



MARCO TEORICO

Unidad.2. Sesion.5. Actividad.2



12 DE MAYO DE 2019
ALEXIS HIRAM ARELLANO MENDEZ
Licenciatura en Ingeniería en Telemática

1. CONCEPTOS BASICOS DE CCTV

1.1. Historia e introducción a CCTV

Circuito cerrado de televisión o CCTV es una tecnología de video vigilancia visual diseñada para supervisar una diversidad de ambientes y actividades.

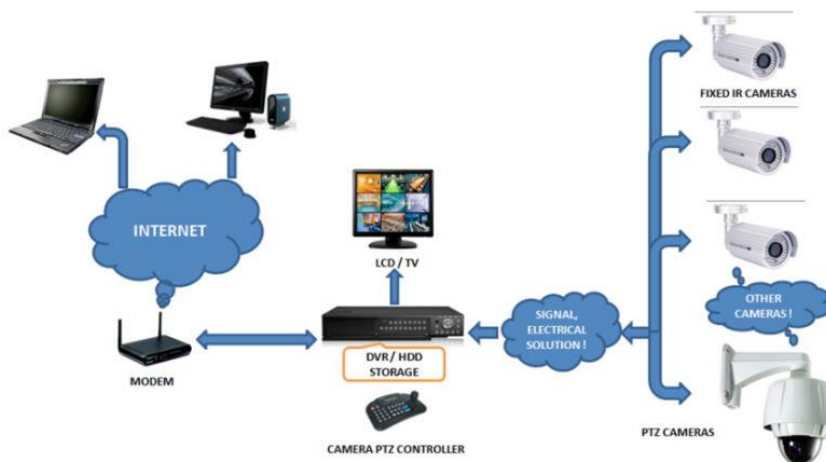
Se le denomina circuito cerrado ya que, al contrario de lo que pasa con la difusión, todos sus componentes están enlazados.

Las ventajas de circuito cerrado de televisión CCTV incluyen la capacidad de observar las situaciones de peligro a distancia, la capacidad de proporcionar un ojo constante de las actividades rutinarias, y una gran herramienta para el hogar y las empresas de seguridad, en un esfuerzo para combatir la delincuencia, o bien en el hogar u oficina para checar el desempeño de los trabajadores.

Al principio se hacían este tipo de instalaciones para disuadir o detectar robos y, hoy en día, no solo se utiliza para seguridad, sino también para otros propósitos específicos como pueden ser los de la medicina, la educación o la lucha contra eventos antisociales.

1.2. Composición

En general el circuito está compuesto, aparte de las cámaras y monitores, de un dispositivo de almacenamiento de video (DVR Digital Video Recorder, NVR Network Video Recorder) dependiendo la estructura del circuito ya sea analógico o basado en redes IP, aunque se pueden realizar combinaciones dependiendo las necesidades del sitio. Se muestra un esquema de posible



1.3. Sistemas analógicos y sistemas digitales (IP)

Inicialmente, todo el conjunto de elementos que componen un cctv era analógico. Monitores, grabadores, cámaras, medios de transmisión, etc.

Poco a poco, se han ido introduciendo componentes digitales aunque con precaución ya que los sistemas analógicos en el sector de la seguridad disponen de una tecnología muy madura y tienen un largo historial de servicio. Es evidente que las necesidades tecnológicas se investigan en el ámbito digital y no en el analógico por su escalabilidad y sus respectivas integraciones con el mundo de las telecomunicaciones. Por ello, cualquier sistema de video vigilancia con perspectiva del futuro debería disponer del mayor número de componentes digitales.

El alcance actual de la tecnología digital ha cubierto muchas de las limitaciones de la tecnología analógica. Los sistemas de CCTV analógicos generalmente precisan un mantenimiento intensivo, no ofrecen accesibilidad remota y son notablemente difíciles de integrar con otros sistemas.

1.4. Transmisión de señal

La transmisión de la señal de video es un elemento de gran importancia en los sistemas de video vigilancia. Esto es así por lo que puede llegar a variar entre un entorno u otro a la hora de planificar una instalación. Se deben tener en cuenta muchos factores, como:

- Interior/Exterior.
- Capacidad de aprovechar medios existentes.
- Longitud entre los puntos a transmitir.
- Puntos desde donde obtener la alimentación eléctrica.
- Interferencias con otros sistemas.

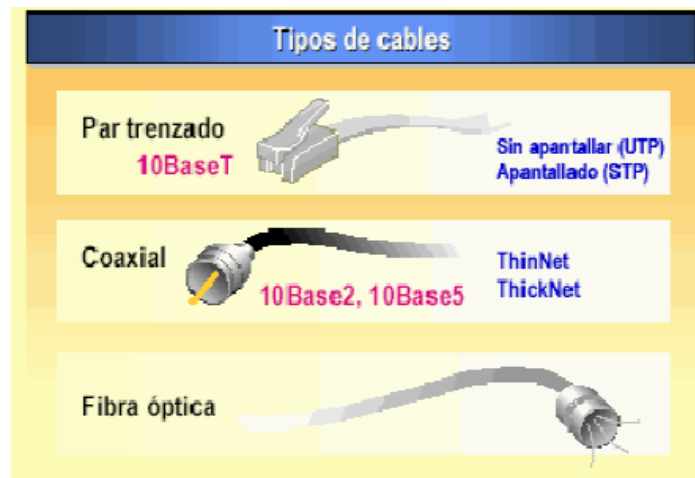
Por ello se suelen mantener dos vertientes diferenciadas en la forma de transmitir dichas señales: mediante cableado o de forma inalámbrica.

1.4.1. Cableado

Actualmente en CCTV se utiliza cableado coaxial, fibra óptica o par trenzado. El cableado es una parte muy importante a tener en cuenta ya que más del 70% de los problemas en la instalación de un sistema de CCTV están referidos al cableado.

El coaxiales medio de transmisión por antonomasia de los sistemas de cctv analógicos. Aunque está siendo mejorado por otros tipos de cableado como el par trenzado o la fibra óptica.

Por otro lado, la fibra óptica es un medio excelente para la transmisión de información por sus características: gran ancho de banda, baja atenuación de la señal que permite cubrir grandes distancias sin repetidores, integridad - proporción de errores baja, inmunidad a interferencias electromagnéticas, alta seguridad y larga duración, resistente a la corrosión y altas temperaturas.



1.4.2. Transmisión Inalámbrica

El objetivo fundamental de las redes inalámbricas es el de proporcionar las facilidades no disponibles en los sistemas cableados y formar una red global donde se complementen ambas, enlazando los diferentes equipos y ofreciendo una flexibilidad total de la comunicación.

Actualmente cuando se habla de transmisión de video vigilancia vía radio, se da por hecho que la señal a transmitir es "IP". Los sistemas de transmisión analógicos por RF en CCTV "profesional" están prácticamente obsoletos por su inestabilidad, vulnerabilidad y poca eficiencia.

Las soluciones de transmisión de banda ancha por IP permiten instalar cámaras con un ahorro importante de costos asociados a la instalación de cableado Ethernet o de fibra óptica. En muchos casos, las tecnologías inalámbricas hacen posibles instalaciones que de otra forma serían inviables desde el punto de vista técnico y económico.

Dentro de los estándares inalámbricos más adecuados para facilitar este tipo de conectividad destacan los siguientes:

- WiFi (WirelessFidelity)
- WiMAX (Worldwide Interoperability for Microwave Access)

En los últimos años, ha habido empresas que han promovido mucho el uso de WIFI como sistema de transmisión para video vigilancia.

Aunque el uso de WiFi está muy extendido y muy maduro, es evidente que tiene limitaciones conocidas como las interferencias, la distancia, la seguridad, la velocidad y limitaciones que en algunas instalaciones no se pueden permitir.

WiMAX, por otro lado, ha sido diseñado para complementar a la tecnología WiFi en estas y otras limitaciones.

2. Control de Acceso

2.1. Definición de un sistema de control de acceso.

¿Qué es Control de Acceso?

Un sistema electrónico autónomo que tiene la facultad de permitir o impedir el acceso de una o más personas a una área física designada, tomando en cuenta una base de datos y condiciones establecidas, llevando un registro electrónico de cada incidente ocurrido.

En términos generales la base de datos está compuesto por:

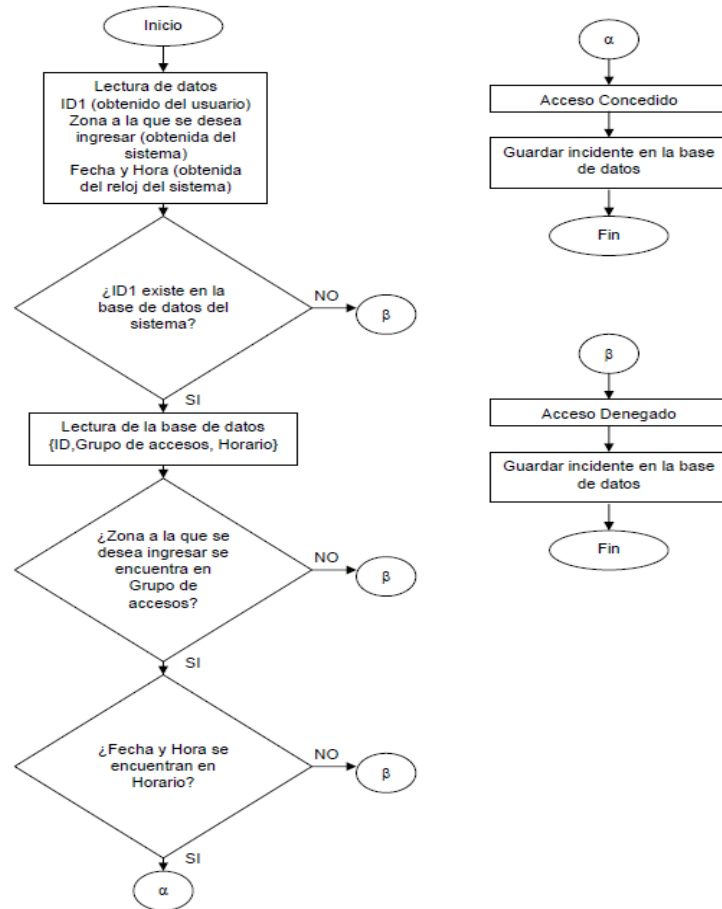
- Números de identificación personal (ID´s)
- Grupos de accesos
- Horarios

De esta manera definiremos también a un usuario del sistema como: “Una persona que cuenta con un número de identificación personal válido para el sistema.

El número de identificación personal para cada usuario es único, el grupo de accesos identifica las áreas autorizadas en las que puede ingresar un usuario y el horario hace referencia al intervalo de tiempo en el cual un usuario puede ingresar a un área que pertenezca a su grupo de accesos.

Otros datos como el nombre completo de cada usuario, el puesto que desempeña en la empresa, o su edad, son meramente informativos y no tienen relación con los requisitos o condiciones que se deben cumplir para conceder o no el acceso a un área determinada.

Las condiciones más comunes en un sistema de control de acceso típico, así como una descripción general del proceso que realiza el sistema con los datos y las condiciones establecidas para conceder o negar el acceso se pueden observar en el siguiente diagrama de flujo.



En el diagrama de flujo se observa como el sistema necesita de tres datos para empezar su proceso, un número que designamos como ID1 ingresado al sistema por el usuario, una Zona que es un identificador del área en donde se está solicitando un acceso; este identificador lo conoce el sistema y está asociado al campo de Grupo de accesos de la base de datos, el cual puede contener a su vez uno o más identificadores de Zona. Por último el sistema también lee la fecha y la hora en que se ha hecho la solicitud de acceso; este dato lo obtiene de un reloj interno con el que cuenta el sistema.

Algo más que podemos resaltar, es el hecho de que no importando si se concede o no el acceso, se guarda el registro del incidente ocurrido en la base de datos, lo que permite conocer porque el sistema negó o concedió un acceso, logrando con esto tener un control de los usuarios que ingresaron a un área determinada y de los posibles intentos de violación a áreas no autorizadas en horarios no autorizados realizados por usuarios del sistema.

En un Sistema de Control de Acceso, todos los componentes del sistema están conectados entre sí, y se centraliza todo el manejo y supervisión del sistema en una computadora, que tendrá instalado un Software de Gestión, Administración, Control y Supervisión.

Independientemente del Sistema de Control de Acceso que se trate, para el caso de los sistemas completos, se agregan otros elementos adicionales.

2.2. Componentes de un sistema de control de acceso.

Un sistema de control de acceso físico básico está compuesto por:

- Lectores
- Tarjetas
- Un panel de control
- Cerraduras
- Fuentes de alimentación
- Software de control, monitoreo y reporte

Un lector es un dispositivo electrónico que se encarga de ingresar y transmitir la información al sistema de control de acceso, mediante la lectura de un medio electrónico, biométrico o una combinación de los dos. Los lectores más comunes son los lectores de código de barras, de banda magnética, de proximidad, tarjeta inteligente y biométricos.

Un acceso que se desee controlar requiere forzosamente de un lector y de una cerradura, se puede agregar un lector más si se desea controlar la entrada y la salida a un acceso. En el caso de que se utilice un solo lector por acceso, es necesario contar con un dispositivo (que puede ser un botón o palanca de emergencia por ejemplo) para liberar la salida.

Al panel de control o unidad de control, entran y salen las distintas conexiones del sistema, como son los lectores y las cerraduras, y también los sensores y las bocinas, si se usa con señales de alarmas.

Tendremos también, todas las borneras para hacer las conexiones de los lectores, las cerraduras o el elemento que se utilice y las entradas de sensores y salidas de alarmas.

En este dispositivo se encuentra el microprocesador que realiza el proceso al que se hace referencia en el diagrama de flujo, en el cual se lleva a cabo la lógica de funcionamiento del sistema. Además, está compuesto por los dispositivos electrónicos necesarios para poder mandar señales eléctricas a los lectores, las cerraduras para que estas se abran o se cierren y para poder recibir señales provenientes de diferentes tipos de sensores (de puerta abierta, de vidriocroto, de humo, etc.) la memoria donde se guardan las tarjetas habilitadas, el reloj de tiempo real y la memoria para los eventos que se registran.

Todas las Unidades de Control necesitan recibir la energía de alimentación para su funcionamiento, es por ello que se vuelven importantes contar con las suficientes fuentes de alimentación. Seguramente, no todos los fabricantes de equipos, poseen el mismo criterio, así que es posible que nos encontremos con

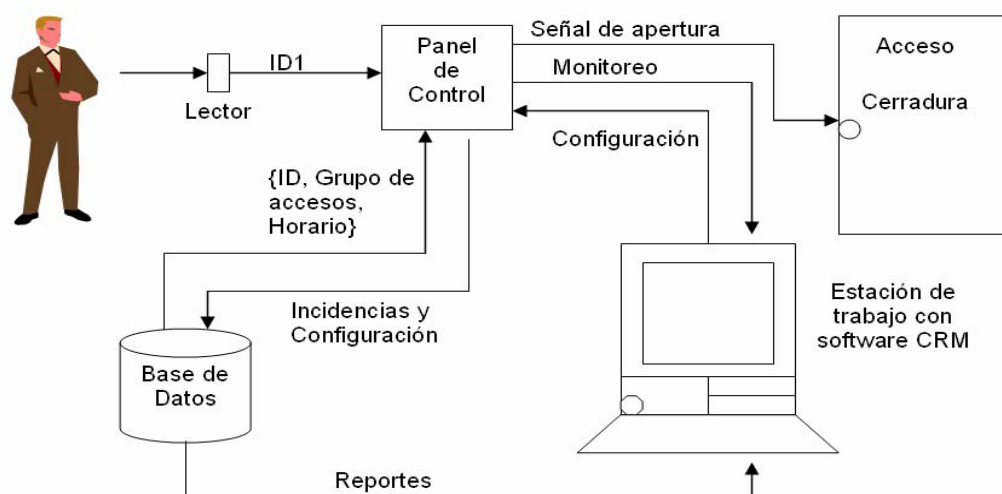
equipos que se alimentan directamente con la red de 110 VAC y otros que lo harán con 12 o 24 VDC. También debemos contemplar, de la misma forma, las fuentes de alimentación para la cerradura o dispositivo y sirenas, si se utilizan.

Por último una cerradura es un dispositivo electrónico que mantiene un acceso cerrado, hasta que recibe una señal del panel de control, momento en el cual la cerradura se libera permitiendo el acceso. Las cerraduras más comunes son las chapas eléctricas, los electroimanes y otras chapas electromagnéticas, las barreras vehiculares y los torniquetes de media altura o de altura completa.

2.3. Funcionamiento de un sistema de control de acceso típico.

El proceso comienza con la llegada del usuario al acceso por el cual desea entrar o salir, el usuario presenta ante el lector el medio en el cual está almacenado su número de identificación personal (este medio puede ser una tarjeta, una característica biométrica o ambas, como mencionamos con anterioridad). El lector entonces envía una cadena de bits codificada con información del medio utilizado, en donde se encuentra el número de identificación ID1 del usuario, al panel de control; el microprocesador dentro del panel de control toma esta cadena de bits, la decodifica y realiza el proceso para conceder o negar el acceso. Una vez que el sistema decide conceder el acceso, el panel manda una señal para cambiar el estado de un relevador (asociado a ese acceso) al cual está conectado una cerradura; de esta manera la cerradura se libera y el usuario puede pasar a través del acceso.

El sistema cuenta además con un software de configuración, monitoreo y reporte (CMR) instalado en una computadora preferentemente dedicada; con este software se configuran los parámetros relacionados al sistema de control de acceso como son: Los usuarios, los lectores, los horarios, los grupos de accesos las asociaciones de los relevadores con los accesos a controlar. También mediante este software se monitorea en tiempo real cada una de las incidencias que ocurren en el sistema y que son almacenadas en la base de datos; por último con este software se pueden generar reportes filtrados por incidencias, por usuarios o por fechas tal como se muestra en la siguiente imagen.



2.4. Tecnologías aplicadas al control de acceso.

Un sistema de control de acceso puede estar integrado de tarjetas de identificación, lectoras, cerraduras automáticas y computadoras para procesar diversos reportes y su eficacia dependerá de las características técnicas de los equipos utilizados y del software. Un buen diseño del sistema de control de acceso es fundamental para determinar las jerarquías de acceso para empleados y visitantes y, en base a las necesidades del usuario, determinar el tipo de tarjetas de identificación (de banda magnética, de código de barras, de chip, con fotografía, etc.), el tipo de lectoras (de aproximación, de ranura, de lectura de huella digital, de iris, etc.) y el tipo de reportes de control que el usuario requerirá.

Ya mencionamos que lo primero que debemos determinar es justamente qué tipo de tecnología vamos a instalar y para esto es necesario nombrar las tecnologías más comunes existentes en el mercado.

2.4.1. Banda Magnética

Es la tecnología más conocida y difundida. Su ventaja es su difusión, popularidad y el bajo costo, pero en sí es, de todos los medios de identificación, el más vulnerable de todos. Sólo se recomiendan en oficinas o establecimientos administrativos.

El lector en sí, es de los más económicos, pero posee un cabezal magnético, el cual sufre cierto desgaste cada vez que se pasan las tarjetas. El tiempo de duración, depende exclusivamente del ambiente, frecuencia de uso y el trato que se le dé al utilizarlos.



2.4.2. Código de Barras

La ventaja de esta tecnología, es que sus tarjetas al ser pasarlas por el lector, no existe rozamiento con un cabezal, con lo cual su vida útil es levemente mayor, pero si se raya el código impreso puede quedar ilegible, obligando al cambio de tarjeta. El costo de las tarjetas es similar a las magnéticas, y a pesar de que se las puede proteger contra fotocopias, son bastante vulnerables en lo que a seguridad se refiere.



2.4.3. Proximidad

Con este tipo de tecnología es imposible que pueda duplicarse una credencial o tarjeta. La tarjeta no tiene rozamiento de ningún tipo (se comunica con el equipo por radio frecuencia), por lo cual no se desgasta. Hoy en día es una de las tecnologías más moderna y efectiva, por su practicidad y bajo costo de mantenimiento. Son ideales en situaciones de máxima seguridad y alta tecnología. Es el sistema más ágil, porque no necesita que la tarjeta sea pasada en un sentido específico, lo que le da una mayor velocidad de lectura y poca resistencia al uso por parte de los usuarios, porque incluso puede ser leída la tarjeta dentro de una billetera, una cartera, etc.

El precio de esta tecnología se ha equiparado actualmente con los lectores comunes de código de barras. Logra sin dudas, la mejor relación precio/rendimiento.



2.4.4. Touch Memories

Es una pastilla electrónica, encapsulada en acero inoxidable de unos 16mm de diámetro, que se transportan con un soporte plástico tipo llavero. Brindan un muy alto nivel de seguridad, ya que son altamente resistentes al desgaste, siendo ideales para ambientes industriales, aunque no son recomendables para ambientes con alto grado de generación de corriente estática (P. Ej.: oficinas con mucha alfombra y ambientes muy secos). Su tecnología de avanzada evita la posibilidad de duplicarlas. Realmente muy confiables.



2.4.5. Biométricos

El funcionamiento de esta tecnología se basa en la lectura de alguna parte del cuerpo humano, eliminando por completo el uso de las tarjetas. Su principal ventaja radica en la seguridad, pero hasta el momento no son de uso masivo. Seguramente con el tiempo se irán superando algunas dificultades, entre ellas el costo, y en un futuro de mediano plazo, llegarán a ser un estándar más. Con la identificación biométrica se puede tener un control realmente eficiente y preciso de los usuarios de un sistema de control de acceso, logrando saber con certeza, en base a uno o varios parámetros biométricos, que la persona que utilice esta forma de reconocimiento sea en verdad el usuario al que corresponda el mismo parámetro o parámetros biométricos. Esto no sucede con él, código de barras o la banda magnética. Solamente la identificación biométrica puede proveer un registro real de las actividades de las personas, eliminando la posibilidad de que estas accedan a lugares a los que no tienen autorización. En este trabajo revisaremos los aspectos básicos de cada uno de los tipos de sistemas biométricos, dedicándole un mayor espacio a los sistemas y lectores de huella digital.

