# Implementación de comunicaciones unificadas y sistemas de seguridad

**Breve descripción:**

Este componente aborda la implementación de comunicaciones unificadas y sistemas de seguridad y abarca el diseño y ejecución de sistemas VoIP, integración de comunicaciones empresariales, y soluciones de seguridad electrónica como CCTV y alarmas. Por otra parte, también detalla la importancia de centros de control y la gestión de incidentes, orientados a optimizar la seguridad y la colaboración en entornos corporativos.

**Noviembre 2024**

## Tabla de contenido

# Introducción

La implementación de comunicaciones unificadas y sistemas de seguridad representa un pilar fundamental en la gestión de infraestructura empresarial moderna, donde la conectividad y la protección de la información son esenciales para garantizar operaciones fluidas y seguras. Este componente formativo profundiza en las tecnologías y estrategias necesarias para integrar redes de comunicación confiables y sistemas de seguridad efectivos en distintos entornos.

El contenido inicia con un análisis de la telefonía IP, abordando los conceptos de Voice over IP (VoIP), los protocolos de señalización y los criterios de calidad de servicio que permiten comunicaciones de voz de alta fidelidad a través de redes IP. A continuación, se estudian las comunicaciones unificadas, que integran diversos sistemas de mensajería y colaboración para mejorar la eficiencia operativa en las organizaciones, promoviendo un ambiente de trabajo más conectado y productivo.

El módulo también examina aspectos de seguridad electrónica, tales como los sistemas de CCTV, control de acceso y alarmas, que proporcionan medidas de protección robustas y eficaces en tiempo real. Estos sistemas contribuyen a prevenir incidentes y a responder de manera oportuna a amenazas de seguridad.

Para finalizar, se exploran los centros de control y la gestión de incidentes, apoyados por herramientas de analítica de video. Estos elementos permiten una supervisión continua de la infraestructura y una capacidad de respuesta ante emergencias, asegurando así la continuidad operativa y la seguridad de los activos empresariales.

¡Bienvenido al mundo de la Implementación de comunicaciones unificadas y sistemas de seguridad!

**Video 1.** Implementación de comunicaciones unificadas y sistemas de seguridad


Enlace de reproducción del video

| **Síntesis del video: Implementación de comunicaciones unificadas y sistemas de seguridad** |
| --- |
| En el componente formativo «Implementación de comunicaciones unificadas y sistemas de seguridad», se abordan los conocimientos y habilidades necesarias para configurar y gestionar infraestructuras avanzadas que integren tecnologías de comunicación y medidas de seguridad electrónica. |

Se aborda el diseño de soluciones VoIP, la configuración de sistemas de mensajería, y la implementación de mecanismos de seguridad como CCTV y sistemas de control de acceso.

Este componente destaca la importancia de actualizar y mantener las soluciones de comunicación y seguridad, asegurando que las infraestructuras estén preparadas para enfrentar nuevas amenazas y demandas tecnológicas.

Se promueve la integración de tecnologías emergentes para optimizar la gestión de recursos y fortalecer la seguridad de la información en entornos corporativos y organizacionales.

Las comunicaciones unificadas son esenciales en entornos empresariales modernos, permitiendo la integración de múltiples canales como voz, video, y mensajería en una plataforma centralizada.

Este enfoque mejora la productividad y asegura una interacción eficiente en tiempo real entre equipos, independientemente de su ubicación.

La seguridad electrónica es determinante en la protección de activos e información, y se exploran sistemas como videovigilancia, alarmas, y gestión de incidentes para prevenir y responder de manera eficiente a amenazas potenciales.

La correcta implementación de estas soluciones asegura un entorno seguro y resiliente, capaz de adaptarse a los desafíos actuales.

Se enfatiza la gestión proactiva de incidentes mediante el uso de centros de control y tecnologías de analítica de video, que optimizan la supervisión y garantizan una respuesta rápida y coordinada.

Con este componente adquirirás las herramientas necesarias para crear soluciones robustas que combinen eficiencia operativa y protección integral.

¡Bienvenido al mundo de las comunicaciones unificadas y la seguridad electrónica, donde la innovación y la protección trabajan de la mano para crear infraestructuras seguras y eficaces!

# 1. Telefonía IP

La Telefonía IP utiliza redes de protocolo de Internet para gestionar comunicaciones de voz, video y datos, transformando la manera en que se llevan a cabo las interacciones telefónicas tradicionales. Este tipo de telefonía se basa en la tecnología VoIP (Voice over IP), la cual permite transmitir la voz mediante paquetes de datos digitales en vez de señales analógicas, lo que optimiza costos y aumenta la flexibilidad de uso en redes ya existentes.

Para operar de manera eficaz, la Telefonía IP depende de protocolos de señalización como SIP (Session Initiation Protocol) y H.323, los cuales establecen y finalizan las conexiones entre dispositivos. Estos protocolos son primordiales para coordinar los elementos de la red, garantizando que las llamadas y los datos multimedia se envíen y reciban correctamente.

La calidad de servicio (QoS) es una característica crítica en la Telefonía IP, ya que asegura la claridad de la comunicación, evitando interferencias y pérdida de datos en el proceso. Este control de calidad implica técnicas de priorización y gestión del ancho de banda que evitan retrasos en las transmisiones, lo cual es determinante para aplicaciones empresariales y de atención al cliente donde la fiabilidad es fundamental.

## 1.1. Arquitectura VoIP

La arquitectura VoIP (Voice over IP) permite transmitir voz y multimedia a través de redes de datos IP en lugar de redes de telefonía tradicional. La infraestructura VoIP está compuesta por varios elementos clave, como gateways de voz, servidores de señalización y redes de transporte IP. Estos componentes colaboran para convertir

señales de voz en paquetes de datos digitales, transmitiéndolos de forma eficiente y económica.

Un elemento indispensable en esta arquitectura es la red IP subyacente, que soporta una estructura escalable y adaptable. Esta arquitectura también permite la integración con sistemas telefónicos convencionales, facilitando el uso de tecnologías IP y tradicionales en un mismo entorno. Asimismo, el diseño de la arquitectura VoIP es flexible, permitiendo implementaciones en una variedad de entornos, desde pequeñas empresas hasta grandes organizaciones multinacionales.

La VoIP se beneficia de protocolos específicos como SIP (Session Initiation Protocol) y H.323, que facilitan la conexión, configuración y finalización de llamadas. Estos protocolos son imprescindibles para mantener la calidad de servicio (QoS) y asegurar una experiencia de comunicación de alta calidad.

## 1.2. Protocolos de señalización

Estos protocolos son fundamentales en la transmisión de voz y datos en la Telefonía IP (VoIP), ya que permiten la configuración, modificación y finalización de llamadas. Entre los más relevantes destacan Session Initiation Protocol (SIP), H.323, y Media Gateway Control Protocol (MGCP). Cada uno de estos protocolos cumple funciones primordiales en la comunicación de datos en redes de telefonía IP, estableciendo la ruta que los datos deben seguir y la estructura de cada sesión, asegurando así una conexión fluida entre los dispositivos.

El Session Initiation Protocol (SIP) es ampliamente utilizado debido a su flexibilidad y eficiencia para iniciar y finalizar sesiones de comunicación. Este protocolo es preferido en aplicaciones de telefonía IP por su estructura y su capacidad de

integración con otras tecnologías, facilitando la interoperabilidad entre diversos sistemas y dispositivos. SIP permite la conexión de múltiples dispositivos en una única llamada, soportando una variedad de dispositivos de comunicación, como teléfonos IP, aplicaciones de software y sistemas de mensajería.

Por otro lado, el protocolo H.323 es otro estándar importante, especialmente en redes que combinan voz, video y datos en una sola transmisión. Aunque requiere mayor capacidad de procesamiento, ofrece un alto nivel de calidad de servicio y seguridad, especialmente en aplicaciones corporativas. La arquitectura de H.323 es útil en escenarios de comunicaciones donde la confiabilidad y la seguridad son críticas, por lo que sigue siendo una opción relevante en ciertos contextos empresariales.

**Tabla 1.** Protocolos de señalización

| Protocolo de señalización | Función principal | Características clave | Aplicaciones comunes |
|---|---|---|---|
| SIP (Session Initiation Protocol). | Establecer, modificar y finalizar sesiones de comunicación. | Facilita la interoperabilidad, extensibilidad. | Comunicaciones VoIP, videoconferencias. |
| H.323. | Estándar para multimedia sobre redes IP. | Amplio soporte en videoconferencias y VoIP. | Videoconferencias empresariales. |
| MGCP (Media Gateway Control Protocol). | Control de Gateways para llamadas. | Permite interoperabilidad entre diferentes redes. | Telefonía IP. |
| SCCP (Skinny Client Control Protocol). | Protocolo propietario de Cisco. | Mayor integración con sistemas de Cisco. | Redes VoIP de Cisco. |

Fuente. OIT, 2024.

## 1.3. Calidad de servicio

**La calidad de servicio (QoS, por sus siglas en inglés)** es un componente crítico en sistemas de comunicaciones unificadas, especialmente en la **Telefonía IP (VoIP)**, donde es fundamental garantizar que la transmisión de voz y datos se mantenga en un nivel de calidad óptimo para evitar interrupciones o pérdida de información. La QoS se encarga de definir las prioridades en el tráfico de red, permitiendo que la transmisión de voz tenga preferencia sobre otros tipos de datos en momentos de alta demanda. Esto se logra mediante técnicas como la gestión de ancho de banda, la priorización de paquetes y el control de congestión en la red.

Para implementar una calidad de servicio eficiente, las redes deben contar con sistemas de monitoreo y control que identifiquen y gestionen los tipos de tráfico, priorizando aquellos que demanden menor latencia y mayor consistencia, como es el caso de las llamadas de voz. De esta manera, los dispositivos y protocolos de señalización en la red, como RTP y SIP, colaboran para asignar el ancho de banda y los recursos necesarios para mantener la calidad de la llamada, incluso en condiciones de congestión.

Los desafíos de la QoS se amplían cuando se integran servicios adicionales, como videollamadas y mensajería, dentro de una misma infraestructura. Para estos casos, las arquitecturas de red deben adaptarse para soportar distintos tipos de tráfico simultáneamente, asegurando que cada servicio reciba los recursos que necesita para operar con eficacia. Esta gestión cuidadosa es primordial para garantizar una experiencia de usuario consistente y confiable en entornos de colaboración empresarial y comunicaciones unificadas.

## 2. Integración de sistemas

En la implementación de comunicaciones unificadas y sistemas de seguridad, la integración de sistemas es necesaria para centralizar y optimizar los distintos métodos de comunicación dentro de una empresa. En este contexto, las comunicaciones unificadas reúnen servicios de voz, mensajería, videoconferencias y otros canales, lo que permite una mayor fluidez en la interacción entre empleados y clientes, promoviendo una comunicación eficiente y en tiempo real.

Los sistemas de integración también abarcan los servicios de mensajería, que incluyen el envío de mensajes de texto, correos electrónicos, y notificaciones en diversas plataformas. Estos servicios son fundamentales para asegurar que la comunicación se mantenga constante y accesible desde cualquier dispositivo, contribuyendo a una experiencia de usuario optimizada y continua. Por su parte, los sistemas de integración permiten que la información esté disponible de manera más rápida, facilitando el flujo de datos y permitiendo la interoperabilidad entre aplicaciones y dispositivos.

La colaboración empresarial es otro pilar de la integración de sistemas, que va más allá de la comunicación básica al incluir herramientas que promuevan el trabajo colaborativo. Estas herramientas integradas mejoran la productividad al facilitar el acceso a datos compartidos y al permitir la creación de entornos de trabajo digitales. Extra, con la implementación de aplicaciones en la nube, los usuarios pueden colaborar en tiempo real sin importar la ubicación, optimizando así los procesos empresariales y potenciando la toma de decisiones informada y rápida.

## 2.1. Comunicaciones unificadas

Las comunicaciones unificadas integran diversos servicios de comunicación, como mensajería instantánea, videoconferencia, telefonía IP y correo electrónico, en una plataforma centralizada que permite una colaboración más eficiente. Este enfoque elimina la fragmentación en las herramientas de comunicación, lo que resulta en un flujo de trabajo más continuo y una mejor sincronización entre los equipos. La centralización de estos sistemas mejora tanto la accesibilidad de la información como la rapidez de respuesta en contextos empresariales y de teletrabajo.

Este sistema permite la interoperabilidad entre diferentes dispositivos y plataformas, facilitando la comunicación en tiempo real y aumentando la flexibilidad en los entornos de trabajo remoto e híbrido. Las comunicaciones unificadas ofrecen una arquitectura modular que puede adaptarse a las necesidades específicas de cada organización, desde servicios básicos de mensajería hasta sistemas avanzados de videoconferencia. La capacidad de integrar diferentes tecnologías permite la optimización de recursos y reduce la necesidad de infraestructura adicional, lo cual es fundamental para reducir costos operativos.

Asimismo, las plataformas de comunicaciones unificadas incorporan medidas de seguridad para proteger la información transmitida y evitar accesos no autorizados. La implementación de encriptación de extremo a extremo y de autenticación multifactorial ayuda a garantizar la privacidad de los datos, lo cual es esencial en industrias con altos requisitos de confidencialidad. Con estas soluciones, las organizaciones pueden mejorar la experiencia de usuario, reducir el tiempo de respuesta y minimizar el riesgo de incidentes de seguridad.

Entre los beneficios más destacados de las comunicaciones unificadas se encuentran la reducción de tiempos de respuesta, el mejor aprovechamiento de los recursos y la posibilidad de integrar nuevas herramientas conforme la tecnología avanza. También permite a las organizaciones centralizar la gestión de la infraestructura de comunicación, facilitando el monitoreo y control de la calidad de los servicios de comunicación. La implementación de esta tecnología requiere una arquitectura robusta de red y el uso de protocolos avanzados que aseguren tanto la calidad como la seguridad de los datos transmitidos.

## 2.2. Servicios de mensajería

Los servicios de mensajería constituyen uno de los pilares fundamentales en el entorno de las comunicaciones unificadas, facilitando la comunicación rápida y eficiente a través de diversas plataformas, como la mensajería instantánea, correos electrónicos, y notificaciones push. Estos servicios permiten a los usuarios interactuar y transmitir información de manera sincrónica y asincrónica, contribuyendo a la continuidad operativa y mejorando la comunicación entre equipos y departamentos. Por otra parte, ofrecen la posibilidad de integrar diferentes aplicaciones, permitiendo que la información fluya sin interrupciones en el entorno laboral.

La implementación de servicios de mensajería permite mantener un flujo de comunicación ininterrumpido, incluso en situaciones de alta demanda o cuando el equipo de trabajo está distribuido geográficamente. Mediante herramientas como chats empresariales, plataformas de mensajería instantánea y correos electrónicos, los empleados pueden colaborar en tiempo real y mantener la coherencia en los procesos. Este tipo de servicios también integra funcionalidades de archivo, rastreo y búsqueda de mensajes, lo cual facilita la gestión de la información y el cumplimiento normativo.

Por otro lado, los servicios de mensajería también enfrentan desafíos relacionados con la privacidad y la seguridad de los datos, especialmente cuando se trata de información sensible o clasificada. Para abordar estos desafíos, las plataformas de mensajería incluyen medidas avanzadas de seguridad, como el cifrado de extremo a extremo, la autenticación de usuarios y el control de acceso, asegurando que la información compartida se mantenga protegida frente a accesos no autorizados. Así, los servicios de mensajería representan una herramienta versátil y segura para las organizaciones modernas, adaptándose a las necesidades cambiantes de comunicación y colaboración.

## 2.3. Colaboración empresarial

La colaboración empresarial se ha convertido en un aspecto primordial en los entornos de trabajo modernos, especialmente en aquellos que adoptan plataformas de comunicaciones unificadas. Estas herramientas integradas permiten que los equipos trabajen de manera conjunta y coordinada, sin importar su ubicación geográfica. La colaboración empresarial incluye el uso de diversas aplicaciones, como videoconferencias, gestión de documentos compartidos, y entornos de trabajo en línea, lo que optimiza el flujo de información y facilita el trabajo en equipo. En un mundo laboral cada vez más remoto y globalizado, estas herramientas fomentan una mayor eficiencia y permiten responder ágilmente a las demandas del mercado.

Uno de los beneficios primordiales de las soluciones de colaboración empresarial es la posibilidad de unificar diversas formas de comunicación en una sola plataforma, lo que disminuye la necesidad de cambiar entre aplicaciones. Esto no solo mejora la productividad, sino que también reduce los costos asociados a la administración de múltiples sistemas. Las soluciones de colaboración empresarial suelen incluir

funcionalidades como mensajería instantánea, conferencias web, almacenamiento en la nube, y gestión de proyectos en tiempo real. Al centralizar estas herramientas en un sistema unificado, las organizaciones pueden mantener una comunicación fluida y continua, potenciando el trabajo colaborativo.

La implementación de tecnologías para la colaboración empresarial también presenta desafíos, entre los cuales se encuentran la seguridad de la información y la gestión adecuada de permisos y accesos. Para garantizar la integridad y confidencialidad de los datos, es fundamental aplicar protocolos de seguridad robustos, tales como el cifrado de información, la autenticación multifactor y las políticas de acceso basadas en roles. Esto ayuda a proteger la información empresarial y asegura que los datos compartidos a través de estas plataformas estén a salvo de posibles amenazas externas.

Un aspecto central de la colaboración empresarial en la integración de sistemas es la interoperabilidad. Las empresas deben trabajar juntas para garantizar que los sistemas de comunicaciones unificadas sean compatibles con los sistemas de seguridad existentes, como CCTV, control de acceso y sistemas de alarma. Esto requiere una estrecha coordinación y comunicación entre los equipos técnicos y de gestión para asegurar que todos los componentes funcionen de manera coherente y eficiente.

Igualmente, la colaboración empresarial facilita la innovación y el desarrollo de nuevas soluciones tecnológicas. Las empresas pueden compartir conocimientos y recursos para desarrollar productos y servicios que mejoren la seguridad y la eficiencia operativa. Por ejemplo, la integración de análisis de video avanzados con sistemas de comunicaciones unificadas puede proporcionar a las empresas una capacidad mejorada para monitorear y gestionar incidentes de seguridad en tiempo real.

Por último, la colaboración empresarial también es vital para la formación y el desarrollo de capacidades. Las empresas pueden colaborar en programas de capacitación y desarrollo profesional para asegurar que sus empleados estén equipados con las habilidades necesarias para manejar y mantener los sistemas integrados. Esto no solo mejora la eficacia operativa, sino que también promueve una cultura de aprendizaje continuo y mejora la retención de talento en la organización.

## 3. Seguridad electrónica

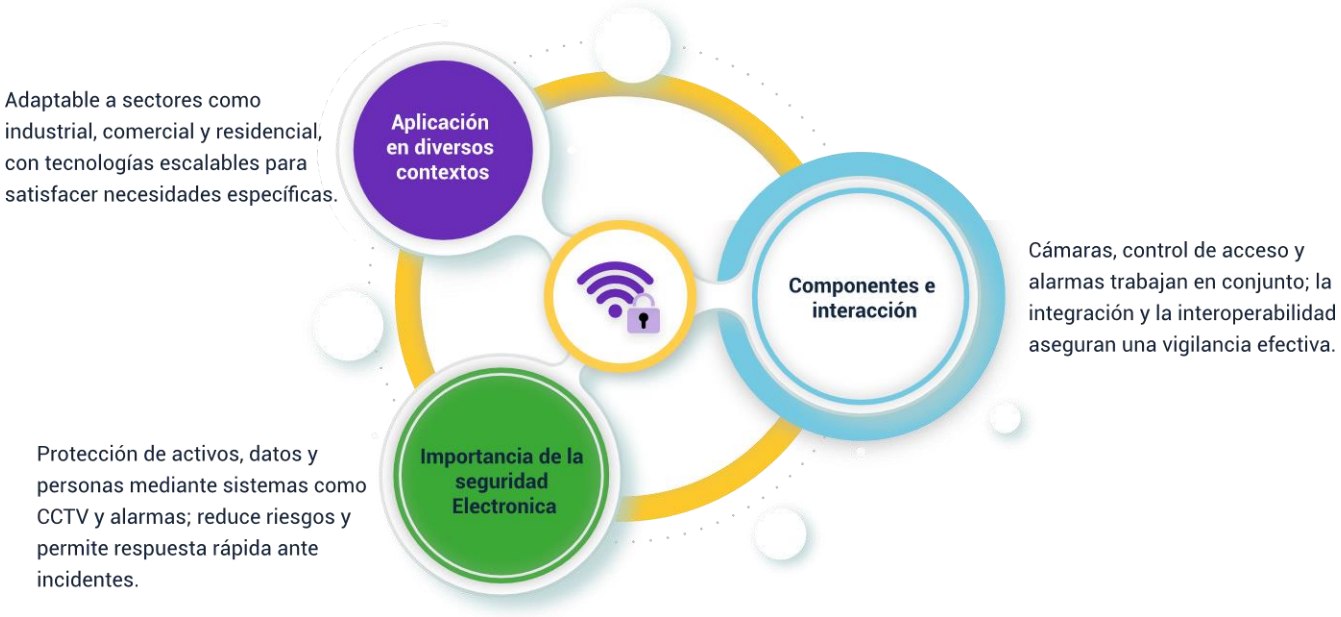
La seguridad electrónica es un componente primordial en sistemas de infraestructura moderna, donde la implementación de tecnología avanzada en vigilancia y control garantiza un entorno protegido para bienes y personas. Al integrar sistemas de videovigilancia, control de acceso, y sistemas de alarma, se construye un ecosistema de seguridad que abarca prevención, monitoreo y respuesta a incidentes.

La seguridad electrónica abarca sistemas y tecnologías diseñadas para proteger personas, bienes, y datos, estableciendo mecanismos de vigilancia y control en entornos físicos y digitales. Este campo ha cobrado relevancia en los últimos años debido al crecimiento de amenazas y vulnerabilidades en el ámbito empresarial y residencial. Las soluciones de seguridad electrónica incluyen una variedad de dispositivos, como cámaras de vigilancia, sistemas de control de acceso, y alarmas, que actúan como barreras protectoras y como herramientas de monitoreo en tiempo real. En entornos corporativos, estas herramientas son integradas para ofrecer una capa de seguridad completa que abarca desde la supervisión del personal hasta la protección de infraestructuras críticas.

Es importante considerar que, para una implementación efectiva de la seguridad electrónica, se deben respetar las normativas legales y estándares de calidad, como los establecidos por la Organización Internacional de Normalización (ISO) y las leyes locales sobre privacidad y protección de datos. La Ley de Protección de Datos en diferentes países regula la recopilación y almacenamiento de imágenes y datos personales obtenidos mediante sistemas de seguridad, y la ISO/IEC 27001 establece pautas sobre la gestión de seguridad de la información en entornos organizacionales.

En la actualidad, la evolución de la seguridad electrónica también integra tecnologías avanzadas como la inteligencia artificial y el análisis de video, que mejoran la capacidad de predicción y detección de amenazas. Estas herramientas permiten identificar patrones sospechosos, alertar en tiempo real, y optimizar la respuesta ante incidentes. Por lo tanto, los profesionales en el área deben estar capacitados no solo en el uso de estos sistemas, sino también en el cumplimiento de normativas que regulan su aplicación y en la interpretación de la información que estos sistemas proporcionan.

**Figura 1.** Elementos de la seguridad electrónica




Fuente. OIT, 2024.

a) **Importancia de la seguridad electrónica**: este campo es vital para garantizar la protección de activos, datos y personas. Los sistemas de seguridad electrónica abarcan desde dispositivos como cámaras de videovigilancia (CCTV) y sistemas de control de acceso hasta alarmas avanzadas, todos diseñados para responder a amenazas de manera

preventiva y reactiva. La seguridad electrónica es fundamental en la reducción de riesgos asociados a accesos no autorizados y actividades sospechosas, permitiendo así una respuesta rápida y efectiva ante posibles incidentes.

b) **Aplicación en diversos contextos**: las tecnologías de seguridad electrónica han evolucionado y ahora se aplican en diversos sectores, desde instalaciones industriales y comerciales hasta residencias particulares. Gracias a su escalabilidad, es posible configurar estos sistemas de acuerdo con las necesidades específicas de cada entorno, logrando un equilibrio entre seguridad y usabilidad. La instalación de cámaras de alta definición, controles de acceso mediante biometría, y alarmas inteligentes son algunos de los elementos que, cuando trabajan conjuntamente, ofrecen soluciones integrales y decisivas para la seguridad de un espacio.

c) **Componentes principales y su interacción**: los sistemas de seguridad electrónica están integrados por múltiples componentes interconectados. Entre los más comunes se encuentran las cámaras de videovigilancia, que permiten monitorear áreas en tiempo real; los sistemas de control de acceso, que restringen la entrada a personal autorizado; y los sistemas de alarma, que alertan ante cualquier actividad anómala. La efectividad de estos sistemas reside en la capacidad de integración y en la interoperabilidad entre estos dispositivos, logrando una vigilancia continua y efectiva.

## 3.1. Sistemas CCTV

Los sistemas de circuito cerrado de televisión (CCTV) constituyen una herramienta determinante en el ámbito de la seguridad electrónica, proporcionando una vigilancia continua de espacios específicos mediante cámaras conectadas a un sistema cerrado de monitores. Estos sistemas permiten una supervisión en tiempo real, y su implementación es común en edificios empresariales, zonas residenciales, instituciones públicas y áreas de acceso restringido. Los sistemas CCTV son altamente versátiles, ya que pueden configurarse para grabar imágenes, transmitir en directo o activar alertas en respuesta a ciertos movimientos o actividades. La calidad de imagen y las capacidades de almacenamiento han mejorado notablemente con el tiempo, ofreciendo imágenes en alta definición y opciones de almacenamiento en la nube, que facilitan el acceso a las grabaciones desde cualquier ubicación.

Los sistemas de CCTV son una medida de seguridad disuasoria, ya que la presencia de cámaras puede reducir el número de incidentes, como robos o actos de vandalismo, al crear un entorno en el que las personas están conscientes de la vigilancia. Además, los videos capturados por estos sistemas pueden servir como evidencia en investigaciones, facilitando la identificación de personas o actividades específicas. Esta capacidad de registro es especialmente útil en casos donde se requiere documentación visual para procesos legales o investigaciones internas.

En términos de normatividad, el uso de sistemas CCTV debe cumplir con regulaciones de privacidad y protección de datos en cada país. Por ejemplo, la Ley de Protección de Datos Personales establece directrices sobre la recopilación, tratamiento y almacenamiento de imágenes de personas, y en muchos casos, exige que las áreas vigiladas informen de la presencia de cámaras mediante avisos visibles. Asimismo, es

necesario que los administradores de estos sistemas garanticen que las grabaciones estén protegidas contra accesos no autorizados, en concordancia con normativas como la ISO/IEC 27001, que regula la seguridad de la información.

En los últimos años, los sistemas CCTV han integrado tecnologías avanzadas, como la inteligencia artificial y el reconocimiento facial, lo cual amplía sus capacidades y eficiencia en la detección de eventos o comportamientos sospechosos. Estos avances permiten una respuesta más ágil ante situaciones de riesgo y una gestión más precisa de las incidencias. La analítica de video, por ejemplo, facilita el reconocimiento de patrones específicos, lo que resulta útil para la identificación de amenazas en tiempo real. Sin embargo, el uso de estas tecnologías debe gestionarse cuidadosamente para evitar problemas éticos relacionados con la privacidad.

**Tabla 2.** Sistemas de seguridad electrónica

| Sistema de Seguridad | Descripción | Componentes Centrales | Aplicaciones |
|---|---|---|---|
| CCTV. | Sistema de videovigilancia. | Cámaras, monitores, grabadores. | Monitoreo de espacios. |
| Control de acceso. | Permite restringir la entrada y salida. | Tarjetas de acceso, lectores biométricos. | Seguridad en edificios y áreas restringidas. |
| Sistemas de alarma. | Detecta intrusiones y emergencias. | Sensores, alarmas, panel de control. | Seguridad en viviendas y oficinas. |
| Analítica de video. | Análisis automatizado de videos. | Software de IA, cámaras inteligentes. | Detección de anomalías en tiempo real. |

Fuente. OIT, 2024.

## 3.2. Control de acceso

El control de acceso es una medida de seguridad que restringe y gestiona el ingreso a áreas específicas dentro de una instalación o edificio. Este sistema permite establecer niveles de autorización para cada persona, lo que garantiza que solo individuos con permisos específicos puedan acceder a zonas restringidas, reduciendo así el riesgo de intrusiones y protegiendo tanto los activos físicos como la información sensible. Los métodos de control de acceso varían desde tecnologías simples, como tarjetas de proximidad o claves de acceso, hasta sistemas más avanzados que integran autenticación biométrica (huellas digitales, reconocimiento facial, etc.) para asegurar que únicamente las personas autorizadas puedan ingresar a ciertos espacios.

Los sistemas de control de acceso no solo se implementan en áreas de alto riesgo, como salas de servidores o zonas de almacenamiento, sino también en edificios corporativos, hospitales, medios de comunicación, entidades estatales y áreas residenciales, donde es importante mantener un control de flujo de personas. Adicionalmente, estos sistemas suelen integrarse con otras soluciones de seguridad, como CCTV y alarmas, para ofrecer un monitoreo integral. Esta integración permite registrar eventos de acceso en tiempo real, generando informes detallados de actividad, lo cual es útil en caso de auditorías o investigaciones internas.

Para que los sistemas de control de acceso cumplan su función de manera efectiva, es fundamental que se adhieran a normativas y estándares de seguridad. Por ejemplo, el estándar ISO/IEC 27001 establece requisitos para la protección de información, lo cual incluye el control de acceso a datos físicos y digitales. De la misma forma, los reglamentos locales de protección de datos son aplicables cuando el sistema recopila información de los usuarios, especialmente en caso de emplear biometría, ya

que se considera un dato sensible. Cumplir con estos estándares garantiza la legalidad y efectividad del sistema, al tiempo que protege la privacidad de los individuos.

Los avances tecnológicos han permitido que los sistemas de control de acceso sean cada vez más seguros y adaptables a diferentes necesidades. Actualmente, existen soluciones que permiten la gestión remota del acceso, lo cual facilita la administración de permisos en tiempo real desde dispositivos móviles o plataformas en la nube. Esta flexibilidad es particularmente útil en entornos empresariales o en casos de emergencia, donde es necesario ajustar rápidamente los permisos de acceso según las circunstancias. Con el continuo desarrollo de la tecnología, los sistemas de control de acceso seguirán evolucionando, integrando nuevas funciones para mejorar la seguridad y optimizar la gestión de acceso.

**Tabla 3.** Gestión de incidentes y monitoreo

| Etapa de Gestión de Incidentes | Descripción | Componentes Centrales |
|---|---|---|
| Identificación. | Detectar y registrar incidentes de seguridad. | Minimizar el tiempo de respuesta. |
| Contención. | Limitar el impacto del incidente en la red o sistema. | Evitar la propagación del problema. |
| Erradicación. | Eliminar la causa raíz del incidente. | Restaurar la seguridad del sistema. |
| Recuperación. | Restaurar el funcionamiento normal. | Reducir el impacto en el servicio. |

| Etapa de Gestión de Incidentes | Descripción | Componentes Centrales |
|---|---|---|
| Revisión. | Analizar el incidente para evitar futuras ocurrencias. | Mejorar la respuesta y prevención de incidentes. |

Fuente. OIT, 2024.

## 3.3. Sistemas de alarma

Los sistemas de alarma son componentes fundamentales de la seguridad electrónica, diseñados para detectar y alertar sobre situaciones de riesgo, como intrusiones, incendios, o emergencias en general. Estos sistemas funcionan mediante una combinación de sensores, paneles de control, y dispositivos de notificación (sirenas, luces o avisos remotos) que activan alertas en el momento en que se detecta una anomalía o se produce un evento que desencadena la alarma. En entornos comerciales y residenciales, los sistemas de alarma ayudan a prevenir robos y a mitigar daños mediante la detección temprana de amenazas.

Existen diversos tipos de sistemas de alarma, adaptados a las necesidades y características de cada espacio. Las alarmas antirrobo, por ejemplo, suelen emplear sensores de movimiento y de apertura en puertas y ventanas, mientras que las alarmas contra incendios utilizan detectores de humo, calor o gases tóxicos. Cada sistema se puede personalizar de acuerdo con el nivel de riesgo, la distribución de los espacios, y el tipo de amenaza que se desea mitigar. Las alarmas también pueden integrarse con sistemas de videovigilancia y control de acceso para ofrecer una solución de seguridad completa, que facilite el monitoreo y la gestión de incidentes.

El uso de sistemas de alarma debe cumplir con normativas específicas de seguridad y protección. En muchos países, los sistemas de detección y alerta de incendios, por ejemplo, están regulados por estándares nacionales e internacionales que establecen las características y especificaciones técnicas de los equipos. También existen requisitos en cuanto a la instalación, mantenimiento y supervisión de estos sistemas, como los que se encuentran en la Norma NFPA 72 para sistemas de detección de incendios y en las directrices de seguridad de la ISO 7240-1. Estas regulaciones aseguran que los sistemas funcionen de manera confiable y efectiva en situaciones de emergencia.

En términos de innovación, los sistemas de alarma han evolucionado significativamente en los últimos años. Hoy en día, muchos sistemas están conectados a plataformas de monitoreo remoto y ofrecen la posibilidad de recibir alertas directamente en dispositivos móviles. Esto permite a los propietarios y responsables de seguridad supervisar el estado del sistema en tiempo real y responder rápidamente ante cualquier alerta. La tecnología moderna también permite la implementación de alarmas inteligentes, que utilizan inteligencia artificial para diferenciar entre falsas alarmas y amenazas reales, reduciendo así la frecuencia de activaciones innecesarias.

Las alarmas de riesgo ambiental desempeñan un papel vital en la protección de comunidades y entornos naturales, especialmente en territorios expuestos a amenazas naturales o ambientales, como ciudades, municipios y pueblos. Estos sistemas de alarma están diseñados para detectar eventos como inundaciones, incendios forestales, deslizamientos de tierra, y emisiones de gases tóxicos, alertando a la población y a los servicios de emergencia de manera oportuna.

Su implementación permite la activación de planes de evacuación, cierres de rutas de acceso y coordinación de recursos, minimizando el impacto de estos eventos en la población y en la infraestructura local. En algunos territorios, estas alarmas se integran con redes de sensores y estaciones meteorológicas que monitorean en tiempo real variables como la humedad, temperatura y movimientos de tierra, permitiendo a las autoridades anticiparse a fenómenos que podrían poner en riesgo a las personas y los ecosistemas.

# 4. Monitoreo y gestión

El monitoreo y la gestión son componentes fundamentales en los sistemas de seguridad electrónica, ya que permiten supervisar de manera continua las condiciones de un entorno y reaccionar ante cualquier evento que pueda suponer una amenaza. Estas prácticas comprenden desde el control de accesos y la vigilancia por CCTV, hasta el seguimiento de alarmas y la gestión de incidentes. La supervisión en tiempo real proporciona una capa de protección adicional al permitir una respuesta rápida y adecuada ante situaciones de emergencia, lo que es esencial para minimizar daños y optimizar los recursos de seguridad disponibles.

En el contexto de infraestructuras críticas, como instalaciones gubernamentales, centros de salud, y sistemas de transporte, el monitoreo constante resulta indispensable para proteger tanto los activos como a las personas que interactúan en dichos entornos. Los centros de control centralizan esta tarea, facilitando la coordinación entre los diferentes dispositivos y sistemas de seguridad. Estos centros están equipados con herramientas avanzadas de gestión de incidentes y analítica de video, que ayudan a los operadores a identificar patrones sospechosos y a tomar decisiones informadas en momentos críticos. La integración de diversas tecnologías permite que el personal de seguridad mantenga una visión completa y en tiempo real de la situación.

Uno de los aspectos más innovadores en el monitoreo y gestión es el uso de la analítica de video, que aplica inteligencia artificial para mejorar la precisión y eficiencia de la supervisión. Con esta tecnología, es posible realizar tareas como el reconocimiento facial, la detección de comportamientos anómalos, y el análisis de multitudes, lo que contribuye a una respuesta más proactiva ante posibles amenazas.

Estas capacidades avanzadas permiten que los sistemas detecten patrones de riesgo antes de que se conviertan en problemas graves, optimizando así los recursos de seguridad y mejorando la protección en lugares de alta concurrencia.

La gestión de incidentes es otra pieza fundamental dentro de estos sistemas, ya que implica coordinar la respuesta a situaciones específicas, desde emergencias médicas hasta riesgos ambientales. Los protocolos de gestión de incidentes permiten que el personal de seguridad actúe rápidamente, siguiendo una serie de procedimientos estandarizados para cada tipo de amenaza. Esto reduce la posibilidad de errores y garantiza que la respuesta sea adecuada a la magnitud del incidente. La tecnología actual permite registrar cada incidente y generar reportes automáticos, lo que resulta útil para análisis posteriores y para mejorar las estrategias de prevención y respuesta.

Finalmente, el monitoreo y la gestión son fundamentales en la planificación de la seguridad a largo plazo, ya que los datos recopilados proporcionan información valiosa sobre las tendencias de riesgo en un territorio o instalación específica. Este análisis permite anticiparse a posibles problemas y ajustar los recursos de seguridad de acuerdo con las necesidades emergentes. En la actualidad, muchas instituciones públicas y privadas están invirtiendo en plataformas de monitoreo avanzado que integran diferentes fuentes de datos, promoviendo una gestión de la seguridad más precisa y efectiva.

## 4.1. Centros de control

Los centros de control son espacios centralizados dedicados a la supervisión, coordinación y gestión de los sistemas de seguridad en una instalación o territorio. En estos centros, los operadores pueden monitorear en tiempo real las actividades

capturadas por cámaras de videovigilancia, sistemas de control de acceso, alarmas, y otros dispositivos electrónicos de seguridad. Estos espacios suelen estar equipados con múltiples pantallas, consolas de control y sistemas de comunicación, que permiten una visión integral de la seguridad en toda la instalación. Gracias a la tecnología moderna, los centros de control también pueden recibir y procesar información proveniente de sensores y redes externas, facilitando una respuesta rápida y coordinada ante cualquier incidente.

La organización de los centros de control varía según el tamaño y las necesidades de la instalación que protegen. En grandes instalaciones o infraestructuras críticas, como aeropuertos, hospitales o centrales eléctricas, los centros de control pueden contar con múltiples operadores especializados en distintas áreas de seguridad. Esta estructura permite una división del trabajo más eficiente y asegura que cada aspecto de la seguridad esté cubierto por personal capacitado en la tecnología específica que se monitorea. Asimismo, los centros de control suelen integrarse con los servicios de emergencia locales, como bomberos o policía, facilitando una respuesta conjunta ante situaciones críticas.

La importancia de los centros de control radica en su capacidad para coordinar respuestas a incidentes de manera ágil y precisa. Los operadores pueden seguir protocolos establecidos para cada tipo de situación, como intrusiones, incendios o emergencias médicas, reduciendo el tiempo de reacción y minimizando los daños potenciales. Igualmente, los centros de control permiten el registro y análisis de los incidentes, generando informes detallados que pueden utilizarse para mejorar la planificación de seguridad y ajustar los protocolos según las necesidades específicas del

entorno. Estos registros también son útiles para el análisis de patrones de riesgo, lo que contribuye a la prevención de futuros incidentes.

Los avances en tecnología han permitido que los centros de control se modernicen, integrando herramientas de inteligencia artificial y analítica de video que optimizan la vigilancia y el análisis de datos en tiempo real. Con estas tecnologías, es posible detectar automáticamente comportamientos sospechosos o patrones de riesgo, lo cual facilita la identificación temprana de amenazas y reduce la dependencia en la supervisión manual. Esta automatización no solo incrementa la eficiencia del centro de control, sino que también permite al personal concentrarse en decisiones estratégicas y respuestas tácticas, apoyándose en datos precisos y alertas inteligentes.

## 4.2. Analítica de video

La analítica de video es una tecnología avanzada que emplea algoritmos de inteligencia artificial para procesar y analizar imágenes capturadas por cámaras de seguridad en tiempo real. Esta herramienta permite detectar y evaluar actividades sospechosas, como movimientos inusuales, comportamiento agresivo o la presencia de objetos abandonados en áreas restringidas. La analítica de video facilita la gestión proactiva de la seguridad al identificar automáticamente patrones de riesgo, lo que permite a los operadores tomar decisiones rápidas y efectivas. Además, esta tecnología reduce la carga de trabajo en el monitoreo manual, permitiendo que el personal de seguridad se enfoque en incidentes de mayor relevancia.

Existen múltiples aplicaciones de la analítica de video en diversos sectores, desde el control de multitudes en eventos públicos hasta la detección de intrusos en áreas restringidas. En entornos urbanos, por ejemplo, se utiliza para mejorar la seguridad en el transporte público y en espacios concurridos, al identificar comportamientos que

podrían representar un riesgo para la ciudadanía. Asimismo, es de gran utilidad en infraestructuras críticas, como aeropuertos y estaciones de tren, donde permite la detección anticipada de posibles amenazas, minimizando los tiempos de respuesta ante incidentes.

La analítica de video también permite implementar tecnologías de reconocimiento facial y análisis de objetos, lo cual es particularmente útil en sistemas de control de acceso y en la vigilancia de áreas de alto riesgo. Estos sistemas identifican individuos previamente registrados en bases de datos de seguridad, lo que es fundamental para proteger instalaciones sensibles y detectar posibles infractores o personas de interés en investigaciones. Sin embargo, su uso debe cumplir con regulaciones de privacidad y protección de datos, ya que el reconocimiento facial puede involucrar la recopilación de información sensible.

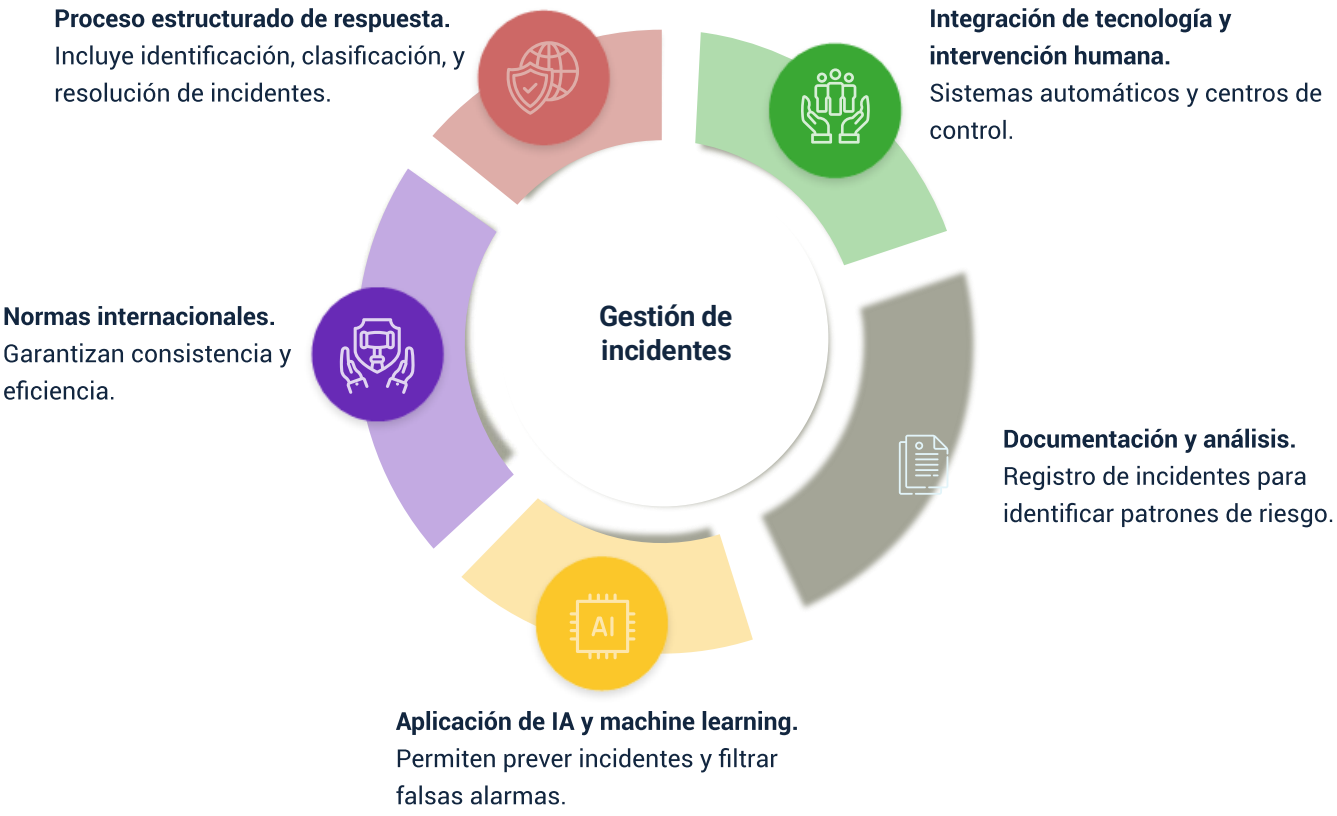
Los avances en inteligencia artificial y aprendizaje automático han mejorado significativamente la precisión y capacidad predictiva de los sistemas de analítica de video. Actualmente, estos sistemas pueden aprender a partir de patrones y comportamientos históricos, incrementando su efectividad con el tiempo. Estos desarrollos no solo aumentan la seguridad, sino que también permiten la recopilación de datos valiosos para mejorar la planificación y prevención en los sistemas de vigilancia. En este sentido, la analítica de video representa una herramienta indispensable para cualquier sistema de seguridad moderno que busque una gestión más eficiente y preventiva de los riesgos

## 4.3. Gestión de incidentes

La gestión de incidentes es un proceso estructurado que permite responder de manera eficaz a situaciones críticas, como emergencias de seguridad, fallos en los

sistemas, o desastres naturales. Este proceso incluye la identificación, clasificación, y resolución de incidentes, así como la implementación de acciones correctivas para evitar la recurrencia de problemas similares.

**Figura 2.** Gestión de incidentes




Fuente. OIT, 2024.

La gestión de incidentes es fundamental en el ámbito de la seguridad, ya que permite minimizar los daños, coordinar recursos, y optimizar la respuesta de los equipos encargados de proteger a las personas y bienes en una organización o territorio. Las etapas de gestión de incidentes son diseñadas según protocolos estandarizados que establecen procedimientos claros y precisos para cada tipo de amenaza.

En el contexto de la seguridad electrónica, la gestión de incidentes involucra tanto sistemas automáticos como la intervención humana. Los sistemas de monitoreo y analítica de video pueden detectar incidentes y activar alertas en tiempo real, facilitando una respuesta rápida. Los centros de control actúan como el núcleo de coordinación, donde los operadores reciben la información del incidente y despliegan los recursos necesarios. Esta capacidad de respuesta rápida es crucial para mitigar daños y proteger a los usuarios de un espacio determinado. Adicionalmente, la gestión de incidentes incluye la documentación de cada suceso, lo que permite realizar análisis posteriores para identificar patrones de riesgo y mejorar los protocolos de seguridad.

La tecnología ha avanzado en la gestión de incidentes mediante la integración de sistemas de inteligencia artificial y machine learning, los cuales permiten prever ciertos tipos de incidentes a través de la identificación de patrones en datos históricos. Estos sistemas predictivos facilitan la preparación ante posibles amenazas, y al automatizar algunas de las tareas de gestión, los equipos de seguridad pueden enfocarse en situaciones críticas que requieren intervención humana. Las aplicaciones de inteligencia artificial también permiten filtrar falsas alarmas y priorizar aquellos eventos que realmente suponen un riesgo, aumentando la efectividad de la respuesta ante incidentes.

Por otro lado, la gestión de incidentes está regulada por normas internacionales que definen las mejores prácticas para su implementación, como la ISO 22320, que proporciona directrices para la gestión de emergencias y seguridad pública. Estas normativas aseguran que los procedimientos de gestión de incidentes sean consistentes y eficientes, estableciendo un marco común que facilita la colaboración entre distintos

equipos de respuesta, tanto a nivel interno de una organización como en cooperación con servicios de emergencia externos.

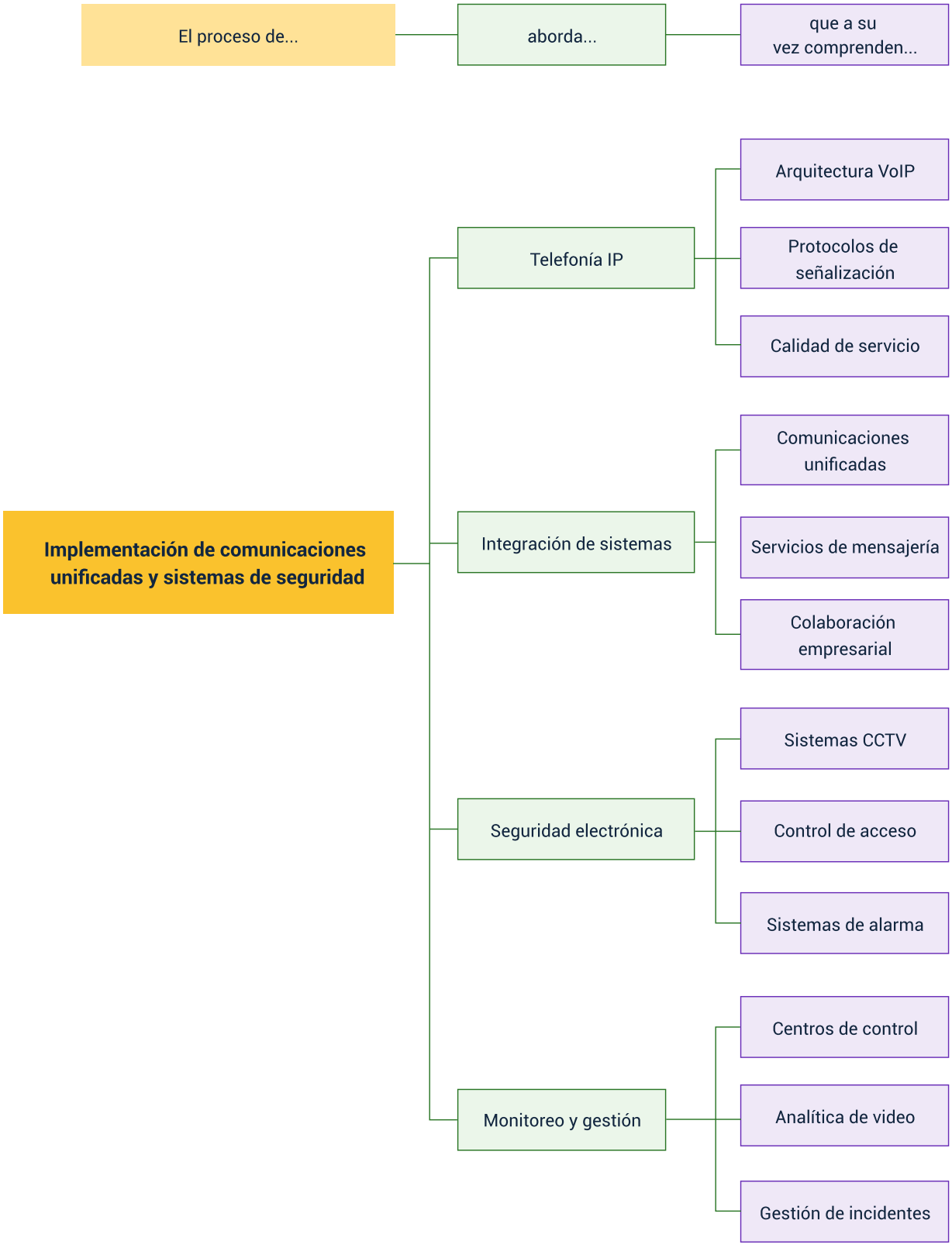
## Síntesis

El presente componente que trata sobre la implementación de comunicaciones unificadas y sistemas de seguridad abarca los fundamentos y aplicaciones de la tecnología de comunicación y los sistemas de seguridad en un entorno empresarial. Comienza con la telefonía IP, abordando los principios de Voice over IP (VoIP), los protocolos de señalización y la calidad de servicio, elementos esenciales para facilitar llamadas de voz claras y fiables a través de redes digitales. Esta base tecnológica es vital para la comunicación efectiva y el soporte de operaciones a distancia.

Asimismo, se exploran las comunicaciones unificadas y los sistemas de colaboración, que integran diversos medios de mensajería y trabajo colaborativo. Esta integración fomenta la eficiencia y conectividad dentro de las organizaciones, permitiendo una comunicación ágil y adaptada a las necesidades modernas de trabajo.

Adicionalmente, se examinan los dispositivos que permiten el intercambio de datos de manera inteligente y eficiente en la red, considerando no solo los componentes básicos, sino también aquellos que habilitan funcionalidades avanzadas, como la integración de sensores y controladores. Esta interconectividad resulta fundamental en el contexto del Internet de las Cosas (IoT), donde los dispositivos deben operar en conjunto para lograr una red funcional, autónoma y escalable, capaz de sostener múltiples usuarios y aplicaciones.

En conjunto, este componente proporciona una visión integral de las tecnologías y estrategias necesarias para mantener un ambiente seguro y eficiente en cualquier infraestructura de comunicaciones empresariales, optimizando tanto la colaboración como la protección organizacional.




Fuente. OIT, 2024.

## Material complementario

| Tema | Referencia | Tipo de material | Enlace del recurso |
|---|---|---|---|
| 1. Integración de sistemas | Cisco. (2011). Cisco simplifica y reduce los costos de su solución de comunicaciones unificadas para las empresas medianas. Blog Cisco Latinoamérica. Comunicaciones Unificadas | Blog Digital Web | https://gblogs.cisco.com/la/cisco-simplifica-reduce-los-costos-de-su-solucion-de-comunicaciones-unificadas-para-las-empresas-medianas/?form=MG0AV3 |
| 2. Monitoreo y gestión | Ecosistema de Recursos Educativos Digitales SENA. (2023, octubre 04). Monitoreo de seguridad web. | Video | https://www.youtube.com/watch?v=VusaSKjpYLg |
| 3. Seguridad electrónica | Ecosistema de Recursos Educativos Digitales SENA. (2022, marzo 11). Introducción a la Ciberseguridad, sus fundamentos y normativa. | Video | https://www.youtube.com/watch?v=3rqfPRqnKIM |
| 4. Seguridad electrónica | Ecosistema de Recursos Educativos Digitales SENA. (2023, febrero 01). Metodología y estrategias de la ciberseguridad | Video | https://www.youtube.com/watch?v=Dc7PGh5Aiss |
| 5. Gestión de incidentes | Ecosistema de Recursos Educativos Digitales SENA. (2023, diciembre 01). Monitoreo y respuesta de incidentes de seguridad digital | Video | https://www.youtube.com/watch?v=Gwu7EATxkZ0 |

## Glosario

**Analítica de video**: proceso de análisis de imágenes de video para detectar y comprender patrones o eventos específicos en tiempo real o diferido.

**Arquitectura VoIP**: estructura tecnológica que permite transmitir comunicaciones de voz a través de internet utilizando el protocolo IP, optimizando costos y recursos.

**Calidad de servicio (QoS)**: conjunto de técnicas y parámetros que garantizan el rendimiento adecuado de una red para la transmisión de datos críticos, como voz y video.

**CCTV (Circuito Cerrado de Televisión)**: sistema de cámaras de video instaladas para la vigilancia y monitoreo de espacios específicos, utilizado en seguridad electrónica.

**Centros de control**: instalaciones especializadas donde se monitorean y gestionan sistemas de seguridad y comunicaciones en tiempo real.

**Colaboración empresarial**: estrategias y herramientas que facilitan la comunicación y cooperación entre empleados, equipos y organizaciones para mejorar la productividad.

**Comunicaciones unificadas**: integración de múltiples herramientas de comunicación (mensajería, videollamadas, email, etc.) en una plataforma única para mejorar la eficiencia.

**Control de acceso**: mecanismos y tecnologías que regulan quién puede entrar o salir de un área física o acceder a información digital, basándose en permisos y autenticaciones.

**Documentación**: proceso de registro y organización de información relacionada con sistemas de seguridad y comunicaciones para referencia futura.

**Gestión de incidentes**: metodología de identificación, evaluación y resolución de incidentes de seguridad para minimizar riesgos y restablecer el servicio.

**Integración de sistemas**: proceso de conectar y unificar diferentes sistemas de comunicación para que funcionen de manera coordinada y eficiente.

**Mensajería**: servicio que permite el envío y recepción de mensajes en tiempo real, facilitando la comunicación rápida y efectiva en entornos corporativos.

**Monitoreo**: vigilancia constante de sistemas y redes para asegurar su correcto funcionamiento y prevenir o detectar problemas de seguridad.

**Protocolo de señalización**: normas que regulan el establecimiento, mantenimiento y finalización de conexiones en sistemas de comunicación, como SIP o H.323 en VoIP.

**Redes IP**: redes basadas en el Protocolo de Internet (IP), que permiten la transmisión de datos de manera eficiente y son la base para servicios como VoIP

**Seguridad electrónica**: conjunto de tecnologías y métodos utilizados para proteger sistemas e infraestructuras mediante equipos electrónicos como cámaras y sensores.

**Servicios de mensajería**: herramientas digitales que permiten el envío de mensajes entre usuarios de manera instantánea, contribuyendo a la comunicación en tiempo real.

**Sistemas de alarma**: dispositivos y sensores que detectan eventos no deseados, como intrusiones, y alertan a los responsables de seguridad.

**Telefonía IP**: tecnología que permite realizar llamadas de voz a través de redes IP, reduciendo costos y mejorando la flexibilidad en la comunicación.

**VoIP (Voice over IP)**: tecnología que permite la transmisión de voz sobre internet en lugar de líneas telefónicas convencionales, facilitando la telefonía IP.

## Referencias bibliográficas


Bosch Security and Safety Systems. (s.f.). Documentación técnica de Video Analytics. https://www.boschsecurity.com/xl/es/soluciones/sistemas-de-video/video-analytics/documentacion-tecnica-de-video-analytics/

Chao, H. C., & Lin, J. (2019). Quality of Service in VoIP and Unified Communications. Journal of Communications, 43(4), 257-266. https://www.fortinet.com/resources/cyberglossary/qos-quality-of-service

Eagle Eye Networks. (2021). GUÍA DE BUENAS PRÁCTICAS Manual de Videoseguridad. https://www.een.com/wp-content/uploads/2021/05/Video-Security-Primer-20210519_ES_compressed.pdf

García, M., & Fernández, L. (2018). Tecnologías de comunicaciones unificadas en entornos empresariales. Editorial Reverte. https://alphaenginyeria.com/la-importancia-de-las-comunicaciones-unificadas-en-el-entorno-empresarial

Kumar, R., & Rodrigues, J. J. P. C. (2010). Voice over IP Security: Vulnerabilities, Threats, and Countermeasures. In Security for Telecommunications Networks. Springer, 125-151.

Martínez, C., & Pérez, L. (2020). Centros de control y operaciones en sistemas de seguridad avanzada. Universidad de Alcalá. Repositorio Institucional de la Universidad de Alcalá

Microsoft. (2023). Messaging Services in Unified Communication Systems. https://learn.microsoft.com/en-us/microsoftteams/teams-security-guide

Nolasco-Mamani, M. A., Espinoza, S. A., & Choque-Salcedo, R. (2023). Innovación y Transformación Digital en el Empresa. Revista de Innovación Empresarial, 10(2), 123-145. https://www.researchgate.net/publication/376210760_Innovacion_y_Transformacion_Digital_en_el_Empresa

Organización Internacional de Normalización (ISO). (2013). ISO/IEC 27001:2013: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos.

Reinhold, S., & Peterson, L. (2020). Signaling Protocols in VoIP Communication Systems. Journal of Digital Communication Systems, 47(3), 134-150. https://www.researchgate.net/publication/221034718_Patterns_for_VoIP_Signaling_Protocol_Architectures

Sánchez, D. (2021). Analítica de video en la seguridad urbana: Implementación y resultados. Revista Científica de Tecnología y Seguridad Urbana. https://innovacionindustrial.net/ciudades-inteligentes/como-analitica-video-transformando-seguridad-ciudades-inteligentes/

Securitas España. (s.f.). Analítica de vídeo: lo que el ojo no ve. https://www.securitas.es/blog/analitica-de-video/

## Créditos

Elaborado por:


Organización Internacional del Trabajo