamadas de Denuncia Anónima 089 de un Complejo de Seguridad (CS).

Este centro debe ser independiente al servicio del Centro de Atención de Llamadas de Emergencia a través del número único armonizado 9-1-1 (Nueve-Uno-Uno) y no deben compartir áreas físicas comunes con ninguna otra área del CS.

Los aspectos técnicos que se considerarán en este apartado son:

a) Aplicativo "Despacho Asistido por Computadora" (*Computer Aided Dispatch*, CAD)
b) Central Telefónica (Conmutador – *Gateway* y tarjetas de expansión)
c) Equipo y funcionalidades de los Equipos de los Operadores
d) Grabación de audio

En la figura VII.1 se presenta un diagrama general a bloques de los elementos que integran al Centro de Atención de Llamadas de Denuncia Anónima 089: área de operadores (equipo de los operadores y aplicativo), Central Telefónica y su conexión a la red de área local (LAN) del CS. Las denuncias anónimas se reciben vía llamada telefónica y deben almacenarse todas y cada una de ellas en la Central Telefónica.

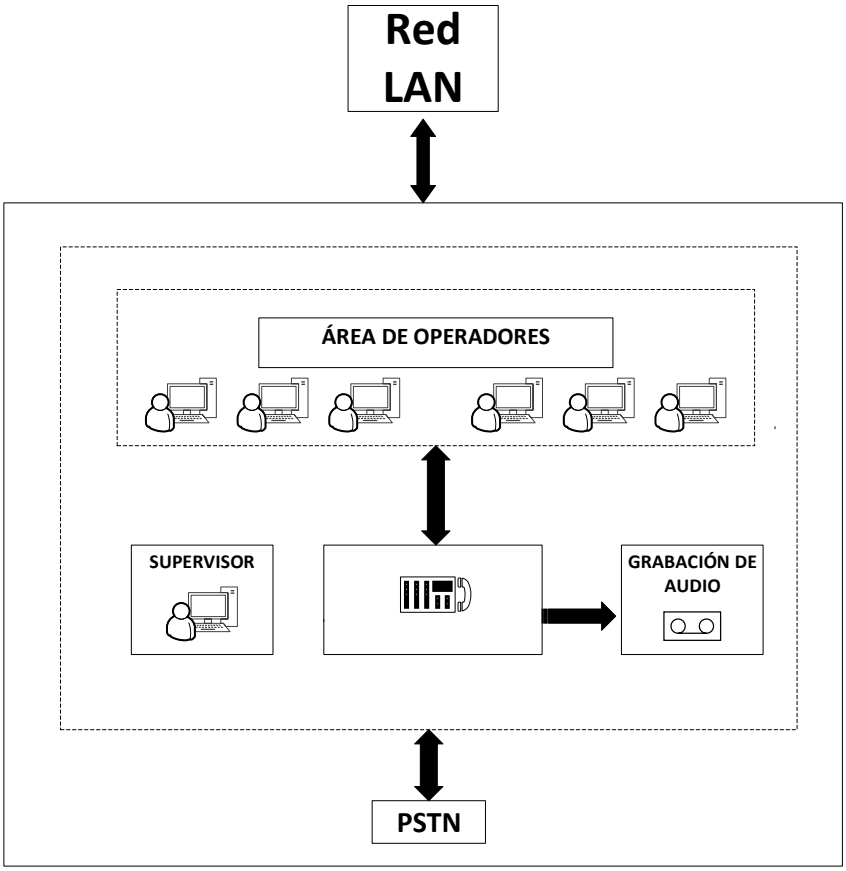


Figura VII. 1 Diagrama General a Bloques de los elementos que integran el Sistema de Atención de Llamadas de Denuncia Anónima 089

Esta norma no incluye el diseño de sistemas de tierra, aire acondicionado, respaldo de energía, y en general el acondicionamiento del área del Complejo de atención de llamadas de denuncia anónima.

5.7.5 Norma para el Servicio del Complejo de Atención de Denuncia Anónima 089

5.7.5.1 Despacho Asistido por Computadora (CAD)

Los requerimientos necesarios que debe cumplir el CAD para su implementación en el Sistema de Llamadas de Denuncia Anónima 089 son las que se exponen a continuación.

5.7.5.1.1 Especificaciones Técnicas y Funcionalidades del CAD

- Debe ser capaz de integrarse a cualquier sistema operativo.
- Sin importar si se trata de un *software* comercial o propietario, éste debe ser abierto para los desarrolladores con que se cuente en el CS.
- Debe estar alojado en los equipos de los operadores del 089 y ser capaz de integrarse a una red local.
- Debe tener un servidor asociado en el cual se almacenen al menos los siguientes registros de las llamadas al 089:

  - Llamadas entrantes
  - Enmascaramiento del número de origen de la llamada
  - Llamadas pérdidas
  - Llamadas en cola
  - Duración de llamada
  - Tiempo de llamada en cola

- Debe poder abrir registros y obtener sus actualizaciones en tiempo real.
- Debe poder consultar el historial de todos los registros de llamadas.
- Debe poder integrar voz y datos para una comunicación óptima.
- Debe poder establecer una comunicación a nivel de red con la Central Telefónica.
- Las llamadas entrantes del 089 y registradas en el CAD se deben grabar en la Central Telefónica. El tiempo de registro de las llamadas debe ser de al menos 1 año. Dicho respaldo debe realizarse automáticamente, así como el borrado de la información.
- La información recibida de cada llamada de denuncia anónima debe almacenarse de forma automática en un sistema manejador de base de datos, generándose el *"Número de Identificación de Evento"* (folio), de tal forma que pueda distinguirse cada evento y se le pueda dar seguimiento. Asimismo, este identificador debe ser único.
- Los registros del CAD se deben almacenar en su servidor en formatos estándar.
- Se debe poder realizar una relación entre los registros del CAD y su correspondiente archivo de audio almacenado en la Central Telefónica.
- Debe poder registrar las incidencias atendidas por cada operador y se deben almacenar en su servidor correspondiente.
- Se debe dimensionar la Central Telefónica de acuerdo al análisis del volumen de llamadas recibidas por el CS definido en la NOM Norma Oficial Mexicana

NOM-227-SCFI-2017, Estandarización de los Servicios de Llamadas de Emergencia a través del Número Único Armonizado 9-1-1 (Nueve, Uno, Uno).

- Se debe dimensionar el sistema de almacenamiento de llamadas de acuerdo al análisis del volumen de llamadas recibidas por el CS. Se debe considerar los siguientes factores:
  - Número de llamadas al día
  - Número promedio de duración de llamadas
  - Tipo de codificador
  - Tiempo de almacenamiento de llamadas
  - Factor del 30% de espacio libre
  - Número de troncales asignadas.

5.7.5.1.2 Controles de Acceso del CAD

- El acceso al aplicativo CAD debe realizarse por medio de usuario y contraseña. Cada operador debe tener un nombre de usuario que lo identifique. Las contraseñas se deben actualizar de acuerdo a las políticas de seguridad del CS.

- A los usuarios que hagan uso del aplicativo CAD se les debe definir su nivel de acceso a través de perfiles. El perfil mínimo debe definir tres niveles de acceso, sin restringir que el aplicativo CAD pueda definir más. Los tres niveles de acceso en un perfil pueden ser:

  - Administrador General: tiene derecho a todas las opciones del aplicativo CAD.
  - Operador: puede tener acceso a todas las opciones del aplicativo CAD pero tiene restringido crear, modificar o borrar usuarios de mayor nivel que él como restricción básica, pudiendo restringírsele más opciones.
  - Acceso: sólo puede consultar el estado o servicios que ofrece el aplicativo CAD.

Nota: conjuntamente con estas características, se debe restringir las terminales que pueden acceder al aplicativo CAD implementando un mecanismo de autentificación a través del mismo aplicativo CAD o con un dispositivo de seguridad aparte.

5.7.5.2 Central Telefónica

La Central Telefónica estará integrada por: conmutador y no debe ser independiente a la Central Telefónica del sistema 9-1-1.

Los requerimientos necesarios que debe cumplir la Central Telefónica para su implementación en el sistema 089 son los que se presentan a continuación.

5.7.5.2.1 Especificaciones Técnicas de la Central Telefónica

- Debe tener la capacidad de integrarse con los sistemas del Complejo de Seguridad que corresponda, mediante el uso de protocolos y/o estándares abiertos. De igual forma debe poder integrar cualquier aplicación necesaria para el correcto funcionamiento del Sistema de Atención de Denuncia Anónima a través de protocolos y/o estándares abiertos.
- Se debe contar con:
  - conmutador tipo PBX IP para los servicios de Telefonía
  - dispositivo *Gateway* de interconexión
  - el conmutador y el *Gateway* pueden o no estar integrados en un mismo dispositivo
- Debe contar con al menos TIER III.
- Debe poder conectarse a la Red Telefónica Pública Conmutada (PSTN, por sus siglas en inglés) a través de troncales digitales E1 o líneas telefónicas digitales de acuerdo a las necesidades del análisis de dimensionamiento de llamadas del CS.
- Las intercomunicaciones deben basarse en el protocolo de comunicación IP.
- Debe poder integrarse a la red de Sistema Global para las Comunicaciones Móviles (GSM, por sus siglas en inglés) para el Servicio de Mensajes Cortos (SMS, por sus siglas en inglés).
- Debe tener puertos de Red de Área Local (LAN).
- Debe tener puertos de red para interconectarse a la Red de Área Amplia (WAN, por sus siglas en inglés) para intercomunicarse con otras centrales telefónicas.
- Debe tener puertos analógicos para teléfonos analógicos, en caso de que se requieran.
- De acuerdo al análisis de dimensionamiento de llamadas, la central debe soportar el máximo número de llamadas en las horas pico más un 20%.
- Debe ser escalable a futuras necesidades del sistema 089. La Central Telefónica debe estar preparada para crecer por adición de nuevos módulos de conexión a la PSTN, integrarse con otra Central Telefónica de extensión y agregar más extensiones.
- La Central Telefónica debe estar bajo un esquema de alta disponibilidad con un conmutador redundante en el mismo CS.
- Debe soportar los siguientes codificadores: G.711, G.723v1 y/o G.729.
- Debe soportar el protocolo H.323, SIP y/o IAX2, dependiendo de los requerimientos del CS.

- Debe tener la capacidad de grabar todas las conversaciones telefónicas recibidas a su disco local, en red SAN o NAS, dependiendo de los requerimientos del almacenamiento del CS.
- Debe soportar la adición de más extensiones telefónicas sin necesidad de adquirir licencias extras.
- Debe tener contratado un servicio de mantenimiento con el proveedor o fabricante.
  - Servicio de soporte técnico vía telefónica de 24x7 todo el año
  - Servicio de soporte técnico en sitio
  - Servicio de cambio de partes dañadas
  - Acceso a nuevos *firmwares* para la Central Telefónica
  - Actualización de *firmware*

- El proveedor, en el momento de la entrega, instalación y puesta en marcha de la Central Telefónica, debe entregar:

  - Manual Técnico
  - Manual de Instalación
  - Manual de Mantenimiento
  - Manual de Operación
  - Protocolos de prueba
  - Pruebas de Aceptación
  - Memoria Técnica

5.7.5.2.2 Funcionalidades de la Central Telefónica

- Debe integrarse y/o incluir un tarificador de llamadas que registre al menos lo siguiente:
  - número de llamadas entrantes
  - duración de llamadas
  - número de llamadas perdidas
  - tiempo de cola de llamadas
  - número de llamadas en cola

- Debe poder generar estadísticas del traficador de llamadas.
- Debe contar con la aplicación de Distribución Automática de Llamadas (ACD, por sus siglas en inglés).
- Debe contar con la aplicación de Respuesta de Voz Interactiva (IVR, por sus siglas en inglés), dependiendo de los requerimientos del CS.
- Debe contar con un módulo para controlar las llamadas de broma.
- Debe contar con las siguientes funcionalidades, sin restringir otras que dependen de requerimientos específicos del 089:

- desvío de llamadas
- transferencia de llamada
- llamada en espera
- remarcación de último número para llamadas internas y externas
- anuncio de llamada
- grabación de voz automática o manual, dependiendo de los requerimientos del 089
- discado abreviado
- marcación automática para llamadas perdidas

5.7.5.2.3 Controles de Acceso a la Central Telefónica

Los controles de acceso deben cumplir los lineamientos de la sección II, Apartado II.7.2.1, y además los listados a continuación:

- El Servidor Telefónico Central debe estar colocado en el cuarto de telecomunicaciones o cuarto de equipo y ser de acceso restringido.
- Las personas que tengan acceso lógico y/o físico a la Central Telefónica deben ser autorizadas por el Director del 089 y/o Director del Centro de Atención de Llamadas de Emergencia.
- El acceso a la Central Telefónica debe realizarse por medio de usuario y contraseña. Cada administrador de la Central Telefónica debe tener un nombre de usuario que lo identifique. Las contraseñas se deben actualizar de acuerdo a las políticas de seguridad del CS.
- A los usuarios que hagan uso de la Central Telefónica se les debe definir su nivel de acceso a través de perfiles. El perfil mínimo debe definir dos niveles de acceso, sin restringir que la Central Telefónica pueda definir más. Los dos niveles de acceso en un perfil pueden ser:

  - Administrador General: tiene derecho a todas las opciones de la Central Telefónica.
  - Acceso: sólo puede consultar el estado o servicios que ofrece la Central Telefónica.

Nota: conjuntamente con estas características, se debe restringir las terminales que pueden acceder a la Central Telefónica, implementando un mecanismo de autentificación con un dispositivo de seguridad aparte.

5.7.5.2.4 Alimentación Redundante a la Central Telefónica

Para alimentar la central telefónica se puede utilizar uno de los dos siguientes métodos:

- Fuentes de corriente redundantes residentes en la Central Telefónica
- Alimentación externa a través de un banco de baterías. El banco de baterías debe cumplir con los siguientes requerimientos:
  - La Central Telefónica debe contar con una red de baterías exclusiva para su respaldo.
  - La red de baterías de la Central Telefónica debe dar respaldo mínimamente de 30 minutos.
  - La planta de emergencia del CS debe ser capaz de respaldar o de alimentar al banco de baterías por 4 días o más.

5.7.5.3 Equipo y Funcionalidades de los Equipos de los Operadores

5.7.5.3.1 Equipo de cómputo

5.7.5.3.1.1 Características de las computadoras personales

Cada operador debe contar con una Computadora Personal (PC) de escritorio que:

a) Tenga un procesador de última generación para computadoras personales de escritorio con suficiente velocidad de procesamiento para ejecutar adecuadamente todas las aplicaciones y/o programas que se requieran.
b) Tenga la capacidad necesaria de almacenamiento para la instalación de aplicativos e información para su labor.
c) Cuente con suficiente memoria RAM para ejecutar adecuadamente todas las aplicaciones y/o programas que se requieran.
d) Cuente con los siguientes puertos: USB, puertos para audífono, micrófono, y entrada y salida de línea; conexión para red y puerto de salida a video.
e) Debe contar con dos salidas de video o más, dependiendo de los requerimientos del CS.

5.7.5.3.1.2 Características de los monitores

a) Cada operador debe tener al menos un monitor para la captura de datos requeridos en la atención de una llamada de denuncia anónima en el CAD.
b) La resolución del monitor debe permitir una visualización adecuada en la captura de datos de cada una de las emergencias recibidas (CAD).
c) El monitor debe facilitar la apertura de diferentes ventanas en pantalla.
d) El monitor debe contar con ajuste para su orientación e inclinación.

e) La imagen en la pantalla debe ser estable, sin destellos ni reflejos.
f) El monitor debe tener la posibilidad de ajustar los niveles de intensidad luminosa, brillo y contraste, para adaptar la pantalla a las condiciones del entorno.
g) La pantalla debe tener una relación de aspecto de al menos 16:9.

5.7.5.3.1.3 Características de los periféricos

a) Cada operador debe de tener un ratón ergonómico que:

- Pueda ser utilizado cómodamente tanto por personas diestras como zurdas.
- Puede ser alámbrico o inalámbrico.

b) Cada operador debe de tener un teclado ergonómico que:

- Puede ser alámbrico o inalámbrico.
- Cuente con una superficie mate para evitar reflejos.
- Tenga las teclas suficientemente legibles desde la posición normal de trabajo.

5.7.5.3.2 Equipo telefónico

Se puede usar indiferentemente un teléfono físico con tecnología VoIP o una aplicación *softphone* para la computadora, y ambas deben cumplir con las siguientes características:

a) transferencia de llamadas
b) conferencia
c) llamada en espera
d) registro de llamada sin almacenar el número telefónico desde el cual se realiza la denuncia anónima
e) deben contar con teclas administrativas como:

   - llamada en espera
   - silencio
   - conferencia
   - transferencia
   - altavoz
   - subir/bajar volumen
   - menú
   - auriculares

f) Para teléfonos físicos:

- debe contar con pantalla telefónica.
- debe tener puerto para *FastEthernet* o *GigaEthernet* para conectarse a la Red LAN y puerto *FastEthernet o GigaEthernet* para conectarse a la PC.
- debe ser alimentado por *Ethernet* (PoE)
- debe tener puerto y/o enchufe para auriculares

g) El operador debe contar con una diadema para lograr la comunicación con las personas que hacen las llamadas de denuncia anónima, con las siguientes características:

- la diadema debe ser capaz de integrarse funcionalmente a un teléfono de escritorio (estándar)
- debe tener micrófono, auricular y horquilla de alta calidad
- debe tener micrófono anti ruido
- debe tener cancelación de ruido externo

El proveedor debe entregar en el momento de la instalación y puesta en marcha de cada uno de los equipos:

- Manual Técnico
- Manual de Instalación
- Manual de Mantenimiento
- Manual de Operación
- Protocolos de prueba
- Memoria Técnica

5.7.5.3.3 Controles de Acceso al Equipo del Operador

Debe cumplir los lineamientos de seguridad del capítulo 5.2, Apartado 5.2.6.3.

Nota: conjuntamente con estas características, se debe restringir las terminales que pueden acceder al equipo de cómputo.

5.7.5.4 Pruebas de Desempeño del Sistema de Atención de Denuncia Anónima 089

Deben realizarse pruebas de desempeño del sistema de denuncia anónima en la atención de las llamadas. Debido a que las denuncias se hacen exclusivamente por llamada telefónica, en la atención de una de ellas se debe:

1. llenar la información de la denuncia anónima en el CAD

2. verificar la asignación del "*Número de Identificación de Evento*" (folio)

Asimismo, deben realizarse pruebas en la atención de llamadas para determinar el desempeño del sistema, tales como:

a) Prueba de llamadas simultáneas

Tomando en cuenta la cantidad de operadores del sistema de denuncia anónima 089 con que cuente el CS, se debe:

1. realizar llamadas al CS, de tal forma que se supere a la cantidad de operadores del Sistema de Denuncia Anónima 089 (doble de llamadas con respecto a la cantidad de los operadores)
2. observar la asignación de turnos en el CAD ante esta situación
3. registrar el tiempo de atención a cada una de las llamadas

b) Prueba en la recepción de llamadas de broma/falsas:

1. se debe realizar llamadas de broma y/o falsas hacia el sistema de denuncia anónima 089
2. se debe verificar que el CAD registre la llamada
3. el protocolo que seguirá cada operador del Sistema de Denuncia Anónima 089 para la atención de este tipo de llamadas, dependerá del proceso establecido en el CS
4. se debe volver a marcar del mismo número para verificar si la Central Telefónica lo bloquea

5.8 Sistema de Alta Disponibilidad TIER III (ANSI/TIA-942)

5.8.1 Objetivo

Definir elementos, características y funcionalidades de topologías basadas en conmutadores de datos y enrutadores para mantener los servicios que estos ofrecen en alta disponibilidad.

5.8.2 Alcance

Se muestran esquemas que pueden ser aplicables a la red de datos del Complejo de Seguridad, las cuales pueden ser modificadas para mejorar la redundancia propuesta, siempre que se usen los protocolos de redundancia mencionados.

5.8.3 Campo de aplicación

Complejos de Seguridad.

5.8.4 Características del conmutador de datos y enrutadores de alto desempeño

5.8.4.1 Características físicas del conmutador de datos para sistemas de alta disponibilidad

El Conmutador de Datos Principal tiene la posición de nodo raíz en la topología de árbol o estrella en una red de datos, por lo que para mantener la disponibilidad de la red de datos debe cumplir con las siguientes características:

a) debe ser tipo chasis con varias ranuras para insertar tarjetas de puertos de red de la familia *Ethernet*, se debe considerar ranuras extras para crecimientos futuros y redundancia de tarjetas;
b) las tarjetas para el chasis deben cumplir con tarjetas para UTP RJ-45 y de fibra óptica con cualquiera de los siguientes conectores LC, ST, SC, FC, MTRJ o MPO;
c) las tarjetas deben ser *Hot Swap*. Esta característica permite el intercambio de una tarjeta sin necesidad de apagar el equipo;
d) debe proveer alta densidad de puertos. Debe proveer tarjetas de diferentes cantidades de puertos tipo UTP RJ-45 y para fibra óptica;
e) debe tener un MTBF que cubra 10 años de servicio o más, dependiendo del tiempo de vida que exija el diseño del sistema al que va a proveer;

f) el conmutador de datos debe tener soporte por parte del fabricante por el tiempo marcado en el MTBF o más. Dicho soporte debe incluir el cambio de tarjetas y fuentes de alimentación como mínimo;
g) el *backplane* del chasis debe proveer una capacidad de ancho de banda superior a la que demanda el chasis con todas las ranuras ocupadas y a su máxima capacidad de puertos;
h) el *backplane* debe tener un diseño pasivo;
i) si una tarjeta se daña, ésta no debe interferir o impactar con el funcionamiento de las demás tarjetas;
j) el conmutador de datos debe tener fuentes redundantes que balanceen la demanda eléctrica y, si falla una fuente, la que siga funcionando debe ser suficiente para poder soportar la demanda eléctrica de trabajo del conmutador de datos;
k) en caso de cambio de una fuente, ésta se debe poder cambiar sin necesidad de apagar el conmutador de datos;
l) debe proveer intercambio de ventiladores en caso de su daño, sin necesidad de apagar el conmutador de datos.

5.8.4.2 Características lógicas del conmutador de datos para sistemas de alta disponibilidad

El Conmutador de Datos Principal debe proveer en su parte lógica mecanismos que mantengan la alta disponibilidad en el servicio. La siguiente lista enumera protocolos y características que soportan la imagen del conmutador de datos relacionados a la alta disponibilidad. Los protocolos mencionados en la lista deben estar certificados en conformidad con una norma internacional. La lista no restringe el uso de otro protocolo de alta disponibilidad certificado en conformidad con una norma internacional.

a) El conmutador de datos debe ser de capa 2 y 3.
b) Debe poder aceptar actualizaciones de parches y *firmware* cuando sea requerido a través del protocolo ftp, sftp o tftp.
c) Soportar los siguientes protocolos de capa 2 del modelo OSI:
    i. El Protocolo de *Spanning Tree* Rápido (RSTP)
    ii. Protocolo de *Spanning Tree* Múltiple (MSTP) de la norma IEEE 802.1s.
    iii. Protocolo de Adición de Puertos de la norma IEEE 802.3ad
    iv. Protocolo de registro de VLAN GARP de la norma IEEE 802.1ak
    v. Protocolos para crear túneles GRE. Se aceptan otros certificados por un organismo internacional.

d) Soportar los siguientes protocolos de capa 3 de la IETF:
   i. OSPF
   ii. RIP
   iii. BGP
   iv. IS-IS
   v. DVMRP
   vi. Protocolo de Redundancia de Enrutador Virtual (VRRP)

5.8.4.3 Características de seguridad del conmutador de datos para sistemas de alta disponibilidad

a) Su administración debe ser a través de los siguientes protocolos seguros. Todo protocolo que se considere inseguro debe deshabilitarse:
   i. HTTPS
   ii. Ssh
   iii. Puerto de consola
   iv. Snmp v2c y v3
b) Debe estar protegido por un *firewall*, para restringir accesos desde computadoras no autorizadas.
c) Debe estar en un cuarto de telecomunicaciones con las condiciones especificadas en el apartado II.6.6.2 y sus subapartados.
d) El acceso al cuarto de telecomunicaciones debe ser controlado de acuerdo a los apartados II.8.1 en todos sus incisos.

5.8.4.4 Características físicas del enrutador de datos para sistemas de alta disponibilidad

El enrutador conecta la red LAN con Internet o a una red MAN o a la WAN. También puede estar conectando a todos los segmentos IP de la red del Complejo de Seguridad. Incluso el enrutador si tiene tarjetas de forma directa o a través del conmutador de datos principal. Su diseño físico debe cumplir con las características del apartado VIII.6.1 en todos sus incisos, además de estos debe tener tarjetas con puertos WAN apropiados para conectar la red LAN hacia la WAN, MAN o Internet.

5.8.4.5 Características lógicas del enrutador para sistemas de alta disponibilidad

Debe cumplir con el apartado VIII.6.2 en los incisos b) y d) quedando como opcional el inciso c), dependiendo de los requerimientos del Complejo de Seguridad.

5.8.4.6 Características de seguridad del enrutador para sistemas de alta disponibilidad

Debe cumplir con el apartado VIII.6.3 en todos sus incisos.

5.8.5 Esquemas de alta disponibilidad a nivel capa 2 en la Red LAN

5.8.5.1 Esquema de alta disponibilidad a nivel capa 2 para respaldar el conmutador de datos principal

El Conmutador de Datos Principal debe estar respaldado por otro de iguales características para tener alta disponibilidad en el caso de que el conmutador de datos falle. Estos dos conmutadores están conectados a los conmutadores de datos de acceso. La figura VIII.1 muestra un ejemplo de una topología que se puede usar en los Complejos de Seguridad sin limitar a otras que cubran los requerimientos de diseño. Se debe considerar para este diseño los siguientes requerimientos.

a) Considerar en el dimensionamiento de conmutadores de datos, puertos para la conexión redundante.
b) Los equipos pueden estar en el mismo cuarto de telecomunicaciones o en cuartos separados.
c) Si están en cuartos de telecomunicaciones separados, usar fibra óptica.
d) Si están en el mismo cuarto de telecomunicaciones, es opcional usar fibra óptica o cable UTP.
e) El uso de esta topología requiere la habilitación del protocolo *Spanning Tree* Rápido. El protocolo de *Spanning Tree* Rápido debe estar en conformidad con una norma de un organismo internacional.

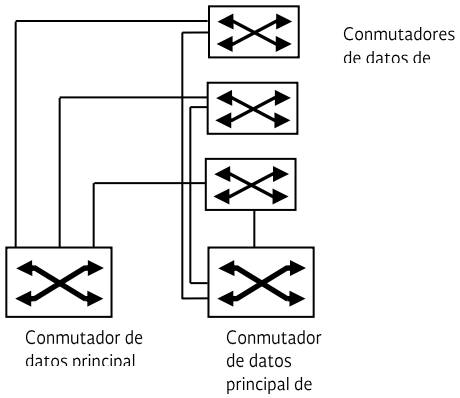


Figura VIII. 1Respaldo del conmutador de datos principal

5.8.5.2 Alta disponibilidad con redundancia de enlaces y VLAN

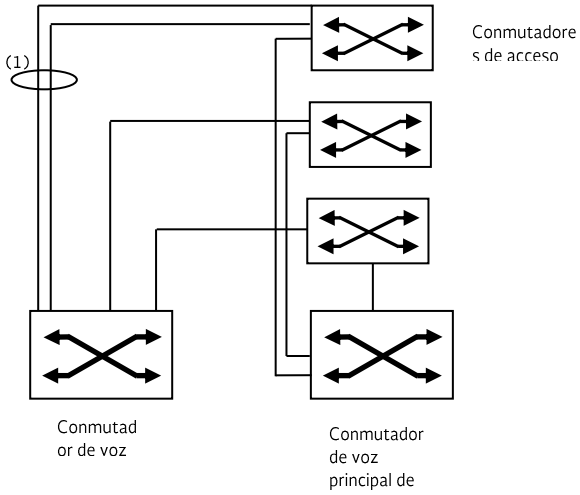
Como topología opcional y dependiendo del diseño de la red de datos del Complejo de Seguridad, se permite conectar dos conmutadores de datos a través de dos o más puertos que lleven tramas de VLAN, cumpliéndose las siguientes características:

a) debe funcionar con el protocolo *Spanning Tree* Múltiple, que debe estar en conformidad con una norma internacional
b) el protocolo *Spanning Tree* Múltiple debe crear una topología diferente de comunicación para cada VLAN

5.8.5.3 Alta disponibilidad con aumento de ancho de banda usando Adición de Puertos de la IEEE802.1.ad

En el caso de que se requiera aumentar el ancho de banda entre dos conmutadores de datos y al mismo tiempo tener respaldo de la conexión entre estos, si un cable falla, se permite conectar más de un cable de tecnología de la familia *Ethernet* de conmutador de datos a conmutador de datos. La figura VIII.2 es un ejemplo del uso del protocolo 802.1ad sin limitar poder usar otras con el protocolo 802.1ad. Para este tipo de conexión entre conmutadores de datos se debe cumplir lo siguiente:

a) las conexiones deben ser entre puertos que sean de algún tipo de tecnología *Ethernet*
b) los puertos deben estar configurados en full dúplex
c) se debe habilitar un protocolo de adición de puertos certificado de acuerdo a una norma internacional
d) se puede conectar dos o más cables entre dos conmutadores de datos
e) los anchos de banda de los cables conectados entre conmutadores de datos se suman y están todos activos, de tal forma que todos llevan tráfico de datos de usuario
f) en caso de falla de un cable, los restantes seguirán proveyendo la conectividad.



(1) Enlace tipo adición de puerto.

Figura VIII. 2Conexiones tipo adición de puertos

5.8.6 Esquema de alta disponibilidad con enrutadores y conmutadores de datos de capa 3 en la red LAN

5.8.6.1 Alta disponibilidad de las puertas de enlace

5.8.6.1.1 Uso de respaldo de puertas de enlace

Si se tienen dos salidas a Internet o dos salidas hacia la misma red, llámense WAN o MAN, conectar esas dos salidas a diferentes enrutadores quedando como indica la figura VIII.3, que muestra un ejemplo del respaldo de las salidas a Internet, sin que se limite el usar otras (en esta figura, el ejemplo es una salida a Internet pero puede ser hacia una WAN o MAN); asimismo, configurar un servicio de respaldo de la puerta de enlace como se indica en el apartado 5.8.6.1.2. La figura VIII.3 muestra un conmutador principal y enrutador separados, se permite que estos dos elementos estén en el mismo equipo.

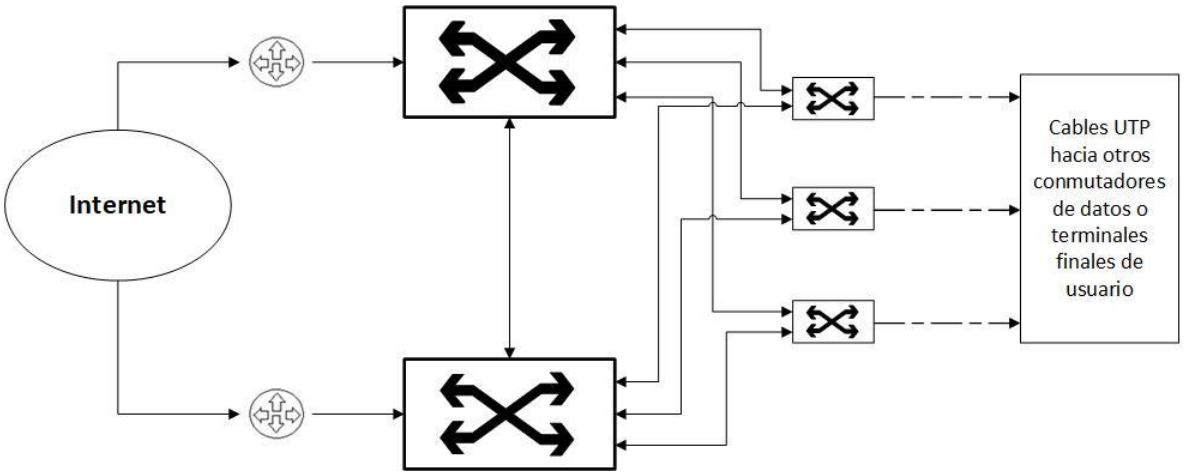


Figura VIII. 3 Topología de respaldo de la puerta de enlace para acceder a Internet con dos enrutadores

5.8.6.1.2 Características del respaldo de la puerta de enlace con enrutadores

Se debe cumplir los siguientes requisitos para un sistema de respaldo de puerta de enlace:

a) Las terminales finales de usuario verán como puerta de enlace las direcciones IP respaldadas por los enrutadores.
b) Debe haber por lo menos un enrutador de respaldo para respaldar al enrutador que da servicio como puerta de enlace. Se permite tener más de un enrutador de respaldo.
c) En caso de que el enrutador que da servicio como puerta de enlace falle, debe tomar su lugar cualquiera de los enrutadores de respaldo.
d) Cuando el enrutador que falló se restablezca, éste nuevamente atenderá las peticiones que se hagan a la puerta de enlace.
e) Se debe implementar la solución con el protocolo VRRP, en conformidad con normas internacionales.
f) Debe haber una puerta de enlace para cada VLAN o segmento IP, y cada una de ellas debe estar respaldada.
g) Se debe hacer la configuración de respaldo, de tal forma que las terminales de algunos segmentos IP salgan por un enrutador y las otras terminales de usuario salgan por el otro enrutador.

5.8.7 Alta disponibilidad para la red entre Complejos de Seguridad

5.8.7.1 Topologías de redundancia

Cuando se cuenta con una red estatal que interconecta a los Complejos de Seguridad se permite realizar interconexiones redundantes entre dichos Complejos, conectando los equipos de comunicaciones en una red en forma de anillo, doble anillo o en malla (ver la figura VII.4, VII.5 y VII.6); en el caso de la topología en malla y dependiendo de los requerimientos del sistema, no es necesario poner todas las conexiones entre nodos para que la malla esté completa. Cualquiera de las dos topologías puede ser usada, escoger una topología depende de los requerimientos del Complejo de Seguridad. Los medios usados para conectar estas topologías pueden ser cualquiera que soporte los anchos de banda establecidos en el diseño del sistema.

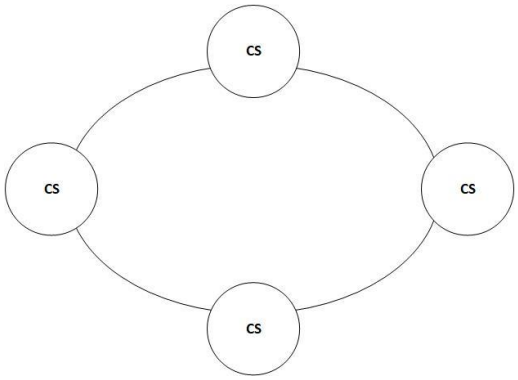


Figura VIII. 4 Topología en anillo para conectar Complejos de Seguridad (CS)

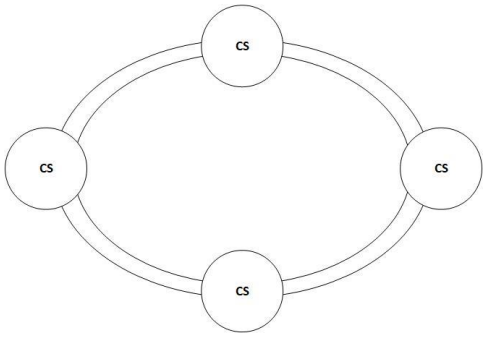


Figura VIII. 5 Topología en doble anillo para conectar Complejos de Seguridad (CS

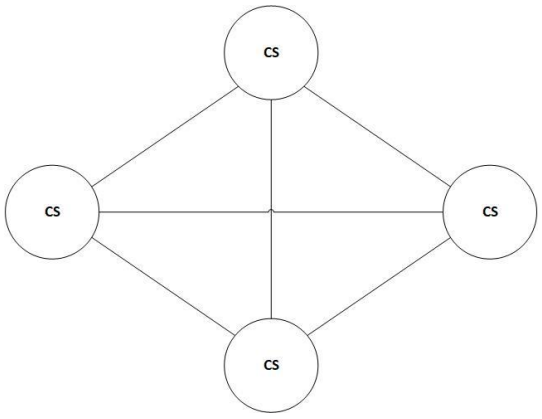


Figura VIII. 6 Topología en malla para conectar Complejos de Seguridad (CS)

5.8.7.2 Protocolos de ruteo para la redundancia

La redundancia está basada en protocolos de enrutamiento, de la IETF los cuales son los listados a continuación. Para que funcionen los protocolos de enrutamiento enlistados, la red debe usar el protocolo IP de la capa de red. No se restringe el uso de algún otro protocolo si está certificado en concordancia con normas internacionales.

a) OSPF
b) RIP
c) BGP
d) IS-IS
e) DVMRP

5.8.8 Soporte técnico

El soporte técnico es requerido para dar solución a incidencias en los equipos de comunicaciones. Se enlistan los servicios que debe dar el soporte técnico sin restringir algún otro que se considere necesario para cubrir los requerimientos del Complejo de Seguridad.

a) Debe proveerlo el fabricante conjuntamente con la compañía consultora o integrador, o la encargada de instalar y configurar el sistema.
b) Debe cubrir reemplazo de partes.
c) Debe tener en almacén respaldo de partes para que en caso de un cambio físico, se realice en plazos de tiempo cortos.
d) Debe dar soporte técnico las 24 horas del día los 365 días del año.
e) Debe dar asistencia en sitio para arreglar fallas.

f) La compañía que dé soporte debe estar de acuerdo en mantener los requerimientos de disponibilidad del equipo a nivel Tier III.
g) Debe haber un contrato de Nivel Servicio Acordado donde se estipulen los tiempos de respuestas.

5.9 Arquitectura de Servidores, Sistemas de Almacenamiento y Especificaciones para Recuperación de Desastres

5.9.1 Objetivo

Definir un marco normativo con los lineamientos necesarios para la correcta planeación, diseño, construcción, puesta en marcha y administración, de las diferentes arquitecturas de servidores y sistemas de almacenamiento para las instalaciones del Complejo de Seguridad, empleando las normas nacionales e internacionales vigentes que garanticen la adecuada operación de la infraestructura de equipos y servicios de voz, video, datos y aplicativos.

5.9.2 Alcance

Se dan especificaciones de las diferentes arquitecturas de alta disponibilidad que deben cumplir los Complejos de Seguridad. Se mencionan arquitecturas para servidores y bases de datos diferentes empezando con básicas hasta muy complejas; si un complejo determina que basta con una arquitectura simple y en lo futuro requiere migrar a otra más robusta, podrá escalar la actual a una superior, ya que los requerimientos aquí especificados lo permiten. No se debe tomar este apartado como una guía de diseño.

5.9.3 Campo de aplicación

Complejos de Seguridad.

5.9.4 Arquitectura de Servidores para mantener Alta Disponibilidad

5.9.4.1 Elección de una arquitectura de servidores

Cada arquitectura debe tener la capacidad de escalar a una arquitectura mejor, de tal forma que si el Complejo de Seguridad demanda mayor capacidad de cómputo ésta será solventada con base en las necesidades.

5.9.4.2 Arquitectura básica: dos servidores en espejo

La arquitectura básica está compuesta de dos servidores de características similares, uno llamado primario y el otro secundario. El primario está atendiendo a los usuarios que requieren del servicio; el secundario es un espejo del primario, donde el

secundario se actualiza tomando datos y configuraciones que se están ejecutando en el primario, o el primario manda los datos que mantiene y cambios de configuraciones al secundario. Los servidores primario y secundario en un ambiente de servidores, deben tener las siguientes características para mantener los servicios básicos necesarios de la operación:

a) Deben tener tarjetas de red redundantes con varios puertos cada una para garantizar la alta disponibilidad de velocidad nativa.
b) Deben tener 2 *sockets* o más en los servidores para procesadores, que soporten tecnologías de virtualización, para prever el crecimiento del sistema y su alta disponibilidad.
c) Fuentes de poder redundantes para cada servidor.
d) Cantidad de memoria RAM suficiente en lo servidores para cumplir la operación de los aplicativos y servicios instalados.
e) Capacidad de procesamiento suficiente en los servidores para cumplir la operación de los aplicativos y servicios instalados que se determinará con base en el número de puertos que se tengan y la velocidad que maneje el switch.
f) Discos duros locales en arreglos RAID con capacidad redundante para la recuperación de datos y compatibles con tecnologías NAS y SAN.
g) El almacenamiento de datos en los servidores debe ser local.
h) Los discos duros deben ser superiores a los 180 IOPS.
i) En caso de que el servidor primario pierda la operabilidad, la operación debe conmutar en el servidor secundario con los datos y servicios que se mantenían en el servidor primario.
j) El diseño LAN en los servidores debe contemplar tolerancia a fallos, de tal manera que en el momento de que entre ellos conmute, se sigan manteniendo los servicios disponibles.
k) El diseño de LAN debe contemplar el balanceo de carga en los enlaces para los servidores.
l) La arquitectura básica no contempla el uso de *hardware* con las tecnologías iSCSI y *fibre channel*, sin embargo los servidores deben tener la opción de implantación a futuro.
m) La arquitectura básica debe estar contemplada para que a futuro sea escalable según el apartado 5.9.4.3.

5.9.4.3 Arquitectura de servidores escalable

La arquitectura de servidores escalable debe tener las siguientes características, para mantener los servicios necesarios de la operación:

a) Se debe cumplir las especificaciones de la sección 5.9.4.2 los incisos a), b), c), d), e), f), h), j), k) e l).
b) De la sección 5.9.4.2 el inciso g) es opcional, dependiendo de los requerimientos de instalación y almacenamiento.

c) La arquitectura debe contemplar una escalabilidad vertical, es decir añadir más recursos al nodo o servidor, ejemplo memoria, discos más rápidos, etc.
d) La arquitectura escalable se debe implantar cuando se requiera hacer crecer los recursos de la arquitectura básica, como capacidad de almacenamiento, aplicaciones o servicios.
e) Esta arquitectura escalable contempla varios servidores primarios y secundarios, de tal forma que cada primario tiene su correspondiente espejo en un servidor secundario.
f) La arquitectura escalable o ambiente de producción debe contemplar la capacidad de servidores primarios y secundarios para garantizar la alta disponibilidad de los servicios.
g) La arquitectura de escalamiento debe tener la función de agregar más servidores heterogéneos en el mismo ambiente de producción.
h) La arquitectura escalable puede contemplar arreglos de discos RAID compartidos entre servidores, con capacidad redundante para la recuperación de datos.
i) Los servidores deben tener una facilidad de administración; se considera que 3 servidores primarios y 3 secundarios cumplen con esto. Si se requiere más potencia de cómputo, se debe pasar a la arquitectura de alta demanda de cómputo del apartado 5.9.4.4.
j) En caso de limitante en el almacenamiento local en los servidores, los discos RAID deben ser compatibles con tecnologías NAS y sus protocolos existentes en el mercado.
k) La arquitectura de escalamiento debe estar contemplada para que a futuro se integre a la arquitectura de alta demanda de cómputo del apartado 5.9.4.4.

5.9.4.4 Arquitectura para ambientes de alta demanda de cómputo

La arquitectura para ambientes de alta demanda de cómputo debe tener las siguientes características para mantener los servicios necesarios de la operación:

a) La arquitectura debe contemplar una escalabilidad vertical, es decir agregar más recursos al nodo o servidor, ejemplo memoria, discos más rápidos, etc.
b) La arquitectura debe contemplar una escalabilidad horizontal, es decir agregar más nodos o servidores permitiendo un balanceo de carga sobre los recursos de cómputo.
c) Se debe contar con máquinas virtuales, las cuales contarán con los servicios y aplicaciones necesarias.
d) Las máquinas virtuales deben contar con tolerancia a fallos para garantizar la alta disponibilidad entre ellas.

e) Las máquinas virtuales contarán con un escalamiento de recursos de cómputo, es decir incremento de CPU, memoria, disco duro, etc.
f) El ambiente de alta demanda de cómputo debe tener la capacidad de aprovechar al 80% o superior los recursos físicos de cómputo.
g) El ambiente de alta demanda de cómputo debe tener la opción de aceptar servidores heterogéneos, permitiendo la operabilidad entre ellos.
i) El ambiente de alta demanda de cómputo físico debe tener alta disponibilidad, alta confiabilidad y alto rendimiento.
j) El ambiente de alta demanda de cómputo físico debe garantizar una alta disponibilidad y confiabilidad de 99.999% o superior, basándose en indicadores MTTF, MTBF, MTTT y MTTR.
k) La arquitectura de escalamiento contempla el uso de *hardware* con las tecnologías iSCSI y *fibre channel,* las cuales permitirán la funcionalidad correcta en un ambiente de tipo SAN.
l) El ambiente de alta demanda de cómputo debe ofrecer una rápida elasticidad, es decir que los servicios de TI se escalen de acuerdo a sus necesidades, así sea triplicando de manera inmediata la capacidad de servidores.
m) El ambiente de alta demanda de cómputo debe tener la capacidad de migrar instancias a otro ambiente de alta demanda de cómputo ubicado en un centro de datos geográficamente diferente.

5.9.4.5 Características de aplicativos para su funcionamiento en alta disponibilidad

Las características de aplicativos para el funcionamiento de alta disponibilidad, en cualquier escenario de arquitectura de servidores, deben tener las siguientes características para mantener los servicios necesarios de la operación:

a) Los aplicativos deben estar diseñados para soportar la conectividad necesaria ya sea en sesiones múltiples o con múltiples usuarios conectados dependiendo de las necesidades y requerimientos del Complejo de Seguridad.
b) Los aplicativos deben soportar diferentes perfiles para su administración.
c) Los aplicativos deben tener distribuciones para ser instalados con más de 2 sistemas operativos existentes en el mercado.
d) Los aplicativos deben aprovechar los recursos de cómputo asignados, conforme los necesiten, hasta al 80%.
e) Los aplicativos deben soportar conexiones concurrentes.
f) Los aplicativos deben soportar conexiones simultáneas.
g) Los aplicativos deben estar diseñados para funcionar en ambientes virtuales.

5.9.5 Arquitectura de Almacenamiento

5.9.5.1 Arquitectura de almacenamiento para servidores espejo

Las características de almacenamiento para mantener la integridad de los datos deben ser las siguientes:

a) El sistema de almacenamiento local en los servidores debe tener la opción de configuración de tipo DAS.
b) Los discos duros deben ser superiores a los 180 IOPS.
c) El sistema de almacenamiento debe manejar configuraciones de tipo *offline*, es decir no poner discos *online* por la fuerza.
d) La configuración de almacenamiento en los servidores debe ser sencilla, pero garantizando la redundancia e integridad de los datos.
e) La capacidad de uso en cada uno de los discos no debe sobrepasar el 80%.
f) Las tecnologías de discos duros deben ser compatibles para sistemas NAS y SAN.
g) El sistema de almacenamiento debe tener como mínimo sistemas de respaldos completos, ya sean manuales o automáticos.

5.9.5.2 Arquitectura de almacenamiento para servidores escalables

a) El sistema de almacenamiento para los servidores escalables debe tener la configuración de funcionar con tecnología tipo NAS y SAN.
b) Los discos duros deben ser superiores a los 180 IOPS.
c) El sistema de almacenamiento debe manejar configuraciones de tipo *offline* y *online*.
d) La configuración de almacenamiento y administración debe garantizar la redundancia e integridad de los datos.
e) La capacidad de uso en cada uno de los discos no debe sobrepasar el 80%.
f) Las tecnologías de discos duros deben ser compatibles para sistemas NAS y SAN.
g) El sistema de almacenamiento debe tener sistemas de respaldos completos, diferenciales e Incrementales.
h) El sistema de almacenamiento debe tener sistemas de respaldos manuales y automáticos.

5.9.5.3 Arquitectura de almacenamiento para ambientes de alta demanda de cómputo

a) La arquitectura de almacenamiento para ambientes de alta demanda de cómputo debe funcionar con tecnologías de tipo SAN.
b) Los discos duros deben ser superiores a los 180 IOPS.
c) La arquitectura de almacenamiento para ambientes de alta demanda de cómputo debe tener canales de alta velocidad como *fibre channel*, iSCSI o mejor.

d) Los discos duros de la arquitectura de almacenamiento para servidores en espejos del apartado 5.9.5.1 deben funcionar con la arquitectura de almacenamiento para ambientes de alta demanda de cómputo.
e) Los discos duros de la arquitectura de almacenamiento para servidores escalables del apartado 5.9.5.2deben funcionar con la arquitectura de almacenamiento para ambientes de alta demanda de cómputo.
f) La arquitectura de almacenamiento para ambientes de alta demanda de cómputo debe garantizar la integridad de los datos, redundancia de datos y velocidad de transferencia idónea para cumplir con el correcto funcionamiento de los servicios y aplicaciones.
g) La arquitectura de almacenamiento de alta demanda de cómputo debe tener los protocolos básicos del mercado actual tales como FC-AL, FC-SW, iSCSI y FCoE.
h) La arquitectura de almacenamiento de alta demanda de cómputo debe funcionar con redes de tipo *Fibre Channel*, IP o mejor.
i) La arquitectura de almacenamiento de alta demanda de cómputo debe tener compatibilidad con tecnologías de almacenamiento de tipo DAS y NAS.

5.9.6 Alta Disponibilidad para Tarjetas de Red de Servidores

Las tarjetas de red que estén proporcionando la alta disponibilidad del enlace, en caso de fallo de una tarjeta o puerto, deben activar su puerto o todos los puertos necesarios para garantizar la alta disponibilidad del enlace.

5.9.7 Monitoreo de la Arquitectura de Servidores y Almacenamiento

5.9.7.1 Propósito del monitoreo

Con base en un análisis previo de requerimientos y necesidades para garantizar las capacidades de cómputo de los servicios, se debe contemplar un monitoreo para ambientes de servidores y ambientes de almacenamiento, con el fin detectar posibles problemas y tomar medidas correctivas.

5.9.7.2 Monitoreo para ambientes de servidores de arquitectura básica y servidores escalable

El monitoreo para ambientes de servidores debe tener las siguientes características para mantener los servicios necesarios de la operación:

a) El monitoreo para ambientes de servidores, ya sea local o en red deben contemplar las medidas de seguridad mencionadas en las secciones 5.2.6.1, 5.2.6.2, 5.2.6.6.1, 5.2.6.6.2, 5.2.6.6.3 del presente manual técnico. Se debe tener un esquema de monitoreo con el fin de conocer su estado físico, contemplando el estado de cada uno en tiempo real.

b) El monitoreo local debe tener notificador de alarma visual cuando cualquiera de los componentes físicos del servidor se encuentre comprometido.
c) El monitoreo debe contemplar notificaciones cuando los discos duros comiencen a tener una degradación de uso.
d) Los servidores deben tener la opción de manejar *syslog*, los cuales serán recolectados en un monitoreo centralizado que servirá para realizar análisis posteriores con respecto a los rendimientos de los servicios o equipos.
e) Se debe contar con un ambiente de monitoreo en el mismo centro de datos local, el cual debe ser multidispositivo, es decir que soporte dispositivos tales como *Tablets*, móviles e incluso *Smart* TV.
f) El ambiente de monitoreo debe contar con un diseño de escalamiento, es decir que si la organización crece no sea necesario cambiar la herramienta de monitoreo.
g) Se debe contar con ambiente de monitoreo en el mismo centro de datos local, el cual debe generar mensajes legibles (formato html) y que tenga la opción de enviarlos a distintos dispositivos, tales como correo electrónico, móvil o mediante diferentes protocolos *Whatsapp,* SMTP, push, entre otros.
h) El ambiente de monitoreo debe permitir medir el ancho de banda y el estado de cada enlace de conexión entre servidores, al igual que los principales aplicativos que estén sobre ellos, tales como servicios *Web*, CRM, servidores de correo, DNS, etc., y demás servicios que soporte.
i) El ambiente de monitoreo debe contar con un *pulling* menor de 5 minutos, teniendo el estado en un tiempo casi real.
j) El ambiente de monitoreo debe contar con paneles que puedan ser configurables y personalizables, el cual debe definir roles y accesos por rol.
k) El ambiente de monitoreo debe tener la flexibilidad de adaptar herramientas o *software* de particulares.
l) El ambiente de monitoreo debe contar con manejo de API de tipo SOA, para que otras aplicaciones aprovechen el trabajo o funcionamiento de la herramienta de monitoreo.
m) El ambiente de monitoreo debe tener integración a más de un motor de base de datos.
n) Se debe contar con un ambiente de monitoreo remoto, con las mismas características mencionadas en este apartado, en otro Complejo de Seguridad de respaldo.

5.9.7.3 Monitoreo para ambientes de almacenamiento

El monitoreo para ambientes de almacenamiento debe tener las siguientes características para mantener los servicios necesarios de la operación:

a) El monitoreo para ambientes de almacenamiento debe tener seguridad, ya sea local o en la red, para que los datos almacenados no se vean comprometidos.

b) El monitoreo para ambientes de almacenamiento debe mostrar métricas de capacidad de almacenamiento que determinen los recursos de almacenamiento utilizable y disponible.
c) El ambiente de monitoreo de almacenamiento debe contar con una visualización de detalles en las características de los arreglos de discos.
d) Tanto en los ambientes NAS como en los SAN se debe contemplar el monitoreo de almacenamiento de *pools* y *lun*, los cuales deben mostrar detalles de su capacidad utilizada y libre.
e) El ambiente de monitoreo de almacenamiento debe contar con un sistema de notificación o alarma, cuando esté por llegar a su capacidad máxima.

5.9.7.4 Monitoreo para ambientes de alta demanda de cómputo

El monitoreo para ambientes de alta demanda de cómputo debe tener las siguientes características para mantener los servicios necesarios de la operación:

a) Se debe cumplir las especificaciones de la sección 5.9.7.2 en sus incisos a), e), f), g), h), i), j), k), l), m), n).
b) El monitoreo para ambientes de alta demanda de cómputo debe contemplar el monitoreo de las máquinas virtuales y su disponibilidad.
c) El monitoreo para ambientes de alta demanda de cómputo debe contemplar el monitoreo de cada uno de los hypervisores.
d) El monitoreo para ambientes de alta demanda de cómputo debe ser de tipo geolocalización, es decir, compatibilidad con servicios o aplicaciones en la nube privada o pública.

5.9.8 Alta Disponibilidad de Central Telefónica

5.9.8.1 Requerimientos básicos de alta disponibilidad

a) Se debe contar con un equipo físico redundante (pasivo), el cual tendrá una réplica de configuración del equipo físico activo. Este debe estar en el Complejo de Seguridad donde está el equipo activo. Si hay un Complejo de Seguridad de respaldo, se permite un equipo físico redundante en dicho Complejo.
b) El ambiente de la Central Telefónica debe ser tolerante a fallos, con capacidad de administrar la tolerancia a fallos de forma manual o automática.
c) El ambiente de la Central Telefónica, en el caso de una contingencia, debe tener la capacidad de conmutar las llamadas o servicios a un Complejo de Seguridad de respaldo donde se tenga otro ambiente de central telefónica.
d) El ambiente de la Central Telefónica debe tener la capacidad de redirigir llamadas a un Complejo de Seguridad de respaldo donde se tenga otro ambiente de central telefónica.
e) El ambiente de la Central Telefónica debe tener la capacidad de manejar troncales redundantes SIP, digitales o analógicas.

5.9.9 Disponibilidad de un CS en caso de Desastre

5.9.9.1 Introducción

Se debe tener un Plan de Disponibilidad y Continuidad del Servicio, el cual está bajo la responsabilidad del departamento de Área de TIC, Seguridad Informática y Planeación. Esta norma contempla los mecanismos técnicos de comunicaciones y cómputo que se pueden considerar en dicho plan, la implementación de dichos mecanismos no es obligatoria y depende del Plan de Disponibilidad y Continuidad del servicio. A forma de resumen se describe los mecanismos técnicos cuyas especificaciones se mencionan en esta norma para la recuperación de los servicios en caso de un desastre.

Como prerrequisitos, en caso de un desastre, la recuperación de los servicios de un Complejo de Seguridad se realizará en uno alterno o de respaldo que puede ser tanto alguno diseñado para este fin u otro que esté en operación y que tenga las condiciones para, adicionalmente, funcionar como Complejo de Seguridad de Respaldo. Las condiciones necesarias que debe tener un Complejo de Seguridad de Respaldo son: infraestructura tecnológica en materia de telecomunicaciones, servidores, teléfonos, computadoras personales, sistemas de almacenamiento y personal estratégico que se requiera para proporcionar los servicios básicos, de acuerdo al Plan de Disponibilidad y Continuidad del Servicio; debe también estar conectado a la red de datos que comunica los Complejos de Seguridad dela misma entidad.

En la parte de las llamadas telefónicas, se debe tener como prerrequisito que la compañía telefónica que provee el servicio tenga un mecanismo de enrutamiento de llamadas al Complejo de Seguridad de Respaldo, así como enlaces directos a la red telefónica pública para mantener el servicio. El Complejo de Seguridad de respaldo tendrá un conmutador pasivo y/o activo, dimensionado para soportar las llamadas del Complejo de Seguridad respaldado. El conmutador pasivo y el activo tendrán un mecanismo de comunicación de tal forma que cuando el conmutador activo se inhabilite, el conmutador pasivo se vuelva activo y tome las llamadas que la compañía telefónica enruta a las líneas de respaldo en el Complejo de Seguridad principal.

En la parte del servidor de video vigilancia, se debe tener un dispositivo configurado de fábrica para esta función o un servidor virtual dimensionado e instalado por el proveedor; en ambos casos, debe haber un dispositivo o servidor de video vigilancia de respaldo en el Complejo de Seguridad de respaldo, en el que las cámaras dadas de alta serán las mismas para ambos Complejos de Seguridad, al igual que las

configuraciones de administración y funcionalidad de acuerdo a los requerimientos de video vigilancia, es decir deben estar sincronizados, de tal forma que si un complejo de seguridad queda deshabilitado tendrá su dispositivo o servidor de video vigilancia de respaldo en el Complejo de Seguridad destinado para esta función.

Los servidores para los servicios que tenga el Complejo de Seguridad, serán virtualizados en un servidor pasivo de respaldo, en el Complejo de Seguridad de respaldo. Las configuraciones del servidor activo en un Complejo de Seguridad podrán ser transferidas de manera manual o automática al servidor virtualizado pasivo del Complejo de Seguridad de respaldo. Debe haber un mecanismo de comunicación entre servidores activo y pasivo, de tal forma que si el servidor activo deja de funcionar, el servidor pasivo tomará su lugar. El servidor pasivo podrá cambiar su estado a activo de manera manual o automática, para esto los Complejos de Seguridad se deben apoyar también en un sistema de monitoreo de los servidores virtualizados, ya que en este tipo de ambientes pueden suceder falsos positivos.

Las bases de datos deben estar en espejo en ambos Complejos de Seguridad, de tal forma que los cambios que se realicen en la base de datos del Complejo de Seguridad respaldada se actualicen de manera automática en la base de datos del Complejo de Seguridad de Respaldo.

5.9.9.2 Especificaciones para los sistemas de recuperación de servidores en caso de un desastre,

En caso de contemplar un Complejo de Seguridad de respaldo para otro Complejo, éste debe cumplir con lo siguiente.

a) Para la arquitectura de servidores de ambiente básico, en el caso de que el Complejo de Seguridad se encuentre inoperable, se activará un servidor secundario en el Complejo de Seguridad de respaldo, con los datos y servicios del servidor primario. Este servidor secundario debe cumplir con el apartado 5.9.4.2 de los incisos a) a la f), k) y l). Y para el sistema de almacenamiento debe cumplir con el apartado 5.9.5.1 en todos sus incisos.

b) Para la arquitectura de servidores de ambiente básico el almacenamiento del Complejo de Seguridad de respaldo debe ser local, además de ser espejo del servidor primario.

c) Para la arquitectura de servidores de ambiente básico, el servidor secundario del Complejo de Seguridad de respaldo debe ser tolerante a fallos, manteniendo los servicios disponibles del servidor primario cuando el Complejo de Seguridad respaldado falle.

d) Para la arquitectura de servidores de ambiente escalable en el caso de que el Complejo de Seguridad se encuentre inoperable, se activarán los servidores secundarios en el Complejo de Seguridad de respaldo, con los datos y servicios de los servidores primarios. Estos servidores secundarios deben cumplir con el apartado 5.9.4.3 en los incisos a) a la d) y h), j) y k).

e) Para la arquitectura de servidores de ambiente escalable, los servidores secundarios del Complejo de Seguridad de respaldo deben tener una facilidad de administración. Si se requiere más potencia de cómputo se debe pasar a la arquitectura de alta demanda de cómputo del apartado 5.9.4.4.

f)Para la arquitectura de servidores de ambiente escalable, el sistema de almacenamiento del Complejo de Seguridad de respaldo debe tener la configuración de funcionar con tecnología tipo NAS y SAN, además de cumplir con el apartado 5.9.5.2 de los incisos b) a la h).

g) Para la arquitectura de ambientes de alta demanda de cómputo en el Complejo de Seguridad de respaldo, se debe cumplir el apartado 5.9.4.4 en todos sus incisos.

h) Para la arquitectura de ambientes de alta demanda de cómputo, el sistema de almacenamiento del Complejo de Seguridad de respaldo debe cumplir el apartado 5.9.5.3 en todos sus incisos.

i) Los servidores secundarios del Complejo de Seguridad de respaldo en lo referente de las tarjetas de red, deben cumplir con el apartado 5.9.6.

j) Los servidores secundarios de arquitectura básicos o servidores escalables del Complejo de Seguridad de respaldo deben tener un ambiente de monitoreo que cumpla el punto 5.9.7.2.

j) Los sistemas de almacenamiento del Complejo de Seguridad de respaldo deben cumplir con el punto 5.9.7.3

k) Los sistemas de ambiente de alta demanda de cómputo del Complejo de Seguridad de respaldo deben cumplir con el monitoreo especificado en el punto 5.9.7.4 en todos sus incisos.

5.9.9.3 Especificaciones para el conmutador de recuperación de la telefonía en caso de un desastre

Para la recuperación de la telefonía, el conmutador debe cumplir el apartado 5.9.8.

5.9.9.4 Especificaciones para los servidores de video vigilancia de recuperación de la video vigilancia en caso de un desastre

Los servidores de video vigilancia instalados en un Complejo de Seguridad de respaldo deben cumplir con lo siguiente:

a) El Sistema de Video Vigilancia del Complejo de Seguridad de respaldo debe cumplir con el capítulo 4 en todos sus apartados.

b) En caso de que el servidor de video vigilancia se instale en un servidor físico o virtual con un sistema operativo tipo servidor, debe cumplir con el apartado 5.9.9.2

c) El sistema de video vigilancia del Complejo de Seguridad de respaldo debe tener dadas de alta a las cámaras que tiene los Complejos de Seguridad respaldados.

5.9.9.5 Recuperación de servicios críticos

Los servicios de las áreas prioritarias a recuperar en un Plan de Disponibilidad y Continuidad del Servicio, específicamente en su Plan de Recuperación contra Desastres, se listan a continuación. No se limita la recuperación de otros servicios que se consideren críticos, dependiendo de lo establecido en el Plan de Disponibilidad y Continuidad del Servicio, en su Análisis de Riesgo.

a) 9-1-1.
b) Despacho.
c) Radiocomunicación.
d) Sistema de Video Vigilancia.
e) Voz
f) Datos
g) 089

5.10 Protocolos de Comunicación y el Diseño de Red de Datos: Interoperabilidad

5.10.1 Objetivo

El objetivo de este apartado es definir los protocolos de comunicación y el diseño de la red de datos para satisfacer las necesidades de las entidades públicas que acceden a los servicios brindados por el CS, así como para fortalecer funcionamiento del Complejo de Seguridad a partir de la interoperabilidad interna y externa, es decir, el intercambio de datos de las siguientes bases de datos:

i. Informe Policial Homologado
ii. Licencias de Conducir
iii. Mandamientos Judiciales
iv. Registro Nacional de Armamento y Equipos
v. Registro Nacional de Información Penitenciaria
vi. Registro Nacional de Personal de Seguridad Pública
vii. Registro de Vehículos Robados y Recuperados
viii. Registro Público Vehicular
ix. Incidencia Delictiva
x. Sistema de Atención de Emergencias 9-1-1 y Denuncia Anónima 089

5.10.2 Alcance

El alcance de este apartado comprende las siguientes bases de datos:

i. Informe Policial Homologado
ii. Licencias de Conducir
iii. Mandamientos Judiciales
iv. Registro Nacional de Armamento y Equipos
v. Registro Nacional de Información Penitenciaria
vi. Registro Nacional de Personal de Seguridad Pública
vii. Registro de Vehículos Robados y Recuperados
viii. Registro Público Vehicular
ix. Incidencia Delictiva
xi. Sistema de Atención de Emergencias 9-1-1 y Denuncia Anónima 089

La figura X.1 muestra la comunicación entre los Complejos de Seguridad.

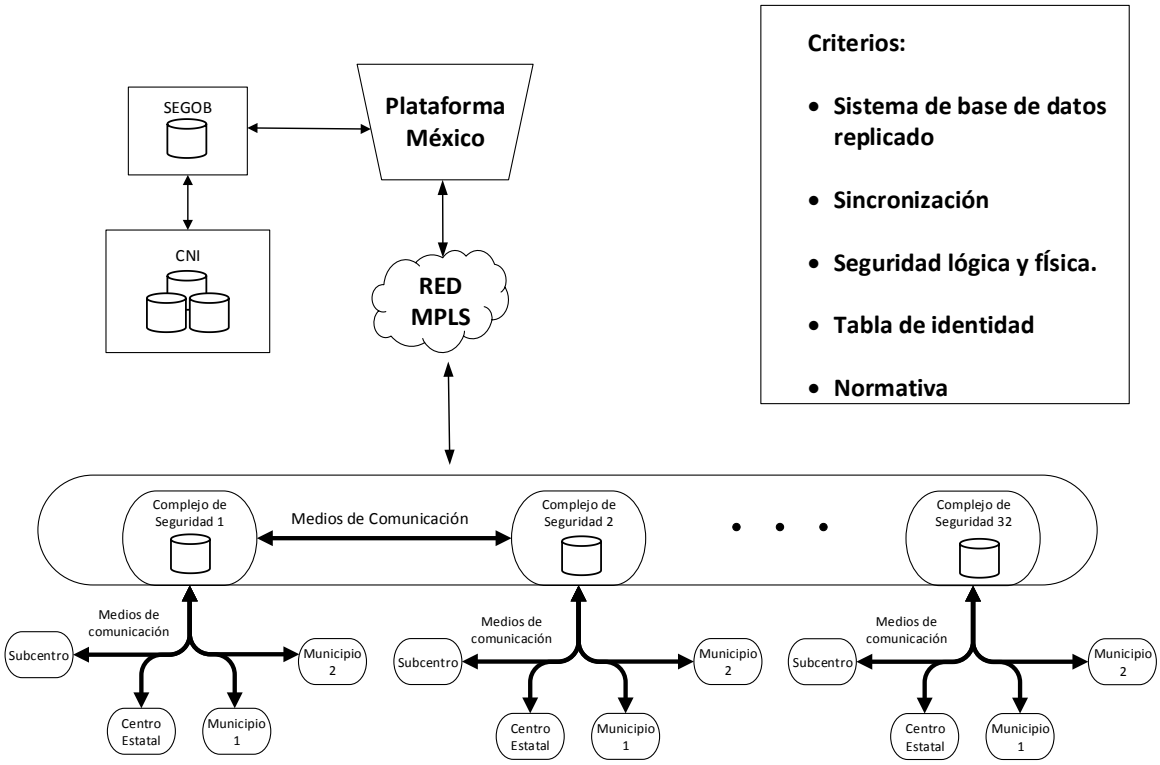


Figura X. 1 Esquema de comunicación entre los Complejos de Seguridad

5.10.3 Campo de aplicación

El campo de aplicación de este apartado es hacia los Complejos de Seguridad, en específico en lo relativo a las características técnicas para un adecuado protocolo de comunicación y diseño de red de datos (interoperabilidad interna y externa).

5.10.4 Descripción

En todas las organizaciones, entre ellas las públicas como los Complejos de Seguridad, se maneja información, y ésta se interrelaciona mediante redes, por lo que se tiene la necesidad de contar con un sistema para compartir información, a partir de la cual se puedan tomar decisiones críticas y claras. Se precisa disponer de información clara, confiable y oportuna, lo cual redundará en una mayor calidad de los procesos que se operan a partir de la misma.

Una Plataforma Tecnológica para la Integración de Información que permita al Complejo de Seguridad (CS) contar con un sistema para compartir datos en tiempo

real, permite favorecer el conocimiento y la actualización de información para brindar un servicio con mayor eficiencia y calidad.

Este apartado propone la definición de protocolos de comunicación y el diseño de la red de datos para el funcionamiento del Complejo de Seguridad en su interoperabilidad interna y externa, de modo que se contribuya a una mejora en la calidad de los procesos de comunicación internos y externos del CS: mayor eficiencia, reducción de errores, eliminación de duplicidad de datos, entre otros.

Lo anterior, para el cumplimiento de los objetivos en materia de operación policial, emergencias, comunicaciones de seguridad pública y para consulta y explotación de las bases de datos: 1. Informe Policial Homologado, 2. Licencias de Conducir, 3. Mandamientos Judiciales, 4. Registro Nacional de Armamento y Equipos, 5. Registro Nacional de Información Penitenciaria, 6. Registro Nacional de Personal de Seguridad Pública, 7. Registro de Vehículos Robados y Recuperados, 8. Registro Público Vehicular, 9. Incidencia Delictiva y 10. Sistema de Atención de Emergencias 9-1-1 y Denuncia Anónima 089.

A partir de la información que se fue recolectando en visitas de campo, entrevistas y cuestionarios aplicados a personas de los Complejos de Seguridad de Aguascalientes, Hidalgo, Jalisco, Durango, Baja California Sur, Michoacán, Nayarit, Oaxaca, Quintana Roo, San Luis Potosí, Tlaxcala, Veracruz, Toluca y Querétaro, se identificó que la información se encuentra dispersa y las bases de datos muestran heterogeneidad en su estructura y organización; consecuentemente, puede haber funcionalidades redundantes, baja eficiencia y mayor esfuerzo de análisis dada tal dispersión. Asimismo, el acceso a la información puede ser parcial, y en consecuencia se limitan las opciones y variables para la toma de decisiones, lo que redunda en acciones y políticas públicas poco eficaces e incluso ineficientes. Ese fenómeno se produce por la baja calidad e ineficiencia del manejo de la información, que se traducen en duplicidad de procedimientos e información para la toma de decisiones. Adicionalmente, la información disponible puede estar desactualizada, lo que genera impactos negativos a nivel operativo e inclusive económico.

Por lo anterior, atendiendo a la necesidad de asegurar una adecuada interoperabilidad interna y externa de la información del CS, entendida ésta como la capacidad de comunicación entre diferentes bases de datos de manera oportuna y confiable, se buscará la integración de las bases de datos en un sistema que permita la interoperabilidad, a efecto de brindar acceso inmediato para consultas y explotación de la información en materia de operación policial, emergencias y comunicaciones de seguridad pública, entre otras posibilidades.

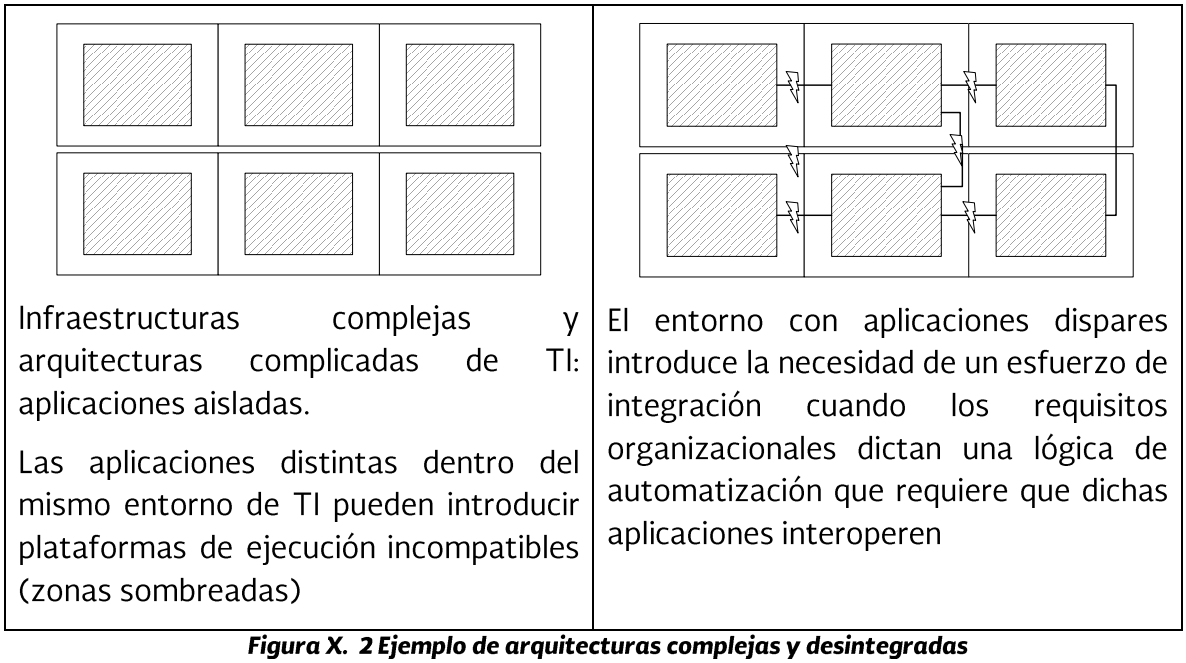
5.10.5 Aplicación de las Especificaciones en Sistemas de Bases de Datos para los Complejos de Seguridad

Se describen las características de las bases de datos (Informe Policial Homologado, Licencias de Conducir, Mandamientos Judiciales, Registro Nacional de Armamento y Equipos, Registro Nacional de Información Penitenciaria, Registro Nacional de Personal de Seguridad Pública, Registro de Vehículos Robados y Recuperados, Registro Público Vehicular, Incidencia Delictiva, Sistema de Atención de Emergencias 9-1-1 y Denuncia Anónima 089),así como la forma en la que interoperarán para el intercambio eficiente de información entre las instancias municipales, estatales o federales, a través de la implementación de formatos definidos por el Centro Nacional de Información la (CNI) del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública.

5.10.6 Principios Fundamentales

5.10.6.1 Interoperabilidad

Es común la existencia de aplicaciones desarrolladas de manera independiente, lo que puede resultar redundante en términos de funcionalidad; de este modo, un Sistema de Tecnologías de Información puede acumular numerosas aplicaciones con un propósito redundante, lo que resulta innecesario o mejorable; en este punto, es importante visualizar que distintas aplicaciones pueden despegarse en plataformas de ejecución incompatibles, lo que implica un esfuerzo de integración cuando se trata de propiciar que las aplicaciones interoperen, como se muestra en la siguiente figura X.2.



Infraestructuras complejas y arquitecturas complicadas de TI: aplicaciones aisladas. Las aplicaciones distintas dentro del mismo entorno de TI pueden introducir plataformas de ejecución incompatibles (zonas sombreadas)	El entorno con aplicaciones dispares introduce la necesidad de un esfuerzo de integración cuando los requisitos organizacionales dictan una lógica de automatización que requiere que dichas aplicaciones interoperen

Figura X. 2 Ejemplo de arquitecturas complejas y desintegradas

Interoperabilidad se refiere al intercambio de datos, por lo que cuanto más interoperables sean las bases de datos, más fácil será el intercambio de información. De este modo, resulta recomendable disponer de un buen nivel de interoperabilidad intrínseca de un servicio, es decir, los servicios deben diseñarse para ser interoperables entre sí, independientemente de cuándo y para qué fin se entregan.

La interoperabilidad comienza con la utilización de estándares, los cuales pueden ser internos o de diseño de los CS.

Establecer y mantener la interoperabilidad, se asocia a los preceptos y procesos de gobernanza de SOA (Arquitectura Orientada a Servicios), los cuales establecen reglas y normas que regulan la forma en la que los servicios se planifican, se entregan y evolucionan en apoyo al mantenimiento de la interoperabilidad intrínseca.

5.10.7 Nivel de Servicios

La Plataforma Tecnológica para la Integración de Información del CS, debe cumplir con determinados Niveles de Servicio, mismos que habrán de considerar las funcionalidades requeridas para su disponibilidad: servicios de interoperabilidad de información entre los CS, CNI y Plataforma México.

En este apartado se especifican los Niveles de Servicio sólo en los puntos de salida: entrega a entidad “origen” de las peticiones y envío de peticiones a entidades “destino” para la obtención de los datos solicitados. De manera intermedia, el CS debe considerar y cumplir los acuerdos de niveles de operación entre los elementos de la arquitectura de la Plataforma.

5.10.7.1 Especificaciones del Nivel del Servicio en el CS

Las mediciones de los tiempos de respuesta de los elementos de la Plataforma se deben realizar sobre el intercambio de mensajes y datos que se efectúe entre cada elemento, de acuerdo al modelo de operación y a los estándares requeridos siguientes (ver tabla X.1):

Tabla X. 1 Especificaciones del Nivel del Servicio

Ref.	Nivel de Servicio	Estándar Requerido
1	Disponibilidad de la infraestructura medida en periodo de 30 días hacia atrás, considerando las ventanas de tiempo.	99.99%
2	Transacciones exitosas.	100%
3	Peticiones al sistema atendidas sin exceder 2 segundos.	100%
4	Disponibilidad del Servicio de Monitoreo, considerando las ventanas de tiempo.	99.90%
5	Disponibilidad, integridad y resguardo permanente de la información de la plataforma incluyendo las bitácoras, respaldos y todo aquel registro que conforma el servicio, considerando las ventanas de tiempo.	100%
6	Rechazo a ataques o infiltraciones a la plataforma no autorizados.	100%
7	Tiempos de atención a fallas dentro de los tiempos comprometidos.	100%
8	Eventos de contingencia devueltos a operación en el sitio principal en menos de 24 horas (máximo un evento por mes).	100%

5.10.7.2 Ventanas de Tiempo

Las ventanas de tiempo válidas y/o permitidas para considerar los niveles de servicio que debe proporcionar la Plataforma en cada uno de sus elementos se indican en la siguiente tabla, señalando las requeridas para efectuar las actividades de respaldo y/o mantenimiento de los elementos que integran dicha Plataforma. Ver tabla X.2.

Tabla X. 2 Ventanas de Tiempo

Evento	Descripción del requerimiento de tiempo	Duración de la Ventana	Número de eventos
Mantenimiento de infraestructura	Se requiere intervenir sobre algún elemento de la Capa por fallos físicos o de configuración.	2 (dos) horas.	Máximo 1 (un) evento por trimestre
Recuperación de Respaldos	En caso de que se requiera la recuperación de un respaldo, previa solicitud con al menos 7 días naturales de antelación.	24 (veinticuatro) horas	Máximo 1 (un) evento por mes
Capa de Datos	Se requiere intervenir sobre algún elemento de *software* (herramienta o aplicación) por fallos en su configuración o en su funcionalidad.	1 (una) hora	Máximo 2 (dos) eventos por mes
Capa de Gestión	Se requiere intervenir sobre algún elemento de *software* (herramienta o aplicación) por fallos en su configuración o en su funcionalidad.	1 (una) hora	Máximo 2 (dos) eventos por mes

La calendarización de la ventana de tiempo debe ser acordada y aprobada por el CS con los usuarios para no afectar el servicio. Asimismo, durante la ventana de tiempo no se medirán dichos tiempos para la evaluación de niveles de servicio en el ámbito de afectación de la ventana, hasta la normalización del servicio.

Las ventanas de tiempo deben ser autorizadas por el la Alta dirección del CS.

5.10.7.3 Fallas en el servicio

El no cumplir con el estándar requerido en los niveles de servicio originará una falla en el servicio.

Al precisar la no disponibilidad de la infraestructura (nivel de servicio con referencia 1) se puede generar una afectación total o parcial, de este modo el número de categorías de Fallas en el Servicio son 9, como se muestra en la siguiente tabla X.3.

Tabla X. 3 Fallas en el servicio

Ref.	Nivel de Servicio	Estándar Requerido	Categoría de Falla	Descripción
1	Disponibilidad de la infraestructura medida en periodo de 30 días hacia atrás, considerando las ventanas de tiempo.	99.99%	Afectación Total	La Plataforma es incapaz de responder a peticiones tanto desde su sitio principal como del sitio de respaldo.
2	Disponibilidad de la infraestructura medida en periodo de 30 días hacia atrás, considerando las ventanas de tiempo.	99.99%	Afectación Parcial	No tiene acceso parcial o total a la Plataforma alguno de los CS.
3	Transacciones exitosas.	100%	Transacción No Exitosa	Cuando una transacción recibida no se vuelva exitosa, por causa imputable al Proveedor o por error de procesamiento.
4	Peticiones al sistema atendidas sin exceder 2 segundos.	100%	Falla de Desempeño	Cuando una petición al sistema excede 2 segundos en ser respondida por el sistema.
5	Disponibilidad del Servicio de Monitoreo, considerando las ventanas de tiempo.	99.90%	Afectación en el Servicio de Monitoreo	No disponibilidad parcial o total del Servicio de Monitoreo mayor al tiempo permitido, afectando la visibilidad desde el CS sobre el desempeño y disponibilidad del servicio.
6	Disponibilidad, integridad y resguardo	100%	Pérdida de	No disponibilidad, error en la integridad o no

Ref.	Nivel de Servicio	Estándar Requerido	Categoría de Falla	Descripción
	permanente de la información de la plataforma incluyendo las bitácoras, respaldos y todo aquel registro que conforma el servicio, considerando las ventanas de tiempo.		Información	resguardo permanente de cualquier información contenida o manejada por la plataforma tecnológica, incluyendo las bitácoras, respaldos y todo aquel registro que conforma el servicio.
7	Rechazo a infiltraciones a la plataforma no autorizados.	100%	Intrusiones al Sistema	Cualquier infiltración no autorizada a la plataforma tecnológica.
8	Tiempos de atención a fallas dentro de los tiempos comprometidos.	100%	Tiempo de Atención a Fallas	Cuando una Falla en el Servicio es atendida fuera de los tiempos comprometidos.
9	Eventos de contingencia devueltos a operación en el sitio principal en menos de 24 horas (máximo un evento por mes).	100%	Operación en Contingencia	Operación bajo contingencia mayor a 24 horas.

5.10.7.4 Indicadores de Desempeño

Los Indicadores de Desempeño permiten medir si el Nivel de Servicio ha alcanzado o no el estándar requerido en el período de evaluación. Los indicadores de desempeño y el período de medición son listados en la tabla X.4.

Tabla X. 4 Indicadores de Desempeño

Ref.	Categoría de Falla	Descripción	Período de evaluación	Indicador de Desempeño
1	Afectación Total	La Plataforma es incapaz de responder a peticiones tanto desde su sitio principal como del sitio de respaldo.	30 días hacia atrás contados desde el minuto actual.	Disponibilidad de la infraestructura para todos los usuarios, medida en minutos, considerando las ventanas de tiempo.
2	Afectación Parcial	No tiene acceso parcial o total a la Plataforma alguno de los CS.	30 días hacia atrás contados desde el minuto actual.	Disponibilidad de la infraestructura para todos los usuarios de un nodo de acceso, medida en minutos, considerando las ventanas de tiempo.
3	Transacción No Exitosa	Cuando una transacción recibida no sea exitosa, por causa imputable al Proveedor o por error de procesamiento.	Tiempo de espera para que una transacción recibida se vuelva exitosa.	Tiempo transcurrido desde la recepción de una transacción hasta que se vuelva exitosa.
4	Falla de Desempeño	Cuando una petición al sistema excede 2 segundos en ser respondida por el sistema.	1 segundo después de recibir el sistema una petición.	Tiempo transcurrido entre la petición al sistema y la respuesta del sistema.
5	Afectación en el Servicio de Monitoreo	No disponibilidad parcial o total del Servicio de Monitoreo mayor al tiempo permitido, afectando la visibilidad desde el CS sobre el desempeño y	30 días hacia atrás contados desde el minuto actual.	Disponibilidad del Servicio de Monitoreo para el CS, medida en minutos, considerando las ventanas de tiempo.

Ref.	Categoría de Falla	Descripción	Período de evaluación	Indicador de Desempeño
		disponibilidad del servicio.		
6	Pérdida de Información	No disponibilidad, error en la integridad o no resguardo permanente de cualquier información contenida o manejada por la Plataforma tecnológica, incluyendo las bitácoras, respaldos y todo aquel registro que conforma el servicio.	Continuo en tiempo real durante el tiempo que determine el CS.	Detección por medios relacionados a la Plataforma o por medios externos de que se ha presentado una pérdida de información.
7	Intrusiones al Sistema	Cualquier infiltración no autorizada a la plataforma tecnológica.	Continúo en tiempo real durante el mes contractual.	Detección por medios relacionados a la Plataforma o por medios externos de que se ha presentado un intento de infiltración no autorizado.
8	Tiempo de Atención a Fallas	Cuando una Falla en el Servicio es atendida fuera de los tiempos comprometidos.	Tiempo comprometido por el proveedor para la atención a fallas.	Tiempo transcurrido entre la detección de una falla por el Sistema de Monitoreo o reportada por un usuario, y la atención a la misma.
9	Operación en Contingencia	Operación bajo contingencia mayor a 24 horas.	24 horas después de iniciar la contingencia.	Tiempo transcurrido, después de iniciar la operación bajo contingencia.

5.10.7.5 Supervisión del desempeño

Para supervisar de manera permanente el desempeño y la disponibilidad del servicio se debe contar con un módulo de monitoreo en el que se pueda observar no solamente el desempeño de los Niveles de Servicios solicitados, sino también el desempeño de los procesos de negocio (transacciones) que se realizan por tipo en la Plataforma. Dicho módulo debe desplegar gráficas de desempeño y una consola para la obtención automática de reportes de desempeño. La información estadística presentada podrá ser consultada de forma histórica y por el periodo de tiempo que determine conveniente el CS.

5.10.8 Infraestructura

5.10.8.1 Arquitectura de Interoperabilidad SOA (Modelo)

Para asegurar una adecuada interoperabilidad interna y externa de las bases de datos del CS se diseñará una red de datos y su correspondiente SOA (Arquitectura Orientada a Servicios[1]). Se trata de asegurar la integración de aplicaciones para optimizar procesos, responder de manera efectiva, reducir los costos de Tecnologías de la Información (TI) y lograr la flexibilidad requerida por el CS.

La alta disponibilidad de información buscará una mayor integración y comunicación para interconectar procesos, personas e información, apoyados en protocolos de comunicación e infraestructura que permitan responder a tal encomienda.

SOA será el marco de trabajo conceptual para la integración de aplicaciones, en aras de optimizar procesos y así, reducir costos, innovar en los servicios, proporcionar flexibilidad y adaptación efectiva y rápida ante cambios tecnológicos, razones por las que se considera la más conveniente. Es fundamental que complementariamente se tomen en cuenta los mecanismos de acceso seguro y estándares de intercambio de información. De este modo, la seguridad es un factor de importancia en la adopción de una tecnología SOA, dado que los servicios Web utilizan protocolos de Internet para el envío y recepción de mensajes a través de un navegador.

Dentro de las medidas de seguridad que se pueden adoptar está la utilización de estándares, de este modo, las peticiones HTTP generadas desde los navegadores de los usuarios son resueltas en un servidor conectado a la red pública; ahora bien, los

[1]Para mayor información sobre el tema, se sugiere consultar Erl, T., (2005), SOA Principles of Service Design.

servidores de aplicación tanto públicos como privados se comunican entre sí cuando la aplicación lo demande.

La arquitectura para operar la Plataforma Tecnológica para la Integración de Información (PTII) del CS se debe conformar por 5 Capas independientes entre sí, pero que se acoplan para cumplir la funcionalidad requerida y soportar así los requerimientos de los usuarios y los procesos de negocio.

Esta arquitectura está diseñada para enlazar servicios y recursos computacionales de una entidad central, así como aplicaciones y datos, para obtener los resultados demandados por los usuarios de los servicios del CS, que pueden ser usuarios finales, otros servicios de la Plataforma y otros servicios de otros sistemas relacionados que puedan aprovechar los datos que residen en la PTII y/o otras dependencias.

La siguiente figura X.3 del diseño de la arquitectura de la Plataforma Tecnológica para la Integración de Información, muestra las Capas que la conforman:

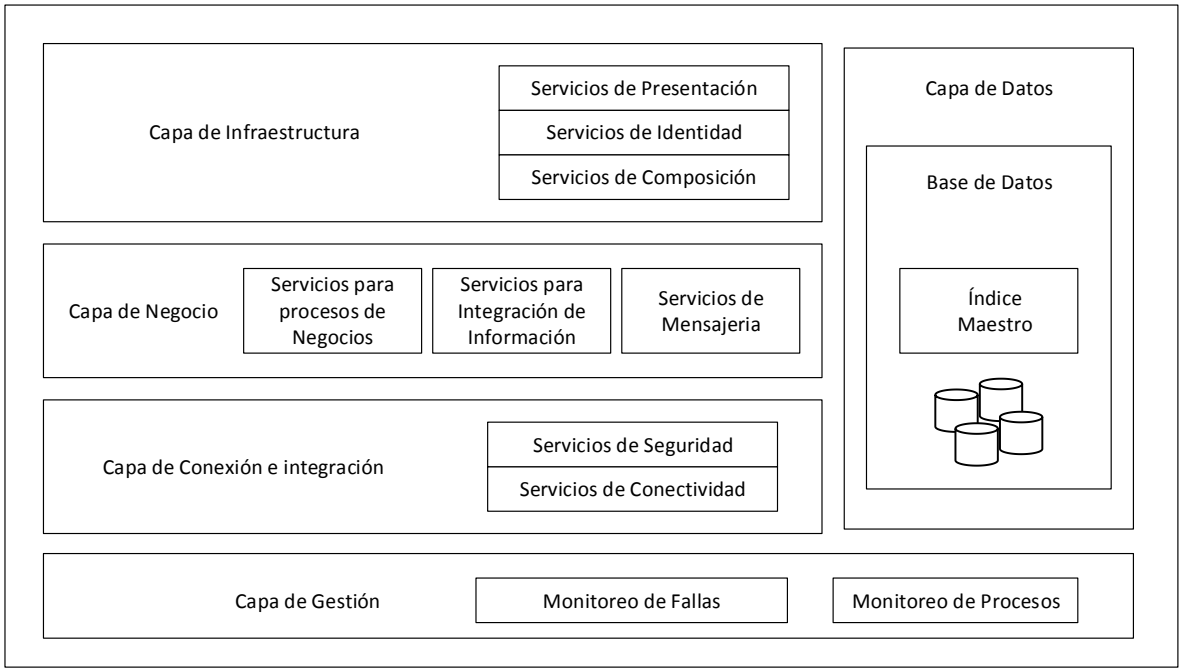


Figura X. 3 Arquitectura de la Plataforma Tecnológica para la Integración de Información (PTII)

La PTII debe apegarse a las siguientes medidas para el desarrollo, mantenimiento y uso de la SOA:

- Reusabilidad, granularidad, modularidad, relacionamiento de los componentes e interoperabilidad.
- Identificación y categorización de servicios, aprovisionamiento y despacho, así como monitoreo y seguimiento.
- Los siguientes son los principios específicos de la arquitectura SOA para el diseño y definición, enfocada en servicios que deben ser aplicados a la Plataforma PTII:
  - Encapsulamiento de servicios.
  - Servicios de Acoplamiento Débil (*Service Loose Coupling*): este servicio mantiene un relacionamiento que minimiza las dependencias entre sistemas y únicamente requiere que cada parte simplemente tenga conocimiento de que la otra existe.
  - Contrato de servicios: los servicios se deben incluir en los acuerdos de comunicaciones que se definen en los documentos de descripción de servicios entre uno o más servicios.
  - Abstracción de servicios: describir cómo funciona el servicio en el mundo real.
  - Reutilización o reusabilidad del servicio: se deben plantear servicios que puedan ser fácilmente reutilizados.
  - Empaquetamiento de servicios: una colección de servicios que pueden ser coordinados y ensamblados para formar un paquete compuesto de servicios.
  - Autonomía de servicios: servicios que tienen el control sobre la lógica que ellos encapsulan.
  - Optimización de servicios: aseguramiento de servicios de alta calidad.
  - Habilidad de descubrimiento de servicios: los servicios son creados con descripciones necesarias y son descubiertos utilizando los mecanismos contenidos para tal fin.
- Cumplimiento con estándares.
- Documentación del servicio.

La arquitectura de sistema que se utilizará debe precisar al menos los rubros que se describen a continuación.

5.10.8.2 Requerimientos de la Arquitectura Orientada a Servicios

Debe apegarse a estándares para garantizar la no existencia de limitaciones para futuras migraciones del sistema a otras plataformas, de acuerdo a las necesidades que surjan. Los estándares de la *Web Services Interoperability Organization* (WS-I) mínimos a los que se deben apegar los componentes de Arquitectura Orientada a Servicios son:

- XML *Schema* 1.0
- *Simple Object Access Protocol* (SOAP 1.1)
- *Web Services Description Language* (WSDL 1.1 o superior)
- *Universal Description, Discovery and Integration* (UDDI 2.0, opcional)

El cumplimiento de dichos estándares debe ser avalado mediante catálogos originales del fabricante de los elementos de *software* o registros ante la WS-I.

5.10.8.3 Capa de Negocio

La capa de negocio debe establecer la lógica de interacción entre los distintos *Web Services* que hacen que el sistema funcione. La Capa de Negocio debe estar creada bajo el concepto de WS-BPEL, permitiendo crear "orquestaciones" en las que intervengan los servicios y por lo tanto puede crear flujos que representen procesos de negocio del CS.

La solución debe contar con una herramienta visual para crear, editar y eliminar las orquestaciones. A continuación se muestra una figura X.4 que muestra la Capa de Negocios de la Plataforma Tecnológica para la Integración de Información (PTII).

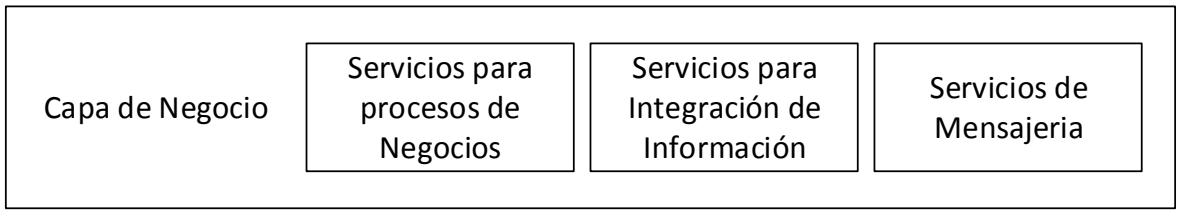


Figura X. 4 Capa de Negocio de la Plataforma Tecnológica para la Integración de Información

Funcionamiento

La Capa de Negocio debe ser la encargada de establecer y ejecutar la lógica de operación de los servicios que intervienen en la Plataforma Tecnológica para la Integración de Información del CS. Esta Capa debe proporcionar facilidades

suficientes para permitir la interacción de ella con los servicios y el intercambio de mensajes entre los mismos. Además debe actuar como un medio que facilite la interacción, el intercambio de mensajes y la orquestación de los *Web Services* que componen la Plataforma.

Los *Web Services* a los que esta Capa debe dar servicios estarán alojados en las Capas de Conexión e Integración y en la Capa de Datos. Es decir, la Capa de Negocio actúa como una interfaz entre la Capa de Conexión e Integración y la Capa de Datos; además permite que los servicios contenidos en ambas Capas intervengan en la lógica orquestada por ella.

La orquestación de los servicios debe ser creada utilizando una interfaz gráfica que permita establecer la orquestación de manera más sencilla. Esta interfaz gráfica debe ejecutarse en el sistema operativo *Windows* u otro de escritorio equivalente, independientemente del servidor y sistema operativo donde se ejecuten la plataforma de WS-BPEL y los servicios a coordinar.

La interfaz gráfica debe ser capaz de crear procesos de negocio ejecutables y procesos de negocio abstractos, de forma que se puedan crear librerías de procesos que sean reutilizables según las necesidades de la Plataforma.

Las características con las que debe contar la Capa de Negocio son las siguientes (ver tabla X.5):

Tabla X. 5 Características de la Capa de Negocios

Número	Capa de Negocio
1	La Capa de Negocios debe ser capaz de soportar la arquitectura SOA, es decir, los *Web Services* deben estar creados en cualquier tecnología, siempre y cuando cumplan con los estándares del W3C.
2	La Capa de Negocios debe ser capaz de utilizar un registro *Web* e interactuar con *Web Services* basados en UDDI.
3	La Capa de Negocios debe estar basada en WS-BPEL y debe cumplir con todas la recomendaciones establecidas por OASIS. El documento donde se especifica WS-BPEL en su versión 1.0 como mínimo o preferentemente en la más reciente que es "*Web Services Business Process Execution Language* Versión 2.0" de fecha 11 de Abril de 2007.
4	Debe contar con una interfaz gráfica para la creación de las

Número	Capa de Negocio
	orquestaciones que involucran los *Web Services*.
5	Debe ser capaz de manejar excepciones y fallas de los procesos.
6	La interfaz gráfica debe ejecutarse sobre Sistema Operativo u otro de escritorio equivalente.
7	La interfaz gráfica debe poder modelar procesos ejecutables y abstractos.

Especificaciones de protocolos y *Web Services*

1. *Web Services Description Language* (WSDL)

WSDL es el lenguaje usado para la definición de los *Web Services*, está basado en XML y tiene una especificación dentro de los estándares de W3C; el documento de definición del WSDL es "*Web Services Description Language* (WSDL) Version1.1" o superior.

Los procesos de orquestación creados con WS-BPEL se deben modelar y exponer utilizando WSDL.

2. XML *Schema*

Los esquemas XML se deben utilizar para establecer la estructura, contenido y semántica de documentos XML. Los esquemas XML a utilizar serán los que están definidos por el W3C dentro del documento "XML *Schema Part* 0: Primer *Second Edition*" (verificar en la bibliografía). Este documento está acompañado por los siguientes, para efectos del presente apartado (referidos en la bibliografía):

1) XML *Schema Part* 1: *Structures Second Edition.*
2) XML Schema Definition Language (XSD): *Component Designators.*
3) *Guide to Versioning* XML *Languages using new* XML *Schema* 1.1 *features.*
4) *Processing* XML 1.1 *documents with* XML *Schema* 1.0 *processors.*

3. *Extensible Stylesheet Language Transformations* (XSLT)

XSLT se debe utilizar para transformar documentos XML en otros documentos XML. La versión de XSLT a utilizar será la definida por el W3C dentro del documento "XSL *Transformation* (XSLT) *Version*1.0" o superior. Los demás documentos de la familia y que son importantes para la definición de XSLT son:

1) XML *Path Language* (XPath) *Version* 1.0 o superior
2) *Extensible Stylesheet Language* (XSL) *Version* 1.0 o superior

4. *Web Services Business Process Execution Language Version* (WS-BPEL)

Al momento de crear cualquier proceso de negocios es mandatario ejecutar un análisis estático básico de dichos procesos, de forma que se puedan eliminar aquellos en los que el análisis falla. Es posible que algunas implementaciones de WS-BPEL agreguen análisis no listados en la especificación (para revisar cosas adicionales o enviar *warnings*); en esos casos, dichos análisis deben ser configurables para poder ser habilitados o deshabilitados según las necesidades del desarrollador.

La Capa de Negocio debe cumplir con los análisis estáticos descritos dentro de la especificación. Los análisis estáticos especificados están descritos en el documento "*Web Services Business Process Execution Language Version1*.0".

El cumplimiento de los requerimientos anteriores puede ser comprobado mediante certificaciones o membresías en los diferentes cuerpos de estándares responsables.

5.10.8.4 Capa de Conexión e Integración

Estructura

La Capa de Conexión e Integración es la responsable de contener los *Web Services* y establecer la conexión desde la Plataforma Tecnológica para la Integración de la Información del CS con los sistemas:

i. Informe Policial Homologado
ii. Licencias de Conducir
iii. Mandamientos Judiciales
iv. Registro Nacional de Armamento y Equipos
v. Registro Nacional de Información Penitenciaria
vi. Registro Nacional de Personal de Seguridad Pública
vii. Registro de Vehículos Robados y Recuperados

viii. Registro Público Vehicular
ix. Incidencia Delictiva
x. Sistema de Atención de Emergencias 9-1-1 y Denuncia Anónima 089

Esta Capa debe poseer los componentes necesarios para contener un sistema con Arquitectura Orientada a Servicios (SOA). La Capa debe, por tanto, tener capacidad de:

1) Ejecutar aplicaciones de la plataforma de ejecución Java, .Net o cualquier plataforma de ejecución y/o desarrollo que sea capaz de ejecutar *Web Services*.
2) Tener la capacidad de trabajar con el protocolo SOAP (*Service Oriented Architecture Protocol*).
3) Contar con registro de los servicios proporcionados, UDDI (*Universal Description Discovery and Integration*) (opcional).
4) Escalabilidad y distribución.

El sistema debe estar basado en estándares, aun cuando los componentes utilizados sean comerciales. La Capa de Conexión e Integración de la Plataforma Tecnológica para la Integración de Información del CS se muestra a continuación. Ver figura X. 5.

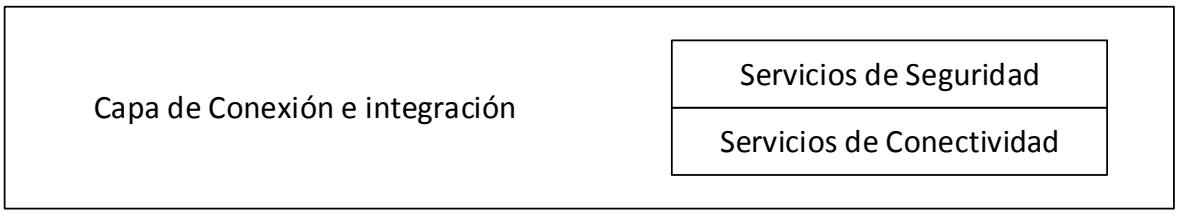


Figura X. 5 Capa de Conexión e Integración de la Plataforma Tecnológica para la Integración de Información

Funcionamiento

Esta Capa debe funcionar como una interfaz entre la Plataforma Tecnológica para la Integración de la Información del CS y los sistemas:

i. Informe Policial Homologado
ii. Licencias de Conducir
iii. Mandamientos Judiciales
iv. Registro Nacional de Armamento y Equipos
v. Registro Nacional de Información Penitenciaria
vi. Registro Nacional de Personal de Seguridad Pública

vii. Registro de Vehículos Robados y Recuperados
viii. Registro Público Vehicular
ix. Incidencia Delictiva
x. Sistema de Atención de Emergencias 9-1-1 y Denuncia Anónima 089

Además, debe ser capaz de solicitar servicios a otras dependencias y/o instituciones utilizando *Web Services* públicos o privados. La Plataforma debe poder comunicarse con *Web Services* incluyentes, es decir, el hecho de que esta Capa tenga la capacidad de comunicarse con algunos en específico, no excluye la posibilidad de comunicarse con otros servicios en cualquier momento.

Por otro lado, esta Capa debe ser capaz de alojar servicios *Web* cuya funcionalidad pueda ser requerida por los Sistemas del CS.

Características

1) La Capa de Conexión e Integración debe ser capaz de soportar la arquitectura SOA (*Service Oriented Architecture*).
2) La Capa debe estar basada en contenedores de aplicaciones Java, .Net o cualquier plataforma de ejecución y/o desarrollo que sea capaz de ejecutar *Web Services*.
3) La Capa debe poder alojar y ejecutar *Web Services* y debe ser capaz de alojar y ejecutar aplicaciones que sean capaces de solicitar servicios de *Web Services* alojados en otros servidores o lugares físicos.
4) La Capa debe poseer un registro UDDI (*Universal Description Discovery and Integration*) donde registre los Servicios que proporciona la Capa de Conexión e Integración (opcional).
5) Debe tener la capacidad de trabajar con el protocolo SOAP (*Service Oriented Architecture Protocol*).

5.10.8.5 Capa de Datos

La Capa de Datos de la Plataforma es la encargada de almacenar la información. En esta Capa se encuentran las bases de datos:

i. Informe Policial Homologado
ii. Licencias de Conducir
iii. Mandamientos Judiciales
iv. Registro Nacional de Armamento y Equipos

v. Registro Nacional de Información Penitenciaria
vi. Registro Nacional de Personal de Seguridad Pública
vii. Registro de Vehículos Robados y Recuperados
viii. Registro Público Vehicular
ix. Incidencia Delictiva
x. Sistema de Atención de Emergencias 9-1-1 y Denuncia Anónima 089

En esta Capa se manejará la lógica de la relación entre las bases de datos, la forma en la que se deben llenar, los campos requeridos por registro en cada base de datos y los estándares a seguir para lograrlo

La siguiente figura X. 6 muestra los aspectos que se deben cubrir para esta Capa.

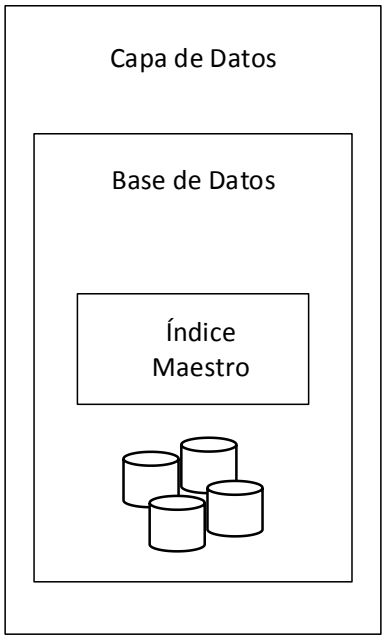


Figura X. 6 Capa de Datos de la Plataforma Tecnológica para la Integración de Información

La solución propuesta debe contener los Servicios *Web* necesarios para:

- Alimentar los identificadores de cada Registro de las bases de datos
- Identificar a cada Registro Judicial en los diferentes dominios del sistema
- Agregar Registro
- Modificar información de Registro
- Notificar a otros CS del sistema de eventos en el Registro

- Resolver duplicados de información (saber que los datos de dos Registros corresponden al mismo registro)
- Borrar registros (inhabilitación de los registros) cuando así se determine por la instancia correspondiente.

El CS debe crear perfiles jerárquicos de administración, lectura, escritura y/o ejecución en relación a las funciones del personal y de acuerdo a sus políticas de seguridad informática.

Se debe contar con una base de datos de referencia llamada Repositorio de Referencias Judiciales para almacenar las referencias a los sistemas CS municipales. Las bases de datos deben estar en espejo para asegurar que la información siempre esté disponible y consistente para así posibilitar el análisis secundario de la información.

Las especificaciones que se debe desarrollar, en la arquitectura de la solución de la Capa de Datos de la Plataforma, son las que se muestran en la siguiente figura X.7.

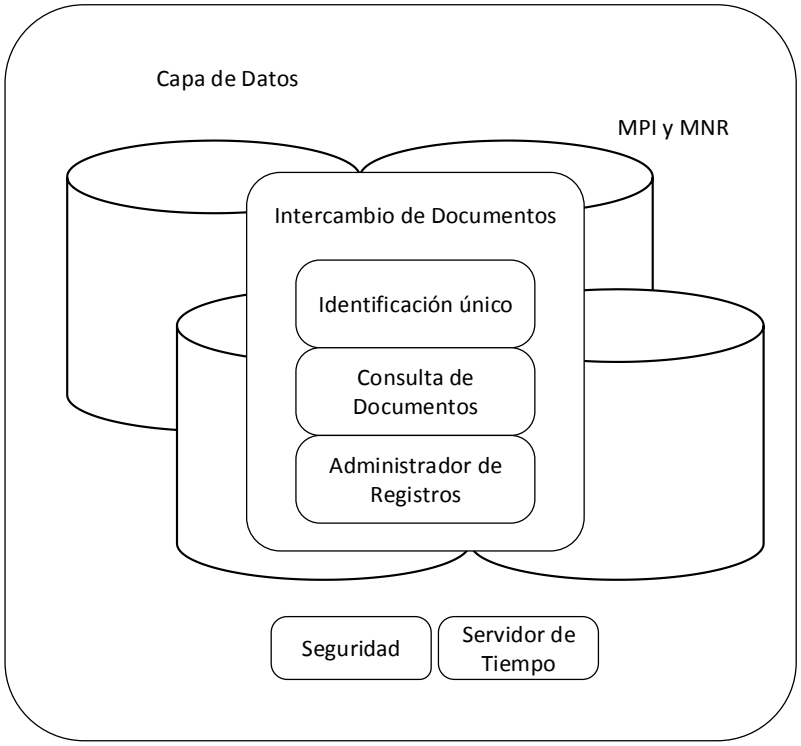


Figura X. 7 Capa de Datos de la Plataforma Tecnológica para la Integración de Información

La Plataforma Tecnológica para la Integración de Información usará el Perfil de Referencia Cruzada para Compartir Documentos (XDS por sus siglas en inglés), el cual es un conjunto de información judicial estructurada que ha sido guardada en él, y forma un elemento de información judicial que va a ser compartida a nivel de CS. Éste debe ser legible para personas y aplicaciones y tener un identificador único.

Los principios base de los XDS son:

- Distribuido: cada CS publica información para otros. Los documentos permanecen en la SOA origen.
- Centrado en los documentos: la información publicada son expedientes, en los cuales sólo el CS fuente y el CS consumidor del documento procesan la información.

Los Actores y Transacciones del Perfil XDS de la PTII se muestran en la siguiente figura X.8.

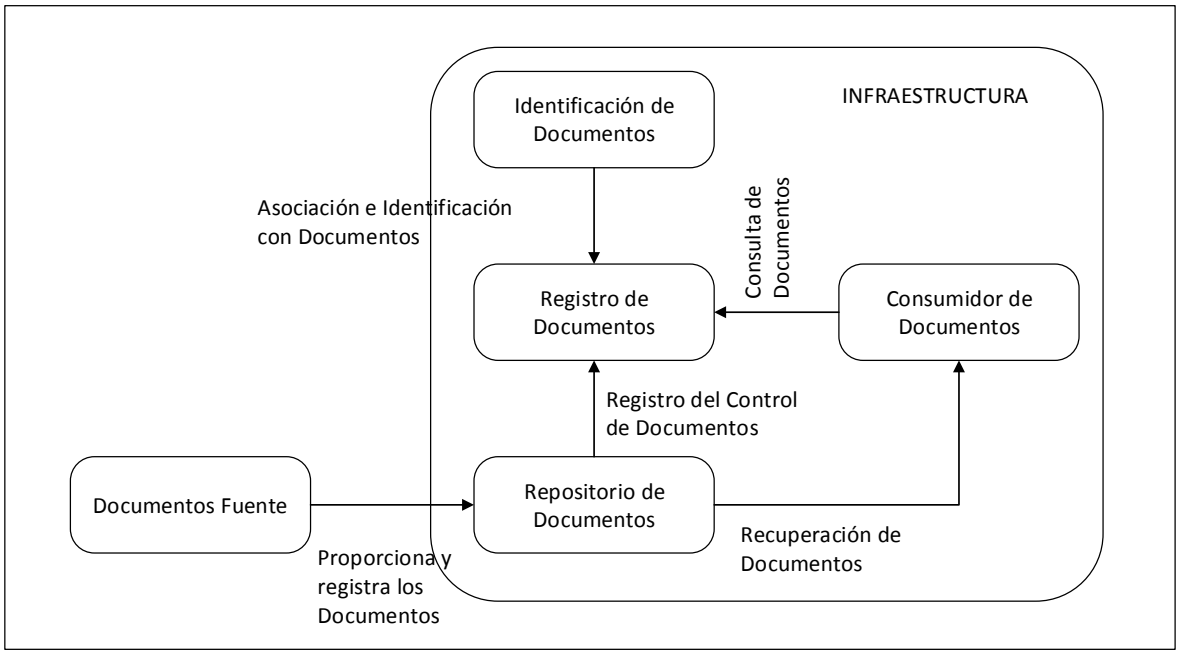


Figura X. 8 Flujo para el intercambio de documentos

Actores y transacciones

- Documento Fuente
- Sistema de información que genera el documento
- Repositorio de Documentos
- Acepta documentos y metadatos del "Documento Fuente"

- Almacena el documento, reenvía los metadatos al registro, reproduce el documento bajo petición (permite recuperación del documento)
- Registro de Documento
- Registro, en el que se almacena
- Metadatos del documento
- Enlace al lugar donde se encuentra realmente el documento
- Responde a consultas de acuerdo con unos determinados metadatos
- Consumidor de Documentos
- Hace queries, es decir, consultas al registro, muestra listado de documentos disponibles
- Recupera los documentos elegidos por usuario
- Utiliza los documentos para mostrarlos por pantalla
- Identificador de Referencias Judiciales
- Fuente de identidad de Referencias Judiciales

Transacciones

1. Proporciona y Registra los Documentos
2. Recuperación de Documentos
3. Registro del Control de Documentos
4. Consulta de Documentos
5. Asociación e Identificación con Documentos

Perfil de Referencias Cruzadas

El Perfil de Referencias Cruzadas (PRC) soportará las referencias cruzadas de los expedientes que tengan identificadores múltiples en diferentes dominios de la PTII y se encargará de:

- Transmitir la información de identificación de Registros Judiciales desde la fuente hasta el administrador de PRC
- Proporcionar la habilidad de acceder a los identificadores de las listas de referencias vía búsqueda de base de datos o actualizaciones de notificación

Con la utilización de PRC en la PTII se obtendrá un vínculo y una referencia de toda la información de los Registros Judiciales para proporcionar la interoperabilidad necesaria de intercambio de información entre dominios de los CS mientras se mantiene la flexibilidad entre los procesos involucrados. El Diseño Detallado y Flujo del Proceso se muestran en la siguiente figura X. 9.

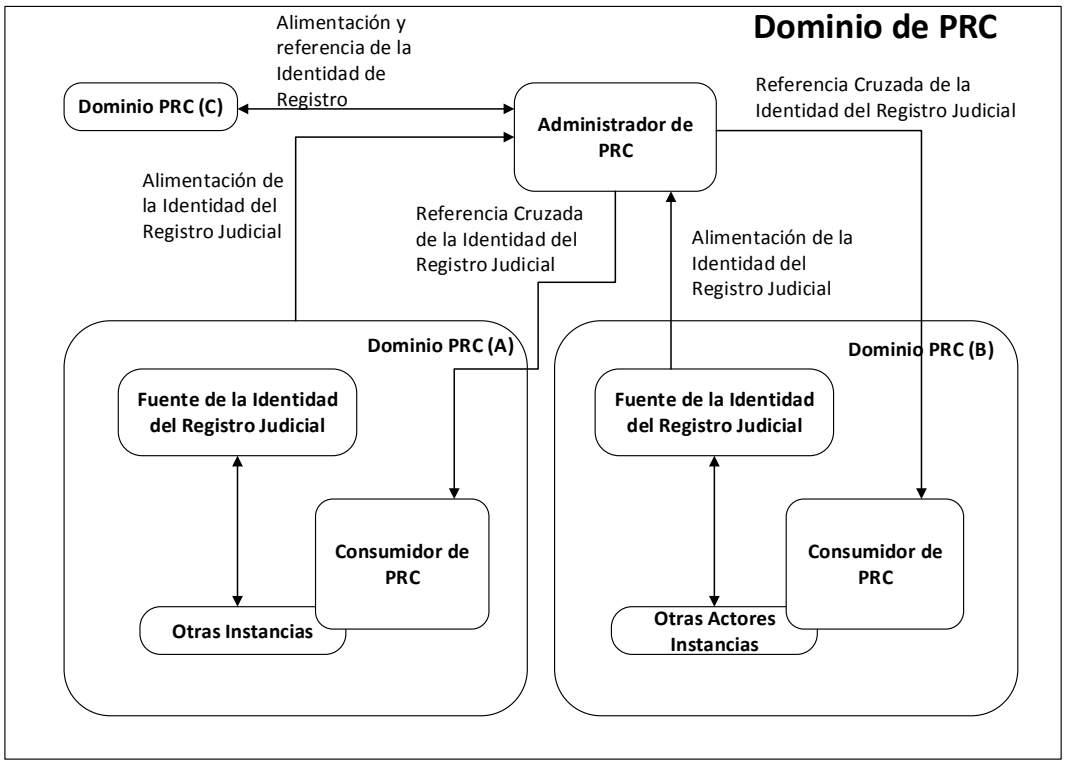


Figura X. 9 Diseño detallado del Perfil de Referencias Cruzadas (PRC)

El Perfil de Integración de PRC soporta dos Dominios:

- Dominio de Identificación de los CS, que se define como un único sistema o un conjunto de redes interconectadas donde todos comparten un esquema de identificación común (un identificador y un proceso de asignación por Registro Judicial).
- Dominio de Perfil de Referencias Cruzadas (PRC) que incorpora las siguientes hipótesis:
  a) Acordar un conjunto de políticas que describen cómo se hará la referencia cruzada de los Registros Judiciales a través de los dominios que participan
  b) Acordar un conjunto de procesos para la gestión de estas políticas
  c) Acordar una autoridad administrativa para la gestión de estos procesos y políticas

Los Actores y Transacciones del Perfil PRC de la Plataforma Tecnológica para la Integración de Información, mismos que se encargarán de transmitir la información de identificación de Registros, así como de proporcionar la habilidad de acceder a los identificadores de las listas de referencias, se muestran en la siguiente figura X.10.

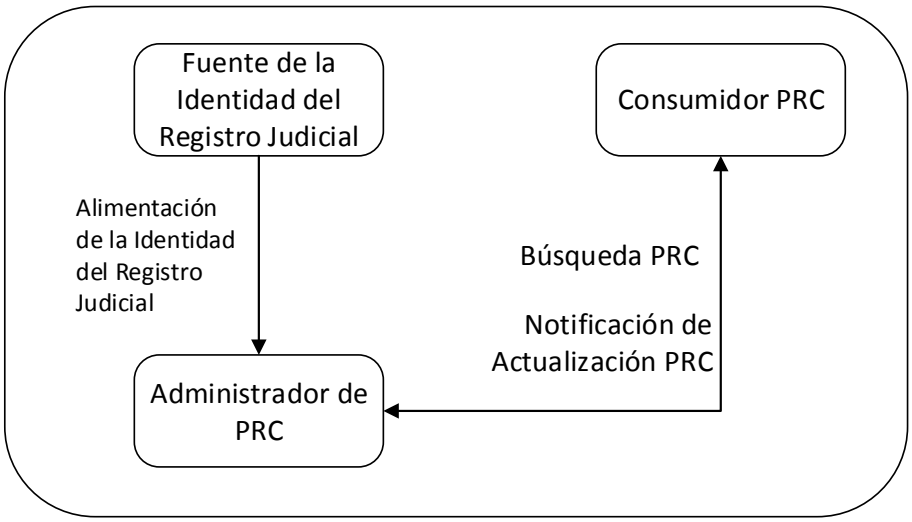


Figura X. 10 Perfil PRC de la Plataforma Tecnológica para la Integración de Información

Actores y transacciones

- Fuente de la Identidad del Registro Judicial
- Administrador PRC
- Consumidor PRC

Transacciones

1. Alimentación de la Identidad del Registro Judicial
2. Búsqueda PRC
3. Notificación de Actualización PRC

Consulta Demográfica del Registro Judicial

La Consulta Demográfica del Registro Judicial (RJDQ) proporcionará la búsqueda de información de diferentes fuentes. Ésta estará basada en un criterio de búsqueda definido por el usuario, el cual regrese, de todas las bases de datos, la información demográfica completa del Registro Judicial.

Los Actores y Transacciones del Perfil RJDQ de la Plataforma Tecnológica para la Integración de Información se muestran en la siguiente figura X.11.

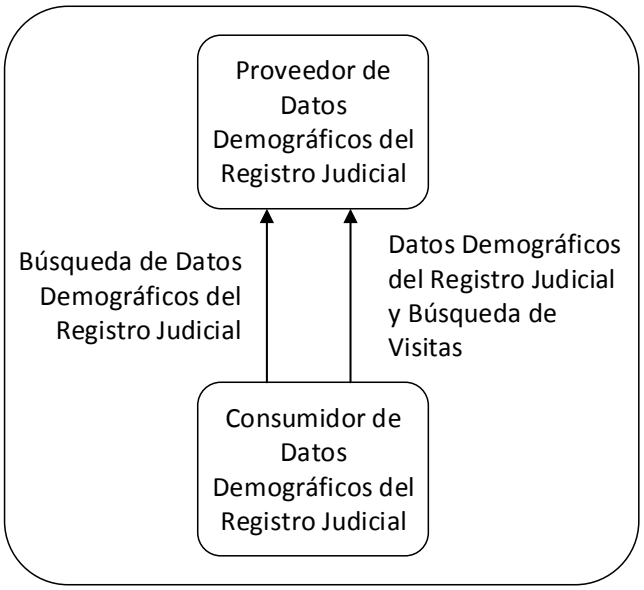


Figura X. 11 Flujo de Datos Demográficos

Actores

El proveedor de Datos Demográficos del Registro Judicial desempeñará las siguientes funciones:

a) Recibe registros judiciales y actualizaciones de mensajes de registro de otros sistemas en el CS que pueden o no representar a los diferentes dominios de Identificación del Registro Judicial. El método por el que el proveedor Datos Demográficos del Registro Judicial obtiene la información actualizada de dichos datos, no es manejado por este perfil.

b) Responde a las búsquedas de información.

Los métodos específicos para la adquisición de información demográfica están fuera del alcance de este perfil, estos tendrán que agregarse como servicios *Web* adicionales.

Es un requisito indispensable que el proveedor de Datos Demográficos del Registro Judicial tenga la información demográfica actualizada.

En todos los casos, el proveedor de Datos Demográficos del Registro Judicial recibe una consulta y envía la solicitud al Consumidor de Datos Demográficos del Registro Judicial, y devuelve la información de los datos de un sólo dominio, que se asocia con la aplicación a la consulta que envía el mensaje.

El Consumidor de Datos Demográficos del Registro Judicialdesempeña la siguiente función:

Solicita información demográfica del Registro Judicial

Los métodos específicos para la adquisición de información demográfica están fuera del alcance de este perfil, estos tendrán que agregarse como servicios *Web* adicionales.

Transacciones

1. Búsqueda de datos demográficos del Registro Judicial
2. Datos demográficos del Registro Judicial y Búsquedas de Visitas

Consistencia del Tiempo

La Consistencia del Tiempo asegura que los relojes y '*time stamps*' de los servidores de la red de la Plataforma Tecnológica para la Integración de Información estén sincronizados.

Este Perfil proporciona un mecanismo que asegura que los registros de tiempo en los distintos sistemas sean coherentes. También permite asegurar que las diferencias en el registro de tiempo de los sistemas que funcionan de forma integrada sean inferiores a 1 segundo.

Los Actores y Transacciones de la Plataforma se muestran en la siguiente figura X.12.

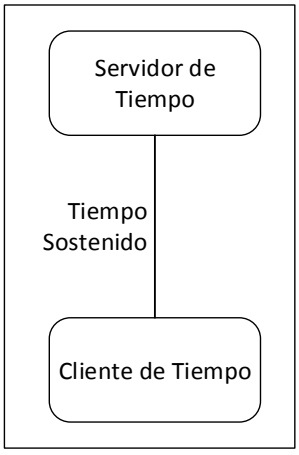


Figura X. 12 Servidor de Tiempo

Actores

- Servidor de Tiempo.- Provee servicios de tiempo como NTP a clientes de tiempo. Debe estar directamente sincronizado con un reloj maestro UTC o sincronizado por un grupo de servidores de tiempo.
- Cliente de Tiempo.- Establece la sincronización del tiempo con el o los servidores de tiempo utilizando el protocolo NTP y los algoritmos NTP o SNTP. Mantiene el reloj de sistema del servidor sincronizado con el Servidor de Tiempo.

Los estándares y transacciones principales en las que se basa son:

- *Network Time Protocol* (NTP) *defined in* RFC 1305 (disponibleenhttps://tools.ietf.org/html/rfc1305)
- SNTP: Protocolo Simple de Hora de Red (en inglés *Simple Network Time Protocol*).

Transacciones

1. Tiempo Sostenido, Transacciones de NTP usadas para sostener la sincronización del tiempo en la Plataforma.

Estructura

La Capa de Gestión es la encargada de proporcionar (en tiempo real) información sobre el estado y los resultados de las operaciones, procesos y transacciones que componen la plataforma completa. La información proporcionada por la Capa de Gestión debe permitir:

1) Monitorear el comportamiento y fallas de la plataforma
2) Monitorear el flujo de mensajes
3) Encontrar cuellos de botella
4) Correlacionar eventos
5) Mejorar el proceso de toma de decisiones
6) Optimizar orquestaciones (de la Capa de Negocio)
7) Monitorear KPI (*Key Performance Indicators*)

8) Verificar el cumplimiento instantáneo de SLA y OLA

En el caso específico de la Plataforma, la Capa de Gestión debe estar basada en el Marco de Administración del Desempeño de Aplicaciones (*Application Performance Management Framework* en inglés), trabajar con sistemas basados en SOA (es decir, capaz de monitorear mensajes SOAP y XML y *Web Services* basados en Java, .net o cualquier plataforma de ejecución y/o desarrollo que sea capaz de ejecutar *Web Services*) y debe operar sobre recomendaciones y estándares de los organismos W3C, OASIS (Organización para el Avance de Estándares de Información Estructurada) o cualquier otro organismo involucrado en el desarrollo y estandarización de SOA.

La información obtenida con la Capa de Gestión debe mostrarse a través de una interfaz gráfica a la que se tiene acceso utilizando un *Web Browser*. Además, debe estar disponible en una base de datos para su análisis, utilizando herramientas de *Business Intelligence* (BI), *Corporate Performance Management* (CPM), entre otras.

Funcionamiento

La Capa de Gestión es la que debe permitir tener una visión global y/o específica del estado y resultado de las operaciones, procesos y transacciones que ocurren dentro y que conforman la Plataforma Tecnológica para la Integración de información del CS. Esta Capa debe permitir detectar eventos, en tiempo real, provenientes del resto de la plataforma. De estos eventos se obtiene la información necesaria para el monitoreo de las operaciones, procesos y transacciones. El Marco de Administración del Desempeño de Aplicaciones debe ser capaz de procesar grandes volúmenes transaccionales para manejar el cuantioso número de eventos generados en la Capa de Gestión.

La Capa de Gestión debe permitir: verificar en tiempo real el estado de la plataforma desde distintos puntos de vista, es decir, tener varias interfaces con distintos grados de detalles para diferentes entidades que monitorean la plataforma. La administración y configuración del Marco de Administración del Desempeño de Aplicaciones se hace usando una interfaz gráfica.

La arquitectura de la Capa de Gestión debe ser escalable y distribuida. Esto es para que la arquitectura de la Plataforma sea abierta, configurable y permita que su tamaño y complejidad se incrementen, dependiendo de las características y las necesidades de procesamiento de la plataforma misma.

La Capa de Gestión debe ser capaz de correlacionar eventos. La correlación es configurada (creada), modificada o eliminada por el usuario (usando una interfaz gráfica). El resultado de esta correlación puede ser un nuevo evento, una notificación

o una acción. Además, con base en los eventos, aun cuando no sean correlacionados o resultados de una correlación, se deben poder generar notificaciones y/o acciones en respuesta a eventos generados.

Las características con las que debe contar la Capa de Gestión de la Plataforma son las siguientes:

1) La Capa de Gestión debe estar basada en un Marco de Administración del Desempeño de Aplicaciones.
2) La Capa de Gestión debe ser capaz de soportar la Arquitectura Orientada a Servicios (SOA).
3) La Capa de Gestión debe poder interactuar con *Web Services* creados en cualquier tecnología, siempre y cuando cumplan con los estándares del W3C.
4) La información proveniente de la PTII debe ser recibida, procesada, mostrada y almacenada en tiempo real.
5) La Arquitectura de la Capa de Gestión debe ser escalable y distribuida.
6) La Capa de Gestión debe ser capaz de mostrar la información obtenida a través de una interfaz gráfica. Esta información debe ser mostrada en forma gráfica como un conjunto de *dashboards* o en forma de texto como reportes en texto. El acceso a esta interfaz debe ser a través de un *Web Browser*.
7) La información obtenida por la Capa de Gestión debe ser almacenada en una base de datos relacional. Debe poder tenerse acceso a la base de datos para su posible uso con herramientas de *Business Intelligence* y/o herramientas de *Corporate Performance Management*. Por lo tanto, la estructura de la base de datos donde se almacena la información de Administración del Desempeño de Aplicaciones debe ser pública.
8) La interfaz de administración y configuración debe ser completamente gráfica y el acceso a ella debe ser a través de un *Web Browser*.
9) Debe ser posible ejecutar operaciones dentro de la Capa de Gestión para poder crear datos derivados como promedios, KPI, y establecer las SLA.
10) Debe ser posible monitorear datos primitivos y derivados utilizando gráficas y reportes de texto en *dashboards* a través de una interfaz gráfica de monitoreo. El acceso a esta interfaz debe hacerse utilizando un *Web Browser*.
11) Es indispensable que el CS tenga acceso a la interfaz gráfica de monitoreo *Web*.

12) Debe ser posible crear notificaciones y acciones configurables por el usuario y ejecutables a partir de la existencia de cierto evento.

13) La Capa de Gestión debe ser capaz de correlacionar eventos.

14) Debe ser posible establecer procesos de correlación de eventos y generar a partir de ellos nuevos eventos, notificaciones y/o acciones configurables por el usuario.

15) Debe existir una interfaz gráfica para la creación de correlaciones de eventos. El acceso a la interfaz de correlación debe ser a través de un *Web Browser*.

5.10.8.6 Repositorio de Datos

Como condiciones generales, los repositorios de datos deben contar con una sola base de datos por cada dominio en producción. El repositorio se debe mantener en la última versión estable liberada por el fabricante.

El acceso a los registros de la base de datos debe ser exclusivamente por las aplicaciones que componen las diferentes capas de la solución, no permitiendo la consulta directa de información por parte de usuarios o administradores de la base de datos directamente. Se debe bloquear y documentar cualquier intento de modificar o extraer información de dichos repositorios

La confidencialidad de los datos contenidos en dichos repositorios, se debe mantener mediante un Sistema de Gestión de Seguridad de la Información (SGSI).

5.10.8.7 Centro de Datos

El lugar físico donde se alojen los equipos (o equipo) sobre los que se ejecuta la Plataforma de Tecnología para la Integración de Información (PTII) debe cumplir con ciertos requerimientos, mismos que serán definidos por el CS para poder garantizar que los equipos, aplicaciones y datos estén seguros y tengan sistemas de protección y respaldo físico.

Además, es indispensable que el proveedor cuente con sistemas y métodos de un Plan de Continuidad del Negocio (en inglés *Business Continuity Plan* "BCP") y un Plan de Recuperación ante Desastres (en inglés *Disaster Recovery Plan* "DRP") que garanticen que la PTII cumplirá con los Acuerdos de los Niveles de Servicio (SLA por sus siglas en inglés: *Service Level Agreement*).

5.10.8.8 Seguridad

Dependiendo de los requerimientos del Complejo de Seguridad se debe cumplir lo indicado en el apartado 5.2.6.

5.10.8.9 Requerimientos de Gestión

La gestión de los equipos es una de las necesidades principales de las personas que laboran en los CS. Es necesario tener un sistema de gestión de fallas que informe de fallas en los componentes de *hardware* y/o sistemas operativos de la plataforma. El sistema de gestión de fallas con que cuente el centro de datos debe ser capaz de recibir y procesar eventos de dos modalidades:

1) Recepción de alarmas (traps) del Protocolo Simple de Administración de Red (en inglés *Simple Network Management Protocol* "SNMP").
2) Utilización de agentes propietarios de algún *software* de gestión de sistemas.

Tanto los agentes SNMP, como los agentes propietarios, deben estar instalados sobre los equipos donde se ejecuta la PTII.

La interfaz de visualización del sistema de gestión debe ser gráfica y el CS debe poder tener acceso a ella, en cualquier momento, a través de un cliente *Web*.

El componente de gestión del centro de datos debe contar con una interfaz gráfica *Web* de monitoreo que despliegue, en forma de reportes de texto y/o gráficas, el comportamiento de cada uno de los componentes que intervengan en la definición de los SLA. El CS debe tener acceso a la herramienta de gestión del centro de datos utilizando la interfaz *Web* de monitoreo.

5.10.8.10 Estimaciones de Carga

Tomando como base la diversidad de las bases de datos que se manejan en los Complejos de Seguridad, los volúmenes transaccionales que deben ser atendidos por la plataforma tecnológica para la atención del servicio deben ajustarse al punto X.10.7 (cumpliendo con los Acuerdos de los Niveles de Servicio (SLA)) y al punto 5.9.4.4. (Arquitectura para ambientes de alta demanda de cómputo). De los Niveles de Servicio (SLA) en entornos *Web* se recomienda cumplir con al menos las siguientes características:

- Principalmente orientados al usuario
- Límite superior del tiempo de respuesta. El tiempo de respuesta de la transacción debe ser menor a 6 segundos
- Productividad mínima por el servidor *Web*. El sitio estará operativo al menos el 99.999% del tiempo.
- Porcentaje de transacciones que han de tener un tiempo de respuesta menor o igual que un cierto valor. Al menos el 95% de las transacciones deben tener un tiempo de respuesta inferior a 2 segundos.

Para definir la capacidad adecuada del sistema basado en *Web* se recomienda al menos tomar en cuenta:

- Compromisos de Nivel de Servicio
- Estándares y Tecnologías Adoptadas
- Restricciones de costo
- Cada CS establecerá una metodología de *planeación de capacidad* tomando como referencia el número de bases de datos que se manejen.

Adicionalmente se recomienda tomar en cuenta las métricas de dimensionamiento, las cuales incluyen cantidad de usuarios, volúmenes transaccionales por tipo y frecuencia y volumen de datos, entre otros.

Para realizar una estimación de carga de los volúmenes transaccionales se realizará un ejemplo que podrá aplicarse a las diferentes bases de datos de los CS. Tomando como referencia 100 usuarios con un porcentaje de concurrencia del 28% = 28 usuarios concurrentes por cada 6 horas. Y una base de datos con 5 millones de registros, cada registro con 250 campos y cada campo almacena 10 kB. Cada transacción tendrá una longitud de:

Trans= No. de registros x longitud de campo= 250 x 125 kB = 31,250 kB

Para estimar la carga de trabajo:

Carga de trabajo = Trans x usuarios concurrentes = 31,250 kB x 28 = 875,000 kB

La carga de trabajo por año será 875,000 kB x 4 x 365 = 1,277,500,000 kB

Tomando una variación del 13 % del total de transacciones al año se obtiene

Variación = 1,277,500,000 kB *0.13 = 166,075,000 kB

Máximo = 1,277,500,000 kB + 166,075,000 kB = 1,443,575,000 kB

Mínimo = 1,277,500,000 kB – 166,075,000 kB= 1,111,425,000 kB

Realizando una proyección de crecimiento del 10 % anual se obtiene 1,277,500,000 kB x 0.1 = 127,750,000 kB para el año 2. Para el año 3 se tendrá un crecimiento de 157,132,500 kB. Los volúmenes transaccionales que se estiman deben ser atendidos por la plataforma tecnológica para la atención del servicio serán con base en la siguiente Tabla x.6

Tabla X. 6 Estimaciones de Carga

	Año 1	**Año 2**	**Año 3**
Máximo en kB	1,443,575,000	1,571,325,000	1,728,457,500
Mínimo en kB	1,111,425,000	1,239,175,000	1,396,307,500

Finalmente, para la evaluación de las bases de datos existentes en los CS se recomienda aplicar documento “Nueva Metodología para la Evaluación de las Bases de Datos” donde se establece que a través de la Metodología de Evaluación las dependencias que aportan información para el Sistema Nacional de Seguridad Pública (SNSP), contarán con un solo procedimiento de evaluación que les proporcionará mayores elementos para identificar áreas de mejora en sus bases de datos, así como protocolos para generar y administrar información, en un contexto de transparencia que les permita los indicadores por medio de los cuales se llevará a cabo el proceso de evaluación.

5.10.8.11 Flujos de Transacciones

La comunicación e interacción de las Capas debe efectuarse a través de *Web Services*. Cualquier orquestación debe ser creada utilizando la Capa de Negocio que definirá las reglas de los procesos mediante Lenguaje de Ejecución de Procesos de Negocio con Servicios *Web* (WS-BPEL por sus siglas en inglés: *Web Services Bussines Process Execution Language*). De esta forma, es posible establecer cualquier interacción entre los servicios de una forma centralizada y fácilmente administrable.

5.10.8.11.1 Integración Externa

La PTII cuenta con un registro UDDI (su disposición es opcional y el CS define su implementación o no de acuerdo a sus necesidades y normatividad) donde los Servicios proporcionados por la PTII están registrados, de modo que puedan ser usados por las entidades autorizadas y habilitadas para su uso.

La conexión entre la Capa de Conexión e Integración y entidades externas se debe establecer utilizando como protocolo de transporte SOAP, que es un protocolo ligero orientado al intercambio de información (en forma de mensajes) en ambientes descentralizados/distribuidos.

Utiliza tecnología XML para crear un sistema de mensajes que puedan ser intercambiados independientemente de los protocolos que subyacen. SOAP es altamente extensible y permite crear extensiones para proporcionarle funcionalidades adicionales.

Es necesario mencionar que cualquier *Web Service* que requiera utilizar los Servicios contenidos en la Capa de Conexión e Integración debe, además de utilizar SOAP, implementar las recomendaciones mencionadas en la sección de este documento correspondiente a la Capa de Conexión e Integración.

5.10.8.11.2 Integración Interna

Los servicios proporcionados por la PTII se pueden visualizar como secuencias de servicios e intercambios de mensajes.
La integración entre las Capas de Datos y la Capa de Conexión e Integración se hace utilizando los Servicios de orquestación proporcionados por la Capa de Negocios.
Al utilizar la arquitectura SOA se podrá crear, modificar y/o eliminar Servicios y orquestaciones, agilizando cambios o adiciones a la funcionalidad proporcionada por la PTII. Esta capacidad de aumentar, modificar y/o eliminar funcionalidad a través de Servicios y orquestaciones nuevas o modificadas, debe existir en la PTII.
Para poder dar cumplimiento a la característica descrita en el párrafo anterior, la PTII está basada en recomendaciones estándares y cumple, en cada uno de los componentes que están describiéndose en este apartado (Capa de Conexión e Integración, Capa de Datos, Capa de Negocio y Capa de Infraestructura), con las recomendaciones aplicables del W3C y OASIS.

5.10.8.11.3 Interacción a Nivel Servicios

En esta sección se describe el flujo de mensajes en la PTII. La interacción entre las Capas puede ilustrarse a través de diagramas de flujo de intercambio de mensajes entre los Servicios que la conforman.
Estos mensajes son básicos para su funcionamiento y son implementados dentro de la plataforma.
Las interacciones entre los Servicios deben ser almacenadas en una bitácora, incluyendo los mensajes y el contenido de los mismos. La interacción y los mensajes deben permanecer dentro de la PTII por un plazo no menor a tres meses.
Los procesos (descripciones en texto) y diagramas mostrados en esta sección muestran la funcionalidad requerida de la PTII.

1. Registro Judicial

El Registro Judicial es indispensable para que la PTII se entere de que se ha realizado un registro en algún CS o alguna otra instancia municipal, estatal o federal con alguna base de datos que comparta información.

Operación exitosa

A continuación, en la figura X.13 se muestra el flujo del proceso de registro, Operación exitosa.

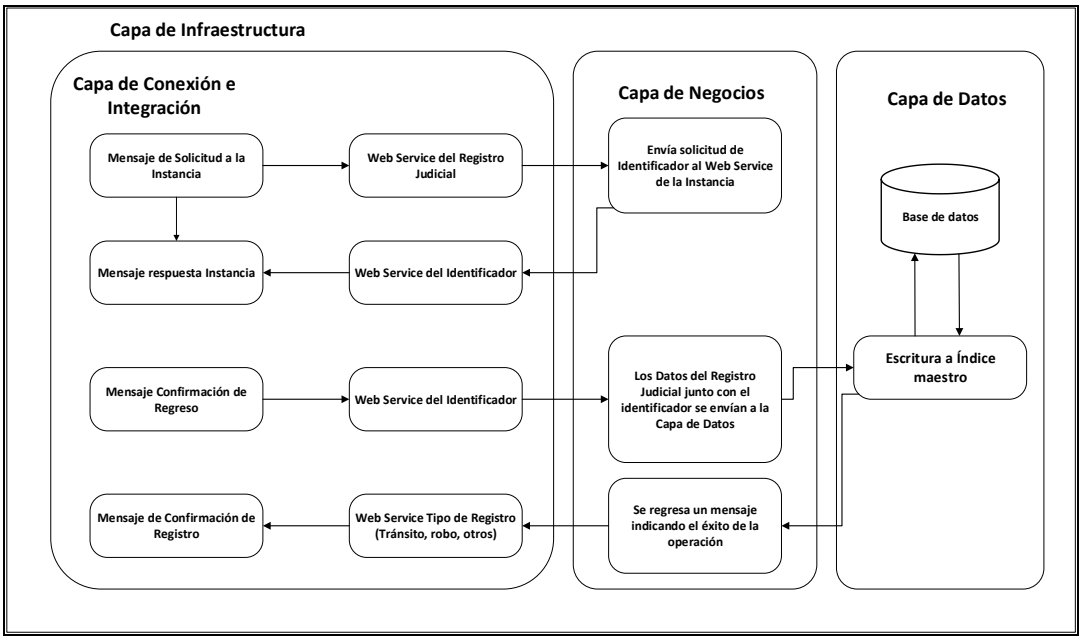


Figura X. 13 Diagrama de flujo del proceso de registro, operación exitosa

1) El servicio del Registro Judicial (que está alojado en la Capa de Conexión e Integración) recibe un mensaje de solicitud a la instancia. Un mensaje es enviado a la orquestación adecuada dentro de la Capa de Negocio.
2) La orquestación indica la necesidad de obtener y/o verificar el identificador del Registro Judicial. La orquestación solicita los servicios del *Web Service* del identificador (que está alojado en la Capa de Conexión e Integración). Este servicio envía entonces un mensaje solicitando el identificador al *Web Service* de la instancia.
3) Ante la llamada del *Web Service* de CS o alguna otra instancia municipal, estatal o federal con alguna base de datos que comparta información, existen dos escenarios que pueden presentarse:
    a. El *Web Service* del CS o alguna otra instancia municipal, estatal o federal con alguna base de datos que comparta información, regresa al *Web Service* de Identificador (contenido dentro de la Capa de Conexión e Integración) un mensaje que contiene el identificador del registro judicial; se hace cualquier proceso necesario y se envía un mensaje, ya con el identificador, a la orquestación de WS-BPEL.
    b. Si después de un tiempo de espera T1 (tiempo de espera configurado al inicio de la operación de la PTII, según los parámetros establecidos en los SLA) el *Web Service* de la instancia no regresa ningún mensaje, el *Web Service* del identificador genera una excepción y envía un mensaje indicando esta situación a la orquestación de WS-BPEL.
4) La orquestación envía un mensaje de escritura a la Capa de Datos e inicia un temporizador de espera T2 (que debe ser definido por el operador de la PTII).
5) Dentro del tiempo de espera T2, la Capa de Datos regresa un mensaje a la Capa de Negocio (la orquestación) indicando que el registro se ha escrito exitosamente.
6) La orquestación usa los servicios del *Web Service* del Registro Judicial para regresar un mensaje indicando el éxito del registro.
7)

Operación fallida (no se puede escribir al Índice Maestro)

El flujo del proceso de registro, Operación Fallida, muestra que la PTII no pudo escribir al Índice Maestro algún registro en algún CS o en alguna otra instancia municipal, estatal o federal, con alguna base de datos que comparta información.

A continuación, en la figura X.14, se muestra el flujo del proceso de registro, Operación fallida.

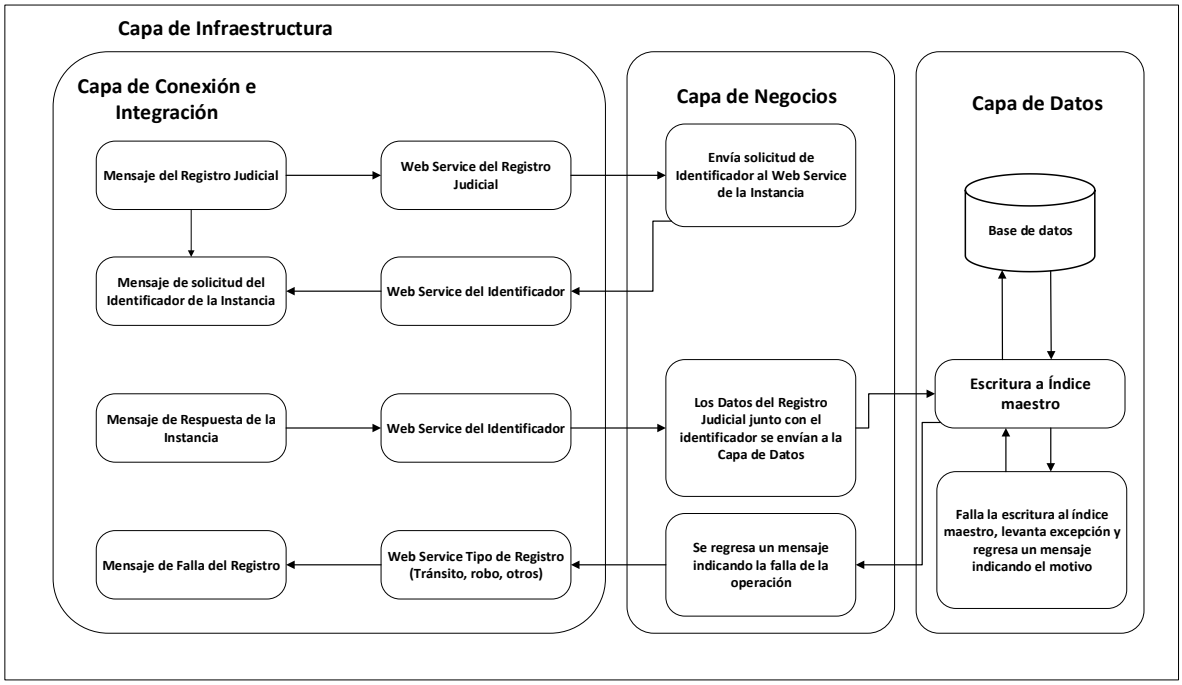


Figura X. 14 Diagrama de flujo del proceso de registro, operación fallida (no se puede escribir al índice maestro)

1) El servicio de Registro Judicial (que está alojado en la Capa de Conexión e integración) recibe un mensaje de solicitud a la instancia. Un mensaje es enviado a la orquestación adecuada dentro de la Capa de Negocio.
2) La orquestación creada indica la necesidad de obtener y/o verificar el identificador del Registro Judicial. La orquestación solicita los servicios del *Web Service* del identificador (que está alojado en la Capa de Conexión e Integración). Este servicio envía entonces un mensaje solicitando el identificador al *Web Service* de la instancia.
3) Ante la llamada del *Web Service* del CS o alguna otra instancia municipal, estatal o federal con alguna base de datos que comparta información, existen dos escenarios que pueden presentarse:
    a. El *Web Service* del CS o alguna otra instancia municipal, estatal o federal con alguna base de datos que comparta información, regresa al *Web Service* de Identificador (contenido dentro de la Capa de Conexión e Integración) un mensaje que contiene el identificador del registro judicial, se hace cualquier proceso necesario y se envía un mensaje, ya con el identificador, a la orquestación de WS-BPEL.

b. Si después de un tiempo de espera T1 (tiempo de espera configurado al inicio de la operación de la PTII, según los parámetros establecidos en los SLA) el *Web Service* de la Instancia no regresa ningún mensaje, el *Web Service* del identificador genera una excepción y envía un mensaje indicando esta situación a la orquestación de WS-BPEL.

4) La orquestación envía un mensaje de escritura a la Capa de Datos e inicia un temporizador de espera T2 (el tiempo de espera debe ser configurado al inicio de la operación de la PTII; sin embargo este tiempo debe ser optimizado durante la operación; al establecer y optimizar este tiempo es necesario considerar los parámetros establecidos en los SLA).
5) Cuando la escritura falla, se presenta el siguiente escenario:
   a. La Capa de Datos está disponible pero no puede escribir el registro. La Capa de Datos genera una excepción (que indica el motivo de la falla). La Capa de Datos envía un mensaje de regreso a la orquestación indicando el motivo de la falla. La Capa de Datos debe enviar el mensaje antes de que transcurra el tiempo T2.
6) Bajo este escenario, la Capa de Negocio utiliza los servicios del *Web Service* del Registro Judicial para regresar un mensaje indicando que el registro ha fallado y la causa de la falla.

Operación fallida (la Capa de Datos no está disponible)

El flujo del proceso de registro, Operación fallida, la Capa de Datos no está disponible, muestra que la Capa de Datos no está disponible para realizar un determinado registro en algún CS o alguna otra instancia municipal, estatal o federal con base de datos que comparta información.

A continuación, en la figura X.15 se muestra el flujo del proceso de registro, Operación fallida (la Capa de Datos no está disponible).

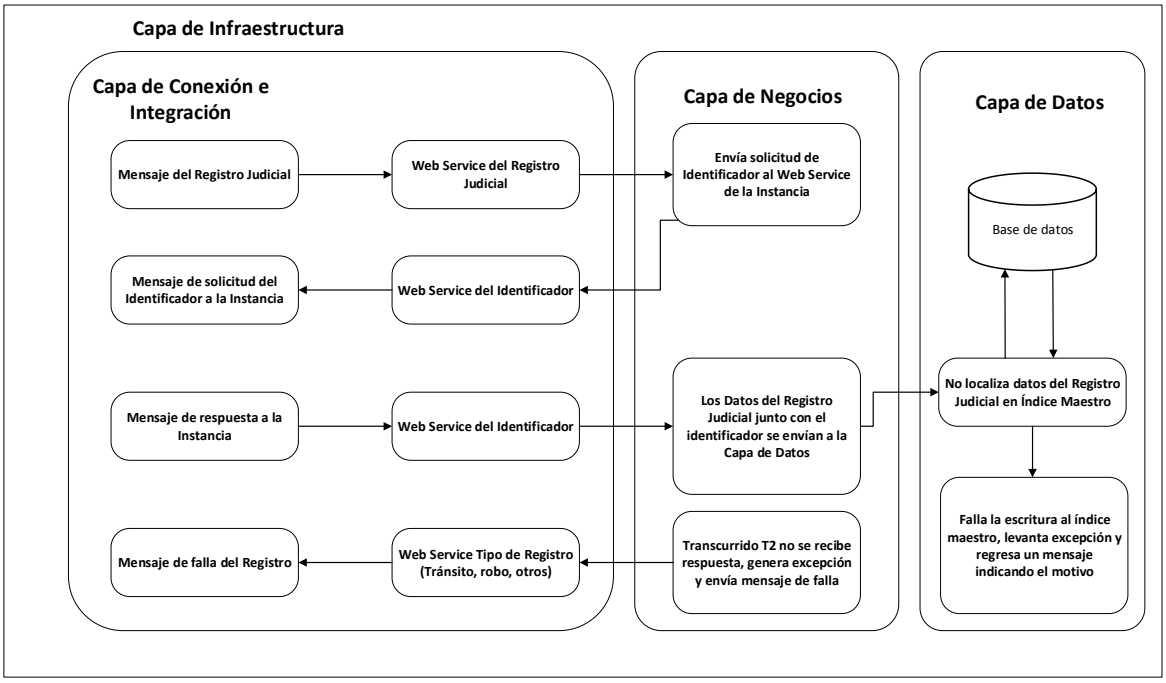


Figura X. 15 Diagrama de flujo del proceso de registro, operación fallida (la Capa de Datos no está disponible)

1) El servicio de Registro Judicial (que está alojado en la Capa de Conexión e Integración) recibe un mensaje de solicitud a la instancia. Un mensaje es enviado a la orquestación adecuada dentro de la Capa de Negocio.
2) La orquestación creada indica la necesidad de obtener y/o verificar el identificador del Registro Judicial a través del servicio proporcionado para este efecto por el *Web Service* de la instancia. La orquestación solicita los servicios del *Web Service* del identificador (que está alojado en la Capa de Conexión e Integración). Este servicio envía entonces un mensaje solicitando el identificador al *Web Service* de la instancia.
3) Ante la llamada del *Web Service* de CS o alguna otra instancia municipal, estatal o federal con alguna base de datos que comparta información, existen dos escenarios que pueden presentarse:
    a. El *Web Service* del CS o alguna otra instancia municipal, estatal o federal con alguna base de datos que comparta información, regresa al *Web Service* de Identificador (contenido dentro de la Capa de Conexión e Integración) un mensaje que contiene el identificador del registro judicial, se hace cualquier proceso necesario y se envía un mensaje, ya con el identificador, a la orquestación de WS-BPEL.

b. Si después de un tiempo de espera T1 (tiempo de espera configurado al inicio de la operación de la PTII, según los parámetros establecidos en los SLA) el *Web Service* de la Instancia no regresa ningún mensaje, el *Web Service* del identificador genera una excepción y envía un mensaje indicando esta situación a la orquestación de WS-BPEL.

4) La orquestación envía un mensaje de escritura a la Capa de Datos e inicia un temporizador de espera T2 (el tiempo de espera debe ser configurado al inicio de la operación de la PTII; sin embargo este tiempo debe ser optimizado durante la operación; al establecer y optimizar este tiempo es necesario considerar los parámetros establecidos en los SLA).
5) Si después de que ha transcurrido el tiempo de espera T2, la orquestación (contenida dentro de la Capa de Negocios) no recibe un mensaje proveniente de la Capa de Datos, se genera una excepción que indica que la orquestación debe enviar un mensaje al *Web Service* de registro judicial, indicando que la Capa de Datos está fuera de servicio.
6) El *Web Service* de Registro judicial envía un mensaje indicando al *Web Service* que solicitó el servicio que la Capa de Datos está fuera de servicio.

Operación fallida (el *Web Service* de Registro Judicial no está disponible)

Si un *Web Service*, perteneciente a una Instancia, solicita el Servicio de registro al *Web Service* de Registro Judicial y este último no está disponible, no hay forma de que se regrese un mensaje de error (un mensaje de error que indique la no disponibilidad del *Web Service* de Registro judicial), por lo tanto es necesario que el *Web Service* que solicita el servicio de Registro judicial sea capaz de manejar las excepciones generadas por la falta de disponibilidad del *Web Service* de Registro Judicial.

Operación fallida (la Capa de Negocio no puede atender la petición)

El flujo del proceso de registro, Operación fallida, la Capa de Negocio no puede atender la petición, muestra que la Capa de Negocio no está disponible para realizar un determinado registro en un CS o alguna otra instancia municipal, estatal o federal con alguna base de datos que comparta información.
A continuación, en la figura X.16 se muestra el flujo del proceso de registro, Operación fallida (la Capa de Negocio no puede atender la petición).

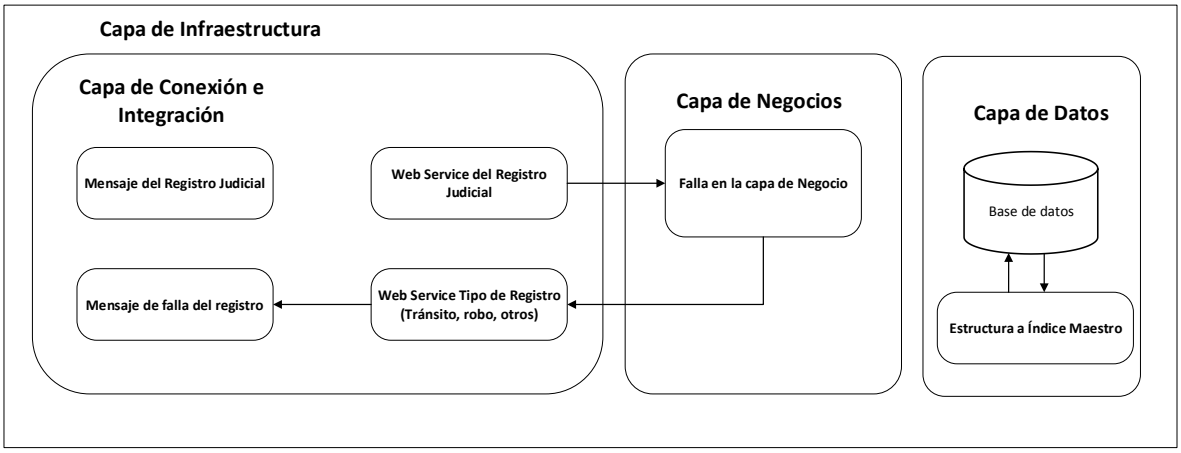


Figura X. 16 Diagrama de flujo del proceso de registro, operación fallida (la Capa de Negocio no puede atender la petición)

1) El servicio de Registro Judicial (que está alojado en la Capa de Conexión e Integración) recibe un mensaje de solicitud a la instancia. Un mensaje es enviado a la orquestación adecuada dentro de la Capa de Negocio.
2) En caso de falla de la Capa de Negocio puede presentarse el siguiente escenario:
   a. La Capa de Negocio no puede procesar la solicitud proveniente de la Capa de Conexión e Integración, levanta una excepción y regresa un mensaje (a la Capa de Conexión e Integración) indicando el motivo de la falla.
3) La Capa de Conexión e Integración utiliza el servicio de Registro Judicial para regresar un mensaje al *Web Service* que le solicitó el registro indicándole el motivo de la falla.

Operación fallida (falla en la Capa de Negocio)

El flujo del proceso de registro, Operación fallida, falla en la Capa de Negocio, muestra una falla en la Capa de Negocio para realizar un determinado registro en un CS o alguna otra instancia municipal, estatal o federal con alguna base de datos que comparta información.
A continuación, en la figura X.17 se muestra el flujo del proceso de registro, Operación fallida (falla en la Capa de Negocio).

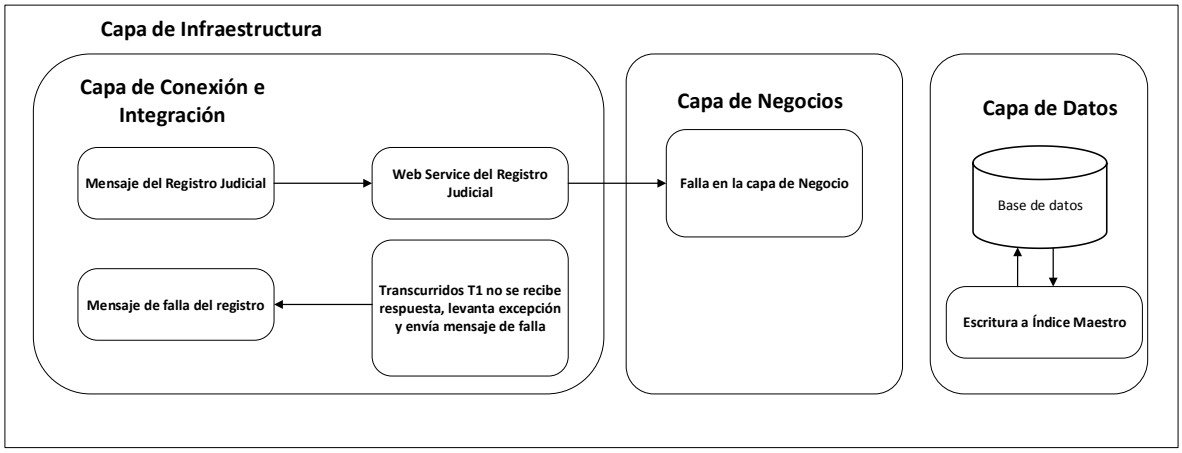


Figura X. 17 Diagrama de flujo del proceso de registro, operación fallida (falla en la Capa de Negocio)

1) El servicio de Registro Judicial (que está alojado en la Capa de Conexión e Integración) recibe un mensaje de solicitud a la instancia. Un mensaje es enviado a la orquestación adecuada dentro de la Capa de Negocio.
2) En caso de falla de la Capa de Negocio puede presentarse el siguiente escenario:
    a. Si después de un tiempo de espera T1 (tiempo de espera configurado al inicio de la operación de la PTII, según los parámetros establecidos en los SLA), el Servicio de Registro Judicial no recibe ningún mensaje de la Capa de Negocio, se genera una excepción que indica la falla.
    b. La Capa de Negocio no puede procesar la solicitud proveniente de la Capa de Conexión e Integración, levanta una excepción y regresa un mensaje (a la Capa de Conexión e Integración) indicando el motivo de la falla.
3) La Capa de Conexión e Integración utiliza el servicio de Registro Judicial para regresar un mensaje al *Web Service* que le solicitó el registro, indicándole el motivo de la falla.

5.10.8.12 Actualización de Registro Judicial

La actualización de los Registros Judiciales tiene como objetivo mantener la información contenida dentro del Índice Maestro consistente con la información real de CS o alguna otra instancia municipal, estatal o federal con alguna base de datos que comparta información.

Operación exitosa

El flujo del proceso de actualización de un registro, Operación exitosa, muestra que se pudo realizar la actualización de un determinado registro en un CS o alguna otra instancia municipal, estatal o federal con alguna base de datos que comparta información.
A continuación, en la figura X.18 se muestra el flujo del proceso de actualización de registro, Operación exitosa.

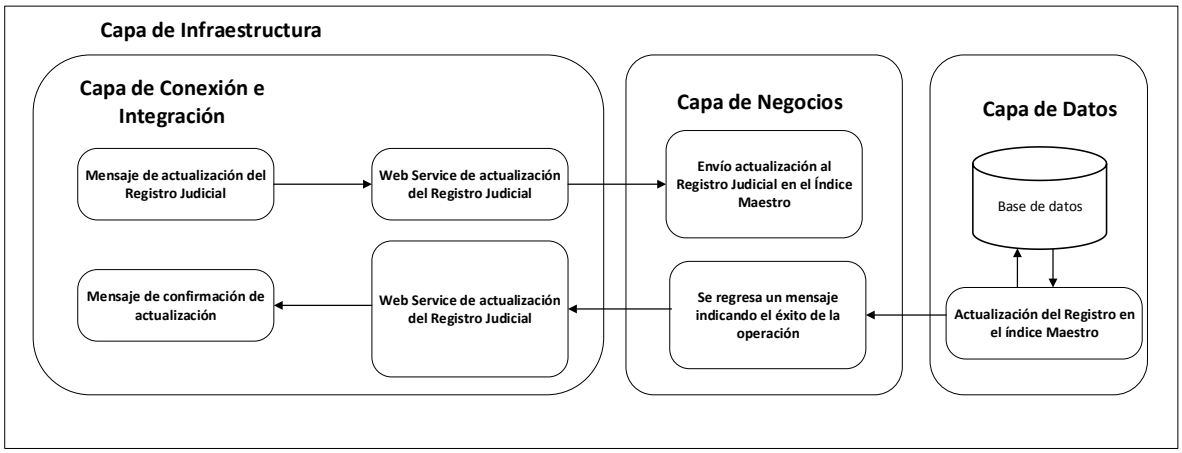


Figura X. 18 Diagrama de flujo del proceso de actualización de un registro, operación exitosa

1) El servicio de Actualización del Registro Judicial (que está alojado en la Capa de Conexión e Integración) recibe un mensaje de Actualización de un Registro Judicial. Un mensaje es enviado a la orquestación adecuada dentro de la Capa de Negocio.
2) La orquestación envía un mensaje de actualización a la Capa de Datos e inicia un temporizador de espera T1 (tiempo de espera configurado al inicio de la operación de la PTII, según los parámetros establecidos en los SLA).
3) Dentro del tiempo de espera T1, la Capa de Datos regresa un mensaje a la Capa de Negocio (la orquestación) indicando que el registro se ha escrito exitosamente.
4) La orquestación usa los servicios del *Web Service* de Actualización de Registro Judicial para regresar un mensaje indicando el éxito de la operación.

Operación fallida (no se puede escribir al Índice Maestro)

El flujo del proceso de actualización de un registro, Operación fallida, no se puede escribir al Índice Maestro, muestra que no se pudo realizar la actualización de un determinado registro en un CS o alguna otra instancia municipal, estatal o federal con alguna base de datos que comparta información.

A continuación, en la figura X.19 se muestra el flujo del proceso de actualización de registro, Operación fallida (no se puede escribir al Índice Maestro).

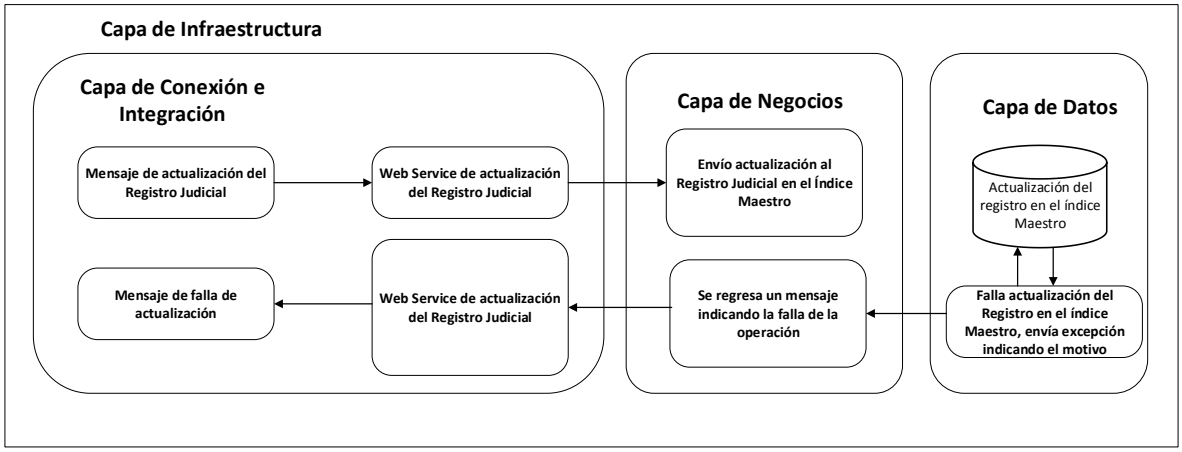


Figura X. 19 Diagrama de flujo del proceso de actualización de un registro, operación fallida (no se puede escribir al Índice Maestro)

1) El servicio de Actualización de Registro Judicial (que está alojado en la Capa de Conexión e Integración) recibe un mensaje de Actualización de Registro Judicial. Un mensaje es enviado a la orquestación adecuada dentro de la Capa de Negocio.
2) La orquestación envía un mensaje de actualización a la Capa de Datos e inicia un temporizador de espera T1 (tiempo de espera configurado al inicio de la operación de la PTII, según los parámetros establecidos en los SLA).
3) Cuando la actualización falla, se presenta el siguiente escenario:
    a. La Capa de Datos está disponible pero no puede actualizar el registro. La Capa de Datos genera una excepción (que indica el motivo de la falla). La Capa de Datos envía un mensaje de regreso a la orquestación indicando el motivo de la falla. La Capa de Datos debe enviar el mensaje antes de que transcurra el tiempo T1.

4) Bajo este escenario, la Capa de Negocio utiliza los servicios del *Web Service* de Actualización de Registro Judicial para regresar un mensaje indicando que el registro ha fallado y la causa de la falla.

Operación fallida (la Capa de Datos no está disponible)

El flujo del proceso de actualización de un registro, Operación fallida, la Capa de Datos no está disponible, muestra que no se pudo realizar la actualización de un determinado registro en un CS o alguna otra instancia municipal, estatal o federal con alguna base de datos que comparta información.
A continuación, en la figura X.20 se muestra el flujo del proceso de actualización de registro, Operación fallida (la Capa de Datos no está disponible).

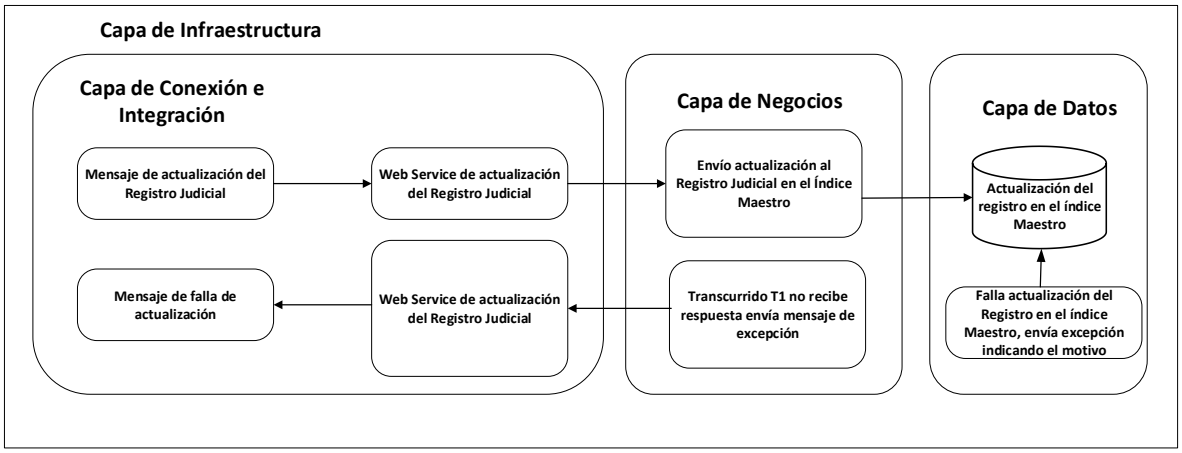


Figura X. 20 Diagrama de flujo del proceso de actualización de un registro, operación fallida (la Capa de Datos no está disponible)

1) El servicio de Actualización de Registro Judicial (que está alojado en la Capa de Conexión e Integración) recibe un mensaje de Actualización de un Registro Judicial. Un mensaje es enviado a la orquestación adecuada dentro de la Capa de Negocio.
2) La orquestación envía un mensaje de actualización a la Capa de Datos e inicia un temporizador de espera T1 (tiempo de espera configurado al inicio de la operación de la PTII, según los parámetros establecidos en los SLA).
3) Si después de que ha transcurrido el tiempo de espera T1, la orquestación (contenida dentro de la Capa de Negocio) no recibe un mensaje proveniente

de la Capa de Datos, se genera una excepción que indica que la orquestación debe enviar un mensaje al *Web Service* de Actualización de Registro Judicial, indicando que la Capa de Datos está fuera de servicio.

4) El *Web Service* de Actualización de Registro Judicial envía un mensaje indicando al *Web Service* que solicitó el servicio que la Capa de Datos está fuera de servicio.

Operación fallida (el *Web Service* de actualización de un registro no está disponible)

Si un *Web Service*, perteneciente a un CS o a alguna otra instancia municipal, estatal o federal con alguna base de datos que comparta información, solicita el Servicio de actualización al *Web Service* de Actualización del Registro Judicial y este último no está disponible, no hay forma de que se regrese un mensaje de error (un mensaje de error que indique la no disposición del *Web Service* de Actualización del Registro Judicial), por lo tanto es necesario que el *Web Service* que solicita el servicio de Actualización del Registro Judicial sea capaz de manejar las excepciones generadas por la falta de disponibilidad del *Web Service* de Actualización del Registro Judicial.

Operación fallida (la Capa de Negocio no puede atender la petición)

El flujo del proceso de actualización de un registro, Operación fallida, la Capa de Negocio no puede atender la petición, muestra que no se pudo realizar la actualización de un determinado registro en un CS o alguna otra instancia municipal, estatal o federal con alguna base de datos que comparta información.
A continuación, en la figura X.21 se muestra el flujo del proceso de actualización de registro, Operación fallida (la Capa de Negocio no puede atender la petición).

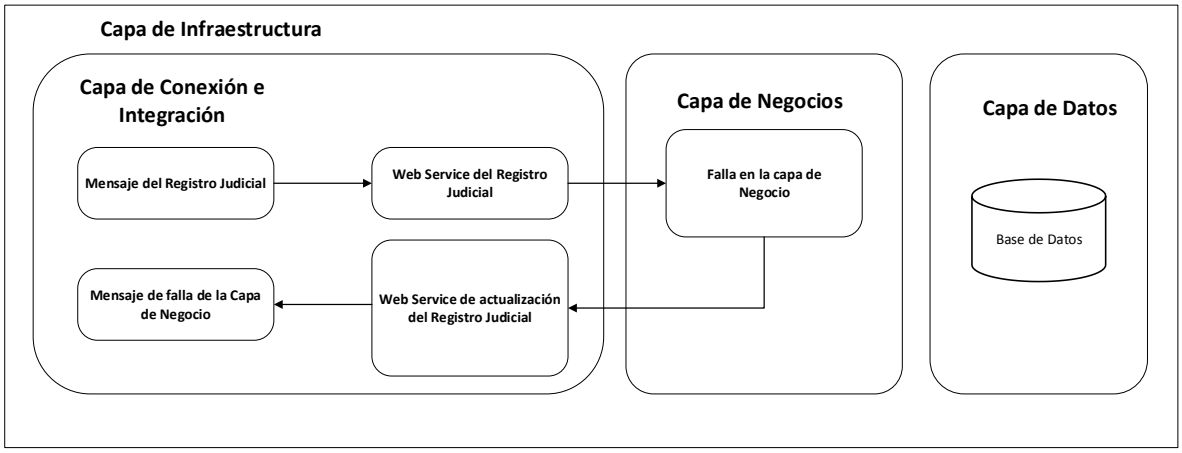


Figura X. 21 Diagrama de flujo del proceso de actualización de un registro, operación fallida (la Capa de Negocio no puede atender la petición)

1) El servicio de Actualización de Registro Judicial (que está alojado en la Capa de Conexión e Integración) recibe un mensaje de actualización de Registro Judicial. Un mensaje es enviado a la orquestación adecuada dentro de la Capa de Negocio.
2) En caso de falla de la Capa de Negocio puede presentarse el siguiente escenario:
    a. La Capa de Negocio no puede procesar la solicitud proveniente de la Capa de Conexión e Integración, levanta una excepción y regresa un mensaje (a la Capa de Conexión e Integración) indicando el motivo de la falla.
3) La Capa de Conexión e Integración utiliza el servicio de Actualización de Registro Judicial para regresar un mensaje al *Web Service* que le solicitó la actualización, indicándole el motivo de la falla.

Operación fallida (falla en la Capa de Negocio)

El flujo del proceso de actualización de un registro, Operación fallida, falla en la Capa de Negocio, muestra que no se pudo realizar la actualización de un determinado registro en un CS o alguna otra instancia municipal, estatal o federal con alguna base de datos que comparta información.

A continuación, en la figura X. 22 se muestra el flujo del proceso de actualización de registro, Operación fallida (falla en la Capa de Negocio).

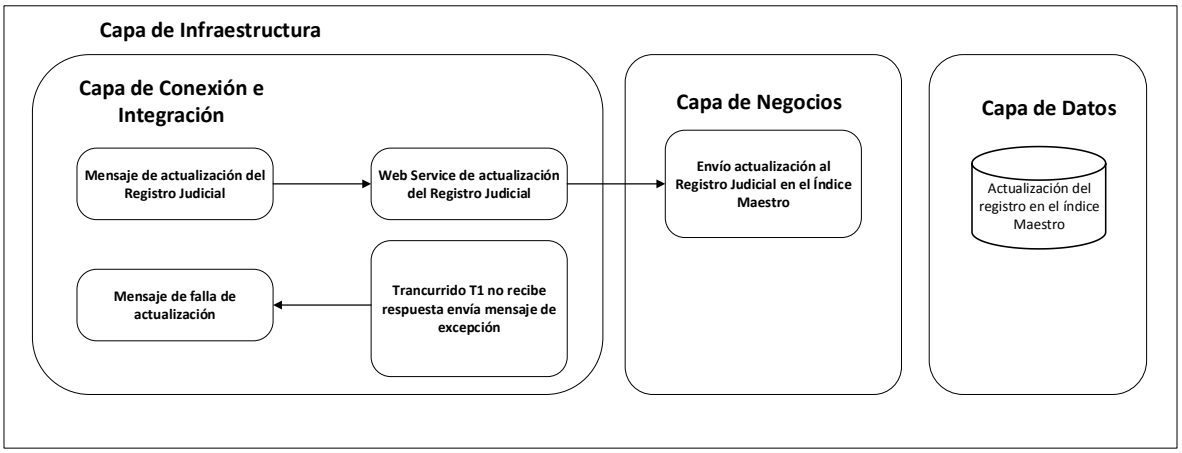


Figura X. 22 Diagrama de flujo del proceso de actualización de un registro, operación fallida (falla en la Capa de Negocio)

1) El servicio de Actualización de Registro Judicial (que está alojado en la Capa de Conexión e Integración) recibe un mensaje de actualización de Registro Judicial. Un mensaje es enviado a la orquestación adecuada dentro de la Capa de Negocio.
2) En caso de falla de la Capa de Negocio puede presentarse el siguiente escenario:
    a. Si después de un tiempo de espera T1 (tiempo de espera configurado al inicio de la operación de la PTII, según los parámetros establecidos en los SLA), el Servicio de Actualización de Registro Judicial no recibe ningún mensaje de la Capa de Negocio, se genera una excepción que indica la falla.
    b. La Capa de Negocio no puede procesar la solicitud proveniente de la Capa de Conexión e Integración, levanta una excepción y regresa un mensaje (a la Capa de Conexión e Integración) indicando el motivo de la falla.
3) La Capa de Conexión e Integración utiliza el servicio de Actualización de Registro Judicial para regresar un mensaje al *Web Service* que le solicitó el registro, indicándole el motivo de la falla.

5.10.8.13 Recepción y Envío de Datos del Expediente

En este caso la información almacenada en los sistemas debe ser obtenida a través de *queries* (consultas de datos) utilizando información demográfica del registro judicial para hacer las discriminaciones adecuadas que acoten el *query*, es decir, la consulta. Es necesario aclarar que el Expediente puede contener datos de uno o varios tipos (por ejemplo, texto, imágenes, etc.), por lo cual los *Web Services* y mensajes deben ser capaces de manejar estos distintos tipos.

Operación exitosa

El flujo del proceso de búsqueda y recepción/envío de Expediente, Operación exitosa, muestra que se pudo realizar la búsqueda y recepción/envío de Expediente en un CS o alguna otra instancia municipal, estatal o federal con alguna base de datos que comparta información.

A continuación, en la figura X.23 y figura X.24, se muestra el flujo del proceso de búsqueda y recepción/envío de Expediente y el de Operación exitosa.

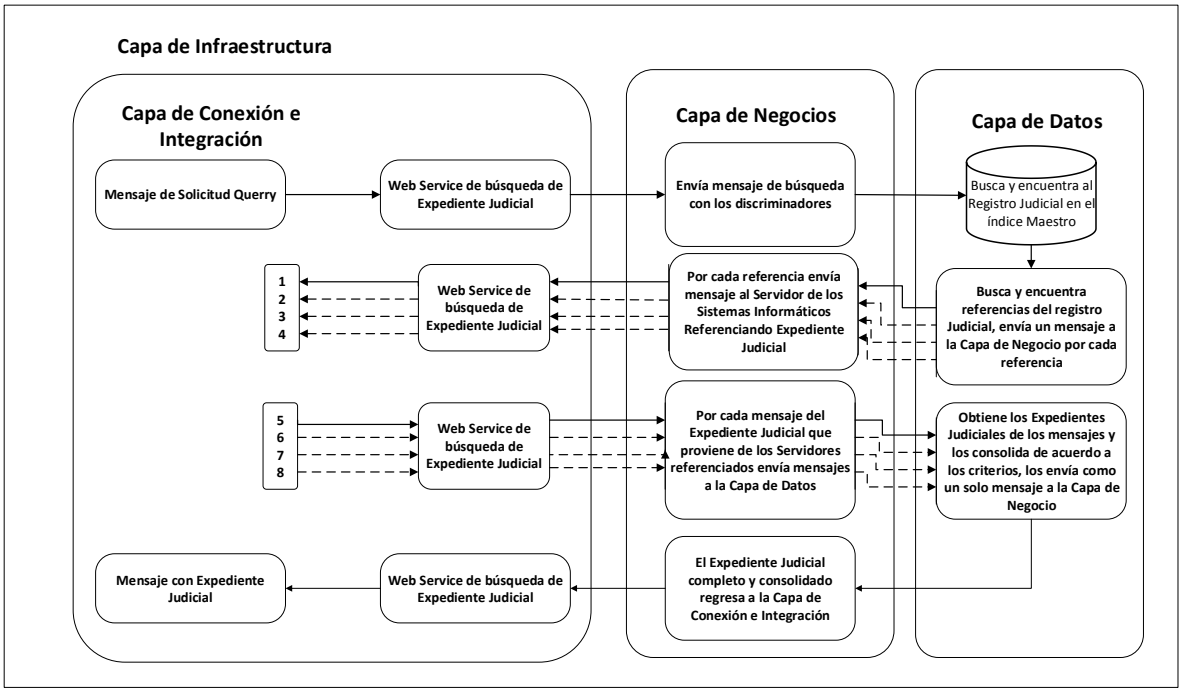


Figura X. 23 Diagrama de flujo del proceso de búsqueda y recepción/envío de Expediente

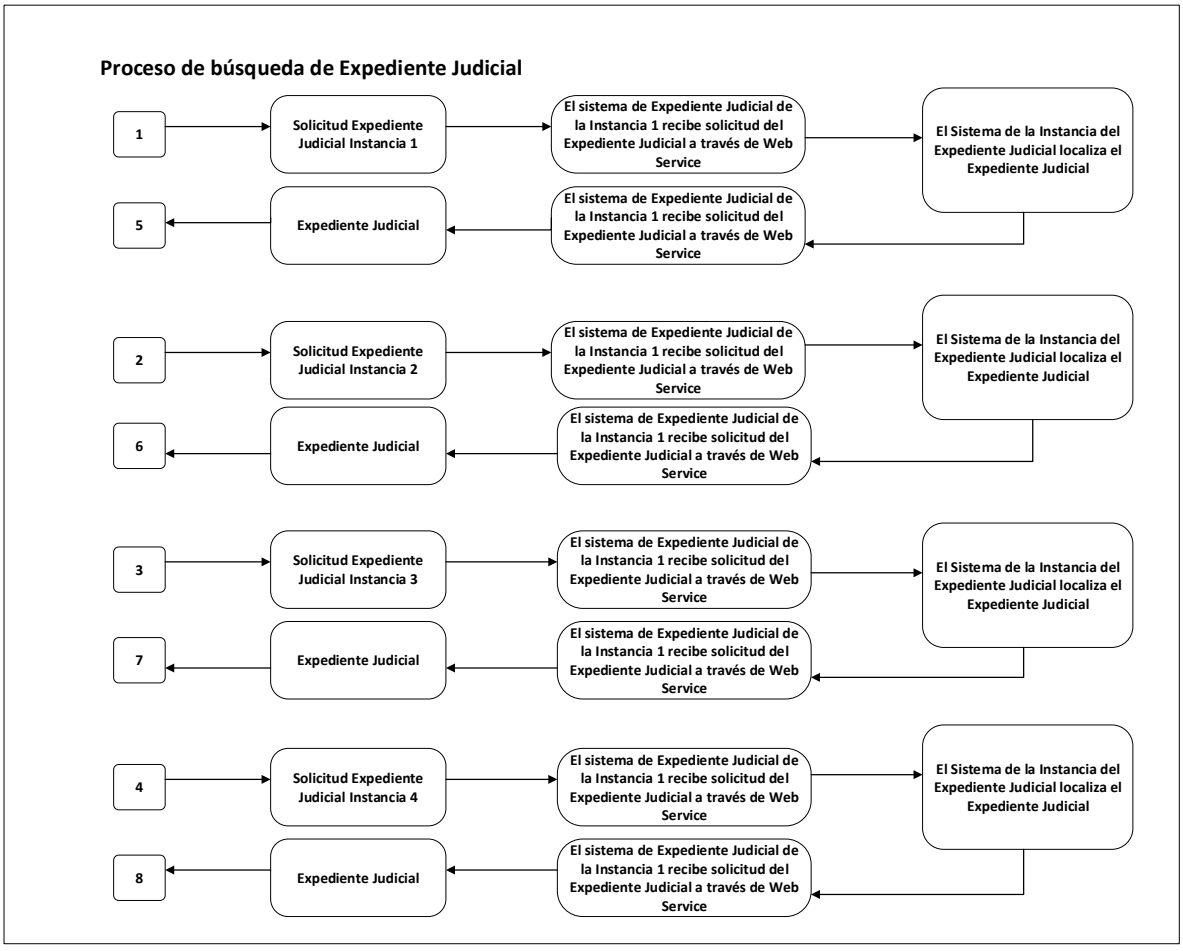


Figura X. 24 Diagrama de flujo del proceso de búsqueda y recepción/envío de Expediente (operación exitosa)

El *Web Service* de búsqueda de Expediente (que está alojado en la Capa de Conexión e Integración) recibe un mensaje de solicitud de Expediente de un registro judicial, la información demográfica necesaria para la ejecución de la búsqueda (*query*) está contenida dentro del mensaje.

Desde la Capa de Conexión e Integración se envía un mensaje a la Capa de Negocio (a la orquestación requerida), indicándole de la existencia de un nuevo mensaje de solicitud de información de un registro judicial, usando sus datos demográficos para discriminar.

La Capa de Negocio envía el mensaje de solicitud a la Capa de Datos que contiene la información demográfica del registro judicial, para efectos de discriminación de Capa. La Capa de Negocio queda en espera de la respuesta por un tiempo T1 (el tiempo de espera debe ser configurado al inicio de la operación de la PTII; sin embargo, este

tiempo debe ser optimizado durante la operación; al establecer y optimizar este tiempo es necesario considerar los parámetros establecidos en los SLA).

La Capa de Datos hace la búsqueda del Registro Judicial en el Índice Maestro. Si se ha localizado al Registro Judicial dentro del Índice Maestro se buscan las referencias existentes en el Expediente de las instancias municipales, estatales o federales donde haya expedientes del Registro Judicial. Si el Registro Judicial es encontrado en el Índice Maestro, debe existir, al menos, una entrada.

Por cada una de las entidades donde se reporta información del Registro Judicial, la Capa de Datos envía un mensaje a la Capa de Negocio (a la orquestación adecuada).

Por cada mensaje enviado por la Capa de Datos, la Capa de Negocio envía un mensaje a la Capa de Conexión e Integración.

Por cada mensaje recibido por la Capa de Conexión e Integración, el *Web Service* de búsqueda de Expediente envía un mensaje de solicitud de información a cada una de las entidades que, dentro del Expediente de las instancias municipales, estatales o federales, reportan tener datos del Registro Judicial.

Los mensajes son recibidos por los *Web Services* alojados en los servidores de Expediente de cada uno de los estados y/o de las instancias municipales, estatales o federales. El Expediente de cada uno de las instancias municipales, estatales o federales procesa la solicitud de información y en su caso devuelve el Expediente en cuestión.

Por cada mensaje enviado la Capa de Negocio espera por un tiempo T2 (el tiempo de espera debe ser configurado al inicio de la operación de la PTII; sin embargo, este tiempo debe ser optimizado durante la operación; al establecer y optimizar este tiempo es necesario considerar los parámetros establecidos en los SLA). En este paso pueden ocurrir los siguientes escenarios:

- Después de transcurrido el tiempo T2 no se ha recibido ningún mensaje de respuesta y la Capa de Conexión e Integración genera una excepción.
- Después de transcurrido el tiempo T2 se recibe un mensaje pero está vacío, entonces la Capa de Conexión e Integración genera una excepción.
- Después de transcurrido el tiempo T2 se recibe un mensaje de respuesta con la información solicitada.

La Capa de Conexión e Integración envía un mensaje de respuesta a la Capa de Negocio por cada uno de los mensajes recibidos y/o excepciones generadas al solicitar información a las entidades que, dentro de la Referencia, reportan tener

datos del Registro Judicial. En los casos donde haya habido respuesta con datos (los mensajes contienen datos en los casos en que haya ocurrido una excepción), los mensajes contienen la razón de la excepción.

Por cada mensaje recibido de la Capa de Conexión e Integración, la Capa de Negocio envía uno hacia la Capa de Datos que contiene información y/o la razón de la excepción.

La información se consolida en la Capa de Datos y se ordena según la fecha de creación reportada. Si alguna de las Referencias encontradas no regresa información, es necesario informarlo en el mensaje de respuesta.

La información del Expediente encontrada es enviada de regreso a la Capa de Negocio desde donde (a través de la orquestación definida) es enviada a la Capa de Conexión e Integración.

El *Web Service* de búsqueda de Expediente regresa un mensaje (o varios, dependiendo del tamaño de la información transferida) que contiene el Expediente del Registro Judicial al *Web Service* que le solicitó la información.

Operación fallida (no es posible consultar al Índice Maestro)

El flujo del proceso de búsqueda de Expediente, Operación fallida, no es posible consultar al Índice Maestro, muestra que no se pudo realizar la búsqueda de Expediente en un CS o alguna otra instancia municipal, estatal o federal con alguna base de datos que comparta información.

A continuación, en la figura X.25 se muestra el flujo del proceso Operación fallida, no es posible consultar al Índice Maestro.

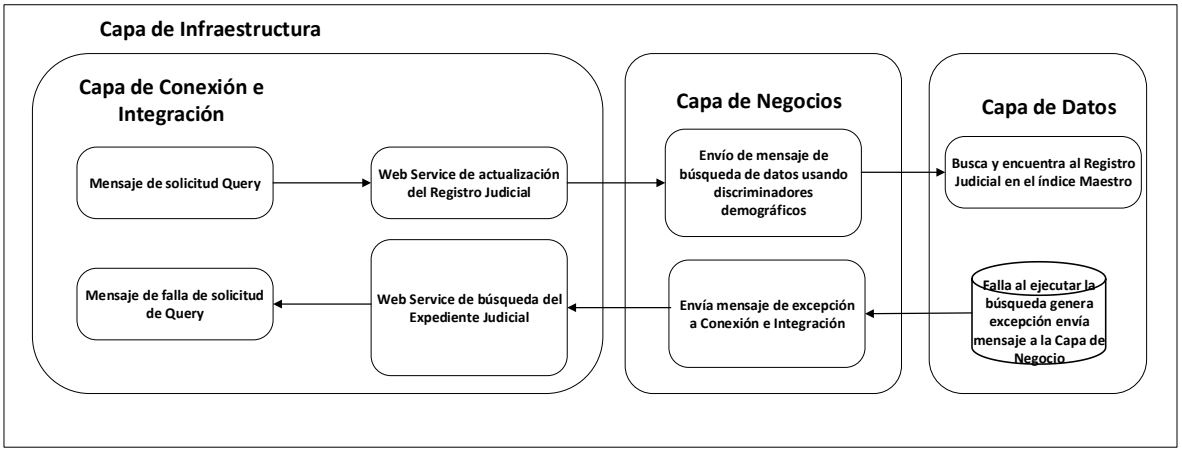


Figura X. 25 Diagrama de flujo del proceso de búsqueda de Expediente (no es posible consultar al Índice Maestro)

1. El *Web Service* de búsqueda de Expediente (que está alojado en la Capa de Conexión e Integración) recibe un mensaje de solicitud de Expediente de un Registro Judicial. La información demográfica necesaria para la ejecución de la búsqueda (*query*) está contenida dentro del mensaje.
2. Desde la Capa de Conexión e Integración se envía un mensaje a la Capa de Negocio (a la orquestación adecuada) indicándole de la existencia de un nuevo mensaje de solicitud de información de un Registro Judicial, usando sus datos demográficos para discriminar.
3. La Capa de Negocio envía un mensaje (que contiene, además, la información demográfica del Registro Judicial, para efectos de discriminación) de solicitud de información a la Capa de Datos. La Capa de Negocio queda en espera de la respuesta por un tiempo T1 (el tiempo de espera debe ser configurado al inicio de la operación de la PTII; sin embargo este tiempo debe ser optimizado durante la operación; al establecer y optimizar este tiempo es necesario considerar los parámetros establecidos en los SLA).
4. Si la consulta a la Capa de Datos falla se puede presentar el siguiente escenario:
    a. La Capa de Datos está disponible pero no se puede ejecutar la consulta. La Capa de Datos genera una excepción (que indica el motivo de la falla). La Capa de Datos envía un mensaje de regreso a la orquestación indicando el motivo de la falla. La Capa de Datos debe enviar el mensaje antes de que transcurra el tiempo T1.
5. La Capa de Negocio (en cumplimiento con la orquestación ejecutada), basada en el mensaje recibido, genera una excepción y envía un mensaje a la Capa de Conexión e Integración, informando de la excepción.
6. Al recibir el mensaje la Capa de Conexión e Integración genera una nueva excepción y envía un mensaje avisándole al *Web Service*, que le solicitó el servicio del *query*, de la ocurrencia de la excepción y las causas de la misma.

Operación fallida (está fallando el Índice Maestro)

El flujo del proceso de búsqueda de Expediente, Operación fallida, está fallando el Índice Maestro, muestra que no se pudo realizar la búsqueda de Expediente en un CS o alguna otra instancia municipal, estatal o federal con alguna base de datos que comparta información.

A continuación, en la figura X.26 se muestra el flujo del proceso Operación fallida, está fallando el Índice Maestro.

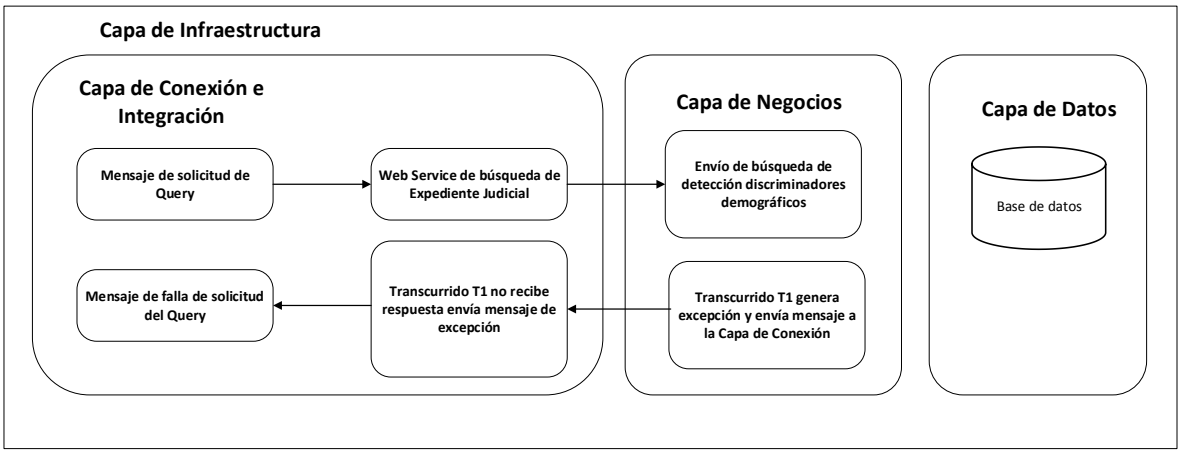


Figura X. 26 Diagrama de flujo del proceso de búsqueda de Expediente (está fallando el Índice Maestro)

1. El *Web Service* de búsqueda de Expediente (que está alojado en la Capa de Conexión e Integración) recibe un mensaje de solicitud de Expediente de un Registro Judicial; la información demográfica necesaria para la ejecución de la búsqueda (*query*) está contenida dentro del mensaje.
2. Desde la Capa de Conexión e Integración se envía un mensaje a la Capa de Negocio (a la orquestación adecuada) indicándole de la existencia de un nuevo mensaje de solicitud de información de un Registro Judicial, usando sus datos demográficos para discriminar.
3. La Capa de Negocio envía un mensaje (que contiene, además, la información demográfica del Registro Judicial, para efectos de discriminación) de solicitud de información a la Capa de Datos. La Capa de Negocio queda en espera de la respuesta por un tiempo T1 (el tiempo de espera debe ser configurado al inicio de la operación de la PTII; sin embargo, este tiempo debe ser optimizado durante la operación; al establecer y optimizar este tiempo es necesario considerar los parámetros establecidos en los SLA).
4. La consulta a la Capa de Datos puede presentar el siguiente escenario:
    a. Después de transcurrido el tiempo T1, la Capa de Datos no regresa ningún mensaje.
5. La Capa de Negocio (en cumplimiento con la orquestación ejecutada) detecta la situación anterior, genera una excepción y envía un mensaje a la Capa de Conexión e Integración, informando de la excepción.

6. Al recibir el mensaje la Capa de Conexión e Integración genera una nueva excepción y envía un mensaje avisándole al *Web Service* que le solicitó el servicio del *query*, de la ocurrencia de la excepción y las causas de la misma.

Operación fallida (la Capa de Negocio no puede atender la petición)

El flujo del proceso de búsqueda de Expediente, Operación fallida, la Capa de Negocio no puede atender la petición, muestra que no se pudo realizar la búsqueda de Expediente en un CS o alguna otra instancia municipal, estatal o federal con alguna base de datos que comparta información.

A continuación, en la figura X.27 se muestra el flujo del proceso Operación fallida, la Capa de Negocio no puede atender la petición.

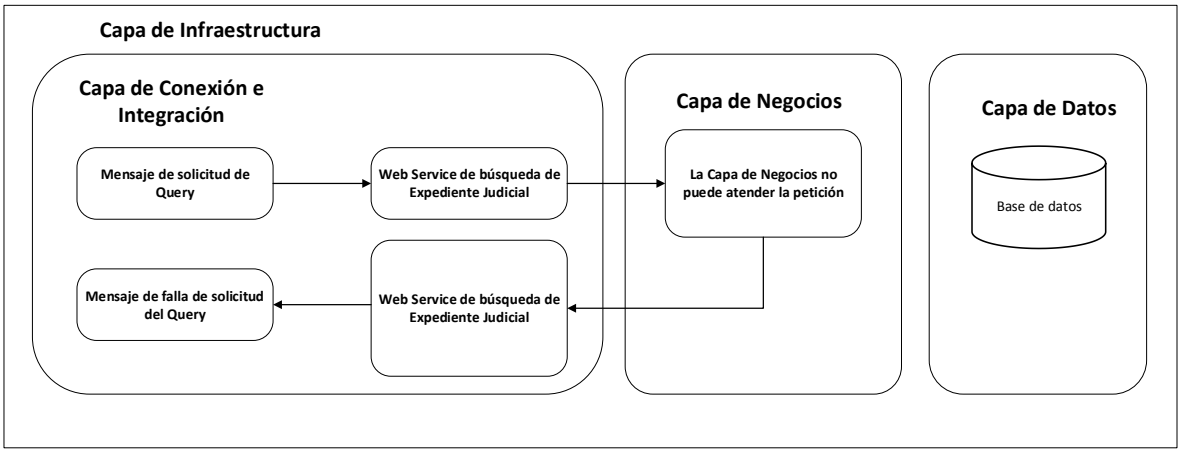


Figura X. 27 Diagrama de flujo del proceso de búsqueda de Expediente (la Capa de Negocio no puede atender la petición)

1. El *Web Service* de búsqueda de Expediente (que está alojado en la Capa de Conexión e Integración) recibe un mensaje de solicitud de Expediente de un Registro Judicial; la información demográfica necesaria para la ejecución de la búsqueda (*query*) está contenida dentro del mensaje.
2. Desde la Capa de Conexión e Integración se envía un mensaje a la Capa de Negocio (a la orquestación adecuada) indicándole de la existencia de un nuevo mensaje de solicitud de información de un Registro Judicial usando sus datos demográficos para discriminar. Se inicia un temporizador T1 (el tiempo de espera debe ser configurado al inicio de la operación de la PTII; sin embargo,

este tiempo debe ser optimizado durante la operación; al establecer y optimizar este tiempo es necesario considerar los parámetros establecidos en los SLA). En este punto se puede presentar el siguiente escenario:

   a. La Capa de Negocio no puede atender la petición enviada por la Capa de Conexión e Integración. La Capa de Negocio levanta una excepción y regresa un mensaje a la Capa de Conexión e Integración, informándole el motivo. El mensaje a la Capa de Conexión e Integración debe ser enviado antes de que el tiempo T1 transcurra.

3. La Capa de Conexión e Integración envía un mensaje al *Web Service* que le solicitó el servicio, informándole de la falla y el motivo de la misma.

Operación fallida (la Capa de Negocio está fallando)

El flujo del proceso de búsqueda de Expediente, Operación fallida, la Capa de Negocio está fallando, muestra que no se pudo realizar la búsqueda de Expediente en un CS o alguna otra instancia municipal, estatal o federal con alguna base de datos que comparta información.

A continuación, en la figura X.28 se muestra el flujo del proceso Operación fallida, la Capa de Negocio está fallando.

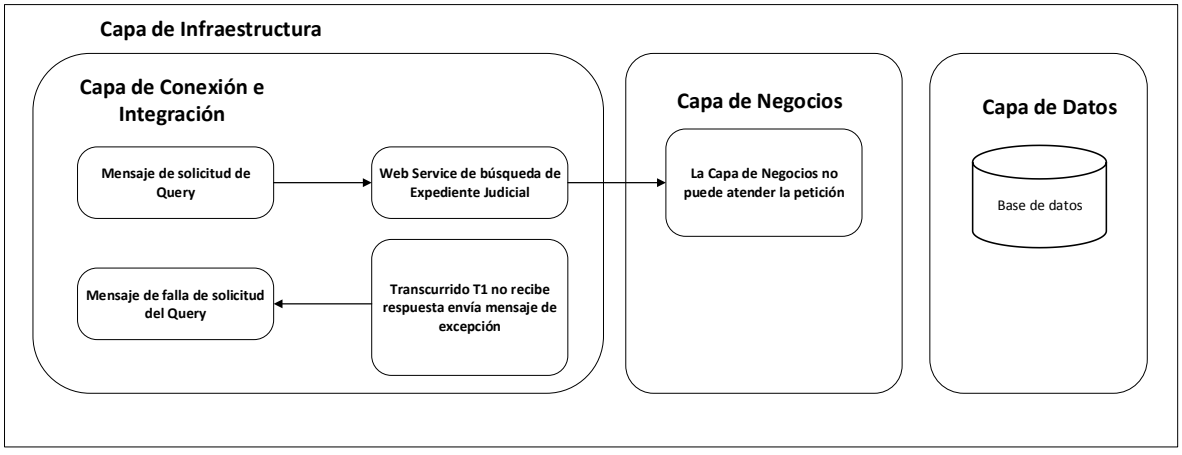


Figura X. 28 Diagrama de flujo del proceso de búsqueda de Expediente (la Capa de Negocio está fallando)

1. El *Web Service* búsqueda de Expediente (que está alojado en la Capa de Conexión e Integración) recibe un mensaje de solicitud de Expediente de un Registro Judicial; la información demográfica necesaria para la ejecución de la búsqueda (*query*) está contenida dentro del mensaje.
2. Desde la Capa de Conexión e Integración se envía un mensaje a la Capa de Negocio (a la orquestación adecuada) indicándole de la existencia de un nuevo mensaje de solicitud de información de un Registro Judicial, usando sus datos demográficos para discriminar. Se inicia un temporizador T1 (el tiempo de espera debe ser configurado al inicio de la operación de la PTII; sin embargo, este tiempo debe ser optimizado durante la operación; al establecer y optimizar este tiempo es necesario considerar los parámetros establecidos en los SLA). En este punto se puede presentar el siguiente escenario:
    a. Después de un tiempo de espera T1 la Capa de Negocio no regresa ningún mensaje.
3. La Capa de Conexión e Integración levanta una excepción y envía un mensaje al *Web Service* que le solicitó el servicio informándole de la falla y el motivo de la misma.

Operación fallida (no es posible contactar a la Capa de Conexión e Integración)

Si un *Web Service*, perteneciente a un Sistema de Expediente Judicial o Instancias municipales, estatales o federales, solicita el Servicio de Búsqueda de Expediente al *Web Service* de Búsqueda de Expediente y este último no está disponible, no hay forma de que se regrese un mensaje de error (un mensaje de error que indique la no disposición del *Web Service* de Búsqueda de Expediente), por lo tanto es necesario que el *Web Service* que solicita el servicio de Búsqueda de Expediente sea capaz de manejar las excepciones generadas por la falta de disponibilidad del *Web Service* de Búsqueda de Expediente.

5.10.8.14 Niveles de Servicio

Los Niveles de Servicio que debe cumplir la PTII consideran la funcionalidad requerida por el CS.

Los Niveles de Servicio se especifican solamente en los puntos de salida: entrega a entidad “origen” de las peticiones y envío de peticiones a entidades “destino” para la obtención de los datos solicitados; de manera intermedia se deben considerar y

cumplir los acuerdos de niveles de operación entre los elementos de la arquitectura de la PTII.

5.10.8.14.1 Criterios para la definición del Nivel del Servicio

Las mediciones de los tiempos de respuesta se harán exclusivamente sobre los elementos de la PTII y sobre el intercambio de mensajes y datos que se efectúe entre cada elemento, de acuerdo al modelo de operación y la tabla X.7 de Disponibilidad y Tiempos de respuesta siguiente:

Tabla X. 7 Criterios para la definición del Nivel del Servicio

Punto/ Componente	Impacto en el resultado de una petición	Disponibilidad requerida	Nivel de Servicio (Tiempo de respuesta)
Afectación Total	La PTII es incapaz de responder peticiones tanto desde su sitio principal como del respaldo.	Sin interrupción (excepción en ventanas de tiempo)	99.99% de disponibilidad de la infraestructura medida en periodo de 30 días (30 *day Rolling period*)
Afectación Parcial	Afectación al acceso a alguno de los Servicios de las Instancias municipales, estatales o federales con alguna base de datos que comparta información.	Sin interrupción.	99.99% de disponibilidad de la infraestructura medida en periodo de 30 días (30 *day Rolling period*)
Afectación por Transacción	Transacciones que por causas imputables al proveedor o errores de procesamiento no sean completadas adecuadamente.	Sin excepción	100% de las transacciones recibidas procesadas de manera correcta.
Desempeño	Afectación en tiempos de respuesta, peticiones exceden 2 segundos en ser respondidas por el sistema. La recepción del mensaje de respuesta del sistema	Sin excepción	100% de las peticiones deben ser atendidas en el tiempo establecido.

Punto/ Componente	Impacto en el resultado de una petición	Disponibilidad requerida	Nivel de Servicio (Tiempo de respuesta)
	contará como elemento de terminación de medición de dicho tiempo.		
Afectación en los Servicios de Monitoreo	Afectación a la visibilidad desde el CS, sobre el desempeño y disponibilidad del servicio.	Sin interrupción (excepción en ventanas de tiempo)	99.9% del tiempo se encuentra disponible el servicio.
Pérdida de Información.	Afectación en la disponibilidad o integridad de información de la plataforma incluyendo las bitácoras, respaldos y todo aquel registro que conforma el servicio. Se considerará como pérdida cualquier información que no pueda ser reconstruida en un plazo de una semana a partir de la solicitud de CNI o cualquier CS.	Sin interrupción (excepción en ventanas de tiempo)	100% de la información debe resguardarse de manera permanente.
Intrusiones al Sistema	Cualquier acceso no autorizado a la información almacenada en la plataforma.	Sin excepción	100% intentos de infiltración deben ser repelidos.
Tiempos de atención a fallas	Atención a fallas fuera de los tiempos comprometidos.	Sin excepción	100% de las fallas atendidas dentro de los tiempos comprometidos.
Operación en Contingencia	Operación bajo contingencia mayor al tiempo permitido por evento.	Sin excepción	100% de los eventos de contingencia son devueltos a operación en el sitio principal en menos de 24 horas (máximo un evento por mes).

5.10.8.14.2 Ventanas de tiempo

Las ventanas de tiempo que se describen en la siguiente tabla, conjuntamente con las requeridas para efectuar las actividades de respaldo y/o mantenimiento de los elementos que integran la PTII, serán las únicas validadas y/o permitidas para considerar los niveles de servicio que ello debe proporcionar.

Tabla X. 8 Ventanas de Tiempo por Capa

Ventanas de tiempo por Capa			
Evento	**Descripción del requerimiento de tiempo**	**Duración de la Ventana**	**Número de eventos**
Mantenimiento de infraestructura	Es necesario intervenir sobre algún elemento de la Capa por fallos físicos o de configuración.	2 (dos) horas	Máximo 1 (un) evento por trimestre
Reubicación de enlaces de telecomunicaciones	Es necesario reubicar un enlace a solicitud de una Instancia municipal, estatal o federal con alguna base de datos que comparta información, previa solicitud de por lo menos 15 días naturales.	24 (veinticuatro) horas	N/A
Recuperación de Respaldos	En caso de requerirse por parte del CNI o cualquier CS la recuperación de un respaldo, previa solicitud al menos 7 días naturales antes.	24 (veinticuatro)horas	Máximo 1 (un) evento por mes
Capa de Datos	Es necesario intervenir sobre algún elemento de software (herramienta o aplicación) por fallos en su configuración o en su funcionalidad.	1 (una) hora	Máximo 2 (dos) eventos por mes
Capa de Gestión	Es necesario intervenir sobre algún elemento de software (herramienta o aplicación) por fallos en su configuración o en su funcionalidad.	1 (una) hora	Máximo 2 (dos) eventos por mes

5.10.9 Bases de Datos

5.10.9.1 Características de las bases de datos que se comunicarán

Las bases de datos deben estar normalizadas, es decir, las tablas de datos deben eliminar incoherencias y redundancias, así como minimizar la ineficiencia. Las bases de datos deben presentar al menos las tres primeras formas normales (1FN, 2FN y 3FN), a efecto de poder crear, entender y utilizar una base de datos relacionar.

Tabla X. 9 Normalización de Bases de Datos

Primera Forma Normal (1FN)	Una relación se encuentra en primera forma normal si, y sólo si, todos los dominios simples subyacentes de los atributos contienen valores atómicos y monovalentes.
Segunda Forma Normal (2FN)	Una relación se encuentra en segunda forma normal si, y sólo si, se encuentra en 1FN y, además, todos los atributos no clave dependen por completo de la clave primaria.
Tercera Forma Normal (3FN)	Una relación se encuentra en tercera forma normal si, y sólo si, se encuentra en 2FN; y si ningún subconjunto de atributos no claves tiene dependencia funcional entre sí.
Cuarta Forma Normal (4FN)	Una relación R está en cuarta forma normal, si primero está en forma normal *Boyce-Codd*[a] y, además, todas sus dependencias multivaluadas en esta relación R son "dependencias funcionales". El concepto de dependencia multivaluada, pero que no es una dependencia funcional, es lo que impide que una relación se encuentre en cuarta forma normal.
Quinta Forma	Una relación R está en quinta forma normal si, y sólo si, toda dependencia de reunión en R es una

Normal (5FN)	consecuencia de las claves candidatas en R. Una relación R está en 5FN si, y sólo si, toda dependencia de reunión está condicionada por las claves candidatas de R.
[a] Forma Normal de *Boyce-Codd* (FNBC): • Una relación está en FNBC si, y sólo si, todo determinante es una clave candidata. Determinante es el atributo del que depende, funcionalmente y de manera completa, otro atributo o conjunto de estos. • Una relación está en FNBC si primero está en tercera forma normal y luego, si y sólo si, las únicas dependencias funcionales triviales se encuentran dadas entre la clave primaria y uno o varios atributos.	

Fuente: Elaboración propia a partir de Reinosa E.J., Maldonado C.A., Muñoz R., Damiano L.E. &Abrustsky M.A. 2012.[11]

Las bases de datos que a continuación se muestran en la tabla X.10 son enunciativas más no limitativas para la operación del Complejo de Seguridad.

Tabla X. 10 Bases de Datos del CS

Base de datos
1. Informe Policial Homologado
2. Licencias de Conducir
3. Mandamientos Judiciales
4. Registro Nacional de Armamento y Equipos
5. Registro Nacional de Información Penitenciaria
6. Registro Nacional de Personal de Seguridad Pública
7. Registro de Vehículos Robados y Recuperados
8. Registro Público Vehicular
9. Incidencia Delictiva
10. Sistema de Atención de Emergencias 9-1-1 y Denuncia Anónima 089

El Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública determinará, con fundamento en sus atribuciones, el o los campos que pueden compartirse y las bases de datos que puedan operar e interoperar entre los Complejos de Seguridad. Asimismo, definirá el número de bases de datos y la estructura lógica con la que operarán.

Por otra parte, la disponibilidad de la información expresada en porcentajes se presenta en la siguiente tabla, tomando en consideración que los CS operan 24 horas al día y que la información debe estar altamente disponible, es decir, su disponibilidad debe darse en un elevado porcentaje. Cabe señalar que cuando la información deje de estar disponible, se precisará del tiempo indicado para volver a recuperar el porcentaje de disponibilidad señalado.

Tabla X. 11 Porcentaje de disponibilidad de la información y tiempo para su recuperación en caso de que no esté disponible

Porcentaje de disponibilidad	Día de 24 horas (tiempo requerido para recuperar el porcentaje de disponibilidad)
90%	876 horas (36,5 días)
95%	438 horas (18,25 días)
99%	87,6 horas (3,65 días)
99.9%	8,76 horas
99.99%	52,56 minutos
99,999% (“cinco nueves”)	5,256 minutos
99.9999%	31,536 segundos

Fuente: Modificado de Microsoft, 2005

5.10.9.2 Mecanismos para el intercambio de información

El Complejo de Seguridad debe contar con interfaces para el intercambio de información.

5.10.9.3 Dimensionamiento de infraestructura tecnológica

Para el dimensionamiento de infraestructura tecnológica, se sugiere el uso de una herramienta que permita el levantamiento y registro de información relativa al equipo de que se dispone en los CS, las características o el estado que guarda, el número de usuarios y su concurrencia, así como el área en la que se ubica, de modo que sea

posible la toma de decisiones para la adquisición, reubicación y/o arrendamiento. Como es posible advertir, se trata de algo más que un inventario de equipo, de forma tal que a partir del dimensionamiento realizado se procura una mejora en la integración de la infraestructura, según las necesidades y funcionalidades requeridas para la operación de procesos.

Un buen dimensionamiento de infraestructura contribuye a la implementación exitosa de la tecnología y en este caso, a hacer eficientes los procesos operados a través de la Plataforma Tecnológica para la Integración de Información (PTII), y las correspondientes Bases de Datos del CS: 1. Informe Policial Homologado, 2. Licencias de Conducir, 3. Mandamientos Judiciales, 4. Registro Nacional de Armamento y Equipos, 5. Registro Nacional de Información Penitenciaria, 6. Registro Nacional de Personal de Seguridad Pública, 7. Registro de Vehículos Robados y Recuperados, 8. Registro Público Vehicular, 9. Incidencia Delictiva y 10. Sistema de Atención de Emergencias 9-1-1 y Denuncia Anónima 089.

La herramienta propuesta para el dimensionamiento de la infraestructura tecnológica debe considerar los siguientes criterios:

a. Dimensionamiento de memoria RAM y capacidad de Procesamiento
    1) Usuarios concurrentes
    2) Requerimientos por usuario
b. Dimensionamiento de ancho de banda
    1) Usuarios Nombrados
    2) Requerimientos por usuario
c. Dimensionamiento de almacenamiento en Disco Duro
    1) Registros
    2) Expedientes
    3) Almacenamiento para Aplicativos
d. Características de Servidor
    1) Aplicación Web
    2) Base de datos
e. Servidores requeridos
    1) Servidor Web y Aplicación
    2) Servidor de base de datos

Para cada criterio debe estimarse lo siguiente (ver tabla X.12):

Tabla X. 12 Estimación de criterios para el dimensionamiento de infraestructura tecnológica

Criterio	Especificación del criterio			Nota para cálculo
a.Dimensionamiento de memoria RAM y capacidad de Procesamiento	Usuarios concurrentes			Se estima a partir del número total de usuarios y el porcentaje de concurrencia, por ejemplo: 1,000 usuarios con un porcentaje de concurrencia del 30% = 300 usuarios concurrentes
	1) Requerimientos por usuario	1. Servidor Web	a. Memoria (Mb)	- El conjunto de la suma del consumo en MB del sistema operativo más el consumo en MB del servidor de aplicaciones más el consumo en MB del servidor *web* - Más el consumo en MB por usuario - Por el número de usuario concurrentes
			b. Procesamiento (MHz)	- El conjunto de la suma del consumo en MHz del sistema operativo más el consumo en MHz del servidor de aplicaciones más el consumo en MHz del servidor *web* - Más el consumo en MHz por usuario - Por el número de usuario concurrentes
		2. Servidor de aplicaciones	a. Memoria (Mb)	- El conjunto de la suma del consumo en MB del sistema operativo más el consumo en MB del servidor de aplicaciones más el consumo en MB del servidor *web* - Más el consumo en MB por usuario - Por el número de usuario concurrentes
			b. Procesamiento (MHz)	- El conjunto de la suma del consumo en MHz del sistema operativo más el consumo en MHz del servidor de aplicaciones más el consumo en MHz del servidor *web* - Más el consumo en MHz por usuario - Por el número de usuario concurrentes
		3 Servidor de base de datos	a. Memoria (Mb)	- El conjunto de la suma del consumo en MB del sistema operativo más el consumo en MB del Sistema Manejador de Base de Datos - Más el consumo en MB por usuario - Por el número de usuario concurrentes
			b. Procesamiento (Mhz)	- El producto del número de usuarios concurrentes por el consumo en MHz por el número de usuarios concurrentes
b.Dimensionamiento de almacenamiento en Disco Duro	1) Variable 1 determinada por los CS, por ejemplo: Registro	1. Cantidad		Corresponde al número registrado por el CS
		2. Tamaño unitario (KB)		Corresponde al número registrado por el CS
		3. Tamaño total (KB)		Es el producto de la Cantidad indicada por el tamaño unitario (KB)
		4. Tamaño total (MB)		Es el resultado del Tamaño total (KB) calculado entre 1024Mb
		5. Tamaño total (GB)		Es el resultado del tamaño total (MB) calculado entre 1024MB
	2) Variable 2 determinada por los CS, por ejemplo: Registro	1. Cantidad		Corresponde al número registrado por el CS
		2. Tamaño unitario (KB)		Corresponde al número registrado por el CS
		3. Tamaño total (KB)		Es el producto de la Cantidad indicada

			por el tamaño unitario (KB)
		3. Tamaño total (MB)	Es el resultado del Tamaño total (KB) calculado entre 1024MB
		4. Tamaño total (GB)	Es el resultado del tamaño total (MB) calculado entre 1024MB
	3) Variable N determinada por los CS, por ejemplo: Registro	1. Cantidad	Corresponde al número a registrar por el CS
		2. Tamaño unitario (KB)	Corresponde al número a registrar por el CS
		3. Tamaño total (KB)	Es el producto de la Cantidad indicada por el tamaño unitario (KB)
		3. Tamaño total (MB)	Es el resultado del Tamaño total (KB) calculado entre 1024MB
		4. Tamaño total (GB)	Es el resultado del tamaño total (MB) calculado entre 1024MB
	TOTAL DEL DISCO DURO		Para calcular el total de Dimensionamiento de almacenamiento de Disco Duro se suman los valores de tamaño total (KB), tamaño total (MB) y tamaño total (GB)
d.Características de Servidor	1) Aplicación y Web	1. Número total de Cores x Servidor	Se estima a partir de las características del servidor que se va a utilizar
		2. Velocidad de procesador en KHz	
	2) Base de datos	1. Número total de Cores x Servidor	Se estima a partir de las características del servidor que se va a utilizar
		2. Velocidad de procesador en KHz	
d.Servidores requeridos	1) Servidor Web y Aplicación	1. Cores requeridos en total	Se estima a partir del total de procesamiento (MHz) del servidor Web, entre la velocidad de procesador en KHz de la Aplicación y Web del servidor
		2. Memoria requerida en GB	Se estima a partir del total de Memoria (Mb) del servidor *web*, entre 1024MB
		3. Cantidad de Servidores necesarios según valores seleccionados	Es el producto de Cores requeridos en total para el Servidor Web y Aplicación, por el Número total de Cores x Servidor de la Aplicación y *Web*
	2) Servidor de base de datos	1. Cores requeridos en total	Se estima a partir del total de procesamiento (MHz) del servidor de base de datos, entre la velocidad de procesador en KHz de la Base de datos del servidor
		2. Memoria requerida en GB	Se estima a partir del total de Memoria (Mb) del servidor de base de datos, entre 1024MB
		3. Cantidad de Servidores necesarios según valores seleccionados	Es el producto de Cores requeridos en total para el Servidor de Base de datos, por el Número total de Cores x Servidor de Base de datos

5.11 Infraestructura Física

5.11.1 Objetivo

Definir las instalaciones, infraestructura, servicios, seguridad de instalaciones y áreas de la estructura física de los Complejos de Seguridad, determinando las dimensiones y organización del espacio, áreas dedicadas a las funciones específicas, servicios óptimos de cada área funcional, criterios de seguridad para las instalaciones y de acceso de personal en áreas que albergan servidores de bases de datos (BD), equipos de red de transporte, radio, voz y datos.

5.11.2 Alcance

Complejos de Seguridad.

5.11.3 Campo de aplicación

El campo de aplicación de este apartado establece los requerimientos necesarios de la Estructura Física de los Complejos de Seguridad.

5.11.4 Instalaciones

5.11.4.1 Especificaciones Técnicas para la conceptualización arquitectónica de espacios y distribución de áreas de operación de los Complejos de Seguridad

~~1.~~ El Complejo de Seguridad se debe concebir como un centro de operaciones, en cuyo diseño arquitectónico se consideren espacios y áreas acordes a las necesidades de coordinación entre entidades y corporaciones, atención de emergencias y de denuncoia anónima, así como las labores de apoyo en materia de comunicación, transferencias de datos e información

2. Un Complejo de seguridad debe diseñarse para recibir datos de múltiples fuentes, que requieren de espacios adecuados para recibir y transmitir la información. Las fuentes básicas de información de un Complejo de Seguridad son dos: a) Pantallas que reciben la señal de las cámaras y b) Sensores que estarán instalados en diversos sitios de una colonia, municipio o entidad federativa de la República Mexica.

3. En el diseño arquitectónico se debe considerar los espacios y áreas para los equipos con que contará el CS, así como las instalaciones necesarias para efectos de su operación, de acuerdo a las necesidades específicas de cada CS.

4. En el diseño de los espacios de las instalaciones se debe considerar que sean accesibles a las personas servidoras públicas que laboran y operan el CS, así

como al público externo que requiera visitarlo, de igual forma se debe establecer un área o espacio estratégico, que estará bajo control de los distintos mandos de gobierno, donde puedan supervisar la información captada por los operadores de los monitores, por lo que esta área debe tener un campo visual abierto para que sea un punto de observación de operadores, supervisores y mandos responsables de la operación del centro, así como de gobierno.

A continuación se describe el diagrama de anteproyecto arquitectónico

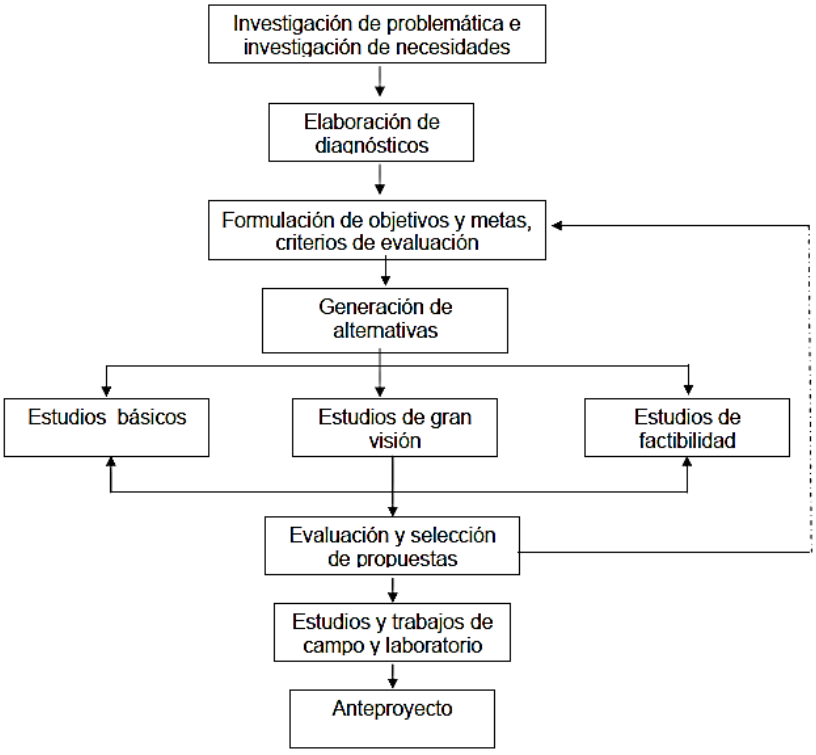


Figura XI. 1 Flujograma de Anteproyecto Arquitectónico

El proyecto arquitectónico debe considerar la adecuada interrelación del personal, operadores de monitoreo y mandos en general; las áreas deben tener una adecuada visibilidad, con el objeto de lograr cumplir con las necesidades que requiere el personal operativo, para un adecuado y eficiente flujo de información.

Un Complejo de Seguridad requiere considerar en su concepción de diseño las siguientes áreas y espacios para la operación de los subsistemas:

1. **Centro de monitoreo**: es el área en la que se ubican los operadores que monitorean la señal de las cámaras y sensores mediante una o varias pantallas en su estación de trabajo. Esta área debe estar cerrada hacia el exterior, además de contar con un *Video Wall*, que es una pared con grandes pantallas adicionales a su estación de trabajo, con una adecuada visibilidad desde cualquier punto del centro de monitoreo.

   El espacio para la proyección de cada uno de los módulos de los operarios estará de acuerdo al mobiliario bajo las siguientes condiciones:

   - La distancia entre el muro de pantallas y la primera fila de operadores de monitoreo debe tener una adecuada distancia para la visibilidad del personal operativo, como mínimo debe ser de 2.50m; la distancia estará en función de la altura de las pantallas; considerando la posición de la primera fila de operadores de monitoreo, debe tener un ángulo mínimo de visión de 25° hacia el muro de pantallas, y el alto del muro de pantallas, considerado desde la parte inferior de las mismas, debe de ser como mínimo de 1.20 m desde nivel de piso; la distancia de separación entre el muro de pantallas y los operadores que monitorean desde la segunda fila, no debe ser menor a 4.60m.
   - De igual forma se debe considerar el área de mantenimiento en la parte posterior del videowall, para el personal técnico de mantenimiento.
   - Los espacios que se requieren en el centro de monitoreo deben tener circulaciones entre pasillos de los operadores, así como un acceso y una salida controlada, de igual forma debe contar con circulación directa al centro de llamadas, al cuarto o central de comunicaciones, (*SITE*), a la salas de juntas y oficinas de mandos.

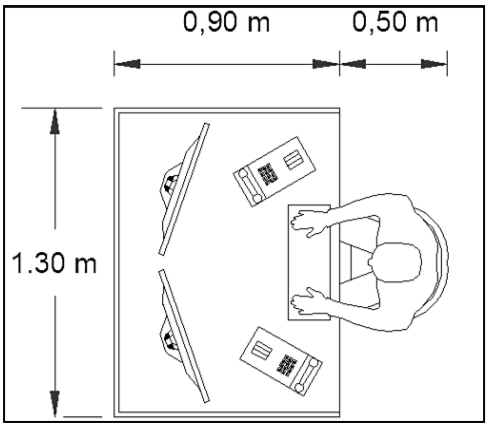


Figura XI. 2Área aproximada para un operador de monitoreo

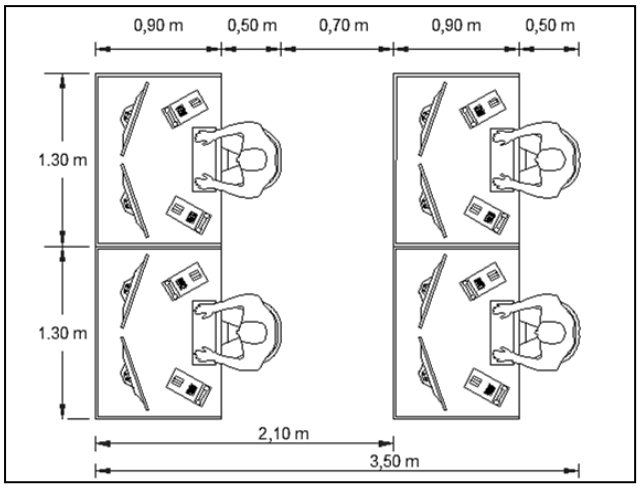


Figura XI. 3 Dimensiones de pasillo de separación de operadores de monitoreo

- **Centro de Atención de Llamadas de Emergencia:** este espacio debe incluir el mobiliario adecuado para los operadores, con mamparas divisorias integrales entre cada uno de ellos. El área debe tener circulación directa con el centro de monitoreo, por medio de un pasillo; de igual forma debe tener un cancel que permita la visibilidad hacia el muro de pantallas.

2. **Sala de crisis:** área estará anexa al centro de monitoreo, con uno o varios accesos controlados, debe contar con visibilidad hacia el centro de monitoreo, de igual forma debe contar con un mobiliario adecuado, así como equipo audiovisual, pantallas y proyectores.

3. **Central de comunicaciones**: esta área debe estar adyacente al centro de monitoreo, sus dimensiones estarán en función de los requerimientos del CS según sus necesidades, demandas, capacidades y características de los equipos en cada uno de sus centros. El diseño debe considerar la proyección de un acceso de servicio posterior a esta área, de tal manera que el personal de mantenimiento no tenga acceso por el Centro de Monitoreo.

4. **Equipos de Energía**: esta área debe estar adyacente al Centro de Monitoreo, sus dimensiones estarán en función de los requerimientos del CS según sus necesidades, demandas, capacidades y características de los equipos en cada uno de sus centros. El diseño debe considerar la proyección de un acceso de servicio posterior a esta área, de tal manera que el personal de mantenimiento no tenga acceso por el Centro de Monitoreo.

5. **Cuarto de Aire Acondicionado:** esta área debe estar adyacente al Centro de Monitoreo, sus dimensiones estarán en función a los requerimientos del CS sus necesidades, demandas, capacidades y características de los equipos en cada uno de sus centros. El diseño debe considerar la proyección de un acceso de servicio posterior a esta área, de tal manera que el personal de mantenimiento no tenga acceso por el Centro de Monitoreo.

6. **Cuarto de equipo de comunicación:** debe tener un área con suficiente capacidad para albergar los equipos centrales de telecomunicaciones del CS.

   La distribución de espacios en el cuarto de equipos se debe realizar considerando los siguientes rubros:

   - Los equipos activos, paneles de fibra óptica y paneles de parcheo se ubicarán en Racks abiertos. Para facilitar y asegurar el correcto manejo de los cables en el cuarto de equipo, se utilizarán paneles modulares angulados y organizadores verticales de alta densidad y con accesorios de organización. Los administradores deben ser dobles (frente/atrás). Todos los equipos, racks y paneles.

El diseño de las áreas de los subsistemas del Complejo de Seguridad debe considerar, como información de referencia, las áreas probables de construir en el complejo, de modo que el proyecto arquitectónico considere los espacios requeridos por el mobiliario, número de muebles sanitarios, cajones de estacionamiento y el equipo, debiendo resultar el espacio suficiente y adecuado desde un estudio ergonómico que satisfaga todas las necesidades de los usuarios; el diseño debe cumplir con los requerimientos mínimos expresados en este documento, además de considerar las dimensiones y requerimientos mínimos que se estipulan en la legislación vigente con respecto a Reglamentos de Construcción y Manuales de Diseño de cada municipio, estado o Gobierno Federal de la República Mexicana, o en su caso de Organismos internacionales.

A continuación, se describen las áreas y dimensiones mínimas que se deben considerar por usuario para el diseño de los espacios de los subsistemas, las áreas totales dependerán del número de usuarios y personal que opere en cada CS.

1.- Acceso Peatonal Principal al Complejo de Seguridad.
2.- Acceso Peatonal Secundario al Complejo de Seguridad.
3.- Acceso Vehicular al Complejo de Seguridad.
4.- Área de Estacionamiento Directivo.
5.- Área de Estacionamiento Operativo.
6.- Área de Estacionamiento para Discapacitados.
7.- Área de Estacionamiento Visitas.
8.- Área de Recepción y Vestíbulo.
9.- Área de acceso de seguridad con arcos detectores de metales y rayos X.
10.- Área de Control de Monitoreo Interno del Complejo CCTV.

11.- Área de Equipos de CCTV.
12.- Área de Plataforma México.
13.- Área de Mantenimiento de Radio Comunicaciones.
14.- Área de Equipos de Energía.
15.- Área de Equipos de Bombas.
16.- Área de Equipos de Aire de Precisión y Acondicionado.
17.- Área de Centro de Datos SITE (área seccionada por equipo).
18.- Área de Comunicaciones MDF.
19.- Área de Reparación de Equipos de Radio y Configuración.
20.- Área de Gestión de Voz, Datos y Radiocomunicaciones.
21.- Área de Sistemas.
22.- Área de Mesa de Ayuda.
23.- Área de Sanitarios de Hombres y Mujeres.
24.- Área de Casilleros.
25.- Área de Ciberseguridad
26.- Área de Centro de Llamadas y Operadores 9-1-1.
27.- Área de Centro de Llamadas y Operadores 089.
28.- Área de Centro de Monitoreo de Redes y Análisis Predictivo.
29.- Área de Administración.
30.- Área de Gestión de Base de Datos.
31.- Área de Inteligencia.
32.- Área de Protección Civil.
33.- Área de Estadística y Análisis Estratégico.
34.- Área de Tecnología.
35.- Área de Emergencias Médicas.
36.- Área de Dirección de Operaciones.
37.- Área de Calidad.
38.- Área de Sala de Crisis.
39.- Área de Dirección General del Complejo de Seguridad.
40.- Área de Antenas para telecomunicaciones, microondas, radio VHF.
41.- Área de Cocina.
42.- Área de Esparcimiento.
43.- Área de Sala de Contención.

Nota: la propuesta de edificación (planos) se podrá visualizar en la siguiente liga:

https://drive.google.com/drive/folders/1fOJg4Lga4LFwky2Dy-ABzoVyel9XTIYJ?usp=sharing

Tabla XI. 1 Áreas promedio para cada subsistema del Complejo de Seguridad

No	Subsistema	Unidad	Cantidad	Personal por Unidad	Dimensiones (m)			Área por persona (m^2)
					Largo	Ancho	Altura	
1	Recepción	Recepción	1	1	2.0	1.5	Variable	3.0
2	Oficina de Seguridad	Oficina	1	1	3.0	3.5	2.5	10.5
3	Oficina Técnica	Oficina	1	1	3.0	3.5	2.5	10.5
4	Oficina de Inteligencia	Oficina	1	1	3.0	3.5	2.5	10.5
5	Oficina de Protección Civil	Oficina	1	1	3.0	3.5	2.5	10.5
6	Oficina de Seguridad Pública	Oficina	1	1	3.0	3.5	2.5	10.5
7	Oficina del Comandante	Oficina	1	1	4.0	3.5	2.5	14.0
8	Oficina del Asesor o secretario	Oficina	1	1	4.0	2.5	2.5	10.0
9	Cocineta con área de esparcimiento (v)	Cocina	1	1	4.0	2.5	2.5	10.0
10	Baño Hombre	Baño	1	1	2.0	1.5	2.5	3.0
11	Baño Mujeres	Baño	1	1	2.0	1.5	2.5	3.0
12	Aire Acondicionado	Equipo	1	N/A	3.5	3.5	Variable	12.3
13	Cuarto de energía	Equipo	1	N/A	5.0	5.0	Variable	25.0
14	Cuarto de Equipos de comunicación	Equipo	1	N/A	2.0	2.0	Variable	4.0
15	Centro de datos (SITE, conmutador)	Equipo	1	N/A	2.0	2.0	Variable	4.0
16	Centro de atención telefónica (variable)	Operador	1	1	1.5	2.0	Variable	3.0
17	Centro de Monitoreo (variable)	Operador	1	1	1.5	2.0	Variable	3.0
18	Área de visitas	Cuarto	1	1	1.5	1.5	2.5	2.3

No	Subsistema	Unidad	Cantidad	Personal por Unidad	Dimensiones (m)			Área por persona (m^2)
					Largo	Ancho	Altura	
19	Jefe de turno (oficina)	Cuarto	1	1	3.0	3.5	2.5	10.5
20	Archivo y almacén	Gabinete	1	1	1.0	1.5	2.5	
21	Sala de Juntas	Cuarto	1	1	2.0	2.0	2.5	4.0
22	Circulaciones	Pasillos	1	1	variable	2.0	2.5	variable

5.11.4.2 Requerimientos mínimos para diseño del proyecto ejecutivo de un Complejo de Seguridad

5.11.4.2.1 Recopilación de información

Se debe recopilar la información mínima necesaria correspondiente al **"Proyecto Ejecutivo de los Complejos de Seguridad",** de la cual disponga la dependencia, referente a los siguientes rubros:

I. Ubicación del Predio
II. Estudios Preliminares
   a) Levantamiento topográfico del predio
   b) Estudios Geológicos y Geofísicos
   c) Estudio de impacto ambiental
   d) Documentación que requiere la dependencia para llevar a cabo la gestión de licencias y permisos
III. Cuadro de Necesidades de los Complejos de Seguridad
   a) Volumen promedio de Usuarios y Administrativos del Centro
   b) Volumen promedio de Operadores de Monitoreo
   c) Volumen promedio del Operadores de Llamadas
   d) Requerimiento de espacio para equipos de Fuerza
   e) Requerimiento de espacio para equipos de Telecomunicaciones
   f) Requerimiento de espacio para equipos de Aire Acondicionado
   g) Requerimiento de espacio para equipos del SITE

La información recabada se debe analizar con la finalidad de elaborar un plan de trabajo estratégico, para el desarrollo del proyecto ejecutivo; así como para las visitas y recorridos al predio para verificar y evaluar las condiciones actuales de la zona; además de realizar los estudios preliminares correspondientes.

5.11.4.2.2 Visitas de reconocimiento

Se debe realizar visitas de reconocimiento en la zona en donde se desarrollará el **"Proyecto Ejecutivo del Complejo de Seguridad"**, con la finalidad de ubicar el predio y la delimitación del terreno, los accesos viales y carreteros al predio, así como para identificar los servicios existentes en la zona, el tipo de superficie del terreno (Topografía, Orografía), y evaluar las condiciones actuales del predio, como por ejemplo si hay que retirar basura o escombro. De igual forma se debe identificar las zonas en donde es necesario realizar deshierbe y desmonte o reubicación de árboles.

En los recorridos de reconocimiento se debe ubicar los vértices de la poligonal del terreno en coordenadas geográficas y UTM, así como la orientación del predio con respecto al Norte; estos trabajos de reconocimiento estarán soportados por un anexo fotográfico, a su vez el número de las fotos se identificará en un plano llave del predio.

De igual forma el reconocimiento del predio determinará de manera cualitativa las acciones previas al desarrollo del Proyecto Ejecutivo, así como la propuesta de cantidades de obra y costos.

5.11.4.2.3 Estudios Preliminares

5.11.4.2.3.1 Levantamiento Topográfico

Se debe realizar el levantamiento topográfico determinando la altimetría y la planimetría del terreno, así como las instalaciones existentes en el mismo; la poligonal que se obtenga del levantamiento del predio se georeferenciará con coordenadas WGS 84, empleando un receptor de Sistema de Posicionamiento Global (GPS, por sus siglas en inglés), de una o dos frecuencias geodésicas en tiempo real, con precisión horizontal y vertical de 10 a 50 mm.

La captura de datos y predeterminación de la posición en coordenadas (X, Y) de la poligonal del predio, se debe realizar empleando uno de los siguientes métodos: Estático, Estático Rápido o Diferencial, que permitirá obtener una precisión en la información recolectada.

La información recopilada se debe proyectar en un plano topográfico con el objeto de establecer con precisión la delimitación del terreno por medio de la poligonal, así como su ubicación.

5.11.4.2.3.2 Exploración Geotécnica (Estudio de Mecánica de Suelos)

Se debe de realizar el estudio de mecánica de suelos, en el predio donde se desarrollara el Complejo de Seguridad, considerando los siguientes rubros a realizar para llevar a cabo el estudio:

- Sondeos tipo STP con profundidad de 3.0 a 3.5 m, con lectura del número de golpes de acuerdo a la norma ASTM-D- 1586.
- Toma de muestras alteradas y lecturas de penetración en los estratos de suelo natural.
- Ensayes de laboratorio geotécnico a las muestras tomadas, para propiedades índice.
- Análisis de pruebas de laboratorio, toma de lecturas de penetrómetro.
- Determinación de capacidad de carga y resistencia de suelo.
- Evidencia fotográfica de cada sondeo.

Las investigaciones y estudios del subsuelo a realizar, serán los mínimos necesarios que se requieran, para determinar las propiedades mecánicas del suelo y las condiciones del subsuelo.

I. El número mínimo de exploraciones a realizar (pozos a cielo abierto o sondeos) será de una por cada 80 m o fracción del perímetro, o envolvente de mínima extensión de la superficie cubierta por la estructura en suelos rocosos y de transición, y de una por cada 120 m o fracción de dicho perímetro en suelos lacustres.

II. La profundidad de las exploraciones dependerá del tipo de cimentación y de las condiciones del subsuelo, pero no será inferior a dos metros bajo el nivel de desplante. Los sondeos que se realicen con el propósito de explorar el espesor de los materiales compresibles en los suelos de transición y lacustres deben, además, penetrar en el estrato incompresible al menos 3m y, en su caso, en las capas compresibles subyacentes si se requiriera apoyar pilotes o pilas en dicho estrato.

III. Los procedimientos para localizar rellenos artificiales, galerías de minas y otras oquedades serán directos, es decir basados en observaciones y mediciones en las cavidades o en sondeos. Los métodos indirectos, incluyendo los geofísicos, solamente se emplearán como apoyo de las investigaciones directas.

IV. Los sondeos que se realizarán podrán ser de los tipos indicados a continuación:

a) Sondeos con recuperación continua de muestras alteradas mediante la herramienta de penetración estándar. Servirán para evaluar la consistencia o compacidad de los materiales superficiales de los suelos rocosos y de los estratos resistentes de los suelos de transición y lacustres. También se emplearán en las arcillas blandas de los suelos de transición y lacustres con objeto de obtener un perfil continuo del contenido de agua y otras propiedades índice.

b) Sondeos mixtos con recuperación alternada de muestras inalteradas y alteradas en los suelos de transición y lacustres. Sólo las primeras serán aceptables para determinar propiedades mecánicas. Las profundidades de muestreo inalterado se definirán a partir de perfiles de contenido de agua,

determinados previamente mediante sondeos con recuperación de muestras alteradas.

c) Sondeos consistentes en realizar, en forma continua o selectiva, una determinada prueba de campo, con o sin recuperación de muestras. La prueba podrá consistir en medir:
   - El número de golpes requeridos para lograr, mediante impactos, cierta penetración de un muestreador estándar (prueba SPT) o de un dispositivo mecánico cónico (prueba dinámica de cono).
   - La resistencia a la penetración de un cono mecánico o eléctrico u otro dispositivo similar (prueba estática de cono o prueba penetrométrica). Al ejecutar este tipo de prueba de campo, deben respetarse los procedimientos aceptados, en particular en cuanto a la velocidad de penetración, la cual estará comprendida entre 1 y 2 cm/s.
   - La respuesta esfuerzo–deformación del suelo y la presión límite registradas al provocar en el sondeo la expansión de una cavidad cilíndrica (prueba presiométrica). Este tipo de prueba se considerará principalmente aplicable para determinar las características de los suelos firmes rocosos o de los estratos duros de los suelos de transición y lacustres.
   - La resistencia al cortante del suelo (prueba de veleta o similar). Este tipo de prueba se considerará principalmente aplicable a los suelos blandos de transición y lacustres.
   - La velocidad de propagación de ondas en el suelo. Se podrá recurrir a ensayes de campo para estimar el valor máximo del módulo de rigidez al cortante G, a partir de la velocidad de propagación de las ondas de corte V_s, que podrá obtenerse de ensayes geofísicos de campo como los de pozo abajo, pozo arriba, el ensaye de cono sísmico, el de sonda suspendida o el ensaye de pozos cruzados. En este tipo de pruebas es recomendable emplear un inclinómetro para conocer y controlar la posición de los geófonos para el registro de vibraciones y la de la fuente emisora de vibraciones.
   - Estos sondeos podrán usarse para fines de verificación estratigráfica, con objeto de extender los resultados del estudio a un área mayor. Sus resultados también podrán emplearse para fines de estimación de las propiedades mecánicas de los suelos siempre que se cuente con una calibración precisa y reciente del dispositivo usado y se disponga de correlaciones confiables con resultados de pruebas de laboratorio establecidas o verificadas localmente.

V. Sondeos con equipo rotatorio y muestreadores de barril. Se usarán en los materiales firmes y suelos rocosos a fin de recuperar núcleos para clasificación y para ensayes mecánicos, siempre que el diámetro de los mismos sea suficiente. Asimismo, se podrán utilizar para obtener muestras en las capas duras de los suelos de transición y lacustres.

VI. Sondeos de percusión o de avance con equipo tricónico o sondeos con variables de perforación controladas, es decir sondeos con registros continuos de la presión en las tuberías o mangueras de la máquina de perforar, de la velocidad de avance, de la torsión aplicada, etc. Serán aceptables para identificar tipos de material o descubrir oquedades.

5.11.4.2.3.3 Elaboración de Proyecto Ejecutivo

El desarrollo del proyecto ejecutivo debe contener las memorias de cálculo, planos a detalle, costos y precios unitarios, validación de perito, certificación de instalación y especificaciones técnicas de cada ingeniería; así como también debe contener los estudios preliminares (Levantamiento Topográfico, Estudio de Mecánica de Suelos), el costo total estimado de la ejecución de la obra y manual de documentos que se requieren para la gestión del Estudio de Impacto Ambiental y los permisos y licencias; de igual forma el proyecto ejecutivo debe contener los requisitos mínimos necesarios para el proceso licitatorio y posteriormente la implementación y ejecución; la proyección del proyecto ejecutivo debe considerar los servicios que proporcionará el Complejo de Seguridad, como es el resguardo, preservación y administración de la información y datos obtenidos de los STV.

El diseño de las instalaciones de los Complejos de Seguridad debe considerar los siguientes rubros en la proyección arquitectónica, como mínimo:

- Logotipo del Complejo de Seguridad
- Sistemas de almacenamiento de información
- Sistemas de detección contra de fuego, equipos contraincendios, alarmas
- Sistemas de circuito cerrado de vigilancia
- Sistema eléctrico
- Equipos para de Telecomunicaciones para Operación del CS
- Servicios sanitarios (WC)
- Área de recepción de usuarios
- Oficinas para personal del Centro
- Áreas para operación y consulta de información
- Áreas, espacios y accesos para personas con capacidades diferentes

  - Proyecto Arquitectónico
    - Memoria Descriptiva
    - Elaboración de Anteproyecto
    - Plantas arquitectónicas
    - Elaboración de programa de necesidades
    - Elaboración de organigramas
    - Elaboración de diagramas de flujo
    - Elaboración de diagramas de interrelaciones

- Apuntes perspectivos
- Especificaciones generales
- Propuesta de acabados
- Materiales
- Presupuestos estimados
- Estimación de costos
- Cálculo aproximado del valor de la obra, de acuerdo a los materiales y acabados propuestos, incluyendo números generadores por concepto y cantidades de obra en cifras generales
- Carpeta de especificaciones incluyendo folletos, catálogos, muestras físicas y todo lo necesario para realizar la obra sin dificultad
- Números generadores por concepto y cantidad de obra (catálogo de conceptos)
- Memoria descriptiva del proyecto (incluyendo: ubicación, características del terreno, criterio de solución arquitectónica, análisis general de acabados
- Firma de Responsable o Perito
- Planos detallados
  - Plantas
  - Planta de conjunto
  - Planta de azoteas
  - Plantas arquitectónica
  - Plantas de detalle por área
  - Cortes
  - Corte arquitectónico
  - Cortes por fachada
  - Cortes de detalles constructivos
  - Fachadas
  - Fachadas generales
  - Fachadas interiores
  - Mobiliario
  - Carpintería
  - Herrería
  - Cancelería
  - Acabados
  - Albañilerías
  - Detalles constructivos

➢ Proyecto Estructural (Cimentación y Estructura)
- Memoria descriptiva del proyecto
- Memoria de Cálculo
- Planos de Diseño
- Especificaciones Técnicas

- Catálogo de Conceptos
- Proyecto de cimentación
- Proyecto de superestructura
- Proyecto de subestación
- Revisión de bardas exteriores
- Firma de Responsable y Corresponsable de la Seguridad Estructural

➢ Proyecto de Instalación Hidráulica
- Memoria Descriptiva
- Memoria de Cálculo
- Planos de Diseño
- Especificaciones Técnicas
- Catálogo de Conceptos
- Descripción del proyecto
- Descripción del sistema hidráulico
- Instalación de las redes de tuberías en general
- Ángulo de conexión entre tuberías
- Válvulas de seccionamiento
- Orden de las instalaciones
- Distribución de agua
- Materiales a utilizar en tuberías
- Firma de Responsable o Corresponsable en Instalaciones

➢ Proyecto de Instalación Sanitaria
- Memoria Descriptiva
- Memoria de Cálculo
- Planos de Diseño
- Especificaciones Técnicas
- Catálogo de Conceptos
- Descripción del proyecto
- Descripción del sistema sanitario
- Instalación de las redes de tuberías en general
- Ángulo de conexión entre tuberías
- Válvulas de seccionamiento
- Orden de las instalaciones
- Distribución de tuberías
- Materiales a utilizar en tuberías
- Firma de Responsable o Corresponsable en Instalaciones

➢ Proyecto de Instalación Eléctrica e Iluminación
- Memoria Descriptiva
- Memoria de Cálculo
- Planos de Diseño

- Especificaciones Técnicas
- Catálogo de Conceptos
- Tiempo Estimado de Ejecución
- Firma de Validación de Perito especialista por área

➢ Proyecto de Fuerza y Subestación
- Memoria Descriptiva
- Memoria de Cálculo
- Planos de Diseño
- Especificaciones Técnicas
- Catálogo de Conceptos
- Tiempo Estimado de Ejecución
- Firma de Validación de Perito especialista por área

➢ Proyecto de Sistema de Tierras
- Memoria Descriptiva
- Memoria de Cálculo
- Planos de Diseño
- Especificaciones Técnicas
- Catálogo de Conceptos
- Tiempo Estimado de Ejecución
- Firma de Validación de Perito especialista por área

➢ Proyecto de Celdas Solares
- Memoria Descriptiva
- Memoria de Cálculo
- Planos de Diseño
- Especificaciones Técnicas
- Catálogo de Conceptos
- Tiempo Estimado de Ejecución
- Firma de Validación de Perito especialista por área

➢ Proyecto Aire Acondicionado y Confort
- Memoria Descriptiva
- Memoria de Cálculo
- Planos de Diseño
- Especificaciones Técnicas
- Catálogo de Conceptos
- Firma de Corresponsable en Instalaciones
- Distribución de equipos y ductos en planta
- Distribución de tuberías
- Distribución de drenes
- Cortes
- Ubicación de equipos en planta y azotea

- Detalle de instalación y cuadros de equipos

➢ Proyecto de Sistema contra Incendio
- Memoria Descriptiva
- Memoria de Cálculo
- Planos de Diseño
- Especificaciones Técnicas
- Catálogo de Conceptos
- Tiempo Estimado de Ejecución
- Firma de Validación de Perito especialista por área

➢ Proyecto de Circuito Cerrado de Televisión (CCTV)
- Memoria Descriptiva
- Memoria de Cálculo
- Planos de Diseño
- Especificaciones Técnicas
- Catálogo de Conceptos
- Tiempo Estimado de Ejecución
- Firma de Validación de Perito especialista por área

➢ Proyecto de Control de Acceso
- Memoria Descriptiva
- Memoria de Cálculo
- Planos de Diseño
- Especificaciones Técnicas
- Catálogo de Conceptos
- Tiempo Estimado de Ejecución
- Firma de Validación de Perito especialista por área

➢ Estudio de impacto ambiental
- Carpeta de especificaciones incluyendo folletos, catálogos, muestras físicas y todo lo necesario para realizar la obra sin dificultad.

➢ Proyecto de Automatización
- Memoria Descriptiva
- Memoria de Cálculo
- Planos de Diseño
- Especificaciones Técnicas
- Catálogo de Conceptos
- Tiempo Estimado de Ejecución
- Firma de Validación de Perito especialista por área

➢ Proyecto de Comunicación

- Memoria Descriptiva
- Memoria de Cálculo
- Planos de Diseño
- Especificaciones Técnicas
- Catálogo de Conceptos
- Tiempo Estimado de Ejecución
- Firma de Validación de Perito especialista por área

➢ Documentación para llevar a cabo la Gestión de licencias y permisos

➢ Levantamiento Topográfico
- Elaboración de levantamiento topográfico
- Plantas
- Poligonales
- Niveles
- Cortes
- Alzados
- Sondeos mixtos
- Pozos a cielo abierto
- Recomendaciones de pavimentos
- Recomendaciones y capacidad de carga de cimientos
- Ademados para estudios *Down-Hole*
- Estudios Geo-Hidrológico
- Resistencia del terreno
- Espectro de sitio

5.11.5 Normas Técnicas Complementarias para el Diseño y Construcción de Estructuras de Mampostería

- En la elaboración del concreto y morteros se empleará cualquier tipo de cemento hidráulico que cumpla con los requisitos especificados en la norma **NMX-C-414-ONNCCE**.
- En la elaboración de morteros se podrá usar cemento de albañilería que cumpla con los requisitos especificados en la norma **NMX-C-021**.
- Los agregados deben cumplir con las especificaciones de la norma **NMX-C-111**.
- El agua para el mezclado del mortero o del concreto debe cumplir con las especificaciones de la norma **NMX-C-122**. El agua debe almacenarse en depósitos limpios y cubiertos.
- La resistencia a compresión del mortero, sea para pegar piezas o de relleno, se determinará de acuerdo con el ensaye especificado en la norma **NMX-C-061-ONNCCE**.

- La resistencia a compresión del concreto de relleno se determinará del ensaye de cilindros elaborados, curados y probados de acuerdo con las normas **NMX-C-160** y **NMXC-083-ONNCCE**.
- El refuerzo que se emplee en castillos, dalas, elementos colocados en el interior del muro y/o en el exterior del muro, estará constituido por barras corrugadas, por malla de acero, por alambres corrugados laminados en frío, o por armaduras soldadas por resistencia eléctrica de alambre de acero para castillos y dalas, que cumplan con las normas mexicanas correspondientes.
- Se admitirá el uso de barras lisas, como el alambrón, únicamente en estribos, en mallas de alambre soldado o en conectores. El diámetro mínimo del alambrón para ser usado en estribos es de 5.5mm.
- Se podrá utilizar otros tipos de acero siempre y cuando se demuestre a satisfacción de la administración su eficiencia como refuerzo estructural. El módulo de elasticidad del acero de refuerzo ordinario, se supondrá igual a 2×105 MPa (2×106 kg/cm²); para diseño se considerará el esfuerzo de fluencia mínimo, fy, establecido en las normas citadas.

6 BIBLIOGRAFÍA

1. Adler S., Berglund A., Caruso J., Deach S., Graham T., Grosso P., Gutentag E., Milowski A., Parnell S., Richman J. & Zilles S. 2001. Extensible Stylesheet Language (XSL) Version 1.0. W3C Recommendation 15 October 2001. IBM, Pageflex, Adobe, Sun, Arbortext, Xerox, Compuserve. Recuperado de http://www.w3.org/TR/2001/REC-xsl-20011015/ (PDF by RenderX, XML file, HTML (one large file), ZIP file).

2. Ariganello, E. *Redes CISCO. Guía de estudio para la certificación CNNA Routing y Switching*. 1er edición. Alfaomega Grupo Editor SA de CV, México, junio 2014. ISBN: 978-607-622-171-6.

3. Axis Communications. *Consideraciones sobre ancho de banda y almacenamiento* [en línea]. [Fecha de consulta: 15 de noviembre de 2017]. Disponible en: https://www.axis.com/mx/es/learning/web-articles/technical-guide-to-network-video/bandwidth-considerations.

4. Axis Communications. *Video management systems* [en línea]. [Fecha de consulta: 13 de noviembre de 2017]. Disponible en: https://www.axis.com/mx/es/learning/web-articles/technical-guide-to-network-video/video-management-systems.

5. Axis Communications. *Video management systems* [en línea]. [Fecha de consulta: 13 de noviembre de 2017]. Disponible en: https://www.axis.com/mx/es/learning/web-articles/technical-guide-to-network-video/system-features.

6. Clark J. & De Rose S. 1999. XML Path Language (XPath) Version 1.0. W3C Recommendation 16 November 1999 (Status updated October 2016). Inso Corp. and Brown University. Recuperado de http://www.w3.org/TR/1999/REC-xpath-19991116 (available in XML or HTML).

7. Clark J. 1999. XSL Transformations (XSLT) Version 1.0. W3C Recommendation 16 November 1999. Recuperado de http://www.w3.org/TR/1999/REC-xslt-19991116 (available in XML or HTML).

8. Curbera F., Goland Y., Klein J., Leymann F., Roller D., Thatte S., Weerawarana S. & Satish Thatte. 2002. Business Process Execution Language for Web Services, Version 1.0. 31 July 2002. IBM, BEA Systems, Microsoft. Recuperado de http://download.boulder.ibm.com/ibmdl/pub/software/dw/specs/ws-bpel/ws-bpel1.pdf.

9. Erik Christensen E., Curbera F., Meredith G. &Weerawarana, S., 2001. Web Services Description Language (WSDL) 1.1. W3C Note 15 March 2001. Microsoft and IBM Research. Recuperado de http://www.w3.org/TR/2001/NOTE-wsdl-20010315.

10. Erl, T., (2005), SOA Principles of Service Design.

11. Fallside D. C. &Walmsley P. 2004. XML Schema Part 0: Primer Second Edition. W3C Recommendation 28 October 2004. IBM. Recuperado de http://www.w3.org/TR/2004/REC-xmlschema-0-20041028/.

12. Fine, L. H. *Seguridad en Centros de Cómputo Políticas y Procedimientos.* 2da edición, Trillas, México D.F. 2007. ISBN: 978-968-24-4097-7

13. Foundation, S. S. *Squid-Cache.org* [en línea]. [Fecha de consulta 5 de Octubre 2017] Disponible en: https://wiki.squid-cache.org/SquidFaq.

14. Holstege M. &Vedamuthu A. S. 2010. W3C XML Schema Definition Language (XSD): Component Designators. W3C Candidate Recommendation 19 January 2010. Mark Logic Corporation, webMethods. Recuperado de http://www.w3.org/TR/2010/CR-xmlschema-ref-20100119/.

15. Joyanes Aguilar, L. *Computación de cloud computing en las empresas.* 1era edición, Alfaomega Grupo Editor SA de CV, julio 2012. ISBN: 978-607-707-468-7.

16. KO, Ryan K L, Jagadpramana, Peter, Mowbray, Miranda, Pearson, Siani, Kirchberg, Markus, Liang, Qianhui, LEE, Bu Sung. Trust Cloud: A Framework for Accountability and Trust in Cloud Computing. *2nd IEEE Cloud Forum for Practitioners (IEEE ICFP 2011)* [en línea],22 de junio de 2011, [Fecha de consulta 25 de noviembre]. Disponible en:

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.225.1441&rep=rep1&type=pdf.

17. Lowe, Scott. *Calculate IOPS in a storage array.*[en línea].[Fecha de consulta 20 de noviembre] Disponible en: https://www.techrepublic.com/blog/the-enterprise-cloud/calculate-iops-in-a-storage-array/.

18. Microsoft. 2005. Descripción de la disponibilidad, la confiabilidad y la escalabilidad. Recuperado de: https://technet.microsoft.com/es-es/library/aa996704(v=exchg.65).aspx.

19. Normas Técnicas Complementarias de RCDF.

20. Orchard D. 2007. Guide to Versioning XML Languages using new XML Schema 1.1 features. W3C Working Draft 20 July 2007. BEA Systems, Inc. Recuperado de http://www.w3.org/TR/2007/WD-xmlschema-guide2versioning-20070720.

21. Reglamento de Construcción para el Distrito Federal.

22. Reinosa E.J., Maldonado C.A., Muñoz R., Damiano L.E. & Abrustsky M.A. 2012. Bases de Datos. Ed. Alfaomega. Buenos Aires. 384 p.

23. Sguil. *The Analyst Console for Network Security Monitoring* [en línea]. [Fecha de consulta 17 de Octubre 2017] Disponible en: http://bammv.github.io/sguil/index.html.

24. Stalling, W. *Fundamentos de seguridad en redes. Aplicaciones y estándares.* 2da edición, Pearson Education SA de CV, Madrid, 2004. ISBN: 978-84-205-4002-3.

25. Thompson H. S. 2005. Processing XML 1.1 documents with XML Schema 1.0 processors. W3C Working Group Note 11 May 2005. University of Edinburgh. Recuperado de http://www.w3.org/TR/2005/NOTE-xml11schema10-20050511.

26. Thompson H. S., Beech D., Maloney M. & Mendelsohn N. 2004. XML Schema Part 1: Structures Second Edition. W3C Recommendation 28 October 2004. University of Edinburgh, Oracle Corporation, Commerce One y Lotus

Development Corporation. Recuperado de http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/.

27. Vieites, Á. G. *Enciclopedia de la Seguridad en Informática.* 2da edición, México D.F.: Alfaomega Ra-Ma, 2011. ISBN 978-607-707-181-5.

Referencias legales

1. Bejtlich, R. *El Tao de la monitorización de seguridad en redes* (pág. 730). Pearson Addison Wesley. Madrid, 2005. ISBN: 84-205-4600-3
Disponible en: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips.

2. Leland, M, Knapp, E. *Sound Practice in Intrusion Detection & Prevention using NitroSecurity* [en línea]. [Fecha de consulta 10 de Octubre 2017]. Obtenido de https://www.sans.edu/cyber-research/security-laboratory/article/nitrosecurity-seclab.

3. Moran, G. *Hacking y seguridad en internet.* 2da edición, (pág. 577). Bogotá: Ra-Ma, 2013. ISBN 978-958-762-080-1.

4. Networks, Paloalto. *WHAT IS AN INTRUSION PREVENTION SYSTEM, Intrusion Prevention and Detection System Basics* [en línea]. [Fecha de consulta 7 de Octubre 2017].

5. Secretariado Ejecutivo Del Sistema Nacional De Seguridad Pública. *Norma técnica para estandarizar las características técnicas y de interoperabilidad de los sistemas de video vigilancia para la seguridad pública* [en línea]. P 109-113 y 123-126. [Fecha de consulta 2 de noviembre de 2017]. Disponible en:http://www.secretariadoejecutivo.gob.mx/docs/pdfs/consejo/Norma_tecnica_sistemas_video_vigilancia.pdf.

Apéndice A.- "Pruebas de compatibilidad con la Red Nacional de Radio"

1. Pruebas IP

1.1 Supervisión técnica y grafica de una Red con conectividad IP.
- *1.1.1* Visualizar el sinóptico de una red con conectividad IP (Control Node, Repetidores y Componentes de la red) a través de la aplicación del TMP.
- *1.1.2* Observar de forma gráfica y con colores el funcionamiento de una red con conectividad IP.
- *1.1.3* Presentar en pantalla las cadenas "A" y "B" del Control Node sin alarmas.

1.2 Mostrar la pasarela de datos operando en estado redundante.
- *1.2.1* A través de la aplicación del TMP, visualizar en el sinóptico, la compuerta de datos sin alarmas.
- *1.2.2* Visualizar gráficamente que la pasarela de datos opere con las cadenas "A" y "B", mostrando la situación de sus tarjetas SUP.
- *1.2.3* Identificar la cadena activa de la compuerta de datos.

1.3 Comunicación con llamadas privadas.
- *1.3.1* Establecer llamada privada entre la terminal TR1 con RFSI 1 y TR2 con RFSI 2, bajo la cobertura de un repetidor con conectividad IP.
- *1.3.2* Visualizar en el TWP de la red, la llamada privada en la lista de comunicaciones y los TRX utilizados en el repetidor.

1.4 Comunicación con llamadas múltiples.
- *1.4.1* Establecer comunicación múltiple de TR1 hacia TR2, TR3 y TR4.
- *1.4.2* Visualizar en el TWP de la red, las llamadas privadas en la lista de comunicaciones y los TRX utilizados en el repetidor con conectividad IP.

1.5 Comunicación de grupo local
- *1.5.1* Verificar que los terminales TR1 y TR2 se registran correctamente en el repetidor y reciben el TKG1.
- *1.5.2* Verificar que se establece comunicación cifrada.

1.6 Comunicación de grupo nacional
- *1.6.1* Verificar que las terminales TR1 y TR2 se registran correctamente en el repetidor y reciben el TKG1 (Nacional).
- *1.6.2* Verificar que se establece comunicación cifrada con el Grupo Nacional.

1.7 Creación de una cobertura multired.
- *1.7.1* Por medio del TWP crear una cobertura multired, seleccionando los repetidores de dos redes con conectividad IP.
- *1.7.2* Visualizar cobertura creada.

1.8 Comunicación de grupos multired.
- *1.8.1* Verificar que se establece la comunicación entre terminal TR1 registrado en red con conectividad TDM y TR2 registrado en red con conectividad IP.

1.8.2 Verificar que se activa la fonía en la pasarela de voz.

1.9 Establecimiento de conferencias con redes IP.

1.9.1 Verificar la correcta apertura de sesión del TWP.

1.9.2 Seleccionar dos redes con conectividad IP, unir los grupos y validar la comunicación entre los grupos participantes en la conferencia.

1.10 Validación de cifrado.

1.10.1 Verificar que las terminales TR1 y TR2 están registradas en el repetidor con conectividad IP y tienen comunicación cifrada en una comunicación de grupo y/o llamada privada.

1.11 Llamada de un terminal inscrito en un red TDM a un número erróneo de una Red IP.

1.11.1 Visualizar que en la terminal TR1 se muestra el mensaje "Número incorrecto" cuando la terminal TR1 registrada en una red con conectividad en TDM llama a un número erróneo de una Red con conectividad IP.

1.12 Llamada de una terminal inscrita en una red con conectividad IP a un número erróneo de una Red con conectividad TDM.

1.12.1 Visualizar que en la terminal TR1 se muestra el mensaje "Número incorrecto" cuando la terminal TR1 registrada en una red con conectividad IP llama a un número erróneo de una red con conectividad TDM.

1.13 Establecimiento de Llamadas Privadas entre un terminal inscrito en un repetidor con conectividad IP y un terminal inscrito en un repetidor con conectividad TDM.

1.14 Llamadas simultáneas con radios inscritos en red con conexión IP a terminales inscritos en una red con conexión TDM.

1.14.1 Verificar que la terminal TR1 registrada en la red con conectividad IP llama a la terminal TR5 registrada en Repetidor con conectividad TDM, finalizando la llamada.

1.14.2 Verificar que las terminales TR1 y TR2 registradas en una red con conectividad IP llaman simultáneamente a las terminales TR5 y TR6 registradas en una red con conexión TDM, finalizando la llamada.

1.15 Transmisión de Datos en una red con conectividad IP.

1.15.1 Verificar el envío de mensajes entre terminales bajo la cobertura de repetidor.

1.15.2 Verificar el envío de mensaje SMS a una terminal TR1 registrado en una red con conectividad TDM desde el puesto del operador de la red IP o a otra terminal registrada en la Red IP.

1.16 Pruebas de funcionamiento de los Equipos de Explotación de una Red con conexión IP.

1.16.1 Validar la salvaguarda de la Base de Datos de Explotación.

1.17 Extracción de alarmas y anomalías registradas en la red.

1.17.1 Validar la extracción de alarmas desde la aplicación TMP y generación de anomalías desde la aplicación OMC.

1.18 TMP (Puesto de Administración Técnica).

1.18.1 Visualizar los diferentes elementos que componen el Control Node, así como sus funciones.

1.19 Supervisión de una Célula Radio.

1.19.1 Visualizar el sinóptico de la Célula Radio, describiendo los diferentes elementos que la componen y funciones asociadas.

1.20 Modificación de los elementos de la infraestructura.

1.20.1 Verificar la ejecución del comando de fuera de servicio en los elementos de la infraestructura.

1.21 Puesta en servicio y fuera de servicio de un repetidor de radio y sus elementos.

1.21.1 Verificar la ejecución del comando de Puesta en Servicio y Fuera de Servicio de Elementos de una célula. Visualizando el cambio de estado operacional en los elementos de una célula.

1.22 Reporte de síntesis de alarmas.

1.22.1 Visualizar la síntesis de las alarmas desde el TMP.

1.23 TWP (Puesto de Administración Táctica).

1.23.1 Apertura de sesión en el TWP.

1.23.1.1 Visualizar el sinóptico de la red en el TWP.

1.23.2 Crear un abonado desde el TWP.

1.23.2.1 Visualizar la creación del abonado.

1.23.3 Establecer una comunicación privada y visualizarla en el TWP.

1.23.3.1 Supervisar una llamada privada en el sinóptico de comunicaciones en el TWP y los TRX utilizados en el repetidor.

1.23.4 Establecer una comunicación de Grupo y su visualización en el TWP.

1.23.4.1 Visualizar un TKG creado en la lista de comunicaciones del TWP.

1.23.5 Establecimiento de una comunicación de Merging Mono-RB.

1.23.5.1 Verificar la funcionalidad de unión de grupos de la red con conectividad IP en el TWP.

1.23.6 Actualización de la Base de Datos de Explotación.

1.23.6.1 Verificar la puesta en servicio de un abonado creado en el TWP IP.

1.23.7 Verificar el listado de conferencias desde el TWP.

1.23.8 Listar los grupos elementales de abonados GEA´S y grupos funcionales de abonados GFA desde el TWP.

1.23.9 Ejecutar comandos de generación de diarios de alarmas, comandos y explotación para su obtención.

1.23.10 Generación y visualización de Listado de Abonados.

1.23.11 Ejecutar comandos de generación de diarios de fonía y visualizar su resultado.

1.23.12 Ejecutar comandos de generación de diarios de inscripciones para su presentación.

1.23.13 Listar los abonados inscritos en una célula.

1.23.13.1 Obtener la lista de radios que están registrados en la célula seleccionada.

2 Pruebas TDM-IP

2.1 Pruebas de Comunicación.

2.1.1 Verificar que se establece la llamada entre el terminal TR1 registrado en repetidor con conectividad IP cuando llama a un terminal TR2 registrado en un repetidor con conectividad TDM. La comunicación debe ser cifrada.

2.1.2 Verificar que se establece la llamada entre una terminal TR2 registrado en el repetidor con conectividad TDM con una terminal TR1 registrado en el repetidor con conectividad IP. La comunicación debe ser cifrada.

2.2 Comunicación de grupo TDM-IP/IP_TDM.

2.2.1 Verificar la interacción a través del VGW entre una terminal TR1, registrado en el repetidor conectividad TDM y una terminal TR2 registrado en la red con conectividad IP.

2.3 Establecimiento de conferencias TDM-IP/IP-TDM.

2.3.1 Por medio de la explotación de la red definir una conferencia y establecerla.

2.3.2 Verificar que una terminal TR1 registrada en el repetidor con conectividad TDM y una terminal TR2 registrado en red con conectividad IP en los grupos seleccionados para la conferencia, interactúan en la conferencia establecida.

2.4 Validación de cifrado TDM-IP/IP_TDM.

2.4.1 Establecer una llamada privada cifrada entre una terminal TR1, registrada en una red con conexión TDM y una terminal TR2 registrado en red con conexión IP.

2.4.2 Verificar que los terminales TR1 y TR2 pertenecen al mismo TKG, cada uno registrado en repetidor con conexión TDM y repetidor con conexión IP respectivamente, interactúan y se comunican de manera cifrada.

2.5 Llamada de un terminal inscrito en un Repetidor con conexión TDM a un número erróneo de una Red IP para verificar la comunicación a nivel señalización entre las dos redes.

2.6 Llamada de un terminal inscrito en un Repetidor con conexión IP a un número erróneo de una Red TDM para verificar la comunicación a nivel señalización entre las dos redes.

2.7 Establecimiento de Llamadas Privadas entre un terminal inscrito en un Repetidor TDM y un terminal inscrito en un Repetidor IP externo.

2.7.1 Verificar el funcionamiento entre una terminal TR1 que está registrado en el repetidor TDM y una terminal TR2 registrada en el repetidor IP.

2.8 Prueba de transmisión de datos entre una red con conexión TDM y una red con conexión IP.

2.8.1 Verificar que una terminal TR1 registrada en red con conexión TDM envía mensaje SMS a una terminal TR2 que está registrada en red con conexión IP.

2.8.2 Verificar que el puesto de operador registrado en red con conexión TDM envía mensaje SMS a la terminal TR2 registrada en red con conexión IP.

2.9 Pruebas de funcionamiento de los Equipos de Explotación de la Red con conexión IP, TMP Remoto (Puesto de Administración Técnica).

2.9.1 Verificar la supervisión del Control Node y sus elementos en el sinóptico del TMP.

2.10 Supervisión de una Célula Radio.

2.10.1 Supervisión de la Célula Radio y descripción de sus funciones en el sinóptico del TMP.

2.11 Modificación de los Elementos de la Infraestructura.

2.11.1 Prueba del comando Fuera de Servicio del AC activo de la red.

2.12 Puesta en Servicio y en Fuera de Servicio de un Repetidor Radio y sus Elementos.

2.12.1 Prueba del comando Fuera de Servicio de los elementos de una célula.

2.13 Reporte de Síntesis de Alarmas.

2.13.1 Visualización de alarmas desde el TMP.

2.14 TWP Remoto (Puesto de Administración Táctica).

2.14.1 Apertura de sesión en el TWP.

2.14.1.1 Visualización del sinóptico de la red en el TWP.

2.14.2 Creación de un Abonado.

2.14.3 Establecimiento de una Comunicación Privada y visualización en el TWP.

2.14.3.1 Supervisión de una llamada privada en el sinóptico de comunicaciones en el TWP.

2.14.4 Establecimiento de una Comunicación de Grupo y visualización en el TWP.

2.14.4.1.1 Visualización de un TKG creado en la lista de comunicaciones del TWP.

Centro Nacional de Información