

UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO
FACULTAD DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA, INFORMÁTICA Y
MECÁNICA
ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA
Y DE SISTEMAS



**“Implementación de un sistema de videovigilancia con
reconocimiento facial”**

ASIGNATURA: FORMULACIÓN DE PROYECTOS DE TIC

DOCENTE: COSIO LOAIZA, Stephan Jhoel

ESTUDIANTES:

- | | |
|----------------------------------|--------|
| • CHOQUEPATA HUAMÁN, Vanessa | 182899 |
| • CHUNGA CASTILLO, Gary Btrigham | 182900 |
| • CUYO TTITO, Denis Omar | 182906 |
| • SALINAS ATAUSINCHI, Jerson | 171605 |
| • SANGA MONRROY, Roger | 150406 |
| • SAPACAYO HUAYHUA, Teofilo S. | 182934 |
| • VILLALOBOS QUISPE, Pamela A. | 182939 |

1. Finalidad Pública

Identificar hechos delictivos, monitorear/diferenciar a las personas al ingreso y salida de los ambientes y vigilar los bienes materiales, que se espera atender a través de la implementación del sistema de video vigilancia con reconocimiento facial y así contribuir en el bienestar y seguridad en las instalaciones a la comunidad informática.

2. Antecedentes:

- El hospital de México desde hace una década gracias a ofrecer un servicio asistencial de primer nivel en unas instalaciones de vanguardia. Para poder ofrecer un trato diferencial a sus clientes, el Hospital invierte sistemas de reconocimiento facial y lectura de matrículas de SCATI que les permite identificar a sus pacientes a su llegada a las instalaciones.
- En 2018, en la universidad Politécnica del Ecuador, desarrollaron un sistema de acceso usando tecnología RFIID y reconocimiento facial cuenta con un directorio donde se encuentran alrededor de 310 fotografías almacenadas y así poder realizar la comparación para luego arrojar el resultado de la verificación. Por otro lado, el hardware que se utiliza para este sistema es una Raspberry Pi 3 B+ y un lector de tarjetas de RFIID, que es el encargado de enviar la información de la tarjeta a la Raspberry y así lograr el acceso a la persona.
- En la Universidad Católica de Bogotá se planteó el desarrollo de un sistema de reconocimiento facial que permite controlar el acceso a viviendas. Es importante buscar opciones para afrontar esta problemática ya que esto influye en el estado físico o mental de las personas, por esto, este sistema de reconocimiento facial planea disminuir el porcentaje de hurto y que los propietarios, para el acceso a sus viviendas no dependan de objetos que se puedan extraviar.
- En el Ecuador es parte de los sectores estratégicos con decisiva influencia social política y económica el haber formado el ecu 911, una de las instituciones insignias del país que funciona como una herramienta tecnológica integradora de servicios de emergencia desplegados en todo el país para contribuir a la estabilidad y seguridad del territorio ecuatoriano. Con este caso de estudio, se analizarán tecnologías de video vigilancia como estrategias especializadas para el monitoreo y alarmas ciudadanas, con técnicas fundamentadas en el reconocimiento facial que se basa en la biometría y características de conducta o fisiológicas del cuerpo humano.
- El departamento de Tecnología de la información del Instituto de Tecnología de Vidyalankar , Mumbai en India desarrolló un sistema de vigilancia para la detección de intrusos mediante reconocimiento facial a través del uso de una placa Nvidia Jetson Nano para calcular el algoritmo de red neuronal convolucional que permite almacenar

una base de datos de los rostros existentes y cuando la cámara detecte un rostro nuevo enviará una alerta al personal de seguridad. Esto ayudará a disminuir la inseguridad en lugares muy concurridos como universidades, colegios, escuelas, etc [1]

3. Marco teórico

a. Reconocimiento facial

b. Cámaras DOMO IP

Cámara domo IP de infrarrojos Día/noche

La cámara domo de infrarrojos IP NDN-265-PIO HD de 720p de Bosch es una resistente cámara en red lista para usar. Con esta cámara es posible introducir la tecnología de alto rendimiento de Bosch en oficinas y pequeños comercios, ya que se trata de una solución asequible para un gran número de aplicaciones. Esta robusta cámara domo tiene una calificación IP66, ofrece resistencia al agua y al polvo y se adapta a entornos exigentes. Los LED infrarrojos incorporados permiten una vigilancia nocturna de calidad a una distancia de visualización de 15 m (50 pies) en la oscuridad. La tecnología de compresión H.264 proporciona imágenes nítidas, al mismo tiempo que reduce el ancho de banda y el almacenamiento hasta un 30%. (Bosch Security System, 2013)

c. IP

La dirección IP es un identificador único dentro de una red que usa el protocolo IP (internet protocol). IP es un protocolo no confiable ya que no se garantiza que un paquete llegue a su destino. El mecanismo de manejo de errores de IP es descartar el paquete y devolver un mensaje al emisor indicando el error.

La dirección IP puede ser dinámica o estática (JACKELINE, 2009).

Características de la direcciones IP (CAPITULO II MARCO TEÓRICO, n.d.):

- Tiene un longitud de 32 bits
- Identifica a las redes y los nodos conectados a ellas
- Especifica la conexión entre redes
- Se representan mediante cuatro octetos, escritos en formato decimal, separados por puntos

Características del protocolo IP

- Protocolo orientado a no conexión
- Si es necesario se fragmentan los paquetes
- Realiza el direccionamiento mediante direcciones lógicas de 32 bits
- Si no se recibe un paquete, éste permanece en la red por un tiempo determinado
- El tamaño máximo de paquete que puede ser enviado es 65535 bytes
- Realiza la verificación del paquete por el encabezado mediante suma.

IP Dinámica: Esta dirección es asignada mediante DHCP y tiene un tiempo de duración determinada y cambia en el tiempo.

IP Estática o Fija: Este tipo de dirección la asigna el usuario manualmente. Es usado generalmente para sitios de internet y servidores

Clases de direcciones IP

1. Clase A
 - a. Número de redes: 127
 - b. Número de nodos: 16777215
 - c. Rango de direcciones: 1.0.0.0 - 127.0.0.0
2. Clase B
 - a. Número de redes: 4095
 - b. Número de nodos: 65535
 - c. Rango de direcciones: 128.0.0.0 - 191.255.0.0
3. Clase C
 - a. Número de redes: 2097151
 - b. Número de nodos: 255
 - c. Rango de direcciones: 192.0.0.0 - 23.255.255.0

d. Sistema de video vigilancia

Un sistema de videovigilancia, es el conjunto de cámaras, monitores y software para la mejora de supervisión de la vigilancia y seguridad de un espacio público o privado, por medio del enlace de las cámaras con los monitores, estos enlaces pueden variar desde conexiones de wifi, por cable analógico y mediante cable de red. De la misma forma podemos ver distintos tipos de sistema de videovigilancia, entre los principales podrían ser el circuito cerrado de televisión y videovigilancia inteligente, la instalación de estos sistemas también varía de acuerdo al sistema elegido.

e. Centro de control de acceso de videovigilancia

El control de acceso de videovigilancia incluye un panel de control, un lector y una credencial. El panel de control, que está montado en una ubicación interior segura, procesa cualquier entrada al lector desde una credencial autorizada, que podría ser una tarjeta de acceso, un identificador biométrico como un escaneo de huellas dactilares o una contraseña. El sistema de control de acceso también puede incorporar una cerradura de puerta magnética que se abre cuando se presenta una credencial autorizada.

Además, el control de acceso también se puede configurar en áreas más temporales como por ejemplo en un lugar donde se estén realizando obras de construcción (para evitar el acceso no autorizado a áreas peligrosas) o en un evento concreto(feria, concierto, etcétera, para mantener el equipo protegido o permitir áreas seguras de un stand)

f. Redes

Una red de computadoras es un conjunto de computadoras interconectadas las cuales comparten información. (Blanco, 1993). Las redes consisten de conexiones de hardware e interfaces de software, las cuales permiten transferir información a través de un medio de transmisión.

Según Tanenbaum (2007), una red de computadoras es "un conjunto de dispositivos conectados mediante medios de comunicación para compartir recursos y permitir la comunicación entre dispositivos". Este autor destaca que las redes de computadoras proporcionan una variedad de servicios, como compartir recursos, comunicarse entre dispositivos, y acceder a la información.

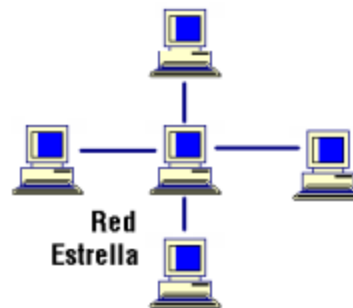
Clasificación de redes

A. Por su topología:

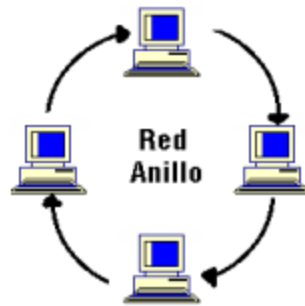
- Red en bus: Su funcionamiento es similar a la de red anillo, permite conectar las computadoras en red en una sola línea con el fin de poder identificar hacia cual se debe enviar.



- Red en estrella: Aquí una computadora hace la función de Servidor y se ubica en el centro de la configuración y todas las otras computadoras o estaciones de trabajo se conectan a él.



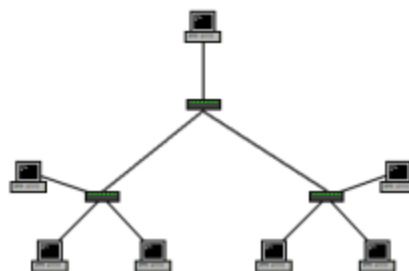
- Red en anillo (o doble anillo) En ésta, las computadoras se conectan en un circuito cerrado formando un anillo por donde circula la información en una sola dirección, con esta característica permite tener un control de recepción de mensajes pero si el anillo se corta los mensajes se pierden.



- Red en malla (o totalmente conexa) cada dispositivo tiene un enlace punto a punto y dedicado con cualquier otro dispositivo. El término dedicado significa que el enlace conduce el tráfico únicamente entre los dos dispositivos que conecta.



- Red en árbol: es una variante de la de estrella. Como en la estrella, los nodos del árbol están conectados a un concentrador central que controla el tráfico de la red. Sin embargo, no todos los dispositivos se conectan directamente al concentrador central. La mayoría de los dispositivos se conectan a un concentrador secundario que a su vez se conecta al concentrador central.”



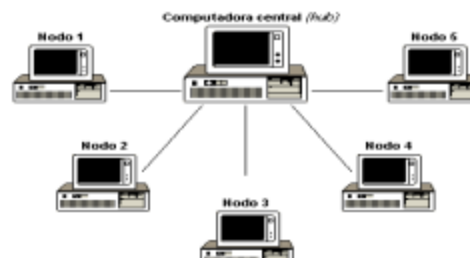
Una topología de red describe la disposición de los cables y los dispositivos, así como las rutas utilizadas para las transmisiones de datos. La topología influye enormemente en el funcionamiento de la red.

B. Por la distribución geográfica:

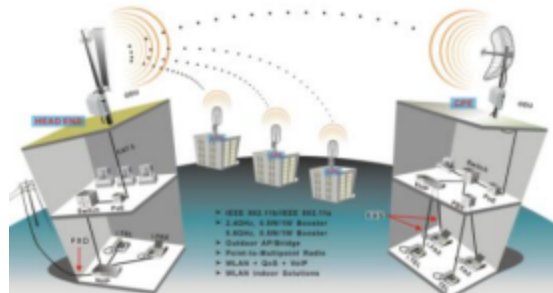
- Red de área local (LAN) Permiten la interconexión desde unas pocas hasta miles de computadoras en la misma área de trabajo como por ejemplo un edificio. Son las redes más pequeñas que abarcan de unos pocos metros a unos pocos kilómetros.



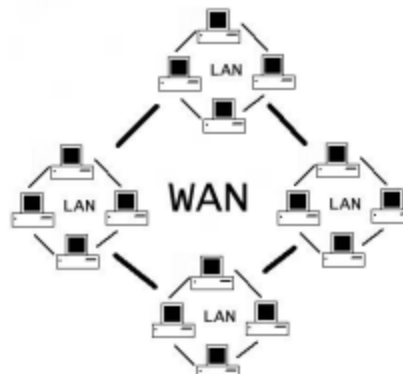
- Red de área de campus (CAN) es una colección de LAN dispersadas geográficamente dentro de un campus (universitario, oficinas de gobierno o industrias) pertenecientes a una misma entidad en una área delimitada en kilómetros.



- Red de área metropolitana (MAN) Tiene cubrimiento en ciudades enteras o partes de las mismas. Su uso se encuentra concentrado en entidades de servicios públicos como bancos



- Red de área amplia (WAN) Esta cubre áreas de trabajo dispersas en un país o varios países o continentes. Para lograr esto se necesitan distintos tipos de medios: satélites, cables interoceánicos, radio, etc.



- Red de área de almacenamiento (SAN) es una red concebida para conectar servidores, matrices de discos y librerías de soporte. Su función es la de conectar de manera rápida, segura y fiable los distintos elementos que la conforman.
- Red de área local virtual (VLAN) es un grupo de computadoras, con un conjunto común de recursos a compartir y de requerimientos. Que se comunican como si estuvieran adjuntos a una división lógica de redes de computadoras en la cual todos los nodos pueden alcanzar a los otros por medio de broadcast (dominio de broadcast).
- Red de área Personal (PAN) es una red de ordenadores usada para la comunicación entre los dispositivos de la computadora (teléfonos incluyendo las ayudantes digitales personales) cerca de una persona.

Los dispositivos pueden o no pueden pertenecer a la persona en cuestión. red de alto nivel y el Internet (un up link).”

C. Por la conexión:

- Medios guiados: cable coaxial, cable de par trenzado, fibra óptica y otros tipos de cables.
- Medios no guiados: radio, infrarrojos, microondas, láser y otras redes inalámbricas.

Las redes de ordenadores se pueden clasificar según la tecnología que se utiliza para conectar los dispositivos o su línea comunicación

g. Seguridad

Es la completa eliminación del riesgo, peligro o daño, haciendo que una persona se encuentre libre y protegida, es decir sin temor a nada. La seguridad tiene doble enfoque, una es la objetiva donde existen evidencias de absoluta seguridad y la subjetiva que la persona se siente en un lugar seguro y confiado.

4. Objetivos:

- Objetivo General: Diseñar e implementar un sistema de videovigilancia con reconocimiento facial en el pabellón de la escuela profesional de Ingeniería informática y de sistemas.
- Objetivos específicos:
 - Monitorear el acceso de las personas que ingresan al pabellón de la escuela profesional.
 - Establecer que tipos de dispositivos se deben emplear para el monitoreo según el tipo de cámaras implementadas.
 - Mejorar la seguridad tradicional de los salones de clase.
 - Identificar las áreas vulnerables de la escuela profesional

- Identificar a las personas que realicen algún acto que dañe la infraestructura de la escuela profesional

5. Justificación:

En los últimos se reportó daños a la infraestructura de los laboratorios ya que muchos alumnos de la facultad y de otras facultades que venían a hacer uso de estos equipos no sabían cómo mantenerlos en buen estado, lo cual generó un problema ya que no se podía identificar a las personas responsables, ya que si bien existen cámaras estas no tienen reconocimiento facial, aparte no hay personas que lo monitoreen este sistema.

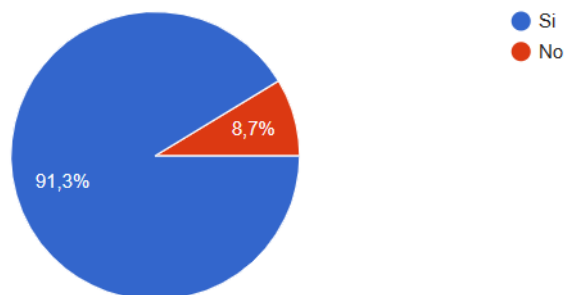
Ahora existen nuevas tecnologías que facilitan la realización de tareas de la vida diaria, entre ellos mantener la seguridad y estos son de gran ayuda para mejorar la calidad de esta, por lo cual en este proyecto se usará la tecnología de reconocimiento facial dentro de un sistema de videovigilancia para poder identificar a los presuntos actores de estas acciones. Este proyecto permitirá supervisar y reducir los hechos delictivos o actividades irregulares dentro del pabellón de informática y además de llevar un registro interno de las personas que ingresan o salen.

Esto nos otorgará mayor seguridad y confianza para una mejor protección de la infraestructura de la facultad de ingeniería informática y el libre tránsito de las personas.

6. Estudio de mercado

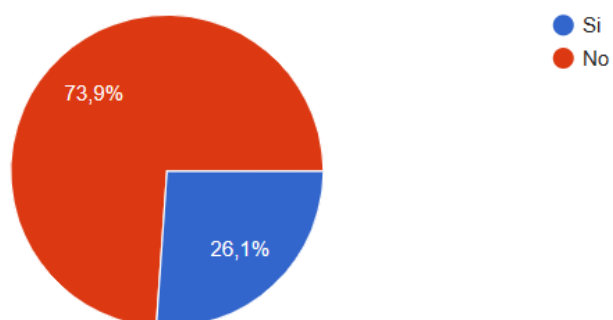
De acuerdo al tiempo que Ud se encuentra en la EPIIS ¿Considera que es importante la implementación de un sistema de videovigilancia?

23 respuestas



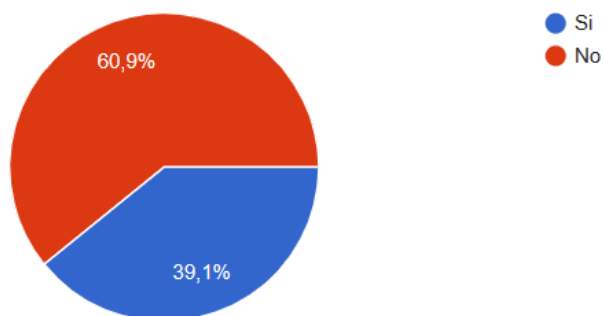
De acuerdo al tiempo que Ud se encuentra en la EPIIS ¿Considera que todos sus ambientes son seguros?

23 respuestas



De acuerdo al tiempo que Ud se encuentra en la EPIIS ¿Conoce de algún suceso delictivo? ejemplo: Robo

23 respuestas



De ser su respuesta (Si) en la anterior pregunta, ¿Qué tipo de suceso fue?

12 respuestas

Desaparición de proyectores de las aulas

ME PARECE INNESARIO ESTA INICIATIVA

las pertenencias de una compañera desaparecieron y solo le devolvieron el dni

el robo de proyectores multimedia y robo de casilleros

Robo de proyector

—

Se robaron el cañón de uno de los salones

Hace años se robaron los proyectores

Robo de cañones multimedia

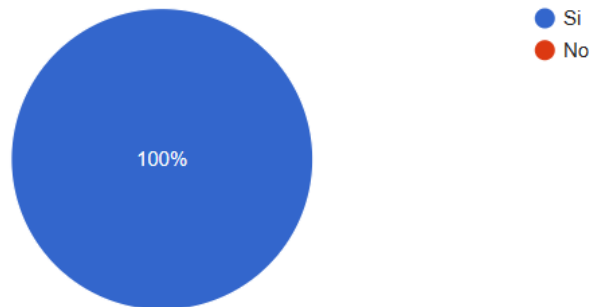
No

Robo de proyectores, pérdida de objetos

Robo de cañón multimedia

¿Ud cree que un sistema de videovigilancia mejoraría la situación de seguridad actual del pabellón de la EPIIS ?

23 respuestas



7. Forma de pago:

El formato de pago que se realizará para el proyecto se dará de dos formas.

- Se realizará un pago único para la compra de materiales que sean necesarios para el proyecto por medio de un tercero que gestione la compra y verificación de los productos.
- La otra forma de pago se relaciona con la instalación de los equipos en la infraestructura de la facultad de ingeniería informática

8. Penalidades:

En caso de retraso injustificado en la ejecución de la instalación y funcionamiento del sistema de vigilancia, dentro de los plazos dispuestos al efecto, la Entidad (E.P. Informática) aplicará a la empresa encargada una penalidad por mora por cada día de atraso, de conformidad con la siguiente fórmula:

Penalidad Diaria = $0.10 \times \text{Monto} / F \times \text{Plazo en día}$, donde:
Para plazos mayores a sesenta (60) días: $F = 0.25$

OTRAS PENALIDADES

Con el objeto de asegurar una mejor calidad de la ejecución de los trabajos, se establecen estas otras penalidades:

N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento
1	Cuando el contratista cambie el producto propuesto sin contar con la autorización previa de la Entidad.	25% de la UIT vigente por cada día de ocurrencia	Según informe de la Supervisión
2	No cumple con proveer el producto ofrecido en su propuesta, salvo hecho fortuito o fuerza mayor, debidamente acreditado, y con autorización de la Entidad.	50% de la UIT vigente por cada día de ocurrencia	Según informe de la Supervisión
3	No cumple con proveer los productos ofrecidos en su propuesta o que se encuentre 100% inoperativa.	25% de la UIT vigente por cada día de ocurrencia	Según informe de la Supervisión
4	Cuando el Contratista no cumple en presentar el informe correspondiente, dentro del plazo señalado.	20% de la UIT vigente por cada día de ocurrencia	Según informe de la Supervisión
5	Reemplazar al Ingeniero Director Técnico propuesto en su oferta técnica, en el periodo comprendido desde la firma del contrato y hasta el 50% del plazo de ejecución transcurrido, por considerarse determinante, entre otros, que con dicho Director Técnico en ese periodo se debe garantizar que la actividad se efectúe en forma oportuna y bajo las mejores condiciones de precio y calidad.	50% de la UIT vigente por cada día de ausencia del personal en obra en el plazo previsto.	Según informe de la Supervisión

9. Plan de trabajo

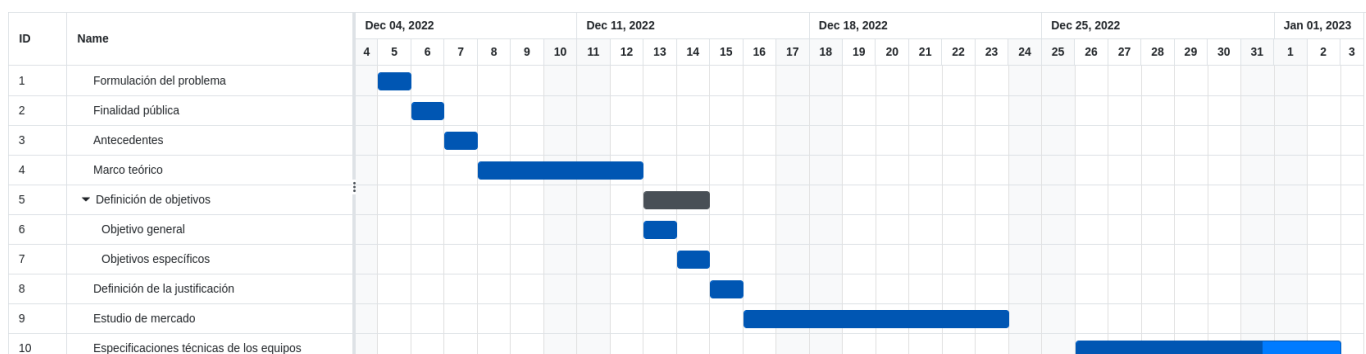


Fig 1. Diagrama de Gantt para el plan de trabajo

7. Supervisión del estudio y medidas de control durante el servicio

- El equipo encargado de realizar la supervisión son: Residente del proyecto, comisión de docentes y estudiantes del pabellón de informática.
- Dicho equipo está encargado de realizar un monitoreo del correcto funcionamiento de los equipos del sistema de videovigilancia. Como también está encargado de controlar y hacer cumplir los requisitos de garantía.
- Los trabajos mal ejecutados deberán ser satisfactoriamente corregidos y el material rechazado deberá ser reemplazado por otro aprobado, por cuenta del Postor. El Postor deberá facilitar sin cargo para la Entidad ni su representante el "Supervisor"; todas las inspecciones y pruebas que sean necesarias para que cumpla con su función de supervisión.

8. Responsabilidad por vicios ocultos

El proveedor en un tiempo de garantía, comete un incumplimiento del contrato, responderá éste a los daños y perjuicios durante un plazo de 1 año a contar desde la recepción.

Tales casos como:

- Los equipos no funcionan correctamente
- Equipos en mal estado
- No llegan el total de equipos

Una vez finalizado el contrato de garantía se aplica un incremento de pago de S/6000 como garantía extendida para un plazo de 1 años adicional

Si el proyecto se arruinara con posterioridad a la expiración del plazo de garantía y garantía extendida y no se hubiera manifestado ningún daño o perjuicio, quedará totalmente extinguida la responsabilidad del proveedor.

9. Características técnicas del sistema (especificaciones técnicas)

Cámara IP				
Item	Cantidad	Tipo	Requerimientos técnicos mínimos	
1	24	Equipo	Características	Especificaciones
			Lente varifocal	entre 2.7 mm a 13.5 mm
			Máxima apertura	Entre F1.4 y F1.6
			Ángulo de vista	112.5° a 30°
			Zoom óptico	2x o superiores
			Zoom digital	8x
			Distancia de grabación	15m
			Sensor de imagen	Entre 1/2.7" CMOS y 1/3" CMOS
			Resolución	1080p
			Píxeles	8MP (mínimo)
			Ethernet	10/100 Mbps (mínimo)
			Modo nocturno	Debe soportar
			Audio	Incluido
			Alimentación	Incluida
			Motion detection	Debe soportar
			Fuente y PoE	12V y debe soportar PoE

2. Switch PoE TP-LINK				
Item	Cantidad	Tipo	Requerimientos técnicos mínimos	
2	04	Equipo	Características	Especificaciones
			Puertos	5

			Ethernet	10/100/1000 Mbps
			Auto-Negociación	AUTO/AUTO MDI/MDIX
			Modelo	LS105G
			Medios de red	10BASE-T: cable UTP categoría 3, 4, 5 (máximo 50 m) EIA / TIA-568 100 Ω STP (50 m máximo) 100BASE-TX: cable de categoría 5, 5e de UTP (máximo 50 m) EIA / TIA-568 100 Ω STP (50 m máximo) 1000BASE-T: cable UTP de categoría 5, 5e, 6 o superior (50 m) EIA / TIA-568 100 Ω STP (50 m máximo)
			Consumo de energía	64 W (máximo con dispositivo PoE de 56w conectado) 4 W (máximo dispositivo sin PoE conectado)
			Fuente de alimentación	Adaptador de corriente externo (Salida: 48VDC / 1.25A)
			Puertos PoE	Estándar: compatible con 802.3 af Fuente de alimentación: 56W
			Compatibilidad con cámaras IP	Si
			Protección por sobrecarga	Si, PD \geq 56W
			Configuración e instalación	Requerida

3. Grabadoras de video en red 48 canales				
Item	Cantidad	Tipo	Requerimientos técnicos mínimos	
3	5	Equipo	Características	Especificaciones
			Entrada de Video/Audio	Debe ser capaz de hasta 48 canales
				Tendrá formato de compresión H.264
				Debe tener las siguientes resoluciones 8MP(4K), 6MP, 5MP, 4MP, 3MP, 1080p, UXGA, 960p, 720p, XGA, SVGA, D1, CIF, QCIF
				Debe tener un ancho de banda entrante de hasta 240Mbps
			Vista / viewing	Tendrá 1x HDMI y 1x VGA
				Debe cumplir hasta 4 pantallas simultáneas
				Debe tener mapeo electrónico
			Grabación	Debe tener modo manual, modo continuo, modo horario y Modo de evento (antes/después)
				Debe ser capaz de etiquetar
			Búsqueda y reproducción	Debe tener modos de búsqueda de fecha y hora (calendario) y eventos
				Debe tener una resolución de 16 x 4K@30fps o 16 x 3MP@30fps para reproducción (cliente)
				Debe tener las capacidades de Avance lento, Avance rápido, Bucle, Único reproducción de fotogramas.
			Almacenamiento	Será un disco duro de 8 x 3,5" HDD máx. 48 TB (hasta 6 TB/cada uno)
				Debe ser RAID 0/1/5/6/10
				Debe ser capaz de almacenamiento externo con Max. 100T y máx. escribevelocidad 128Mbps
Audio	Debe tener compresiones de audio G.711a, G.711u, ADPCM, G.722, G.722.1c y AAC-LC			

			Alarma	Tendrá entrada de alarma, pérdida de video, detección de movimiento, manipulación, Línea de guardia, Desenfoque, Cambio de sentido, Entrar al área de guardia, Salir de área de guardia, Objeto dejado, Eliminación de objeto, Recopilación y Aumento de audio como disparadores de alarma de servicio
				Tendrá disparadores de alarma del sistema, especialmente conflicto de dirección MAC
			Sistema	Debe ser Linux Embebido
				Tendrá inicio de sesión de usuario, operación de usuario, alarma, copia de seguridad y actualización como Gestión de registros
			Red	Debe tener protocolos de red TCP/IP, UDP, HTTP, DHCP, DNS/DDNS, RTP/RTCP, RTSP, PPPoE, FTP, SNTP, VSIP, UPNP, SMTP, IPv4, IPv6 (opcional)
				Debe tener funcionalidades de NAT, Socks5, Acceso múltiple de red, Recuperación de pérdida de paquetes y organización automática de la red
				Debe admitir pruebas de red
			Interfaz	Deberá tener 2 puertos de red Gigabite, interfaz RJ45
				Deberá tener línea RCA para entrada y salida de audio
				Tendrá 2 entradas y salidas de alarma
				Debe tener 2x RS485
				Debe tener 4x USB 2.0
				Tendrá 1x e-sata
			Operando	Condiciones Debe operar hasta 55°C y 10%-85% de humedad relativa
			Regulador	Debe estar listado en CE, FCC y Rohs
			Software	Base Vendrá con software gratuito para PC
			Teléfono inteligente	Acceso Deberá ser capaz de visualización de teléfonos inteligentes para IOS/Android
			Hard disk	8 unidades de disco duro de vigilancia de 4 TB

Servidor local (computadora) para registrar los archivos de video y los reconocimientos faciales				
ítem	cantidad	tipo	Requerimientos técnicos mínimos	
4	2	Equipo: Estación de trabajo NVR4X	características	Especificaciones
			Velocidad de datos de grabación	Hasta 120 Mbps
			Reproducción y transmisión de secuencias en directo	Hasta 100 Mbps
			Rendimiento de reproducción de vídeo de 16 MP a 24 fps	2 transmisiones principales + 16 transmisiones secundarias
			Interfaces de supervisión admitida	Combinación de hasta 2: mDP, DP y HDMI
			Sistema operativo	Microsoft Windows 10 IoT Enterprise LTSB (2019)
			Procesador	Intel Core i3 (10ª generación)
			Memoria	8 GB DDR4 RAM
			Unidad del sistema operativo	M.2 256 GB PCIe NVMe Clase 40 SSD
			Unidad de datos de vídeo	1 unidad SATA, disco duro de 8 TB
			Interfaz de red	2 puertos de 1 Gigabit Ethernet RJ-45 (1000Base-T)
			Salidas de vídeo	2 activas (4 × mDP)
			Unidad óptica	DVD-RW
			Formato	Pequeño formato
			Dimensiones (Pr x An x Al)	292 mm × 92,6 mm × 290 mm (11,50" × 3,65" × 11,42")
			Peso	5,26 kg (11,57 lb)
			Entrada de potencia	De 100 a 240 VCA, 50/60 Hz, conmutación automática
			Fuente de alimentación	Única no redundante
			Consumo de energía	260 W
			Temperatura de funcionamiento	De 10 °C a 35 °C (de 50 °F a 95 °F)
			Temperatura de almacenamiento	De -40 °C a 65 °C (de -40 °F a 149 °F)
			Humedad	Humedad relativa entre el 5 y el 95 % con un punto de rocío máximo de 33 °C (91 °F) (sin condensación)
			Vibración en funcionamiento	0,26 Grms entre 5 Hz y 350 Hz
			Vibración en almacenamiento	1,88 Grms entre 10 Hz y 500 Hz durante 15 minutos

			NVR4X-WKS-8TB	Teclado USB, ratón USB, cable de alimentación, 2 adaptadores de mDP a DP, 2 adaptadores de mPD a HDMI, El monitor se vende por separado
			Certificaciones/Directivas	UL, cUL, CE, RCM, CCC, KC, VCCI, EAC, BSMI, NOM, RoHS, Reach (SVHC)
			Seguridad	EN/IEC 62368-1
			Garantía	Asistencia técnica por teléfono ininterrumpida e ilimitada y 3 años de garantía de servicio al siguiente día hábil

650 VA Uninterruptible Power Supply				
ítem	cantidad	tipo	Requerimientos técnicos mínimos	
5	2	UPS en línea de doble conversión	características	Especificaciones
			Gestión de red integrada para automatización de apagado	controlar y automatizar el proceso de apagado del UPS en caso de falla en la alimentación
			UL1778, FFC Clase A, IEC62040-2 e ISTA 1A:	son normas internacionales y especificaciones de seguridad
			Rango de temperatura de funcionamiento:	rango de temperatura 0°-40°C
			LCD como panel de control:	Un panel de control con una pantalla LCD
			Potencia nominal:	La potencia nominal de 650VA / 360W debería ser suficiente para alimentar las cámaras y los dispositivos conectados.
			Conectividad:	conexiones USB, RS-232, Ethernet
			Control remoto:	Tenga una interfaz de usuario web o una API para poder acceder y configurar el UPS de manera remota
			Pequeño tamaño y portabilidad:	tamaño compacto y fácil de transportar para aplicaciones móviles.
			Comunicación	protocolos de comunicación SNMP para integrarse con sistemas de monitoreo y gestión de redes.
			Pure Sinewave:	alimentación pura senoidal

Sistema central de gestión de video (incluye software)

ítem	cantidad	tipo	Requerimientos técnicos mínimos	
6	01	Equipo	características	Especificaciones
			Debe soportar NVR	Hasta 128 NVR
			Acceso a diferentes niveles de usuario	Debe tener superadministrador/administrador/usuario
			Windows	Windows 10 o posterior
			Actualización de señal en vivo	Deberá tener la funcionalidad para tomar instantáneas.
			Capacidad de crear	Lista de grupos
			Ventanas múltiples	Hasta 64 ventanas
			Controlador PTZ	Tipo de software GUI
			Monitoreo de vista múltiple	Debe tener criterios de búsqueda a través de NVR, cámara, fecha y hora
			Tendrá en E-mapping	Debe tener criterios de búsqueda como personas, vehículos, objetos, dirección y color-

Cableado				
Item	Cantidad	Tipo	Requerimientos técnicos mínimos	
01		Equipo	Cable tray	300 mm x 100 mm galvanizadas
			Cable UTP	conductores cobre de 0.5 mm de diámetro y cubierta por PVC requisitos IEEE 802.3 10/100/1000 Base T RJ45 Categoría 6
			Cable UTP 4 pares	Homologado como CM o CMR Cumplir o superar ISO/IEC 11801:2002

Plazos de ejecución

Valor referencial: (500 soles por camara)

Experiencia del postor

Responsabilidad del contratista

Referencias:

https://link.springer.com/chapter/10.1007/978-981-15-7421-4_18
<http://dspace.utb.edu.ec/bitstream/handle/49000/10519/E-UTB-FAFI-SIST-000252.pdf?sequence=1&isAllowed=y>
<https://cuadernosdeseguridad.com/2021/03/sistemas-de-reconocimiento-facial-hospitales-scati-videovigilancia/>
<https://repository.ucatolica.edu.co/bitstream/10983/24032/1/Final%20Trabajo%20de%20grado.pdf>
<https://www.monografias.com/trabajos-pdf4/redes-computacionales/redes-computacionales.pdf>

References

Bosch Security System. (2013, 10 1). *Cámara domo IP de infrarrojos Día/noche HD de 720p*.

https://resources-boschsecurity-cdn.azureedge.net/public/documents/Data_sheet_esES_7720061835.pdf

CAPITULO II MARCO TEÓRICO. (n.d.). URBE. Retrieved January 24, 2023, from

<http://virtual.urbe.edu/tesispub/0033007/cap02.pdf>

JACKELINE, D. (2009, October 25). *MARCO TEÓRICO*. IMPORTANCIA DE LA IP. Retrieved

January 24, 2023, from

<http://proyectolasalle.blogspot.com/2009/10/anexos-de-la-investigacion.html>