LIBRO: **PRY. PROYECTO**

TEMA: **CAR. Carreteras**

PARTE: ***13. PROYECTO DE SISTEMAS INTELIGENTES DE TRANSPORTE***

TÍTULO: 01. Sistemas Inteligentes de Transporte

CAPÍTULO: *005. Criterios para el Diseño de Sistemas de Centro de Control (Sistema de Procesamiento de Información) de los Sistemas Inteligentes de Transporte*

A. CONTENIDO

Esta Norma contiene los criterios para el diseño del centro de control, de los proyectos de sistemas inteligentes de transporte (ITS por sus siglas en inglés, *Intelligent Transport Systems*) para carreteras, que realiza la Secretaría con recursos propios o mediante un Contratista de Servicios.

B. DEFINICIONES

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

B.1. TIPOS DE PERFILES

B.1.1. Supervisor de línea

Será el responsable de la operación de instalaciones para el sistema inteligente de transporte y la coordinación de todos los operadores del centro de control y operación (CCO). Como tal, el supervisor de Línea tendrá el control y el acceso a toda la información referente a lo que esté pasando en las instalaciones, así como en el centro de control y operación (CCO).

B.1.2. Operador de energía

Responsable de supervisar el sistema eléctrico de transformación y distribución de media tensión, el sistema de tracción eléctrica y el sistema de recepción de energía en alta tensión.

B.1.3. Operador de instalaciones y túnel

Responsable de la supervisión y el correcto funcionamiento de los siguientes sistemas de estación: media tensión, baja tensión, alumbrado y peaje.

B.1.4. Operador de seguridad

Se responsabilizará de la supervisión de los sistemas de seguridad y emergencia ubicados a lo largo del tramo a observar, como son por ejemplo los siguientes: control de accesos, protección contra incendios, videovigilancia, entre otros.

B.1.5. Coordinador de seguridad

Será el responsable y coordinador tanto del área de seguridad como del área de contacto con el usuario. Realizará la coordinación entre operadores del centro de seguridad, así como con entidades externas de seguridad y emergencia.

B.1.6. Operador de atención al usuario

Se responsabilizará de atender las llamadas de información procedentes de los interfonos del tramo a analizar o por parte de los usuarios de la línea, así como de la supervisión de su estado de funcionamiento. En el caso de llamadas con carácter de emergencia, estas serán redirigidas al Área de Seguridad.

B.1.7. Operador de información al usuario

Se responsabilizará de la difusión de mensajes de interés para los usuarios del tramo. Además, se encarga de la supervisión del estado de funcionamiento de los dispositivos pertenecientes a dichos sistemas.

B.1.8. Ingeniero de mantenimiento

En el centro de control y operación (CCO) existirán ingenieros de mantenimiento, cuya función principal será la monitorización y diagnóstico continuo (veinticuatro (24) por siete (7)) de todos los sistemas del tramo a analizar para determinar qué acción de mantenimiento se realizará en cada momento.

B.2. TIPOS DE ROLES

B.2.1. Nivel de observador

No tiene ninguna facultad para manipular u operar los sistemas. Únicamente tendrá acceso a la información de los distintos sistemas y será, como indica su nombre, observador de las situaciones y eventos que tienen lugar en los mismos.

NORMATIVIDAD SCT
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

B.2.2. Nivel de analista

Posee las capacidades del rol de observador y además puede desempeñar las siguientes funciones:

- Obtención de la información de los sistemas.
- Creación de estadísticas y gráficas.
- Análisis de la información para sugerir cambios y mejoras.

B.2.3. Nivel de operador

Permite llevar a cabo todas las operaciones propias de los roles de observador y analista. Además, es responsable de la supervisión de los telemandos que le correspondan (energía, tráfico, sistemas de instalaciones electromecánicas, entre otros.).

B.2.4. Nivel de supervisor

Las facultades asignadas a este rol incluyen las mismas del observador, el analista y el operador y adicionalmente permiten realizar la modificación y restricción de ciertos parámetros accesibles por el operador.

B.2.5. Nivel de administrador

Se distinguen dos categorías con responsabilidades, funcionalidades y capacidades diferenciadas sobre los diferentes sistemas que componen el centro de control y operación (CCO):

- Administrador de los sistemas de control.
- Administrador de sistemas.

B.3. CENTRO DE CONTROL Y OPERACIÓN BASADO EN LA NUBE

Un centro de control y operación basado en la nube hace referencia a un centro de datos donde se virtualiza la infraestructura, a través de la abstracción, la agrupación de recursos y la automatización.

Un centro de procesamiento de datos (CPD) virtual simula la ejecución de un centro de procesamiento de datos (CPD) en un entorno virtualizado. De este modo, se emula un CPD dentro de una máquina virtual, por lo que el CPD no está ligado a un servidor o equipo físico.

B.4. RACK

Un rack es una base, estructura metálica o soporte con dimensiones normalizadas que permite alojar sistemas informáticos y redes de telecomunicaciones principalmente de red en un CPD. La característica principal de este tipo de bastidores es la optimización que se hace del espacio cuando se dispone de varios equipos. Hay que contar que el equipamiento utilizado en centros de procesamiento de datos (CPD) tiene formas y tamaños específicos para ubicarse en estos armarios y ahorrar el mayor espacio posible. La unidad mínima de los racks es conocida como unidad Rack “U”; cada unidad rack equivale a cuatro coma cuarenta y cinco (4,45) centímetros.

B.5 TIPOS DE SISTEMAS DE ALMACENAMIENTO DE DATOS

B.5.1. Almacenamiento de Conexión Directa

COMUNICACIONES
Secretaría de Infraestructura, Comunicaciones y Transportes

Almacenamiento de Conexión Directa (DAS por sus siglas en inglés *Direct Attached Storage*) es un dispositivo de almacenamiento que se conecta directamente a un servidor, puede utilizar el mismo *enclosure* o ser conectado por medio de un cable a otro diferente.

B.5.2. Almacenamiento Conectado en Red

El Almacenamiento Conectado en Red (NAS por sus siglas en inglés, *Network Attached Storage*) es el nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un servidor con computadoras que funcionan como clientes a través de una red (generalmente TCP/IP) o incluso inalámbrica haciendo uso de un sistema operativo optimizado para dar acceso a los archivos almacenados.

B.5.3. Red de Área de Almacenamiento

La Red de área de almacenamiento (SAN por sus siglas en inglés, *Storage Area Network*) es una red de alta velocidad (o subred) que interconecta diferentes tipos de dispositivos de almacenamiento de datos con los servidores asociados para dar servicio a una amplia red de usuarios.

Integra el almacenamiento a través de un único sistema cuyo suministro, asignación y gestión pueden llevarse a cabo de forma centralizada. Los aspectos como la capacidad de almacenamiento, el rendimiento, la administración y la conectividad entre cada dispositivo SAN desempeñan un papel crucial para que la implantación tenga éxito.

B.5.4. iSCSI (Internet SCSI)

Estándar que permite el uso del protocolo SCSI sobre redes TCP/IP. Facilita la transferencia de datos a través de intranets y es una tecnología utilizada para la consolidación de datos de almacenamiento a través de la red Ethernet existente.

B.5.5. Protocolo de Canal de Fibra

El protocolo de canal de fibra (FCP por sus siglas en inglés, *Fibre Channel Protocol*) transporta información en gigabites/segundo, está optimizado para almacenamiento y otras aplicaciones de alta velocidad que necesitan transferir un gran volumen de información entre servidores y dispositivos de almacenamiento.

B.5.6. Canal de Fibra sobre Ethernet

El canal de fibra sobre ethernet (FCoE por sus siglas en inglés, *Fibre Channel over Ethernet*) es una tecnología de red de computadoras que encapsula las tramas de fibra canal a través de redes Ethernet. Esto le permite a FCoE utilizar redes Ethernet de diez (10) Gigabit (o velocidades más altas), preservando el protocolo canal de fibra.

B.6. CAPAS DE RED DE COMUNICACIONES

B.6.1. Capa troncal

Los nodos troncales (NT) operarán como enrutadores de alta capacidad y realizarán el enrutamiento de los paquetes de datos de los servicios soportados a través de las interfaces y enlaces disponibles. La elección de interfaz o enlace en cada nodo será pre-configurada manualmente mediante enrutamiento estático o de forma automática por parte de la propia red a través de enrutamiento dinámico.

B.6.2. Capa de distribución

COMUNICACIONES

La capa de distribución tendrá como finalidad definir las diferentes Redes de área Local (LAN por sus siglas en inglés *Local Area Network*) de las instalaciones, así como gestionar el acceso a la capa Troncal de los diferentes servicios de datos.

La capa de distribución del centro de control y operación (CCO) asumirá las funcionalidades de distribución conectando la capa Troncal de la línea con la capa de acceso del centro de control y operación (CCO). Además, esta capa será la encargada de asumir posibles interconexiones entre las distintas redes.

B.6.3. Capa de acceso

Punto en el que cada usuario/servicio se conecta a la red de comunicaciones.

La capa de acceso de centro de control y operación (CCO) proporcionará acceso a la red de comunicaciones a los principales elementos de control y operación del sistema de monitoreo de instrumentación.

B.7. TIPOS DE CLIMATIZACIÓN

B.7.1. Refrigeración InRow (Entre Racks)

Esta solución se basa en minimizar la mezcla de aire entre pasillos fríos y calientes, consiguiendo mayor eficiencia energética en el centro de procesamiento de datos (CPD), los equipos de refrigeración se instalan entre racks. Estos aspiran el aire del pasillo caliente, lo filtran, enfrían y lo impulsan al pasillo frío.

B.7.2. Refrigeración por pasillos caliente-frío

Esta solución de refrigeración se podrá emplear en centros de procesos con ratios de hasta cinco kilowatts por rack. Esta opción se fundamenta en proyectar aire frio por las rejillas colocadas en los pasillos fríos (piso falso), pasando a su vez a través de los servidores y retornando el aire caliente a los acondicionadores a través de la parte superior de los mismos.

B.7.3. Instalación de cerramiento pasillo frío-caliente

Esta solución de refrigeración se podrá emplear en centros de procesos de datos con ratios de hasta quince (15) kilowatts por rack. Esta opción se fundamenta en la compartimentación del pasillo frío, aportando una distribución óptima en el lado de aspiración de los servidores.

B.7.4. Instalación de climatización complementaria

Esta solución de refrigeración se podrá emplear en centros de procesos de datos con ratios de hasta dieciséis (16) kilowatts por rack. Esta opción se fundamenta en la instalación de equipos de refrigeración en la parte superior del rack, incrementando la capacidad de los sistemas de aire acondicionado actualmente instalados en los centros de procesamiento de datos. Instalación de climatización directa al rack. Esta solución se fundamenta en la instalación de gabinetes refrigerados con climatización directa al rack. Esta opción se podrá emplear en centros de procesos de datos con ratios de dieciséis (16) < kilowatts/rack < veinticuatro (24).

B.7.5. Instalación de cerramiento pasillo frío-caliente y sistema de suelo activo

Esta solución de refrigeración se podrá emplear en centros de procesos de datos con ratios de hasta veinticinco (25) kilowatts por rack. Esta solución se fundamenta en la compartimentación del pasillo frío, y la instalación de un suelo activo que aumenta la capacidad de refrigeración.

B.8. SISTEMA DE PUESTA A TIERRA O TIERRA FÍSICA

COMUNICACIONES

Es un conjunto de elementos formados por electrodos, cables, conexiones, platinas y líneas de tierra física de una instalación eléctrica, que permiten conducir, drenar y disipar al planeta tierra una corriente no deseada.

Un sistema de puesta a tierra consiste en la conexión de artefactos eléctricos y electrónicos a tierra, para evitar que sufran daño, tanto las personas como los equipos, en caso de una corriente de falla.

B.9. SISTEMA DE PARARRAYOS

Son elementos metálicos cuya función es ofrecer un punto de incidencia para recibir la descarga atmosférica y un camino controlado para la conducción y disipación posterior de la corriente del rayo a tierra; se compone de tres partes:

- Pararrayos propiamente dicho.
- Cable o elemento conductor.
- Tierra física, elemento de descarga a tierra.

B.10. GRUPO ELECTRÓGENO

Una planta generadora de energía de respaldo o emergencia es una máquina que mueve un generador de electricidad a través de un motor de combustión interna. Son comúnmente utilizadas cuando hay déficit en la generación de energía eléctrica de algún lugar, cuando son frecuentes los cortes en el suministro eléctrico o para garantizar el funcionamiento del centro de control y operación (CCO) en periodos largos de cortes del suministro de energía principal.

B.11. ARQUITECTURA PEAJE

B.11.1. Nivel de vía

Es la entidad mínima identificable en el sistema y está integrada por los elementos necesarios para permitir y facilitar el cobro del peaje a los usuarios.

B.11.2. Nivel de estación

Compuesto por las vías instaladas en una misma área y formado por los elementos necesarios para recibir y transmitir información a las vías que estén dentro del ámbito de esa estación.

B.11.3. Nivel de gestión

Situado en uno o varios centros de control y operación (CCO) está formado por los elementos necesarios para el tratamiento de la información (consolidación y gestión) y la correspondiente supervisión.

B.12. ZONA DESMILITARIZADA

La zona desmilitarizada (DMZ por sus siglas en inglés, *Demilitarized Zone*) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet.

El objetivo de una zona desmilitarizada DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa, es decir: los equipos locales (hosts) en la DMZ no pueden conectar con la red interna.

COMUNICACIONES

Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

B.13. RED PRIVADA VIRTUAL

La red privada virtual (VPN por sus siglas en inglés, virtual private network) es una tecnología de red que permite establecer una conexión segura de la red local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, encriptación o la combinación de ambos métodos. Un ejemplo es la posibilidad de conectar dos o más oficinas utilizando como vínculo Internet para permitir, a los miembros autorizados del centro de control y operación (CCO), la conexión desde su casa para cierto tipo de actividades que no afecten o impacten la seguridad.

B.14. SISTEMA DE PREVENCIÓN DE INTRUSIONES

Sistema de prevención de intrusiones (IPS por sus siglas en inglés, *intrusion prevention system*) cuya función consiste en poner normas o reglas que permiten restringir el acceso a usuarios, aplicaciones y a computadoras siempre y cuando se detectan que estos están realizando actividades malintencionadas o transfiriendo código malicioso en el tránsito de la red.

Un IPS toma medidas activas para prevenir por completo las intrusiones, dichos sistemas de prevención de intrusiones permiten a los administradores rechazar activamente cualquier actividad considerada como maliciosa por naturaleza.

B.15. SISTEMA DE DETECCIÓN DE INTRUSIONES

Es el proceso de monitorizar redes de computadoras y sistemas en busca de violaciones de políticas de seguridad. Estos sistemas están compuestos básicamente por tres elementos funcionales:

- Una fuente de Información que proporciona eventos de sistema.
- Un motor de análisis que busca evidencias de intrusiones.
- Un mecanismo de respuesta que actúa según los resultados del motor de análisis.

El sistema de detección de intrusiones (IDS por sus siglas en inglés, *intrusion detection system*) realiza dos tareas fundamentales: la prevención y la reacción. La prevención de las actividades de intrusos se realiza a través de herramientas que escuchan el tránsito en la red o en una computadora. Estos programas identifican el ataque aplicando el reconocimiento de patrones (normas) o técnicas inteligentes. Esta labor permite informar de los intentos de ataques o de actividades sospechosas de manera inmediata. El método reactivo se garantiza utilizando programas que básicamente realizan el análisis de archivos de registros en los sistemas. Se trata de detectar patrones de intrusión en las trazas de los servicios red o en el comportamiento del sistema.

B.16. FIREWALL

COMUNICACIONES

Dispositivo físico de seguridad que protege una red de comunicaciones mediante el monitoreo y control del tráfico entrante y saliente basado en una serie de reglas de seguridad predefinidas. Comúnmente se instalan entre una red corporativa y redes más grandes como puede ser Internet.

B.17. PROTOCOLOS DE COMUNICACIÓN

B.17.1. Comunicaciones centro a campo

Las comunicaciones Centro a campo (C2F por sus siglas en inglés *Center to Field)* son comunicaciones de los sistemas inteligentes de transporte que tienen lugar entre un centro de control y uno o varios dispositivos de campo gestionados por ese centro; por ejemplo, los protocolos de comunicaciones de envío de mensajes de actualización del reloj enviados a todos los dispositivos. La mayoría de solicitudes de este tipo implican un servidor central en un centro de control que se comunica con diversos dispositivos de la carretera o vía urbana.

B.17.2. Comunicaciones centro a centro

Las comunicaciones centro a centro (C2C por sus siglas en inglés, *Center to Center*) abarcan todo el dominio del sistema inteligente de transporte correspondiente al intercambio de datos entre computadores ubicadas físicamente en diferentes centros de gestión del transporte (por ejemplo, centros de gestión de tráfico, centros de gestión de tránsito, seguridad pública, centros de gestión de parkings, y así sucesivamente). Las normas C2C permiten este intercambio de datos, especificando qué información intercambian, cómo y cuándo se intercambia, y los mecanismos subyacentes de transporte.

B.17.3. Gestor de red

El gestor de red (NMS por sus siglas en inglés *Network Management System*) es una aplicación o conjunto de aplicaciones que permitirá a los administradores de red administrar los componentes independientes de una red dentro de un marco de administración de red más grande.

C. REFERENCIAS

Son referencia de esta Norma, las siguientes:

Normas oficiales mexicanas:

- NOM-001-SEDE-2012, *Instalaciones Eléctricas* (*utilización*).
- NOM-022-STPS-2015, *Electricidad Estática en los Centros de Trabajo-Condiciones de Seguridad.*
- NOM-025-STPS-2008, *Condiciones de Iluminación en Centros de Trabajo.*
- NOM-28-ENER- 2010, *Eficiencia Energética de Lámparas para Uso General. Límites y Métodos de Prueba*.
- NOM-002-STPS-2000, *Condiciones de Seguridad, Prevención, Protección y Combate de Incendios en los Centros de Trabajo.*
- NOM-154-SCFI-2005, *Equipos Contra Incendios-Extintores-Servicio de Mantenimiento y Servicio de Recarga*.
- NOM-002-STPS-2010, *Condiciones de Seguridad- Prevención, Protección y Combate de Incendios en los Centros de Trabajo*.
- NOM-053-SCFI-2000, *Elevadores Eléctricos de Tracción para Pasajeros y Carga-Especificaciones de Seguridad y Métodos de Prueba para Equipos Nuevos*.
- NOM-001-STPS-2008, *Edificios, Locales, Instalaciones y Áreas en los Centros de Trabajo-Condiciones de Seguridad*.
- NOM-008-ENER-2001, *Eficiencia Energética en Edificaciones, Envolvente de Edificios no Residenciales*.
- NOM-001-STPS-1999, *Edificios, Locales, Instalaciones y Áreas en los Centros de Trabajo-Condiciones de Seguridad e Higiene*.

Normas mexicanas:

- NMX-J-010-1-ANCE-2010, *Conductores dde Aislamiento Termoplástico a Base de Policloruro de Vinilo con Medidas Internacionales- Especificaciones*.
- NMX-J-498-ANCE-2000, *Productos Eléctricos-Conductores-Determinación de Resistencia a la Propagación de la Flama en Conductores Eléctricos Colocados en Charola Vertical-Método de Prueba*.

Normas internacionales:

- ANSI/ASHRAE Standard 62-2001, *Ventilation for Acceptable Indoor Air Quality*.
- ANSI/TIA/EIA 569-A, *Commercial Building Standard for Telecommunication Pathways and Spaces*.
- ANSI / TIA / EIA 942, *Guías de Diseño del Centro de Datos y las Normas de Cableado Estructurado*.
- ANSI/EIA/TIA-568A, *Las Topologías, la Distancia Máxima de los Cables, el Rendimiento de los Componentes, las Tomas y los Conectores de Telecomunicaciones*.
- EIA/TIA 569, *Rutas y Espacios para Cables de Telecomunicaciones en una Edificación*.
- EIA/TIA 606, *Administración de la Infraestructura de Telecomunicaciones para Edificios Comerciales*.
- EIA/TIA 607, *Tierras y Juntas*.

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

- EIA/TIA 570, *Infraestructura de Telecomunicaciones Residencial*.

Norma ISO:

- ISO 11064, *Norma Internacional ISO 11064 (partes 1,2, 3, 4, 6 y 7). Diseño Ergonómico de los Centros de Control*.

Normas del Código Eléctrico Nacional:

- NFPA-70, *National Electrical Code Handbook Eleventh Edition*.
- NFPA-70, *National Electrical Code 2002 Edition*.
- NFPA-70E, *Standard for Electrical Safety in the Workplace 2009 Edition*.
- NFPA 90A, *Standard for the Installation of Air-Conditioning and Ventilating Systems 2002 Edition*.
- NFPA 96, *Standard for Ventilation Control and Fire Protection of Commercial Cooking Operations 2008 Edition*.
- NFPA 72, *National Fire Alarm Code. 2010 edition*.
- NFPA 10, *Standard for Portable Fire Extinguishers*.
- NFPA 101, *Life Safety Code 2012 Edition*.

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

Otros:

- NRF-011-CFE, *Sistema de Tierra para Plantas y Subestaciones Eléctricas*.
- NTP 602, *El diseño Ergonómico del Puesto de Trabajo con Pantallas de Visualización: el Equipo de Trabajo*.
- UNE 23007-14, *Sistemas de Detección y Alarma de Incendios. Parte 14: Planificación, Diseño, Instalación, puesta en Servicio, Uso y Mantenimiento*.
- UNE-EN 13501-2:2004, *Clasificación de los Productos de Construcción y de los Elementos Constructivos en Función de su Comportamiento ante el Fuego. Parte 2: Clasificación a partir de Datos Obtenidos de los Ensayos de Resistencia al Fuego Excluidas las Instalaciones de Ventilación*.

Además, esta Norma se complementa con las siguientes:

NORMAS	DESIGNACIÓN
Criterios para el diseño de sistemas de comunicaciones SIT, Gestor de Red (NMS) ……..	N·PRY·CAR·13·01·003
Cámaras de Video para Reconocimiento de Placas ……..….....	N·EIP·1·01·011
Cámaras de Video para Detección Automática de Incidentes ……..……	N·EIP·1·01·012
Protocolos de Comunicación para Tableros de Señalamiento Cambiable con LED´s …….	N·EIP·2·01·002
Protocolos de Comunicación para Tableros de Señalamiento de Encendido-Apagado con LED´s ……..…..……	N·EIP·2·01·003
Protocolos de Comunicación para Tableros de Señalamiento de Velocidad Variable con LED´s ……..……	N·EIP·2·01·004
Protocolos de Comunicación para Tableros de Señalamiento de Velocidad Real con LED´s ……	N·EIP·2·01·005

Protocolos de Comunicación para Tableros de Señalamiento de Tiempo Estimado de Viaje con LED´s	N·EIP·2·01·006
Protocolos de Comunicación para Cámaras de Video	N·EIP·2·01·010

D. CRITERIOS PARTICULARES PARA EL DISEÑO DE SISTEMAS DE CENTRO DE CONTROL (SISTEMA DE PROCESAMIENTO DE INFORMACIÓN) DE LOS SISTEMAS INTELIGENTES DE TRANSPORTE

D.1. CENTRO DE CONTROL Y OPERACIONES

En este apartado se define la arquitectura de los centros de control y operación (CCO) de instalaciones de sistemas inteligentes de transporte de la Red Nacional de Carreteras, que garantizará la integración de todos los sistemas, con una inteligencia distribuida, redundante y resistente a fallos. Presentará una arquitectura dividida en cuatro niveles, según el siguiente modelo:

- Nivel cero (0) o nivel de campo: Equipos de control UPD (Unidad de periferia distribuida).
- Nivel Uno (1) o nivel de control y comunicaciones: PLC de cielo abierto, túnel, entre otros; redes de comunicaciones multiservicio.
- Nivel Dos (2) o nivel de supervisión y operación: Aplicaciones y módulos de monitorización y telemando del sistema inteligente de transporte.
- Nivel Tres (3) o nivel de organización y explotación de los centros de control y operación (CCO): Manual de Explotación, Plan de Autoprotección y Plan de Mantenimiento.

COMUNICACIONES

D.1.1. Arquitecturas funcionales (Categorización de centros de control y operación en función de la tipología de las infraestructuras a gestionar)

La definición de la jerarquía de los centros de control y operación (CCO) de instalaciones del sistema inteligente de transporte de la Red Nacional de Carreteras, se realiza con base en la propuesta de regionalización citada anteriormente.

Se diseña una jerarquía de intercambio de información en tres niveles, considerándose para ello la funcionalidad a desempeñar por cada uno de los tipos de centros de control y operación (CCO) dentro del proceso de intercambio información.

- Nivel Cero (0).
- Nivel Uno (1).
- Nivel Dos (2).

D.1.1.1. Nivel 0

Los Centros de Control y Operación de instalaciones de sistemas inteligentes de transporte de una carretera o vía urbana de cuota, se consideran dentro del Nivel 0 de la jerarquía mencionada anteriormente, en donde la principal funcionalidad de los mismos es recoger la información del equipamiento de campo.

- Estación de Toma de Datos (ETD).
- Tableros de Mensajes Variables (VMS por sus siglas en inglés Variable Message Sign).
- Cámaras de Videovigilancia.

- Sensores de Variables Atmosféricas en Carretera (SEVAC) (incluyendo visibilidad y condiciones de humedad/congelamiento de la superficie de rodamiento)
- Pago de Peaje y Peaje Electrónico de Peaje (Telepeaje).
- Sistema de Pesaje Dinámico (WIM por sus siglas en inglés Weigh in Motion).
- Lectura de Reconocimiento de Placas (LPR por sus siglas en inglés Licence Plate Recognition).
- Detección Automática de Incidentes (DAI).
- Detectores de Velocidad (CINEMÓMETRO).
- Sistema de Comunicación para Emergencias (SOS).
- Emergencias.

Una vez tratada la información del equipamiento de campo, se difundirá hacia los centros de control y operación (CCO) regional (Nivel Uno (1)).

Asimismo, los propios centros de control y operaciones (CCO) de las carreteras y vías urbanas mes de cuota, serán usuarios de la información generada por los actores involucrados en el proceso de interoperabilidad y de los centros de control y operación (CCO) de jerarquía superior (Nivel Uno (1) y Nivel Dos (2)).

D.1.1.2. Nivel Uno (1)

COMUNICACIONES

Los centros de control y operación (CCO) de instalaciones de sistemas inteligentes de transporte regionales, se consideran dentro del Nivel Uno (1), en los que se recogerá la información de los centros de control y operación (CCO) de las carreteras y vías urbanas es de cuota, para posteriormente difundirla a los actores involucrados en el proceso de interoperabilidad y al centro de control y operación (CCO) Nacional (Nivel Dos (2)).

La información a intercambiar entre los centros de control y operación (CCO) de carreteras y vías urbanas es de cuota y los regionales será:

- Información de situación del tránsito.
- Información de seguridad.
- Información de operaciones de mantenimiento.
- Información de gestión de emergencias.
- Información de equipos del sistema inteligente de transporte.
- Información del equipamiento de peaje.
- Información del equipamiento de telepeaje.
- Información de control de pesajes.
- Información de indicadores de desempeño.
- Información meteorológica.

Asimismo, los propios centros de control y operaciones (CCO) regionales serán usuarios de la información generada por los actores involucrados el proceso de interoperabilidad y por los centros de control y operación (CCO) de jerarquía superior (nivel dos (2)).

En la jerarquía propuesta, los centros de control y operación (CCO) regionales (nivel uno (1)), intercambiarán información que afecte a la operativa de las infraestructuras de otra región, para ello se intercambiarán entre sí la siguiente información:

- Información de situación de tránsito.
- Información de operaciones de mantenimiento.
- Información de seguridad.
- Información de gestión de emergencias.
- Información de meteorología.

D.1.1.3. Nivel Dos (2)

Los centros de control y operación (CCO) de instalaciones de los sistemas inteligentes de transporte nacionales, se consideran dentro del nivel dos (2) de la jerarquía propuesta, en los mismos se recogerá información de los centros de control y operación (CCO) regionales:

- Información de situación del tránsito.
- Información de seguridad.
- Información de gestión de emergencias.
- Información de operaciones de mantenimiento.

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

Los centros de control y operación (CCO) nacionales difundirán esta información a los actores de nivel superior involucrados en el proceso de interoperabilidad. Asimismo, los niveles inferiores de la jerarquía (nivel cero (0) y nivel uno (1)) serán usuarios de la información generada por los actores involucrados de nivel superior y por el centro de control y operación (CCO) nacional.

D.1.2. Distribución de los centros de control y operación en carreteras y túneles

A continuación, se muestra la distribución de los centros de control y operaciones (CCO) dependiendo de la distancia de la carretera o vía urbana y si posee túneles.

- Las carreteras y vías urbanas son a cielo abierto con una longitud menor que doscientos (200) kilómetros y sin túneles carreteros inteligentes (L menor que cuatrocientos (400) metros) en su trazado, se dotarán con un (1) centro de control y operaciones (CCO).
- Las carreteras y vías urbanas son a cielo abierto con una longitud mayor que doscientos (200) kilómetros y sin túneles carreteros inteligentes (L menor que cuatrocientos (400) metros) en su trazado, se dotarán con dos (2) Centros de Control y Operaciones (CCO).
- Las carreteras y vías urbanas son con un (1) túnel carretero inteligente (L mayor que cuatrocientos (400) metros) en su trazado, se dotarán con un (1) Centro de Control y Operaciones.
- Las carreteras y vías urbanas son con más de tres (3) túneles carreteros inteligentes (L mayor que cuatrocientos (400) metros) en su trazado, se dotarán con más de un centro de control y operaciones (CCO).
- Los túneles inteligentes (L mayor que cuatrocientos (400) metros), se dotarán de un (1) Centro de Control y Operación (CCO) situado en las inmediaciones de los túneles.

D.1.3. Distribución de los centros de control y operaciones a nivel regional y nacional

La Secretaría dispondrá de un (1) centro de control y operaciones a nivel regional y dos (2) centros de control y operaciones a nivel nacional.

D.1.4. Funcionalidades del centro de control y operación

A continuación, se describen las características y requerimientos funcionales más importantes a tener en cuenta de los centros de control y operación (CCO):

- Capas físicas: Se definirán los criterios de diseño arquitectónico y ergonomía de los CCO de instalaciones de los sistemas inteligentes de transporte.
- Capas de infraestructura: Se definirán las necesidades y requerimientos funcionales de las instalaciones auxiliares del CCO de instalaciones de los sistemas inteligentes de transporte, criterios eléctricos, alumbrado, protección contra incendios, climatización y ventilación, comunicaciones, seguridad, control de accesos, entre otros.
- Capas operativas: Se definirán las necesidades y funcionalidades operativas de un CCO de instalaciones de sistemas inteligentes de transporte (equipamiento, operación, supervisión, detección, protocolos de actuación, actores).
- Capas de información: Se definirán las instancias, autoridades, estadísticas, protocolos, interfaces de compartición, posteo, políticas de respaldo, seguridad de información, entre otros.
- Arquitecturas de CCO, Hardware y Software: Se definirán arquitecturas de los CCO, el Hardware y Software, considerándose las necesidades de los CCO de instalaciones de los sistemas inteligentes de transporte.
- Seguridad de la información: Se desarrollarán los aspectos a considerar en materia de seguridad.
- Redes: Se establecerán los aspectos básicos a considerar en redes de comunicaciones.
- Gobierno y gestión, explotación de información y referencias de normativa.

D.1.5. Roles y dimensionamiento de operadores

En este capítulo se presentan los distintos perfiles de personal y roles de operación de software a implantar en los centros de control y operación de instalaciones del sistema inteligente de transporte.

D.1.5.1. Perfiles

- Supervisor de línea.
- Operador de energía.
- Operador de instalaciones y túnel.
- Operador de seguridad
- Coordinador de seguridad.
- Operador de atención al usuario.
- Operador de información al usuario.
- Ingeniero de mantenimiento.

D.1.5.2. Roles

El centro de control y operación dispondrá de distintos roles de operación definidos para los operadores de cada área de trabajo, de manera que usuarios distintos dispongan también de distintos privilegios y capacidades dentro del sistema, atendiendo al nivel de responsabilidad que cada uno de dichos usuarios ocupa dentro del centro de control y operación.

Los cinco roles de operación que se definen para cada uno de los telemandos son los siguientes:

- Nivel de observador.
- Nivel de analista.
- Nivel de operador.
- Nivel de supervisor.
- Nivel de administrador.

D.1.6. Estaciones de trabajo

D.1.6.1. Jefes, Supervisores y tipos de operadores

Las estaciones de trabajo de los operadores tendrán los siguientes elementos:

- Estación de trabajo que cumpla con las especificaciones técnicas recomendadas para cubrir con las necesidades y funcionalidades operativas.
- Por lo menos dos (2) pantallas de mínimo cincuenta y ocho coma cuarenta y dos centímetros (8,40) (veintitrés 23 pulgadas) LED y para uso continuo las veinticuatro (24) horas, los siete (7) días de la semana.
- Teclado, USB y ratón.
- Unidad lectora y grabadora de CD/DVD.
- Teléfono de sobre mesa.
- Pupitre de megafonía.

D.1.6.2. Niveles de usuario (accesos)

El sistema contará con elementos de seguridad que permitan la definición de diferentes perfiles de usuario y su nivel de acceso a las aplicaciones. Esto es, se dotará al Sistema de un conjunto de niveles de servicio de uso de los recursos, datos y aplicaciones. Los posibles niveles a definir incluirán los de: operador, supervisor, administrador y observador.

La función de seguridad proporcionará la capacidad de asignar usuarios y grupos a las categorías con acceso a niveles específicos de funcionalidad del software. Cada usuario añadido a un grupo heredará la funcionalidad del grupo.

El sistema dispondrá de un control de acciones de usuario, de esta manera cualquier operador que ingrese al sistema, y generará un registro histórico, así como todas las acciones realizadas.

El sistema permitirá el uso de un firewall a nivel de aplicación de escritorio sin provocar fallos de compatibilidad con las herramientas del sistema operativo.

D.1.6.3. Workstations y pantallas

Se considerarán los monitores y estaciones de trabajo necesarias para explotar satisfactoriamente las instalaciones del sistema inteligente de transporte que se gestionen desde el centro de control y operación (CCO).

D.1.7. Sistema de Pantallas de visualización de imágenes (Videowall)

Las pantallas a instalar en las salas del CCO son de mínimo cincuenta y ocho coma cuarenta y dos (58,42) centímetros (veintitrés (23) pulgadas) Videowall.

En el CCO se dispone de un sistema de visualización compuesto por un Videowall y seis (6) pantallas de mínimo cincuenta y ocho coma cuarenta y dos (58,42) centímetros (23 in). El sistema de visualización permite la vigilancia de las imágenes captadas por las cámaras del sistema de CCTV del tramo.

Se dispondrá en la sala de operaciones de un sistema de visualización basado en Videowall formado por mínimo cuatro (4) pantallas de LCD de ciento dieciséis coma ochenta y cuatro (116,84) centímetros o cuarenta y seis (46 pulgadas) y seis (6) pantallas de LED de cincuenta y ocho coma cuarenta y dos (58,42) centímetros (23 pulgadas).

Un sistema de Pantallas de visualización de imágenes (Videowall) será capaz de visualizar una gran cantidad de datos y dado lo delicado de su aplicación, la elección de una tecnología de visualización adecuada resulta fundamental.

Dada la importancia del despliegue de información en un CCO, las pantallas o módulos dispondrán de redundancia en sus componentes más críticos, sistemas de refrigeración avanzada y calibración a todo color y blanco.

D.1.8. Mobiliario técnico

Dentro de las características que se tendrán en cuenta para diseñar el mobiliario de un CCO se encuentran:

- Fácil configuración y expansión.
- Diseño modular.
- Estructura fuerte y estable.
- Fácil acceso a los equipos y al cableado.
- Completa visibilidad a las pantallas de visualización de imágenes (Videowall).

D.1.9. Equipos auxiliares

En las diferentes salas del CCO se instalarán equipos auxiliares tales como impresora, teléfono fijo IP, fax, porta documentos, entre otros, para poder ejecutar las funciones de los operadores.

D.1.10. Iluminación regulable en sala de operadores

Se diseñará una iluminación general regulable que permita establecer el grado de luminosidad necesario para observar el sistema de Pantallas de visualización de imágenes (Videowall) además de una iluminación puntual incorporada a las mesas de los operadores.

D.1.11. Ergonomía

Debido a que los puestos de los operadores se utilizaran veinticuatro (24) horas es importante que para su diseño se contemple la ergonomía.

D.1.11.1 Para el sistema de pantallas de visualización de imágenes (Videowall) se definirá una correcta distancia de las mesas al mismo, con un ángulo de cono de visión nítida en quince (15) grados respecto de eje al que se le suman a ambos lados treinta (30) grados de giro de cabeza en sentido vertical y cuarenta y cinco (45) grados de giro de cabeza en sentido horizontal.

D.2. UBICACIÓN GEOGRÁFICA DEL CENTRO DE CONTROL Y OPERACIÓN

La ubicación de los centros de control y operación (CCO) cumplirá con funcionalidades básicas que les permitan disponer de infraestructuras y servicios que garanticen su funcionamiento y el acceso a los mismos evitando sobrecostos.

Los criterios funcionales serán los siguientes:

D.2.1. Acceso vial

Tendrán accesos viales a los mismos dentro de los tramos carreteros, se situarán en zonas de fácil acceso y lo más cercano al tramo carretero.

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

D.2.2. Abastecimiento de agua

Se ubicarán preferentemente, cerca de fuentes de abastecimiento de agua, con la calidad suficiente y con la presión necesaria para evitar la instalación de grupos de bombeo de abastecimiento.

D.2.3. Evacuación de agua

Los centros de control y operación dispondrán de acceso a la red de alcantarillado público, con objeto de evitar la instalación de depuradoras.

D.2.4. Suministro eléctrico

Los centros de control y operación se ubicarán en localizaciones de fácil acceso al suministro eléctrico, que eviten grandes inversiones en obra para su suministro.

D.2.5. Red de comunicaciones

Los centros de control y operación, para el correcto desempeño de sus funciones, se ubicarán en zonas con acceso a red de datos de alta capacidad, telefonía y una buena señal de televisión y radio.

D.2.6. Zonas sísmicas, inundables o con desprendimientos

Se recomienda que los CCO se ubiquen en zonas que no sean sísmicas, libres de posibles inundaciones y alejadas de áreas con peligro de desprendimientos o derrumbes.

D.3. DISEÑO ARQUITECTÓNICO Y DIMENSIONAMIENTO DEL CENTROS DE CONTROL Y OPERACIÓN

El diseño de los centros de control y operación (CCO) se regirá por conceptos funcionales, espaciales y ergonómicos que permitan el correcto desempeño de sus funciones garantizando la máxima funcionalidad de los espacios y confort de los operadores y trabajadores del centro.

El dimensionamiento de los centros de control y operación será en función de las infraestructuras a gestionar y operadores de cada centro.

D.3.1. Sala de control y operaciones

El centro de control y operación dispondrá de, al menos, una (1) sala de control y operaciones que permita a los operadores realizar, en condiciones de seguridad y confort, las funciones de monitorización, control y gestión de los sistemas inteligentes de transporte, peaje, telepeaje y demás sistemas gestionados desde el centro de control y operación.

La sala estará dimensionada para alojar las mesas y consolas de los operadores, en función del número de operadores, un sistema de Pantallas de visualización de imágenes (Videowall) para la visualización de las imágenes de video y demás elementos auxiliares necesarios. A su vez, estará dimensionada para poder ser ampliada.

La sala de control y operaciones, será una sala con luminosidad, amplitud y podrá ser libre de columnas u obstáculos que dificulten la visibilidad de los operadores hacia las pantallas de visualización de imágenes (Videowall). A su vez, la propia distribución de las consolas de operadores favorecerá la comunicación visual, gestual y por voz entre ellos.

D.3.1.1. Suelo y techo técnico

Para una correcta canalización del cableado de la sala de control y operaciones con el centro de procesamiento de datos y otras salas técnicas y su conexionado con las consolas de los operadores se instalará piso falso en toda la superficie de la sala.

SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

La altura libre entre piso real y piso técnico (plenum de piso) será de sesenta (60) centímetros como mínimo, debiendo tener una resistencia entre los cuatrocientos cincuenta (450) kilogramos y quinientos (500) kilogramos por pulgada cuadrada, para evitar deflexiones por el peso. El piso falso estará puesto a tierra.

D.3.1.2. Distribución de la sala y visibilidad de las Pantallas de visualización de imágenes (Videowall)

La sala tendrá una distribución amplia, abierta y homogénea, evitando recovecos y ángulos que dificulten la visibilidad y operabilidad de los operadores entre ellos y hacia el Videowall.

D.3.1.3. Otras consideraciones

La sala de control y operaciones estará provista de infraestructuras y servicios que garanticen la seguridad y confort del personal, equipamiento e infraestructura de la misma.

Para seguridad de los operadores y del equipamiento e información gestionada desde la sala se dotará a la misma de un control de accesos y de cámaras de videovigilancia. Estará aislada acústicamente del exterior, disponiendo de una iluminación adaptada a la funcionalidad de la sala. Además, dispondrá de un sistema de climatización.

D.3.2. Centro de procesamiento de datos

El centro de procesamiento de datos (CPD) es el núcleo de concentración de la información del centro de control y operación. En él se localizan los servidores centrales donde se aloja el software de control y gestión de los datos de las infraestructuras del sistema inteligente de transporte gestionadas y explotadas en el centro de control y operación. A su vez, alberga

el equipamiento de red necesario para la interconexión de los equipos y sistemas, así como los equipos de los sistemas propios del centro de control y operación.

D.3.2.1. Criterios de diseño para centro de control y operaciones basados en las instalaciones

A continuación, se muestran varios de los elementos e instalaciones incluidos en el Centro de Proceso de Datos (CPD) que, por su nivel de importancia y participación, deben considerarse en los diseños.

a) Cerramientos, forrado de paredes/tabiques

Tabiquería de placa de yeso laminado resistente al fuego (RF) (según resistencia al fuego que sea aconsejable, RF-sesenta (60), noventa (90), ciento veinte (120) milímetros, entre otros.) formada por una estructura de perfiles de chapa de acero galvanizado de setenta (70) milímetros de ancho, a base de montantes (elementos verticales) colocados cada seiscientos (600) milímetros, y canales (elementos horizontales), a cuyo lado externo se atornillan placas según resistencia al fuego que se vaya a instalar RF-sesenta (60), noventa (90), ciento veinte (120) milímetros, entre otros), placas tipo F contra fuego (FOC) de quince (15) milímetros de espesor, dando un ancho total del tabique terminado de ciento quince (115) milímetros según normativa vigente.

b) Suelo y techo técnico

Suelo técnico: loseta de seiscientos (600) por seiscientos (600) por treinta (30) milímetros, revestimiento superior estratificado, contra cara en aluminio, núcleo aglomerado prensado y cantos perimetrales en policloruro de vinilo (PVC). El suelo técnico elevado está compuesto por baldosas y la estructura que las sustenta. Sus múltiples usos se basan en que por debajo de él puede transitar todo lo que conlleva una instalación en general (cables, tuberías de cualquier tipo, aire acondicionado, entre otros.).

Techo técnico: formado por una estructura de perfiles de chapa de acero galvanizado de veinticuatro (24) milímetros. Ésta, revestida por una lámina prelavada en su cara vista, en color blanco, modulada, basada en perfiles angulares perimetrales, primarios y secundarios, debidamente fijada, formando una cuadrícula de seiscientos (600) por seiscientos (600) milímetros, y sobre la cual se colocan, simplemente apoyados, los paneles de sulfato cálcico acabado en canto recto de seiscientos (600) por seiscientos (600) milímetros y doce (12) milímetros de espesor.

Puerta cortafuegos: Puerta cortafuegos Resistente al Fuego (RF) (según resistencia al fuego que sea aconsejable RF-sesenta (60), noventa (90), ciento veinte (120) milímetros, entre otros.) de gran robustez, derivada de una construcción con chapas de acero zincadas. Todo el proceso de fabricación de la puerta blindada está estudiado hasta el último detalle para ofrecer un gran nivel de comportamiento frente al fuego. La puerta cortafuegos tendrá la siguiente estructura:

- Una/dos hojas.
- Barra Antipánico.
- Mirilla Ojo de Buey.

Su función es la de resistir al incendio con relación a las características de comportamiento al fuego de la norma NMX-C-307-2-ONNCCE-2019, *industria de la construcción-edificaciones-resistencia al fuego de elementos y componentes-parte 2: sellos cortafuego en penetración*.

- Revestimientos y acabados
- Pintura no propagadora del fuego: Las pinturas no propagadoras son resinas y cargas caracterizadas por no propagar el fuego. Están especialmente indicadas en zonas de alto riesgo de incendios, salidas de emergencia o zonas de evacuación. Las pinturas ignífugas, pinturas resistentes al calor o pinturas intumescentes, pueden resistir hasta seiscientos (600) grados centígrados, El equipamiento necesario constará de los siguientes elementos:
- Instalación y configuración de los servidores.
- Despliegue del cableado y configuración de la electrónica de red, pasarelas, encaminadores.
- Segmentación de redes locales y creación de redes virtuales.
- Creación de zonas desmilitarizadas.
- Creación de la red de almacenamiento de la información.
- Creación de los entornos de explotación, pre explotación, desarrollo de aplicaciones, y gestión de red.

D.3.2.2. Distribución y topología de gabinetes de rack

Todo el equipamiento hardware, servidores, equipos de red, equipos de sistemas propios del CCO se alojarán en gabinetes tipo rack, con el dimensionamiento necesario para permitir el acomodo de cables y dejando espacio entre equipos que permitan disipar el calor.

SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

Los gabinetes rack se instalarán alineados y en filas permitiendo una óptima disipación del calor emitido por los equipos alojados y permitiendo espacio para su mantenimiento.

Se evitará que canalizaciones de abastecimiento de agua, fecales, ductos de ventilación o climatización ajenos al centro de procesamiento de datos (CPD), así como canalizaciones eléctricas o de otro tipo ajenas al CPD crucen, o su trayectoria discurra sobre el CPD o se ubiquen incrustadas en el piso o losa sobre la que se localiza el propio CPD, así como apoyadas en sus paredes laterales.

D.3.2.3. Otras consideraciones

El Centro de Procesamiento de Datos (CPD) estará en un área segura y protegida dentro del CCO, primando plantas bajas y evitando zonas inundables, con muros gruesos y robustos y evitando la instalación de ventanas para salvaguardar su integridad y privacidad. Además, estará provisto por un sistema de climatización con la capacidad de enfriamiento, para contrarrestar el calor generado de los equipos y la temperatura ambiente.

Para mayor seguridad se dotará a los sistemas redundancia en el suministro eléctrico, así como sistemas de sistemas de alimentación ininterrumpida (SAI).

D.3.3. Sala de Crisis

En los centros de control y operación (CCO) se diseñará una sala de crisis para la gestión de situaciones de crisis y emergencia, diseñada de forma que se visualice directamente la sala de control y operaciones, el sistema de pantallas de visualización de imágenes Videowall y los operadores.

Dispondrá de una mesa de reuniones dimensionada en función de la categorización del CCO y el número de personas a interactuar. Esta mesa dispondrá de un puesto de trabajo equipado con tomas para el conexionado de energía, voz y datos.

D.3.4. Locales técnicos

Para albergar el equipamiento eléctrico, electromecánico y de comunicaciones necesario para el correcto funcionamiento del Centro de Control y Operación (CCO) será necesario el diseño de varios locales técnicos, entre otros:

D.3.4.1. Local técnico de media tensión

En el caso que el suministro eléctrico de los Centros de Control y Operación (CCO) se realice en media tensión, se proyectará un local técnico para ubicar todo el equipamiento eléctrico de media tensión (celdas, transformadores, baterías de condensadores, contadores, tableros, entre otros). El local técnico de media tensión se diseñará con piso falso practicable para albergar los cables de interconexión entre equipos y los elementos auxiliares necesarios.

D.3.4.2. Local técnico de baja tensión

Se proyectará un local técnico para ubicar todo el equipamiento eléctrico de Baja Tensión (BT) que da servicio al CCO. El local técnico de Baja Tensión se diseñará con piso falso practicable para albergar los cables de interconexión entre equipos y los elementos auxiliares necesarios.

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

D.3.4.3. Local técnico suministro de respaldo

En el caso que sea necesario que el sistema de energía de los CCO disponga de un sistema de respaldo para el suministro eléctrico, se proyectará un local técnico para su ubicación y del equipamiento requerido (tablero de maniobra, grupo electrógeno, entre otros) para su correcta puesta en servicio. El local técnico se diseñará con piso falso practicable para albergar los cables de interconexión entre equipos y los elementos auxiliares necesarios

D.3.4.4. Local técnico electromecánico

Los Sistemas de ventilación, calefacción y aire acondicionado (HVAC por sus siglas en inglés, Heating, Ventilating Air Conditioned), contra incendios, entre otros, dispondrán de un local técnico para su instalación y de todo el equipamiento requerido. El local técnico se diseñará con piso falso practicable para albergar los cables de interconexión entre equipos y los elementos auxiliares necesarios

D.3.5. Cuarto técnico del sistema de Pantallas de visualización de imágenes

Para albergar el equipamiento de gestión y control del sistema de Pantallas de visualización de imágenes (Videowall), y por cuestiones de distancias y operatividad, se recomienda la disponibilidad de una sala técnica en la parte posterior a la pared donde se instalará el Videowall. Estará dimensionada de acuerdo con el equipamiento necesario y disponer de un sistema de climatización que asegure una correcta temperatura y humedad en el interior de la sala.

Para una correcta canalización del cableado del equipamiento se instalará en piso falso en toda su superficie. Las condiciones y especificaciones del suelo técnico serán las mismas que en el resto de las salas técnicas.

D.3.6. Áreas administrativas

Las áreas administrativas se corresponden con la o las salas para el personal administrativo del CCO, dimensionadas en función del personal necesario. Estas salas dispondrán de piso falso para el cableado, así como acceso a la red de voz y datos para el desempeño de sus funciones.

D.3.7. Salas de reuniones

El CCO dispondrá de una sala de reuniones multifuncional. La sala dispondrá de un sistema audiovisual que proporcione inteligibilidad de audio y resolución de video mayor a 1080p, conectividad con otros dispositivos y gestión de medios. Así como mesas, sillas y demás elementos auxiliares dimensionados correctamente.

La sala de reuniones dispondrá de piso falso para el cableado necesario, así como acceso a la red de voz y datos para el desempeño de sus funciones.

D.3.8. Áreas comunes / Cocineta

Se dispondrá de un área de esparcimiento, descanso o cocineta dotada de una barra de apoyo, gabinetes o alacenas con puertas, frigo bar, servicio de café y muebles para el reposo del personal del CCO.

D.3.9. Sanitarios y vestuarios

En los CCO se proyectarán zonas de higiene y riesgos laborales. Se dotará de sanitarios y vestuarios que serán dimensionados en función de la estimación del personal a albergar en el centro de control y operación.

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

D.3.10. Estacionamiento

Se dispondrá de zonas de estacionamiento para los vehículos de los trabajadores tomando en cuenta para el dimensionamiento la cantidad de personal a albergar en el CCO.

D.3.11. Bodega

Se diseñará una bodega en el interior del CCO para salvaguardar equipamiento, material y documentación generada durante la explotación de las instalaciones gestionadas desde el centro de control y operación.

D.3.12. Taller

Se dispondrá de un taller de mantenimiento, donde también se podrán almacenar las herramientas y el material necesario para la reparación de las averías.

El taller dispondrá de piso falso para el cableado necesario, así como acceso a la red de voz y datos y ser suministrado de mesas, herramienta y mobiliario necesario para el desempeño de sus funciones.

D.3.13. Cocheras para vehículos utilitarios

Para salvaguardar y almacenar los vehículos utilizados para el mantenimiento, operación y explotación de las funcionales propias del tramo carretero.

D.4. HARDWARE

En este apartado se establecen los aspectos a considerar en la implementación de un CCO y en la selección del centro de proceso de datos (CPD) a nivel de equipamiento.

D.4.1. Sistema inteligente de transporte

D.4.1.1. SCADA

a) Arquitectura

La arquitectura básica del Hardware está formada por los siguientes elementos:

- Terminales de operación Software de supervisión, control y adquisición de datos (SCADA por sus siglas en inglés, Supervisory Control And Data Acquisition), en los cuales se visualizará la interfaz gráfica donde se monitorearán y controlarán los estados de los activos controlados. Los clientes acceden a la información del servidor SCADA en tiempo real y simultáneamente mediante el bus de comunicaciones de red local.
- Terminales de mantenimiento con el software del índice de evaluación.
- Servidor de Aplicaciones virtualizado en clúster que brinda una redundancia física. Sobre éste se instalarán las máquinas virtuales de los servidores más importantes, como lo son:
- El servidor redundante del sistema Software de supervisión, control y adquisición de datos (SCADA por sus siglas en inglés, Supervisory Control And Data Acquisition)
- El servidor de procesamiento de datos e Intercambio de Información, por ello de la importancia de tener una redundancia física.

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

b) Controlador lógico programable y unidad de terminal remota

El controlador lógico programable (PLC por sus siglas en inglés, *Programmable Logic Controller*) y la unidad de terminal remota (RTU por sus siglas en inglés, *Remote Terminal Unit*) se conectarán físicamente estos equipos para recopilar la información del estado operativo.

D.4.2. Centro de procesamiento de datos (gestión de recursos)

La elección del tipo de Centro de Proceso de Datos (CPD) a implantar en un centro de control y operación (CCO) y dimensionamiento de la arquitectura hardware se realizará con base en:

- La tipología de las infraestructuras a gestionar desde los centros de control y operación .
- Las variables de los sistemas inteligentes de transporte a gestionar desde el centro de control.

A continuación, se describen los tipos de centro de proceso de datos (CPD) y arquitecturas hardware, en función de la tipología de las infraestructuras a gestionar:

D.4.2.1. Tipos de centro de procesamiento de datos (CPD)

a) El Centro de procesamiento de datos (CPD) de nivel elemental dispondrá de la siguiente arquitectura Hardware:

- Clúster de servidores para instalaciones del sistema inteligente de transporte.
- Clúster de servidores para el sistema de peaje.
- Arquitectura de servidores.

Red de almacenamiento masivo para instalaciones: Se especificará una cabina de Red de Área de Almacenamiento (SAN por sus siglas en inglés Storage Area Network) y se dimensionará en función de las necesidades de almacenamiento. La red de almacenamiento se definirá con redundancia de fuentes de alimentación y controladoras de la cabina.

Red de almacenamiento para políticas de respaldo en disco, ésta se dimensionará en función de las instalaciones del sistema inteligente de transporte y Peaje a gestionar desde el CCO.

b) El Centro de procesamiento de datos (CPD) de nivel básico dispone de la siguiente arquitectura Hardware:

- Clúster de servidores para instalaciones del sistema inteligente de transporte.
- Clúster de servidores para el sistema de peaje.
- Arquitectura de servidores.
- En el nivel básico del Centro de Procesamiento de Datos (CPD), se recomienda virtualizar los servidores, con el fin de dotar de mayor disponibilidad a las aplicaciones residentes en los mismos.
- Red de almacenamiento masivo para instalaciones de los sistemas inteligentes de transporte y peaje: Se especificará una cabina para la Red de Área de Almacenamiento (SAN por sus siglas en inglés Storage Area Network) y se dimensionará en función de las necesidades de almacenamiento. La red de almacenamiento se definirá con redundancia de fuentes de alimentación y controladoras de la cabina.
- Red de almacenamiento para políticas de respaldo (Backup) en disco, ésta se dimensionará en función de las instalaciones del sistema inteligente de transporte y Peaje a gestionar desde el centro de control y operación .
- Se diseñará con replicación asíncrona las Redes de Área de Almacenamiento (SAN por sus siglas en inglés Storage Area Network).
- Centro de Procesamiento de Datos (CPD) de Nivel Medio dispone de la siguiente arquitectura Hardware:
- Grupo (Clúster) de servidores para las instalaciones del túnel.
- Clúster de servidores para las instalaciones del sistema inteligente de transporte.
- Clúster de servidores para instalaciones de Peaje.
- Virtualización de servidores.
- Red de almacenamiento masivo para instalaciones del sistema inteligente de transporte, Peaje y Túnel: Se especificará una cabina de Red de Área de Almacenamiento (SAN por sus siglas en inglés Storage Area Network) y se dimensionará en función de las necesidades de almacenamiento. La red de almacenamiento se definirá con redundancia de fuentes de alimentación y controladoras de la cabina.
- Red de almacenamiento para políticas de Backup en disco, ésta se dimensionará en función de las instalaciones del sistema inteligente de transporte y Peaje a gestionar desde el CCO.
- Se recomienda configurar las dos redes de área de almacenamiento (SAN) (sistemas inteligentes de transporte–Túnel y Peaje) de forma que puedan trabajar en modo replicación y en alta disponibilidad.

COPIA NO CONTROLADA
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

c) Centro de procesamiento de datos (CPD) de nivel avanzado dispone de la siguiente arquitectura Hardware:

- Grupo (Clúster) de servidores para las instalaciones del túnel.
- Grupo (Clúster) de servidores para las instalaciones del sistema inteligente de transporte.
- Grupo (Clúster) de servidores para instalaciones de Peaje.
- Virtualización de servidores.
- Red de almacenamiento masivo para instalaciones del sistema inteligente de transporte y Peaje: Se especificará una cabina de área de almacenamiento (SAN) y se dimensionará en función de las necesidades de almacenamiento. La red de almacenamiento se definirá con redundancia de fuentes de alimentación y controladoras de la cabina.
- Red de almacenamiento para políticas de Resaldo (Backup) en disco, ésta se dimensionará en función de las instalaciones de SIT y Peaje a gestionar desde el CCO.
- Se configurarán las dos redes de área de almacenamiento (sistema inteligente de transporte -Túnel y Peaje) de forma que puedan trabajar en modo replicación y en alta disponibilidad.

d) El Centro de procesamiento de datos (CPD) de nivel Alto dispone de la siguiente arquitectura Hardware:

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

- Clúster de servidores para las instalaciones del túnel.
- Clúster de servidores para las instalaciones del sistema inteligente de transporte.
- Clúster de servidores para instalaciones de peaje.
- Virtualización de servidores.
- Red de almacenamiento masivo para instalaciones del sistema inteligente de transporte, peaje y túnel: Se especificará una cabina de área de almacenamiento (SAN)y se dimensionará en función de las necesidades de almacenamiento. La red de almacenamiento se definirá con redundancia de fuentes de alimentación y controladoras de la cabina.
- Red de almacenamiento para políticas de Respaldo en disco, ésta se dimensionará en función de las instalaciones del sistema inteligente de transporte y peaje a gestionar desde el centro de control y operación.
- Se configurarán las dos redes de área de almacenamiento (SAN) (sistema inteligente de transporte -túnel y peaje) de forma que puedan trabajar en modo replicación y en alta disponibilidad.
- Se realizarán replicaciones asíncronas entre los centros de control y operación. En función de las comunicaciones se optará por las siguientes posibilidades:
- Replicación de la información de cada uno de los Centros de control y operación en el resto y en uno centralizado.
- Se diseñarán caminos redundantes de tendido de cableado entre Centros de control y operación, con el fin de dotar de alta disponibilidad a la red de comunicaciones.
- Se especificarán enlaces dedicados de comunicaciones, para realizar mediante VPN el intercambio de información entre centros de control y operación.

- Centro de Procesamiento de Datos (CPD)de Nivel Regional dispone de la siguiente arquitectura Hardware:
- Grupo (Clúster) para la aplicación de intercambio de información.
- Virtualización de servidores.
- Zona desmilitarizada (DMZ por sus siglas en inglés, *Demilitarized Zone*) para el intercambio de información con la información del viajero (Infoviaje).
- Red de almacenamiento masivo para la información (aforos, ingresos, entre otros.) recibida de otros Centros de control y operación, se especificará una cabina para la red de área de almacenamiento y se dimensionará en función de las necesidades de almacenamiento requeridas. La red de almacenamiento se definirá con redundancia de fuentes de alimentación y controladoras de la cabina.
- Red de almacenamiento para políticas de respaldo en disco, ésta se dimensionará en función de las necesidades de almacenamiento requeridas en el centro de control y operación.
- Se recomienda un internet dedicado simétrico para la compartición de información entre los concesionarios con el centro de control y operación regional de la SICT.

  Intercambio de la información: aforos, ingresos, estado de las carreteras y vías urbanas es, incidencias, cortes y mantenimientos, entre otros.

e) Centro de procesamiento de datos (CPD) de Nivel Nacional dispone de la siguiente arquitectura Hardware:

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

- Grupo (Clúster) para la aplicación de intercambio de información.
- Virtualización de servidores.
- Zona desmilitarizada (DMZ por sus siglas en inglés Desmilitarized) para el intercambio de información con Infoviaje.
- Red de almacenamiento masivo para la información (aforos, ingresos, entre otros.) recibida de otros centros de control y operación, se especificará una cabina para la Red de área de almacenamiento (SAN) y se dimensionará en función de las necesidades de almacenamiento requeridas. La red de almacenamiento se definirá con redundancia de fuentes de alimentación y controladoras de la cabina.
- Red de almacenamiento para políticas de Respaldo (Backup) en disco, ésta se dimensionará en función de las necesidades de almacenamiento requeridas en el centro de control y operación.
- En todos los centros de control y operación regionales, se especificarán enlaces dedicados de comunicaciones para el intercambio de información con los centros de control y operación nacionales.
- Se configurarán los dos centros de control y operación nacionales de forma que puedan trabajar en modo replicación y en alta disponibilidad.
- Intercambio de la información: aforos, ingresos, estado de las carreteras y vías urbanas es, incidencias, cortes y mantenimientos, entre otros.

f) Centro de procesamiento de datos (CPD) Local Túnel Inteligente dispone de la siguiente arquitectura Hardware:

- Servidor para la aplicación de túnel y almacenamiento en base datos.

D.4.2.2. Criterios de diseño para centros de control y operación basados en la nube

Los criterios principales de un centro de procesamiento de datos basado en la nube son los siguientes:

- Máquinas virtuales: Despliegue rápido de servidores con posibilidad de ampliar los recursos de sus máquinas al instante y reducción de la afectación al servicio por fallos hardware.
- Gestión centralizada: Panel de gestión para llevar a cabo una gestión multiusuario con asignación individual de roles y cuotas de máquinas desplegadas. Posibilidad de gestionar e integrar la solución con sistemas externos.
- Balanceo de carga: Arquitecturas en alta disponibilidad utilizando múltiples servidores, alojados en el mismo centro de datos virtual, para atender un único servicio.
- Imágenes: Catálogo de sistemas operativos y de plantillas de máquinas y redes virtuales. Posibilidad de importar máquinas virtuales e imágenes ISO.
- Herramientas de seguridad, como protección perimetral, cortafuegos (firewall) y red privada virtual (VPN por sus siglas en inglés, Virtual Private Network) para la gestión de seguridad perimetral, tolerancia a fallos, entre otros.

D.4.2.3. Redundancia y alta disponibilidad

COMUNICACIONES

El centro de procesamiento de datos (CPD) proporcionará tolerancia a fallos mediante la redundancia en dispositivos, contará con dispositivos con las mismas propiedades técnicas para seguir funcionando en caso de falla del equipo principal, sin que se afecte el funcionamiento y su rendimiento.

El TIER o niveles de desempeño para **evaluar** un Centro de Datos (Data Center) es un estándar internacional ideado por el Uptime Institute que básicamente establece cuatro (4) categorías, en función del nivel de redundancia de los componentes que soportan el Data Center.

a) TIER I - Centro de datos básico

Es una instalación que no tiene redundadas sus componentes vitales (climatización, suministro eléctrico) y que por tanto perderá su capacidad de operación ante el fallo de cualquiera de ellas.

b) TIER II - Centro de datos redundante

Los Centros de Datos de esta categoría tienen redundados sistemas vitales, como la refrigeración, pero cuentan con un único camino de suministro eléctrico. componentes redundantes (N+1); es decir, que existe por lo menos un duplicado de cada componente.

c) TIER III - Centro de datos concurrentemente mantenibles

Un Centro de Datos (Data Center) TIER III además de cumplir los requisitos de TIER II, tiene niveles importantes de tolerancia a fallos al contar con todos los equipamientos básicos redundados incluido el suministro eléctrico permitiéndose una configuración Activo / Pasivo.

d) TIER IV - Centro de datos tolerante a fallos

Esta es la clasificación más exigente que implica cumplir con los requisitos de TIER III además de soportar fallos en cualquier de sus componentes que inhabilite una línea (suministro, refrigeración).

D.4.2.4. Equipamiento de red

Se dispondrá de los componentes necesarios como conmutadores, enrutadores y demás dispositivos de red que proporcionen el ancho de banda necesario para el flujo de información generada desde los dispositivos en campo y con otros Centros de Control; además de ser robusta, contará con los elementos necesarios para proporcionar redundancia física y lógica de acuerdo con la topología de red diseñada.

D.4.2.5. Cableado y canalización de comunicaciones

Se dispondrá de una canalización independiente y dedicada para el cableado utilizado para comunicaciones de acuerdo con lo especificado en la norma de cableado estructurado ANSI/EIA/TIA-568A, *Las Topologías, la Distancia Máxima de los Cables, el Rendimiento de los Componentes; las Tomas y los Conectores de Telecomunicaciones*. Las topologías, la distancia máxima de los cables, el rendimiento de los componentes, las tomas y los conectores de telecomunicaciones; así como las propiedades del cable, en función de los requerimientos para el envío de datos.

D.4.2.6. Interfaces de comunicación

El Centro de Procesamiento de Datos dispondrá de los medios necesarios que garanticen la comunicación permanente con los dispositivos de campo y otros centros de control; para su cumplimiento, se podrá hacer uso de medios físicos como fibra óptica e inalámbricos como microondas o enlaces satelitales.

D.4.2.7. Servidores

Las principales características de los procesadores son las dimensiones y velocidades de los buses principales, el mayor número de núcleos, mayor cantidad de memoria caché, y en algunos otros aspectos que les proporcionan un rendimiento y precio superior en comparación con los modelos de uso particular o destinado a estaciones de trabajo.

D.4.2.8. Sistema de almacenamiento de datos

Las principales soluciones para consolidar el almacenamiento serán las siguientes:

- Almacenamiento Directamente Conectado (DAS por sus siglas en inglés, *Direct Attached Storage*).
- Almacenamiento conectado en red (NAS por sus siglas en inglés, Network Attached Storage).
- Redes de Área de Almacenamiento (SAN por sus siglas en inglés Storage Area Network). asociados para dar servicio a una amplia red de usuarios.
- iSCSI (Internet SCSI).
- Canal de fibra (FC por sus siglas en inglés, Fibre Channel).
- Canal de fibra sobre ethernet (FCoE por sus siglas en inglés, Fibre Channel over Ethernet).

Es importante considerar que cualquier solución de almacenamiento para un CCO irá acompañada de una solución de software que permita aprovechar al máximo las funcionalidades de los diferentes tipos de equipos descritos en este apartado.

D.4.2.9. Sistema de respaldo (backup)

Se considerarán las siguientes opciones para respaldo de la información y aspectos técnicos, en el diseño del sistema de almacenamiento:

- Incremental a nivel de bloque: Un sistema sofisticado de copia de seguridad de archivos se basa solamente en copiar los bloques físicos del archivo que ha sufrido algún cambio.
- Incremental o diferencial binaria: El método es similar al Incremental a nivel de bloque, pero basado en reflejar las variaciones binarias que sufren los archivos respecto al anterior backup.
- Versionado del sistema de archivos: El versionado del sistema de archivos se mantiene atento a los cambios del archivo y crea estos cambios accesibles al usuario.
- Copia de seguridad de archivos abiertos – archivos bloqueados: Algunos paquetes de software de respaldos no poseen la capacidad de realizar copias de archivos abiertos. Simplemente comprueban que el archivo esté cerrado y si no lo está lo intentan más tarde.
- Copias de seguridad de bases de datos en caliente: Algunos sistemas de gestión de bases de datos ofrecen medios para realizar imágenes de copias de seguridad de una base de datos mientras esté activa y en uso (en caliente).
- De-duplicación: Esta técnica de respaldo elimina los datos redundantes almacenados, guardando una única copia idéntica de los datos, y reemplazando las copias redundantes por indicadores que apuntan a esa única copia.
- Compresión: La compresión es el mejor método para disminuir el espacio de almacenamiento necesario y de ese modo reducir el costo.
- Cifrado: La alta capacidad de los equipos de almacenamiento desmontables implica un riesgo de perderse o ser robados. Si se cifra la información se puede proteger, aunque esto presenta nuevos inconvenientes. Sistema de Sincronización Horaria (Master clock).

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

D.4.2.10. Detección y extinción de incendios

En las salas de salas de sistemas y servicios (CPD), se instalará uno de los siguientes sistemas de extinción automática actuado mediante un sistema de detección por aspiración, tanto en ambiente como en falso suelo:

- Extinción por agua Nebulizada a alta presión.
- Extinción Automática por gas FM 200.
- Extinción Automática por gas NOVEC 1230.

D.4.2.11. Sistema de monitoreo de temperatura y humedad

En los centros de control y operación (CCO) se monitorizará la temperatura ambiente del centro de procesamiento de datos (CPD) puesto que un sobrecalentamiento en cualquiera de los sistemas puede provocar un fallo de mantenimiento.

Para ello se instalarán sistemas de aire acondicionado en las salas donde se ubica el centro de procesamiento de datos, así como medidas de control de temperatura y humedad. En el caso de los CPD muy grandes, se añadirán medidas de refrigeración líquida, como por ejemplo columnas de agua donde pasa el aire caliente de los racks y se convierte en frio.

D.4.2.12. Control de accesos y sistema de video vigilancia interno

En cuanto al control de acceso a las instalaciones, es importante disponer de circuito cerrado de televisión propio, control de acceso mediante tarjetas de identificación, o cualquier otro tipo de medida como escáneres biométricos para proteger el acceso físico al recinto.

D.4.2.13. Sistema eléctrico especializado

El sistema eléctrico se dotará de un cuadro específico para los servicios de información, comprobando la calidad de la tierra, y dimensionándolo para futuros crecimientos. Los materiales (interruptores, magnetotérmicos, diferenciales, entre otros) se instalarán con las últimas tecnologías para conexiones en caliente.

Se contará con dispositivos SAI (Sistema de Alimentación Ininterrumpida) en casos de fallos eléctricos, que no son más que baterías que son capaces de mantener, durante un tiempo muy limitado, la corriente que llega a todo el Centro de Procesamiento de Datos, o al menos a sus partes más críticas.

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

D.4.3. Red de comunicaciones entre centros de control y operación

La columna vertebral de un centro de control y operación es la red de comunicaciones, conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben (transportan) datos, con la finalidad de compartir información, recursos y ofrecer servicios.

D.4.3.1. Arquitectura de red

La red de comunicaciones basará su funcionamiento en tecnología digital Ethernet TCP/IP a nivel de troncal y distribución, proporcionando una conectividad de extremo a extremo fiable, segura y transparente a todos los servicios de datos de la línea.

Se considerará una única red de transmisión, aunque se podrán identificar ciertas zonas de la propia red con funcionalidades muy específicas. Estas zonas estarán agrupadas bajo el concepto de capa y se identifican en:

- Capa Troncal.
- Capa de Distribución.
- Capa de Acceso.

La arquitectura de red, se compatibilizará para trabajar con la red de comunicaciones de los sistemas inteligentes de transporte.

D.4.3.2. Redundancia y networking

Las redes de comunicaciones serán gestionadas para posibilitar la planificación, organización, supervisión y control de los elementos que forman una red garantizando un nivel de servicio adecuado. Una correcta gestión mejora la disponibilidad y rendimiento de las redes e incrementan su efectividad, los principales conceptos a tomar en cuenta son:

- Configuración: Inicialización de una red, el mantenimiento, la adición y la actualización de sus componentes.

- Contabilidad: Uso eficiente de los recursos, conocer la utilización del sistema y sus servicios para una planificación adecuada.

- Seguridad: Protección de los recursos, generación, distribución y almacenamiento de llaves de seguridad, así como monitoreo y control de acceso logs.

- Fallos: Contemplar la detección, aislamiento, información, solución y seguimiento.

- Desempeño: Generar datos estadísticos del comportamiento y las prestaciones del sistema, para detectar cuellos de botella potenciales y establecer una acción proactiva.

- Se logará un nivel de redundancia igual a N+1 en todos aquellos componentes críticos que afecten la disponibilidad del centro de control y operación.

- Permitir el trabajo remoto.

- Contar con diferentes niveles de autenticación.

- Limitar el acceso a los equipos y nivel de privilegios a los que el usuario requiera tener consolas de administración que puedan ser accedidas sólo desde el centro de control y operación o mediante una VPN con doble mecanismo de autenticación.

CONTROLADO
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

D.4.3.3. Red troncal de fibra óptica

Se establecen los siguientes criterios de escalabilidad:

a) Cableado

- Los cables troncales de fibra óptica, dado que concentrarán el transporte de la totalidad de los servicios de la carretera o vía urbana estarán redundados (instalación existente).
- Todo el cableado de fibra óptica instalado en la carretera o vía urbana proporcionará una amplia protección mecánica, que le permita seguir en operación aún a pesar de impactos o deterioros fruto de un exceso de tracción, aplastamiento o la acción de roedores.
- En el caso de servicios que dispongan de fibras ópticas activas y fibras ópticas de reserva en un mismo cable, en la medida de lo posible harán uso de tubos diferentes. Por tanto, los cables de fibra óptica tendrán una configuración de agrupación de fibras en múltiples tubos.

b) Tendido del cableado

- El cable troncal de fibra óptica principal está instalado por caminos independientes y sectorizados a lo largo de todo el trazado. De este modo, en caso de incidente o incendio se garantizará que solamente un cable pueda ser afectado.
- El tendido de los cableados troncales y verticales de fibra óptica que representen los caminos principales para el transporte de los servicios siempre se realizarán acorde a topologías redundantes, como por ejemplo “tresbolillo” o “anillo”.

- La entrada y salida a cualquier emplazamiento principal (estación, edificio técnico o centro de control y operación) así como a cualquier local técnico de telecomunicación principal será independiente. Por tanto, siempre se garantizarán dos vías de entrada/salida. En caso de no ser posible, se aplicarán los criterios del punto anterior.

D.4.3.4. Nodos/Conmutadoresde comunicaciones

Los equipos empleados y su configuración proporcionarán una baja latencia, que en ningún caso condicionará la tecnología de los sistemas que va a transportar, así como una redundancia de camino ante la caída de cualquier elemento que forme la red.

La capacidad máxima soportada será suficiente para el transporte de toda la información necesaria en la línea con un margen mínimo de un cincuenta (50) por ciento al alza sin necesidad de ampliaciones de hardware, firmware o software. Además, esta capacidad podrá ser ampliada mediante la agregación de múltiples enlaces de alta capacidad de forma que la escalabilidad de la red quede asegurada.

Los Nodos Troncales (NT) operarán como enrutadores de alta capacidad y realizarán el enrutamiento de los paquetes de datos de los servicios soportados a través de las interfaces y enlaces disponibles. La elección de interfaz o enlace en cada nodo será pre-configurada manualmente mediante enrutamiento estático o de forma automática por parte de la propia red a través de enrutamiento dinámico.

Los nodos de distribución (ND) se conectarán mediante enlaces de alta capacidad y estarán interconectados en los extremos a NT.

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

Los nodos de acceso (NA) y el enrutamiento interno y externo serán gestionados por un nodo de distribución. Los nodos de acceso proporcionarán acceso a la red de comunicaciones a los servicios de datos mediante las interfaces necesarias.

D.4.4. Sistemas especiales

En este apartado se describen los diferentes sistemas a implementar en los centros de control y operación, complementarios a los sistemas descritos anteriormente.

D.4.4.1. Sistema de ventilación, calefacción y aire acondicionado

En los centros de control de operaciones se diseñará un Sistema de ventilación, calefacción y aire acondicionado (HVAC por sus siglas en inglés, Heating, Ventilating Air Conditioned) que cumplirá con los requisitos para conseguir que el personal empleado y usuarios, así como los equipos y elementos situados en las distintas áreas técnicas, se encuentren en las condiciones ambientales que la normativa exige.

Los aspectos más relevantes con fuerte incidencia en el medio ambiental creado en el interior de las distintas salas son:

- Temperatura y humedad.
- Calidad del aire (olores, gases, partículas).
- Velocidad del aire.
- Ruido.

Los sistemas de ventilación serán aplicables a aquellas salas en las que se contempla algunas de las siguientes situaciones:

- Estancia de personas por un corto espacio de tiempo y actividades de tipo ligero.

- Ambientes nocivos o molestos.
- Posibilidad de elevación de la temperatura por falta de ventilación.

En cuanto a los Sistemas de Aire Acondicionado/Climatización, éstos serán aplicables a aquellas áreas en las que es necesario mantener o bien condiciones de confort para los empleados y usuarios, o bien unas condiciones ambientales determinadas para los equipos que se encuentran en dichas áreas.

A continuación, se indica el tratamiento a considerar en las diferentes áreas de los centros de control y operación:

a) Áreas ventiladas.

- En estacionamientos subterráneos, aseos y vestuarios y locales técnicos (acometida PCI, contadores, cuartos eléctricos, salas de calderas, centros de transformación, entre otros).

b) Áreas climatizadas:

- Zonas de ocupación habitual (despachos, comedores, oficinas abiertas, salas de reuniones).
- Sala Multifunción.
- Archivos.
- Sala de control.
- Sala de crisis.
- Vestuarios.
- Sala taller.
- Salas electrónicas (salas de racks y UPS, salas de sistemas y servicios).
- Cocineta.

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

En las salas de equipos electrónicos se instalará un sistema de climatización; para su diseño se considerarán las tendencias actuales de instalación de servidores de alta densidad, que presenta desafíos significativos que obligan a utilizar novedosas estrategias de refrigeración, orientadas a incrementar la eficiencia y capacidad de los sistemas de aire acondicionado actualmente instalados en los Centro de Procesamiento de Datos.

El sistema de climatización, se dimensionará en función de la potencia por rack y en base a las siguientes soluciones:

- Refrigeración entre racks (*In–Row*).
- Refrigeración por pasillos caliente-frío.
- Instalación de cerramiento pasillo frío-caliente.
- Instalación de climatización complementaria.
- Instalación de cerramiento pasillo frío-caliente y sistema de suelo activo.

Con el fin de evitar entradas de aire incontroladas, se mantendrán en ligera sobrepresión respecto a áreas circundantes las siguientes áreas:

- Locales de ocupación habitual (despachos, oficinas, salas de reuniones, sala de control, entre otros).
- Áreas generales de circulación.
- Cuartos técnicos (salas eléctricas, sala de racks y UPS, salas de sistemas y servicios, entre otros).

A fin de evitar el escape de olores/gases, se mantendrán en ligera depresión respecto a sus áreas circundantes las áreas siguientes:

- Aseos y vestuario.
- Estacionamientos.

D.4.4.2. Sistemas de detección y extinción de incendios

Para el diseño del sistema de protección contra incendios de los centros de control y operación se tendrá en cuenta, siempre que sea posible, los criterios de la Normativa aplicable.

Las funciones básicas del sistema de protección contra incendios serán las siguientes:

- Prevención de incendios.
- Sectorización.
- Detección y localización.
- Alarmas.
- Extinción del incendio.
- Señalización de rutas de evacuación y elementos de protección.

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

El sistema de protección contra incendios de los centros de control y operación de instalaciones SIT estará formado por:

- Sistema de detección y alarma.
- Sistema de extinción.
- Señalización de elementos de protección y evacuación.

a) Sistema de detección y alarma

En los centros de control y operación se dispondrá de un sistema de detección analógica puntual en todas las áreas, excepto en vestuarios y aseos, en donde no será necesario. Por otra parte, el sistema de detección estará basado en el siguiente equipamiento:

- Detectores iónicos: en zonas con atmósferas limpias y con mantenimiento y limpieza adecuados. En este caso se instalarán en zonas de concurrencia tales como pasillos, oficinas y salas de control.
- Detectores térmicos (Termovelocimétricos): Se instalarán este tipo de detectores en aquellas zonas donde se puedan producir aumentos rápidos de temperaturas.
- Detectores por aspiración: La detección precoz por aspiración permite la detección de fuegos en sus etapas iniciales. Este tipo de detector se instalará en la sala de informática y telemática.

Las centrales se integrarán en la red de comunicaciones y serán las encargadas tanto de realizar la detección, como de realizar la supervisión de los equipos de extinción.

Se instalarán semáforos que nos indiquen el estado de alarma del edificio, pulsadores de alarma y elementos de aviso acústico (sirenas).

b) Sistema de extinción

En los centros de control y operación se dispondrá de un sistema de extinción de incendios siguiendo las exigencias de la normativa aplicable.

En todo el conjunto de los centros de control y operación se situarán extintores y bocas de incendio (BIEs) de acuerdo a la normativa vigente.

- Instalación de Extintores. En las salas de los centros de control y operación se instalarán extintores siguiendo las recomendaciones de la NOM-002-STPS-2000, *Condiciones de seguridad-Prevención y protección contra incendios en los centros de trabajo*, la distancia máxima hasta alcanzar un extintor será de quince (15) metros, por tanto, se ubicarán extintores teniendo un criterio de separación máxima entre ellos de treinta (30) metros. Estos extintores seguirán las condiciones de instalación citadas en el mismo punto (se fijarán a una altura del piso no menor de diez (10) centímetros, medidos del suelo a la parte más baja) y una altura máxima de uno coma cincuenta (1,50) metros, medidos del piso a la parte más alta del extintor).
- Los tipos de extintores que se instalarán en los centros de control y operación serán principalmente de polvo químico ABC para cubrir ampliamente los diferentes tipos de incendios más probables.
- Por último, en lo referente a la eficacia y carga de los extintores, esta será, como mínimo veintiuno (21) A, ciento trece (113) B y C, siendo la carga de seis (6) kilogramos de polvo químico.
- Por su parte, los extintores para protección de riesgos eléctricos tendrán una eficacia mínima de ochenta y nueve (89) B y una carga de cinco (5) kilogramos.
- Instalación de bocas de incendio (BIE). En los centros de control y operación (CCO) se instalarán bocas de incendio (BIEs) y se ubicarán en zonas visibles y, la distancia máxima hasta alcanzar una de ellas sea de veinticinco (25) metros, del mismo modo que con los extintores, esto indica que la separación entre dos (2) BIE será como máximo de cincuenta (50) metros.

c) Señalización de elementos de protección y evacuación

En los centros de control y operación se situarán señales informativas relativas a los equipos de extinción según la normativa aplicable, tales como extintores, BIE, pulsadores de alarma y recorridos de evacuación.

El sistema de protección contra incendios enviará señales para ejecutar acciones sobre los siguientes elementos:

- Compuertas cortafuego (cierre en caso de incendio, excepto en el caso de sistemas de extracción de humo).
- Elevador (parada y apertura de puertas en planta de salida de edificio).
- Ventilación (parada de ventiladores y unidades de tratamiento de aire).
- Sistemas automáticos de extinción (funcionamiento).

D.4.4.3. Control de accesos

En los centros de control y operación se diseñará un sistema de control de accesos que servirá para vigilar el acceso del personal al centro de control y operación, al recinto del edificio y al interior del mismo, como a aquellas salas que alberguen equipos críticos para el funcionamiento de las instalaciones SIT. El sistema de control de accesos estará constituido por dos sistemas:

- Control peatonal.
- Control vehicular.

Ambos sistemas lo conformarán una red de concentradores o CPUs que gestionarán los elementos de identificación, permitirá la apertura de las puertas, o elementos de bloqueo y provocarán alarmas en el caso de ser abiertas sin autorización. La comunicación se realizará mediante comunicación TCP-IP (ETHERNET).

Todo ello estará gobernado por una aplicación que permitirá trabajar con las bases de datos generadas por todos los equipos, dar de alta visitas, jerarquizar los accesos, verificar las rondas de seguridad, así como cumplir con las exigencias del proyecto.

Esta aplicación se integrará dentro de una aplicación de gestión integral de sistemas de seguridad.

COMUNICACIONES
SECRETARÍA DE COMUNICACIONES Y TRANSPORTES

d) Usuarios

Control peatonal. El sistema de seguridad de control de acceso peatonal se diseñará con base en el siguiente equipamiento.

- Torniquete de cuerpo completo en la entrada exterior peatonal que obligara a estar identificado antes de entrar.
- Ventosas magnéticas o rejillas magnéticas en las puertas.
- Tornos de acceso y salida de las oficinas.
- Elementos de identificación: Lectores biométricos de huella con lector de tarjeta de proximidad incorporado y Pulsadores de salida para facilitar el tránsito de personas en las oficinas.

e) Estacionamiento

El sistema de seguridad de control acceso vehicular, se diseñará con base en el siguiente equipamiento:

- El sistema de control vehicular está regido igualmente por CPU's que controlan tanto entrada como salida.
- Bolardos electro neumáticos de alta seguridad como primer elemento en el acceso al recinto.
- Barrera vehicular como segundo elemento que impedirá el libre acceso y permitirá la revisión del vehículo si se considera necesario.
- Sistema de lector de huella para el control de la barrera.
- Lazos de detección de vehículos con su correspondiente detector de canal para bucles inductivos.

D.4.4.4. Voz y datos

En los centros de control y operación se diseñará una red local de voz y datos que permitirán la comunicación dentro de los mismos entre sus diferentes dependencias y con las redes públicas de los operadores.

En los mismos se proyectará un sistema de telefonía e interfonía IP, motivo por el que se diseñará una red de datos con el Hardware (servidor, centralita IP, enrutador de servicios integrados) necesario para gestionar conjuntamente el tratamiento de datos, telefonía IP, Interfonía IP y conexión pública a Internet.

El tendido vertical de cableado estructurado se llevará a cabo a través de bandejas dedicadas a comunicaciones y dispuestas en los registros.

El tendido horizontalmente, y para dar servicio a cada toma de datos de usuarios, se llevará a cabo a través de bandejas dedicadas a comunicaciones y dispuestas por el piso falso del edificio, o en su defecto por el falso techo.

Todo el cableado estructurado de los centros de control y operación se realizará con cable de par trenzado (UTP por sus siglas en inglés, *Unshielded Twister Pair*) categoría (CAT) CAT seis (6) o siete (7). El hardware de la red de datos del centro de control y operación estará alimentado del sistema de alimentación ininterrumpida (UPS) del propio edificio.

Finalmente, el cableado estructurado soportará la comunicación mediante paquetes de datos, telefonía y video IP, basados en tecnología Ethernet 100/1000, asimismo soportará el estándar de la IEEE, 802.3af para alimentación eléctrica de equipos en la red Ethernet, así como permitir la interconexión de equipo activo compatible para redes de área local (LAN) en edificios.

D.4.4.5. CCTV interno

Se diseñará un sistema de video vigilancia basado cámaras fijas o PTZ (Por sus siglas en inglés, Pan-Tilt-Zoom) con pre posicionamientos de tecnología IP para la vigilancia de las siguientes dependencias de los centros de control y operación:

- Zona perimetral a los centros de control y operación.
- Accesos y salidas de vehículos del recinto del edificio.
- Acceso al edificio desde el interior del recinto.
- Zona de estacionamiento exterior.
- Acceso y zona de estacionamiento interior del edificio.
- Acceso a escaleras y elevadores.
- Vestíbulos y pasillos del edificio.
- Las funcionalidades básicas del sistema de video vigilancia serán las siguientes:
- Selección de imágenes captadas por una cámara determinada para ser visualizadas en un monitor.
- Selección de imágenes captadas por varias cámaras para ser visualizadas simultáneamente.
- Secuenciación de las imágenes captadas por un grupo de cámaras.
- Grabación de las imágenes captadas por una o varias cámaras.

- Reproducción de grabaciones de seguridad de cualquier cámara.
- Gestión de alarmas y anomalías que se puedan producir en el sistema.

La totalidad de las cámaras se conectarán mediante cable UTP categoría seis (6) o siete (7) a la red de datos local del edificio, la transmisión de imágenes se almacenará en un grabador digital de vídeo. Igualmente se podrá diseñar que las imágenes de las cámaras de seguridad se almacenen en el Hardware de almacenamiento masivo de instalaciones del sistema inteligente de transporte.

El grabador digital de vídeo dispondrá de una interfaz de red Ethernet para comunicación vía protocolo TCP/IP a través de la red de datos local del edificio, con el servidor de los sistemas de seguridad.

Desde la aplicación de gestión integral de la seguridad se podrán monitorizar y controlar desde un único PC el sistema de cámaras, conjuntamente con el resto de sistemas de seguridad.

D.4.4.6. Megafonía

En función del tipo de centro de control y operación, se valorará en el diseño de sistema de control de accesos la instalación de un sistema de megafonía, como complemento al sistema de interfonía.

D.4.4.7. Telefonía e interfonía

COMUNICACIONES

En los centros de control y operación, se diseñará un sistema de interfonía que estará asociado al control de accesos y permitirá la comunicación desde cada uno de los interfonos repartidos en los accesos a los centros de control y operación, en el edificio y en las distintas dependencias del mismo, con la sala de control o personal de seguridad.

El sistema se basará en una solución IP, con micrófono de alta sensibilidad, altavoz, pulsador de llamada y unidad de comunicación. Los interfonos dispondrán de una interfaz que permitirá su conexión directa a la red local del edificio mediante cableado UTP categoría seis (6), UTP categoría siete (7) o fibra óptica en aquellos casos en las que la distancia a cubrir con el cableado este por encima de los noventa (90) metros.

D.4.4.8. Red de televisión y radio

En los centros de control y operación se diseñará un sistema de red de televisión y radio, proporcionando señal de radiotelevisión pública en la diferente toma previstas de los edificios, se diseñará una instalación de radio y televisión formada por tres grandes bloques:

- Equipamiento de captación de señales de radiodifusión.
- Cabecera de procesado y amplificación.
- Red de distribución.

El objetivo de esta red será el de proporcionar los siguientes servicios:

- Televisión digital terrestre o analógica (configurable).
- Radio FM analógica.

Cada una de las antenas se conectará mediante cable coaxial, preferentemente de baja atenuación, con los equipos que conforman la cabecera de procesado y amplificación de señal.

Para el diseño de la red de televisión y radio se considerará la normativa aplicable.

D.4.4.9. Instalaciones electromecánicas

Se instalará un sistema de transporte vertical (elevador) en los centros de control y operación (CCO), en función de la tipología y necesidades del edificio.

D.4.5. Sistema eléctrico

La instalación eléctrica del centro de control y operación se dimensionará en función de las necesidades técnicas y operativas, así como de las partidas presupuestarias destinadas para su implantación, además el diseño considerará la normativa aplicable y los siguientes bloques diferenciados:

- Alimentación de red con doble suministro en media tensión, con apoyo de un Sistema de Alimentación ininterrumpida para la alimentación de los servicios críticos en caso de emergencia.
- Alimentación de red con suministro simple de media tensión con el apoyo de una planta de emergencia y un sistema de alimentación ininterrumpida para la alimentación de los servicios críticos en caso de emergencia.
- Alimentación de red en baja tensión con el apoyo de una planta de emergencia y un Sistema de Alimentación ininterrumpida para la alimentación de los servicios críticos en caso de emergencia.
- Alimentación de red en baja tensión con el apoyo un sistema de alimentación ininterrumpida para la alimentación de los servicios críticos en caso de emergencia.

D.4.5.1. Media tensión

Cuando el suministro eléctrico de los centros de control y operación de instalaciones se realice en media tensión, se proyectará un local técnico para ubicar todo el equipamiento eléctrico de media tensión (celdas, transformadores, baterías de condensadores, contadores, tableros, entre otros). El local técnico de media tensión se diseñará con piso falso practicable para albergar los cables de interconexión entre equipos y los elementos auxiliares necesarios.

D.4.5.2. Baja tensión

Cuando el suministro eléctrico de los centros de control y operación se realice en media o baja Tensión, se proyectará un local técnico para ubicar todo el equipamiento eléctrico de BT (tableros de BT, UPS's, grupos electrógenos, entre otros). El local técnico de baja tensión se diseñará con piso falso practicable para albergar los cables de interconexión entre equipos y los elementos auxiliares necesarios.

a) Cuadro de transferencia y protección

Cada una de las salas del centro de control y operación dispone de un cuadro de transferencia y protección. Este cuadro protegerá las protecciones eléctricas de los tableros de baja tensión, del alumbrado de las distintas zonas en el centro de control y operación, circuitos independientes por zonas, entre otros.

b) Sistema de alumbrado e iluminación

El sistema de alumbrado e iluminación permite aportar la iluminación necesaria en el centro de control y operación (CCO). Para ello este sistema de alumbrado e iluminación irá asociado al suministro eléctrico de Media o Baja Tensión.

El sistema de alumbrado e iluminación estará diferenciado por zonas, siendo así, la iluminación diferente según, la zona en la que se esté trabajando, por ejemplo: sala de Pantallas de visualización de imágenes (Videowall), sala de control, entre otros.

D.4.5.3. Sistema de alimentación ininterrumpida

Los sistema de alimentación ininterrumpida (UPS), se conectarán a la alimentación de los equipos especializados de un centro de control y operación (CCO) como pantallas de visualización de imágenes (Videowall), servidores, computadoras, permitiendo usarlas varios minutos en el caso de que se produzca un corte eléctrico y en tanto entra en operación la planta generadora de energía de respaldo o emergencia permitiendo con esto eliminar cualquier posible afectación al servicio brindado por los centros de control y operación.

Los UPS instalados en el centro de control y operación aportarán suministro eléctrico durante treinta (30) minutos.

D.4.5.4. Grupo electrógeno

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

Se considerarán las siguientes clasificaciones de las plantas de emergencia para la implementación dentro del CCO:

a) De acuerdo al tipo de combustible

- Con motor a gas (LP) o natural.
- Con motor a gasolina.
- Con motor a diesel.
- Sistema Bifuel (diesel/gas).

b) De acuerdo a su instalación

- Estacionarias.
- Móviles.

c) Por su operación

- Manual.
- Semiautomática.
- Automática (ATS).
- Automática (sincronía/peak shaving).

d) Por su aplicación:

- Emergencia.
- Continua.

D.4.5.5. Cableado y canalización eléctrica

La distribución de las canalizaciones en el centro de control y operación (CCO) se diseñará pensando en disponer de una óptima distribución del cableado de datos, eléctrico y tuberías. Por ello, se recomienda que el espacio entre el piso falso y el piso firme sea como mínimo de sesenta (60) centímetros, con el fin de facilitar los trabajos de tendido de cableado hacia los equipos.

La instalación de las canalizaciones se realizará en los siguientes niveles:

a) Primer nivel

Canalización destinada para cableado de datos.

b) Segundo nivel

Canalización para el cableado eléctrico.

c) Tercer nivel

Tuberías de agua de las manejadoras de aire acondicionado.

Las canalizaciones serán de aluminio y cumplirán con lo establecido en los estándares ANSI/TIA/EIA-569 para espacios y canalizaciones para telecomunicaciones, con el fin de evitar la influencia de campos magnéticos o materiales trasmisores de electricidad.

Las canalizaciones se dimensionarán en función de las necesidades de espacio que requieran el cableado de energía y comunicaciones para dar servicio al equipamiento del centro de control y operación (CCO).

La ocupación de las tuberías conduit se regirá por lo indicado en la Tabla 1 del capítulo 10 de la NOM-001-SEDE-2012, *Instalaciones Eléctricas (utilización).*

Se recomienda que la ocupación en charolas siga las indicaciones de la Tabla 1 del capítulo 10 de la NOM-001-SEDE-2012, *Instalaciones Eléctricas (utilización).*

La charola de datos no puede ir a una distancia inferior a quince (15) centímetros de la charola de energía, con objeto de evitar la inducción eléctrica que generan los cables eléctricos sobre el cableado de comunicaciones y evitar que este fenómeno interfiera en el modo de operación.

D.4.5.6. Sistema de tierras y pararrayos

a) Sistema de tierras

Se proveerá de un sistema de puesta a tierra según lo expuesto en la norma NOM-001-SEDE-2012 *Instalaciones Eléctricas (Utilización).*

b) Sistema de pararrayos

Se proveerá de un sistema de protección contra descargas eléctricas atmosféricas de acuerdo con lo especificado en la norma NOM-022-STPS-2015, *Electricidad Estática en los Centros de Trabajo-Condiciones de Seguridad*, y contará con un sistema de puesta a tierra independiente y exclusivo para el sistema.

D.5. SOFTWARE

En este apartado se definen las necesidades software de los Centros de Control y Operación (CCO), considerando sus necesidades,

D.5.1. Peaje y telepeaje

Dentro de los sistemas de peaje, se diferenciará entre:

- Sistema de telepeaje.
- Sistema de peaje.

D.5.1.1. Arquitectura telepeaje

Los niveles de procesado de información para el telepeaje:

a) Punto de cobro (PC)

Donde se realiza la captura de la información y se genera la Transacción Primaria.

b) Nivel central o centro de operaciones (COP)

Donde se centraliza la información y la operación del sistema.

c) Atención a clientes o centro de atención al cliente (CAC)

Donde se procesa la información y se mantiene la relación con los usuarios.

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

El nivel de generación de la información es identificado como el nivel de “Punto de Cobro”, y el nivel de procesado es denominado como “Nivel de Gestión”, compuesto este último por el “Centro de Operación” y el “Centro de Atención al Cliente”.

D.5.1.2. Arquitectura peaje

En el peaje canalizado se consideran los siguientes niveles de procesado de información:

- Nivel de vía (NV).
- Nivel de estación (NE).
- Nivel de gestión (NG).

D.5.1.3. Niveles de peaje en centro de control y operación

De los niveles de peaje descritos en los apartados anteriores, el nivel central o centro de operaciones (COP) del peaje electrónico, el nivel de gestión (NG) del peaje canalizado y el nivel de atención a clientes o centro de atención al cliente (CAC), son los niveles que se encuentran en el centro de control y operación

Las características básicas del sistema en general y de los niveles de centro de control y operación en particular son:

- Seguro y fiable.
- Se utilizarán estándares abiertos, en la medida de lo posible.
- El sistema será interoperable tanto desde el punto de vista de varios centros trabajando de forma conjunta, como de múltiples sistemas de peaje operados desde las mismas plataformas de gestión.

- Estará basado en una tecnología madura y probada. Los sistemas se basarán en productos existentes ya probados y perfectamente adaptados.
- El sistema utilizará Hardware y Software modular y estructurado.
- El sistema será económicamente competitivo.
- El sistema tendrá el mínimo impacto medioambiental posible.
- Homogeneidad de tecnologías y componentes.
- El Software suministrado será cien (100) por ciento compatible con los otros subsistemas con los cuales se integrará.
- Capacidad para no saturarse o bloquearse en la hora de máxima demanda (Hora Pico).
- Fiabilidad y redundancia. Para algunos sistemas no se considera el desarrollo de redundancias, pero se considerará el funcionamiento autónomo de los equipos.
- Escalabilidad del sistema. Los sistemas se diseñarán de forma que sean altamente escalables y modulables.
- Mantenimiento. Los sistemas incluirán una herramienta específica a través de una aplicación para la administración y mantenimiento del sistema.

En los siguientes apartados se recogen los módulos y características mínimas que cumplirá el software de los sistemas de peaje.

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

D.5.1.4. Módulos centro de operaciones del peaje electrónico, el nivel de gestión del peaje canalizado

La plataforma software del centro de operaciones se concibe de forma modular, de forma que se garantice la flexibilidad.

Constará de los siguientes módulos:

- Módulo de interfaz (IHM).
- Módulo de tratamiento de las transacciones.
- Módulo de operación del sistema.
- Módulo de procesamiento de infractores.
- Módulo de monitorización del sistema de cobro.
- Módulo de reportes e informes.
- Módulo de auditoría.
- Módulo de gestión de base de datos.
- Módulo de respaldo (Back–up).

D.5.1.5 Módulos centro de atención al cliente

El sistema de atención a clientes se basará en un diseño sólido con aplicaciones fácil de usar, eficiente y completamente auditable.

La plataforma de atención al cliente responderá a un diseño modular y flexible, permitirá posibles cambios futuros en las políticas, procedimientos y operaciones del sistema de cobro, además de permitir integrar nuevas concesiones.

El sistema tiene que dejar huella de cualquier modificación y posibles ingresos para la conciliación de datos.

Constará de los siguientes módulos:

- Módulo de atención al cliente.
- Módulo de tratamiento de infractores.
- Módulo de facturación, recaudación y cobro de morosos.
- Módulo de auditoría.
- Módulo de informes.
- Módulo de Back–up.
- Módulo de promoción y mercadotecnia (marketing).
- Módulo de administración de cuentas y clientes.
- Módulo de monitorización y mantenimiento.

D.5.1.6. Interfaces con sistemas externos

El sistema de peaje se relacionará para un adecuado funcionamiento con otros sistemas.

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

- Registro nacional de vehículos.
- Con emisores de tarjetas mediante ficheros ".TXT". Los archivos contendrán toda la información necesaria.
- Con entidades bancarias.
- Con empresas de cobranza.
- Con empresas de impresión y facturación

D.5.1.7. Módulo back office de peaje y telepeaje

En los centros de control y operación con instalaciones de peaje y telepeaje, se proyectará una sala de Back Office, con el software necesario en función de la estimación del personal a ubicar en la misma.

D.5.2. Sistemas inteligentes de transporte

A continuación, se definen las necesidades y requerimientos del software de los sistemas inteligentes de transporte de los centros de control y operación.

B.5.2.1. Sistema de supervisión y adquisición de datos

Un Sistema de ventilación, calefacción y aire acondicionado (HVAC por sus siglas en inglés, *Heating, Ventilating Air Conditioned*) se empleará para monitorizar, operar y mantener desde un software especialmente diseñado para su uso en computadoras.

Las funciones de un sistema SCADA son:

- Monitorizar procesos físicos o químicos.
- Gestión del servicio mediante la automatización de los actuadores.
- Mantenimiento a través de la detección de fallos recurrentes.

- Proporcionar información necesaria para el control de calidad.
- Procesamiento de datos y comparación con datos anteriores, para asegurar la fiabilidad del sistema.
- Visualización gráfica dinámica del sistema, para que el operador pueda tomar decisiones con una interface más amigable y a través de la generación de informes.
- Generación de alarmas personalizadas al obtener datos fuera del rango aceptable predefinido.
- Programación de eventos, como pueden ser la generación de informes mensuales o estadísticas.
- Almacenar información histórica para análisis llevados a cabo a posteriori, que permita mejorar la toma de decisiones y detectar problemas recurrentes.
- Evaluación de datos espaciales mediante la integración de Sistemas de Información Geográfica.

SCADA es la base de cualquier centro de control y operación. Abarca todos los aspectos de monitoreo, control y operación.

El SCADA contará con los siguientes módulos:

- Módulo de operación del sistema inteligente de transporte.
- Administración del sistema inteligente de transporte.
- Gestión de históricos.
- Módulo de gestión de planes.
- Módulo de gestión de incidencias.
- Gestión de los sistemas de túneles.
- Sistema de Información Geográfica (GIS).
- Interfaz humano máquina (HMI por sus siglas en inglés, Human Machine Interface).
- Módulo de ayuda al usuario.
- Módulo de gestión de mantenimiento.

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

D.5.2.2. Sistemas de seguridad, vigilancia y control

En el centro de control y operación se incluirán los sistemas de las instalaciones de seguridad que se indican a continuación:

- Sistemas de video vigilancia.
- Sistema de seguridad.
- Sistema de control de accesos.
- Sistema de interfonía.
- Sistema de megafonía.
- Sistema de protección contra incendios.
- Sistema HVAC
- El centro de control y operación contará con un software específico para la gestión de estos sistemas, ya sea de manera independiente o de manera conjunta centralizando toda la gestión y monitoreo en una única herramienta de software.

En los centros de control y operación se diseñará un sistema de seguridad que servirá para vigilar la zona perimetral, exterior e interior del edificio. El sistema de seguridad de un centro de control y Operación, se diseñará con base en el equipamiento de software descrito en los siguientes apartados.

D.5.3. Centro de procesamiento de datos

A continuación, se describen los recursos informáticos utilizados en el Centro de procesamiento de datos.

D.5.3.1 Virtualización de servidores

En los centros de control y operación se optará por la virtualización del siguiente equipamiento Hardware:

- Servidores.
- Grupo (Clúster) de servidores.
- Procesadores de carriles de Peaje.

D.5.3.2 Paquetes de programas informáticos para oficina

Se consideran herramientas ofimáticas del paquete tales como procesador de texto, hoja de cálculo, correo electrónico, plataforma de videollamadas, entre otras para el desempeño de las funciones de los operadores del CPD.

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

B.5.3.3 Softwares de gestión empresarial

El software será desarrollado preferentemente con herramientas de software libre y no propietarias, en caso contrario se considerarán aplicaciones con estándares abiertos que permitan la integración con herramientas de software libre.

D.5.3.4 Sistema de sincronización horaria (Reloj maestro)

Todos los elementos que forman parte del sistema de interoperabilidad estarán sincronizados con un error inferior a un segundo, con el objetivo de que cualquier evento registrado y fechado en alguno de los subsistemas pueda ser analizado en correspondencia con otros eventos de otros centros de control y operación (CCO), manteniendo la integridad de la información.

D.5.3.5 Sistema de almacenamiento de datos

La aplicación utilizará como repositorio de datos cualquier sistema de gestión de base de datos de alta difusión. Las fuentes de datos incluirán, pero no se limitarán a datos de eventos, incidentes, accidentes, telepeaje, datos de los sensores de tráfico y datos meteorológicos. Se garantizará que el repositorio central de datos contiene los datos más recientes, contemplando la integridad de la información.

Los datos recogidos del sistema actualizarán las tablas de la base de datos tan pronto como se reciban los datos y el contenido disponible por cada solicitud en cualquier período de tiempo será obtenido desde la misma fuente de información.

La gestión y explotación de la base de datos del sistema se realizará con apoyo de las herramientas existentes del propio gestor, incluidas dentro de la instalación del modelo de datos, a través de interfaces remotas desarrolladas para tal efecto.

D.5.3.6 Sistema de Respaldo (Backup)

El software de gestión del sistema de almacenamiento integrará de forma automática las funciones de respaldo y recuperación, de archivo y recuperación, gestores de jerarquía de almacenamiento y recuperación de desastres.

Esta aplicación permitirá reducir los costos en hardware por la gestión que realiza sobre los recursos de almacenamiento, y ahorros potenciales de red y mejora de la disponibilidad con soluciones sin “Redes de área local (LAN por sus siglas en inglés, *Local Area Network*).

D.5.4. Sistemas especiales

El centro de control y operación contará con un software específico para la gestión de los sistemas especiales, ya sea de manera independiente o de manera conjunta centralizando toda la gestión en una única herramienta o en herramientas software compartidas por varios sistemas.

La gestión y control de los equipos, así como los eventos y alarmas que puedan producir se centralizarán en el sistema SCADA. Se gestionarán y monitorizarán los siguientes subsistemas a través del NMS:

- Sistemas de circuito cerrado de televisión.
- Sistema de control de accesos.
- Sistema de interfonía y telefonía.
- Sistema de megafonía.
- Sistema de protección y detección de incendios.

COMUNICACIONES
RA, COMUNICACIONES Y TRANSPORTES

También se llevará a cabo la gestión y el control de los estados del sistema eléctrico y el sistema HVAC.

D.5.5. Controlador de Pantallas de visualización de imágenes

El controlador de las Pantallas de visualización de imágenes (Videowall) se ubicará en el centro de control y operación, en la misma sala donde esté instalado el Videowall.

Las funcionalidades que el software será capaz de ejecutar, se enlistan a continuación de manera descriptiva, más no limitativa:

- Será accesible desde cualquier puesto de operación. Todos los puestos de operación podrán eliminar señales o información presente, agregar nuevas fuentes, desplazar o modificar las existentes de forma simultánea, en tiempo real y sin ningún tipo de interferencia entre puestos
- Será capaz de representar en la terminal que esté siendo utilizada para su control, una imagen esquemática simulada del conjunto de pantallas; en el podrá mostrarse toda la información y señales presentes en el conjunto de pantallas, visualizando el contenido íntegro del mural (incluyendo datos y señales RGB y video)
- Cualquier cambio de posición o forma de las imágenes o información presentes en las pantallas se reflejará en todas las terminales que se estén utilizando para realizar el control de las pantallas en tiempo real.

- Dispondrá de una interface gráfico intuitivo que permite eliminar fácilmente señales o información presente, agregar nuevas fuentes, desplazar o modificar las existentes de forma simultánea, en tiempo real y sin ningún tipo de interferencia entre puestos.

- Dispondrá de las funciones arrastrar y soltar (Drag & Drop). El usuario podrá añadir una nueva fuente simplemente seleccionándola de la lista de posibles fuentes, arrastrándola y eligiendo la zona donde quiera que sea posicionada.

- Una vez colocadas las ventanas todas son libremente desplazables y podrá cambiarse su tamaño.

- Será capaz de manejar distintos tipos de fuente, como señales de video compuesto, señales gráficas entre otras.

- Registrará la posición y tipo de la diferente información presente para crear un escenario.
1Seguridad en redes y comunicaciones

Se recomienda dividir (segmentar) la red de acuerdo a una agrupación lógica pensada en grupos de trabajo que comparten recursos y servicios entre sí.

La división se realizará a través del uso de VLANs o ruteadores que establecen la segmentación necesaria, por ejemplo, para los centros de control y operación (CCO) algunas divisiones recomendadas son:

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

- Red local centros de control y operación (CCO).
- Sistemas inteligentes de transporte
- Sistemas de Peaje y Telepeaje.
- Red de almacenamiento.
- Red de backoffice.
- DMZ o servidores de web públicos (extranet).

D.5.5.1. VLAN

La definición y configuración de las VLAN's se llevará a cabo en los conmutadoresy enrutadores mediante software. En estos equipos se efectuarán reservas de puertos para cada VLAN definida según las subredes de cada sistema.

Las características de las VLAN son las siguientes:

- Segmentan lógicamente la infraestructura física en distintas subredes (dominios de difusión), de forma que las tramas de difusión sólo son conmutadas entre puertos de la misma VLAN.
- Pueden aumentar la seguridad de la red, definiendo cuáles son los nodos de la red que se pueden comunicar entre sí.
- Pueden agrupar los puertos de los nodos en grupos lógicamente definidos.
- Se pueden agrupar puertos de diferentes nodos de la red.
- Capacidad de transportar la información de las VLAN a través de los nodos de las redes de comunicaciones.

D.5.5.2. Zona desmilitarizada

La zona desmilitarizada (DMZ por sus siglas en inglés, *Demilitarized Zone*) se configurará para ubicar servidores que es necesario que sean accedidos desde fuera (internet), como servidores de correo electrónico, Web y DNS.

En la arquitectura y puesta en marcha de la red de comunicaciones del centro de control y operación (CCO) se considerará la seguridad de la red como el pilar en el cual se basará la estrategia de protección.

D.5.5.3. VPN

Para cualquier tipo de acceso remoto, se asegurarán las conexiones externas (VPN, SSL, SSH–2) utilizando sistemas de autenticación como por ejemplo los protocolos de autenticación: RADIUS (acrónimo en inglés de Remote Authentication Dial-In User Service) o TACACS TACACS (acrónimo de Terminal Access Controller Access Control System.

D.5.5.4. IPS

Se considerarán los siguientes tipos de IPS para su implementación en ciberseguridad:

- Detección basada en firmas.
- Detección basada en políticas.
- Detección basada en anomalías.
- Detección a través de un sistema trampa (honeypot).

COMUNICACIONES
SECRETARÍA DE COMUNICACIONES Y TRANSPORTES

D.5.5.5. Sistema de detección de intrusos IDS

Se contemplará un sistema de detección de intrusos (IDS por sus siglas en inglés, *Intrusion Detection System*) para la supervisión de la red de comunicaciones, para ello se considerarán los siguientes lineamientos mínimos:

- No supondrá una carga para la red de comunicaciones ni para los servidores.
- El sistema funcionará de forma automática
- No causará incompatibilidades con el resto del software instalado en el centro de control.
- Tendrá la capacidad de identificar de dónde vienen los ataques a la red de comunicaciones.

D.5.5.6. FIREWALL

Se considerará la instalación de un firewall dentro del centro de procesamiento de datos (CPD).

D.5.5.7. Plan de continuidad de negocio

Incluirá planos de las instalaciones de trabajo, los medios y formas de comunicar información crítica a los empleados, servicios de telefonía, estaciones de trabajo / servidores para reanudar las operaciones y los procedimientos para la restauración del CCO al estado anterior.

El plan de continuidad de negocio (BCP por sus siglas en inglés, *Bussines Continuity Plan*) se compondrá a su vez de procesos y procedimientos que describan cómo la organización puede operar durante o inmediatamente después de una emergencia. El BCP describirá cómo gestionar cualquier incidencia que afecte al centro de control y operación (CCO) interrumpiendo o deteniendo su operativa normal, no sólo en caso de grandes desastres. Un aspecto a tener en cuenta es que un plan de continuidad de negocio no es un lugar donde se describe pormenorizadamente cómo solventar cada problema que nos podamos encontrar durante un incidente.

El BCP contará con la protección de los servicios de misión crítica que permita restablecer los servicios a un nivel completamente funcional lo más rápido y fácil posible.

D.5.5.8. Seguridad de la información

Los sistemas de Seguridad de los centros de control y operación se dimensionarán en función de las necesidades técnicas y operativas de los mismos.

D.5.6. Comunicaciones

Además de lo citado en esta Norma, la presentación del proyecto se llevará a cabo de acuerdo a lo estipulado en la Norma N·PRY·CAR·13·01·003, *Criterios para el diseño de sistemas de comunicaciones SIT, Gestor de Red (NMS)*

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

Permitirá monitorizar componentes de software y hardware en la red. Permitirá registrar los datos de los puntos remotos de una red para llevar a cabo informes centrales a un administrador del sistema.

El gestor facilitará las siguientes tareas:

- Descubrimiento de los dispositivos de red.
- Supervisión de los dispositivos de red.
- Análisis de rendimiento de la red.
- Gestión de dispositivos de la red.
- Notificaciones inteligentes o alertas personalizables.

D.5.6.1. Protocolos de comunicación

Considerará una comunicación basada en protocolos abiertos, no propietarios para la comunicación desde el centro de control y con los elementos de campo (C2F por sus siglas en inglés, *Center to Field*), y con otros centros de control (C2C por sus siglas en inglés, *Center to Center*), cumpliendo con el protocolo de intercambio de información (SNMP por sus siglas en inglés, *Simple Network Management Protocol*) y con los protocolos de comunicación establecidos en las normas NTCIP correspondientes.

D.6. PROCESAMIENTO E INTERCAMBIO DE LA INFORMACIÓN

Se desarrollará un proceso para el intercambio de información identificando los siguientes pasos a tomar:

- Identificación de los actores involucrados.
- Especificación de la regionalización de la red nacional de carreteras.

- Especificación de la jerarquía de los centros de control y operación.

- Identificación de los grupos de información a compartir entre los actores involucrados.

Una vez definido lo anterior el intercambio de información cumplirá las siguientes funcionalidades:

- Distribución de la información. Se definirá una lista de distribución, en la que se especifiquen las instancias, autoridades, centros de control y operación y la información a distribuir o intercambiar entre los mismos.

- Protocolos de intercambio de información. Se especifican para el intercambio de información estándares NTCIP (C2F y C2C) que ofrecen mayor flexibilidad y opciones para los organismos que operan los sistemas de gestión del transporte.

- Arquitectura hardware para el intercambio de información. Las arquitecturas de los centros de control y operación dispondrán de una DMZ (zona desmilitarizada), sobre la que se implementará el intercambio de información de forma segura entre centros de control y operación y demás organismos involucrados.

- Interfaces para el intercambio de datos y video. Se especifican diferentes posibilidades de formatos para el intercambio de datos (web services) y video (codec-decodec).

- Interfaces Web ESPAÑOL (*INGLES*). Se indica que los centros de control y operación de Concesionarios dispondrán de una web ESPAÑOL (*INGLES*) pública para información de los usuarios de la vía, así como una web privada para los clientes del peaje.

- Documentación para la Seguridad de la Información. Se definen las funcionalidades que contemplará un plan de contingencia, que será el instrumento de gestión para el buen manejo de las tecnologías de la información y de las comunicaciones.

DOCUMENTO DE CONSULTA
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

D.6.1. Identificación de los actores involucrados en el intercambio de información

Primeramente, se identificará a los actores involucrados en el intercambio de información, que estarán implicados en la gestión y explotación de las autopistas de la Red Nacional de Carreteras.

Los actores identificados en el proceso de intercambio de información, se clasifican según la siguiente tipificación:

D.6.1.1. Dependencias y organismos públicos

Se distinguen los siguientes organismos:

- Secretaría de Infraestructura, Comunicaciones y Transportes (SICT).
- Dirección General de Planeación de Centros SiCT.
- Unidad de Tecnologías de la Información y Comunicaciones (UTIC).
- Secretarías de Seguridad Pública/ Federales / Estatales / Municipales / Policía.
- Guardia Nacional.
- Secretaría de Gobernación (SEGOB).
- Cruz Roja y cuerpos de atención a emergencias médicas.
- Bomberos y Organismos de Protección Civil.

- Secretaría de Hacienda y Crédito Público / Servicio de Administración Tributaria (SAT).
- Control de Aduanas.
- Caminos y Puentes Federales (CAPUFE).
- Dependencias de Gobierno a Nivel Federal/Estatal/Municipal en relación con vías de comunicación.
- Banco Nacional de Obras y Servicios Públicos SNC (Banobras).
- Infoviaje
- Comisión Nacional del Agua (CONAGUA).
- Secretaria de Economía (SE).
- Secretaria de Turismo (SECTUR).

D.6.1.2. Empresas privadas, usuarios y servicios web

Se distinguen los siguientes actores:

- Servicios de emergencia privados.
- Concesionarios.
- Servicios de operadores logísticos.
- Servicios web de información al usuario público.
- Servicios web de información al usuario privado.
- Centros de control y operación urbanos.
- Particulares.
- Comerciales.

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

D.6.1.3. Cámaras organismos privados

Se distinguen los siguientes organismos:

- Operadores privados
- Cámara de compensación.
- Concesionarios de diversas autopistas.
- Centros de control y operación de carreteras y vías urbanas es libres de peaje
- Centros de control y operación que gestionen carriles SENTRI (Secure Electronic Network For Traveler´s Rapid Inspection)
- Centros de control y operación de carreteras y vías urbanas es de cuota que compartirán información de señalización dinámica, vigilancia, colas en los entronques con las autopistas libres.
- Cámara Nacional de Autotransporte de Pasaje y Turismo.
- Asociaciones de Transporte Privado.
- Cámara Nacional de Autotransporte de Carga.

D.6.1.4. Organismos de seguridad nacional

Se distinguen los siguientes organismos:

- Comisión Nacional de Seguridad.
- Plataforma México.
- Penitenciarías.

D.6.2. Esferas de información entre instituciones

A continuación, se muestra una clasificación de las esferas de acción y la información a intercambiar entre actores involucrados para la correcta gestión y explotación de las infraestructuras:

D.6.2.1. Situación de tránsito

- Datos de aforos, intensidad y congestión.
- Tiempos de recorrido.
- Información de colas.

D.6.2.2. Seguridad

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

a) Incidencias leves

- Accidente sin heridos.
- Desprendimientos.
- Vehículo detenido.
- Avería.
- Retención.

b) Afección de las incidencias leves

- Acotamiento.
- Carril.
- Calzada.

c) Restricciones de circulación

- Prohibición del paso a vehículos pesados.
- Mercancías peligrosas.

d) Incidencias graves

- Accidente con heridos.
- Incendio.
- Accidentes con daños a infraestructura.
- Otros.

e) Afección de las incidencias graves

- Calzada.
- Ambas calzadas.
- Otros.

f) Avisos de riesgo para la ciudadanía y funcionalidad de las infraestructuras

- Sismos.
- Atentados.
- Manifestaciones.
- Otros.

g) Avisos de riesgo asociados a causas naturales

- Fenómenos meteorológicos adversos (nieve, hielo, granizo, niebla, viento, tormentas, rayos, huracanes).
- Filtraciones de carácter grave.
- Efectos sísmicos.
- Deslizamiento de tierras.
- Presencia de animales.

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

h) Avisos de riesgo asociados al entorno

- Emergencia en instalación del entorno.
- Fuego o explosión en instalación del entorno.
- Vertido de empresa del entorno.

i) Operaciones de mantenimiento

- Obras de mantenimiento puntuales en la carretera o vía urbana.
- Obras de mantenimiento de larga duración en la carretera o vía urbana.
- Afección de las obras de mantenimiento.
- Mantenimiento preventivo y correctivo a equipo instalado.
- Mantenimiento preventivo y correctivo a software.
- Gestión y acciones de mantenimiento.

j) Gestión de emergencias

- Ubicación de la emergencia.
- Tramo de cielo abierto.
- Túnel.
- Afección de la emergencia.
- Clasificación de emergencia, según el manual de explotación.
- Preemergencia.

- Emergencia de nivel cero (0).
- Emergencia de Nivel uno (1).
- Emergencia de Nivel dos (2).
- Actores involucrados para la resolución de la emergencia, según el manual de explotación.

k) Información de equipos del sistema inteligente de transporte

- Gestión del incidente.
- Cámara de Videovigilancia.
- Detección Automática de Incidentes (DAI).
- Gestión del tránsito.
- Información de Estaciones de Toma de Datos (ETD).
- Información de Lectura de Reconocimiento de Placas (LPR).
- Información del Sistema de Pesaje Dinámico (WIM).
- Detectores de Velocidad (CINEMÓMETRO).
- Información al usuario.
- Información de Tablero de Mensaje Variable (VMS).
- Estaciones de sensores de variables atmosféricas en carretera (SEVAC).

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

l) Información de los equipos de peaje

- Sistema de video vigilancia.
- Información bancaria.
- Información de aforo.
- Información de ingresos.

m) Telepeaje

- Tipos de estado de transpondedores de telepeaje o TAG's.
- Listas de transpondedores de telepeaje.
- Lista blanca.
- Lista gris.
- Lista negra.
- Versiones Completas: El listado completo de los transpondedores de Telepeaje de un operador.
- Actualizaciones o Deltas: El grupo de uno o varios cambios de estado en los transpondedores de Telepeaje de un operador.
- Datos de cruces de telepeaje.
- Estados de cruces.
- Archivos de imágenes.
- Archivo de confirmación de la recepción.

n) Control de pesaje

- Infracciones.
- Imágenes de los vehículos infractores.

o) Indicadores de desempeño

- Atención de incidentes y emergencias.
- Operación y cobro de peaje.
- Servicios al usuario.
- Administración del derecho de vía.
- Mantenimiento de edificios e instalaciones.
- Mantenimiento de sistemas de peaje.
- Mantenimiento de sistemas inteligentes de transporte.
- Servicio de telepeaje y cobro de medios electrónicos.

p) Información climatológica

- Información de Estaciones de Monitoreo Climático (SEVAC).
- Vía urbana invernal y estado de los puertos de montaña. Pueden ser: abierto, cadenas o cerrado.
- Alertas y predicciones climatológicas emitidas por institutos Nacionales de Meteorología.

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

D.6.3. Interfaces y protocolos de comunicación entre entidades

A continuación, se presentan diferentes perfiles de aplicación que se considerarán para el intercambio de mensajes entre los actores involucrados en el proceso de interoperabilidad.

- WSDL (*Web Services Definition Language*), presenta un método para que los centros describan el formato básico de petición de sus sistemas. Este perfil permite desarrollar especificaciones WDSL que cubren las siguientes combinaciones de codificación de mensajes y transporte.

- Protocolo simple de acceso a objetos (SOAP por sus cifras en inglés, Simple Object Access Protocol) sobre HTTP. Usando mensajes codificados SOAP sobre el hypertext transfer protocol.

- HTTP protocolo de transferencia de hipertextos' (http por sus siglas en inglés, protocolo de transferencia de hipertextos'). Los centros serán capaces de describir e implementar interfaces entre centros que soporten los patrones de mensajes de petición–respuesta y suscripción-publicación.

- XML sobre HTTP. Usando mensajes codificados XML sobre HTTP, los centros serán capaces de describir e implementar interfaces entre centros que soporten los patrones de mensajes de petición-respuesta (vía HTTP POST) y patrones de solo petición (HTTP GET). El HTTP POST es apropiado para el intercambio de mensajes (petición-respuesta), mientras que el HTTP GET es apropiado para la petición de un documento XML por su nombre.

- XML sobre FTP. Usando FTP (File Transfer Protocol), los centros serán capaces de describir interfaces que admitan peticiones de documentos XML por su nombre.

- Secretaria de Infraestructura, Comunicaciones y Transportes (SICT): SOAP sobre HTTP.
- Dirección General de Planeación de Centros SICT: SOAP sobre HTTP.
- Unidad de Tecnologías de la Información y Comunicaciones (UTIC): XML sobre HTTP.
- Secretarías de Seguridad Pública / Federales / Estatales / Municipales / Policía / Guardia Nacional: SOAP sobre HTTP.
- Secretaría de Gobernación (SEGOB): SOAP sobre HTTP.
- Cruz Roja y cuerpos de atención de emergencias médicas: SOAP sobre HTTP.
- Bomberos y Organismos de Protección Civil: SOAP sobre HTTP.
- Secretaría de Hacienda y Crédito Público / Servicio de Administración Tributaria (SAT): XML sobre HTTP.
- Control de Aduanas: SOAP sobre HTTP.
- Caminos y Puentes Federales (CAPUFE): XML sobre HTTP
- Dependencias de Gobierno a Nivel Federal / Estatal / Municipal en relación con vías de conmutación: XML sobre HTTP
- Banco Nacional de Obras y Servicios Públicos SNC (Banobras) XML sobre HTTP
- Infoviaje: SOAP sobre HTTP: XML sobre HTTP
- Comisión Nacional del Agua (CONOGUA): SOAP sobre HTTP.
- Secretaría de Economía: XML sobre HTTP
- Secretaría de Turismo (SECTUR): XML sobre HTTP
- Servicios de Emergencia Públicos SOAP sobre HTTP.
- Servicios de Emergencia Concesionados: SOAP sobre HTTP.
- Centros de Control y Operación (CCO) (Nacional, Regional y Concesionario): SOAP sobre HTTP.
- Servicios de operadores logísticos: XML sobre HTTP
- Servicios web de Información a usuarios Públicos: XML sobre HTTP.
- Servicios web de Información a usuarios Privados: XML sobre HTTP.
- Centros de Control y Operación (CCO) Urbanos: SOAP sobre HTTP.
- Operadores Privados: XML sobre HTTP.
- Cámara de Compensación: SOAP sobre HTTP.
- Concesionarios otras Autopistas: SOAP sobre HTTP.
- Cámara Nacional de Autotransporte de Pasaje y Turismo: XML sobre HTTP
- Asociaciones de Transporte Privado: XML sobre HTTP.

COMUNICACIONES

- Cámara Nacional de Autotransporte de Carga y Pasajeros: XML sobre HTTP
- Particulares: XML sobre HTTP.
- Comerciales: XML sobre HTTP.
- Comisión Nacional de Seguridad (CNS): SOAP sobre HTTP.
- Plataforma México: SOAP sobre HTTP.
- Penitenciarias.

D.6.4. Tratamiento y filtrado de información a compartir

En los centros de control y operación (CCO) se gestionará la movilidad de un tramo carretero, encargándose de la supervisión y gestión de la circulación de una carretera o vía urbana a través de los sistemas y estrategias definidas en el sistema de gestión de tránsito y sistema de información.

D.6.4.1. Centro de información (concentración de todos los datos generados del sistema inteligente de transporte)

Concentrará toda la información sobre la situación del tránsito, recogida de diversas fuentes y diseminador de la información elaborada a los diversos organismos implicados y a los usuarios.

COMUNICACIONES

D.6.4.2. Centro de gestión de la movilidad (recogida de datos y tratamiento para compartir a otras instituciones)

Recogerá y elaborará datos que informarán a otros organismos, y tiene la capacidad de influir sobre el estado del tránsito.

D.6.4.3. Información a compartir por sistema y equipo. Formatos y señales

Los equipos y herramientas que dispondrá el centro de control y operación, desde el punto de vista funcional, serán de:

- Entrada de información.
- Diseminación de información.
- Procesamiento.
- Gestión.
- Archivo de información.
- Interacción usuario–sistema.

La información a intercambiar entre entidades se encuentra descrito en el Inciso 0., de esta Norma.

D.6.5. Intercambio de información entre centros de control y operación

Este intercambio de información será acorde a las normas y políticas vigentes aplicables a todos los operadores:

Toda la transferencia de datos se realizará por medios electrónicos pudiendo contemplarse algunas medidas para casos excepcionales de fallos.

Toda la información que se intercambie se efectuará con las medidas de seguridad necesarias para garantizar que:

- La información no se manipula.
- La información no se propaga de forma inadecuada.
- La información sólo la conocen aquellas personas o entes autorizados.

Se almacenará en el centro nacional de interoperabilidad (CNI) o en los centros de control y operación en los que se realice un intercambio de información de interoperabilidad un registro de todas las transacciones procesadas.

El proceso de intercambio de información involucra a diferentes agentes con los cuales se podrá llevar a cabo la transferencia de datos en cualquier sentido, y son:

- Entre concesionarios.
- Entre concesionarios y operadores.
- Entre operadores.
- Con el Centro Nacional de Interoperabilidad (CNI).
- Con los Centros Regionales y Estatales de la SICT.
- Con el Centro Nacional de Control de la SICT.

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

El procedimiento a seguir para el intercambio de información será bidireccional, entre el Centro Nacional de Interoperabilidad (CNI), que recibe todos los cambios, procesa, centraliza y consolida la información de todos los centros de control de los actores o entre los centros de control y operación (CCO) de los diferentes actores.

D.6.6. Información de protocolos de actuación ante incidentes

En el protocolo de actuación ante incidentes se recogen las medidas de actuación frente a incidentes tales como:

- Derrame de líquidos en el suelo.
- Daños eléctricos.
- Deterioro de las instalaciones.

D.6.7. Información de protocolos de actuación ante pre emergencias

En el caso de preemergencias los protocolos de actuación tienen que recoger los incidentes tales como los siguientes:

- Presencia de fenómenos meteorológicos adversos.
- Alta concentración de monóxido de carbono.
- Visibilidad reducida por humos y polvo.
- Retirada de extintor.
- Vehículo detenido en acceso a túnel.
- Tráfico lento.
- Filtraciones de agua.

D.6.8. Información de protocolos de actuación ante emergencias

Las emergencias se distinguen en tres niveles:

- Emergencia Nivel Cero (0): Supone una emergencia o accidente sin daños o con daños limitados para cuyo control son suficientes los medios y recursos de la operación.
- Emergencia Nivel Uno (1): Existen daños leves o riesgo de daño inminente que exigen la intervención de medios o recursos por parte de Protección Civil y organismos de seguridad.
- Emergencia Nivel Dos (2): Es una situación en que, por su naturaleza, gravedad y/o extensión del riesgo, degenera en una aplicación completa por parte de Protección Civil y organismos de seguridad.

La información recogida en los protocolos de actuación estará separada por niveles de emergencia. A continuación, se recoge la información de algunos de los incidentes por cada nivel.

- Emergencias nivel cero (0): Lluvia intensa, nieve o hielo, excesiva concentración de CO, Presencia de peatones, bicicletas o vehículos de tracción animal en la calzada u obstáculo en el acotamiento.
- Emergencias nivel uno (1): CO inadmisible. opacidad inadmisible, vehículo detenido en calzada bloqueando totalmente el paso, inundaciones y desprendimiento de tierras.
- Emergencias nivel dos (2): Accidente grave con riesgo o daño para un gran número de personas. Fuego en instalación. Fuego en vehículo.

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

D.7. MANEJO Y PROCESAMIENTO DE DATOS

Para el manejo y el procesamiento de datos, los CCO disponen de tres elementos importantes:

- Almacenamiento masivo de datos: Los datos recibidos por los equipos que estén situados en campo correspondientes a los sistemas inteligentes de transporte, se almacenarán en dispositivos de almacenamiento masivo de datos para el posterior procesamiento.

- Bases de datos: Las bases de datos de los sistemas inteligentes de transporte, Peaje y telepeaje recogerán toda la información recibida por los equipos situados en campo en las bases de datos del Centro de Control y Operación (CCO) para que pueda ser utilizada por los usuarios de dicho centro.

- Seguridad informática. El Centro de Control y Operaciones (CCO) utilizará los protocolos de seguridad necesarios para que la información recibida por los equipos de campo de los diferentes sistemas (sistema inteligente de transporte, Peaje, Telepeaje) sea segura.

D.8. MANUAL DE EXPLOTACIÓN

Un manual de explotación de un CCO tiene el objeto de fijar las bases para regular la explotación que se realiza desde el mismo, estará compuesto de los siguientes documentos:

- Marco general de explotación.

- Plan de operación. Que incluya: plan de operaciones normales. plan de autoprotección.

- Plan de gestión medioambiental.

- Plan de mantenimiento.
- Plan de implantación y seguimiento.
- Plan de servicios a los usuarios.
- Normas de circulación.
- Libro de competencias.
- Anexos.

D.8.1. Marco general de la explotación

El marco general de la explotación, recogerá la estrategia general a seguir en la explotación del centro de control y operación y de las instalaciones que se gestionen desde el mismo, describiéndose:

- El escenario de la infraestructura carretera, instalaciones de sistemas inteligentes de transporte, peaje y centro de control y operación. Legislación y normativa aplicable y de referencia y medio físico, infraestructura, instalaciones del sistema inteligente de transporte, peaje y Centro de Control y Operación.
- Plan general de explotación. Incluye: actividades de explotación: Actividades de operación. Actividades de autoprotección, actividades de mantenimiento, actividades de administración, y recursos de la explotación, recursos humanos, recursos Materiales y recursos externos.

SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

D.8.2. Plan de operación

El plan de operación del manual de explotación estará compuesto por los siguientes documentos:

- Plan de operaciones normales. Tramos a cielo abierto y túneles. Peajes - Plan de Operaciones Normales de Explotación de Peajes. Centros de control y operación.
- Plan de autoprotección o emergencia.

D.8.3. Plan de gestión medioambiental

En el Plan de Gestión Medioambiental, se recogerán las pautas a llevar a cabo para conseguir un desarrollo sostenible de la actividad de una infraestructura carretera y mitigar sus impactos negativos sobre el medio natural.

- Planificación. Se establecerá la situación actual de la infraestructura carretera con relación al medio ambiente.
- Implantación. Se describirán las medidas ambientales a implantar por la afección de la infraestructura carretera sobre el medioambiente. Para ello, se asignará personal y recursos físicos y financieros, nuevos procedimientos, controles, entre otros.
- Verificación. Se describirán las revisiones para verificar la efectividad y eficiencia de las medidas ambientales implantadas. La verificación se podrá realizar a través de acciones como el monitoreo o la medición de las actividades claves que ocasionan impactos ambientales.
- Actuación y ajuste. Se recogerán las recomendaciones generadas a raíz de las auditorías ambientales y se reflejarán los ajustes adecuados para alcanzar los objetivos ambientales inicialmente propuestos.

D.8.4. Plan de mantenimiento

En el plan de mantenimiento de una infraestructura carretera, se recogerán las labores, actuaciones y planificación orientada a mantener la infraestructura e instalaciones en condiciones óptimas. En el plan de mantenimiento se incluirá al menos los siguientes contenidos.

- Objetivos.
- Descripción de las instalaciones a mantener.
- Inventario de las instalaciones de una infraestructura carretera o vía urbana.
- Recursos y organización.
- Procedimientos: Dentro de plan de mantenimiento se establecerán los siguientes procedimientos: manual de mantenimiento, programa de actuaciones y libro de mantenimiento.

D.8.4.1. Mantenimiento preventivo

El mantenimiento preventivo corresponderá a las actuaciones rutinarias que contribuyen a que los equipos y sistemas mantengan las prestaciones exigidas durante el tiempo de vida de los mismos, minimizando la posibilidad de fallo, asegurando su disponibilidad y alargando su vida útil. Estas actuaciones son planificadas y sirven de base para la elaboración de un programa de actuaciones de mantenimiento.

La programación de los trabajos de mantenimiento preventivo se establecerá teniendo en cuenta las especificaciones y actuaciones previstas por los distintos fabricantes para el correcto mantenimiento de sus equipos, así como por las normativas nacionales y las recomendaciones internacionales vigentes. La experiencia en la operación y explotación de las instalaciones y sistemas será plasmada en la mejora del mantenimiento preventivo, incluyendo tanto nuevas actividades como optimizando su periodicidad.

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

D.8.4.2. Mantenimiento correctivo

Las actividades de mantenimiento correctivo se realizarán al producirse una avería o fallo en un equipo del centro de control y operación o de los sistemas de peaje, telepeaje, sistemas inteligentes de transporte o comunicaciones, para devolverlo a un estado de operación normal.

Dentro del Plan de Mantenimiento se contemplarán los tiempos de respuesta (tiempo que se tarda desde que se tiene constancia de un fallo hasta que el equipo de mantenimiento está trabajando en él) y los tiempos de resolución (el tiempo que ha estado sin funcionar, es decir desde que se produce la avería hasta su resolución), agrupados en función de la criticidad del equipo o sistema afectado. Mediante estos tiempos se asegura la disponibilidad requerida de los equipos y sistemas del centro de control y operación.

D.8.4.3. Mantenimiento predictivo

El mantenimiento predictivo permitirá aumentar la periodicidad del mantenimiento preventivo y programar la sustitución de elementos antes de que se produzca el fallo o avería que generaría un mantenimiento correctivo. Permitirá por tanto reducir costos de mantenimiento, manteniendo e incluso mejorando la disponibilidad de los equipos y sistemas.

Dentro del plan de mantenimiento se incluirá el mantenimiento preventivo, el cual será optimizado con la experiencia de explotación y adecuado a los cambios tecnológicos.

D.8.5. Plan de implantación y seguimiento

El plan de implantación y seguimiento definirá las actuaciones a emprender para la puesta en servicio de la explotación, así como las actuaciones y procedimientos de seguimiento, dentro del proceso de mejora continua de la explotación. En el plan de implantación y seguimiento se describirán los siguientes apartados:

- Implantación del Manual de Explotación.
- Formación del personal de explotación.
- Ejercicios y simulacros.
- Gestión del manual de explotación.
- Seguimiento de la explotación. Se definirá la metodología de seguimiento de la explotación, describiéndose con detalle los procesos de captación de datos, generación y análisis de la información de seguimiento, y propuesta de mejoras.

D.8.6. Plan de servicios a los usuarios

En el plan de servicios a los usuarios se describirán las siguientes funcionalidades del sistema de atención a clientes de una infraestructura carretera.

- Servicios de atención al usuario.
- Estrategia de atención al usuario, atención a quejas y sugerencias.
- Sistema de postes SOS.
- Aplicación de atención al cliente.
- Página Web Pública.

COMUNICACIONES
SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

D.8.7. Normas de circulación

El manual de explotación, contendrá un documento de normas de circulación, en donde se relacionarán las normas de circulación, tanto generales como particulares que aplican a una infraestructura carretera.

D.8.8. Libro de competencias

El manual de explotación contendrá un documento denominado libro de competencias, que determinará las responsabilidades de las instituciones que tienen competencia en la circulación de vehículos a través de una infraestructura carretera.

D.8.9. Anexos del manual de explotación

El manual de explotación contendrá los siguientes documentos como anexos.

- Directorio telefónico. En este documento se mostrará un directorio telefónico de todas las entidades, organizaciones y personas relacionadas con la explotación. Se organizarán por actividades de explotación (mantenimiento, emergencias, entre otros.).
- Documentación de proyecto. Se adjuntará una relación exhaustiva de la documentación de final de obra, que estará disponible para la infraestructura carretera e instalaciones de sistemas inteligentes de transporte, ya que es necesaria para el correcto desempeño de las actividades de mantenimiento, formación del personal y para soportar determinadas tareas de la operación.

COMUNICACIONES

SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

SUBSECRETARÍA DE INFRAESTRUCTURA
Dirección General de Servicios Técnicos
Av. Coyoacán 1895
Col. Acacias, Benito Juárez, 03240
Ciudad de México
www.gob.mx/sct