Sistemas de video seguridad en las redes convergentes

Guillermo Raúl Rodríguez – Universidad de Palermo – Buenos Aires – Argentina
Tutor: Lic. Pablo Alejandro Lena (MBA)

***Resumen*: La realización de este trabajo final aborda los sistemas de video seguridad en las redes convergentes haciendo un análisis de la evolución de los sistemas de videovigilancia, así como también la problemática que existe en las redes convergentes, repasando sus limitaciones y riesgos frente a ciertos ataques que vulneren la información, proponiendo a su vez herramientas y soluciones de seguridad más completas. Se detalla también nuevas tecnologías respecto a video seguridad y lo importante que es la capacitación y sensibilización del personal en esta área.**

Índice de terminos: **Networking**, **Router**, **Internet, software defined networking.**

I. Nomenclatura

API: Application Programming Interface.
DHCP: Dynamic Host Configuration Protocol.
DVR: Digital Video Recorder.
IDS: Intrusion detection system.
IPS: Intrusion detection system.
IoT: Internet of Things.
ISP: Internet service providers.
LAN: Local Area Network.
MAC: Media access control.
MTPL: Modular Plug Terminated Link.
NAS: Network Attached Storage.
NVR: Network Video Recorder.
PD: Powered Device.
POE: Power over Ethernet.
PSE: Power Sourcing Equipment.
QOS: Quality of Service
SAN: Storage Area Networks.
SDN: Software Defined Networking.
TCP: Transmission control protocol.
UDP: User datagram protocol.
VLAN: Virtual Local Area Network.
VPMS: Vlan Membership Policy Server.
VQP: Vlan query protocol.
WAN: Wide Area Network.

II. Introducción

Las primeras cámaras que fueron utilizadas como un elemento de seguridad en un circuito cerrado de CCTV se remonta al año 1942.

Los primeros sistemas solo incluían cámaras en blanco y negro conectadas a monitores y fueron creadas para controlar el lanzamiento de cohetes. Este hecho marca los inicios de la videovigilancia, que a lo largo de todos estos años ha tenido un gran crecimiento.

En sus comienzos, la videovigilancia requería de un circuito cerrado continuamente monitoreado por un humano para funcionar, para luego dar lugar a la primera evolución de esta al incorporar las primeras cintas de video que permitían grabar lo que sucedía en las cámaras.

En los años 60, la videovigilancia se hizo más común ya que durante esta década muchas de las cámaras empezaron a ser colocadas y/o ubicadas en puntos estratégicos en lugares públicos.

Antes de comenzar la próxima década, los bancos y tiendas comienzan a usar esta tecnología como una medida de seguridad en contra del hurto. Durante las siguientes dos décadas al utilizar mejores tecnologías, las cámaras lograron una mejor resolución en situaciones de poca luz. En consonancia, una drástica reducción del tamaño de las mismas, lo que origino que se adentren en los hogares como un método de mantener a la familia y al hogar más seguros.

Durante y después de los años 90's, se marca un nuevo hito con el lanzamiento de las primeras cámaras IP, lo que proporciona el nacimiento de la videovigilancia.

Las cámaras se conectan a la red de internet sin la necesidad de un computador, lo que permitía a los usuarios poder supervisarlas constantemente desde cualquier dispositivo con conexión de Red.

En la actualidad, la videovigilancia es una herramienta indispensable de la seguridad y con el ultimo avance relacionado al reconocimiento facial, hace de la videovigilancia una herramienta atractiva para muchos negocios e inclusive muchos gobiernos de diferentes países. De acuerdo con un reporte de videovigilancia de 2017, dirigido por IFSEC International (exposición y conferencia internacional contra incendios y seguridad, donde impulsan la innovación con áreas claves como videovigilancia, seguridad IP, etc.), se determinó que los sistemas de seguridad basados en DVR y en nube, eran vulnerables a intrusiones maliciosas [1].

Con eventos como la intrusión en el circuito cerrado de televisión de la policía de Washington D.C, ocho días antes de la inauguración presidencial donde asumía Donald Trump, se

vieron comprometidas casi el 70% de las cámaras del circuito cerrado de la policía, donde después de las investigaciones pertinentes encontraron dos tipos de Ransomware en los dispositivos de grabación, en el cual se vieron afectadas 123 de 187 video grabadoras en red. Para resolver esto tuvieron que desactivar todos los dispositivos, eliminar el software y reiniciar el sistema en cada ubicación física [2].

Es por este, uno de los tantos casos, que la preocupación por la seguridad cibernética en la videovigilancia se ha convertido en un punto a seguir para las soluciones de seguridad.

Actualmente, la seguridad es un servicio, que no solo incluye la videovigilancia, sino que incorpora la seguridad de red y la seguridad de software.

Hoy en día, las empresas que fabrican estas cámaras trabajan en el hardware y software, con herramientas como la seguridad de extremo a extremo, permitiendo que las soluciones de seguridad sean más asequibles a los usuarios, más seguras y les permitan mayor control de todo lo que sucede en áreas de trabajo, hogares y espacios públicos. La videovigilancia se convirtió en una parte muy importante e indispensable de la seguridad a un nivel mucho más alto de lo que se habría esperado en la década de los 40's.

Gracias a la construcción de base de datos o nubes ya sean públicas o privadas, han hecho que la videovigilancia sea muy atractiva para cualquiera que quiera estar protegido de cualquier posible ataque, en cualquier momento y con un esfuerzo aceptable.

Aquí trataremos de abordar de acuerdo con el contexto de la videovigilancia IP en redes convergentes, como colaborar y fortalecer con herramientas y técnicas la llegada de la videovigilancia IP a las redes convergentes y es por ello por lo que vamos a detallar más en profundidad en el Capitulo III, que son las redes convergentes. Asimismo, detallamos más en profundidad en el Capítulo IV, sobre la diferencia de las redes dedicadas y las redes convergentes para entender un poco que es cada una de ellas y cuales son las ventajas que introdujeron esta última a las tecnologías de hoy en día nos permiten estar conectados compartiendo una misma infraestructura de red para diferentes tipos de tráfico.

Por otro lado, tenemos que tener en cuenta ciertas estrategias en el diseño e infraestructura al introducir videovigilancia IP en cualquier organización y es por ellos que incursionamos a fondo en el Capítulo V sobre el uso de vlans en redes convergentes y sin dejar de lado el Capitulo VI(Ancho de banda en videovigilancia IP), ya que el mismo es un tema crucial en las redes convergentes para toda aquella organización que desee utilizar Videovigilancia IP, así como las diferentes técnicas detalladas en el Capítulo VIII(Unidifusión, multidifusión y Difusión Amplia en Videovigilancia IP) al momento de seleccionar el mejor método para él envió de tráfico, de acuerdo a su infraestructura y necesidades, y sin dejar de lado en el Capítulo IX la calidad de servicio que en conjunto hacen posible a toda esta infraestructura poder mitigar posibles problemas detallados anteriormente.

No obstante, hay que tener en cuenta muchos factores que vamos a mencionar en el Capítulo X sobre las soluciones propuestas para todo lo que es el diseño, seguridad y herramientas que pueden ayudar a cualquier organización a mitigar y mantener protegida la red, así como también herramientas y técnicas para la misma. En el capítulo XI se describirán las conclusiones de esta investigación y finalmente en el capítulo XII hablaremos de las futuras líneas de investigación junto al anexo en el capítulo XIII que abarca los tipos de ataques mencionados en capítulos anteriores.

III. QUE SON LAS REDES CONVERGENTES Y COMO AYUDAN A ESTE MUNDO CADA VEZ MÁS CONECTADO

Las redes convergentes son aquellas que integran diferentes tipos de servicios de comunicación, como voz, datos y video, en una única infraestructura de red. Esta integración permite la transmisión simultanea de diversos tipos de datos a través de un mismo medio físico, como cables de fibra óptica o redes inalámbricas.

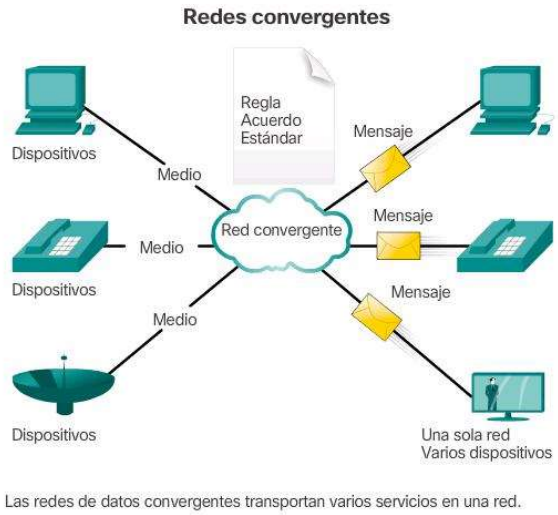


Fig. 1. Gráfico de Redes Convergentes.

La evolución tecnología en las comunicaciones viene avanzando a un ritmo exponencial, por ello se requiere de una infraestructura acorde con estas nuevas tecnologías.

De acuerdo con los comentarios por empresas expertas en el rubro, allá por el año 2017, pensaban que para el año 2023 se esperaba que las aplicaciones de IoT tengan casi 30 mil millones de dispositivos conectados tanto en el hogar, como en edificios, y adentro de las cuidades inteligentes, una cifra que ascenderá hasta los 80 mil millones para 2025. A medida que IoT y los edificios inteligentes continúan adaptándose en Latinoamérica, se están instalando más dispositivos que requieren nuevas formas de conexión.

Tener múltiples sistemas de comunicación en una sola red, ofrece muchos beneficios en cuanto a su administración, rapidez de implementación y otros aspectos que no son posibles con infraestructuras separadas. Por este motivo nacieron las redes convergentes que se posicionaron como la coexistencia eficiente de telecomunicaciones, transmisión de voz sobre IP y video, navegación web, transmisión de medios, juegos en línea, comercio electrónico, y flujo de datos dentro de una sola red.

El diseño de redes también fue una de las cosas que han

evolucionado ya que en el pasado se determinaba el número de puntos de red que se necesitaría para las computados, teléfonos e impresoras y esto en la actualidad ha cambiado y se deben integrar a estos nuevos diseños los nodos de iluminación PoE (que contempla la alimentación a través de Ethernet y con 15.4 Watts de potencia por puerto), control de acceso, cámaras de seguridad, sensores ambientales, sistemas inalámbricos, etc.

Este aumento de los nuevos dispositivos conectados a la red nos lleva a nuevas maneras de conexión, y en este sentido se destacan los enchufes de terminación directa en campo MTPL (enlace terminado con conector modular). El mismo es óptimo para cámaras de seguridad, equipos de iluminación PoE y puntos de acceso inalámbricos. Tecnologías como PoE es la base de la hiper conectividad de dispositivos, ya que el mismo distribuye la energía por el cableado en forma conjunta con los datos, lo que ha permitido incorporar diferentes soluciones y converger la red para mayor control y facilidad de gestión.

Se necesita definir los componentes de cableado estructurado de una manera óptima ya que los mismos tendrán que lidiar con altas temperaturas y garantizar que las aplicaciones de alimentación remota puedan funcionar, con los niveles más altos de potencia ofrecidos por el nuevo estándar IEEE802.3bt que en otras palabras no es más ni menos que PoE++ (el cual ofrece hasta 100watts de potencia por puerto) con sus dos derivaciones tipo 3 y 4 (Equipo de fuente de alimentación PSE y el dispositivo alimentado PD). El cable cat6A (cable de par trenzado estandarizado para Ethernet con soporte de velocidad de 10Gbps) hace un trabajo mucho mejor para disipar el calor en comparación con categorías 5E (cable de par trenzado mejorado) y 6 (cable par trenzado con velocidad de hasta 1Gbps) y por ende es más eficiente ya permite un mejor desempeño térmico lo que traduce más potencia transferida.

Estos productos mencionados anteriormente responden a las tendencias del internet de las cosas y alimentación vía PoE, y son la infraestructura que complementa las redes inalámbricas Wifi6, que también forma parte de las tendencias en las redes convergentes. La misma tiene sus ventajas para las redes inalámbricas como ser capacidades de rendimiento más altas para los usuarios, así como el incremento de la vida útil de las baterías de los dispositivos y mayor seguridad encriptada con WPA3, aunque no olvidemos que WPA3 no es un nuevo estándar o protocolo, sino que se tata de un programa de certificación que especifica los estándares y protocolos que un producto debe soportar. Al permitir múltiples dispositivos en una AP se fortalecen las soluciones de automatización, navegación en la red, aplicaciones de realidad aumentada, sensores de temperatura y dispositivos inalámbricos que la misma permite tasas de hasta 10Gigabits por segundo.

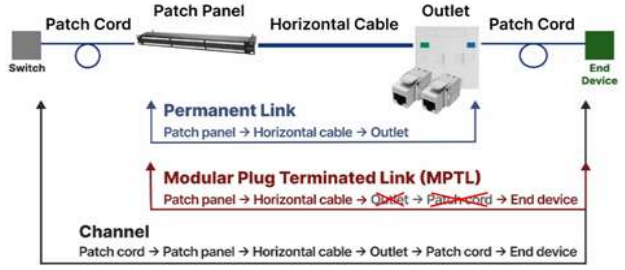


Fig. 2. Gráfico que demuestra uso con MPTL vs Outlets

El objetivo de las empresas que están diseñando redes convergentes o actualizando las redes de sus clientes para soportar estas tendencias, es implementar infraestructuras lo suficientemente robustas que soporten este manejo de información, con componentes certificados y aprovechando todas las capacidades que brindan las soluciones de cableado estructurado y soluciones inalámbricas en cuanto a gestión, seguridad y desempeño [3]-[4].

IV. Redes dedicadas vs redes convergentes en videovigilancia IP.

En las redes dedicadas tenemos una red para datos, una red para telefonía y una red para video y estas redes que están separadas, no pueden comunicarse entre sí.

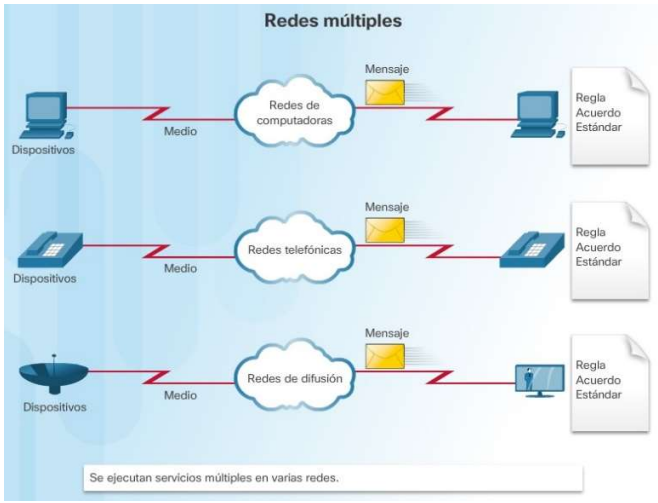


Fig. 3. Gráfico de una red dedicada.

Cada una de estas redes utilizaba una tecnología diferente para transportar las señales de comunicación y adicionalmente cada una también tenía su propio conjunto de reglas y estándares para asegurarse que la comunicación sea satisfactoria.

A diferencia de las redes dedicadas, las redes convergentes pueden transmitir voz, video y datos entre diferentes tipos de dispositivos sobre la misma infraestructura de red y utiliza el mismo conjunto de reglas y estándares de implementación.

Las redes convergentes transformaron durante los últimos años los modelos tradicionales de negocios. Se puede mencionar a modo de ejemplo como la convergencia entre telefonía y acceso a internet, materializada en la telefonía IP, puso en duda al modelo de la telefonía fija tradicional.

La convergencia IP esta basada en los avances a nivel de las redes, que incluye un protocolo único de comunicación, el protocolo IP, a las cuales llamamos redes de nueva generación.

Como detallamos anteriormente se pueden enumerar algunos avances en las diferentes industrias:

A. Telefonía IP

La telefonía IP es la transmisión de voz y datos mediante una única red. Claro ejemplo de esto es la accesibilidad a los

diferentes servicios por parte de los usuarios, ya sea desde su casa como desde otra ubicación, incluso estando de viaje.

B. Televisión Interactiva

Esto es un paquete de software que permite la administración y difusión de una amplia gama de servicios en televisión como se tiene hoy en día.

C. Edificios Inteligentes y Ecología

Se mencionan aquí todo lo relacionado a las alarmas y porteros automáticos conectados a través d video, que mejoran la seguridad de los habitantes.

D. Televisión Interactiva

Esto nos permite utilizar las conexiones existentes, compartir el acceso a internet y velocidades de comunicación mucha más rápida.

De esta manera llegamos a las transformaciones que las redes convergentes están imponiendo hoy en día y ayudando a la videovigilancia IP.

La misma aporta muchísimas prestaciones a los usuarios que según sus necesidades podrían requerir una alta calidad de video y para esto se debe utilizar una red de datos con mayor ancho de banda.

Las redes convergentes en videovigilancia también incluyen el monitoreo, por lo cual las salas de control deben gestionar un numero cada vez mayor de señales de video.

La tecnología IP permite compartir a su vez la información entre los operadores mediante controladores que permiten al mismo tiempo la decodificación de varias decenas de señales de video y su visualización, permitiendo de esta manera un monitoreo y control inteligente.

Podríamos por supuesto utilizar una red dedicada para Videovigilancia IP, pero esto es algo que vamos a mencionar en otro capítulo más adelante para ver las ventajas y desventajas de cuál de los dos tipos de redes mencionadas es conveniente dependiendo las situaciones que se requieran [5].

V. USO DE VLANS EN REDES CONVERGENTES PARA VIDEOVIGILANCIA IP.

El uso de Vlan's en redes de datos es muy común y por ello no es un concepto que precisamente este alejado de los sistemas de videovigilancia, aportan seguridad y organización y esto trae ventajas al sistema.

El termino VLAN significa red de área local virtual, y básicamente el principal objetivo al aplicar VLAN's es el de dividir lógicamente una red en varias redes que pueden estar conectadas físicamente a uno o varios conmutadores de red.

Con esto los dispositivos pertenecientes a un vlan especifica no son visibles o no se pueden comunicar con las de otra vlan perteneciente a otro segmente y viceversa.

El siguiente grafico es un ejemplo de modelo de varias VLAN's en una red compartida.

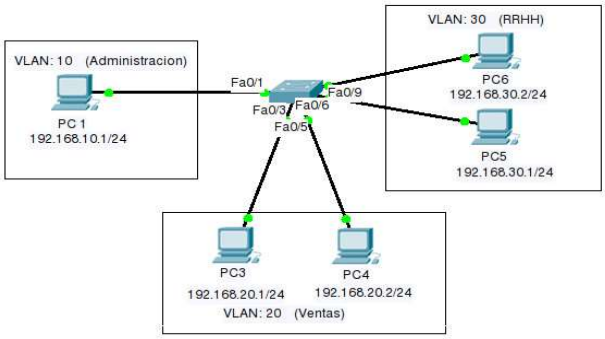


Fig. 4. Gráfico que muestra el uso de distintas vlans en un mismo dispositivo de red.

Hay varios tipos de VLAN, pero vamos a enumerar las dos más importantes en este apartado, estas son las VLAN etiquetadas y las VLAN sin etiquetar.

A. VLAN sin etiquetar

Una vlan que no está etiquetada también se la denomina vlan nativa. En los conmutadores de red por defecto todos los puertos se agregan a una vlan sin etiquetar, en general es la vlan con ID 1, lo que significa que todos los puertos se pueden ver entre sí.

Esta opción generalmente se usa cuando se conectan equipos como estaciones de trabajo o cámaras IP de un sistema de videovigilancia que no etiquetan su propio tráfico, y solo necesitan comunicarse dentro de una VLAN específica.

El beneficio de las VLAN sin etiquetar es una configuración más simple, ya que no se debe realizar ninguna configuración de dispositivos o host como cámaras, servidores, etc., y esto es porque el switch limita el tráfico a la VLAN.

Sin embargo, los puertos de interés solo se pueden asignar a una sola VLAN sin etiquetar. Por lo tanto, si un dispositivo específico debe ver varias VLAN, como el servicio de impresión en un ambiente de oficina, los NVR en un sistema de videovigilancia o un sistema de VoIP, se deberá optar por la opción de VLAN's etiquetadas o de otro modo realizar enrutamiento de los segmentos de VLAN requeridos, lo que agrega costos y complejidad.

B. VLAN etiquetadas

Los puertos también se pueden etiquetar con un ID de VLAN específico, esto se define en el estándar 802.1Q. El tráfico que entra y sale del puerto se etiqueta con una identificación específica que es identificada por el dispositivo receptor.

El beneficio de las VLAN etiquetadas es que los puertos se pueden asignar a más de una VLAN, a diferencia de las no etiquetadas. Sin embargo, los dispositivos o host conectados a estos puertos también deben ser compatibles con 802.1Q.

Algo muy importante a tener en cuenta es que 802.1Q no es compatible con la mayoría de las cámaras IP u otros dispositivos de seguridad, y requiere la instalación o configuración de componentes adicionales del sistema operativo en las PC. Debido a esto, las VLAN etiquetadas generalmente solo se usan para enlaces de tipo troncales o de

alta velocidad.

También es importante entender que diferencias hay entre las VLAN estáticas frente a las dinámicas. En la mayoría de las redes de videovigilancia, la mayoría de las veces se utilizan estáticas por puerto, y al estar basadas en puertos son las más sencillas de configurar, pero se deben de reconfigurar manualmente si se mueven o agregan dispositivos lo cual no lo hace muy práctico. En cambio, al utilizar las mismas dinámicamente, se pueden configurar por MAC, es decir que cuando una cámara de videovigilancia es agregada a un puerto, el conmutador se encargara de consultar la base de datos del servidor de configuración de vlans para la asociación de la vlan correspondiente.

Esto proporciona mayor flexibilidad ya que los dispositivos pueden conectarse a cualquier puerto y reorganizarse según sea necesario. Sin embargo, la configuración inicial de las vlan dinámicas lleva mucho tiempo, ya que se deben crear la base de datos o las macros con los identificadores o las reglas del dispositivo, lo que hace que se usen con menos frecuencia, especialmente en videovigilancia, ya que por lo general los servidores, cámaras y otros equipos suelen permanecer conectados en la misma red, puerto y en general no se mueven.

Ahora podemos enumerar algunos beneficios de utilizar vlan's, ya que este aumenta la seguridad, al estar segmentado el tráfico en su totalidad, haciendo que la vigilancia puede coexistir de forma segura en el mismo switch de red con el trafico general de datos o de voz. Como dijimos antes, son invisibles entre sí. Podemos destacar que al utilizar vlan's, técnicamente estamos reduciendo la cantidad de trafico en la red LAN, ya que las transmisiones no se envían a toda la red física, sino solo a la vlan de interés, pero también es cierto que si en un LAN de 40 cámaras, tendrá poco o ningún efecto ya que podrían superar la capacidad de la red.

Podemos utilizar QoS (calidad de servicio) dentro de una vlan, lo que podría dar lugar a darle prioridad a una vlan de videovigilancia, al poder recibir mayor prioridad de trafico de datos que las vlan generales de datos.

Ahora podríamos describir algunos escenarios de Vlan para videovigilancia, ya que la forma en que se aplican varía según la aplicación [6].

Sistemas pequeños:

En los sistemas que utilizan un número muy reducido de cámaras, como ser algún comercio minorista, las Vlan no se utilizan generalmente ya que se utilizan conmutadores que no son administrados, de bajo costo en general y sin compatibilidad con Vlan.

Red convergente:

Al compartir una red LAN con otros servicios, como puede ser el caso de escuelas, oficinas pequeñas y medianas, se implementan normalmente Vlan's, para separar lo que es voz, datos y otra para seguridad, ya que esto permite segmentar mejor los servicios. Esto requiere el enrutamiento entre la Vlan los servicios de oficina y la vlan de seguridad para dar acceso al video por parte del personal, que deben tener la gestión y el control sobre el mismo.

Red dedicada sin VLAN:

Al utilizar una red separada y dedicada para cámaras, no se requiere a menudo la configuración de vlan's. En caso de necesitar acceso desde la red LAN general, las dos redes físicas que están separadas requerirán de un enrutador (router) para el caso.

Red dedicada con VLAN:

En sistemas de mayor tamaño, se pueden utilizar varias VLAN, a menudo, inclusive si se utiliza una red dedicada para seguridad. Los clientes y las cámaras se colocan en vlan's separadas, ya que esto evita la manipulación por parte de los usuarios de estaciones de monitoreo que acceden directamente a las interfaces web de las cámaras.

VI. Ancho de banda en videovigilancia.

En el ámbito del networking, el ancho de banda para la transmisión de datos de video juega un papel fundamental en el éxito de cualquier proyecto de videovigilancia en red. Ignorar este aspecto o subestimar su importancia puede acarrear una serie de problemas desde el inicio del proyecto, incluso antes de su finalización.

Vamos a enumerar algunos de estos aspectos básicos y más importantes.

Escalas de transmisión en videovigilancia (Bits, bytes):

En informática la unidad básica de información es el "bit", significa dígito binario, puede tener dos valores 0 o 1 y es usada como unidad de medida tanto para flujo de información como para almacenamiento. Es importante que se comprenda la diferencia cuando nos referimos a ancho de banda, velocidad de transmisión de datos, y cuando nos referimos al almacenamiento.

En videovigilancia en red, el ancho de banda también se mide en bits, pero en algunos casos es posible encontrar información técnica relacionada con transmisión de datos en bytes, lo que puede generar alguna confusión. Solo debe tener presente que 8 bits equivalen a 1 byte.

Por ejemplo, si en una ficha técnica de una cámara se refiere al consumo de ancho de banda de 3 megabytes por segundo y en otra, 24 megabits por segundo significan que ambos equipos consumen el mismo ancho de banda.

Sin embargo, lo más común es que en transmisión de datos la medida sea en bits y para almacenamiento se de en bytes. A continuación, mostramos dos tablas de equivalencia como referencia.

Tabla 1
Unidades usadas para la transmisión de datos en bits.

Unidad de ancho de banda	Abreviatura	Equivalencia
bits por segundo	bps	1 bps=unidad fundamental del ancho de banda
Kilobits por segundo	Kbps	1 Kbps=1.000 bps=10^3 bps
Megabits por segundo	Mbps	1 Mbps=1.000.000 bps=10^6 bps
Gigabits por segundo	Gbps	1 Gbps=1.000.000.000 bps=10^9bps
Terabits por segundo	Tbps	1 Tbps=1.000.000.000.000 bps=10^{12}bps

TABLA 2
UNIDADES DE MEDIDA PARA ALMACENAMIENTO EN BYTES.

Unidad de medida almacenamiento	Simbolo	Equivalencia	Equivalencia (bytes)
byte	B	8 bits	1 byte
kilobyte	KB	1024 bytes	1.024 bytes
megabyte	MB	1024 KB	1.048.576 bytes
gigabyte	GB	1024 MB	1.073.741.824 bytes
terabyte	TB	1024 GB	1.099.511.627.776 bytes
petabyte	PB	1024 TB	1.125.899.906.842.624 bytes

Medición del ancho de banda:

El ancho de banda hace referencia a la capacidad de un canal de transmisión para el transporte de datos por unidad de tiempo. Una analogía que se puede usar para ejemplificar el concepto es una autopista; cuanto mayor es el diámetro de la autopista mayor cantidad de autos podrá pasar la misma en un determinado momento.

El ancho de banda en términos de redes nos indica la cantidad de bits que son transmitidos en un segundo por un determinado canal de comunicación, por ejemplo, 100 Kb/s, 1 Mb/s, 1000 Mb/s, etc. Habiendo dicho esto, no se debe confundir la capacidad del ancho de banda con la velocidad de transmisión o recepción también llamadas velocidades de descarga y carga respectivamente.

Generalmente el ancho de banda usado en las redes WAN lo determina la capacidad del proveedor del servicio de internet (ISP), y en las redes más pequeñas estará determinado por la capacidad de las interfaces de red de los equipos que transmiten y reciben la información y el medio de transmisión de la misma.

En los equipos de videovigilancia en red como son las cámaras IP, NVR's DVR's unidades SAN/NAS se deberá consultar las hojas de datos del fabricante para conocer la capacidad de transmisión de los equipos, así como la capacidad de recepción y procesamiento en red para todas las cámaras que puede recibir, lo que generalmente se conoce como "throughput".

También cabe destacar, que muchos fabricantes permiten que mediante la interfaz de usuario se pueda ver el consumo de ancho de banda según la configuración de la cámara.

Cálculo del ancho de banda por cámara:

Es importante realizar el cálculo de consumo de ancho de banda por el total de cámaras que queremos instalar, lo más conveniente es dejar un margen del 25% para crecimiento o ampliación.

Se debe tener en cuenta que la cantidad y ancho de banda que se necesita por cámara puede variar significativamente, y esto va a depender del objetivo de cada una de ellas y de los factores que vamos a enumerar debajo.

A. Resolución

Uno de los problemas que más afectan al consumo de ancho de banda es la resolución de las cámaras, a mayor resolución mayor ancho de banda.

B. Velocidad de fotogramas o imágenes por segundo

Esto hace referencia a la cantidad de imágenes por segundo que la cámara transmite de acuerdo con la configuración del video en vivo, con lo cual esto tiene relación directa con el ancho de banda. Los problemas que más afectan al consumo de ancho de banda es la resolución de las cámaras, a mayor resolución mayor ancho de banda.

C. Escena en vivo

Cuanta más actividad hay en una escena como ser los ambientes de vigilancia ciudadana en donde se dan muchas variables de cambios permanentes, mayor será el ancho de banda necesario.

D. Tasas de bits constantes, variables y máximas

Dependiendo lo que una cámara este captando en un momento y lugar dados, va a ser el resultado de cuanto consuma una cámara. Una cámara podría consumir 2Mbps en una casa, pero la misma en otra casa con mayor afluencia de personas podría consumir 5Mbps. Es por esto que hay varias formas de controlar una cámara en diferentes situaciones con la tasa de bits. Utilizando la tasa de bits variables (VBR), esta cambia para mantener la compresión en un nivel establecido independientemente de la actividad. La tasa de bits máxima (MBR), también cambia, pero no más allá del máximo definido por el usuario y por último con la tasa de bits contantes, esta tasa de bits no cambia, aunque la escena si lo haga. Es por esto por lo que es muy importante, que tasa utilizar dependiendo las escenas.

E. Compresión de datos y ancho de banda

Como mencionamos anteriormente la cantidad e información a procesar en videovigilancia en red es bastante alta, hablamos del orden de miles de millones de bits y más aún si se tienen funciones de análisis de video que aportan metadatos. Es por esto que se deben implementar algoritmos de compresión que se han vuelvo un estándar entre los fabricantes, aunque algunos de ellos desarrollan sus propias versiones.

Entonces podemos decir que existe una relación directa entre la eficiencia del formato de compresión y el consumo de ancho de banda. Es decir, cuanto más eficiente es el formato de compresión de video, menos es el consumo de ancho de banda que se requiere para la transmisión de datos.

Esto es uno de los aspectos de mayor desarrollo y de interés de los fabricantes den videovigilancia en red. Esto podría dar lugar a cámaras más inteligentes lo cual lo vamos a desarrollar en un capítulo aparte.

Los formatos de compresión de videos más utilizados y eficientes son: H264 (ITU-T y ISO/IEC), H265 (ITU-T y ISO/IEC). Estos formatos de compresión vienen evolucionando de manera importante y permitiendo en los últimos años una eficacia de hasta un 80% de consumo de ancho de banda.

F. Ancho de banda para video en vivo y grabación

En algunos diseños las señales de video en red que provienen de las cámaras no siempre llegan primero a un sistema de grabación, incluso puede ocurrir que el sistema de grabación no esté en el mismo sitio o misma red de las cámaras, por ende, es común encontrar dos tipos de tráfico de datos de video: uno para visualización y otro para grabación, ambos consumen ancho de banda y como siempre lo recomendamos deben estimarse a la hora de diseñar la misma.

G. Ancho de banda en redes LAN vs WAN

Los sistemas de videovigilancia pueden estar implementadas en una red de área local (LAN) y sobre la red de área amplia (WAN) como Internet, la transmisión de información a usuarios que pueden consumir datos de video en vivo y grabación redundante.

Un ejemplo puede ser una cadena de supermercados en donde hay una sede principal en una ciudad y sucursales en otras ciudades, cada sede tendrá su sistema de video en red de manera local, pero todos se pueden monitorear de manera centralizada por medio de servicios de canales de Internet.

En este caso, el consumo de ancho de banda local no será un problema por la disponibilidad de la red LAN configurando el perfil de transmisión incluso con la mejor calidad de imagen para visualización y grabación local.

Pero para la transmisión de video por Internet puede resultar muy costoso o simplemente impráctico si no se aplican estrategias de ahorro en consumo de ancho de banda, como vimos anteriormente los formatos de compresión juegan un papel importante en este punto y del mismo modo la configuración de los perfiles de transmisión.

En particular, las conexiones de 100 Mbps y 1000 Mbps son bastante comunes para las redes con interfaces de red en cámaras de videovigilancia típicas. Mientras que las de 10 Gigas suelen ser interfaces de red de los switches de red que concentran las señales y en servidores o NVR`s de última generación.

H. Ancho de banda simétrico vs asimétrico

Que el ancho de banda sea simétrico significa que tanto la transmisión y la descarga serán iguales, es decir si 100Mbps es lo que se tiene de descarga, también se tendrán 100Mbps de subida. Sucede lo contrario con el ancho de banda asimétrico donde la transmisión y la descarga no son iguales, esto último es muy común en hogares o pequeñas empresas. En general se da que las conexiones de ancho de banda asimétricas son los módems de cable con tecnología DSL o algunas satelitales en sitios remotos los cuales llegan a ser muy costosos y poco prácticas para aplicaciones de múltiples cámaras. En cambio, las simétricas son redes de fibra óptica en general pero las mismas se limitan a áreas urbanas densamente pobladas [7].

VII. Seguridad en redes convergentes

En este apartado veremos algunos de los métodos más utilizados por los ciber delincuentes y hackers para vulnerar la seguridad en redes convergentes, que la misma viene dada por un mal diseño a la hora de desarrollarla o incluso por las propias vulnerabilidades de los sistemas que este mismo integran.

Debajo se enumeran algunos de estos ataques:

A. Ataque ARP.

B. Ataque de envenenamiento ARP.

C. Ataque de inundación MAC.

D. Ataque DHCP.

E. Ataque de protocolo de expansión.

F. Ataque de fuerza bruta de multidifusión.

G. Ataque de Vlan privada.

H. Ataque VMPS / VQP.

I. Ataque de salto de Vlan.

J. Ataque de estrés de fotograma aleatorio.

Los Detalles de los ataques se desarrollan en el Anexo I

VIII. Unidifusión, multidifusión y difusión amplia en Videovigilancia IP.

Como mencionamos en capítulos previos el ancho de banda es un tema muy importante en Videovigilancia IP y gracias a mejoras en formatos de compresión de video o códecs, como lo son el H.264 y H.265 han permitido reducir significativamente las demandas de ancho de banda.

De todos modos, muchos integradores y clientes finales enfrentan importantes retos con la gran cantidad de datos de video para transmitir y con la cantidad de múltiples receptores o clientes que deben recibir todos estos datos.

Se analizan debajo los conceptos básicos de las redes de multicas o multidifusión.

Transmisión unidifusión:

Este método se llama también difusión única o unicast, ya que el que envía los datos, se origina desde un único emisor a un único receptor, aun la comunicación sea bidireccional o unidireccional. En la mayoría de las aplicaciones de red, se utiliza la transmisión unidifusión como en el caso del tráfico de datos en internet, cuando un usuario quiere acceder a una página web, se produce una conexión directa entre el cliente y el servidor al cual se está consultando.

En Videovigilancia, el dispositivo origen, en este caso podría ser una cámara IP, trasmite tantas tramas d flujos de video como solicitan los diferentes destinos, esto tiene como inconveniente y es la ineficiencia. Podemos suponer un ejemplo de ellos, al tener una cámara IP está configurada para un tamaño de transmisión de 5Mbps, y 4 clientes solicitan y requieren esos datos, entonces utilizara 20 Mbps de ancho de banda.

A diferencia del ejemplo anterior si al tener una cámara IP que está configurada para un tamaño de transmisión de 5Mbps, y 4 clientes solicitan y requieren esos datos, solo se usaran 5Mbps.

Transmisión multidifusión:

Este método de multidifusión llamado multicast, envía los paquetes de datos de manera simultánea a los receptores que hacen parte de un grupo de interés para la información que se transmite y en este caso no hay una conexión directa entre el origen y los destinos. En este caso, los clientes hacen como parte de un grupo de multidifusión que recibe una sola copia del flujo de datos de video que se replica en cada cliente.

Diferencia entre multidifusión y difusión amplia:

Difusión amplia o broadcast es un modo que permite enviar datos a todos los usuarios que hay en una misma red local, cuando se envían datos a una dirección de IP de broadcast, automáticamente el resto de los usuarios conectados la recibirán.

En los sistemas de videovigilancia IP, la red de difusión amplia no se utilizan sin embargo es importante conocer el concepto. La diferencia importante, es que el hecho de que, en la difusión amplia o broadcast, el envió de información se direcciona siempre a los destinatarios finales de una red o subred, mientras que en el caso multicast o multidifusión, el flujo de datos se transmiten únicamente al grupo de multidifusión, ósea a ciertos destinatarios en donde incluso es posible no todos se encuentren dentro de la misma red.

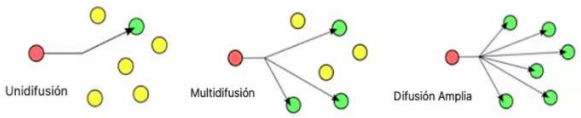


Fig. 5. Gráfico comparativo de unidifusión, multidifusión y difusión amplia.

Uso de multidifusión en sistemas de videovigilancia

Se cree que multidifusión debería estar siempre presente en los sistemas de videovigilancia IP, pero esto no es tan así.

En sistemas típicos de videovigilancia, los destinatarios de los datos de video son pocos, como servidor de grabación, clientes de monitoreo típicamente tres o cuatro y en ocasiones un director o supervisor de seguridad, en estos casos de limitados receptores, el método de multidifusión no estaría ahorrando un gran ancho de banda, y con mayor razón en sistemas pequeños donde inclusive no tengamos cuellos de botella. Incluso, en los casos de que la grabación y la visualización se utilicen en transmisiones separadas, es decir una para el servidor y otra para el cliente, tampoco se ahorrara ancho de banda, ya que, en este caso, cada transmisión se envía solo a un destinatario.

Pero cuando hablamos de implementaciones grandes, donde hay una gran cantidad de clientes que ven una mayor cantidad de cámaras, la multidifusión puede llegar a ser critica. Un ejemplo de esto podría ser un centro de monitoreo para sistemas de vigilancia ciudadana o en ambientes corporativos muy grandes, donde hablamos de cientos o miles de cámaras, que se pueden tener clientes las 24hs del día, que en eventos críticos requieren mucha información simultanea como la policía, bomberos o tránsito [9].

IX. Calidad de servicio en videovigilancia IP

Calidad de servicio (QoS), es el uso de mecanismos o tecnologías que funcionan en una red para controlar el tráfico y garantizar el rendimiento de aplicaciones criticas con capacidades de red limitada.

La calidad de servicio (QoS) está relacionada con la administración del ancho de banda disponible dentro de la red, es bastante usado en video en red y VoIP o incluso cuando dentro de la misma red hay servicios de transferencia de archivos, uso de internet, etc.

El punto principal de utilizar esto es el de tener una mayor estabilidad en la red al priorizar el tráfico de datos, cumpliendo funciones orientadas a mitigar problemas como el retraso, perdida de tramas o paquetes de datos, el bloqueo o congestión de red.

Cuando hablamos de proyectos de videovigilancia, se debe tener mucho cuidado con el uso de calidad de servicio, ya que no siempre hay que implementarlo en un sistema, mas que nada cuando todos los flujos de video provienen de cámaras que están en una única red exclusivamente diseñadas para el sistema de videovigilancia y monitoreo. Si todos son iguales y tienen el mismo nivel de prioridad, no haría falta habilitar calidad de servicio, ya que esto hará que los dispositivos de red como enrutadores o conmutadores utilicen demasiada potencia de procesamiento, cuando no está siendo requerido realmente.

Los dos métodos mas conocidos para calidad de servicio se llaman DiffServ e IntServ. El primero de ellos se utiliza para que los dispositivos marquen los paquetes para hacerlos especiales, para que puedan viajar mediante toda la red y los enrutadores y conmutadores procedan como se explicó anteriormente. A diferencia del primer proceso, IntServ hace la reserva de recursos desde el principio hasta el final de la ruta, esto quiere decir que siempre habrá una cantidad disponible de ancho de banda en la ruda desde la cámara hacia el sistema de grabación.

El método DiffServ, es el medio más común de todos modos para etiquetar el tráfico con base en aplicaciones, ya que permite asignar y clasificar el ancho de banda según el tipo de aplicación que se quiera reservar [10].

X. Soluciones propuestas

La implementación de videovigilancia IP en redes convergentes presenta desafíos en cuanto a diseño y seguridad, debido a la creciente demanda de ancho de banda, la complejidad de la gestión y el aumento de la superficie de ataque. Para mitigar estos impactos, se proponen las siguientes soluciones:

A. Diseño

Segmentación de red: Dividir la red en segmentos para aislar el tráfico de videovigilancia del resto de la red, reduciendo la congestión y mejorando la seguridad.

Implementación de VLANs: Utilizar VLANs para agrupar dispositivos de videovigilancia y asignarles recursos de red dedicados.

Priorización del tráfico: Priorizar el tráfico de videovigilancia para garantizar una calidad de servicio (QoS) adecuada, especialmente en redes congestionadas.

Selección de hardware adecuado: Seleccionar routers, switches y firewalls con capacidad suficiente para manejar el tráfico de videovigilancia y las demandas de seguridad.

Diseño de redundancia: Implementar redundancia en los componentes críticos de la red para garantizar la disponibilidad del sistema de videovigilancia en caso de fallos.

B. Seguridad

Cifrado de datos: Cifrar el tráfico de video y datos para protegerlo de la interceptación y el análisis no autorizado.

Autenticación y autorización: Implementar mecanismos robustos de autenticación y autorización para controlar el acceso a los dispositivos de videovigilancia y los datos.

Protección contra ataques cibernéticos: Implementar medidas de seguridad para proteger las redes convergentes de ataques cibernéticos, como firewalls, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS).

Actualizaciones de software y firmware: Mantener el software y firmware de los dispositivos de videovigilancia y los componentes de red actualizados para corregir vulnerabilidades conocidas.

Monitoreo y auditoría: Implementar un sistema de monitoreo y auditoría continuo para detectar actividades sospechosas y garantizar el cumplimiento de las normas de seguridad.

C. Herramientas y tecnologías adicionales

Sistemas de gestión de videovigilancia (VMS): Utilizar un VMS centralizado para gestionar y administrar los dispositivos de videovigilancia de manera eficiente y segura.

Soluciones de análisis de video: Implementar soluciones de análisis de video para detectar eventos y actividades sospechosas en tiempo real.

Tecnologías de seguridad biométrica: Utilizar tecnologías de seguridad biométrica para controlar el acceso físico a las instalaciones y proteger los dispositivos de videovigilancia.

Se podrían enumerar varias metodologías adicionales para el enfoque de videovigilancia IP en redes convergentes que ayudarían a las herramientas descriptas anteriormente.

Modelo de seguridad en capas:

Este modelo tradicional divide la red en capas concéntricas, cada una con sus propios controles de seguridad. La idea es que un atacante que penetre una capa deba superar múltiples obstáculos antes de llegar a los recursos críticos. El mismo es un enfoque familiar y bien entendido y ofrece una defensa en profundidad contra las amenazas. Por otro lado, puede ser complejo de implementar y administrar. No es tan flexible como Zero Trust para adaptarse a las amenazas en constante evolución.

Seguridad basada en la identidad:

Este enfoque se centra en la autenticación y autorización de usuarios y dispositivos, asegurando que solo las personas y dispositivos autorizados puedan acceder a los recursos de la red.

Simplifica la administración de accesos y mejora la visibilidad de la actividad en la red. Por otro lado, depende en gran medida de la precisión de la información de identidad y no es tan efectiva contra amenazas que no se basan en la identidad.

Seguridad basada en el contexto:

Este enfoque toma en cuenta el contexto de un acceso, como la ubicación del usuario, la hora del día y el dispositivo utilizado, para determinar si se debe permitir o no. Este puede reducir los falsos positivos y mejorar la precisión de las decisiones de acceso. Puede adaptarse a las amenazas en constante evolución. Es muy complejo de implementar y administrar y además requiere una gran cantidad de datos de contexto.

Seguridad basada en la microsegmentación:

Este enfoque divide la red en segmentos muy pequeños, controlando el tráfico entre ellos con gran granularidad. Esto limita el alcance de los ataques potenciales y facilita la aplicación de controles de seguridad específicos para cada segmento. Ofrece un alto nivel de seguridad, siendo el mismo flexible y adaptable. Puede ser complejo de implementar y administrar. Requiere una infraestructura de red adecuada.

Seguridad basada en la red definida por software (SDN)

SDN permite centralizar la gestión y el control de la red, lo que facilita la aplicación de políticas de seguridad consistentes y la respuesta a las amenazas. También simplifica la administración de la red y permite una rápida implementación de políticas de seguridad. Se requiere una infraestructura de red SDN y puede ser vulnerable a ataques a la infraestructura SDN.

La elección de la metodología adecuada dependerá de las necesidades y requisitos específicos de cada organización. Es importante considerar factores como el tamaño y la complejidad de la red, los recursos disponibles, las amenazas potenciales y los objetivos de seguridad. Además, es muy importante seguir las normas debajo mencionadas:

Normas ISO. Encontramos la ISO 27000, que detalla estrategias de implementación de medidas de seguridad física. También la ISO 27002. Esta norma establece un código de práctica para la seguridad de la información, incluyendo la seguridad física y del entorno. Aquí se entiende por seguridad física, las medidas y controles para proteger los sistemas de información, incluyendo servidores, equipos de red,

dispositivos de almacenamiento y hasta documentos impresos.

AIENSE 10/21. Esta norma corresponde a la Guía de buenas prácticas de ciberseguridad en proyectos de seguridad física. Fue diseñada por la Asociación Española de Ingenieros de Seguridad. Evalúa las amenazas, vulnerabilidades e impacto de los riesgos de ciberseguridad en sistemas de seguridad física. También especifica diferentes medidas de ciberseguridad generales y específicas.

NIST 800-82. Emanada del Instituto Nacional de Normas y Tecnología de los Estados Unidos, es una guía de buenas prácticas para la defensa de los sistemas de seguridad física, como protección de ubicaciones, controles de acceso, monitoreo, gestión de factores ambientales y protección de corriente eléctrica entre otros.

XI. CONCLUSIONES

La introducción de las redes convergentes ha tenido un impacto significativo en la videovigilancia IP, transformando la forma en que se diseñan, implementan y administran los sistemas de videovigilancia. Las redes convergentes han revolucionado la videovigilancia IP, permitiendo sistemas más eficientes, escalables y seguros a un costo menor. A medida que la tecnología continúa evolucionando, las redes convergentes seguirán desempeñando un papel crucial en el futuro de la videovigilancia IP.

A continuación, se detallan algunos de los principales impactos:

Optimización de Recursos

Las redes convergentes permiten integrar videovigilancia IP con otras redes existentes, como redes de datos y voz, utilizando una única infraestructura de red. Esto elimina la necesidad de redes separadas para cada tipo de tráfico, lo que reduce significativamente los costos de instalación, mantenimiento y operación.

Mayor escalabilidad

Las redes convergentes ofrecen una mayor escalabilidad, lo que facilita la expansión de los sistemas de videovigilancia IP para adaptarse a las necesidades cambiantes. Se pueden agregar nuevas cámaras y dispositivos de manera sencilla sin necesidad de realizar cambios importantes en la infraestructura de red.

Simplicidad de gestión

La gestión de redes convergentes simplifica la administración de los sistemas de videovigilancia IP. Los administradores pueden utilizar herramientas de gestión centralizadas para monitorear, configurar y solucionar problemas de todos los dispositivos en la red desde una única interfaz.

Mayor flexibilidad

Las redes convergentes proporcionan una mayor flexibilidad para la ubicación de las cámaras IP. Las cámaras se pueden instalar en cualquier lugar de la red, independientemente de su proximidad a los puntos de acceso de red tradicionales.

Integración con otros sistemas

Las redes convergentes facilitan la integración de sistemas de videovigilancia IP con otros sistemas de seguridad y gestión de edificios, como control de acceso y alarmas. Esto permite una visión más completa de la seguridad y el estado de las instalaciones.

Nuevos servicios y aplicaciones

Las redes convergentes abren la puerta a nuevos servicios y aplicaciones de videovigilancia IP, como análisis de video, reconocimiento facial y detección de intrusiones. Estos servicios pueden mejorar significativamente la efectividad de los sistemas de videovigilancia.

Mayor eficiencia en el ancho de banda

Las tecnologías de compresión de video, como H.264 y H.265, permiten optimizar el uso del ancho de banda en las redes convergentes. Esto reduce la cantidad de ancho de banda necesaria para transmitir video de alta calidad, lo que mejora el rendimiento general de la red.

Mayor seguridad

Las redes convergentes pueden incorporar medidas de seguridad avanzadas, como firewalls, VPN y cifrado de datos, para proteger los sistemas de videovigilancia IP contra ataques cibernéticos y accesos no autorizados.

Capacitación

Se recomienda la capacitación a los empleados par mejorar la ciberseguridad, ya que el 85% de los problemas de ciberseguridad son errores humanos y al mismo tiempo es necesario por un tema de protección de datos de las personas, por lo que es necesario en este punto la concientización.

XII. FUTURAS LÍNEAS DE INVESTIGACIÓN

Con el avance de la tecnología, podemos enumerar unas cuantas herramientas que se vienen y alguna de ellas ya están en vigencia respecto a la videovigilancia IP. Podemos nombrar alguna de ellas:

- **Cámaras Smart con inteligencia artificial.**
- **Rastreador y seguimientos de objecto (IA visión Computing).**
- **Modelo detección IA (Armas en video digital).**
- **Videovigilancia solar.**
- **Redes definidas por software (SND).**

Ver Anexo I

XIII. ANEXOS

Explicación detallada y grafica sobre los diversos tipos de ataques en redes convergentes que vulneran la seguridad de esta.

XIV. Agradecimientos

Agradezco profundamente a mi familia, que me apoyaron en estos 2 años que me llevo cursar la carrera para obtener la Licenciatura y por sobre todo a mi esposa e hijos que fueron las 2 personas con las que no pude compartir muchos momentos dado la cantidad de parciales y finales.

Una mención importante también a quien me ayudo en esta tesis, desde el principio, guiándome y ayudándome todo el tiempo, al profesor Lic. Pablo Alejandro Lena.

XV. Referencias

Publicaciones periódicas:

[1] https://www.americacomunicaciones.com/videovigilancia-historia/
[2] https://www.een.com/es/blog/cyber-ataque-washington-d-c-camaras/
[3] https://www.datacenterdynamics.com/es/features/el-impacto-de-las-redes-convergentes-en-las-%C3%BAltimas-tendencias-tecnol%C3%B3gicas/
[4] https://www.exw.com.tw/es/faq/faq-009.html
[5] https://www.tecnoseguro.com/analisis/pro/redes-convergentes-vs-redes-dedicadas-videovigilancia-ip
[6] https://www.tecnoseguro.com/analisis/pro/uso-vlan-en-redes-para-videovigilancia
[7] https://www.tecnoseguro.com/analisis/pro/aspectos-clave-sobre-ancho-de-banda-para-videovigilancia-en-red
[8] https://www.linkedin.com/pulse/hacking-de-vlan-redes-convergentes-seguridad-luis-alberto-nieto/?originalSubdomain=es
[9] https://www.tecnoseguro.com/analisis/pro/multicast-videovigilancia-en-red-que-es-aspectos-tener-cuenta-en-implementacion
[10] https://www.tecnoseguro.com/analisis/pro/qos-en-videovigilancia-en-red-que-es-y-cuando-aplicarlo
[11] https://uss.com.ar/tecnologia-y-equipamiento/sistemas-de-seguridad/

XVI. Biografía



Guillermo Raúl Rodríguez nacido en Buenos Aires, Argentina, el 12 de noviembre de 1979. Es técnico Superior en Análisis de sistemas en la Universidad John F. Kennedy en el año 2015. Próximo a graduarse en la Universidad de Palermo como Licenciatura en Tecnologías de la Información. Su experiencia laboral abarco principalmente el área de Telecomunicaciones durante los últimos 25 años y actualmente se desempeña como Network SRE para el análisis, implementación y soluciones de la infraestructura de trading en JP Morgan.