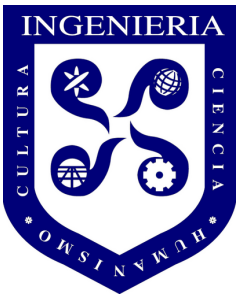


Universidad Autónoma del Estado de México

Facultad de Ingeniería

Ingeniería en Electrónica

Reporte de Aplicación de Conocimientos

Seguridad en redes de telecomunicaciones en el PREP del IEEM

Que para obtener el Título de
Ingeniero en Electrónica

Presenta
Alan Barajas Belmontes

Asesor
M. en. I. Juan Carlos Pérez Merlos

Toluca de Lerdo. Septiembre del 2016

UAEM | Universidad Autónoma del Estado de México

DEPTO. DE EVALUACIÓN PROFESIONAL
No. Oficio: 0037/2016
Ciudad Universitaria, Toluca, Méx. a 02 de Agosto del 2016

C. ALAN BARAJAS BELMONTES
PASANTE DE INGENIERÍA EN ELECTRÓNICA
P R E S E N T E.

En respuesta a su solicitud, a continuación transcribo el tema aprobado por esta Dirección, que propuso el ***M. EN I. JUAN CARLOS PÉREZ MERLOS,*** con el fin de que lo desarrolle en la modalidad de ***REPORTE DE APLICACIÓN DE CONOCIMIENTOS*** le informo que se autoriza la **impresión de su trabajo** para presentar su Evaluación Profesional.

"SEGURIDAD EN REDES DE TELECOMUNICACIONES EN EL PREP DEL IEEM".

ÍNDICE
RESUMEN
INTRODUCCIÓN
CAPÍTULO 1. REDES DE COMUNICACIÓN
CAPÍTULO 2. SEGURIDAD EN REDES DE COMUNICACIONES: FÍSICAS LÓGICAS Y SOFTWARE
CAPÍTULO 3. CASO DE ESTUDIO. PREP 2015 IEEM.
CONCLUSIONES
BIBLIOGRAFÍA
REFERENCIAS

Ruego a usted tomar nota de que en cumplimiento a lo especificado por la Ley de Profesiones, deberá prestar Servicio Social durante un tiempo mínimo de seis meses, como requisito indispensable para sustentar su Evaluación Profesional.

Así mismo, para la elaboración del ***REPORTE DE APLICACIÓN DE CONOCIMIENTOS*** y demás trámites, deberá sujetarse a la reglamentación respectiva de esta Universidad.

A T E N T A M E N T E
PATRIA, CIENCIA Y TRABAJO
"2016, Año del Aniversario de la Universidad Autónoma del Estado de México"
"2016 Año de Leopoldo Flores Valdés"

FACULTAD DE INGENIERÍA
U. A. E. M.

M. EN I. RAÚL VERA NOGUEZ
DIRECTOR

**/Saha.

Cerro de Coatepec S/N, Ciudad Universitaria; Toluca México
Tel. (722) 2-14-08-55 / 2-15-13-51

Dedicatorias y Agradecimientos

A mi familia por los valores que me han inculcado, mi Papá por enseñarme a dar lo mejor y que el esfuerzo constante conduce al éxito; A mi Madre por ser ejemplo, inspiración y lucha, por su apoyo incondicional; A mi Hermana por ser mi compañera en esta aventura de la vida.

A mi Abuelita Esthela por todo su Amor; A Fuen por ser mi motivación para ser una mejor persona; A mis tíos, en especial a Chelita y David por siempre estar con nosotros; Y a la persona que estaría mas orgullosa que nadie por este gran logro, mi Abuelo "Tuto".

A mis profesores que son ejemplo vivo de profesionalismo y entusiasmo, pues su vocación alienta a la comunidad académica a desarrollarnos como mejores Ingenieros; En especial al Ing. Juan Carlos Pérez Merlos y al Ing. Juan Carlos Baca Belmontes por su valiosa ayuda en la elaboración de este trabajo.

A mis amigos, pues en la meta que alcanzo el día de hoy se encuentra un poco de cada uno de ustedes. Gracias por sus enseñanzas, su apoyo, sus horas de estudio, sus palabras y sus risas.

Resumen

El objetivo de este reporte de aplicación de conocimientos es documentar la seguridad en las telecomunicaciones del Programa de Resultados Electorales Preliminares(PREP) del Instituto Electoral del Estado de México (IEEM) en las elecciones de Diputados Locales y Ayuntamientos del 7 de junio del 2015.

El PREP es el sistema de información en el que cualquier persona puede consultar avances el día de la jornada electoral, donde podrá conocer momento a momento los resultados preliminares que van obteniendo los partidos y los candidatos a diversos puestos de elección popular a nivel local.

Mi labor comprendió en realizar una parte de la seguridad para la interconexión de los canales por los cuales fue transmitida la votación plasmada en las Actas de Escrutinio y Cómputo en las más de 18000 casillas electorales instaladas en el Estado de México.

La labor que desempeña el área de Telecomunicaciones de la Unidad de Informática y Estadística (UIE) del IEEM, se enfoca en la interconexión de 125 juntas municipales y 45 juntas distritales, dando un total de 170 sitios hacia el edificio central, realizando la instalación de equipos de red, verificando los enlaces de internet y supervisando los requerimientos de seguridad.

Índice

Resumen. 4
Introducción. 7

CAPÍTULO 1. Redes de comunicación. 10

1.1. Redes de comunicación. 10
1.2. ¿Qué es una red de comunicaciones? 11
1.3. Tipos de red. 12
1.4. Modelos de referencia. 19
1.5. El modelo de referencia OSI. 19
1.6. Modelo de referencia TCP/IP. 25
1.7. VPN. 29
1.8. Direcciones IP. 30

CAPÍTULO 2. Seguridad en redes de comunicaciones:
Físicas, Lógicas, Software. 34

2.1. ¿Qué es la seguridad? 34
2.2. Objetivo de la seguridad. 35
2.3. Activos de información. 37
2.4. Amenazas y vulnerabilidades. 38
2.5. Controles (contramedidas). 39
2.6. El proceso de seguridad contempla 4 actos: 41
2.7. Firewall o cortafuegos. 41
2.8. IPSec. 43
2.9. VLANs. 45

CAPÍTULO 3. Caso de estudio. PREP 2015 IEEM. 47

3.1. Qué es el IEEM y cómo se rige. 47
3.2. Proyecto de comunicaciones. 48
3.3. Lineamientos INE e IEEM. 48
3.4. Qué es el PREP. 49
3.5. Actividades y elementos del PREP. 52
3.6. Proceso Electoral 2015. 53
3.7. Recursos. 55
3.8. Telecomunicaciones. 56
3.9. Arquitecturas de red. 57

3.10. Servidores. 58
3.11. Equipos de cómputo. 58
3.12. Escáneres. 60
3.13. Concentración de resultados. 61
3.14. Transmisión de datos e imágenes. 61
3.15. Procedimiento de concentración de resultados. 63
3.16. Recepción de datos e imágenes y almacenamiento en las bases de datos 64
3.17. Seguridad en los enlaces. 66

Conclusiones. 69

Bibliografía. 72

Referencias. 72

Glosario. 73

Introducción

El Instituto Electoral del Estado de México (IEEM) es un organismo público local que de manera conjunta con el Instituto Nacional Electoral (INE), tiene a su cargo la función estatal de organizar las elecciones locales en el Estado de México. Para la elección de Diputados Locales y Ayuntamientos, del pasado 7 de junio del 2015, se requirió implementar, diseñar y operar el Programa de Resultados Electorales Preliminares (PREP).

El PREP es un mecanismo de información electoral que recaba los datos preliminares y no definitivos, de carácter estrictamente informativo a través de la captura de los datos asentados en las Actas de Escrutinio y Cómputo (AEC) de las casillas que se reciben en los Centros de Acopio y Trasmisión de Datos (CATD).

Se instalaron 170 CATD ubicados en los 125 municipios y en 45 distritos electorales en el Estado de México, todos ellos conectados con el Centro Estatal de Comunicaciones (CESCO) ubicado en IEEM en la Ciudad de Toluca, Estado de México.

Para la transmisión de los datos se deben cumplir los principios de certeza, imparcialidad, independencia, legalidad, máxima publicidad y objetividad. Para lograrlo se implementó un Sistema de Gestión de Seguridad de la Información (SGSI) certificado bajo la norma internacional ISO/IEC 27001:2013. Este brindo seguridad al interconectar las 170 oficinas y transmitir los resultados de la elección.

Al ser información pública muy importante y estar difundida en internet, fue de vital importancia que los datos no fuesen alterados y no existiera alguna intrusión que pudiera afectar la integridad de los datos. Para lograrlo fue necesario crear conexiones seguras por medio de Redes Privadas Virtuales (Virtual Private Network, VPN) las cuales garantizaron un canal seguro para la transmisión de los datos.

El objetivo de este trabajo es documentar la seguridad en las telecomunicaciones del Programa de Resultados Electorales Preliminares del Instituto Electoral del Estado de México. Se describe el desarrollo de este reporte aplicando los conocimientos adquiridos en las unidades de aprendizaje: Programación Básica, Programación Avanzada, Óptica, Comunicación 1, Comunicación 2, Comunicación 3, Redes de Computadoras y Administración.

El documento está formado por tres capítulos los cuales se describen a continuación:

Capítulo 1. Redes de comunicación.

En el primer capítulo, se describe lo que es una red de comunicaciones, los tipos de red y los modelos de referencia que se utilizaron, entre ellos el Modelo OSI.

Capítulo 2. Seguridad en redes de comunicaciones: físicas, lógicas y software.

Existen diferentes maneras de vulnerar una red de comunicaciones; ya sea de manera física, en hardware o software. Por lo que en este segundo capítulo se explican los activos de la información, las amenazas, las vulnerabilidades y los controles o contramedidas que se utilizaron en el PREP.

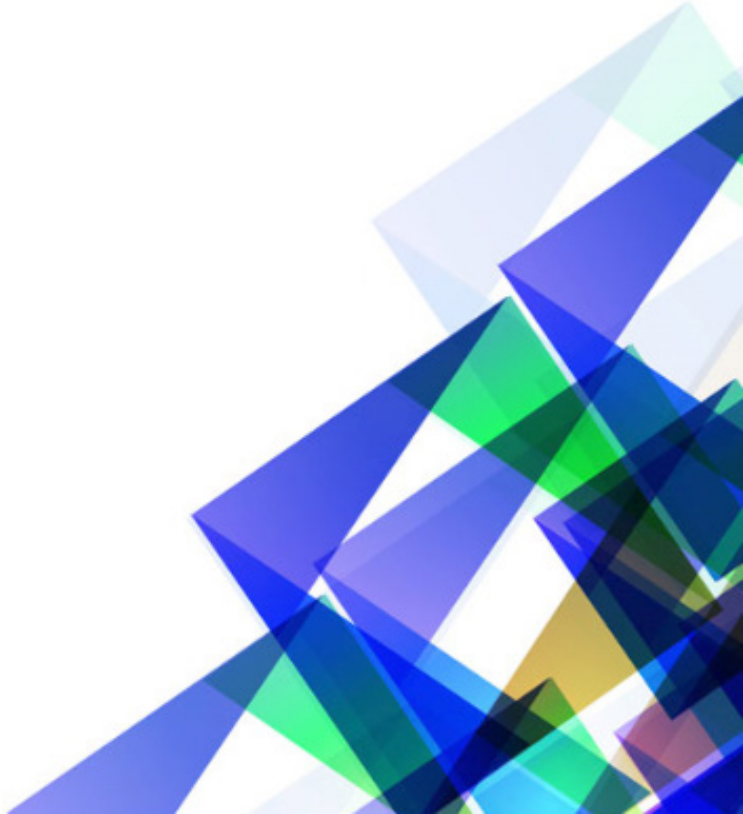
Capítulo 3. Caso de estudio. PREP 2015 IEEM.

Finalmente, en este capítulo se detalla lo que es el IEEM, los lineamientos con los que se rige, el PREP junto con sus actividades y elementos, el sistema informático, la concentración de resultados y las telecomunicaciones que se implementaron.

Las labores que se desempeñaron en el área de Telecomunicaciones en la Unidad de Informática y Estadística (UIE) del IEEM, se enfocaron en la interconexión de los 170 sitios con el edificio central, realizando la instalación de equipos de red, verificando los enlaces de internet y supervisando los requerimientos de seguridad que se implementaron para la correcta comunicación entre los sitios.

Existen algunos aspectos en este documento que no se pueden divulgar debido a su carácter confidencial, sin embargo, se explican con el mayor detalle posible.

Capítulo 1
Redes de comunicación



CAPÍTULO 1
Redes de comunicación

1.1. Redes de comunicación.

La teoría de la información surgió a finales de la Segunda Guerra Mundial, en los años cuarenta. Fue iniciada por Claude E. Shannon a través de un artículo publicado en el Bell System Technical Journal en 1948, titulado "Una teoría matemática de la comunicación". En esta época se buscaba utilizar de manera más eficiente los canales de comunicación, enviando una cantidad de información por un determinado canal y midiendo su capacidad; se buscaba la transmisión óptima de los mensajes. [1]

Esta teoría es el resultado de trabajos comenzados en la década 1910 por Andrei A. Markovi, le siguió Ralp V. L. Hartley en 1927, quien fue el precursor del lenguaje binario. A su vez, Alan Turing en 1936, realizó el esquema de una máquina capaz de tratar información con emisión de símbolos, y finalmente Claude Elwood Shannon, matemático, ingeniero electrónico y criptógrafo estadounidense, conocido como "el padre de la teoría de la información", junto a Warren Weaver, contribuyó en la culminación y el asentamiento de la Teoría Matemática de la Comunicación de 1949 que hoy es mundialmente conocida por todos como la Teoría de la Información. [2]

Weaver consiguió darle un alcance superior al planteamiento inicial, creando un modelo simple y lineal: Fuente/codificador/mensaje canal/decodificador/destino. La necesidad de una base teórica para la tecnología de la comunicación surgió del aumento de la complejidad y de la masificación de las vías de comunicación, tales como el teléfono, las redes de teletipo y los sistemas de comunicación por radio. La teoría de la información también abarca todas las restantes formas de transmisión y almacenamiento de información, incluyendo la televisión y los impulsos eléctricos que se transmiten en las computadoras y en la grabación óptica de datos e imágenes. La idea es garantizar que el transporte masivo de datos no sea en modo alguno una merma de la calidad, incluso si los datos se comprimen de alguna manera. Idealmente, los datos se pueden restaurar a su forma original al llegar a su destino. En algunos casos, el objetivo es permitir que los datos de alguna forma se conviertan para la transmisión en masa, se reciban en el punto de destino y sean convertidos fácilmente a su formato original, sin perder ninguna información transmitida. [2]

1.2. ¿Qué es una red de comunicaciones?

Una red de comunicaciones es el conjunto de medios técnicos que permiten la comunicación a distancia entre equipos autónomos. Normalmente se trata de transmitir datos, audio y video por ondas electromagnéticas a través de diversos medios (antenas, cables de cobre, fibras ópticas, etc.) La información se puede transmitir de forma analógica, digital o mixta, pero siempre es simplificada para el usuario. En la ilustración 1 se muestra la forma en que las personas pueden estar interconectadas entre sí.

Ilustración 1. Red de personas interconectadas.

Las redes más comunes son de computadoras, teléfonos, transmisión de audio y transmisión de video. Las redes están formadas por conexiones entre grupos de computadoras y dispositivos asociados que permiten a los usuarios la transferencia electrónica de información. [3]

La red de área local, representada en la parte izquierda de la Ilustración 2, es un ejemplo de la configuración utilizada en muchas oficinas y empresas. Las diferentes computadoras se denominan estaciones de trabajo y se comunican entre sí a través de un cable o línea telefónica conectada a los servidores. Éstas son computadoras como las estaciones de trabajo, pero poseen funciones administrativas y están dedicados en exclusiva a supervisar y controlar el acceso

de las estaciones de trabajo a la red y a los recursos compartidos (como las impresoras). La línea roja representa una conexión principal entre servidores de red; la línea azul muestra las conexiones locales. [3]

Un módem (modulador/demodulador) permite a las computadoras transferir información a través de las líneas telefónicas normales. El módem convierte las señales digitales a analógicas y viceversa, lo que permite la comunicación entre computadoras muy distantes entre sí.

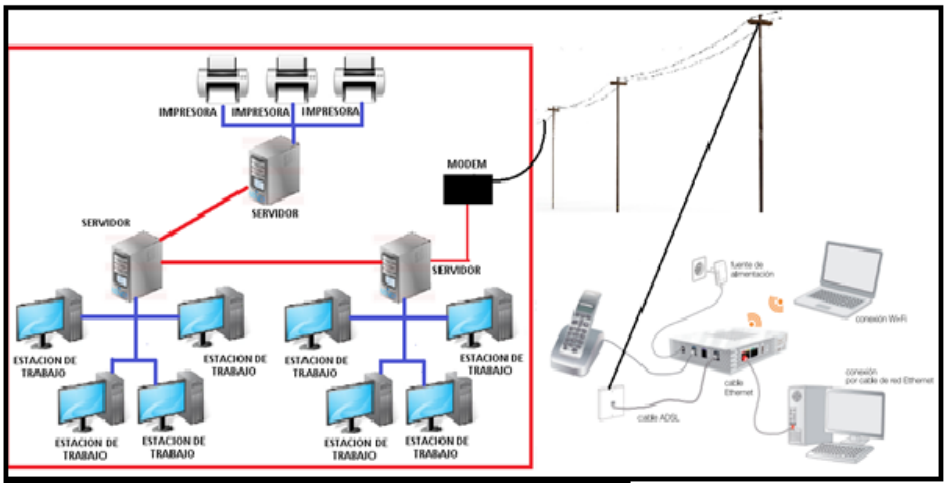


Ilustración 2. Redes de Área Local conectadas por medio de Modem a central telefónica.

1.3. Tipos de red.

Las redes se pueden clasificar de diferentes maneras. Las principales son: [3]

Tabla 1. Tipos de redes.

Por su extensión.			
PAN	LAN	WAN	MAN
Por su topología.			
Bus	Árbol	Doble Anillo	Mixta
Estrella	Malla	Anillo	
Por su conexión física.			
Redes punto a punto (*unicast*).			
Redes multipunto o redes de difusión (*broadcast).*			

Por su técnica de transmisión de datos.
Líneas dedicadas.
Modelos de circuito conmutados (circuit switching).
Modelos de paquetes conmutados (packet switching).

POR SU EXTENSIÓN.

Red PAN. (Personal Area Network):

PAN significa Red de área personal. Se establece que las redes de área personal son una configuración básica llamada así mismo personal la cual está integrada por los dispositivos que están situados en el entorno personal y local del usuario, ya sea en la casa, trabajo, carro, parque, centro comercial, etc. Esta configuración le permite al usuario establecer una comunicación con estos dispositivos a la hora que sea de manera rápida y eficaz.

Actualmente existen diversas tecnologías que permiten su desarrollo, entre ellas se encuentran la tecnología inalámbrica Bluetooth o las tecnologías de infrarrojos. Sin embargo, para su completo desarrollo es necesario que estas redes garanticen una seguridad de alto nivel, que sean altamente adaptables a diversos entornos, y que sean capaces de proporcionar una alta gama de servicios y aplicaciones, tanto aplicaciones que requieran una alta calidad multimedia como pueden ser la video conferencia, la televisión digital o los videojuegos, como aplicaciones de telecontrol que requieran anchos de banda muy bajos soportados sobre dispositivos de muy reducido tamaño. [3]

Red LAN (Local Area Network):

LAN significa Red de área local. Es un conjunto de equipos que pertenecen a la misma organización y están conectados dentro de un área geográfica pequeña mediante una red, generalmente con la misma tecnología (la más utilizada es Ethernet).[3]

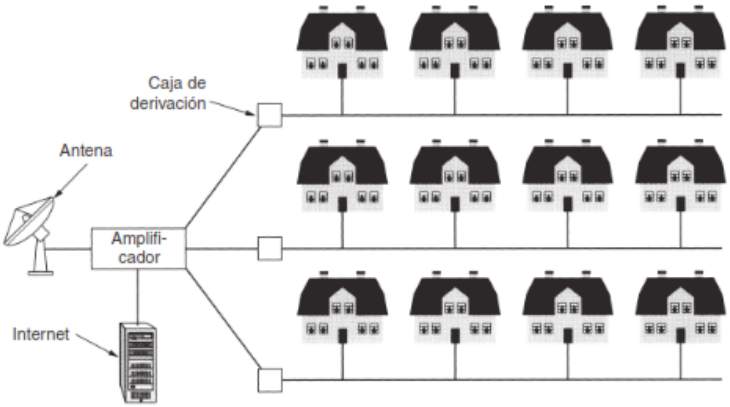


Ilustración 3. Ejemplo de una red de área metropolitana, basada en TV por cable.

Red MAN (Metropolitan Area Network):

MAN significa Redes de Área Metropolitana. Una MAN conecta diversas LAN cercanas geográficamente en un área de cincuenta kilómetros entre sí a alta velocidad. Por lo tanto, una MAN permite que dos nodos remotos se comuniquen como si fueran parte de la misma red de área local. Puede ser privada o pública. Una MAN está compuesta por routers conectados entre sí mediante conexiones de alta velocidad (generalmente cables de fibra óptica). [3]

WAN (Wide Area Network):

WAN significa Redes de Amplia Cobertura o Red de área extensa. Una conecta múltiples LAN entre sí a través de grandes distancias geográficas.

Las líneas de transmisión: Se conocen como circuitos, canales o trúcales. Los elementos de intercambio: Son computadores especializados utilizados para conectar dos más líneas de transmisión.

La velocidad disponible en una WAN varía según el costo de las conexiones, funcionan con routers que pueden optar por la ruta más apropiada para que los datos lleguen a un nodo de la red. La WAN más conocida es Internet.

En la tabla 2 se puede observar la clasificación de las redes de acuerdo a la distancia entre redes. En la ilustración 4 se observa la jerarquía de las redes por su extensión. Para existir una red WAN, necesita existir una red MAN y para existir una red MAN deben existir redes LAN. [3]

Diámetro	Tipo
< 0,01 m	Paralelismo masivo. Procesadores multi-núcleo.
< 0,1 m	Multiprocesadores.
< 10 m	Redes de área personal (PAN: *Personal Area Network*). Redes de infrarrojos o *bluetooth*.
10 m – 3 km	Redes de área local (LAN: *Local Area Network*) y metropolitana (MAN). Ethernet, Wi-Fi.
> 3 km	Redes de área extensa (WAN: *Wide Area Network*) o redes interconectadas. Frame-Relay, RDSI, ATM, SONet/SDH.

Tabla 2. Clasificación de las redes por su extensión.

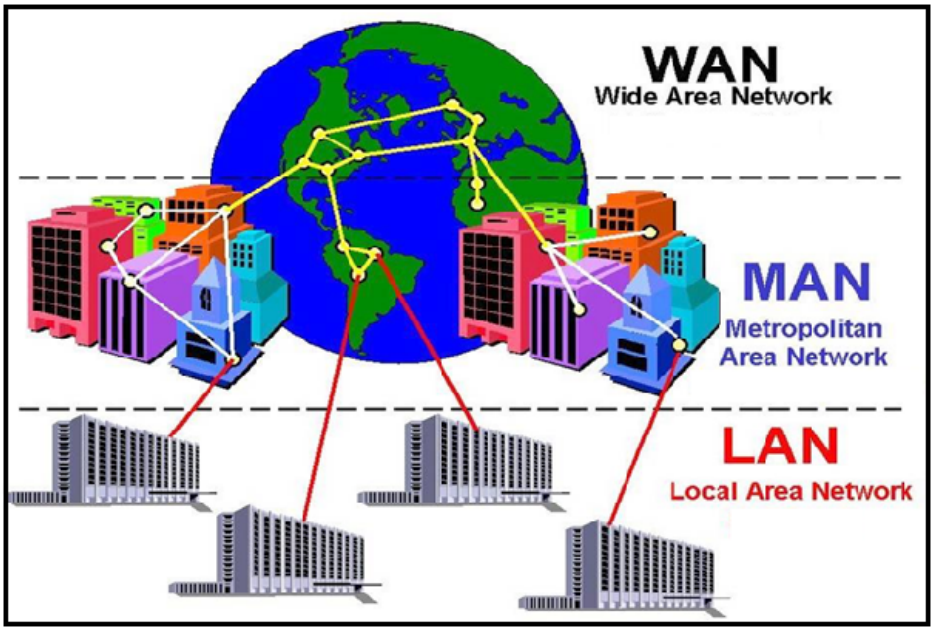


Ilustración 4.Redes por extensión. RED WAN, RED MAN, RED LAN

POR SU TOPOLOGÍA.

La topología de red se define como el mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico. El concepto de red puede definirse como "conjunto de nodos interconectados". Un nodo es el punto en el que una curva se intercepta a sí misma. Lo que un nodo es concretamente, depende del tipo de redes a que nos referimos.

La topología de una red es el diseño de las comunicaciones entre los nodos de la red. Las topologías principales se muestran en la ilustración 5, las cuales son de tipo bus compartido, estrella o anillo, aunque existen más topologías. [3]

Hay que diferenciar entre la topología física, que define como están conectados físicamente los nodos y la topología lógica que es como tratan los nodos las conexiones.

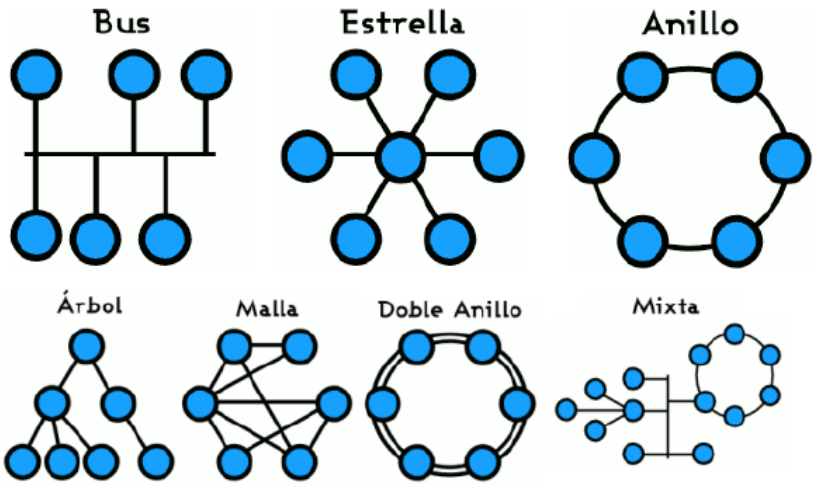


Ilustración 5 Clasificación de las redes por su topología.

POR SU CONEXIÓN FÍSICA.

❖ Redes punto a punto (unicast):

Basadas principalmente en cable y en cada conexión intervienen solo dos equipos.

Se subdividen en:

- Simplex: inútil en redes de computadores (mono direccional).
- Semi-dúplex (Half-duplex): envía datos cada vez en un sentido.
- Dúplex (Full-duplex): envía datos en los dos sentidos a la vez.

En las redes semi-duplex y duplex se puede disponer de la misma capacidad en las dos direcciones de transmisión (conexión simétrica) o no (conexión asimétrica).

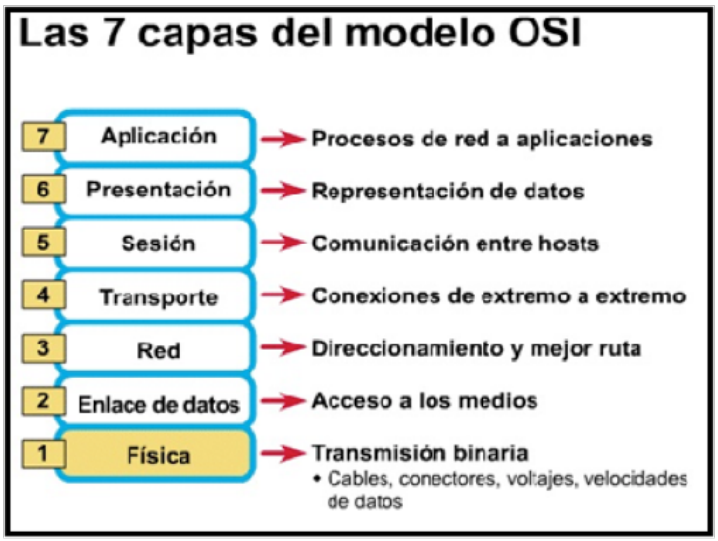


Ilustración 6. Capas del modelo OSI

❖ Redes multipunto o redes de difusión (broadcast):

Basadas principalmente en bus compartido (cable bus y anillo) y redes inalámbricas (radio, satélites...); todos los equipos comparten el mismo medio de transmisión.

- Estática (TDM): No emite si alguien lo está haciendo.
- Dinámica (Centralizada o Distribuida).

Las emisiones pueden estar marcadas como unicast, multicast o broadcast, pero no garantizan la confidencialidad.

POR SU TÉCNICA DE TRANSMISIÓN DE DATOS.

❖ Líneas dedicadas.

Enlace punto a punto permanente y siempre disponible. Se utilizan principalmente en redes WAN con velocidades prefijadas por el proveedor, generalmente simétricas y full-duplex.

Otro caso habitual es el radio enlace. El nivel de enlace utilizado suele ser HDLC o PPP. Suelen tener un coste elevado por lo que solo son adecuadas si hay mucho tráfico continuo.

❖ Modelos de circuito conmutado *(Circuit Switching).*

En ellos las comunicaciones no comparten los medios. Al iniciarse la comunicación se reserva los recursos intermedios necesarios para establecer y mantener el circuito. Si el canal se corta se corta la comunicación.

Los dispositivos mantienen información sobre el estado de la comunicación (*statusfull*).

❖ Modelos de paquetes conmutados *(Packet Switching).*

En ellos las comunicaciones se dividen en paquetes que comparten los medios. Se pueden utilizar varios enlaces en cada interfaz físico.

Ofrece un medio físico de transmisión de datos para los equipos.
Existen dos submodelos:

- Datagramas
- Circuitos virtuales (VC por sus siglas en inglés: *Virtual Circuit*): Simula un circuito conmutado, pero compartiendo los medios. Primero se establece una conexión y los equipos intermedios reservan una parte de sus recursos; después todos los paquetes siguen la misma ruta ordenadamente.

  - PVC (*Permanent VC*): Los PVC son circuitos virtuales definidos estáticamente y permanentes.
  - SVC (*Switched VC*): Se establecen y terminan a petición del usuario de forma dinámica. La implementación de circuitos virtuales es más compleja que la de circuitos permanentes.

1.4. Modelos de referencia.

Tomaremos en cuenta dos arquitecturas de redes importantes: los modelos de referencia OSI y TCP/IP.

Aunque los protocolos asociados con el modelo OSI ya casi no se usan, el modelo en sí es muy general y aún es válido, y las características tratadas en cada capa aún son muy importantes. El modelo TCP/IP tiene las propiedades opuestas: el modelo en sí no se utiliza mucho, pero los protocolos sí. Por estas razones se analizarán con detalle ambos modelos. [6]

1.5. El modelo de referencia OSI.

Este modelo está basado en una propuesta desarrollada por la ISO (Organización Internacional de Estándares) como un primer paso hacia la estandarización internacional de los protocolos utilizados en varias capas (Day y Zimmermann, 1983). Fue revisado en 1995 (Day, 1995). El modelo se llama OSI (Interconexión de Sistemas Abiertos) de ISO porque tiene que ver con la conexión de sistemas abiertos, es decir, sistemas que están abiertos a la comunicación con otros sistemas. Para abreviar, lo llamaremos modelo OSI.

Observe que el modelo OSI no es en sí una arquitectura de red, debido a que no especifica los servicios y protocolos exactos que se utilizarán en cada capa. Sólo indica lo que debe hacer cada capa como se muestra en la Ilustración 6. Sin embargo, ISO también ha producido estándares para todas las capas, aunque éstos no son parte del modelo de referencia mismo. Cada uno se ha publicado como un estándar internacional separado. [6]

❖ La capa física.

En esta capa se lleva a cabo la transmisión de bits puros a través de un canal de comunicación.

Los aspectos del diseño implican asegurarse de que cuando un lado envía un bit 1, éste se reciba en el otro lado como tal, no como bit 0. Las preguntas

típicas aquí son: ¿Cuántos volts se deben emplear para representar un 1? y ¿Cuántos para representar un 0?, ¿Cuántos nanosegundos dura un bit?, ¿La transmisión se debe llevar a cabo en ambas direcciones al mismo tiempo?, ¿Cómo se establece la conexión inicial y cómo se finaliza cuando ambos lados terminan?, ¿Cuántos pines tiene un conector de red y para qué se utiliza cada uno? Los aspectos de diseño tienen que ver mucho con interfaces mecánicas, eléctricas y de temporización, además del medio físico de transmisión, que está bajo la capa física.

❖ La capa de enlace de datos.

La tarea principal de esta capa es transformar un medio de transmisión puro en una línea de comunicación que, al llegar a la capa de red, aparezca libre de errores de transmisión. Logra esta tarea haciendo que el emisor fragmente los datos de entrada en tramas de datos (típicamente, de algunos cientos o miles de bytes) y transmitiendo las tramas de manera secuencial. Si el servicio es confiable, el receptor confirma la recepción correcta de cada trama devolviendo una trama de confirmación de recepción.

Otra cuestión que surge en la capa de enlace de datos (y en la mayoría de las capas superiores) es cómo hacer que un transmisor rápido no sature de datos a un receptor lento. Por lo general se necesita un mecanismo de regulación de tráfico que indique al transmisor cuánto espacio de búfer tiene el receptor en ese momento. Con frecuencia, esta regulación de flujo y el manejo de errores están integrados.

Las redes de difusión tienen un aspecto adicional en la capa de enlace de datos: cómo controlar el acceso al canal compartido. Una subcapa especial de la capa de enlace de datos, la subcapa de control de acceso al medio, se encarga de este problema. En esta capa se define el direccionamiento físico, que permite a los hosts identificar las tramas destinadas a ellos. Este direccionamiento es único, identifica el hardware de red que se está usando y el fabricante, y no se puede cambiar.

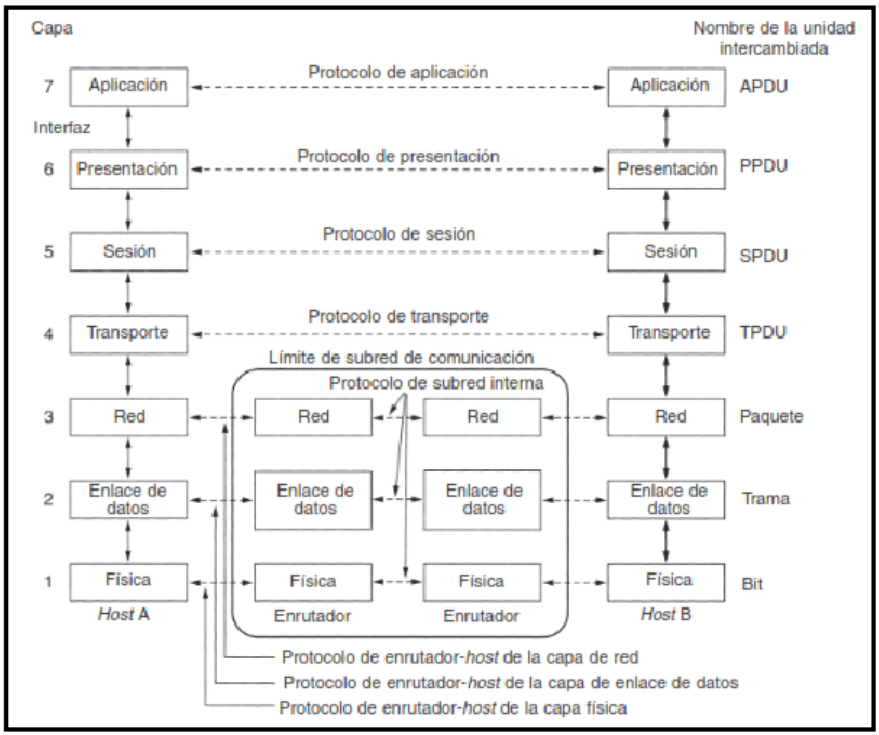


Ilustración 7 El modelo de referencia OSI.

❖ La capa de red.

Esta capa controla las operaciones de la subred. Un aspecto clave del diseño es determinar cómo se enrutan los paquetes desde su origen a su destino. Las rutas pueden estar basadas en tablas estáticas (enrutamiento estático) codificadas en la red y que rara vez cambian.

En el enrutamiento estático la ruta que seguirán los paquetes hacia un destino particular es determinada por el administrador de la red. Las rutas también pueden determinarse cuando los enrutadores intercambian información de enrutamiento (enrutamiento dinámico).

En este tipo de enrutamiento los enrutadores deciden la ruta que seguirán los paquetes hacia un destino sin la intervención del administrador de red. En el enrutamiento dinámico las rutas pueden cambiar para reflejar la topología o el estado de la red.

Si hay demasiados paquetes en la subred al mismo tiempo, se interponen en el camino unos y otros, lo que provoca que se formen cuellos de botella. La responsabilidad de controlar esta congestión también pertenece a la capa de red, aunque esta responsabilidad también puede ser compartida por la capa de transmisión. De manera más general, la calidad del servicio proporcionado (retardo, tiempo de tránsito, inestabilidad, etcétera) también corresponde a la capa de red.

Cuando un paquete tiene que viajar de una red a otra para llegar a su destino, pueden surgir muchos problemas. El direccionamiento utilizado por la segunda red podría ser diferente del de la primera. La segunda podría no aceptar todo el paquete porque es demasiado largo. Los protocolos podrían ser diferentes, etcétera. La capa de red tiene que resolver todos estos problemas para que las redes heterogéneas se interconecten.

En las redes de difusión, el problema de enrutamiento es simple, por lo que la capa de red a veces es delgada o, en ocasiones, ni siquiera existe.

El direccionamiento usado en esta capa es un direccionamiento lógico, diferente al direccionamiento físico empleado en la capa de enlace de datos.

Este direccionamiento lógico permite que una interfaz o puerto pueda tener más de una dirección de capa de red.

❖ La capa de transporte.

La función básica de esta capa es aceptar los datos provenientes de las capas superiores, dividirlos en unidades más pequeñas si es necesario, pasar éstas a la capa de red y asegurarse de que todas las piezas lleguen correctamente al otro extremo. Además, todo esto se debe hacer con eficiencia y de manera que aísle a las capas superiores de los cambios inevitables en la tecnología del hardware.

La capa de transporte también determina qué tipo de servicio proporcionar a la capa de sesión y, finalmente, a los usuarios de la red. El tipo de conexión de transporte más popular es un canal punto a punto libre de errores que entrega mensajes o bytes en el orden en que se enviaron. Sin embargo, otros tipos de servicio de transporte posibles son la transportación de mensajes aislados, que no garantiza el orden de entrega, y la difusión de mensajes a múltiples destinos. El tipo de servicio se determina cuando se establece la conexión.

La capa de transporte es una verdadera conexión de extremo a extremo, en toda la ruta desde el origen hasta el destino. En otras palabras, un programa en la máquina de origen lleva a cabo una conversación con un programa similar en la máquina de destino, usando los encabezados de mensaje y los mensajes de control. En las capas inferiores, los protocolos operan entre cada máquina y sus vecinos inmediatos, y no entre las máquinas de los extremos, la de origen y la de destino, las cuales podrían estar separadas por muchos enrutadores.

En la ilustración 8 se muestra la diferencia entre las capas 1 a 3, que están encadenadas, y las capas 4 a 7, que operan de extremo a extremo.

❖ La capa de sesión.

Esta capa permite que los usuarios de máquinas diferentes establezcan sesiones entre ellos. Las sesiones ofrecen varios servicios, como el control de diálogo (dar seguimiento de a quién le toca transmitir), administración de token (que impide que las dos partes traten de realizar la misma operación crítica al mismo tiempo) y sincronización (la adición de puntos de referencia a transmisiones largas para permitirles continuar desde donde se encontraban después de una caída).

❖ La capa de presentación.

A diferencia de las capas inferiores, a las que les corresponde principalmente mover bits, a la capa de presentación le corresponde la sintaxis y la semántica de la información transmitida. A fin de que las computadoras con diferentes representaciones de datos se puedan comunicar, las estructuras de datos que se intercambiarán se pueden definir de una manera abstracta, junto con una codificación estándar para su uso en el cable.

La capa de presentación maneja estas estructuras de datos abstractas y permite definir e intercambiar estructuras de datos de un nivel más alto (por ejemplo, registros bancarios).

❖ La capa de aplicación.

Esta capa contiene varios protocolos que los usuarios requieren con frecuencia. Un protocolo de aplicación de amplio uso es HTTP (Protocolo de Transferencia de Hipertexto), que es la base de WWW (World Wide Web).

Cuando un navegador desea una página Web, utiliza este protocolo para enviar al servidor el nombre de dicha página. A continuación, el servidor devuelve la página.

Otros protocolos de aplicación se utilizan para la transferencia de archivos, correo electrónico y noticias en la red.

El modelo OSI divide a la red en diferentes capas con el propósito de que cada desarrollador trabaje específicamente en su campo sin la necesidad de depender de otras áreas. Un programador crea una aplicación determinada sin importarle cuáles son los medios por los que se trasladan los datos, inversamente un técnico de comunicaciones provee comunicación sin importarle que datos traslada.

Cada una de estas capas presta servicio a la capa inmediatamente superior siendo la capa de aplicación la única que no lo hace al ser la última capa su servicio está directamente relacionado con el usuario.

Así mismo cada una de estas siete capas del host de origen se comunica directamente con su similar en el host de destino. Las cuatro capas inferiores también son denominadas capas de medios (en algunos casos capas de flujo de datos), mientras que las tres superiores se llaman capas de Host.

- Proporciona una forma de entender cómo operan los dispositivos en una red.
- Es la referencia para crear e implementar estándares de red, dispositivos y esquemas de internetworking (interconexión de redes).
- Separa la compleja operación de una red en elementos más simples.
- Permite a los ingenieros centrarse en el diseño y desarrollo de funciones modulares ocupándose cada uno de su parte especifica.
- Proporciona la posibilidad de definir interfaces estándares para compatibilidad "plug-and-play" e integración multifabricante.

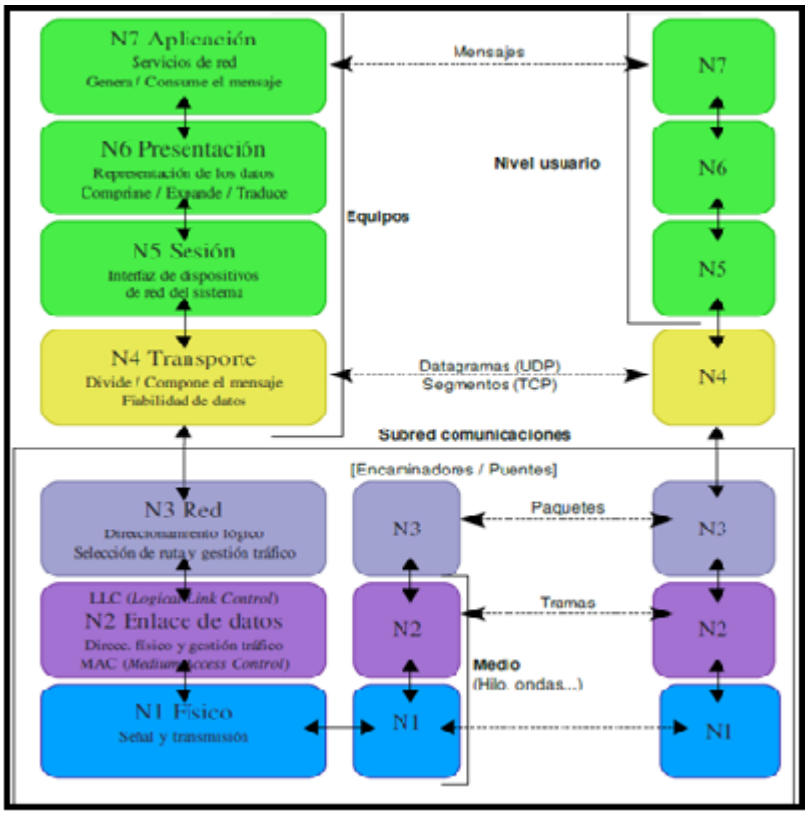


Ilustración 8 Capas e interconexión del Modelo OSI

1.6. Modelo de referencia TCP/IP.

ARPANET fue una red de investigación respaldada por el DoD (Department of Defense, Departamento de Defensa de Estados Unidos). Con el tiempo, conectó cientos de universidades e instalaciones gubernamentales mediante líneas telefónicas alquiladas.

Posteriormente, cuando se agregaron redes satelitales y de radio, los protocolos existentes tuvieron problemas para interactuar con ellas, por lo que se necesitaba una nueva arquitectura de referencia. De este modo, la capacidad para conectar múltiples redes en una manera sólida fue una de las principales metas de diseño desde sus inicios. Más tarde, esta arquitectura se llegó a conocer como el modelo de referencia TCP/IP, de acuerdo con sus dos protocolos

primarios. Su primera definición fue en (Cerf y Kahn, 1974). Posteriormente se definió en (Leiner y cols., 1985). La filosofía del diseño que respalda al modelo se explica en (Clark, 1988).

Ante el temor del DoD de que algunos de sus valiosos hosts, enrutadores y puertas de enlace de interredes explotaran en un instante, otro objetivo fue que la red pudiera sobrevivir a la pérdida de hardware de la subred, sin que las conversaciones existentes se interrumpieran.

En otras palabras, el DoD quería que las conexiones se mantuvieran intactas en tanto las máquinas de origen y destino estuvieran funcionando, aunque algunas de las máquinas o líneas de transmisión intermedias quedaran fuera de operación repentinamente.

Además, se necesitaba una arquitectura flexible debido a que se preveían aplicaciones con requerimientos divergentes, desde transferencia de archivos a transmisión de palabras en tiempo real. [6]

❖ La capa de interred.

Todos estos requerimientos condujeron a la elección de una red de conmutación de paquetes basada en una capa de interred no orientada a la conexión. Esta capa, llamada capa de interred, es la pieza clave que mantiene unida a la arquitectura. Su trabajo es permitir que los hosts inyecten paquetes dentro de cualquier red y que éstos viajen a su destino de manera independiente (podría ser en una red diferente). Tal vez lleguen en un orden diferente al que fueron enviados, en cuyo caso las capas más altas deberán ordenarlos, si se desea una entrega ordenada. Observe que aquí el concepto "interred" se utiliza en un sentido genérico, aun cuando esta capa se presente en Internet.

Aquí la analogía es con el sistema de correo tradicional. Una persona puede depositar una secuencia de cartas internacionales en un buzón y, con un poco de suerte, la mayoría de ellas se entregará en la dirección correcta del país de destino. Es probable que, durante el trayecto, las cartas viajen a través de una o más puertas de enlace de correo internacional, pero esto es transparente para los usuarios.

Además, para los usuarios también es transparente el hecho de que cada país (es decir, cada red) tiene sus propios timbres postales, tamaños preferidos de sobre y reglas de entrega.

La capa de interred define un paquete de formato y protocolo oficial llamado IP (Protocolo de Internet). El trabajo de la capa de interred es entregar paquetes IP al destinatario. Aquí, el enrutamiento de paquetes es claramente el aspecto principal, con el propósito de evitar la congestión.

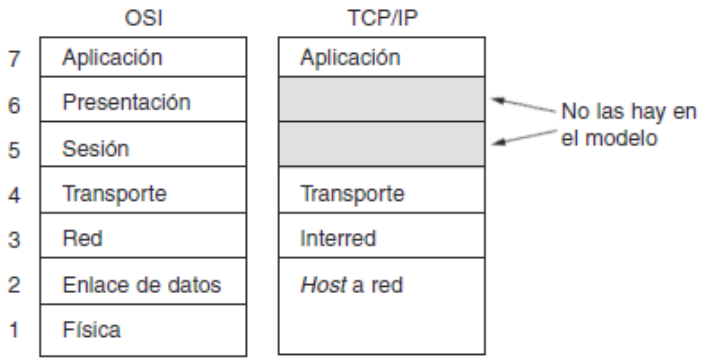
Por estas razones es razonable decir que la capa de interred del modelo TCP/IP es similar en funcionalidad a la capa de red del modelo OSI. La Ilustración 9 muestra esta correspondencia.

❖ La capa de transporte.

La capa que está arriba de la capa de interred en el modelo TCP/IP como se muestra en la Ilustración 9, se llama capa de transporte. Está diseñada para permitir que las entidades iguales en los *hosts* de origen y destino puedan llevar a cabo una conversación, tal como lo hace la capa de transporte OSI. Aquí se han definido dos protocolos de transporte de extremo a extremo.

El primero, TCP (Protocolo de Control de Transmisión), es un protocolo confiable, orientado a la conexión, que permite que un flujo de bytes que se origina en una máquina se entregue sin errores en cualquier otra máquina en la interred. Divide el flujo de bytes entrantes en mensajes discretos y pasa cada uno de ellos a la capa de interred. En el destino, el proceso TCP receptor reensambla en el flujo de salida los mensajes recibidos. TCP también maneja el control de flujo para asegurarse de que un emisor rápido no sature a un receptor lento con más mensajes de los que puede manejar.

Tabla 3. Modelo de referencia TCP/IP.



El segundo protocolo de esta capa, UDP (Protocolo de Datagrama de Usuario), es un protocolo no confiable y no orientado a la conexión para aplicaciones que no desean la secuenciación o el control de flujo de TCP y que desean proporcionar el suyo.

También tiene un amplio uso en consultas únicas de solicitud-respuesta de tipo cliente-servidor en un solo envío, así como aplicaciones en las que la entrega puntual es más importante que la precisa, como en la transmisión de voz o vídeo. La relación de IP, TCP y UDP se muestra en la ilustración 10. Puesto que el modelo se desarrolló, se ha implementado IP en muchas otras redes.

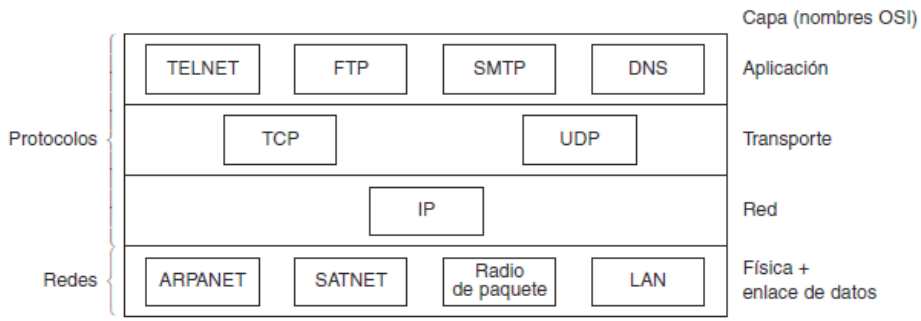


Ilustración 9. Protocolos y redes en el modelo TCP/IP inicialmente.

❖ La capa de aplicación.

El modelo TCP/IP no tiene capas de sesión ni de presentación. No se han necesitado, por lo que no se incluyen. La experiencia con el modelo OSI ha probado que este punto de vista es correcto: son de poco uso para la mayoría de las aplicaciones.

Arriba de la capa de transporte está la capa de aplicación. Contiene todos los protocolos de nivel más alto. Los primeros incluyeron una terminal virtual (TELNET), transferencia de archivos (FTP) y correo electrónico (SMTP), como se muestra en la Ilustración 10. El protocolo de terminal virtual permite que un usuario en una máquina se registre en una máquina remota y trabaje ahí. El protocolo de transferencia de archivos proporciona una manera de mover con eficiencia datos de una máquina a otra. El correo electrónico era originalmente sólo un tipo de transferencia de archivos, pero más tarde se desarrolló un protocolo especializado

(SMTP) para él. Con el tiempo, se han agregado muchos otros protocolos: DNS (Sistema de Nombres de Dominio) para la resolución de nombres de host en sus direcciones de red; NNTP, para transportar los artículos de noticias de USENET; HTTP, para las páginas de World Wide Web, y muchos otros.

❖ La capa host a red.

Debajo de la capa de interred hay un gran vacío. El modelo de referencia TCP/IP en realidad no dice mucho acerca de lo que pasa aquí, excepto que puntualiza que el host se tiene que conectar a la red mediante el mismo protocolo para que le puedan enviar paquetes IP. Este protocolo no está definido y varía de un host a otro y de una red a otra. Este tema rara vez se trata en libros y artículos sobre TCP/IP.

1.7. VPN.

Una VPN (por sus siglas en inglés, *Virtual Private Network*) es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. Las empresas suelen utilizar una VPN para que sus empleados desde sus casas, hoteles, etc., puedan acceder a recursos corporativos que de otro modo, no podrían. Sin embargo, conectar la computadora de un empleado a los recursos corporativos es solo una función de una VPN. En conjunto con lo anterior, una implementación correcta de esta tecnología permite asegurar la confidencialidad e integridad de la información.

Como puede suponerse, a través de una VPN pasa información privada y confidencial que en las manos equivocadas, podría resultar perjudicial para cualquier empresa. Esto se agrava aún más si el empleado en cuestión se conecta utilizando un Wi-Fi público sin protección. Afortunadamente, este problema puede ser mitigado cifrando los datos que se envían y reciben. Para poder lograr este objetivo, se pueden utilizar los siguientes protocolos:[3]

➢ IPSec (Internet Protocol Security).

Permite mejorar la seguridad a través de algoritmos de cifrado robustos y un sistema de autentificación más exhaustivo. IPsec posee dos métodos de encriptado, modo transporte y modo túnel. Asimismo, soporta encriptado de 56 bit y 168 bit (triple DES).

- PPTP/MPPE

Tecnología desarrollada por un consorcio formado por varias empresas. PPTP soporta varios protocolos VPN con cifrado de 40 bit y 128 bit utilizando el protocolo *Microsoft Point to Point Encryption* (MPPE).
PPTP por sí solo no cifra la información.

- L2TP/IPSec (L2TP sobre IPSec)

Tecnología capaz de proveer el nivel de protección de IPsec sobre el protocolo de túnel L2TP. Al igual que PPTP,
L2TP no cifra la información por sí mismo.

Parte de la protección de la información que viaja por una VPN es el cifrado, no obstante, verificar que la misma se mantenga íntegra es igual de trascendental. Para lograr esto, IPSec emplea un mecanismo que si detecta alguna modificación dentro de un paquete, procede a descartarlo. Proteger la confidencialidad e integridad de la información utilizando una VPN es una buena medida para navegar en Wi-Fi públicos e inseguros incluso si no se desea acceder a un recurso corporativo.

1.8. Direcciones IP.

Cada host y enrutador de Internet tiene una dirección IP, que codifica su número de red y su número de host. La combinación es única: no hay dos máquinas que tengan la misma dirección IP.

Todas las direcciones IP versión 4 son de 32 bits de longitud y se usan en los campos de Dirección de origen y de Dirección de destino de los paquetes IP. En importante mencionar que una dirección IP realmente no se refiere a un host. En realidad, se refiere a una interfaz de red, por lo que, si un host está en dos redes, debe tener dos direcciones IP. Sin embargo, en la práctica, la mayoría de los hosts se encuentran en una red y, por lo tanto, tienen una dirección IP.

Por varias décadas, las direcciones IP se dividieron en cinco categorías, las cuales se listan en la Ilustración 10. Esta asignación se ha llamado direccionamiento con clase (classful addressing). [6]

❖ Formatos de direcciones IP.

Los formatos de clase A, B, C y D permiten hasta 128 redes con 16 millones de hosts cada una, 16,382 redes de hasta 64K hosts, 2 millones de redes (por ejemplo, LANs) de hasta 256 hosts cada una (aunque algunas son especiales). También soportan la multidifusión, en la cual un datagrama es dirigido a múltiples hosts.

Las direcciones que comienzan con 1111 se reservan para uso futuro.

Hay cerca de 500,000 redes conectadas a Internet, y la cifra se duplica cada año.

Los números de redes son manejados por una corporación no lucrativa llamada ICANN (Corporación de Internet para la Asignación de Nombres y Números) para evitar conflictos. A su vez, ICANN ha delegado partes del espacio de direcciones a varias autoridades regionales, las cuales han repartido direcciones IP a los ISPs y a otras compañías.

Las direcciones de red, que son números de 32 bits, generalmente se escriben en notación decimal con puntos. En este formato, cada uno de los 4 bytes se escribe en decimal, de 0 a 255. Por ejemplo, la dirección hexadecimal C0290614 se escribe como 192.41.6.20. La dirección IP menor es 0.0.0.0 y la mayor 255.255.255.255.

Los valores 0 y 1(todos 1s) tienen significado especial, como se muestra en la Ilustración 11. El valor 0 significa esta red o este host. El valor 1 se usa como dirección de difusión para indicar todos los hosts de la red indicada.

La dirección IP 0.0.0.0 es usada por los hosts cuando están siendo arrancados, pero no se usa después. Las direcciones IP con 0 como número de red se refieren a la red actual.

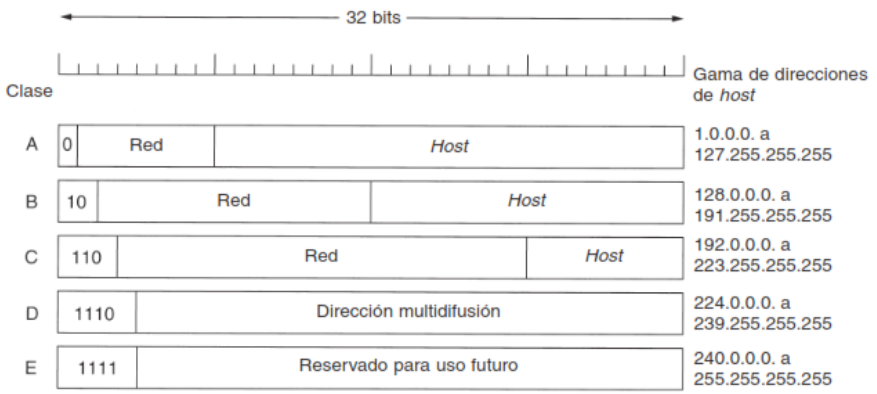


Ilustración 10. Formatos de dirección IP.

Estas direcciones permiten que las máquinas se refieran a su propia red sin saber su número (pero tiene que saber su clase para saber cuántos ceros hay que incluir). La dirección que consiste solamente en unos permite la difusión en la red local, por lo común una LAN. Las direcciones con un número de red propio y solamente unos en el campo de host permiten que las máquinas envíen paquetes de difusión a LANs distantes desde cualquier parte de Internet. Por último, todas las direcciones de la forma 127.xx.yy.zz se reservan para direcciones locales de prueba (loopbacks). Los paquetes enviados a esa dirección no se colocan en el cable; se procesan localmente y se tratan como paquetes de entrada. Esto permite que los paquetes se envíen a la red local sin que el transmisor conozca su número.

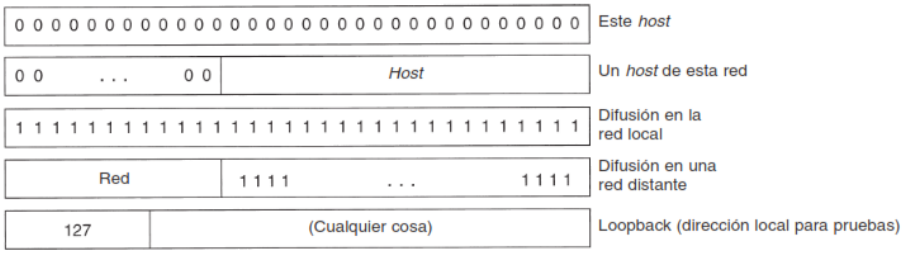
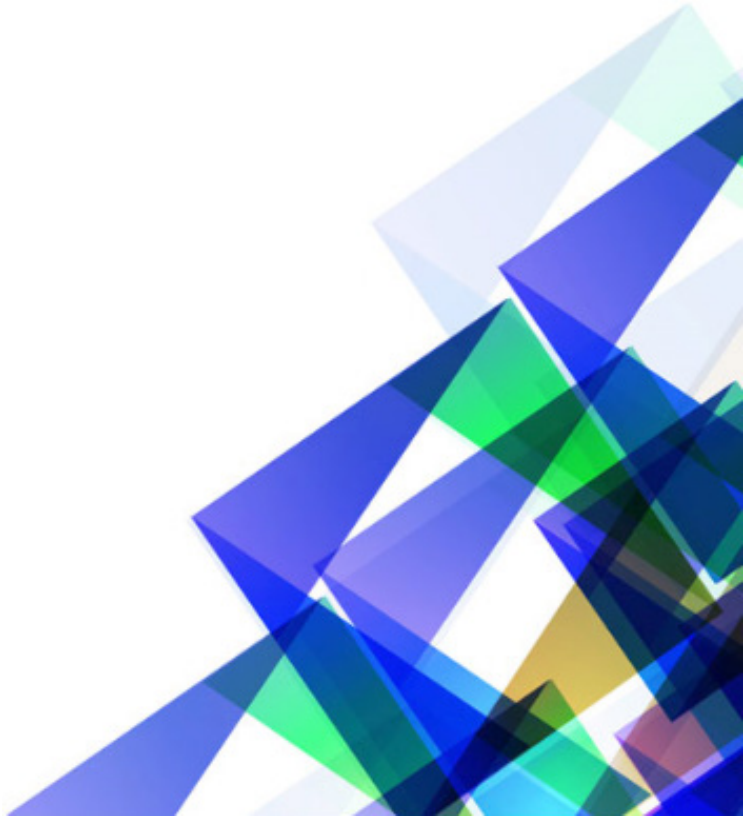


Ilustración 11. Direcciones IP especiales.

Capítulo 2
Seguridad en redes de comunicaciones: físicas, lógicas, software



CAPÍTULO 2
Seguridad en redes de comunicaciones: Físicas, Lógicas, Software

Para que dos sistemas informáticos intercambien información es necesario junto con los medios de transmisión físicos, la existencia de una arquitectura de comunicaciones común estructurada en niveles. Cada uno de estos niveles realiza un subconjunto de las funcionalidades propias necesarias para el intercambio de datos. Es por ello que se hace necesario integrar las funcionalidades propias de la seguridad en las arquitecturas de comunicaciones existentes. Este proceso de integración implicará la implementación de mecanismos y servicios y funciones de seguridad que se apoyarán en muchos casos en servicios, mecanismos y funciones ya implementados en la propia arquitectura de comunicaciones. El resultado final será lo que se denomina *Arquitectura de seguridad.*

Para estimar las necesidades de seguridad de una organización y evaluar y elegir los productos y políticas de seguridad en las comunicaciones, se necesita evaluar los siguientes aspectos en la seguridad de la información:

- Ataques a la seguridad: ¿Qué acciones pueden comprometer la seguridad de la información que pertenece a una organización?
- Mecanismos de seguridad: ¿Qué mecanismos hay que implementar para detectar, prevenir o recuperarse de un ataque a la seguridad de la información?
- Servicios de seguridad: ¿Qué servicios ofrecer al usuario respecto a la transferencia de información en una red de datos? Los servicios de seguridad tratan de contrarrestar los ataques y para ello hacen uso de los mecanismos de seguridad para proporcionar ese servicio.

2.1. ¿Qué es la seguridad?

Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar, proteger la información buscando mantener la Confidencialidad, Integridad, Autenticidad y Disponibilidad.

Seguridad es el proceso consistente en mantener un nivel aceptable del riesgo percibido. Un antiguo director de educación para la International Computer Security Association, el Dr. Mitch Kabay, escribía en 1986 que "la seguridad es un proceso, y no un estado final".

- Confidencialidad. Prevenir la divulgación de información a personas o sistemas. El servicio de confidencialidad asegura que la información no va a ser revelada ni va a estar disponible a individuos no autorizados, entidades o procesos. Este aspecto tiene especial importancia cuando las redes de comunicaciones que transportan la información presentan puntos vulnerables respecto de la seguridad.

    - Confidencialidad orientada a conexión: Consiste en la protección de todos los datos de usuario.
    - Confidencialidad no orientada a conexión: Consiste en la protección de todos los datos de usuario contenidos en una sola unidad de datos del servicio (UDS).

- Integridad. Busca mantener los datos libres de modificaciones no autorizadas.
- Autenticidad. Propiedad que permite identificar el generador de la información.
- Disponibilidad. Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

Estos objetivos pueden traslaparse o pueden ser mutuamente exclusivos. Por ejemplo, requerimientos fuertes de confidencialidad pueden restringir severamente la disponibilidad.

2.2. Objetivo de la seguridad.

El objetivo de la seguridad en redes es mantener la seguridad, disponibilidad, privacidad (sus aspectos fundamentales) control y autenticidad de la información manejada por computadora, a través de procedimientos basados en políticas de seguridad tales que permitan el control de lo adecuado.

Se sustenta en un principio general que es Proporcionalidad y 5 pilares:

1) Proceso.

La información se podrá asegurar en la medida que se entienda cómo se procesa en cada circunstancia.

2) Criptología.

Esta disciplina se basa en técnicas matemáticas que explotan las particularidades de los mecanismos internos y externos que usamos para generar y transmitir la información.

Preserva o mejora la:

- Confidencialidad.
- Autenticidad e integridad.

3) Control de acceso.

Si la información se ha depositado en algún medio, se requiere de una metodología para evitar que quienes no deban conocerla lo hagan, permitiendo además que quienes deban conocerla lo puedan hacer.

- Control de Acceso a Sistemas (equipos).
- Control de Acceso a Aplicaciones.
- Control de Acceso a Instalaciones físicas.
- Control de Acceso a sistemas que no tienen relación directa con la información.

4) Buenas prácticas.

Como cualquier otra actividad colectiva humana se requieren políticas, normas y vigilancia de las mismas para su desempeño.

Cualquier actividad que se trata de llevar a cabo en forma caótica, sin reglas aceptadas por todos los participantes, tiende a fallar o a funcionar en forma torpe y hasta dañina.

5) Mecanismos.

Estos cuatro amplios conceptos solamente se pueden implantar en la realidad para mejorar la seguridad informática a través de mecanismos específicos.
Diversidad de Mecanismos:

- Combate de infecciones de virus computacionales.
- Modelos de Control de acceso.
- Firewalls, IDS, IPS, etc.

Principio general: Proporcionalidad.

La aplicación de mecanismos debe estar regida por un concepto muy general, llamado proporcionalidad.

Nos indica que no vale la pena usar recursos cuyo costo sea mayor al valor de la información que se está protegiendo.

Este principio no es privativo de la seguridad. También es aplicable en casi todas las actividades humanas.

2.3. Activos de información.

La información es un activo que como otros activos importantes tiene valor y requiere en consecuencia una protección adecuada.
Los activos se pueden clasificar en:

- Activos de información (datos, manuales, etc.)
- Software (aplicaciones hechas en casa, software comercial, etc.)
- Activos físicos (Computadoras, redes, etc.)
- Personal (Clientes, personal)
- Servicios (Comunicaciones, outsoursing, etc.)

2.4. Amenazas y vulnerabilidades.

❖ Amenazas.

Es una indicación de un evento desagradable con el potencial de causar daño.

- Naturales: (Inundaciones, tornados, terremotos, etc.)
- A Instalaciones: (Fuego, caída de energía, daño de agua, etc.)
- Humanas: (huelgas, epidemias, perdida de personal clave, etc.)
- Tecnológicas: (Virus, hacking, pérdida de datos, fallas de hardware y software, red, etc.)
- Operacionales: (Falla en equipos, aspectos reguladores, mala publicidad, etc.)

❖ Vulnerabilidades.

Son debilidades de seguridad asociadas con los activos de información de una organización.

Las vulnerabilidades no causan daño, simplemente son condiciones que pueden hacer que una amenaza afecte un activo.

- Seguridad de los recursos humanos: Falta de entrenamiento.
- Control de acceso: Passwords.
- Seguridad física y ambiental: Ubicación de áreas seguras.
- Gestión de operaciones y comunicación: Administración de la red.
- Mantenimiento, desarrollo y adquisición de sistemas de información: Documentación de aplicaciones.

❖ Vulnerabilidades Comunes

- Inadecuado compromiso de la dirección.
- Personal inadecuadamente capacitado y concientizado.
- Inadecuada asignación de responsabilidades.
- Ausencia de políticas/ procedimientos.

- Ausencia de controles. (Físicos/lógicos) (Disuasivos/preventivos/detectivos/correctivos)
- Ausencia de reportes de incidentes y vulnerabilidades.
- Inadecuado seguimiento y monitoreo de los controles.

❖ Riesgo.

Probabilidad de que una amenaza pueda explotar una vulnerabilidad en particular.

El riesgo es una medida de la magnitud de los daños frente a una situación peligrosa. El riesgo se mide asumiendo una determinada vulnerabilidad frente a cada tipo de peligro. Si bien no siempre se hace, debe distinguirse adecuadamente entre peligrosidad (probabilidad de ocurrencia de un peligro), vulnerabilidad (probabilidad de ocurrencia de daños dado que se ha presentado un peligro) y riesgo (propiamente dicho).

Más informalmente se habla de riesgo para hablar de la ocurrencia ante un potencial perjuicio o daño para las unidades, personas, organizaciones o entidades (en general "bienes jurídicos protegidos"). Cuanto mayor es la vulnerabilidad mayor es el riesgo, pero cuanto más factible es el perjuicio o daño, mayor es el peligro. Por tanto, el riesgo se refiere sólo a la teórica "posibilidad de daño" bajo determinadas circunstancias, mientras que el peligro se refiere sólo a la teórica "probabilidad de daño" bajo esas circunstancias.

Sin embargo, los riesgos pueden reducirse o manejarse. Si somos cuidadosos, y si estamos conscientes de nuestras debilidades y vulnerabilidades frente a las amenazas existentes, podemos tomar medidas para asegurarnos de que las amenazas no se conviertan en desastres.

2.5. Controles (contramedidas).

Medios de administrar el riesgo, incluye políticas, procedimientos, guías, prácticas o estructuras organizacionales, que pueden ser administrativas, técnicas, gerenciales o legales.

❖ Tipos de controles.

- Controles físicos.
  - Disuasivos.
  - Bardas, señales de avisos, guardias, perros, etc.
  - Para Retrasos.
  - Cerraduras, defensa por capas, controles de acceso.
  - Detección de intrusos.
  - Externos, internos, CCTV.
  - Evaluación de situaciones.
  - Procedimiento de guardias, arboles de llamadas.
  - Respuesta.
  - Fuerza de respuesta, procedimiento de emergencia, policía, bomberos, médicos, respaldos.

- Controles administrativos.
  - Política de seguridad de información.
  - Procesos de respaldos y verificación de los mismos.
  - Procesos de restauración.
  - Procesos de respuesta a incidentes.
  - Estándares de configuración para Windows.
  - Guías para el manejo de contraseñas.
  - Política de control de cambios.
  - Procesos de control de cambios.
  - Procedimientos de detección de intrusos.

- Controles tecnológicos.
  - Listas de control de accesos.
  - Cifrado
  - Detectores de intrusos.
  - Antivirus, Antimalware, Antispyware.
  - Administración de actualizaciones.
  - Controles de versiones.
  - Firewalls.
  - Scanner.

2.6. El proceso de seguridad contempla 4 actos:

1.- Estimación. Es la preparación de los otros tres componentes. Se ha mostrado como una acción independiente porque se ocupa de las políticas, procedimientos, leyes, reglamentos, presupuestos y demás tareas administrativas, más la evaluación técnica de la actitud respecto a la seguridad. Si no se tiene en cuenta alguno de estos elementos, sufrirán daños todas las operaciones siguientes.

2.- Protección. Es la aplicación de contramedidas para reducir la probabilidad de un compromiso. El termino prevención es equivalente, aunque en ocasiones la prevención fracasa.

3.- Detección. Es el proceso de identificación de intrusiones. Las intrusiones son violaciones de política o incidentes de seguridad en una computadora.

Aunque pueda resultar asombroso, el control externo de los sistemas de una organización no siempre se considera una violación de política. Cuando se enfrentan a un adversario decidido o muy habilidoso, algunas organizaciones prefieren permitir que los intrusos hagan lo que deseen siempre y cuando no interrumpan las operaciones de negocios.

4.- Respuesta. Es el proceso de verificar los resultados de la detección y de dar los pasos necesarios para remediar las intrusiones. Entre las actividades de respuestas se cuentan "parchear y continuar", así como "perseguir y denunciar". El primer punto de vista consiste en restaurar la funcionalidad de los elementos dañados y seguir adelante; el segundo busca remedios legales recogiendo evidencias como pruebas, con objeto de proceder contra el delincuente.

2.7. Firewall o cortafuegos.

Un cortafuegos es un elemento de monitorización y control del tráfico entre redes. Para poder realizar su función, todo el tráfico de entrada o salida debe de atravesarlo.

La función básica y fundamental de un cortafuegos es determinar qué tramas deben transitar de una red a otra. El filtrado se basa en un conjunto de reglas

ordenadas y políticas definidas por el administrador. Las acciones más generales son: aceptar la trama, rechazarla, registrarla, reenviarla o invocar tareas de autenticación. Además, la mayoría de los cortafuegos permite realizar funciones de NAT y de pasarela IP.

El orden de aplicación de las reglas es fundamental. Las políticas principales indican si las tramas que no encajan en ninguna regla de aceptación o rechazo deben ser aceptadas o rechazadas. La política más segura, y más difícil de configurar, es la de rechazar todo lo que no sea aceptado expresamente.

El reenvío de tramas permite la instalación en la red de servidores intermediarios transparentes. Así por ejemplo se pueden redirigir todas las peticiones web a un intermediario web (Web Proxy) o filtrar todo el correo con herramientas antivirus y/o antispam, sin necesidad de configurar nada en los clientes e incluso sin que éstos se enteren.

Los cortafuegos más básicos filtran paquetes a nivel 3 y a nivel 4 (existen encaminadores con capacidades de filtrado a nivel 3, pero no se pueden considerar cortafuegos). También existen cortafuegos extendidos que trabajan a nivel de aplicación (nivel 7) y pueden añadir cifrado, autenticación y traducción de direcciones.

Estos cortafuegos extendidos utilizan más información para posibilitar un mayor refinamiento en la definición de los objetos a proteger. Esta nueva información se divide en:

- ❖ Información relativa al paquete en niveles superiores de la arquitectura; niveles del 4 al 7 (OSI).
- ❖ Información del estado actual y pasado de la comunicación.
- ❖ Información del estado actual y pasado de las aplicaciones.

Como ejemplo de filtrado basado en información de niveles superiores podríamos hablar de protección de URLs, recursos, ficheros, usuarios, etc. O dentro de la gestión del estado puede supervisarse el orden en el que se realizan los diferentes comandos de una conexión FTP: autenticación, apertura de canales, transferencias, etc.

2.8. IPSec.

Los protocolos de IPSec se definieron originalmente en las RFCs 1825 y 1829, publicadas en 1995. IPSec es obligatorio en IPv6 y opcional en IPv4. El objetivo principal de IPSec es proporcionar protección a los paquetes IP.
IPSec establece comunicaciones IP con seguridad de extremo a extremo, lo que significa que los nodos intermedios utilizan el protocolo IP, sin necesidad de una implementación específica para IPSec.

Antes de iniciar el envío de datos, IPSec realiza una autenticación de los extremos y negocia los parámetros de la comunicación. Durante la comunicación utiliza ISAKMP (Internet Security Association and Key Management Protocol) para realizar cambios dinámicos de las claves.

Para la comunicación IPSec permite utilizar dos protocolos diferentes: AH (Authentication Header) y ESP (Encapsulation Security Payload). El protocolo AH permite únicamente verificar la integridad del paquete (mediante firma). El protocolo ESP permite cifrar la información (DES, 3DES...) y opcionalmente verificar la integridad del paquete.

Los protocolos de IPSec actúan en la capa de red, la capa 3 del modelo OSI. Otros protocolos de seguridad para Internet de uso extendido, como SSL, TLS y SSH operan en la capa de transporte o por encima (capas OSI 4 a 7).

Esto hace que IPSec sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP, los protocolos de capa de transporte más usados. Así para que una aplicación pueda usar IPSec no es necesario modificarla, mientras que para usar SSL y otros protocolos de niveles superiores sí.

Hay dos modos de operación de IPSec: modo transporte y modo túnel.

- Modo transporte: El modo transporte permite que dos equipos se comuniquen entre ellos utilizando IPSec igual que utilizarían IP, pero firmando y/o cifrando los datos que se transfieren (la carga útil del paquete IP).
- Este sistema añade poca sobrecarga de bytes y permite a los dispositivos de la red conocer el origen y el destino del paquete, lo que puede ser necesario para algunos servicios como QoS.

El sistema de encaminamiento no varía respecto a IP, ya que no se modifica ni se cifra la cabecera IP; sin embargo, cuando se utiliza integridad con AH -que firma la cabecera IP-, las direcciones IP no pueden ser traducidas (p.e. con NAT), ya que eso invalidaría la firma del paquete (hash). Para encapsular mensajes IPSec a través de NAT se usa NAT Transversal (NAT-T).

- Modo túnel: En el modo túnel dos equipos establecen un canal de comunicación por el que otros equipos o procesos envían información. Es decir, el emisor y el receptor originales siguen enviando y recibiendo sus datos sin cifrar ni firmar mediante las pasarelas del túnel IPSec (IPSec Proxy), que se encargan de cifrar y/o firmar todo el paquete IP original que debe ser encapsulado en un nuevo paquete IP.
- El modo túnel se utiliza para comunicaciones red a red (túneles seguros entre encaminadores, p.e. para VPNs) o comunicaciones ordenador a red u ordenador a ordenador sobre Internet.

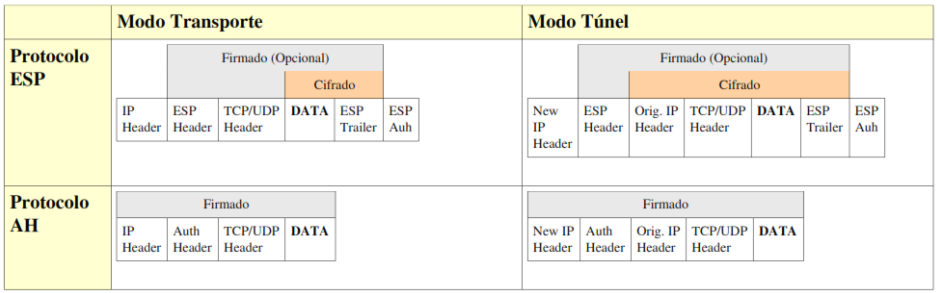


Ilustración 12. Modo TRANSPORTE y Modo TÚNEL.

IPSec no define unos algoritmos específicos de cifrado, sino que mediante ISAKMP permite utilizar IKE (*Internet Key Exchange*) para realizar un autonegociado del algoritmo a utilizar y del intercambio de claves. [3]

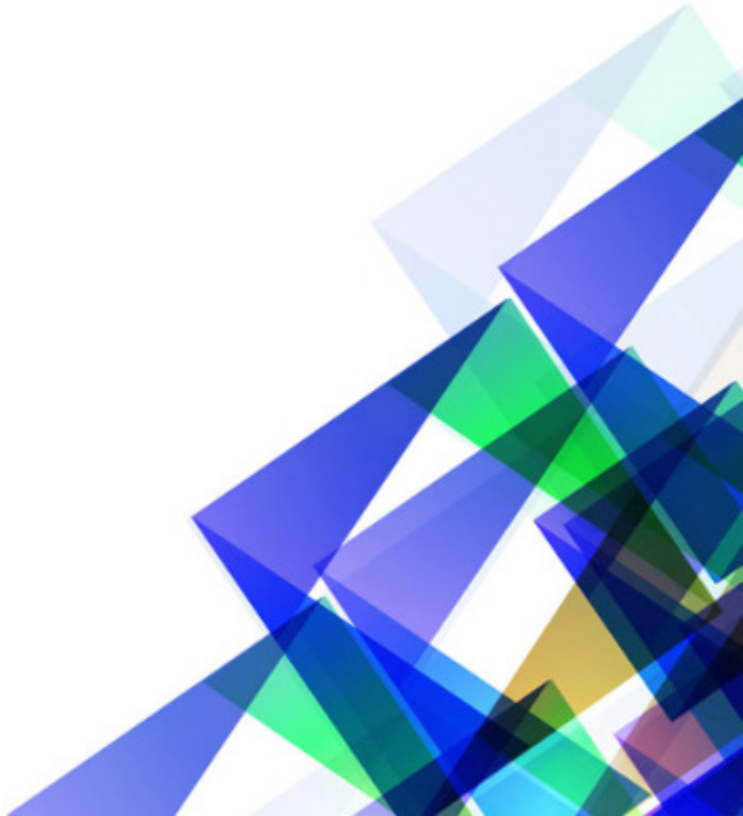
2.9. VLANs.

Las VLANs (Virtual LANs) aparecen para montar redes de nivel 2 independientes compartiendo la electrónica y el cableado. El estándar que las normaliza es el IEEE 802.1Q y su implantación más habitual es por puertos.

Si se configuran 2 puertos de un conmutador en VLANs diferentes, las estaciones conectadas a uno de los puertos no podrán comunicar (en este nivel) con las estaciones del otro puerto.

Se pueden configurar puertos por los que circulen tramas de varias VLANs con un campo especial que define a cuál pertenece cada trama. Estos puertos se suelen llamar 'etiquetados' (tagged) y pueden utilizarse para unir dos conmutadores o un conmutador y un servidor con tarjetas especiales. [3]

Capítulo 3
Caso de estudio
Prep 2015 IEEM



CAPÍTULO 3
Caso de estudio
PREP 2015 IEEM

Programa de Resultados Electorales Preliminares para la elección de Diputados Locales y Ayuntamientos del 7 de junio del 2015 en el Instituto Electoral del Estado de México

3.1. Qué es el IEEM y cómo se rige.

El Instituto Electoral del Estado de México es un organismo público local que de manera conjunta con el Instituto Nacional Electoral, tiene a su cargo la función estatal de la organización de las elecciones locales en el Estado de México.

Conforme la ley que aplica al Instituto Electoral del Estado de México, se encuentra dotado de personalidad jurídica y patrimonio propio, autónomo en su funcionamiento e independiente en sus decisiones, responsable de la organización, desarrollo y vigilancia de los procesos electorales para las elecciones de Gobernador, Diputados a la Legislatura del Estado y miembros de Ayuntamientos, y cuya función la realiza a través del Instituto Nacional Electoral.

Además, es una Institución de carácter permanente, y profesional en su desempeño que se rige por los principios de certeza, imparcialidad, independencia, legalidad, máxima publicidad y objetividad.

Una de las funciones del Instituto Electoral del Estado de México en un proceso electoral es implementar y operar el Programa de Resultados Electorales Preliminares (PREP) de las elecciones locales, de conformidad con las reglas, lineamientos, criterios y formatos que para el efecto emite el Instituto Nacional Electoral (INE).

La Unidad de Informática y Estadística (UIE) del Instituto Electoral del Estado de México, es la responsable del diseño y operación del PREP, por lo cual implementó un Sistema de Gestión de Seguridad de la Información (SGSI) certificado bajo la norma ISO 27001:2013, dentro de este sistema de gestión las telecomunicaciones asumieron un papel fundamental en el proyecto.

El área de Comunicaciones y Servidores de la UIE es responsable de la interconexión de las redes de los 170 Centros de Adquisición y Transmisión de Datos (CATD) y el Centro Estatal de Computo (CEsCo).

El caso de estudio de este reporte, es el proceso de seguridad en la transmisión de los resultados desde los CATD hacia el CEsCo en el PREP, este proyecto operó en la elección pasada de Diputados Locales y Ayuntamientos del 7 de junio del 2015.

3.2. Proyecto de comunicaciones.

Entre más se acerca el proceso electoral, más grande es el interés de la autoridad electoral de mantener la seguridad en la red, por lo tanto, es de suma importancia el mantener la seguridad de la información.

La seguridad no es solamente el implementar usuarios y contraseñas, es el implementar políticas que garanticen la seguridad tanto física como lógica de la información. Dentro del entorno de la red se debe asegurar la privacidad de la información y de proteger las operaciones de daños no intencionados así como deliberados.

3.3. Lineamientos INE e IEEM.

Para realizar las actividades se consideraron los Lineamientos del Programa de Resultados Electorales Preliminares, los cuales establecen que estos son de orden público, de observancia general y obligatoria, tanto para el Instituto Nacional Electoral como para los Organismos Públicos Locales, en materia de la implementación y operación del Programa de Resultados Electorales Preliminares en el ámbito federal y en las entidades federativas, así como para todas las personas que participen en las etapas de preparación, operación y evaluación de dicho programa.

Para mayor información referente a los lineamientos se puede consultar el ACUERDO N°. IEEM/CG/43/2015 en la página electrónica oficial del Instituto Electoral del Estado de México. (www.ieem.org.mx)

Los Lineamientos del PREP estipulan que los objetivos son los siguientes:

1. Establecer las bases y los procedimientos generales a los que deben sujetarse el Instituto Nacional Electoral y los Organismos Públicos Locales para la implementación y operación del Programa de Resultados Electorales Preliminares en sus respectivos ámbitos de competencia.
2. Cumplir con los principios de certeza, legalidad, independencia, imparcialidad, máxima publicidad y objetividad, en el ejercicio de la función electoral relativa al diseño, operación e implementación del Programa de Resultados Electorales Preliminares para el ámbito federal y en cada una de las entidades federativas.

3.4. Qué es el PREP.

El PREP es el sistema de información que la ciudadanía del Estado de México puede consultar a través de la página institucional el día de la jornada electoral, donde podrá conocer momento a momento, los avances de los resultados preliminares que van obteniendo los partidos y los candidatos a diversos puestos de elección popular a nivel local.

Se establece que el mismo es un programa único, conformado por recursos humanos, materiales, procedimientos operativos, procedimientos de digitalización y publicación, seguridad y tecnologías de la información y comunicaciones, cuyas características, así como reglas de operación e implementación son emitidas por el Instituto Nacional Electoral a través de los referidos Lineamientos, con obligatoriedad para el propio Instituto y los Organismos Públicos Locales. También se señala que no existe la posibilidad de otorgar a terceros la coordinación del mencionado Programa.

Para la implementación y operación del Programa de Resultados Electorales Preliminares, el Instituto Nacional Electoral y los Organismos Públicos Locales en este caso el IEEM, realizaron las siguientes actividades de conformidad con lo establecido en los referidos Lineamientos:

1. Seleccionar e implementar el procedimiento técnico-operativo para la recepción, captura y transmisión de la información.
2. Organizar, dirigir, coordinar y supervisar el sistema informático que se implementará para recabar y difundir los resultados electorales preliminares.
3. Coordinar la implementación del sistema informático, mismo que debe in-

tegrar los procesos de captura, validación, transmisión, recepción, consolidación y difusión de los resultados electorales preliminares de las elecciones federales y locales, en el marco de la normatividad vigente.
4. Implementar las medidas de seguridad para la protección, consolidación y difusión de la información de datos recabados.
5. Coordinar y supervisar, la instalación y operación de los equipos de captura.
6. Capacitar al personal encargado del acopio y transmisión de los resultados electorales preliminares.

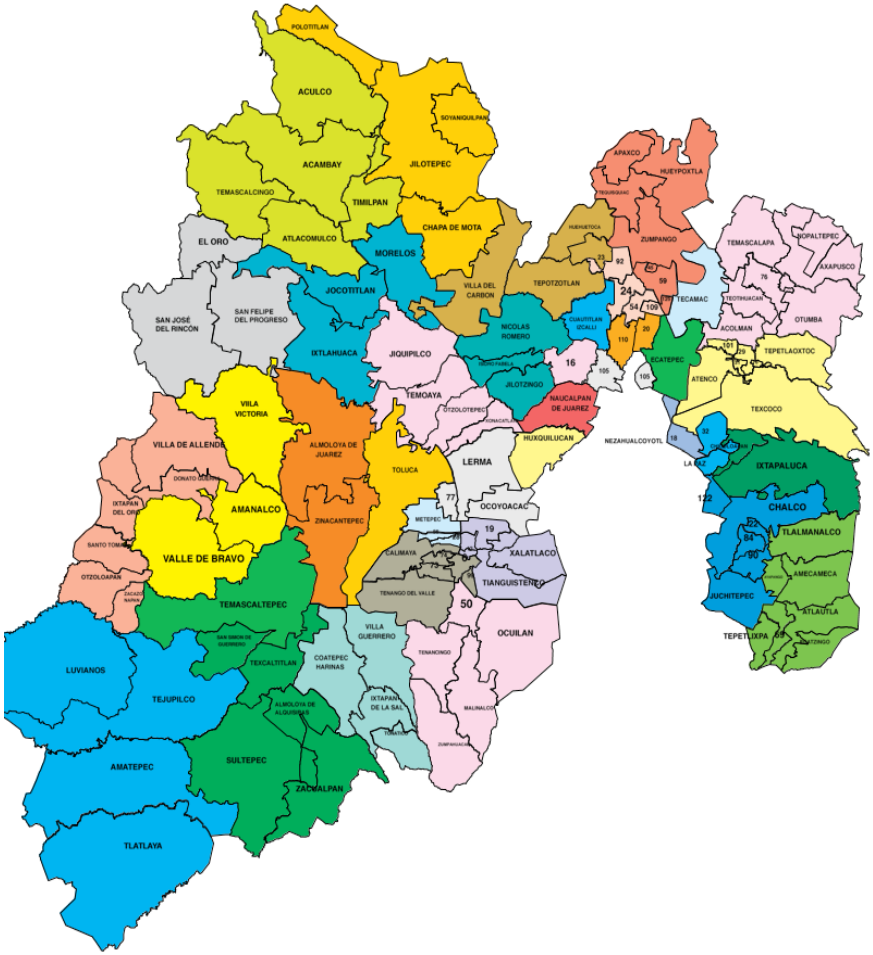
De conformidad con el Código Electoral de la Entidad, se debe establecer un mecanismo para la difusión inmediata en el Consejo General, de los resultados preliminares de las elecciones de Gobernador, diputados o ayuntamientos, al cual tendrán acceso en forma permanente los miembros del Consejo General.

También el Código Electoral del Estado de México, precisa que la etapa de la jornada electoral se inicia a las 08:00 horas del primer domingo de junio del año que corresponda y concluye con la publicación de los resultados electorales en el exterior del local de la casilla y la remisión de la documentación y los expedientes electorales a los respectivos consejos distritales y municipales.

La etapa de resultados y declaraciones de validez de las elecciones se inicia con la recepción de la documentación y los expedientes electorales por los consejos distritales o municipales y concluye con los cómputos y declaraciones que realicen los consejos del Instituto Electoral del Estado de México o con las resoluciones que, en su caso, pronuncie en última instancia el Tribunal Electoral del Estado de México.

La difusión de los resultados iniciará a las 20:00 horas del 7 de junio de 2015 y se actualizarán cada 15 minutos hasta las 20:00 horas del día 8 de junio de 2015, salvo disposición en contrario del Consejo General.

Se determina que la ubicación e instalación de los Centros de Acopio y Transmisión de Datos se realice en las 45 Juntas Distritales y 125 Juntas Municipales del Instituto Electoral del Estado de México.



División Política del Estado de México

06	ALMOLOYA DEL RIO	032	CHIMALHUACAN	077	SAN MATEO ATENCO
012	ATIZAPAN	045	JALTENCO	084	TEMAMATLA
016	ATIZAPAN DE ZARAGOZA	050	JOQUICINGO	090	TENANGO DEL AIRE
019	CAPULHUAC	054	MELCHOR OCAMPO	092	TEOLOYUCAN
020	COACALCO	056	MEXICALCINGO	099	TEXCALYACAC
022	COCOTITLAN	059	NEXTLALPAN	101	TEZOYUCA
023	COYOTEPEC	069	OZUMBA	105	TLALNEPANTLA DE BAZ
024	CUAUTITLAN	070	PAPALOTLA	109	TULTEPEC
028	CHAPULTEPEC	073	RAYON	110	TULTITLAN
029	CHIAUTLA	074	SAN ANTONIO LA ISLA	122	VALLE DE CHALCO SOLIDARIDAD
031	CHICONCUAC	076	SAN MARTIN DE LAS PIRAMIDES	125	TONANITLA

Ilustración 13. División Política del Estado de México.

3.5. Actividades y elementos del PREP.

Las actividades y elementos del PREP son los siguientes:

a) Colocación de la primera copia del AEC en el sobre-PREP de la elección correspondiente, actividad que realizan los funcionarios de la mesa directiva de casilla en presencia de los representantes; es el elemento generador de la información de los resultados electorales.
b) Traslado de los paquetes electorales a los consejos distritales y municipales, y recepción de los paquetes y sobres-PREP; esta última actividad se lleva a cabo en la sede de los consejos respectivos, ante la presencia de los representantes. Incluye la entrega del paquete electoral al pleno del Consejo correspondiente y la entrega del sobre-PREP a los CATD.
c) Captura y Transmisión de los Resultados; en el CATD se transcribirán los resultados asentados en las AEC, utilizando para ello el sistema informático de registro de resultados preliminares, también se digitalizarán las actas; la transmisión de los datos y de las imágenes digitalizadas será continua; asimismo, se verificarán los datos registrados y las imágenes de las AEC.
d) Concentración de los resultados; la llegada de los datos y las imágenes vía enlaces de telecomunicaciones al CEsCo permitirá generar los concentrados estatales. Se confirmará que los datos provengan de lugares reconocidos y que correspondan a parámetros válidos, total de votos contra boletas asignadas.

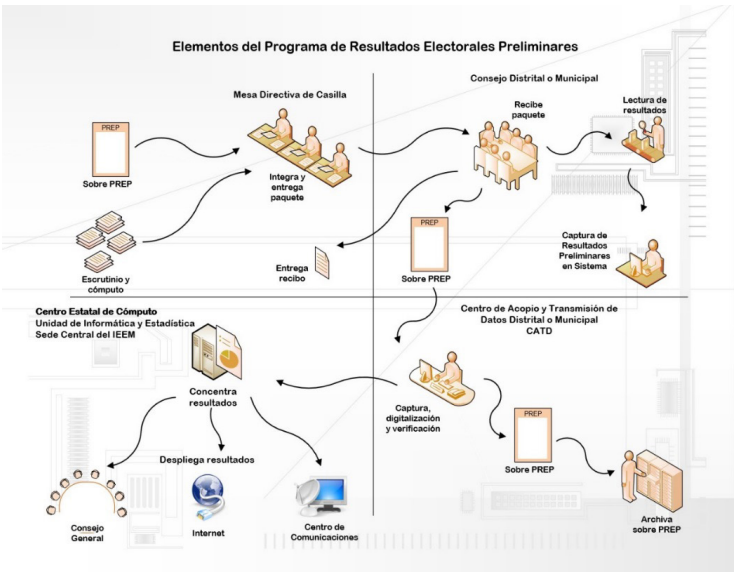


Ilustración 14. Elementos PREP.

e) Presentación de resultados, esta parte utilizará los resultados concentrados y los difundirá a los lugares que se establecen como necesarios: Sala de Sesiones del Consejo General, la red de internet y los portales web de los difusores oficiales; así como al Centro de Comunicaciones, donde se ubicarán los representantes de los medios de comunicación acreditados para la jornada electoral.
f) Seguridad del sistema, para garantizar la continuidad del PREP se estará a lo establecido en el Sistema de Gestión de Seguridad de la Información (SGSI) diseñado para el PREP.

3.6. Proceso Electoral 2015.

Para este proceso electoral se definió lo concerniente a la digitalización del Acta de Escrutinio y Cómputo (AEC), así como su envío y validación, situaciones que se debieron contemplar como parte fundamental del diseño, puesto que condicionó tanto la forma de obtener la imagen del AEC, como el medio de transmisión, así como la plataforma de desarrollo de las aplicaciones.

Construcción: Se elaboró el sistema con tecnología Java Server Pages (JSP), dividido en los módulos de captura numérica de resultados, registro de imágenes y validación de la información numérica, así como las imágenes referentes al AEC.

Asimismo, se elaboró el sistema de respaldo en caso de falla del sistema web, este sistema es de captura local (la información se almacena en las computadoras de las Juntas distritales y municipales).

Pruebas: Dentro de esta fase de pruebas se realizaron los tres simulacros oficiales establecidos en los Lineamientos Operativos, donde se establecieron una serie de compromisos y adecuaciones que fueron atendidos en tiempo y forma. Asimismo, independientemente de estos simulacros oficiales, se llevaron a cabo pruebas extraoficiales durante la última semana de mayo y la primera semana de junio, de lunes a viernes en el horario de 10:00 a 13:00 horas; las pruebas incluyeron tanto la captura y digitalización de las AEC, como los ajustes de equipos servidores y los medios de comunicación, permitiendo con ello llegar a un estado de rendimiento adecuado de toda la infraestructura para el día de la jornada electoral.

Implementación. Los ajustes a los servidores de aplicaciones en cluster, así como los de base de datos, igualmente en cluster, permitieron que la implementación fuera exitosa.

Se aplicaron tres auditorías al sistema informático: dos dentro del Sistema de Gestión de Seguridad de la Información (SGSI) del PREP, y la otra en cumplimiento a lo establecido en el artículo 31° de los Lineamientos del PREP emitidos por el INE.

Sistema de Gestión de Seguridad de la Información, medidas de seguridad para la protección, consolidación, procesamiento y difusión de la información de los datos recabados.

Un SGSI es un medio para minimizar los riesgos, al asegurar que se identifican y valoran los activos y sus riesgos, considerando el impacto para la organización, y adoptando los controles y procedimientos más eficaces y coherentes con la estrategia de la organización que implementa el SGSI.

A partir de la elección de julio de 2009 la Unidad de Informática y Estadística (UIE) del IEEM realizó la primera certificación al SGSI del PREP, bajo la norma ISO/IEC 27001:2005 con vigencia por 3 años; asimismo, en julio de 2012 se obtuvo la re-certificación bajo la misma norma, en ambos eventos auditores externos al IEEM verificaron el cumplimiento de los requerimientos establecidos por la norma.

En este año, el 11 y 12 de abril se llevó a cabo la auditoria interna al SGSI por parte de auditores internos de la UIE, se contó con el apoyo de un auditor invitado de la empresa Seguridad en la Nube S.A. de C.V. (Cloudsec), quienes asesoraron en los trabajos de migración y recertificación; la misión de los auditores fue revisar el cumplimiento de las cláusulas establecidas por la norma ISO/IEC 27001, en la nueva versión 2013; dando como resultado: nueve no conformidades menores y veintinueve observaciones de mejora; se solventaron las 9 acciones correctivas y las 29 acciones de mejora correspondientes, antes de la recertificación del sistema.

Asimismo, los días 17 y 18 de abril se llevó a cabo la auditoria externa de migración, recertificación y cambio de alcance del SGSI; dicha auditoría la realizaron los auditores externos: Leonardo García y Laura Pérez de la empresa BSI Group México, Bristish Management Systems; se evaluaron las áreas/procesos que se definieron en la agenda del evento. Los resultados obtenidos en la auditoría fueron: 28 oportunidades de mejora y ninguna no conformidad menor ni mayor; con estos resultados se obtuvo la recertificación.

Las oportunidades de mejora se sometieron a un análisis cuidadoso, la mayoría de éstas se aplicaron para el PREP 2015, ya que fueron consideradas importantes y oportunas para mejorar el sistema por parte del Comité de Seguridad,

integrado por el Jefe, los Subjefes y los Jefes de área de la UIE; las restantes oportunidades de mejora se atenderán en el siguiente proceso electoral, ya que debido a los tiempos no fue factible aplicarlas en esta ocasión.

La implementación del SGSI para el PREP en los procesos electorales locales de los años 2009, 2011, 2012 y recientemente 2015, ha permitido entregar buenos resultados y ha proporcionado información veraz y oportuna a los interesados; no han ocurrido eventos de seguridad que ponga en riesgo la información; esto ha permitido que el SGSI se haya convertido en una herramienta necesaria para brindar seguridad al PREP.

3.7. Recursos.

Cada CATD contó con los siguientes recursos:

- Un Supervisor que hizo de Coordinador y fue responsable del funcionamiento del Programa en cada Junta; esta persona la designo el Vocal Ejecutivo y fue seleccionado del personal que integró la Junta, observando que cumplía con el perfil que se indicó por parte de la Unidad.
- Los acopiadores de los sobres-PREP fueron personal de la junta municipal o distrital, según se trate; la cantidad de acopiadores dependió de lo que cada Consejo decidió y fue en función de la cantidad de casillas que instalaron.
- Uno o hasta doce capturistas.
- Una o hasta catorce personas que digitalizaron las actas, algunos de ellos realizaron actividades de preparación de las AEC para ser digitalizadas.
- Los verificadores pueden llegar a ser seis.
- Dos o hasta veinticinco computadoras, estas computadoras estuvieron conectadas en red, a través de un enlace de telecomunicaciones tenían conexión con el CEsCo.
- Hasta siete escáneres para digitalizar las AEC.
- Un equipo de seguridad perimetral (firewall).
- Un enlace digital ADSL que funcionó con una red privada virtual (VPN); en el caso de los 30 distritos y las 15 juntas municipales con la mayor cantidad de casillas a instalar se les otorgó un enlace dedicado (punto a punto); además, todas las oficinas desconcentradas contaron con un enlace de respaldo.
- Una impresora.

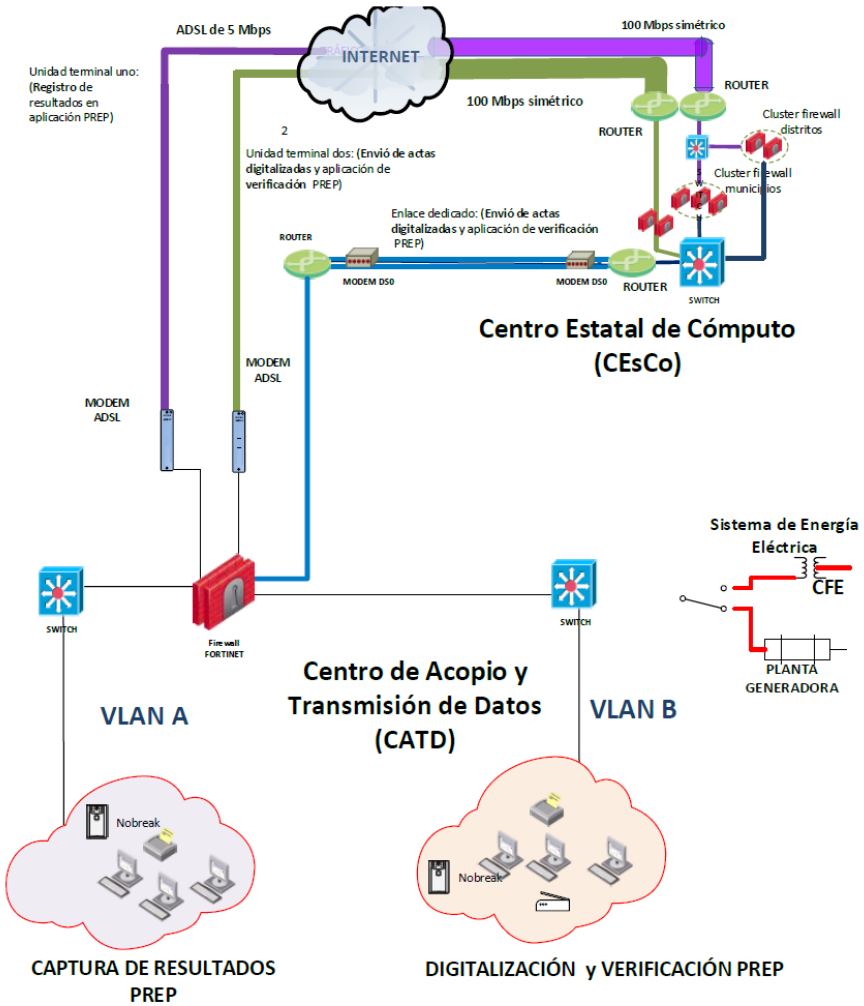


Ilustración 15. Diagrama Centro Acopio y Transmisión de Datos.

3.8. Telecomunicaciones.

Para la operación del PREP se construyó una red de telecomunicaciones que interconectó la red local de cada uno de los 170 CATD (Centro de Acopio y Transmisión de Datos) con el CEsCo (Centro Estatal de Cómputo); además se

adquirió equipo y software para lograr los objetivos planteados en este proyecto, se consideraron las siguientes premisas:

- En primer lugar, se dio prioridad a la captura de los resultados de las AEC.
- En segundo lugar, se consideró la digitalización de las AEC.
- En tercer lugar, se consideró la verificación de las imágenes de las actas contra lo capturado

Además, se consideró como prioridad la seguridad de la información en todo el proyecto del PREP, para lo cual se incluyeron mecanismos de seguridad para dar certeza al manejo de la información.

Se diseñó una red de propósito específico donde se instalaron dos enlaces de comunicaciones en cada uno de los 170 CATD. Por el primer enlace se transmitió la captura de los resultados del PREP, y por el segundo enlace la digitalización de las actas y la verificación de la imagen contra los resultados capturados, dando prioridad a la captura de los resultados.

3.9. Arquitecturas de red.

Este proyecto de red de telecomunicaciones "red IEEM", planteó dos arquitecturas con mecanismos de comunicación independientes:

Arquitectura Tipo 1

Se incluyeron en esta arquitectura los 45 CATD que instalaron la mayor cantidad de casillas, tanto distritales como municipales; en estos CATD, se instalaron dos enlaces para interconectarse con el CEsCo:

El primer enlace fue del tipo ADSL con un ancho de banda de hasta 6 Mbps en promedio, por éste se transmitió la captura de los resultados electorales. Para brindar seguridad en la transmisión de la información a través de esta red de telecomunicaciones, se construyó una red privada virtual (VPN) en cada uno de los CATD, además, la aplicación para la captura fue del tipo web y se utilizó el protocolo HTTPS; las VPN se conectaron desde cada uno de los CATD hasta el CEsCo; para recibirlas en el CEsCo se contó con un enlace a internet dedicado (simétrico) de 100 Mbps.

El segundo enlace fue un enlace digital privado (clear channel) para redes punto a punto, el ancho de banda que se utilizó fue de 256 Kbps, 512 Kbps, 1024 Kbps o 2048 Kbps; la asignación se definió en función a la cantidad de casillas que se procesaron en cada CATD.

En el CEsCo se instalaron 13 multipuntos de 2 Mbps cada uno (en total 26 Mbps), éstos recibieron los 45 enlaces de los CATD; por este enlace se transmitió la digitalización de las actas y se realizó la verificación de las imágenes contra lo capturado; al ser una red privada, los mecanismos de seguridad se dejaron al enlace y a las aplicaciones para la transferencia de archivos (FTP Seguro) y la aplicación de verificación que utilizó el protocolo HTTPS.

Arquitectura Tipo 2

Esta arquitectura se utilizó en los restantes 125 CATD, en éstos se instalaron dos enlaces a internet del tipo ADSL que interconectaron la red de los CATD con el CEsCo; fueron enlaces de hasta 6 Mbps de ancho de banda en promedio. Por uno de estos enlaces se transmitió la captura de los resultados electorales, de la misma forma que en la arquitectura tipo 1.

Por el segundo enlace se transmitió la digitalización de las actas y se realizó la verificación de las mismas, los mecanismos de seguridad que se utilizaron fueron los que se incluyen para la transferencia de archivos (FTP Seguro) y en la aplicación de verificación se utilizó el protocolo HTTPS.

3.10. Servidores.

Se contó con seis servidores, en uno de ellos se instaló un motor de base de datos Oracle versión 12C, sobre un sistema operativo Linux-Oracle, y otro servidor con las mismas características para respaldo de la base de datos; así como dos servidores de transacciones (Front-End), donde se instaló el Web Logic de Oracle versión 12C, y finalmente, dos equipos donde se instaló el servicio de FTP seguro.

3.11. Equipos de cómputo.

Se destinaron 794 computadoras para el registro de los resultados preliminares, la digitalización de las AEC y verificación de datos en cada Junta, la cantidad de computadoras se asignó en función del número de casillas que se ins-

talaron en la demarcación que le correspondía a cada Consejo Distrital local y Municipal –estas casillas fueron aprobadas previamente por el Consejo Distrital del INE que corresponde a cada demarcación-; los criterios se definieron en los Lineamientos Operativos y fueron los siguientes:

a) La captura de datos contó con 397 equipos de cómputo, de los cuales 165 fueron para juntas distritales y 232 para juntas municipales de acuerdo a la política de asignación para captura del PREP.
b) Para digitalizar las actas se asignaron 243 computadoras, 85 para juntas distritales y 158 para juntas municipales.
c) El trabajo de verificación requirió de 154 computadoras, 85 para juntas distritales y 69 para juntas municipales, según las políticas definidas en los Lineamientos Operativos del PREP.
d) El equipo de cómputo que se utilizó para el PREP se instaló a finales del mes de abril de 2015.

La cantidad de computadoras que se destinaron para el registro de los resultados preliminares, la digitalización de las AEC y verificación de datos en cada Junta se asignó en función del número de casillas que se instalaron en la demarcación que le correspondía a cada Consejo Distrital local y Municipal –estas casillas fueron aprobadas previamente por el Consejo Distrital del INE que corresponde a cada demarcación-; los criterios son los siguientes:

a) Para la captura de datos se asignó equipo de cómputo de acuerdo a la política que se define en la siguiente tabla 4:

Tabla 4. Políticas de asignación de equipos de cómputo para captura.

No.	POLÍTICA DE ASIGNACIÓN	COMPUTADORAS
1	Hasta 80 casillas	1 (una)
2	Más de 80 y hasta 200 casillas	2 (dos)
3	Juntas con más de 200 y hasta 350 casillas	3 (tres)
4	Más de 350 y hasta 550 casillas	4 (cuatro)
5	Juntas con más de 550 y hasta 750 casillas	5 (cinco)
6	Más de 750 y hasta 950 casillas	6 (seis)
7	Juntas con más de 950 y hasta 1,150 casillas	7 (siete)
8	Más de 1,150 y hasta 1,600 casillas	9 (nueve)
9	Juntas con más de 1,600 casillas	12 (doce)

b) Para digitalizar las actas se asignó una computadora por cada 300 casillas.

Tabla 5. Políticas de asignación de equipos de cómputo para digitalizar.

No.	POLÍTICA DE ASIGNACIÓN	COMPUTADORAS
1	Hasta 300 casillas	1 (una)
2	Desde 600 casillas	2 (dos)
3	Desde 900 casillas	3 (tres)
4	Desde 1200 casillas	4 (cuatro)
5	Desde 1500 casillas	5 (cinco)

c) El trabajo de verificación requirió una computadora por cada 300 casillas, aunque el primer criterio fue asignar una computadora a partir de las 100 casillas, esto implica que no se les asigno ninguna computadora para esta función, a aquellas juntas que instalaron menos de 100 casillas. Como se observa en la tabla 6.

Tabla 6. Políticas de asignación de equipos de cómputo para verificar.

No.	POLÍTICA DE ASIGNACIÓN	COMPUTADORAS
1	Hasta 99 casillas	0 (cero)
2	Desde 100 hasta 300 casillas	1 (una)
3	Desde 600 casillas	2 (dos)
4	Desde 900 casillas	3 (tres)
5	Desde 1200 casillas	4 (cuatro)
6	Desde 1500 casillas	5 (cinco)

e) El equipo de cómputo que se utilizó para el PREP se instaló a mediados de abril de 2015 en las oficinas distritales y municipales.

3.12. Escáneres.

Se asignaron 243 escáneres de los cuales 85 se instalaron en las juntas distritales, y 158 en las juntas municipales.

Cada escáner fue configurado para funcionar con los siguientes parámetros: el tamaño del Acta es de 43 cm x 21.5 cm, el formato del archivo de salida fue PDF, con una resolución de 200 ppp a color.

3.13. Concentración de resultados.

El procesamiento de concentración de los resultados preliminares se efectuo en el CEsCo, estas actividades estaban contempladas en el SGSI bajo la Norma ISO/IEC 27001:2013.

Sección A. Centro Estatal de Cómputo

En el CEsCo existían los recursos computacionales necesarios para recibir los datos, concentrarlos y consolidarlos estatalmente, así como preparar su presentación y difusión a los sitios determinados por el Consejo General.

El CEsCo se ubicó en la UIE del IEEM, ahí se instalaron los siguientes equipos de cómputo:

- Un servidor de redes virtuales que validó las conexiones de los CATD, rechazando aquellas cuyo origen era desconocido.
- Un equipo de cómputo que registró la llegada de los datos, y los descifró.
- El servidor de base de datos donde se alojaron estructuradamente los resultados preliminares.
- Hubo un equipo que fue respaldo del servidor de base de datos.
- Un servidor que almacenó las imágenes digitalizadas de las AEC.
- Un equipo preparó las presentaciones de los resultados y las colocó en el equipo difusor.
- El equipo que difundió los resultados preliminares también los envió a los otros sitios web (triara).
- Todos estos equipos estuvieron custodiados por un esquema de protección informática ('firewall').
- Se instaló el CEsCo-Res en un lugar diferente al CEsCo, que contaba con equipos de cómputo similares a éste, asimismo, con enlaces de telecomunicaciones suficientes.

3.14. Transmisión de datos e imágenes.

La transmisión se realizó utilizando dos enlaces de telecomunicaciones en cada oficina, uno de ellos se utilizó para transmitir datos y el otro para enviar las imágenes; la actividad de verificación implicó consultar los datos y las imágenes al

mismo tiempo, esto se realizó haciendo uso del segundo enlace. Esta estrategia de transmisión se diseñó de esta forma porque los integrantes de la Comisión de Organización establecieron que se priorizara el procesamiento de los resultados, pero teniendo cuidado de no generar un cuello de botella en la recepción de la información en el Centro Estatal de Cómputo.

En opinión de 163 de 170 órganos desconcentrados la red de cómputo se desempeñó bien o muy bien, y la transmisión de datos obtuvo una buena calificación.

No se presentó ningún incidente de seguridad durante el tiempo de procesamiento de los resultados preliminares; los únicos reportes de malfuncionamiento que se tuvieron se presentaron antes de la operación del PREP en la Jornada Electoral, y éstos fueron los siguientes:

- La oficina municipal de Tenancingo reportó el sábado 6 de junio de 2015 problemas con el acceso a internet, se resolvió el mismo día sábado.
- El distrito de Ixtapaluca manifestó una interrupción del servicio de internet el domingo 7 de junio a partir de las 13:00 horas y que resolvió Telmex a las 15:00 horas del mismo día.

En las 170 oficinas desconcentradas el enlace de telecomunicaciones primario que se instaló fue del tipo asimétricos de tecnología ADSL(Asymmetric Digital Subscriber Line, línea de abonado digital asimétrica) de velocidades diversas de 2 a 10Mbps.

Mientras que el segundo enlace de telecomunicaciones tuvo las siguientes características:

En 45 sitios se instalaron enlaces dedicados síncronos de tecnología Clear Channel (DS0) de diferentes velocidades desde 128Kbps a 512Kbps.

Se instalaron cuatro enlaces satelitales en aquellas Juntas donde no se tenía ninguno de los dos tipos de enlaces.

En los restantes 120 sitios se instalaron enlaces de telecomunicaciones asimetricos del mismo tipo que los enlaces primarios de tipos ADSL.

3.15. Procedimiento de concentración de resultados.

Las actividades que se realizaron en el CEsCo, incluye la verificación y recepción de la información proveniente de los CATD, la generación de una bitácora de transmisiones y/o transacciones a la base de datos, el resguardo y la validación de los datos.

Para el caso de los resultados transmitidos por línea convencional con servicio de ADSL (Asymmetric Digital Subscriber Line, línea de abonado digital asimétrica), la bitácora de transmisiones, que se implementa en el servidor de redes virtuales, contiene datos que hacen referencia a las comunicaciones que se establecen, estos datos fueron los siguientes:

- Identificación del usuario.
- Fecha y hora del inicio de conexión a la red virtual.
- Fecha y hora del fin de la conexión a la red virtual.
- Dirección IP de cada sitio desde donde se conecten.

En el entorno de la base de datos se registraba lo siguiente:

- Directorio o entorno (distrital o municipal) hacia donde se dirige la transacción de origen.
- Acción realizada (registro o corrección).
- Origen de la transacción.

La concentración de los datos implicó que se acumularán los resultados a medida que fueron recibidos, además se realizó la actualización y el respaldo de la base de datos, en la que se acumulaban los resultados electorales ya capturados y transmitidos; guardando una copia de ella, cada 15 minutos, como respaldo. Al recibirse los datos, se adecuaron a un formato preestablecido y se actualizó la bitácora de transmisiones.

Una vez que la transacción se marcó como auténtica, se validaron todos los datos y si la información cumplía con las reglas que se definen para que el acta fuera contabilizada, la información era almacenada en el archivo correspondiente. Todos los indicadores de validación se guardan en una bitácora, independientemente de que el acta sea contabilizada o no.

3.16. Recepción de datos e imágene y almacenamiento en las bases de datos.

Por su parte el enlace de telecomunicaciones que se instaló en el Centro Estatal de Cómputo tuvo un ancho de banda de 100 Mbps, el cual fue suficiente para recibir los datos e imágenes de los 170 órganos desconcentrados, sin que se presentara ningún contratiempo en su funcionamiento.

En la gráfica de utilización del enlace IEEM – Redes privadas virtuales (VPN's) se aprecia en la segunda parte, que la mayor utilización ocurrió entre las 01:00 y hasta las 05:00 horas del 8 de junio, esto coincide con los datos de la llegada de los paquetes electorales.

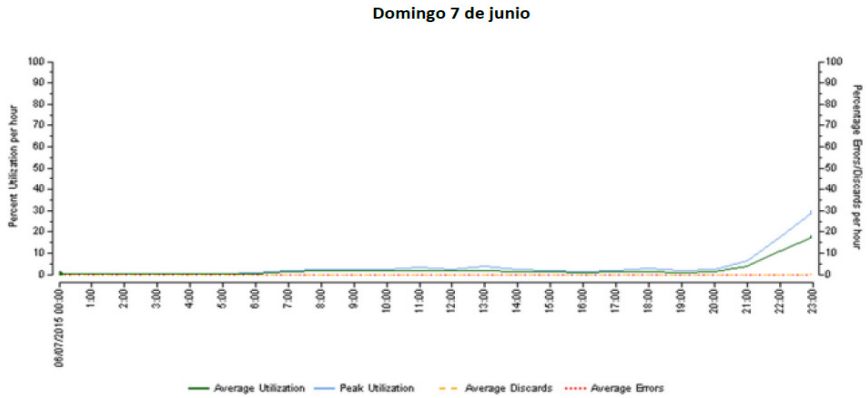


Ilustración 16. Gráfica de utilización del enlace IEEM-REDES VPN de los órganos distritales y municipales. Domingo 7 de junio.

Las telecomunicaciones implementadas para el PREP fueron dimensionadas adecuadamente con el suficiente equipamiento, cluster de dos servidores para el servicio de procesamiento de transacciones y otros tantos para la base de datos; la cifra de utilización del procesador de transacciones fue de 45% de su capacidad de cómputo en el momento de mayor demanda.

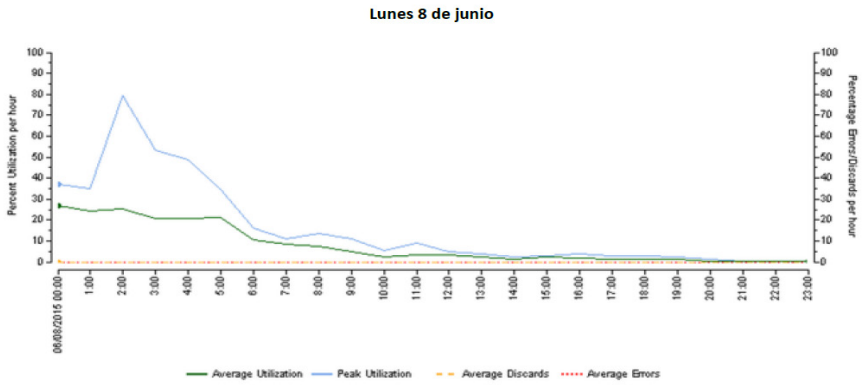


Ilustración 17. Gráfica de utilización del enlace IEEM-REDES VPN de los órganos distritales y municipales. Lunes 8 de Junio.

Por su parte, el manejador de base de datos siempre tuvo un desempeño confiable, para el caso de este servidor el mayor porcentaje de utilización de capacidad de procesamiento se ubicó en 35%.

Asimismo, los equipos que se encargaron de la generación de páginas HTML para dar a conocer los resultados preliminares, trabajaron de manera ininterrumpida y sin contratiempos durante el tiempo de vida del PREP.

Todos los servicios especializados en el Centro Estatal de Cómputo estuvieron resguardados por un esquema de protección de la información –entre sus elementos se contó con un firewall que no fue alterado en ningún momento, permitiendo un desempeño confiable y seguro.

Además de lo anterior, se estableció un Centro Estatal de Cómputo de Respaldo a 40 minutos de distancia de la sede de los órganos centrales del IEEM, donde se instaló equipamiento preparado para la ocasión; estos equipos recibieron datos durante el desarrollo del PREP, fueron monitoreados por personal de la Unidad de Informática y Estadística, quienes se mantuvieron alertas por si fuera necesario procesar y difundir resultados a partir de los datos almacenados en dicho Centro; esto no se requirió, dado que no se tuvo ningún incidente de seguridad en la operación normal del PREP.

3.17. Seguridad en los enlaces.

Ilustración 18. Firewall FortiGate 200D

Para la seguridad en los enlaces se utilizaron redes VPN.

Una Red Privada Virtual (VPN) es una tecnología que permite a los usuarios remotos conectarse a las redes informáticas privadas para ganar el acceso a sus recursos de una manera segura.

En vez de iniciar sesión de forma remota en una red privada que utiliza una conexión a Internet sin cifrar y sin garantía, el uso de una VPN garantiza que terceros no autorizados no tengan acceso a la red y no puedan interceptar la información que se intercambia entre los usuarios y la oficina. También es común el uso de una VPN para conectar las redes privadas de dos o más oficinas. Para formar la VPN se implementaron dispositivos de la marca Fortinet que tienen la capacidad de hablar con el protocolo IPSec por lo tanto entre estos dispositivos establecen túneles virtuales que permiten la comunicación entre ambos dispositivos. Estos túneles son cifrados y cifran la información. Para luego poder ofrecer autenticación y a su vez integridad de la información.

Tunel VPN

La ruta de datos entre la computadora de un CATD y el CESCO a través de la VPN se refiere como un túnel físico, la ruta de datos es accesible sólo en ambos extremos. En el escenario del IEEM, el túnel se extiende entre dos equipos FortiGate. Una conectada en el edificio central del IEEM, y el otro extremo en cada uno de los CATD.

La encapsulación hace esto posible. Paquetes IPsec pasan desde un extremo del túnel al otro como se observa en la ilustración 19y contienen paquetes de datos que se intercambian entre los CATD y el CESCO. El cifrado de los paquetes de datos asegura que algún tercero que intercepta los paquetes IPsec no pueda acceder a los datos.

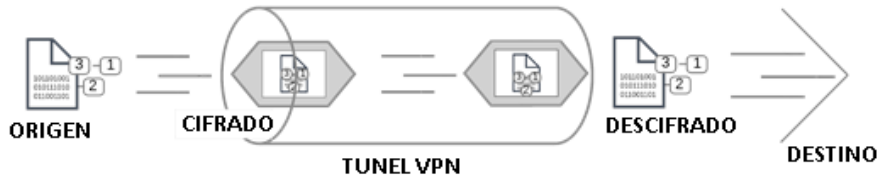


Ilustración 19. Datos codificados que van a través de un túnel VPN.

Puertas de enlace VPN

Una puerta de enlace es un router que conecta la red local a otras redes. La configuración de puerta de enlace predeterminada en las propiedades de TCP/IP de la computadora especifica la puerta de entrada para la red local.

Una puerta de enlace VPN funciona como un extremo de un túnel VPN. Este recibe paquetes IPsec entrantes, descifra los paquetes de datos encapsulados y pasa los paquetes de datos a la red local. Además, cifra paquetes de datos destinados al otro extremo del túnel VPN, los encapsula y envía los paquetes IPSec para la otra puerta de enlace VPN.

La puerta de enlace VPN es una unidad de FortiGate por lo que la red privada local detrás de él está protegida, lo que garantiza la seguridad de los datos no encriptados.

Las direcciones IP de la puerta de enlace VPN fueron la dirección IP de la interfaz de red que se conectó a Internet.

La ilustración 20 muestra una conexión VPN entre dos redes privadas con unidades FortiGate actuando como las puertas de enlace VPN. Esta configuración se conoce comúnmente como VPN IPsec punto a punto.

Aunque el tráfico IPsec puede pasar realmente a través de muchos enrutadores de Internet, se puede visualizar el túnel VPN, como una sencilla conexión segura entre las dos unidades FortiGate.

Una unidad FortiGate en una VPN puede tener una de las siguientes funciones:

- ❖ Servidor - responde a una solicitud para establecer un túnel VPN.
- ❖ Cliente - contacta con una puerta de enlace VPN remoto y solicita un túnel VPN.
- ❖ Punto a punto - nos lleva a un túnel VPN o responde a una solicitud para hacerlo.

La VPN punto a punto se muestra en la ilustración 20, es una relación de igual a igual. Cualquiera de las unidades FortiGate VPN gateway puede establecer el túnel e iniciar las comunicaciones.

Un túnel VPN se establece en dos fases:

En la Fase 1: Se encripta la información, las dos puertas de enlace VPN intercambian información sobre los algoritmos de encriptación que soportan y luego establecen una conexión segura temporal la cual lleva información de los protocolos de seguridad. A su vez esos protocolos nos aseguran la integridad de la información como la autenticación y antireplay.

En la Fase 2: Se instala en el equipo una cabecera de VPN (VPN Header), la cual puede ser AH o ESP o un hibrido entre los dos. Esta cabecera de VPN que tiene información sobre un nuevo paquete IP que es agregado por el Router donde está llevando la información tanto de la IP destino como el origen. Se realiza un intercambio de clave que en IPSec se utiliza el mecanismo IKE y en este escenario se garantiza que la información no es replicada por nada ni por nadie, porque se utiliza el intercambio de claves dinámicas Diffie-Hellman.

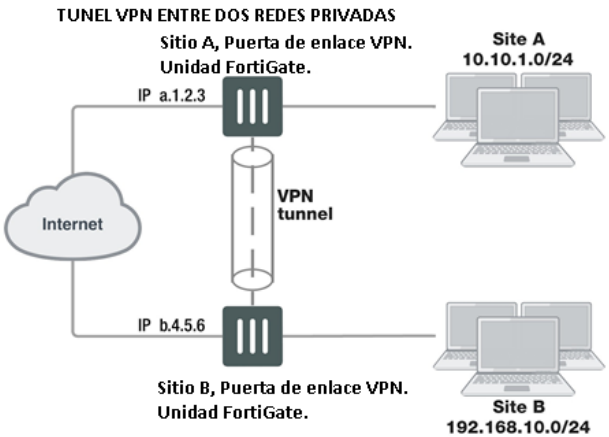


Ilustración 20. Túnel VPN entre dos redes privadas.

Conclusiones.

La labor de la Unidad de Informática y Estadística (UIE) del Instituto Electoral del Estado de México (IEEM) es de suma importancia para las elecciones en el Estado de México ya que implica la gobernabilidad de aproximadamente 15 millones de habitantes. Una de las funciones más importante de la UIE es el Programa de Resultados Electorales Preliminares (PREP). Este programa a mí parecer no solo es el más importante de la UIE, es el más importante en el IEEM ya que el día de la elección es el representativo del trabajo realizado por todas las áreas del Instituto durante un año que es el tiempo que regularmente toma preparar una elección en el Estado de México.

El IEEM cuenta con 324 trabajadores de base, pero para el proceso electoral se requieren aproximadamente 5,000 colaboradores, sumando áreas del edificio central, juntas distritales y juntas municipales.

En cuestiones informáticas hace uso de aproximadamente: 300 ADSL de hasta 6 Mbps (290 para las juntas + 10 de reserva), 45 enlaces digitales (Fracciones de E1 o DS0), 13 multipuntos de 2Mbps (E1), 2 enlaces a internet dedicado simétrico de 100Mbps, 12 servidores, 800 computadoras para el PREP con un total de aproximadamente 1,400 computadoras en todo el IEEM, más de 300 escáneres, más de 340 impresoras. 200 FortiGates 60-D, 5 FortiGates 200-D (2 cluster, en el primer cluster se recibió con 3 Fortigates la información de los municipios y en el segundo cluster se recibió con 2 FortiGates la información de los distritos), y más de700 UPS.

Para todo este equipo la UIE es responsable de la adquisición (compra o renta), distribución, instalación, resguardo, soporte, configuración y mantenimiento.

Los trabajos del PREP 2015 realizados en el proceso electoral 2014-2015, cumplieron lo establecido en los Lineamientos Operativos del IEEM, así como lo requerido por los Lineamientos del PREP emitidos por el INE para lo cual, la tarde de la jornada electoral se certificó ante Notario Público que la base de datos se encontraba en cero, se procesaron los resultados y se digitalizaron las AEC, verificándose que las imágenes correspondieran a los datos registrados; se publicaron los resultados en cortes cada 15 minutos a partir de las 19:00 horas y hasta las mismas 19:00 horas del 8 de junio; durante los días 9 y 10 de junio de 2015 se entregaron los resultados finales y las imágenes digitalizadas que se obtuvieron al cierre del PREP, a los integrantes del Consejo General y de la Junta General.

La infraestructura informática estuvo instalada a tiempo para la jornada electoral conto con sus respectivos respaldos en los enlaces de telecomunicaciones y de otros elementos: tal como computadoras, impresoras y escáneres. El funcionamiento del equipamiento no tuvo contratiempos.

Los controles y salvaguardas que se implantaron en el Centro Estatal de Cómputo y su sitio de respaldo, se diseñaron atendiendo al Sistema de Gestión de Seguridad de la Información (SGSI); no hubo necesidad de acudir a las medidas extremas, ya que el esquema diseñado funcionó adecuadamente, sin haber tenido ningún inconveniente ni mucho menos algún malfuncionamiento.

Respecto a la seguridad en los accesos, pienso que se pudieran implementar accesos biométricos en las áreas que utiliza el personal de la UIE para con ellos poder definir quien tiene acceso en áreas específicas, por ejemplo: sitesswitc, conmutador, access point, idf, almacenes, bodegas, etc. En la seguridad de los CATD se deben verificar las conexiones y asegurar que los equipos se encuentren dentro de los gabinetes con candados que proporciona el instituto ya que si no se hace de esta manera los equipos de comunicación son más vulnerables.

Los equipos que procesaron las transacciones –accesos para registrar o consultar información en la base de datos- y el mismo manejador de bases de datos fueron objeto de un ajuste en su desempeño durante los simulacros las dos semanas previas a la jornada electoral, de tal forma que durante el evento del PREP no presentaron ninguna anomalía.

La difusión de los resultados se priorizó, estableciéndose en primer lugar a los integrantes del Consejo General, luego se indicó que se debían presentar ante los integrantes de la Junta General, posteriormente a los medios de comunicación y después a la ciudadanía en general, a quienes se puso a su disposición hasta tres sitios para la consulta; hubo limitación en la disponibilidad para la ciudadanía, por lo que se necesitan incrementar los puntos de difusión, este es un comentario de los integrantes del Comité Técnico Asesor, de los expertos en la UIE y de la empresa Telmex.

En este documento se describe a detalle la labor que tiene la Unidad de Informática y Estadística del Instituto Electoral del Estado de México en el Programa de Resultados Electorales Preliminares. Dando importancia al Sistema de Gestión de Seguridad de la Información. El cual permitió un ambiente seguro en la interconexión y a su vez afirmo nuestros principios de: certeza, imparcialidad, independencia, legalidad, máxima publicidad y objetividad. Esta información es

un compendio del proceso electoral referente a lo experimentado en la UIE, la información de los acuerdos esta publicada en la página web del IEEM, pero el desarrollo que se describe es una labor de meses de trabajo. Es una elaboración propia utilizando principalmente apuntes de trabajo de diferentes asignaturas universitarias, libros, manuales y acuerdos. Por lo que algunas partes son directamente copia, adecuación o traducción de las fuentes.

Bibliografía.

- Daltabuit, Hernández, Mallen, Vázquez. La seguridad de la información (1ra. Ed.). LIMUSA, 2007.
- Stallings, W. "Fundamentos de seguridad en redes: aplicaciones y estándares" (2ª Ed). Pearson-Prentice Hall, 2004.
- Stallings, W. "Network Security Essentials – Applications and Standars" 3a Edición
- Carracedo, "J. Seguridad en Redes Telemáticas". Mc Graw Hill, 2004.
- Elizabeth D. Zwicky, Simon Cooper "Building Internet Firewalls" (2ª Ed). O'Reilly & Associates, 2000.
- Alberto G. Alexander. "Diseño de un sistema de Gestión de Seguridad de Información Óptica ISO 27001-2005. 2007.
- Acuerdos: INE/CG260/2014, IEEM/CG/81/2014, IEEM/CG/43/2015, IEEM/CO/06/2015.

Referencias.

1. Mathematical Theory of Communication by C.E. Shannon
2. https://prezi.com/tq7ixgpkv8p0/teoria-de-la-informacion-o-teoria-matematica-de-la-comunicacion/
3. http://guimi.net/monograficos/G-Redes_de_comunicaciones/G-Redes_de_comunicaciones.pdf
4. http://serviger.8m.com/ Redes de comunicación.
5. Castells, Manuel (1.997). *La era de la información. Economía, sociedad y cultura (Vol I: La sociedad red)*. Alianza Editorial. Madrid. p. 506. ISBN 84-206-4247-9.
6. Redes de Computadoras - 4ta Edición - Andrew S.Tanenbaum_bye_Axedrez
7. Redes de comunicaciones-2004 2009. http://guimi.net- Montaña. RedIRIS.
8. Alexander, Alberto G. Diseño de un sistema de Seguridad de Información, Óptica iso27001:2005. Editorial Alfaomega.2007.

Acuerdos.

9. Acuerdo INE/CG260/2014.
10. Acuerdo IEEM/CG/81/2014
11. Acuerdo IEEM/CG/43/2015
12. Acuerdo IEEM/CO/06/2015

Glosario.

A

AEC
: Actas de Escrutinio y Computo, 5

C

CATD
: Centro de Acopio y Transmision de Datos., 5

CESCO
: Centro Estatal de Comunicaciones., 5

D

DNS
: Domain Name System. Sistemas de nombres de dominio., 25

DoD
: Department of Defense. Departamento de Defensa de los Estados Unidos de Norteamerica., 22

E

Ethernet
: Es un estándar de redes de área local para computadores con acceso al medio por detección de la onda portadora y con detección de colisiones, 11

F

FTP
: File Transfer Protocol, Protocolo de Transferencia de Archivo, 25

H

HTTP
: Hypertext Transfer Protocol, protocolo de transferencia de hipertextos., 21

I

idf
: IDF Intermediate Distribution Frame
  : Es una habitacion que sirve como distribuidor intermedio de comunicaciones., 64

IEEM
: Instituto Electoral del Estado de México., 5

INE
: Instituo Nacional Electoral, 5

internetworking
: Es la práctica de la conexión de una red de ordenadores con otras redes a través de la utilización de puertas de enlace que proporcionan un método común de encaminamiento de información de paquetes entre las redes., 21

IP
: Internet Protocol, Protocolo de Internet., 16

ISO
: International Organization for Standardization. Organizacion Internacional de Normalizacion., 5

O

OSI
Open System Interconnection, 6

P

PREP
Programa de Resultados Electorales Preliminares, 5

S

SGSI
Sistema de Gestión de Seguridad de la Información., 5
sites
El SITE es una habitacion donde se encuentran los equipos del marco de distribución principal (MDF) y el (POP) (point of presence). Equipos de distribución principal (router, switc, conmutador, access point)., 64
SMTP
Simple Mail Transfer Protocol. En nuestro idioma, dicho concepto puede traducirse como Protocolo para la Transferencia Simple de Correo., 25

T

TCP
Transmission Control Protocol, Protocolo de Control de Transmisión., 16

U

UIE
Unidad de Informatica y Estadistica del IEEM, 6

V

VPN
Virtual Private Network. Redes Privadas Virtuales., 5

W

Web
Conjunto de información que se encuentra en una dirección determinada de internet., 21
WWW
World Wide Web, Red informatíca mundial., 21

CARTA DE CESIÓN DE DERECHOS DE AUTOR

El que suscribe Alan Barajas Belmontes Autor(es) del trabajo escrito de evaluación profesional en la opción de Reporte de aplicación de conocimientos con el título Seguridad en redes de telecomunicaciones en el PREP del IEEM, por medio de la presente con fundamento en lo dispuesto en los artículos 5, 18, 24, 25, 27, 30, 32 y 148 de la Ley Federal de Derechos de Autor, así como los artículos 35 y 36 fracción II de la Ley de la Universidad Autónoma del Estado de México; manifiesto mi autoría y originalidad de la obra mencionada que se presentó en Facultad de Ingeniería.UAEMex (lugar) Toluca, Estado de México. para ser evaluada con el fin de obtener el Título Profesional de INGENIERO EN ELECTRÓNICA.

Así mismo expreso mi conformidad de ceder los derechos de reproducción, difusión y circulación de esta obra, en forma NO EXCLUSIVA, a la Universidad Autónoma del Estado de México; se podrá realizar a nivel nacional e internacional, de manera parcial o total a través de cualquier medio de información que sea susceptible para ello, en una o varias ocasiones, así como en cualquier soporte documental, todo ello siempre y cuando sus fines sean académicos, humanísticos, tecnológicos, históricos, artísticos, sociales, científicos u otra manifestación de la cultura.

Entendiendo que dicha cesión no genera obligación alguna para la Universidad Autónoma del Estado de México y que podrá o no ejercer los derechos cedidos.

Por lo que el autor da su consentimiento para la publicación de su trabajo escrito de evaluación profesional.

a) Texto completo. ☐
b) Por capítulos. ☐
c) Solamente portada y tabla de contenido. ☒

Se firma presente en la ciudad de TOLUCA, ESTADO DE MEXICO a los 10 días del mes de AGOSTO de 2016.

ALAN BARAJAS BELMONTES

Nombre y firma de conformidad