



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería Electrónica y Eléctrica

Escuela Profesional de Ingeniería Electrónica

Uso de cámaras terahertz en entidades financieras para la prevención de robos e intrusiones

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de Ingeniero Electrónico

AUTOR

Luis Angel QUITO CESPEDES

ASESOR

Mg. Wilfredo Baro FANOLA MERINO

Lima, Perú

2025



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Quito, L. (2025). *Uso de cámaras terahertz en entidades financieras para la prevención de robos e intrusiones*. [Trabajo de suficiencia profesional de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería Electrónica y Eléctrica, Escuela Profesional de Ingeniería Electrónica]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Luis Angel Quito Cespedes
Tipo de documento de identidad	DNI
Número de documento de identidad	72890337
URL de ORCID	No Aplica
Datos de asesor	
Nombres y apellidos	Wilfredo Baro Fanola Merino
Tipo de documento de identidad	DNI
Número de documento de identidad	06030740
URL de ORCID	https://orcid.org/0000-0003-0358-4702
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Celso Ysidro Gerónimo Huamán
Tipo de documento	DNI
Número de documento de identidad	09191500
Miembro del jurado 1	
Nombres y apellidos	Carlos Alberto Moreno Paredes
Tipo de documento	DNI
Número de documento de identidad	01292577
Miembro del jurado 2	
Nombres y apellidos	Jean Carlos Malca Fernández
Tipo de documento	DNI
Número de documento de identidad	45535181
Datos de investigación	
Línea de investigación	Sistemas de localización, Sistemas de telemetría y telecontrol, Sistemas de seguridad y videovigilancia.
Grupo de investigación	No Aplica

Agencia de financiamiento	No Aplica
Ubicación geográfica de la investigación	Edificio: Asociación de Bancos del Perú País: Perú Departamento: Lima Provincia: Lima Distrito: San Borja Calle: Morelli 499 Latitud: -12.093866949189007 Longitud: -77.00387570393362
Año o rango de años en que se realizó la investigación	Marzo 2022 - Mayo 2022
URL de disciplinas OCDE	Ingeniería eléctrica, Ingeniería electrónica: https://purl.org/pe-repo/ocde/ford#2.02.01 Ingeniería de sistemas y comunicaciones: https://purl.org/pe-repo/ocde/ford#2.02.04 Sistemas de automatización, Sistemas de control: https://purl.org/pe-repo/ocde/ford#2.02.03



UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
(Universidad del Perú, DECANA DE AMÉRICA)
FACULTAD DE INGENIERÍA ELECTRÓNICA Y ELÉCTRICA
Teléfono 619-7000 Anexo 4226
Calle Germán Amezaga 375 – Lima 1 – Perú



ACTA DE SUSTENTACIÓN
TRABAJO DE
SUFICIENCIA PROFESIONAL
ACTA N°04/FIEE-PPP/2026

Los suscritos Miembros del Jurado, docentes permanentes de las Escuelas Profesionales de la Facultad de Ingeniería Electrónica y Eléctrica, reunidos en la fecha 15 de enero del 2026, como presidente de Jurado el **DR. CELSO YSIDRO GERÓNIMO HUAMÁN**, integrado por el Miembro de Jurado el **DR. CARLOS ALBERTO MORENO PAREDES**, el Miembro de Jurado el **MG. JEAN CARLOS MALCA FERNÁNDEZ** y Miembro Asesor el **MG. WILFREDO BARO FANOLA MERINO**.

Después de escuchar la Sustentación Presencial del Trabajo de Suficiencia Profesional del Bachiller **LUIS ANGEL QUITO CESPEDES** con código 15190169 que para optar el Título Profesional de Ingeniero Electrónico sustentó el Trabajo de Suficiencia Profesional titulado **USO DE CÁMARAS TERAHERTZ EN ENTIDADES FINANCIERAS PARA LA PREVENCIÓN DE ROBOS E INTRUSIONES**.

El jurado examinador procedió a formular las preguntas reglamentarias y, luego de una deliberación en privado, decidió otorgarle el calificativo de 15 (QUINCE).

Ciudad Universitaria, 15 de enero del 2026

DR. CELSO YSIDRO GERÓNIMO HUAMÁN
Presidente Jurado

DR. CARLOS ALBERTO MORENO PAREDES
Miembro Jurado

MG. JEAN CARLOS MALCA FERNÁNDEZ
Miembro Jurado

MG. WILFREDO BARO FANOLA MERINO
Miembro Asesor



UNIVERSIDAD NACIONAL MAYOR DE
SAN MARCOS
Universidad del Perú, Decana de América

CERTIFICADO DE SIMILITUD

Yo, **WILFREDO BARO FANOLA MERINO** en mi condición de asesor acreditado con el Dictamen N°01/FIEE-PPP/2026 del Trabajo de Suficiencia Profesional titulado **USO DE CÁMARAS TERAHERTZ EN ENTIDADES FINANCIERAS PARA LA PREVENCIÓN DE ROBOS E INTRUSIONES**, presentado por el bachiller LUIS ANGEL QUITO CESPEDES, para optar al título profesional de Ingeniero Electrónico. CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante la plataforma PIDS, el documento evaluado cuenta con el 10% de similitud, nivel PERMITIDO para continuar con los trámites correspondientes y para su publicación en el repositorio institucional.

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del título de Ingeniero Electrónico.

Lima, 15 de Enero del 2026



Firma del Asesor

DNI: 06030740

Nombres y apellidos del asesor:
WILFREDO BARO FANOLA MERINO

DEDICATORIA

Este trabajo está dedicado en especial a mis padres y mis hermanos que son mi soporte para seguir adelante, y al ingeniero Wilfredo Fanola Merino, docente FIEE por su paciencia y los consejos para cumplir satisfactoriamente la sustentación.

AGRADECIMIENTOS

Un agradecimiento especial a Jorge, Elias, Marcela, Leonardo, Martin y a mi equipo técnico por el apoyo en mi crecimiento profesional.

RESUMEN

Actualmente, la inseguridad se ha convertido en uno de los problemas que más afecta y preocupa a la ciudadanía ya que refleja el deseo por un entorno más seguro donde puedan vivir y desarrollarse sin temor. En este contexto la implementación de un sistema de Seguridad Electrónica es una alternativa para la reducción de pérdidas de bienes en diversos ámbitos. Principalmente en la parte de la prevención, es decir, los sistemas de seguridad electrónica deben ser del tipo preventivo.

La Asociación de Bancos del Perú (ASBANC) ofrece el servicio de seguridad electrónica, por lo que se le solicitó diseñar e implementar un Sistema Integral de Seguridad Electrónica para una entidad financiera en la ciudad de Lima.

El modelo propuesto no solo incluirá tecnologías tradicionales como alarmas y cámaras de videovigilancia, sino que también incorporará el uso de cámaras Terahertz. Estas cámaras, mediante la detección de ondas en el orden de los terahercios, permiten identificar objetos ocultos bajo la ropa, como armas u otros elementos peligrosos, sin contacto físico ni invasión de la privacidad, contribuyendo significativamente a la prevención de asaltos y robos dentro y fuera de las instalaciones financieras.

Palabras clave: Seguridad Electrónica, Terahertz, ASBANC, Alarmas, Inseguridad.

ABSTRACT

Currently, insecurity has become one of the problems that most affects and concerns citizens, as it reflects the desire for a safer environment where they can live and develop without fear. In this context, the implementation of an Electronic Security system is an alternative for reducing property losses in various areas.

The Association of Banks of Peru (ASBANC) offers electronic security services and was therefore asked to design and implement a Comprehensive Electronic Security System for a financial institution in the city of Lima.

The proposed model will not only include traditional technologies such as alarms and video surveillance cameras, but will also incorporate the use of Terahertz cameras. These cameras, by detecting terahertz waves, make it possible to identify objects hidden under clothing, such as weapons or other dangerous items, without physical contact or invasion of privacy, significantly contributing to the prevention of assaults and robberies within financial facilities.

Keywords: Electronic Security, Terahertz, ASBANC, Alarms, Insecurity.

INDICE GENERAL

RESUMEN.....	iv
ABSTRACT.....	v
INDICE GENERAL.....	vi
LISTA DE FIGURAS.....	viii
LISTA DE TABLAS.....	ix
CAPITULO I: INTRODUCCIÓN.....	11
CAPITULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ	
LA ACTIVIDAD.....	13
2.1 Institución – Actividad que desarrolla.....	13
2.2 Periodo de duración de la actividad.....	13
2.3 Finalidad y objetivos de la entidad.....	13
2.4 Razón social.....	13
2.5 Dirección postal.....	13
2.6 Correo electrónico del profesional a cargo.....	13
CAPITULO III: DESCRIPCIÓN DE LA ACTIVIDAD.....	14
3.1 Organización de la actividad.....	14
3.2 Finalidad y objetivos de la Actividad.....	14
3.2.1 Finalidad.....	14
3.2.2 Objetivo General.....	15
3.2.3 Objetivos Específicos.....	15
3.3 Problemática.....	15
3.3.1 Problema General.....	17
3.3.2 Problemas Específicos.....	17
3.3.3 Justificación e importancia de la investigación.....	17

3.4	Metodología.....	17
3.4.1	Bases teóricas.....	18
3.4.1.1	Tecnologías de Gigahercios y Terahercios para comunicaciones de banda ancha.....	18
3.4.1.2	Avances en tecnologías de fuentes de Terahercios.....	18
3.4.1.3	Detección y comunicación en terahercios para redes inteligentes conectadas del futuro.....	19
3.4.1.4	Ciencia y tecnología de terahercios en astronomía, telecomunicaciones y biofísica.....	20
3.4.2	Marco conceptual.....	21
3.4.2.1	Sistema de videovigilancia CCTV.....	21
3.4.2.1.1	Sistema CCTV analógico.....	22
3.4.2.1.2	Sistema CCTV IP.....	22
3.4.2.1.3	Comparativa entre los tipos de sistemas CCTV.....	23
3.4.2.2	Cámaras Terahertz.....	24
3.4.2.2.1	Fuente emisora de ondas Terahertz.....	25
3.4.2.2.2	Antenas o lentes colimadoras.....	25
3.4.2.2.3	Sensor o Detectores.....	26
3.4.2.2.4	Procesamiento de datos.....	27
3.4.2.2.4.1	Rasterización convencional (Raster Scan).....	28
3.4.2.2.4.2	Transformada Híbrida Inversa (Hybrid Inverse Transform).....	28
3.4.2.3	Middleware.....	31
3.4.2.4	VMS (Video Management System).....	33
3.4.2.5	Ley de Protección de Datos Personales.....	35
3.4.2.6	Reglamento de medidas mínimas de Seguridad para las Entidades del Sistema Financiero.....	36
3.5	Procedimiento.....	36
3.5.1	Capa de Adquisición.....	36
3.5.2	Middleware.....	39
3.5.3	VMS.....	40
3.5.4	Interfaz de Usuario.....	41
3.5.5	Analítica.....	41
3.5.6	Almacenamiento.....	42
3.6	Resultado de la actividad.....	42

CAPITULO IV: DISCUSION DE RESULTADOS.....	45
4.1 Descripción de la implementación.....	45
CAPITULO V: CONCLUSIONES.....	46
CAPITULO VI: RECOMENDACIONES.....	47
CAPITULO VII: BIBLIOGRAFIA.....	48

LISTA DE FIGURAS

Figura 1 Organigrama del área de Tecnología de la información.....	4
Figura 2 Ubicación de las ondas Terahertz en el espacio electromagnético.	15
Figura 3 Diagrama de bloques de una antena THz, fuente y detector.....	17
Figura 4 Esquema de adquisición y reconstrucción de imágenes mediante Escaneo Raster y Reconstrucción Híbrida.....	19
Figura 5 Reconstrucción de imagen de un recorte de hoja de arce en una placa metálica.....	20
Figura 6 Diagrama de bloques para el sistema de cámaras Terahertz integrado.....	22
Figura 7 Diagrama de bloques Sistema Terahertz.....	27
Figura 8 Plano modelo de CCTV en una entidad financiera.....	28
Figura 9 Ubicación en el plano de cámara Terahertz en el ambiente de cajero.....	29
Figura 10 Ubicación en el plano de cámara Terahertz en el ingreso de agencia.....	29
Figura 11 Detección de arma oculta con cámara de Terahertz.....	33
Figura 12 Cotización de servicio de instalación de cámaras Terahertz.....	34
Figura 13 Cotización de servicio de instalación y configuración de servidor VMS para cámaras Terahertz.....	34
Figura 14 Cotización de licencia para cámara Terahertz.....	35

LISTA DE TABLAS

Tabla 1 Denuncias por Comisión de delitos ordenado por delito genérico desde el año 2018 hasta el año 2023.....	6
Tabla 2 Ventajas y desventajas de cámaras análogas.....	12
Tabla 3 Ventajas y desventajas de cámaras IP.....	13
Tabla 4. Comparación de un sistema CCTV analógico vs Sistema CCTV IP.....	14
Tabla 5 Características de los tipos de detectores THz y sus características.....	16
Tabla 6 Características de fuente Terahertz Tipo II.....	30

CAPITULO I: INTRODUCCIÓN

El presente trabajo detallará el uso de cámaras Terahertz en entidades financieras para la detección de objetos y prevención de robos, asaltos e intrusiones. Esta tecnología, basada en ondas electromagnéticas de Terahercios, permite detectar objetos ocultos bajo la ropa, como armas o herramientas metálicas, sin necesidad de contacto físico ni invasión de la privacidad, lo que la convierte en una solución eficaz para reforzar los protocolos de seguridad en espacios bancarios y financieros.

La seguridad electrónica se ha convertido en una necesidad imperante en un mundo cada vez más interconectado y vulnerable a diversas amenazas. Entre los aspectos más relevantes de esta rama de la seguridad se encuentran los sistemas de alarmas contra intrusión, los sistemas de detección de incendios y las cámaras de vigilancia (CCTV), los cuales desempeñan un papel crucial en la protección de personas, propiedades e información.

El uso de cámaras de vigilancia (CCTV) proporciona una herramienta poderosa para la monitorización continua de espacios, permitiendo no solo la disuasión de actividades delictivas, sino también la recopilación de evidencia en caso de incidentes. La integración de tecnología avanzada, como la analítica de video, el reconocimiento facial y, más recientemente, las cámaras Terahertz, ha elevado la eficacia de estos sistemas. En el contexto financiero, estas cámaras pueden instalarse en puntos estratégicos como accesos principales y áreas de espera, detectando objetos peligrosos o sospechosos antes de que se cometa un delito.

Este trabajo de suficiencia se enfocará en el diseño de un sistema de videovigilancia en una agencia modelo y el uso de las cámaras Terahertz como apoyo para reforzar la seguridad, evaluando su funcionamiento, eficacia y las mejores prácticas para su implementación en el entorno de las entidades financieras.

El documento inicia con la introducción, que presenta el propósito y los objetivos de la actividad realizada. En el capítulo 2, Información del lugar donde se desarrolló la actividad, se describe el contexto geográfico, social o cultural en el que tuvo lugar. En el capítulo 3, Descripción de la actividad, se detallan los procedimientos, metodologías y pasos seguidos durante el desarrollo del proyecto. El capítulo 4, Discusión de los resultados, analiza los hallazgos obtenidos, interpretándolos y comparándolos con expectativas previas o investigaciones relacionadas. En el capítulo 5 se presentan las conclusiones donde se resumen los puntos más importantes, destacando los logros o desafíos. El capítulo 6, recomendaciones, sugiere acciones o cambios basados en los resultados obtenidos. Finalmente, en el capítulo 7 se presentan las referencias, que incluyen las fuentes de información utilizadas.

CAPITULO II: INFORMACIÓN DEL LUGAR DONDE SE DESARROLLÓ LA ACTIVIDAD

2.1 Institución – Actividad que desarrolla: Asociación de Bancos del Perú – Asistente de implementaciones de seguridad electrónica

2.2 Periodo de duración de la actividad: 3 meses

2.3 Finalidad y objetivos de la entidad: Promover el fortalecimiento del sistema financiero privado, proporcionando a sus asociados múltiples servicios.

2.4 Razón social: ASOCIACIÓN DE BANCOS DEL PERÚ

2.5 Dirección postal: 15036

2.6 Nombre y correo electrónico del profesional a cargo.

Nombres y apellidos: Jorge Alfredo Matias Mesias

Correo: jmatias@asbanc.com.pe

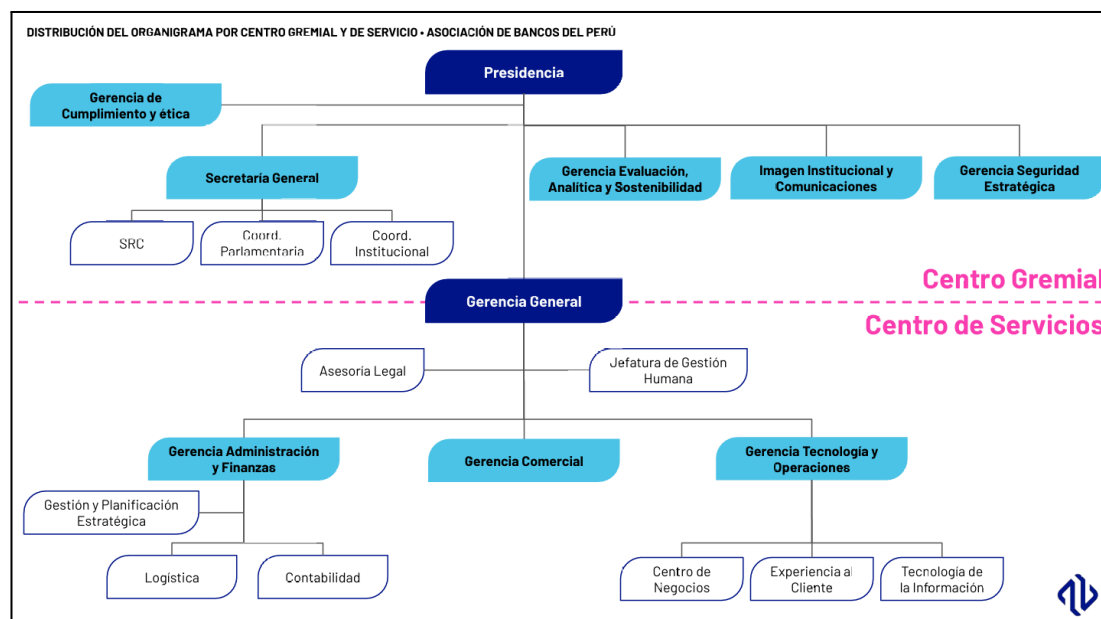
CAPITULO III: DESCRIPCIÓN DE LA ACTIVIDAD

3.1 Organización de la actividad

En la figura 1 se muestra el organigrama del área de Tecnología de la Información de ASBANC.

Figura 1.

Organigrama del área de Tecnología de la información.



3.2 Finalidad y objetivos de la Actividad

3.2.1 Finalidad

Reforzar el sistema CCTV de la agencia bancaria mediante el uso de cámara Terahertz.

3.2.2 *Objetivo General*

Usar cámaras Terahertz en entidades financieras para la detección y prevención de robos e intrusiones.

3.2.3 *Objetivos específicos*

Diseñar una propuesta de sistema de seguridad para entidades financieras incluyendo las cámaras Terahertz.

Analizar los beneficios y riesgos del uso de las cámaras Terahertz en entidades financieras.

3.3 Problemática

Hoy en día una de las principales preocupaciones que se tiene es la inseguridad ya que pueden poner en riesgo los bienes materiales y en el peor de los casos, la vida de las personas.

Los bancos son entidades encargadas de administrar el dinero de las personas, Paredes (2017) señala que esto es bajo la premisa de que guardar los bienes económicos en una entidad financiera es más seguro que tenerlos en casa, al tratarse de entidades que tienen a su cuidado cifras descomunales de dinero, las instituciones bancarias son sumamente susceptibles de sufrir todo tipo de ataques delictivos. Es por esto que están en la necesidad de implementar sistemas de seguridad que garanticen la protección de este tipo de infraestructuras.

Las instituciones están en la necesidad de contar con soluciones que permitan la prevención de riesgos y poder reaccionar a incidentes delictivos mediante tecnología y procesos diseñados de acuerdo con características y necesidades específicas de cada institución.

En Chaverra (2020) se menciona que la protección de las entidades financieras está inmersa tanto en tecnologías de seguridad (software y hardware) como en políticas y procedimientos internos, además que dichas medidas deben estar sujetas a criterios como los riesgos a los

que está expuesta la entidad bancaria, la ubicación geográfica y comercial, etc.

En el Perú, según datos de las denuncias por comisión de delitos (MININTER – SIDPOL), el 66,45 % de delitos registrados en el año 2023 son delitos contra el patrimonio, siendo que las intrusiones al sistema financiero se encuentran en este tipo de delitos por lo que no se debe tomar a la ligera ya que representan más del 50% del total de delitos registrados en el 2023. (Tabla 1)

Tabla 1

Denuncias por Comisión de delitos ordenado por delito genérico desde el año 2018 hasta el año 2023.

Delito Genérico	2018	2019	2020	2021	2022	2023
Total	466 088	446 508	320 819	403 071	497 581	570 890
Delitos contra la vida, el cuerpo y la salud	49 577	44 983	33 927	39 302	45 141	79 046
Delitos contra el honor	243	312	301	258	252	203
Delitos contra la familia	4 562	4 459	3 950	4 857	4 418	3 135
Delitos contra la libertad	29 079	35 259	32 073	36 336	37 718	34 134
Delitos contra el patrimonio	315 542	296 760	189 656	247 672	316 728	379 357
Delitos contra la confianza y la buena fe en los negocios	53	41	28	64	58	132
Delitos contra los derechos intelectuales	112	129	146	220	405	238
Delitos contra el patrimonio cultural	93	71	78	110	62	113
Delitos contra el orden económico	42	22	45	34	44	116
Delitos contra el orden financiero y monetario	737	574	443	504	560	379
Delitos tributarios	216	153	188	293	355	318
Delitos contra la seguridad pública	53 595	46 305	37 673	51 935	68 275	57 368
Delitos ambientales	400	473	564	660	717	453
Delitos contra la tranquilidad pública	572	308	341	318	442	378
Delitos contra la humanidad	2 276	3 072	459	247	305	373

Delitos contra el estado y la defensa nacional	3	6	38	34	30	13
Delitos contra los poderes del estado y el orden constitucional	6	5	5	1	3	7
Delitos contra la voluntad popular	240	117	156	440	653	83
Delitos contra la administración pública	7 202	11 785	18 784	15 772	14 586	10 703
Delitos contra la fe pública	1 538	1 674	1 964	4 014	6 829	4 341

Nota: Datos tomados de MININTER (2023).

3.3.1 *Problema General*

¿Cómo usar cámaras Terahertz en entidades financieras para la detección y prevención de robos e intrusiones?

3.3.2 *Problemas Específicos*

¿Cómo diseñar una propuesta de sistema de seguridad para entidades financieras incluyendo las cámaras Terahertz?

¿Cuáles son los beneficios y riesgos del uso de las cámaras Terahertz en entidades financieras?

3.3.3 *Justificación e importancia de la investigación*

Con la experiencia adquirida como trabajador de ASBANC (Institución gremial bancaria más representativa del medio) en el área de seguridad electrónica se pretende transmitir el conocimiento adquirido a las personas interesadas (técnicos, profesionales e investigadores) en saber más sobre los sistemas de seguridad electrónica bancaria, es por esto que describiremos el proceso de diseño e instalación de sistemas integrales de seguridad electrónica en agencias bancarias para que otras personas tengan conocimiento de estos.

3.4 Metodología

La metodología es de tipo aplicada y descriptiva, esto es porque se

busca proponer una solución tecnológica basada en el uso de cámaras Terahertz para la prevención de robos e intrusiones en entidades financieras.

Además, se adopta un enfoque mixto ya que se busca analizar datos de tipo cualitativo y cuantitativo ya que se buscará analizar datos relacionados con la seguridad en entidades financieras, así como comprender percepciones y conceptos operativos.

3.4.1 Bases teóricas

3.4.1.1 Tecnologías de Gigahercios y Terahercios para comunicaciones de banda ancha

Edwards (2018) describe el rol que desempeñan las frecuencias de terahercios (THz) en la evolución de las tecnologías de comunicación, especialmente en el contexto del aumento exponencial en la demanda de ancho de banda. Los terahercios, que se sitúan por encima de las bandas de microondas y ondas milimétricas tradicionales, representan una solución clave para futuras redes como el 6G, permitiendo tasas de transmisión de datos ultraaltas en distancias cortas, ideales para entornos densamente urbanizados, dispositivos móviles de nueva generación y comunicaciones de baja latencia. El autor explica que las investigaciones en sub-THz, en torno a frecuencias de cientos de gigahercios, están siendo lideradas por empresas como Keysight Technologies y Rohde & Schwarz, que desarrollan equipos de prueba y soluciones de radiofrecuencia adaptadas a esta banda emergente. A pesar de los retos técnicos como la atenuación atmosférica y las limitaciones en componentes activos, el texto muestra que la tecnología THz es clave para superar el límite de Shannon en comunicaciones y habilitar nuevas arquitecturas como superficies inteligentes reconfigurables y enlaces de alta capacidad en sistemas terrestres, satelitales y estratosféricos.

3.4.1.2 Avances en tecnologías de fuentes de Terahercios

Park, Tani, Rieh y Park (2024) plasmaron su trabajo en un libro que

presenta información detallada sobre el desarrollo de tecnologías para la generación de ondas terahertz (THz), haciendo especial énfasis en sus aplicaciones en detección e imagen. Se describe cómo distintas fuentes THz, como antenas fotoconductoras, emisores espintrónicos, generadores paramétricos ópticos y osciladores electrónicos, permiten obtener radiación coherente en este rango espectral, útil para realizar espectroscopía, escaneo e imágenes no invasivas. En particular, se destacan sistemas como los generadores paramétricos de inyección semilla (is-TPG), capaces de producir ondas THz de múltiples longitudes de onda en un solo pulso, lo que permite realizar espectroscopía en tiempo real. Estas fuentes se han utilizado para identificar sustancias orgánicas como azúcares (maltosa, glucosa, lactosa) a través de imágenes espectroscópicas multibanda, incluso dentro de sobres cerrados, demostrando su utilidad para inspección de paquetes y control de calidad. Asimismo, se describe la generación de imágenes por transmisión THz usando osciladores paramétricos de onda hacia atrás (BW-TPO), los cuales permiten obtener imágenes de objetos ocultos (como tijeras dentro de un bolso) gracias a la buena penetración de las ondas THz en materiales dieléctricos. Estas capacidades hacen del espectro THz una herramienta prometedora en áreas como seguridad, medicina, control industrial y ciencia de materiales, debido a su habilidad para revelar estructuras internas sin dañar los objetos ni utilizar radiación ionizante.

3.4.1.3 Detección y comunicación en terahercios para redes inteligentes conectadas del futuro

Wang, Gu, Li, Yu, Li, Liu, Zeng, He, Chen, Lu, Tong, Wessel (2022) presentan un análisis profundo del potencial de las ondas terahercios (THz) para habilitar redes 6G avanzadas, con un enfoque especial en aplicaciones de comunicación y detección integradas. Las tecnologías THz, gracias a su ancho de banda ultraamplio (0.1–10 THz), permiten transmisiones de datos a velocidades de terabits por segundo (Tbit/s)

y habilitan capacidades de detección de alta resolución comparables a las técnicas ópticas, con imágenes en el rango de 100 micrómetros. Este espectro puede penetrar materiales como papel, plásticos o cerámicas, lo que lo hace ideal para aplicaciones de imagen no destructiva, escaneo de seguridad y reconocimiento de materiales. Se discuten ejemplos como la detección de objetos ocultos (como cuchillos en ropa) mediante imágenes THz, sin uso de radiación ionizante. Se presenta una arquitectura híbrida de modelado de canales para abordar los retos únicos del espectro THz en comunicación y detección, y se detallan experimentos de medición en entornos reales con frecuencias de hasta 280 GHz. El documento también revisa tecnologías clave como antenas THz, superficies inteligentes reconfigurables (RIS), integración CMOS/III-V, y sensores directos usados en cámaras THz de matriz focal. En conjunto, el trabajo posiciona las ondas THz como una tecnología crítica para sistemas 6G, no solo por su capacidad de conexión ultra-rápida, sino también por su rol central en servicios emergentes de imagen, posicionamiento, mapeo, y percepción ambiental precisa, todo desde una única plataforma de comunicación-sensorial.

3.4.1.4 Ciencia y tecnología de terahercios en astronomía, telecomunicaciones y biofísica

Deng, Li, Hu, Miao, Lin, Jiang y Shi (2025) ofrecen con este artículo una visión integradora sobre los avances en la tecnología de terahercios (THz) aplicada en tres áreas clave: astronomía, telecomunicaciones y biofísica. En astronomía, se destacan detectores sensibles como mezcladores SIS, sensores HEB, detectores TES y KIDs que permiten observar el universo en el rango submilimétrico con alta resolución. En el ámbito de las telecomunicaciones, se revisan desarrollos en fuentes de estado sólido para comunicación THz, nuevas técnicas de modulación y sistemas transmisores que aprovechan el ancho de banda ultraamplio del espectro THz, encaminados hacia redes como 6G. Finalmente, en

biofísica, se discuten los efectos físicos no térmicos de las ondas THz sobre organismos y moléculas, evidenciando su potencial en aplicaciones biomédicas sensibles y no invasivas. El paper concluye analizando los desafíos (como la atenuación, integración de dispositivos y sensibilidad de detección) y las perspectivas futuras que sitúan la tecnología terahertz como un pilar en investigación astronómica, comunicaciones ultrarrápidas y detección avanzada en ciencias de la vida.

3.4.2 Marco conceptual

3.4.2.1 Sistema de videovigilancia CCTV

Un sistema de videovigilancia basado en circuito cerrado de televisión (CCTV) es una tecnología ampliamente utilizada en el ámbito de la seguridad electrónica para la supervisión continua de espacios físicos. Este sistema está conformado por un conjunto de cámaras conectadas a monitores o dispositivos de grabación, que permiten observar en tiempo real o revisar imágenes almacenadas. Los sistemas CCTV pueden ser análogos o digitales, y con frecuencia se integran con tecnologías de análisis de video, detección de movimiento o reconocimiento facial.

Su implementación se justifica en entornos que requieren vigilancia permanente, como entidades financieras, comercios, instalaciones gubernamentales y espacios públicos. Los objetivos principales de un CCTV son la prevención de incidentes delictivos, la disuasión de conductas ilícitas, y la recolección de evidencia ante posibles eventos. La evolución del CCTV hacia plataformas inteligentes ha permitido una mayor eficiencia en la gestión de riesgos y en la automatización de alertas de seguridad. No obstante, su uso plantea desafíos relacionados con la privacidad, la protección de datos personales y el cumplimiento de la normativa legal vigente.

3.4.2.1.1 Sistema CCTV analógico

El sistema analógico es el tipo más tradicional de videovigilancia y ha sido ampliamente utilizado en bancos, instituciones y espacios públicos desde finales del siglo XX. En este tipo de sistema, las cámaras capturan imágenes en formato analógico y las transmiten a través de cable coaxial a un grabador digital (DVR), donde se almacenan y visualizan.

Las principales ventajas del sistema analógico son su costo reducido, su instalación sencilla y la compatibilidad con equipos más antiguos. Sin embargo, también presenta limitaciones importantes: resolución de imagen baja, menor capacidad de integración con sistemas modernos y escasas funciones inteligentes. Además, su capacidad de acceso remoto es limitada y su escalabilidad resulta más compleja frente a nuevas necesidades.

A continuación, se muestran las ventajas y desventajas de las cámaras de tipo analógicas:

Tabla 2

Ventajas y desventajas de cámaras análogas

Ventajas	Desventajas
Coste inicial más bajo	Menor resolución de imagen
Tecnología madura y ampliamente compatible	Requiere cables coaxiales y alimentación separada
Fácil de instalar en sistemas antiguos	Limitada capacidad de integración con software inteligente
Baja latencia en transmisión	Dificultad para acceder remotamente sin hardware adicional
Menor consumo de ancho de banda	No soporta funciones avanzadas (detección de movimiento, análisis de video)

3.4.2.1.2 Sistema CCTV IP

El sistema IP, también conocido como digital o en red, transmite las imágenes en formato digital utilizando redes de datos (LAN o Internet). En este caso, las cámaras IP capturan imágenes y las envían directamente a un grabador de video en red (NVR) o a la nube, lo que permite almacenamiento remoto, acceso desde múltiples dispositivos y procesamiento avanzado del video.

Entre sus principales ventajas se encuentran la alta calidad de imagen (HD o superior), la flexibilidad en la instalación, la posibilidad de alimentación a través de Ethernet (PoE), y la integración con sistemas de análisis inteligente, como reconocimiento facial, conteo de personas, análisis de movimiento y alertas automatizadas.

Si bien el costo inicial de los sistemas IP puede ser mayor, su eficiencia operativa, escalabilidad y funcionalidades avanzadas los han convertido en la opción preferida en instalaciones modernas, especialmente en entornos de alta seguridad como entidades financieras.

A continuación, se muestran las ventajas y desventajas de las cámaras de tipo IP:

Tabla 3

Ventajas y desventajas de cámaras IP

Ventajas	Desventajas
Alta resolución de imagen (HD, 4K, etc.)	Coste más elevado (cámara y configuración inicial)
Acceso remoto desde cualquier lugar vía red	Puede requerir configuración de red y conocimientos técnicos
Facilidad para integrar analítica avanzada (IA, detección facial, etc.)	Mayor demanda de ancho de banda y almacenamiento

Alimentación por PoE (Power over Ethernet) posible	Dependencia de la red: si la red falla, la cámara puede quedar inactiva
Escalabilidad sencilla en sistemas grandes	Mayor vulnerabilidad a ciberataques si no se configura correctamente

3.4.2.1.3 Comparativa entre los tipos de sistemas CCTV

A continuación, se presenta una comparativa entre los 2 tipos de sistemas (CCTV analógico e IP).

Tabla 4

Comparación de un sistema CCTV analógico vs Sistema CCTV IP.

Característica	Sistema CCTV Analógico	Sistema CCTV IP
Calidad de imagen	Media (hasta 720p)	Alta (Full HD, 4K o más)
Transmisión	Cable coaxial	Red de datos (Ethernet)
Acceso remoto	Limitado	Total (desde cualquier dispositivo)
Escalabilidad	Baja	Alta
Costo inicial	Bajo	Medio a alto
Mantenimiento	Moderado	Bajo a medio

3.4.2.2 Cámaras Terahertz

Las ondas THz cubren un rango de frecuencias de aproximadamente 0.1 a 10 THz y poseen propiedades únicas que las distinguen tanto de las microondas como de las ondas ópticas.

Gracias a su longitud de onda relativamente corta, las ondas THz ofrecen resoluciones de imagen cercanas a los 100 micrómetros, comparables con técnicas ópticas pero sin necesidad de radiación ionizante como los rayos X.

Son no ionizantes, lo que las hace seguras para aplicaciones biomédicas y de seguridad. Además, pueden penetrar materiales opacos como papel, ropa, plástico, madera, cerámica y algunos materiales compuestos, permitiendo visualizar estructuras internas sin dañar los objetos.

Estas características la convierten en una herramienta poderosa para el análisis de objetos ocultos o sellados.

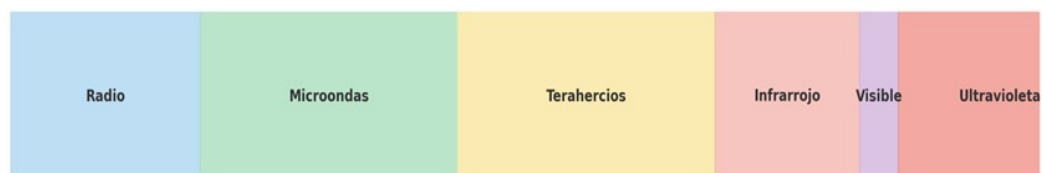
El funcionamiento de un sistema de detección que utiliza Ondas Terahertz se compone de lo siguiente:

3.4.2.2.1 Fuente emisora de ondas Terahertz

Dispositivo que genera radiación electromagnética con frecuencias entre 0,1 y 10 THz, estos se pueden obtener mediante rectificación óptica, multiplicación de frecuencia o generación electrónica directa. Hay que tener en cuenta que los generadores en la banda de Terahertz son de potencias débiles, por lo general la potencia pico alcanzada es muy baja en comparación a otras fuentes generadoras en otras partes del espectro radioeléctrico.

Figura 2

Ubicación de las ondas Terahertz en el espectro electromagnético.



En Figueroa (2018), se menciona un detalle importante, se menciona que las fuentes que puedan generar energía en la frecuencia de los THz son pocos eficientes debido a pérdidas por calentamiento principalmente.

Por ejemplo, los QCL (Quantum Cascade Láser) pueden emitir ondas en Terahertz pero requieren refrigeración criogénica para evitar la pérdida total de la potencia.

3.4.2.2.2 Antenas o lentes colimadoras

Dispositivo que nos servirá para dirigir el haz de Terahertz hacia el objetivo.

Estas antenas tienen limitaciones:

- Longitudes de onda cortas: Las frecuencias de THz tienen longitudes de onda entre 3mm y 30 μm , a estas escalas estas antenas deben ser micro/nano estructuradas.
- Eficiencia de radiación: La radiación con materiales comunes se vuelve ineficiente a estas frecuencias, por lo general, los materiales metálicos presentan pérdidas resistivas altas en el rango de los THz.
- Acoplamiento crítico: El acoplamiento entre la antena y el dispositivo activo (fotoconductor, QCL o diodo Schottky) es crítico y difícil de optimizar.

3.4.2.2.3 Sensor o Detectores

Dispositivo que mide las variaciones de las ondas reflejadas o transmitidas.

En este rango de frecuencias se presentan algunas dificultades:

- Débil señal de potencia.
- Respuesta lenta en algunos tipos.

A continuación, se presenta una tabla de algunos tipos de detectores y sus características:

Tabla 5

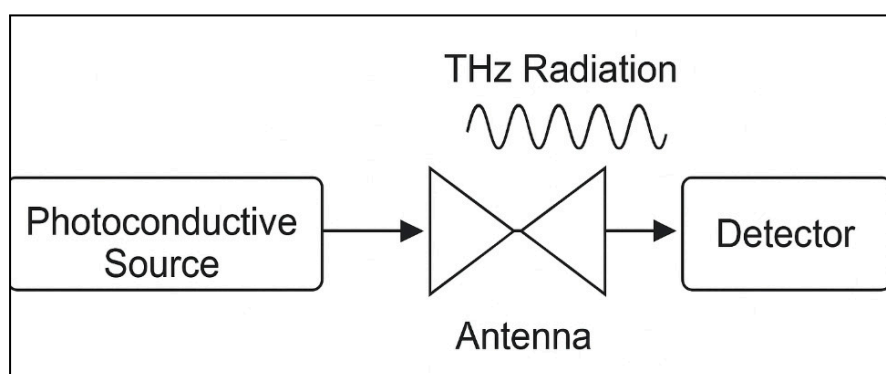
Características de los tipos de detectores THz y sus características.

Tipo de detector	Principio de funcionamiento	Ventajas	Limitaciones
Bolómetro	Cambios de temperatura por absorción	Muy sensible	Respuesta lenta, criogénico

Tipo de detector	Principio de funcionamiento	Ventajas	Limitaciones
Piroeléctrico	Cambios de polarización con calor	Funciona a temperatura ambiente	Baja sensibilidad, ruido térmico
Detector de Golay	Cambios de presión en gas encapsulado	Alta sensibilidad	Lento, voluminoso
Fotoconductorivo (PCA)	Corriente generada al recibir THz	Alta resolución temporal	Requiere láser y sincronización
Rectificador Schottky	Detección por no linealidad de diodo	Compacto, rápido	Eficiencia limitada en rango THz
Detectores basados en grafeno	Efecto termoelectrico o plasmónico	Nanoescala, integración potencial	En fase experimental, difíciles de fabricar

Figura 3

Diagrama de bloques de una antena THz, fuente y detector.



3.4.2.2.4 Procesamiento de datos

Método que es capaz de analizar y construir imágenes a partir de

los datos obtenidos según el material, una técnica común es la espectroscopía de dominio temporal en la que se analiza el retardo de tiempo de las señales reflejadas permitiendo mapear la estructura interna de objetos entre sus capas.

En “Exploiting k-space/frequency duality toward real-time terahertz imaging”(Optica, 2018) nos detallan 2 metodologías para la obtención de imágenes THz, las cuales son las siguientes:

3.4.2.2.4.1. Rasterización convencional (Raster Scan)

Aquí se utiliza una antena fotoconductiva de un solo pixel (THz-PCA) con un escaneo tipo punto por punto en un plano espacial (x-y), se requiere mover el detector o el objetivo sobre una cuadrícula 2D, luego, se utiliza la transformada de Fourier estándar sobre la imagen para poder procesarla y obtener un espectro completo para cada pixel.

La resolución es alta dependiendo del tamaño de la cuadrícula y del foco óptico, sin embargo, el tiempo de adquisición es entre 1 a 5 segundos por pixel, por lo general una imagen simple tarda 1 hora en obtenerse mediante este proceso, aquí el número de mediciones que se realizarían sería de N^2 para una imagen de $N \times N$ pixeles, por ejemplo, 900 mediciones para una imagen de 30×30 pixeles, además, la reconstrucción es compleja y sensible al ruido.

Se realizó una prueba con una máscara metálica con patrón de hoja de arce donde se realizaron 4624 mediciones individuales a una resolución espacial de 1,5 mm por pixel donde cada pixel implica una medición independiente (esto debido a que se toma un espectro completo por punto).

3.4.2.2.4.2. Transformada Híbrida Inversa (Hybrid Inverse Transform)

Se utiliza la misma antena solo que optimizado con un amplificador de bloqueo o bloqueo síncrono (lock-in amplifier), también, un pulso THz de

banda ancha lo que significa que cada medición contiene información de múltiples frecuencias con un escaneo de camino circular sobre el plano de Fourier(k-space) y el uso del espectro, en este caso el detector fijo escanea puntos en una circunferencia(en lugar de barrer 2 dimensiones(x e y) se realiza el barrido en una dimensión espacial teniendo en cuenta el ángulo de la circunferencia utilizando la frecuencia como segunda dimensión), luego, se utiliza un algoritmo híbrido que combina la transformada de Fourier con el espectro de la señal donde el espectro se usa para mapear el espacio de Fourier.

La resolución es alta o incluso mejor que el de rasterización convencional, depende del ancho espectral y del radio de escaneo, aquí el tiempo de obtención de la imagen podría requerir tan solo unas decenas de mediciones respecto al método de rasterización.

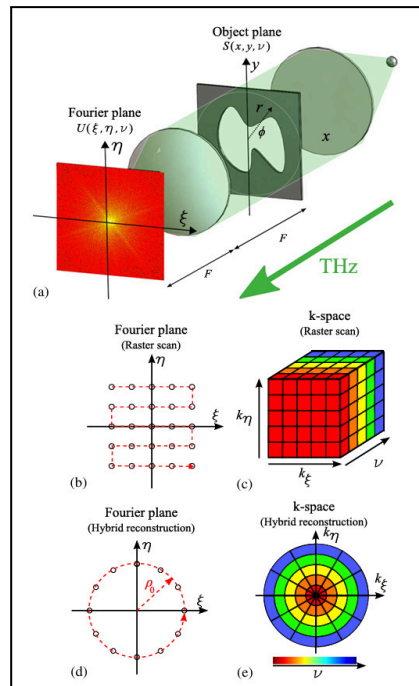
El número de mediciones sería proporcional a N(solo lineal) gracias al uso del espectro, además, cuenta con una alta sensibilidad incluso para grabados superficiales.

Aquí se utilizó una prueba con la hoja de arce y un grabado del símbolo pi sobre una resina transparente (imagen de fase) teniendo como resultado que solo se necesitarían 20 mediciones para poder reconocer la hoja y las imágenes mejoraban notablemente con 45 o 180 mediciones.

A continuación, se muestra una comparativa de las metodologías empleadas.

Figura 4

Esquema de adquisición y reconstrucción de imágenes mediante Escaneo Raster y Reconstrucción Híbrida.

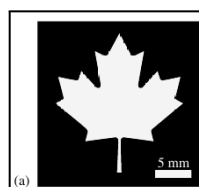


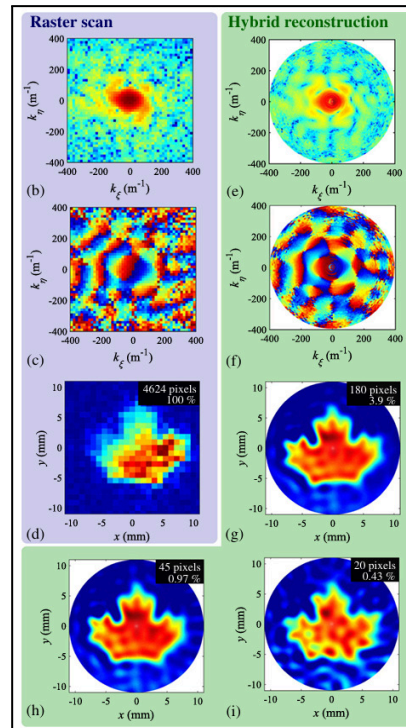
Nota. (a) Esquema del plano del objeto y el plano de Fourier. (b) Raster Scan en un plano cartesiano 2D en el plano de Fourier. (c) Cubo hiperespectral en el espacio k. (d) Algoritmo de reconstrucción híbrido realizando un escaneo circular 1D en el plano de Fourier. (e) Espacio k obtenido a partir de la información espectral. Reproducido de Exploiting k-space/frequency duality toward real-time terahertz imaging, Guerboukha, Nallappan y Skorobogatiy, 2018. (<https://opg.optica.org/optica/fulltext.cfm?uri=optica-5-2-109&id=381085>). Todos los derechos reservados por Optica. Reproducido con permiso del autor.

A continuación, se muestra la comparativa de las imágenes obtenidas mediante ambos métodos.

Figura 5

Reconstrucción de imagen de un recorte de hoja de arce en una placa metálica.



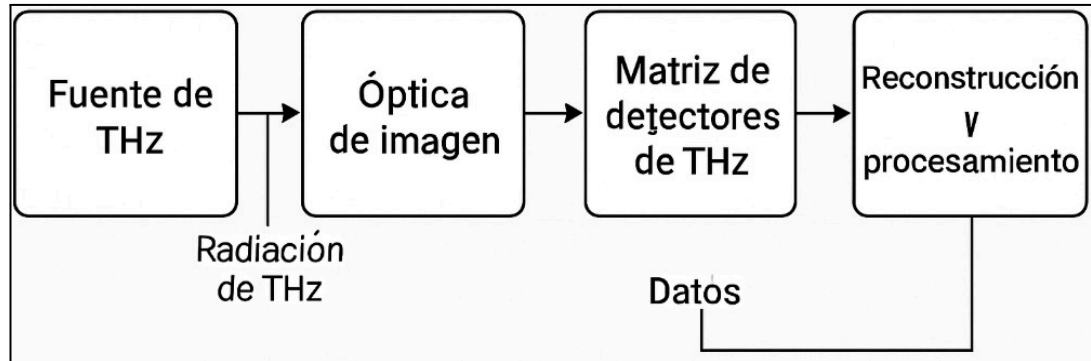


Nota. (a) Esquema del recorte de la hoja de arce. Raster Scan estándar (b) Amplitud y (c) Fase del espacio k a una frecuencia única de 0.57 THz(4624 píxeles). (d) Reconstrucción de la imagen mediante la transformada inversa de Fourier estándar. Reconstrucción de imagen mediante la transformada inversa híbrida: (e) Distribución inferida de la amplitud y (f) fase del espacio k utilizando espectros de las trazas temporales de THz de 25 mm, adquiridas a 180 píxeles y ubicadas a lo largo de un círculo de radio ρ_0 alrededor del origen del plano de Fourier. (g) Imagen reconstruida mediante la transformada inversa híbrida con 180 píxeles, (h) 45 píxeles e (i) 20 píxeles. Tomado de Exploiting k-space/frequency duality toward real-time terahertz imaging, Guerboukha, Nallappan y Skorobogatiy, 2018. (<https://opg.optica.org/optica/fulltext.cfm?uri=optica-5-2-109&id=381085>). Todos los derechos reservados por Optica. Reproducido con permiso del autor.

Ahora, tenemos el diagrama de bloques completo incluyendo el procesamiento de datos:

Figura 6

Diagrama de bloques para el sistema de cámaras Terahertz integrado



3.4.2.3 Middleware

Es una capa de software que se sitúa entre el sistema operativo y las aplicaciones distribuidas, permitiendo la comunicación, el manejo de datos, la autenticación, la mensajería y otros servicios entre componentes de software en entornos heterogéneos.

En otras palabras, facilita la interoperabilidad entre sistemas que, de otro modo, no podrían interactuar directamente.

Las ventajas de utilizar Middleware son las siguientes:

- Al conectar sistemas de manera uniforme, se optimiza la productividad, se minimizan los errores humanos y se incrementa la exactitud en el manejo de los datos.
- La automatización de procesos rutinarios y la optimización del flujo de información permiten aumentar la eficiencia operativa y disminuir los tiempos de respuesta.
- Fomenta el aprovechamiento de componentes y servicios ya existentes, lo cual reduce esfuerzos redundantes y favorece la consistencia en el desarrollo de soluciones. Esto contribuye a disminuir los recursos y el tiempo requeridos para la creación y mantenimiento de sistemas empresariales.

- Proporciona una visión centralizada y control sobre el flujo de información e interacciones entre sistemas conectados, lo cual facilita la supervisión, el diagnóstico proactivo de errores y la gestión eficiente de las operaciones.
- Está diseñado para adaptarse de forma eficiente al crecimiento del volumen de datos y transacciones, permitiendo a las organizaciones escalar sus operaciones y mantener un rendimiento óptimo incluso en entornos de alta demanda.
- Al centralizar el control del flujo de datos, permite aplicar políticas de seguridad sólidas (como cifrado, autenticación y control de accesos), lo que contribuye a proteger la información sensible y a asegurar el cumplimiento con normativas y estándares vigentes.

Las aplicaciones principales de Middleware son las siguientes:

- Comunicación entre aplicaciones (por ejemplo, usando APIs, colas de mensajes o servicios web).
- Acceso a bases de datos desde diferentes sistemas.
- Autenticación y autorización centralizada.
- Sincronización de datos entre múltiples servidores o plataformas.
- Transacciones distribuidas, donde varias operaciones deben completarse correctamente en distintos sistemas.

Dicho esto, en el entorno de videovigilancia, para gestión de video el Middleware tiene la capacidad de:

- Permitir que un VMS se conecte a diferentes marcas y modelos de cámaras.
- Integrar el VMS con sistemas de alarmas, control de acceso o software de análisis de video.

- Actuar como intermediario para el almacenamiento de video en la nube o en servidores locales.

Dicho esto, el middleware es clave ya que muchas cámaras THz no implementan ONVIF nativamente. Este software/hardware intermedio encapsula los datos reconstruidos y permite que el VMS los trate como si provinieran de una cámara IP convencional (ONVIF, 2023).

3.4.2.4 VMS (Video Management System)

Un VMS es una plataforma de software que centraliza la captura, gestión, visualización, archivado y análisis de contenido de video, generalmente proveniente de cámaras de vigilancia.

Su funcionalidad central incluye la integración de múltiples dispositivos de captura (cámaras IP o analógicas), la gestión centralizada de grabaciones y eventos, y la provisión de interfaces para la visualización en tiempo real o diferido.

El desarrollo de los VMS ha estado estrechamente relacionado con el avance de la videovigilancia digital y la convergencia de Tecnologías de la Información con los sistemas de seguridad física. Actualmente, un VMS moderno puede incluir capacidades avanzadas como detección de movimiento, análisis de comportamiento, reconocimiento facial, integración con sistemas de control de acceso y respuesta automatizada ante eventos definidos por el usuario.

Sus funciones clave incluyen:

- Ingesta y normalización de flujos (RTSP, ONVIF, etc.).
- Grabación y almacenamiento gestionado (archivo local/centralizado, retención).
- Visualización en tiempo real y revisión forense.
- Gestión de eventos y metadatos (alarmas, zonas de interés).
- Integración con analítica (detección de intrusión, reconocimiento, correlación de eventos).

La arquitectura típica de un VMS se compone de varios módulos funcionales:

- Captura de video: recepción de flujos de video desde cámaras IP o digitalización de señales analógicas.
- Almacenamiento: administración de bases de datos de video, ya sea en servidores locales, dispositivos de almacenamiento en red (NAS) o en la nube.
- Procesamiento y análisis: aplicación de algoritmos de visión por computadora o inteligencia artificial para extraer información del video.
- Interfaz de usuario: plataformas gráficas (cliente web, aplicaciones móviles, clientes de escritorio) que permiten la visualización y administración del sistema.
- Integración de dispositivos y sistemas: compatibilidad con protocolos estándar (ONVIF, RTSP, etc.) y con otros sistemas como alarmas, sensores o software de análisis externo.

Con el avance de tecnologías como la inteligencia artificial (IA), el aprendizaje automático (machine learning) y la analítica de video, los VMS han evolucionado más allá de la simple grabación. Se habla ahora de Video Intelligence Platforms o plataformas inteligentes de video.

Sin embargo, el despliegue de VMS también enfrenta desafíos importantes:

- Privacidad y protección de datos: el tratamiento de imágenes personales está regulado por normativas como el Reglamento General de Protección de Datos (GDPR) en Europa o leyes locales de protección de datos.

- Ciberseguridad: al estar conectados en red, los VMS son susceptibles a ataques informáticos si no se implementan buenas prácticas de seguridad.
- Interoperabilidad: la integración entre diferentes marcas y sistemas requiere del uso de estándares abiertos.

3.4.2.5 Ley de Protección de Datos Personales

La Ley N° 29733, conocida como la Ley de Protección de Datos Personales en Perú, fue promulgada en 2011 con el objetivo de garantizar el derecho fundamental a la protección de datos personales, regulando el tratamiento, almacenamiento y transferencia de información personal por parte de entidades públicas y privadas.

Como principios y alcance, la ley establece principios como la licitud, finalidad, consentimiento, proporcionalidad, calidad, seguridad y transparencia en el manejo de datos personales. Se aplica a toda información que permita identificar directa o indirectamente a una persona natural, incluyendo datos sensibles que requieren mayor protección, como información sobre salud, origen racial, opiniones políticas o vida sexual.

3.4.2.6 Reglamento de medidas mínimas de Seguridad para las Entidades del Sistema Financiero

Según el título II (Medida mínimas de seguridad), capítulo de I (Servicio de Vigilancia privada), artículo 5 (Medidas mínimas de seguridad sobre vigilancia privada), en el apartado (d) indica que el personal de seguridad debe cautelar que los usuarios y clientes que ingresen a las oficinas de las entidades del sistema financiero no porten objetos peligrosos como armas y elementos filosos o punzantes, o prendas que impidan o dificulten la visualización de sus rostros.

3.5 Procedimiento

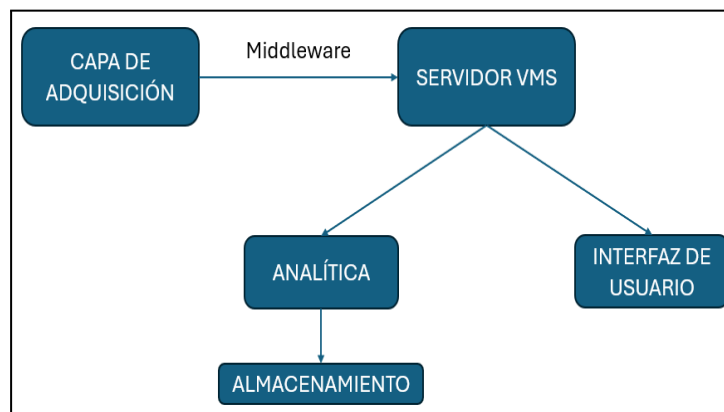
El presente trabajo de sustentación profesional está enfocado en el uso de las cámaras Terahertz en entidades financieras para la prevención

de robos e intrusión.

Se presenta el diagrama de bloques para la integración de cámaras THz en un sistema de CCTV existente, este requiere una arquitectura de varios niveles que permitirá monitorear y mantenerse alerta desde el centro de control de la entidad financiera:

Figura 7

Diagrama de bloques Sistema Terahertz



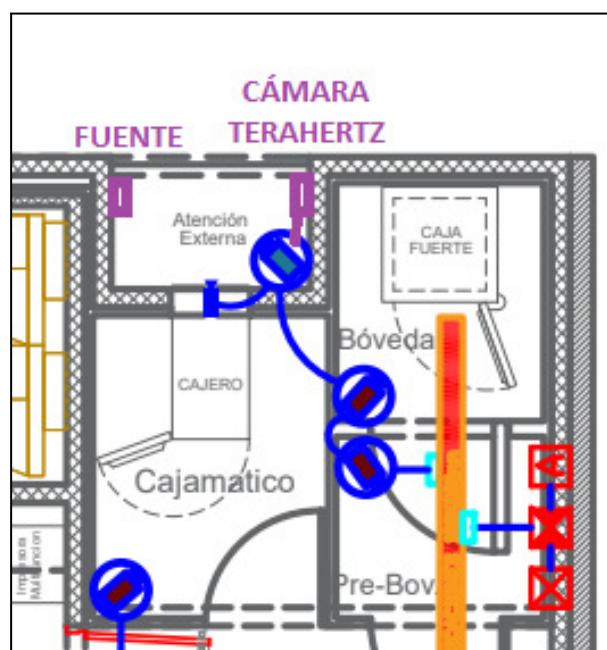
3.5.1 Capa de Adquisición

En este bloque se encuentran las cámaras Terahertz y los sensores que capturan la señal provenientes de las ondas Thz.

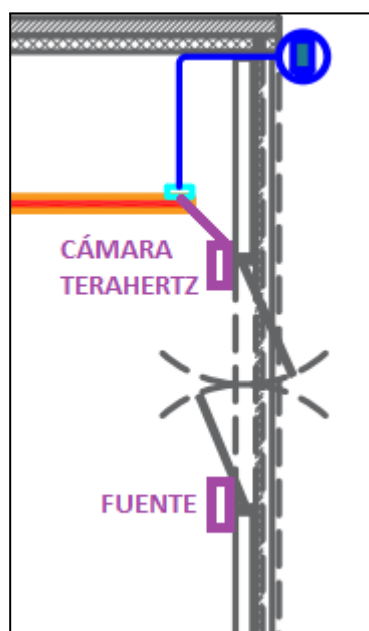
A continuación, se presentará el diseño de acuerdo a un esquema modelo donde se mostrará la ubicación de las cámaras convencionales y la incorporación de la cámara Terahertz.

Figura 9

Ubicación en el plano de cámara Terahertz en el ambiente de cajero

**Figura 10**

Ubicación en el plano de cámara Terahertz en el ingreso de agencia



Para el caso de las cámaras, tomaremos de referencia las Terafast-256 de Terasense(2025) las cuales tienen las siguientes características según el fabricante:

- Tasa de adquisición de imágenes: 5000 fps (5 kHz)
- Velocidad de escaneo: hasta 15 m/seg (900 m/min)
- Min Potencia detectable/píxel: 100 nW (a 5000 fps)
- 256 píxeles (256 x 1 matriz) - talable en tamaño
- Tamaño de píxel de 3 x 1.5 mm
- $Nep = 1 \text{ nW} / \sqrt{\text{Hz}}$

Para el caso de la fuente podemos utilizar de referencia la fuente tipo II de ondas Terahertz de Terasense(2025).

Según el fabricante, sus características son las siguientes:

Tabla 6

Características de fuente Terahertz Tipo II.

Frecuencia	100 GHz
Potencia por píxel	140 μW
Rango dinámico del sistema de imágenes	30 dB
Sistema Óptico	Óptica reflectiva
Tecnología	Super-Hero IMPATT

Nota. Elaborado por Terasense(2025).

3.5.2 Middleware

Actuará como traductor entre la cámara THz (o módulo de procesamiento de la misma) y el servidor VMS, asimismo, debe cumplir los siguientes requisitos.

- Ingesta de datos: recepción de datos raw o preprocesados (imágenes 2D, líneas, espectros, metadatos) desde la cámara (GigE, USB, serial, API propietario).
- Procesamiento: reconstrucción (Hadamard, Transformada de Fourier Inversa, etc), filtrado, reducción de ruido, detección preliminar (para generar eventos ante la detección de un arma, objeto punzocortante, etc.).
- Encapsulado de streams: codificar en H.264/H.265 o empaquetar como RTSP para que el VMS pueda consumirlo.
- Exposición ONVIF: implementar un servidor ONVIF (Profile S/T) que permita descubrimiento, control PTZ (si aplica), transmisión y metadatos/eventos.
- Metadatos y eventos: definir y mapear metadata específicos (tipo de objeto detectado, confianza, región del frame, espectro) a esquemas de eventos que el VMS comprenda.
- Sincronización temporal: adjuntar timestamps sincronizados (NTP/PTP) a cada frame/medición.
- Escalabilidad y latencia: el middleware debe mantener latencias bajas si se requiere respuesta en tiempo real.
- Seguridad: canal seguro (TLS), autenticación mutua si procede, y hardening del gateway.

3.5.3 VMS

Para integrar de manera eficiente cámaras Terahertz en un sistema CCTV a través de un VMS, se debe montar el gestor en un servidor que debe cumplir con ciertas especificaciones técnicas y operativas clave:

- Unidad de procesamiento gráfico compatible con aceleración por hardware para codificación/decodificación H.264/H.265.
- Compatibilidad con protocolos de video IP: ONVIF, RTSP.
- Capacidad para recibir y gestionar flujos de video reconstruidos provenientes del middleware de la cámara THz.
- Registro y auditoría de accesos y eventos.

- Arquitectura modular para añadir más cámaras sin degradación de rendimiento.
- Motor analítico integrado o compatibilidad con módulos de IA externos (API's).
- Interfaz web y cliente nativo para gestión remota.
- Monitoreo en tiempo real de la salud del sistema (uso de CPU/GPU, latencia, pérdida de paquetes).

3.5.4 Interfaz de Usuario

La interfaz de usuario debe tener las siguientes características clave:

- Diseño intuitivo para los usuarios.
- Visualización múltiple: Soporte para ver en paralelo video visible y THz en modo side-by-side o superposición.
- Control en tiempo real.
- Alertas y notificaciones.
- Filtros y búsqueda avanzada: Por fecha, tipo de evento, cámara o metadatos.
- Gestión de eventos con herramientas para marcar, clasificar y exportar clips relevantes.
- Seguridad de acceso que pueda brindarnos perfiles de usuario con permisos diferenciados.
- Compatibilidad multiplataforma que brinde acceso vía cliente nativo, navegador web y dispositivos móviles.
- Mostrar resultados analíticos (objetos detectados, confianza, espectro asociado).
- Contar con un registro de auditoría.

3.5.5 Analítica

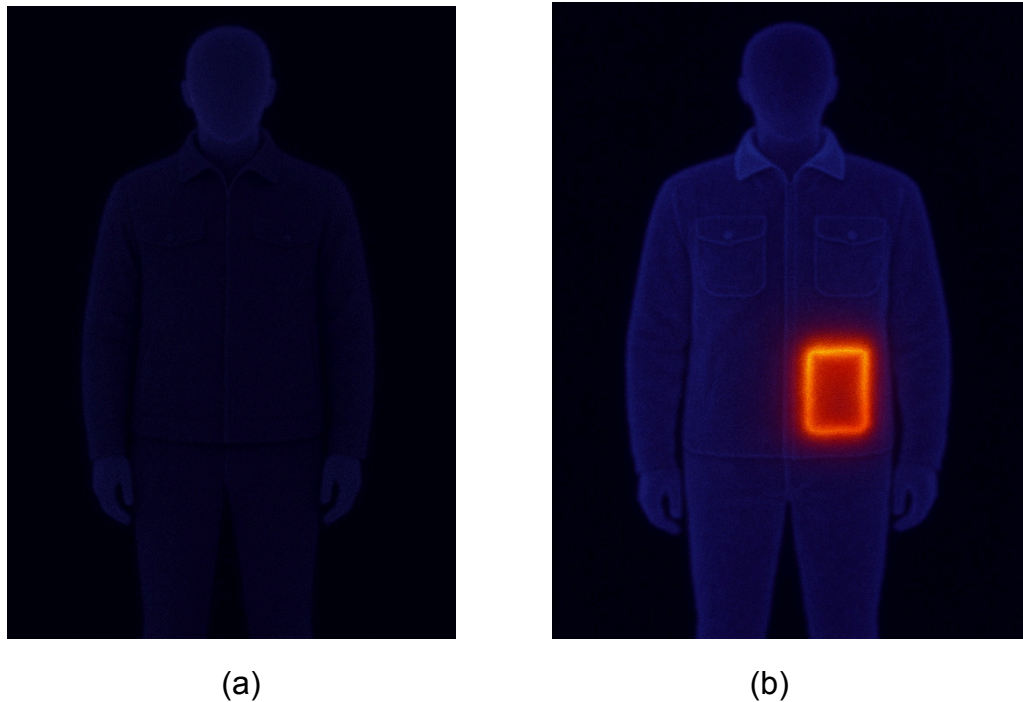
Las características principales que debe tener la analítica de las cámaras Terahertz son las siguientes:

- Detección de objetos ocultos para identificar armas, explosivos, objetos punzocortantes, etc.
- Clasificación por tipo de material para diferenciar metales, plásticos, cerámicos, etc.

- Procesamiento en tiempo real.
- Aprendizaje continuo.
- Integración con VMS.

Figura 11

Detección de arma oculta con cámara de Terahertz.



Nota. (a) Sujeto con objeto cubierto y (b) Detección del objeto mediante las cámaras Terahertz.

3.5.6 Almacenamiento

Debe cumplir con los siguientes requerimientos:

- Alta capacidad y escalabilidad, debe soportar como mínimo 60 días, además, permitir más nodos de almacenamiento sin la interrupción del servicio.
- Las memorias deben ser SSD/NVMe para mejorar la respuesta en búsquedas y reproducción instantánea.
- Gestión centralizada con monitoreo de estado, capacidad y rendimiento.

3.6 Resultado de la actividad

El presente trabajo se centrará en el diseño de la integración de las cámaras Terahertz y un análisis del costo de implementación anual de

acuerdo a las características antes descritas, para esto, se incluirá la mano de obra, los equipos activos(dispositivos) y el desarrollo del VMS para la instalación.

Figura 12

Cotización de servicio de instalación de cámaras Terahertz

SERVICIOS DE RIESGOS Y SEGURIDAD - SEGURIDAD ELECTRÓNICA			
Cliente:			
Servicio:	INSTALACIÓN CCTV		
Agencia:			
Fecha:			
Descripción:	INSTALACIÓN DE CÁMARAS TERAHERTZ		
			Total
			S/.179.828,00
DESCRIPCIÓN	CANTIDAD	PRECIO U.	PRECIO TOTAL
MANO DE OBRA			S/.1.198,00
INSTALACIÓN Y CONFIGURACIÓN DE CÁMARAS	2	S/.599,00	S/.1.198,00
MATERIALES			S/.149,48
CAPUCHONES Y CONECTORES PARA RJ-45 AMP CATEGORIA 6	2	S/.7,54	S/.15,08
CABLE UTP CAT 6 LSZH -DIXON - 9040 (01 mtrs)	70	S/.1,92	S/.134,40
DISPOSITIVOS			S/.178.630,00
CÁMARA TERAFAST-256	2	S/.35.726,00	S/.71.452,00
FUENTE DE TERAHERTZ TIPO II	2	S/.53.589,00	S/.107.178,00
TOTAL			S/.179.828,00
Notas:			
El precio es en soles y no incluye IGV.			

Figura 13

Cotización de servicio de instalación y configuración de servidor VMS para cámaras Terahertz

SERVICIOS DE RIESGOS Y SEGURIDAD - SEGURIDAD ELECTRÓNICA			
Cliente:			
Servicio:	INSTALACIÓN CCTV		
Agencia:			
Fecha:			
Descripción:	INSTALACIÓN Y CONFIGURACIÓN DE SERVIDOR VMS PARA CÁMARAS THZ		
			Total
			S/.263.485,17
DESCRIPCIÓN	CANTIDAD	PRECIO U.	PRECIO TOTAL
MANO DE OBRA			S/.185.684,52
CONFIGURACIÓN DE SERVIDOR VMS	1	S/.35.368,48	S/.35.368,48
DESARROLLO MIDDLEWARE	1	S/.150.316,04	S/.150.316,04
DISPOSITIVOS			S/.77.800,65
SERVIDOR VMS	1	S/.49.515,87	S/.49.515,87
ALMACENAMIENTO(Capacidad para 30 días, 2 cámaras)	1	S/.28.284,78	S/.28.284,78
TOTAL			S/.263.485,17
Notas:			
El precio es en soles y no incluye IGV.			

Figura 14*Cotización de licencia para cámara Terahertz*

SERVICIOS DE RIESGOS Y SEGURIDAD - SEGURIDAD ELECTRÓNICA			
Cliente:			
Servicio:	INSTALACIÓN CCTV		
Agencia:			
Fecha:			
Descripción:	LICENCIA PARA CÁMARA TERAHERTZ		
			Total
			S/.1.591,58
DESCRIPCIÓN	CANTIDAD	PRECIO U.	PRECIO TOTAL
LICENCIA			S/.1.591,58
LICENCIA VMS ANUAL	1	S/.1.591,58	S/.1.591,58
TOTAL			S/.1.591,58
Notas:			
El precio es en soles y no incluye IGV.			

CAPITULO IV: DISCUSION DE RESULTADOS

4.1 Descripción de la implementación

La implementación del proyecto se desarrollará según las siguientes etapas:

- a) Ubicación de agencia: Se tomará en cuenta el desarrollo del proyecto en una agencia que esté en una zona de alto peligro.
- b) Diseño de la implementación: De acuerdo al sistema modelo presentado, se propone colocar el sistema de cámaras Terahertz en el ingreso de agencia y en la puerta de acceso al ATM.
- c) Selección de dispositivos: Los dispositivos fueron seleccionados de acuerdo a las especificaciones técnicas en sus hojas de datos.

CAPITULO V: CONCLUSIONES

1. Los delitos relacionados con atentados o amenazas tienen una tendencia al alza en los últimos años, sobre todo para los delitos contra el patrimonio por lo que no se puede pasar por alto el reforzamiento de la seguridad en las entidades financieras.
2. El uso de cámaras Terahertz eleva el nivel de seguridad sin vulnerar la privacidad, esto debido a que no muestran detalles anatómicos sino contornos u objetos ocultos como drogas, explosivos ocultos, armas metálicas, etc.
3. El uso de cámaras Terahertz se puede extender a otras áreas de alto riesgo/valor como ingreso a bóvedas, cámaras acorazadas, gerencias, etc.
4. Si bien es cierto, los costos de inversión son elevados (en nuestro caso se tornaría en base a los S./ 181419.58 por agencia y S./ 263485.15 por el desarrollo), hay que tener en cuenta que esta inversión es para proteger las vidas humanas, activos críticos y garantizar la continuidad de negocio.
Su uso refuerza la postura de seguridad institucional, reduce riesgos mayores y representa un activo preventivo de alto impacto en contextos donde una sola falla de seguridad puede desencadenar inconvenientes catastróficos.
5. Con las capacidades de la analítica basada en cámaras Terahertz, debemos tener en cuenta que no solo mejora la seguridad, sino que optimiza la eficiencia operativa del sistema CCTV en entornos críticos como entidades financieras.

CAPITULO VI: RECOMENDACIONES

1. El aumento de los delitos sugiere el uso de tecnologías de detección avanzada en tiempo real como las cámaras Terahertz que son justificables en zonas de alto riesgo.
2. Una vez realizada la implementación se recomienda desarrollar un programa de capacitación en operación, mantenimiento preventivo y respuesta ante detecciones anómalas.
3. Se recomienda estar al tanto de actualizaciones de las normativas sobre privacidad y derechos del usuario para garantizar así que el uso de estos sistemas esté respaldado de manera legal y ética.
4. Se sugiere realizar pruebas piloto con una o dos cámaras Terahertz en el entorno real de la agencia bancaria antes del despliegue masivo.
5. Para la optimización de almacenamiento se sugiere emplear codificación H.265 como mínimo para reducir el ancho de banda y espacio requerido.
6. Entrenamiento y capacitación constante al centro de control de la entidad para la interpretación de las imágenes THz y en el uso del VMS desarrollado.

CAPITULO VII: BIBLIOGRAFIA

Chaverra, D. (25 de agosto del 2020). Monitoreo y control para garantizar la seguridad bancaria. VENTAS DE SEGURIDAD. <https://www.ventasdeseguridad.com/2020082512245/noticias/empresas/monitoreo-y-control-para-garantizar-la-seguridad-bancaria.html>

Deng, X., Li, Y., Hu, J., Miao, W., Lin, C., Jiang, J., & Shi, S. (2025). Terahertz science and technology in astronomy, telecommunications, and biophysics. https://spj-science-org.translate.goog/doi/10.34133/research.0586?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Edwards, T. (2024). Gigahertz and Terahertz Technologies for Broadband Communications. <https://us.artechhouse.com/Gigahertz-and-Terahertz-Technologies-for-Broadband-Communications-P1276.aspx>

Guerboukha H., Nallappan K., Skorobogatiy M. (2018). Exploiting k-space/frequency duality toward real-time terahertz imaging <https://opg.optica.org/optica/fulltext.cfm?uri=optica-5-2-109&id=381085>

MININTER (2023). Denuncias por comisión de delitos, según delito genérico. https://m.inei.gob.pe/media/MenuRecursivo/indices_tematicos/1.%20Denuncias%20por%20comision%20de%20delitos%20-%20Delito%20generico_1.xlsx

Paredes, V. (2017). Herramientas de seguridad en entidades financieras. SEGURILATAM.

https://www.segurilatam.com/seguridad-por-sectores/financiero/herramientas-de-seguridad-en-entidades-financieras_20170921.html

Park, G.-S., Tani, M., Rieh, J.-S., & Park, S. Y. (2024). *Advances in terahertz source technologies*.

<https://www.taylorfrancis.com/books/edit/10.1201/9781003459675/advances-terahertz-source-technologies-gun-sik-park-masahiko-tani-jae-sung-rieh-san-g-yoon-park>

Terasense (2018). Terahertz Security Body Scanner. Youtube
<https://www.youtube.com/watch?v=7o9vGYAPkzE>

Terasense (2025). NEW-GENERATION TERAHERTZ IMAGERS

<https://terasense.com>

Wang, G., Gu, H., Li, X., Yu, Z., Li, O., Liu, Q., Zeng, K., He, J., Chen, Y., Lu, J., Tong, W., & Wessel, D. (2022). Terahertz sensing and communication: Towards future intelligence connected networks. Huawei Technologies Co., Ltd.

<https://www.huawei.com/en/huaweitech/future-technologies/terahertz-sensing-communication>