UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO

FACULTAD DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA, INFORMÁTICA Y MECÁNICA

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

TESIS

DISEÑO DE UN SISTEMA INTEGRADO DE SEGURIDAD ELECTRÓNICA BASADO EN IOT PARA EL PABELLÓN DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS DE LA UNSAAC

PRESENTADO POR:
Br. ROXANA HERMOZA CUSI

PARA OPTAR AL TÍTULO PROFESIONAL DE INGENIERO INFORMATICO Y DE SISTEMAS

ASESOR:
Dr. RONY VILLAFUERTE SERNA

CUSCO – PERÚ

2026

Universidad Nacional de San Antonio Abad del Cusco

INFORME DE SIMILITUD

(Aprobado por Resolución Nro.CU-321-2025-UNSAAC)

El que suscribe, el **Asesor** RONY VILLAFUERTE SERNA ..... quien aplica el software de detección de similitud al trabajo de investigación/tesistitulada: DISEÑO DE UN SISTEMA INTEGRADO DE SEGURIDAD ELECTRÓNICA BASADO EN IOT PARA EL PABELLÓN DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS DE LA UNSAAC .....

Presentado por: ROXANA HERMOZA CUSI ..... DNI N° 47493578 ;
presentado por: ..... DNI N°: .....
Para optar el título Profesional/Grado Académico de INGENIERO INFORMATICO Y DE SISTEMAS .....

Informo que el trabajo de investigación ha sido sometido a revisión por 2 veces, mediante el Software de Similitud, conforme al Art. 6° del ***Reglamento para Uso del Sistema Detección de Similitud en la UNSAAC*** y de la evaluación de originalidad se tiene un porcentaje de 1 %.

Evaluación y acciones del reporte de coincidencia para trabajos de investigación conducentes a grado académico o título profesional, tesis

Porcentaje	Evaluación y Acciones	Marque con una (X)
Del 1 al 10%	No sobrepasa el porcentaje aceptado de similitud.	X
Del 11 al 30 %	Devolver al usuario para las subsanaciones.	
Mayor a 31%	El responsable de la revisión del documento emite un informe al inmediato jerárquico, conforme al reglamento, quien a su vez eleva el informe al Vicerrectorado de Investigación para que tome las acciones correspondientes; Sin perjuicio de las sanciones administrativas que correspondan de acuerdo a Ley.	

Por tanto, en mi condición de Asesor, firmo el presente informe en señal de conformidad y **adjunto** las primeras páginas del reporte del Sistema de Detección de Similitud.

Cusco, 07 de Julio de 2026

Firma

Post firma. RONY VILLAFUERTE SERNA

Nro. de DNI. 23957778

ORCID del Asesor. 0000-0003-4607-522X

Se adjunta:

1. Reporte generado por el Sistema Antiplagio.
2. Enlace del Reporte Generado por el Sistema de Detección de Similitud: **oid:** 27259:605365079

Roxana Hermoza Cusi

seguridadINFOv2.pdf

Universidad Nacional San Antonio Abad del Cusco

Detalles del documento

Identificador de la entrega
trn:oid:::27259:605365079

Fecha de entrega
7 jul 2026, 10:54 a.m. GMT-5

Fecha de descarga
7 jul 2026, 10:59 a.m. GMT-5

Nombre del archivo
seguridadINFOv2.pdf

Tamaño del archivo
7.8 MB

205 páginas

34.685 palabras

205.637 caracteres

1% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Coincidencias menores (menos de 20 palabras)

Exclusiones

- N.º de coincidencias excluidas

Fuentes principales

1%	Fuentes de Internet
0%	Publicaciones
1%	Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alerta de integridad para revisión

Caracteres reemplazados
40 caracteres sospechosos en N.º de páginas
Las letras son intercambiadas por caracteres similares de otro alfabeto.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Dedicatoria

DEDICATORIA

A mi madre, Martha,

quien desde el cielo sigue siendo mi guía y mi luz.

Este logro es la culminación de los sueños que sembraste en mí

y el fruto de tu amor incondicional.

Todo lo que soy y lo que he logrado, te lo debo a ti.

Agradecimientos

Agradezco a mi familia por su apoyo, comprensión y motivación constante a lo largo de mi formación académica. Asimismo, expreso mi gratitud a mis amigos por su compañía y ánimo durante este proceso, y a mis docentes por sus enseñanzas, orientación y valioso aporte en el desarrollo de esta investigación.

Resumen

La presente investigación tiene como objetivo diseñar un sistema integrado de seguridad electrónica basado en tecnologías IoT para la Escuela Profesional de Ingeniería Informática y de Sistemas, con la finalidad de mejorar el monitoreo, el control de accesos y la respuesta ante incidentes. La investigación se desarrolló bajo un enfoque descriptivo y de tipo propositivo, mediante el análisis de la infraestructura existente, la identificación de los principales riesgos de seguridad y la recopilación de requerimientos técnicos y funcionales. Como resultado, se propuso una arquitectura de seguridad que integra sistemas de videovigilancia, alarmas electrónicas y control de acceso, gestionados a través de una plataforma centralizada que permite la interoperabilidad entre dispositivos de diferentes fabricantes. Asimismo, se establecieron criterios para la distribución de los equipos en los distintos ambientes del pabellón y se definieron lineamientos generales para el tratamiento de los datos personales generados por los sistemas de seguridad, considerando la normativa vigente y buenas prácticas aplicables al ámbito de la seguridad electrónica y la gestión de la información. El diseño propuesto constituye una base técnica para una futura implementación del sistema, contribuyendo al fortalecimiento de la seguridad institucional.

Palabras clave: Sistema integrado, Seguridad electrónica, Videovigilancia, Control de acceso, Sistemas de alarma.

Abstract

The objective of this research is to design an integrated electronic security system based on IoT technologies for the Professional School of Informatics and Systems Engineering, with the purpose of improving monitoring, access control, and incident response. The research followed a descriptive and propositional approach, analyzing the existing infrastructure, identifying key security risks, and gathering technical and functional requirements. As a result, a security architecture was proposed that integrates video surveillance, electronic alarms, and access control systems, managed through a centralized platform that enables interoperability among devices from different manufacturers. Furthermore, criteria were established for equipment distribution across the various environments of the pavilion, and general guidelines were defined for processing the personal data generated by the security systems, considering current regulations and applicable best practices in electronic security and information management. The proposed design establishes a technical baseline for a future implementation of the system, contributing to the strengthening of institutional security.

Keywords: Integrated system, Electronic security, Video surveillance, Access control, Alarm systems.

Introducción

La presente tesis se encuentra estructurada en cinco capítulos, los cuales desarrollan de manera ordenada los fundamentos teóricos, metodológicos y técnicos que sustentan el diseño de un sistema integrado de seguridad electrónica.

En el Capítulo I se aborda el planteamiento del problema, describiendo la situación actual y la problemática identificada. Asimismo, se formulan los objetivos general y específicos, se expone la justificación de la investigación y se establecen la delimitación del estudio, el método y el alcance de la investigación.

El Capítulo II presenta el marco teórico, en el cual se desarrollan los conceptos, definiciones y antecedentes relacionados con los sistemas de seguridad electrónica, la videovigilancia, el control de accesos, los sistemas de alarmas y las tecnologías IoT, que sirven de sustento teórico para la investigación.

En el Capítulo III se describe la metodología empleada para la recolección de la información, detallándose el diseño de la encuesta aplicada, el número de preguntas, la población y la muestra considerada, así como los procedimientos utilizados para la obtención de los datos.

El Capítulo IV comprende, en primer lugar, el análisis del entorno y de la infraestructura existente, a partir del cual se redefinen los requisitos técnicos y funcionales del sistema de seguridad. Posteriormente, se presenta el diseño de los sistemas de seguridad propuestos, que incluyen el sistema de videovigilancia, el sistema de control de accesos y

el sistema de alarmas, así como las especificaciones técnicas de la plataforma de gestión de seguridad unificada.

El Capítulo V presenta el diseño del sistema de seguridad propuesto, integrando los subsistemas de videovigilancia, control de acceso y alarmas. Se definen la ubicación estratégica de los dispositivos, la arquitectura de red y la interconexión de los equipos, así como los diagramas físicos y lógicos correspondientes, garantizando un diseño funcional, seguro y escalable.

El capítulo VI desarrolla los documentos de gestión y procedimientos necesarios para la correcta operación del sistema de seguridad implementado. Se establecen lineamientos y protocolos que regulan el uso, monitoreo y mantenimiento de los subsistemas de videovigilancia, control de acceso y alarmas, con el fin de asegurar su funcionamiento eficiente y la adecuada respuesta ante incidentes.

Finalmente, en el Capítulo VII se exponen los resultados detallados obtenidos a partir de la encuesta realizada. Asimismo, se desarrolla el análisis de los resultados en relación con los objetivos planteados y la discusión de los mismos, contrastándolos con los antecedentes y estudios previos considerados en la investigación.

Listado de Abreviaturas

ANPD	Autoridad Nacional de Protección de Datos Personales
ARCO	Derechos de Acceso, Rectificación, Cancelación y Oposición
CCTV	Circuito Cerrado de Televisión (*Closed Circuit Television*)
IoT	Internet de las Cosas (*Internet of Things*)
IP	Protocolo de Internet (*Internet Protocol*)
NVR	Grabador de Video en Red (*Network Video Recorder*)
ONVIF	Foro Abierto de Interfaz de Video en Red (*Open Network Video Interface Forum*)
PTZ	Paneo, inclinación y zoom (*Pan Tilt Zoom*)
ANSI	Instituto Nacional Estadounidense de Estándares (*American National Standards Institute*)
ISO	Organización Internacional de Normalización (*International Organization for Standardization*)
IEC	Comisión Electrotécnica Internacional (*International Electrotechnical Commission*)
EIA	Alianza de Industrias Electrónicas (*Electronic Industries Alliance*)

Índice general

Dedicatoria **II**

Agradecimientos **III**

Resumen **IV**

Abstract **V**

Introducción **VI**

Listado de Abreviaturas **VIII**

Índice General **IX**

Índice de figuras **XVI**

Índice de tablas **XVIII**

1. Aspectos Generales **1**

1.1. Planteamiento del Problema 1

1.1.1. Descripción del problema 1

1.1.2. Identificación del problema 3

1.2. Formulación del Problema 5

1.2.1. Problema General 5

1.2.2. Problemas Específicos 5
1.3. Objetivos 5
1.3.1. Objetivo General 5
1.3.2. Objetivos Específicos 6
1.4. Justificación 6
1.4.1. Conveniencia 7
1.4.2. Relevancia 8
1.4.3. Implicancias Prácticas 8
1.4.4. Valor Teórico 9
1.4.5. Utilidad Metodológica 9
1.5. Delimitación de Estudio 9
1.5.1. Delimitación Espacial 9
1.5.2. Delimitación Temporal 10
1.6. Metodología 10
1.6.1. Enfoque 10
1.6.2. Alcance 10
1.6.3. Diseño de Investigación 10
1.7. Diagrama del Modelo Conceptual 12
1.7.1. Poblacion y Muestra 12

2. Marco Teórico **16**

2.1. Antecedentes 16
2.2. Bases Teóricas 22
2.2.1. Sistemas de Seguridad Electrónica 22
2.2.2. Internet de las Cosas (IoT) en la Seguridad 23
2.2.3. Inteligencia Artificial Aplicada a la Seguridad 23

2.2.4. Consideraciones de Ciberseguridad y Privacidad 24
2.2.5. Plataforma de Gestión de Seguridad Unificada 24
2.2.6. Normas Técnicas Internacionales 25
2.2.7. Normas Técnicas Nacionales 31
2.2.8. Reglamentación Nacional 35
2.2.9. Arquitectura de Analítica de Video Basada en Inteligencia Artificial (Deep Learning) 39

3. Metodología de Recolección de Información 42

3.1. Recolección de Información 42
3.1.1. Encuestas 42
3.1.2. Validez y confiabilidad: 43
3.1.3. Aplicación 44
3.2. Resultados de la Encuesta 45
3.2.1. Resultados por Grupo de Encuestados 45

4. Analisis del Entorno y Requisitos del Sistema 80

4.1. Contexto General del Pabellón 80
4.1.1. Identificación de Activos y Caracterización de Ambientes 80
4.1.2. Evaluación de las Medidas de Seguridad Física y Electrónica Existentes 81
4.1.3. Percepción de los Usuarios Sobre la Seguridad 82
4.1.4. Panorama Actual de la Gestión de Protección de Datos Personales . . 85
4.1.5. Identificación de Brechas y Necesidades de Seguridad 85
4.2. Definición de Requerimientos del Sistema de Videovigilancia 87
4.3. Definición de Requerimientos del Sistema de Alarmas de Intrusión 88

4.4. Definición de Requerimientos del Sistema de Control de Acceso 89

4.5. Definición de Requerimientos de la Plataforma de Gestión Unificada 90

4.6. Definición de Requerimientos del Centro de Control y Monitoreo 91

5. Diseño del Sistema de Seguridad 93

5.1. Marco Normativo y Estándares 93

5.2. Diseño del Sistema de Videovigilancia 94

5.2.1. Criterios Técnicos para la Determinación de la Ubicación de Cámaras 94

5.2.2. Nomenclatura del Sistema de Videovigilancia 96

5.2.3. Cuadro de Distribución y Ubicación de Dispositivos de Videovigilancia 97

5.2.4. Plano de Distribución Física del Sistema de Videovigilancia por Nivel 97

5.2.5. Dimensionamiento del Sistema de Almacenamiento de Video 102

5.2.6. Especificaciones Técnicas de los Componentes Principales del Sistema de Videovigilancia 105

5.3. Diseño del Sistema de Control de Acceso 107

5.3.1. Criterios Técnicos para la Ubicación de Dispositivos de Control de Acceso 107

5.3.2. Nomenclatura del Sistema de Control de Acceso 109

5.3.3. Plano de Distribución Física del Sistema de Control de Acceso por Nivel110

5.3.4. Especificaciones Técnicas de los Dispositivos de Control de Acceso . . 114

5.4. Diseño del Sistema de Detección y Alarma de Intrusión 114

5.4.1. Criterios Técnicos para la Ubicación de los Dispositivos de Detección 114

5.4.2. Cuadro de Distribución de Dispositivos del Sistema de Alarma 115

5.4.3. Nomenclatura del Sistema de Alarmas 117

5.4.4. Plano de Distribución Física del Sistema de Alarma por Nivel 117

5.4.5. Especificaciones Técnicas del Sistema de Alarma 121

5.5. Diseño de la Plataforma de Gestión Unificada 122

5.5.1. Arquitectura de Gestión y Control de Acceso 122

5.6. Centro de Control y Monitoreo 123

5.6.1. Infraestructura del centro de monitoreo 124

5.6.2. Diseño Físico del Centro de Monitoreo 125

5.7. Lineamientos Técnicos Generales 128

5.7.1. Diseño del Cableado Estructurado 128

5.8. Presupuesto Referencial 133

5.9. Matriz de Trazabilidad Normativa 133

6. Documentos de Gestión y Procedimientos **137**

6.1. Marco Estratégico y Normativo 137

6.1.1. Ámbito de Aplicación 137

6.1.2. Fundamento Normativo 138

6.2. Gestión de Datos Personales y Análisis de Riesgos 138

6.2.1. Identificación y Clasificación de Datos Personales 138

6.2.2. Análisis de Riesgos en el Tratamiento de Datos 139

6.3. Políticas de Seguridad y Privacidad 140

6.3.1. Políticas de Privacidad y Seguridad desde el Diseño 140

6.3.2. Protocolo para el Ejercicio de Derechos ARCO 141

6.4. Manual de Procedimientos Operativos 142

6.4.1. Gestión de Incidentes en Videovigilancia 142

6.4.2. Gestión del Sistema de Control de Accesos 143

6.4.3. Gestión del Sistema de Alarmas 145

6.5. Continuidad Operativa y Mantenimiento 145

6.5.1. Verificación Operativa Diaria 145

6.5.2. Gestión de Servicios de Terceros 146
6.6. Instrumentos de Control y Verificación 147
6.6.1. Checklist de Cumplimiento de Seguridad 147
6.6.2. Modelo de Aviso de Privacidad 147
6.6.3. Formato de Consentimiento Informado (Datos Biométricos) 147
6.6.4. Bitácora Unificada de Incidentes 148
6.6.5. Checklist de Cumplimiento de Privacidad 148

7. Resultados **151**
7.1. Análisis de resultados obtenidos 151
7.2. Discusión de resultados respecto a los antecedentes 151
7.2.1. Escala de Cobertura y Optimización Teórica frente a Casos de Estudio 152
7.2.2. Dimensionamiento, Escalabilidad y Adaptación del Entorno Operativo 153
7.2.3. Soporte en Estándares Físicos de Telecomunicaciones 154
7.2.4. Operativización de la Gobernanza Tecnológica y Privacidad 154

Conclusiones **156**

Recomendaciones **158**

Trabajos Futuros **159**

Referencias **160**

Glosario de Términos **163**

Anexo A:Cuestionario aplicado **165**

Anexo B: Matriz de operacionalización de variables **168**

Anexo C: Cartel informativo **171**

Anexo D: Carteles Adicionales **173**

Anexo E: Revisión Encuesta **176**

Anexo E: Términos de Referencia (TDR) **181**

Índice de figuras

1.1. *Modelo conceptual* 12

3.1. *Nivel de seguridad del pabellón según el personal administrativo.* 45

3.2. *Nivel de seguridad del pabellón según los docentes.* 46

3.3. *Nivel de seguridad del pabellón según los estudiantes.* 46

3.4. *Incidentes de seguridad según el personal administrativo.* 47

3.5. *Incidentes de seguridad según los docentes.* 48

3.6. *Incidentes de seguridad según los estudiantes.* 49

3.7. *Incidentes de ingreso no autorizado según administrativos.* 50

3.8. *Incidentes de ingreso no autorizado según docentes.* 51

3.9. *Incidentes de ingreso no autorizado según estudiantes.* 51

3.10. *Areas vulnerables según el personal administrativo.* 53

3.11. *Areas vulnerables según los docentes.* 53

3.12. *Areas vulnerables según los estudiantes.* 54

3.13. *Reconocimiento de sistemas de seguridad según administrativos.* 55

3.14. *Reconocimiento de sistemas de seguridad según los docentes.* 56

3.15. *Reconocimiento de sistemas de seguridad según los estudiantes.* 57

3.16. *Efectividad de los sistemas de seguridad según administrativos* 58

3.17. *Efectividad de los sistemas de seguridad según los docentes.* 59

3.18. *Efectividad de los sistemas de seguridad según el personal según los estudiantes.* 59

3.19. *Suficiencia de los controles de acceso según el personal administrativo.* 61

3.20. *Suficiencia de los controles de acces según los docentes.* 61

3.21. *Suficiencia de los controles de acces según los estudiantes.* 62

3.22. *Percepción sobre la seguridad inteligente según personal administrativo* . . . 63

3.23. *Percepción sobre la seguridad inteligente según docentes.* 64

3.24. *Percepción sobre la seguridad inteligente según estudiantes.* 64

3.25. *Comodidad conla identificación biométrica según personal administrativo.* . . 66

3.26. *Comodidad conla identificación biométrica según docentes.* 66

3.27. *Comodidad conla identificación biométrica según estudiantes.* 67

3.28. *Ambientes que requieren sistemas de control de acceso según personal administrativo* 68

3.29. *Ambientes que requieren sistemas de control de acceso según docentes.* 69

3.30. *Ambientes que requieren sistemas de control de acceso según estudiantes.* . . 70

3.31. *Componentes más importantes para un sistema de seguridad según administrativoS.* 71

3.32. *Componentes más importantes para un sistema de seguridad segun docentes.* 72

3.33. *Componentes más importantes para un sistema de seguridad según estudiantes.* 73

3.34. *Preocupación sobre la privacidad de los datos personales según administrativos.* 74

3.35. *Preocupación sobre la privacidad de los datos personales según docentes.* . . . 75

3.36. *Preocupación sobre la privacidad de los datos personales según estudiantes.* . 75

3.37. *Confianza en la gestión de datos personales según personal administrativo.* . 77

3.38. *Confianza en la gestión de datos personales según docentes.* 77

3.39. *Confianza en la gestión de datos personales según estudiantes.* 78

5.1. *Calculo de almacenamiento* 102

Índice de tablas

1.1. *Distribución de participantes por categoría* 12

3.1. *Casos reportados de incidentes de seguridad en el pabellón.* 50

4.1. *Distribución de ambientes y equipos por piso del pabellón de Ingeniería* . . . 81

4.2. *Percepción del nivel de seguridad del pabellón* 83

4.3. *Experiencias personales sobre incidentes de seguridad* 83

4.4. *Percepción de la efectividad de la situación actual* 84

5.1. *Niveles DORI aplicados a cámaras de 4MP* 96

5.2. *Distribución de cámaras IP* 97

5.3. *Especificaciones técnicas recomendadas de la cámaras* 105

5.4. *Especificaciones técnicas del videograbador* 106

5.5. *Especificaciones técnicas del switch principal* 106

5.6. *Especificaciones técnicas del switch PoE* 106

5.7. *Especificaciones técnicas del cable UTP Cat6* 107

5.8. *Control de acceso propuesto – Segundo piso* 109

5.9. *Control de acceso propuesto – Tercer piso* 109

5.10. *Control de acceso propuesto – Cuarto piso* 110

5.11. *Resumen de controles de acceso propuestos por piso* 110

5.12. *Especificaciones tecnicas deL control de acceso* 114

5.13. *Distribución del sistema de alarmas – Segundo piso* 116

5.14. *Distribución del sistema de alarmas – Tercer piso* 116

5.15. *Distribución del sistema de alarmas – Cuarto piso* 116

5.16. *Distribución del sistema de alarmas – Sirenas* 116

5.17. *Resumen del sistema de alarmas propuesto* 116

5.18. *Especificaciones técnicas del panel de alarma* 121

5.19. *Especificaciones técnicas de la sirena electrónica* 121

5.20. *Especificaciones técnicas del sensor PIR* 121

5.21. *Especificaciones técnicas del cableado para alarmas* 122

5.22. *Especificaciones de la Workstation de Monitoreo* 127

5.23. *Distribución y especificaciones de monitores* 127

5.24. *Listado de Equipos de Videovigilancia* 134

5.25. *Listado de Equipos de Sistema de Alarma* 134

5.26. *Listado de Equipos de Control de Acceso* 135

5.27. *Listado de Materiales Compartidos* 135

5.28. *Resumen general del presupuesto* 135

5.29. Matriz de trazabilidad normativa de los requerimientos técnicos 136

6.1. *Matriz de identificación de datos personales* 139

6.2. *Matriz de riesgos en el tratamiento de datos personales* 140

6.3. *Clasificación de Incidentes de Seguridad* 142

6.4. *Contingencias ante fallas del sistema de acceso* 144

6.5. *Checklist de verificación de equipos de seguridad* 145

6.6. *Lista de verificación de controles de seguridad y privacidad* 147

6.7. *Registro General de Incidentes de Seguridad* 148

6.8. *Lista de verificación de controles de seguridad y privacidad* 148

7.1. *Matriz de operacionalización* 168

Capítulo 1

Aspectos Generales

1.1. Planteamiento del Problema

1.1.1. Descripción del problema

La inseguridad es un problema mundial muy complejo que genera sensación de miedo y desconfianza en la sociedad y esta presente en diferentes contextos, en las calles en nuestro hogar, lugar de estudio, centro de trabajo; todos estamos expuestos y propensos a sufrir robos, hurtos, violencia y daños en nuestra propiedad o lugar donde habitamos. En el Perú según el informe de percepción de inseguridad ciudadana del año 2024, elaborado por el INEI, incrementó de 82.6 a 86.1 % que está comprendido en el semestre de enero a junio de 2024 a nivel nacional respecto al año 2023, esto quiere decir que hay un crecimiento de 4.5 %; esto nos da una cifra muy alarmante ya que los ciudadanos cada vez se sienten menos seguros. Los robos, hurtos, violencia, acoso, daños físicos daños contra el patrimonio, nos hacen buscar e implementar soluciones que nos ayuden a sentirnos más seguros.

Según el decreto legislativo N°1218 en el capítulo II " Videovigilancia En Bienes De Dominio Público, Vehículos De Servicio De Transporte Público De Pasajeros Y Establecimientos Comerciales Abiertos Al Público", en el artículo 7.- Uso de cámaras

de videovigilancia en bienes de dominio público nos indica: “Las personas naturales o jurídicas, públicas o privadas que administren bienes de dominio público deben instalar cámaras de videovigilancia, bajo los estándares técnicos establecidos en el reglamento del presente Decreto Legislativo, para contribuir a la seguridad ciudadana y articularse con la Policía Nacional del Perú y las Gerencias de Seguridad Ciudadana de las municipalidades o la que hagan sus veces. La instalación de cámaras de videovigilancia debe responder al planeamiento territorial y de desarrollo urbano y rural, así como a los planes distritales de seguridad ciudadana. Las cámaras de videovigilancia son utilizadas en playas, plazas, parques, infraestructura vial, vías férreas, caminos, sedes gubernativas e institucionales, escuelas, hospitales, estadios, bienes afectados en uso a la defensa nacional, establecimientos penitenciarios, espacios culturales, cementerios, puertos, aeropuertos y otros destinados al cumplimiento de los fines de responsabilidad estatal, o cuya concesión compete al Estado” (Congreso de la República del Perú, 2015).

Este decreto nos hace ver la necesidad de implementar sistemas de videovigilancia que nos ayuden a tener pruebas o evitar algún hecho desafortunado ya que existe una cifra negra de delitos cometidos que no han llegado a ser descubiertos o condenados debido a la falta de pruebas.

Otra cifra preocupante son los casos de bullyng o acoso en las instituciones educativas ya que cada vez va en aumento, por lo cual se instó a las instituciones que realicen la instalación de sistemas de seguridad de videovigilancia para así tener mejor control de los sucesos además tener información y conocimiento de los implicados en este tipo de casos. También ocurren sucesos mucho peores cabe mencionar como ejemplo que el año del 2019 ocurrió un atentado a una joven por parte de su enamorado dentro de la UNSA de Arequipa, Otro hecho que conmocionó a la ciudadanía es el asesinato de un joven de 19 años en el Instituto Khipu del Cusco.

Las universidades, institutos, están propensos a sufrir diferentes tipos de daños a las personas, los bienes y la infraestructura , debido a que la afluencia de personas es numerosa y es imposible tener el control completo de cada espacio además no se puede controlar el acceso de personas externas que puedan causar daños. Al realizar pequeñas entrevistas a los vigilantes del campus universitario de la UNSAAC se pudo evidenciar los robos que ocurren en nuestra universidad, también casos de violencia, daños contra el patrimonio e indicaron que un sistema de videovigilancia sería de gran apoyo en sus tareas.Asimismo, se identificó la necesidad de fortalecer los mecanismos de supervisión ante situaciones que puedan afectar la seguridad y convivencia dentro del pabellón, tales como alteraciones del orden, discusiones o incidentes entre usuarios.

1.1.2. Identificación del problema

El pabellón de la Escuela Profesional de Ingeniería Informática y de Sistemas no cuenta con un sistema de seguridad adecuado que garantice la protección de los estudiantes, docentes y demás personas que desarrollan actividades dentro de la institución. Asimismo, presenta limitaciones en las medidas de resguardo destinadas a la protección de la infraestructura y de los bienes materiales, como máquinas, laboratorios y equipos especializados, los cuales resultan fundamentales para el desarrollo académico y profesional de los estudiantes.

Ante esta problemática, se plantea la proyección de un sistema de seguridad electrónica como una alternativa viable, mediante el aprovechamiento de recursos tecnológicos como cámaras de videovigilancia, sensores, alarmas y controles de acceso. La configuración de estos componentes permite establecer mecanismos orientados a la prevención de incidentes y a la mejora de la capacidad de respuesta frente a posibles amenazas. Además, la integración de dichos sistemas con plataformas digitales facilita la supervisión y gestión centralizada de

la seguridad.

La formulación de un sistema de seguridad electrónica no solo contribuye a definir medidas orientadas a reducir el riesgo de robos o daños a los equipos, sino también a plantear un entorno más seguro y confiable para la comunidad universitaria. Mediante la incorporación de mecanismos de monitoreo y alertas, se establecen lineamientos para una respuesta más eficiente ante eventos sospechosos, fortaleciendo la percepción de seguridad de estudiantes y docentes. Asimismo, la estructuración de registros de acceso y actividad dentro de los laboratorios facilita un mejor control del uso de los recursos, ayudando a prevenir el uso indebido de los equipos y el acceso no autorizado a zonas restringidas.

Otro aspecto relevante del desarrollo teórico del sistema de seguridad electrónica es la posibilidad de integrar herramientas de inteligencia artificial y análisis de datos para optimizar la detección de incidentes. A través de algoritmos de análisis, la plataforma puede identificar comportamientos inusuales y contribuir al planteamiento de estrategias de respuesta ante situaciones de emergencia. Asimismo, la propuesta contempla la generación de reportes sobre el estado de seguridad, lo que favorece la toma de decisiones y la mejora continua de los protocolos de protección dentro de la escuela profesional.

Finalmente, el diseño de un sistema de seguridad electrónica representa una iniciativa que no solo se orienta a la protección de bienes y personas, sino también al fortalecimiento de la imagen institucional. Una institución que prioriza la seguridad evidencia su compromiso con la calidad educativa y el bienestar de su comunidad universitaria. En este sentido, esta solución tecnológica constituye una alternativa moderna y eficiente para contribuir al desarrollo de un entorno académico más protegido, organizado y confiable.

1.2. Formulación del Problema

1.2.1. Problema General

¿De qué manera se puede fortalecer la supervisión, el control de accesos y la respuesta ante situaciones de riesgo en el pabellón de Ingeniería Informática y de Sistemas?

1.2.2. Problemas Específicos

- ¿Cómo optimizar el monitoreo visual y la cobertura de seguridad en las áreas críticas y vulnerables del pabellón?
- ¿Cuáles deben ser los mecanismos de autenticación y restricciones de flujo idóneos para salvaguardar los ambientes de acceso restringido del pabellón?
- ¿De qué forma se puede garantizar una oportuna detección de incidentes y alertamiento temprano ante los riesgos que amenazan las instalaciones del pabellón?
- ¿Cómo superar la falta de articulación y centralización entre las distintas herramientas de control y monitoreo de seguridad existentes en el pabellón?
- ¿Cómo establecer lineamientos para garantizar el tratamiento adecuado de los datos personales generados por el sistema integrado de seguridad electrónica, conforme a la normativa vigente?

1.3. Objetivos

1.3.1. Objetivo General

Diseñar un sistema integrado de seguridad electrónica basado en tecnologías IoT para el pabellón de Ingeniería Informática y de Sistemas.

1.3.2. Objetivos Específicos

- Diseñar un subsistema de videovigilancia inteligente para las áreas críticas del pabellón, considerando criterios de cobertura, supervisión y almacenamiento.
- Diseñar un subsistema inteligente de control de accesos para las áreas de uso restringido, considerando mecanismos de autenticación y gestión de accesos.
- Diseñar un subsistema de alarmas orientado a la detección y respuesta ante riesgos dentro de las instalaciones del pabellón.
- Integrar los subsistemas de videovigilancia, control de accesos y alarmas mediante una plataforma de gestión unificada.
- Diseñar los lineamientos, procedimientos y documentos de gestión necesarios para garantizar el tratamiento adecuado de los datos personales generados por el sistema integrado de seguridad electrónica, conforme a la normativa vigente.

1.4. Justificación

La seguridad del pabellón de ingeniería constituye un aspecto crítico que requiere un análisis técnico detallado de sus necesidades específicas, así como la identificación de sus áreas vulnerables. En este contexto, la presente investigación se justifica en el desarrollo consolidado de un diseño integral de un sistema de seguridad inteligente, el cual establece soluciones tecnológicas adecuadas sin implicar su implementación directa.

El estudio aporta una propuesta estructurada que comprende el diseño de un subsistema de videovigilancia inteligente, orientado al monitoreo continuo de áreas críticas, así como un sistema de alarmas de intrusión y detección de emergencias, enfocado en la prevención y respuesta ante riesgos. Ambos componentes se encuentran definidos a partir de

criterios técnicos, normativos y operativos, asegurando su viabilidad y adecuación al entorno.

Asimismo, la investigación determina los parámetros técnicos para un sistema de control de acceso inteligente, destinado a regular el ingreso a zonas restringidas, fortaleciendo la seguridad y el control del flujo de usuarios dentro del pabellón. Este diseño establece mecanismos eficientes de autenticación y autorización, contribuyendo directamente a la protección de los recursos físicos y humanos.

De igual manera, se configura la integración de los subsistemas de seguridad en una plataforma de gestión unificada basada en protocolos IoT, lo cual facilita la centralización del monitoreo, la interoperabilidad entre dispositivos y la optimización de la toma de decisiones en materia de seguridad.

Adicionalmente, el desarrollo de los planos técnicos y esquemas de distribución documenta de manera precisa la ubicación y configuración de los equipos, constituyendo la base fundamental para una futura implementación. A ello se suma la elaboración de lineamientos de gestión y manuales de procedimientos operativos, los cuales orientan la correcta administración, operación y mantenimiento del sistema propuesto.

En conjunto, esta investigación ofrece un diseño técnico integral que sirve como guía para la futura implementación de un sistema de seguridad inteligente, contribuyendo no solo a la protección de los bienes e instalaciones del pabellón, sino también al monitoreo y respuesta ante incidentes que comprometan la seguridad y el orden dentro de los ambientes universitarios. Asimismo, optimiza la gestión de riesgos y fortalece la planificación de infraestructuras seguras en entornos académicos

1.4.1. Conveniencia

El estudio de un sistema integrado de seguridad electrónica basado en IoT es conveniente porque permite proponer una solución técnica innovadora para mejorar la

protección de instalaciones académicas. Este diseño contribuye al desarrollo académico al integrar tecnologías emergentes, optimizar recursos y fortalecer el conocimiento en áreas como seguridad, redes e Internet de las Cosas. Además, representa una base sólida para futuras investigaciones o proyectos orientados a la transformación digital de los espacios educativos.

1.4.2. Relevancia

Responde a la necesidad de fortalecer la protección de los espacios académicos ante riesgos como robos, accesos no autorizados y emergencias. La creciente digitalización de las instituciones educativas exige soluciones tecnológicas más eficientes, inteligentes y centralizadas. Este estudio busca aprovechar las ventajas del Internet de las Cosas para integrar sensores, cámaras, alarmas y controles de acceso en una sola plataforma, mejorando así la gestión de la seguridad y optimizando los recursos disponibles. Además, permite aplicar conocimientos multidisciplinarios y aporta una propuesta concreta que puede guiar futuras implementaciones en entornos similares.

1.4.3. Implicancias Prácticas

A futuro, este diseño podrá ser utilizado como una base técnica y conceptual para implementar sistemas de seguridad integrados en otros pabellones, laboratorios o instituciones similares. Asimismo servirá como referencia para nuevas investigaciones relacionadas con la aplicación de tecnologías IoT en entornos educativos. Su enfoque modular y escalable facilita la adaptación a distintos contextos, permitiendo que futuras generaciones de estudiantes o profesionales lo mejoren, amplíen o implementen según las necesidades específicas de cada espacio.

1.4.4. Valor Teórico

Este trabajo aporta al ambito académico al desarrollar un enfoque teórico y metodológico para el diseño de sistemas de seguridad electrónica basados en IoT, integrando conocimientos de informática, electrónica y telecomunicaciones. Su valor teórico radica en la propuesta de una arquitectura modular, escalable e interoperable que puede ser aplicada, analizada o adaptada en diferentes contextos académicos o industriales. Además, contribuye a la literatura técnica sobre seguridad inteligente en entornos educativos, ofreciendo una base para futuras investigaciones, comparaciones tecnológicas o mejoras en soluciones de protección automatizada.

1.4.5. Utilidad Metodológica

La utilidad metodológica de este estudio radica en que ofrece un modelo estructurado para el diseño de sistemas de seguridad electrónica integrados, que puede ser reutilizado y adaptado en proyectos similares. La metodología propuesta que abarca desde el análisis de necesidades hasta el diseño de la arquitectura tecnológica y la selección de dispositivos IoT puede servir como guía para futuros trabajos académicos, investigaciones aplicadas o implementaciones reales en diferentes instituciones. Esto permite replicar el enfoque en diversos escenarios, optimizando tiempos de desarrollo y mejorando la toma de decisiones técnicas en proyectos de seguridad.

1.5. Delimitación de Estudio

1.5.1. Delimitación Espacial

El estudio se limitará al Pabellón de Ingeniería Informática y de Sistemas de la Universidad Nacional de San Antonio Abad del Cusco.

1.5.2. Delimitación Temporal

Este estudio se desarrolló durante el periodo comprendido entre enero 2025 y abril del año 2026, abarcando todas las etapas. El diseño propuesto responde a las condiciones tecnológicas y académicas vigentes en ese marco temporal.

1.6. Metodología

1.6.1. Enfoque

La investigación presenta un enfoque cuantitativo, debido a que se recopilarán y analizarán datos numéricos obtenidos mediante encuestas y evaluaciones técnicas, con el propósito de medir y determinar las necesidades de seguridad del pabellón de Ingeniería Informática y de Sistemas (Hernández-Sampieri and Mendoza Torres, 2023).

1.6.2. Alcance

La presente investigación es de alcance descriptivo ya que se orienta al analisis de las condiciones de seguridad del pabellón y la identificación de sus areas criticas (Hernández-Sampieri and Mendoza Torres, 2023). Asimismo posee un componente propositivo debido a que se plantea el diseño de una solución tecnológica basada en IoT para la seguridad universitaria, definiendo la integración y funcionamiento de sus componentes desde una perspectiva técnica.

1.6.3. Diseño de Investigación

El estudio se desarrolla bajo un diseño no experimental de corte transversal, debido a que no se manipulan las variables de estudio ni se realizan experimentaciones en un entorno controlado. Asimismo, la información requerida para el análisis de las condiciones de

seguridad y el planteamiento de la propuesta tecnológica fue recopilada en un único momento temporal, permitiendo evaluar la situación existente del pabellón para el desarrollo del diseño del sistema de seguridad inteligente. (Hernández-Sampieri and Mendoza Torres, 2023).

La presente investigación se desarrolló bajo un diseño no experimental de tipo descriptivo con alcance propositivo.

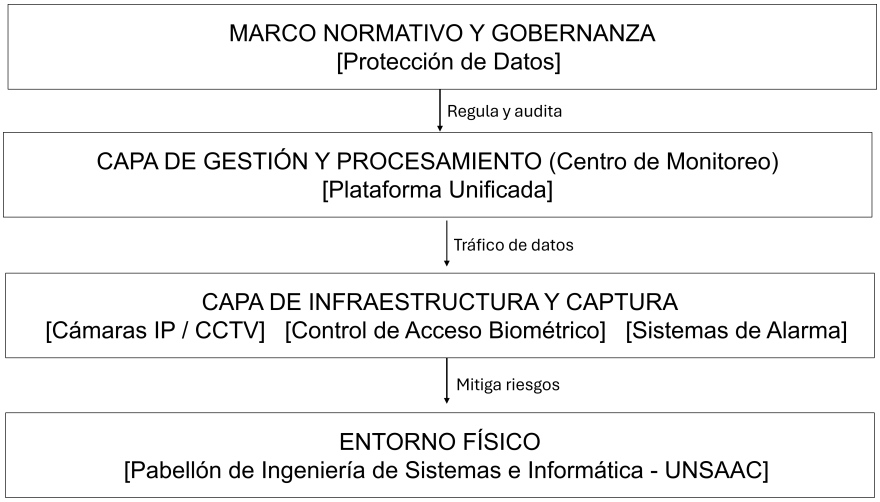
La fase descriptiva estuvo orientada al diagnóstico de la situación actual de seguridad del pabellón de Ingeniería Informática y de Sistemas. En esta etapa se identificaron las características de la infraestructura, los activos a proteger, las vulnerabilidades existentes, los riesgos percibidos y los requerimientos de seguridad mediante la aplicación de instrumentos de recolección de datos y la observación del entorno.

A partir de los resultados obtenidos en el diagnóstico, se desarrolló la fase propositiva, la cual consistió en el diseño de un sistema integrado de seguridad electrónica basado en IoT. Esta fase comprendió la definición de la arquitectura del sistema, la selección de tecnologías, el diseño de los subsistemas de videovigilancia, control de acceso y detección de intrusión, así como la elaboración de los planos, especificaciones técnicas y criterios normativos que sustentan la propuesta.

En consecuencia, la investigación no contempla la implementación ni la evaluación experimental del sistema diseñado, limitándose al diagnóstico de la situación actual y al desarrollo de una propuesta técnica sustentada en los requerimientos identificados.

1.7. Diagrama del Modelo Conceptual

Figura 1.1: *Modelo conceptual*



1.7.1. Poblacion y Muestra

Estos datos representan a todos los miembros activos de la institución durante el semestre 2025-I, abarcando a estudiantes matriculados, docentes con asignación académica y personal administrativo en funciones.

En el pabellón de Ingeniería Informática y de Sistemas, la población se organizo en tres categorías, como se detalla en el siguiente cuadro:

Tabla 1.1: *Distribución de participantes por categoría*

Categoría	**Cantidad**
Docentes	60
Estudiantes	478
Administrativos	6
Total	544

Nota. Los datos son de acuerdo al semestre 2025-I.

Cálculo del tamaño de la muestra para docentes

Para determinar el tamaño óptimo de la muestra de docentes, se aplicó la fórmula para poblaciones finitas, considerando los siguientes parámetros:

- **Tamaño de la población (N):** 60 docentes
- **Nivel de Confianza (NC):** 90 % ($Z = 1{,}645$)
- **Margen de Error (e):** 10 % (0.10)
- **Proporción de Éxito (p):** 0.5 (asumido, ya que no se conoce la proporción real, lo que maximiza el tamaño de la muestra)
- **Proporción de Fracaso (q):** 0.5 ($1 - p$)

La fórmula utilizada para el cálculo del tamaño de la muestra (n) en una población finita es:

$$n = \frac{N \cdot Z^2 \cdot p \cdot q}{(N-1) \cdot e^2 + Z^2 \cdot p \cdot q} \tag{1.1}$$

Sustituyendo los valores en la fórmula, obtenemos:

$$n = \frac{60 \cdot (1{,}645)^2 \cdot 0{,}5 \cdot 0{,}5}{(60-1) \cdot (0{,}10)^2 + (1{,}645)^2 \cdot 0{,}5 \cdot 0{,}5} \tag{1.2}$$

$$n = \frac{60 \cdot 2{,}706025 \cdot 0{,}25}{59 \cdot 0{,}01 + 2{,}706025 \cdot 0{,}25} \tag{1.3}$$

$$n = \frac{40{,}590375}{0{,}59 + 0{,}67650625} \tag{1.4}$$

$$n = \frac{40{,}590375}{1{,}26650625} \tag{1.5}$$

$$n \approx 32{,}049 \tag{1.6}$$

Considerando que el tamaño de la muestra debe ser un número entero de personas, se redondea al número entero superior para asegurar la representatividad.

Por lo tanto, el tamaño de la muestra requerido es de **32 docentes**.

Cálculo del tamaño de la muestra para personal Administrativo

Dado que la población total es de solo 6 personas, se optó por entrevistar a todas ellas en lugar de seleccionar una muestra.

Cálculo del tamaño de la muestra para estudiantes

Para determinar el tamaño óptimo de la muestra de estudiantes, se aplicó la fórmula para poblaciones finitas, considerando los siguientes parámetros:

Para determinar el tamaño de la muestra, se consideran los siguientes parámetros:

- **Tamaño de la población (N):** 478 estudiantes
- **Nivel de Confianza (NC):** 95 % ($Z = 1{,}96$)
- **Margen de Error (e):** 10 % (0.10)
- **Proporción de Éxito (p):** 0.5 (asumido)
- **Proporción de Fracaso (q):** 0.5 ($1 - p$)

La fórmula utilizada para el cálculo del tamaño de la muestra (n) en una población finita es:

$$n = \frac{N \cdot Z^2 \cdot p \cdot q}{(N-1) \cdot e^2 + Z^2 \cdot p \cdot q} \tag{1.7}$$

Sustituyendo los valores en la fórmula, obtenemos:

$$n = \frac{478 \cdot (1{,}96)^2 \cdot 0{,}5 \cdot 0{,}5}{(478-1) \cdot (0{,}10)^2 + (1{,}96)^2 \cdot 0{,}5 \cdot 0{,}5} \tag{1.8}$$

$$n = \frac{478 \cdot 3{,}8416 \cdot 0{,}25}{477 \cdot 0{,}01 + 3{,}8416 \cdot 0{,}25} \tag{1.9}$$

$$n = \frac{459{,}0712}{4{,}77 + 0{,}9604} \tag{1.10}$$

$$n = \frac{459{,}0712}{5{,}7304} \tag{1.11}$$

$$n \approx 80{,}11 \tag{1.12}$$

Considerando que el tamaño de la muestra debe ser un número entero de personas, se redondea al número entero superior para asegurar la representatividad.

Por lo tanto, el tamaño de la muestra requerido es de **81 estudiantes**.

Capítulo 2

Marco Teórico

2.1. Antecedentes

Báez Buelvas D. M, (2019),*Implementación de un Sistema de Video Vigilancia a Través de Cámaras de Seguridad para los Laboratorios de la Facultad de Ingeniería Electrónica*, Universidad Santo Tomas,Colombia.

Conclusiones

La tesis demuestra que la ubicación estratégica de cámaras de seguridad para una cobertura óptima se fundamenta en la combinación de la distancia focal, el tipo de cámara y la definición clara del objetivo de vigilancia, siendo recomendable el uso de software de visualización de campo de visión. A través del diseño e instalación de un sistema de video vigilancia de 9 cámaras en los 6 laboratorios de la Facultad de Ingeniería Electrónica, la tesis aplicó estos principios para determinar los mejores emplazamientos, logrando maximizar la cobertura de las áreas con los recursos disponibles y minimizando los puntos ciegos en cada laboratorio(Báez Buelvas, 2019).

Comentario:

Esta tesis constituye un aporte integral a la presente investigación al proporcionar un modelo metodológico mixto que vincula la percepción de seguridad con la ejecución técnica. Asimismo, su enfoque operativo sobre la selección de materiales y protocolos de instalación ofrece una guía práctica para asegurar la viabilidad técnica y la eficiencia en el despliegue del sistema de videovigilancia propuesto..

Francisco Atl. Aceves Bernal, (2013),*Sistema de Videovigilancia para la Ciudad de México*, Instituto Politécnico Nacional, Escuela Superior De Ingeniería Mecánica Y Eléctrica Sección De Estudios De Posgrado e Investigación, Mexico.

Conclusiones:

La implementación de sistemas de videovigilancia en ciudades como la Ciudad de México ha demostrado ser efectiva, reduciendo los índices delictivos en un 12 %, especialmente cuando se integran tecnologías inteligentes para la detección automática de incidentes. No obstante, esta medida resulta insuficiente por sí sola y debe ser complementada con soluciones sociales, económicas, culturales y educativas. Se propone una respuesta cívica y moral a través de campañas de concientización y justicia social, así como una solución política que incluya mayor inversión en seguridad, reformas que garanticen acceso a la educación y empleo digno, pensiones adecuadas para adultos mayores y seguros de desempleo, atacando así las causas estructurales de la delincuencia.

Comentario: Como se pude evidenciar en esta tesis se comprobó que la hipótesis aplicando el modelo propuesto para el diseño de sistemas de videovigilancia,se logra dar solución a la problemática de inseguridad en la Ciudad de México,manifestándose una reducción en los niveles del índice delictivo.

Cynthia Teresa Perez Morris, (2016),*Diseño de un sistema de seguridad electrónica con monitoreo centralizado para protección de una instalación minera*, Pontificia Universidad Católica del Perú, Perú.

Conclusiones

El diseño de un sistema de monitoreo centralizado de seguridad para una instalación minera promete reducir hurtos y daños al permitir un control unificado. Un análisis de costo-beneficio proyecta un retorno de la inversión en 13 meses optimizando el personal de seguridad, en contraste con 19 meses manteniendo la plantilla actual. Si bien el sistema podría ser más robusto con mayor inversión en redundancia, los equipos seleccionados cumplen los requerimientos del cliente. El sistema tiene una escalabilidad del 25 %, limitada actualmente por la capacidad del servidor de grabación (2TB). Aunque los switches de 10GB están sobredimensionados para la red de fibra de 1GB, el ancho de banda de la fibra óptica (1GB) es suficiente para las 21 cámaras con una resolución de 4CIF recomendada, asegurando la transmisión de video y el almacenamiento de 30 días(Perez Morris, 2016).

Comentario: Esta investigación aporta criterios fundamentales para el diseño del centro de monitoreo unificado y la arquitectura de red necesaria para centralizar el flujo de datos de seguridad. El estudio destaca por la implementación de anillos de seguridad, concepto que permite jerarquizar la protección desde el perímetro hasta las áreas.

Edgar Junior Gonzales Rodriguez, (2024),*Implementación de los sistemas de seguridad electrónica en los locales nuevos de la entidad financiera Caja Cusco*,Universidad Nacional de San Antonio Abad del Cusco, Perú.

Conclusiones

El trabajo evidenció que la implementación sistemática de sistemas de seguridad electrónica en las nuevas agencias de Caja Cusco no solo optimiza la protección física de los activos, sino que establece un modelo de arquitectura de red unificada y centralizada. A través de la documentación detallada de las etapas de diseño, ingeniería de detalle, instalación y comisionamiento (pruebas de funcionamiento), se logró consolidar una solución integral de seguridad. Esta infraestructura garantiza altos niveles de disponibilidad y redundancia en subsistemas críticos como la videovigilancia IP (CCTV), el control de accesos biométrico y los sistemas de detección de intrusión e incendios, logrando una mitigación eficiente de las vulnerabilidades operativas detectadas en el análisis de riesgos previo (Gonzales Rodriguez, 2024).

Asimismo, el proyecto demostró la viabilidad técnica de integrar plataformas multimarca bajo protocolos de comunicación estandarizados, lo que reduce la latencia en la transmisión de alertas hacia el centro de monitoreo principal y optimiza el consumo del ancho de banda en los enlaces de datos de la entidad financiera. Finalmente, se verificó que el despliegue tecnológico no solo cumple con las buenas prácticas de la ingeniería de sistemas, sino que se alinea estrictamente con los estándares internacionales de seguridad de la información y la normativa regulatoria vigente impuesta por la Superintendencia de Banca, Seguros y AFP (SBS) para entornos bancarios en el Perú, asegurando la trazabilidad y la protección de datos sensibles (Gonzales Rodriguez, 2024).

Comentario: Este trabajo aporta a la presente investigación como referencia para el diseño e integración de sistemas de seguridad electrónica en entornos institucionales, especialmente en aspectos relacionados con la implementación de videovigilancia, control de acceso y alarmas. Asimismo, sirve como base para considerar criterios de supervisión, pruebas de

funcionamiento y cumplimiento normativo dentro de la propuesta del sistema de seguridad electrónica.

Lyon David , (2022),*Surveillance*, Internet Policy Review,Alexander von Humboldt Institute for Internet and Society, Alemania.

Conclusiones

El estudio concluye que los sistemas contemporáneos de vigilancia y monitoreo han dejado de ser herramientas pasivas de supervisión para convertirse en infraestructuras digitales complejas basadas en la recopilación masiva y el análisis algorítmico de datos. Frente a este panorama, Lyon (Lyon, 2022) enfatiza que no basta con buscar un equilibrio superficial entre la seguridad institucional y la privacidad individual; se requiere una reconfiguración estructural de la gobernanza tecnológica.

En este sentido, se destaca la urgencia de implementar marcos normativos y medidas de control transnacionales que no solo regulen el tratamiento adecuado de los datos personales, sino que también limiten la capacidad de las corporaciones y los Estados para clasificar, predecir y manipular el comportamiento humano. En última instancia, la supervisión de estas tecnologías debe orientarse hacia la justicia social y la rendición de cuentas, evitando que la vigilancia digital perpetúe las asimetrías de poder y la erosión de los derechos fundamentales en el entorno conectado (Lyon, 2022).

Comentario: Este trabajo aporta a la presente investigación fundamentos teóricos relacionados con la vigilancia tecnológica, la protección de datos personales y el impacto del monitoreo digital en entornos institucionales. Además, sirve como referencia para considerar aspectos de privacidad y tratamiento de información en el diseño de sistemas de seguridad electrónica.

Changoluisa Sibitanga Diego A, Pallo Toaquiza Luz Nelly, (2017),*Cualificación y Certificación*

de la Red LAN con Cableado Estructurado Basado en Normas Internacionales ANSI/TIA/EIA 568 – B2, en el Laboratorio de Investigación de Ingeniería de Software, en el año 2017, Universidad Tecnica de Cotopaxi, Ecuador.

Conclusiones

Se concluyó que el diseño, implementación y posterior certificación de la red LAN bajo las normativas internacionales ANSI/TIA/EIA 568-B2 reduce drásticamente las fallas físicas por atenuación, diafonía (NEXT/FEXT) y pérdida de paquetes. El proceso de cualificación técnica no solo validó la continuidad del mapa de cableado, sino que garantizó que los enlaces canal y permanente operen al máximo rendimiento de su categoría, proporcionando una infraestructura de comunicación y seguridad electrónica altamente robusta, escalable y de fácil administración.

Asimismo, se determinó que contar con una red rigurosamente certificada en un entorno académico y de investigación especializado —como el Laboratorio de Ingeniería de Software— es un factor crítico. Esto asegura el ancho de banda y la estabilidad requeridos para el despliegue de entornos virtuales, pruebas de software concurrentes y transferencia de grandes volúmenes de datos, mitigando los tiempos de inactividad y optimizando los recursos operativos de la institución (Sibitanga and Toaquiza, 2017).

Comentario: Este antecedente aporta el criterio técnico para garantizar la continuidad de los sistemas integrados mediante una red estandarizada. Utiliza la norma ANSI/TIA/EIA 568 para regular los medios de transmisión y asegurar el ancho de banda, y la norma TIA/EIA 569 para diseñar canalizaciones y espacios técnicos. Esta última protege el cableado de daños físicos y de la interferencia electromagnética (EMI), asegurando la estabilidad y escalabilidad de toda la infraestructura de seguridad e informática.

2.2. Bases Teóricas

2.2.1. Sistemas de Seguridad Electrónica

Los sistemas de seguridad electrónica se definen como un ecosistema integrado de dispositivos y tecnologías diseñadas para la protección de activos y personas en un espacio físico. Según su arquitectura, estos sistemas permiten monitorear, detectar y responder ante incidentes de manera automatizada. En la presente investigación, los SSE se abordan desde tres subsistemas convergentes:

Sistemas de Videovigilancia sobre IP

Constituyen la capa de supervisión visual y captura de evidencia. A diferencia de los sistemas analógicos tradicionales, la videovigilancia IP utiliza la red de datos para la transmisión de paquetes de video. Sus componentes esenciales son:

- **Cámaras de Seguridad IP:** Dispositivos de borde que capturan y digitalizan la luz mediante sensores de alta resolución (4MP).
- **Video Management System (VMS):** Capa de software encargada de la lógica de administración, visualización y orquestación del sistema.
- **Gestión de Almacenamiento:** Uso de grabadores de red (NVR) y unidades de disco de alta disponibilidad para garantizar la persistencia de los datos.

Sistemas de Control de Acceso y Alarmas

Estos subsistemas regulan el tránsito de personas y detectan accesos no autorizados. La integración de ambos permite una respuesta reactiva (sirenas y alertas) y una gestión proactiva mediante dispositivos de identificación como lectoras biométricas, teclados y cerraduras electromagnéticas controladas por actuadores(Inria Chile and Baccelli, 2021).

2.2.2. Internet de las Cosas (IoT) en la Seguridad

El Internet de las Cosas (IoT) representa una red de dispositivos interconectados que se comunican entre sí y con servicios en la nube. Esta tecnología permite que dispositivos con recursos limitados recolecten datos mediante sensores y respondan de forma automatizada (Inria Chile and Baccelli, 2021).

Según Inria Chile and Baccelli (2021), el funcionamiento del ecosistema IoT se basa en tres pilares:

1. **Dispositivos Inteligentes:** Hardware dotado de capacidades de computación y conectividad (ej. cámaras IP).

2. **Aplicación de IoT:** Software que utiliza técnicas de *Machine Learning* o Inteligencia Artificial para analizar los datos recibidos y tomar decisiones informadas.

3. **Interfaz de Usuario:** Capa gráfica que permite la administración de la flota de dispositivos mediante aplicaciones móviles o plataformas web.

2.2.3. Inteligencia Artificial Aplicada a la Seguridad

La Inteligencia Artificial (IA) ha transformado los sistemas de seguridad al dotarlos de capacidades analíticas proactivas, permitiendo la toma de decisiones en tiempo real sin intervención humana constante(**?**).

Análisis de Video Inteligente

Emplea algoritmos de visión computacional, como Redes Neuronales Convolucionales (CNN), para interpretar los flujos de video. Sus funciones técnicas incluyen:

- **Clasificación de Objetos:** Capacidad para diferenciar entre humanos, vehículos y animales, reduciendo las falsas alarmas.

- **Detección de Anomalías:** Identificación de comportamientos que se desvían de los patrones normales, como el merodeo o el acceso en horarios no permitidos.
- **Filtros de Eventos:** Funciones de cruce de línea virtual y detección de intrusión perimetral.

Reconocimiento Facial y Biometría

Esta tecnología se basa en la extracción de características faciales mediante modelos de aprendizaje profundo para generar *embeddings* o vectores numéricos únicos. Estos permiten la comparación biométrica contra bases de datos en milisegundos, facilitando un control de acceso eficiente y el registro automatizado de asistencias en entornos institucionales de alta densidad, como los pabellones universitarios(Inria Chile and Baccelli, 2021).

2.2.4. Consideraciones de Ciberseguridad y Privacidad

Debido a la naturaleza interconectada de los sistemas basados en IoT e IA, es imperativo implementar protocolos de ciberseguridad para proteger la integridad de los datos. Asimismo, la implementación de estos sistemas en el marco de la videovigilancia debe alinearse con la normativa de protección de datos personales, asegurando que la recopilación de datos biométricos sea transparente y segura(Inria Chile and Baccelli, 2021).

2.2.5. Plataforma de Gestión de Seguridad Unificada

El concepto de plataforma de gestión unificada constituye el pilar lógico sobre el cual se estructuran los sistemas de protección física contemporáneos, definiéndose como un entorno de software centralizado que fusiona subsistemas de seguridad de distinta naturaleza tales como la videovigilancia (CCTV), el control de accesos, la detección de intrusiones y las alarmas contra incendios bajo una sola interfaz operativa común. De

acuerdo con Norman (Norman, 2014), el diseño de una infraestructura basada en la unificación responde a la necesidad de superar las limitaciones de los sistemas tradicionales fragmentados o independientes, conocidos conceptualmente como sistemas aislados. Al planificar técnicamente una solución unificada, se viabilizan ventajas críticas como la correlación automática de eventos en tiempo real permitiendo, por ejemplo, que un sensor de intrusión active inmediatamente una cámara específica, la reducción drástica de los tiempos de respuesta mediante la mitigación de la fatiga del operador y una escalabilidad estructurada que facilita el crecimiento futuro de la red periférica sin alterar la lógica de administración central. Bajo este enfoque de ingeniería, la especificación de una plataforma unificada en la fase de diseño actúa como una hoja de ruta arquitectónica esencial; por ello, aunque el alcance del presente proyecto no abarque el desarrollo de software ni su despliegue físico en campo, su inclusión teórica es indispensable para asegurar que el hardware y la topología de red propuestos posean la compatibilidad y la viabilidad técnica necesarias para una futura integración automatizada (Norman, 2014).

2.2.6. Normas Técnicas Internacionales

ISO/IEC 62676: Sistemas de Videovigilancia

La norma ISO/IEC 62676 establece los lineamientos internacionales para el diseño, implementación, operación y evaluación de sistemas de videovigilancia utilizados en aplicaciones de seguridad. Su propósito principal es garantizar la interoperabilidad, calidad de imagen, confiabilidad y correcto funcionamiento de los sistemas de CCTV empleados en la protección de personas, bienes e infraestructuras(ISO/IEC, 2014).

Esta norma proporciona criterios técnicos relacionados con la arquitectura de los sistemas de videovigilancia, incluyendo cámaras, grabadores, dispositivos de almacenamiento, transmisión de video y centros de monitoreo. Asimismo, define parámetros para la selección

y ubicación de cámaras, niveles de resolución, cobertura de áreas, calidad de grabación y requisitos de desempeño necesarios para una adecuada supervisión de los entornos monitoreados(ISO/IEC, 2014).

La ISO/IEC 62676 también contempla aspectos vinculados a la gestión del video digital, transmisión en redes IP, compresión de video, interoperabilidad entre dispositivos y almacenamiento seguro de las grabaciones. Estos lineamientos permiten que los sistemas de videovigilancia mantengan un funcionamiento eficiente y escalable, especialmente en infraestructuras donde se requiere monitoreo continuo y administración centralizada(ISO/IEC, 2014).

En el contexto de la presente investigación, la norma ISO/IEC 62676 sirve como referencia técnica para el diseño del sistema de videovigilancia propuesto para el pabellón universitario, permitiendo establecer criterios adecuados para la cobertura de áreas críticas, calidad de supervisión, capacidad de almacenamiento y funcionamiento integrado con los demás subsistemas de seguridad electrónica(ISO/IEC, 2014).

La norma IEEE 802.3af: POE

La norma IEEE 802.3af define el estándar Power over Ethernet (PoE), una tecnología que permite transmitir energía eléctrica y datos simultáneamente a través de un mismo cable de red Ethernet. Esta norma fue desarrollada con el propósito de facilitar la alimentación de dispositivos de red sin necesidad de fuentes de energía independientes, optimizando la instalación y administración de infraestructuras tecnológicas (IEEE Standards Association, 2003).

El estándar IEEE 802.3af suministra hasta 15.4 W de potencia por puerto Ethernet, permitiendo alimentar dispositivos como cámaras IP, teléfonos VoIP, puntos de acceso inalámbricos y equipos de control de acceso. Para ello, emplea cableado de par trenzado bajo

estándares Ethernet convencionales, reduciendo la cantidad de cableado eléctrico requerido y simplificando el despliegue de dispositivos en diferentes entornos (IEEE Standards Association, 2003).

Asimismo, la norma establece mecanismos de detección y clasificación de dispositivos compatibles, garantizando que la energía sea suministrada de manera segura y únicamente a equipos autorizados. Esto contribuye a mejorar la confiabilidad y protección de la infraestructura de red (IEEE Standards Association, 2003).

En la presente investigación, la norma IEEE 802.3af sirve como referencia técnica para la alimentación de cámaras IP y otros dispositivos de seguridad electrónica mediante switches PoE, permitiendo optimizar la distribución de energía y simplificar la implementación del sistema de seguridad inteligente propuesto para el pabellón universitario (IEEE Standards Association, 2003).

ANSI/TIA/EIA-568: Cableado de Telecomunicaciones

La norma ANSI/TIA/EIA-568 establece los lineamientos generales para el diseño e implementación de sistemas de cableado estructurado en edificios comerciales e institucionales. Su finalidad es proporcionar una infraestructura de telecomunicaciones estandarizada que permita soportar servicios de voz, datos y transmisión de información de manera organizada y eficiente (Telecommunications Industry Association, 2001).

Esta norma define criterios relacionados con la topología del cableado, distribución de espacios de telecomunicaciones, rutas de cableado, distancias máximas permitidas y componentes necesarios para garantizar un adecuado desempeño de la red. Asimismo, promueve la interoperabilidad y escalabilidad de las infraestructuras de comunicación, facilitando futuras ampliaciones y mantenimiento de los sistemas (Telecommunications Industry Association, 2001).

La ANSI/TIA/EIA-568-B.1 también establece recomendaciones para la instalación de cableado horizontal y vertical, paneles de conexión, racks de telecomunicaciones y puntos de red, contribuyendo a mantener una correcta organización física de los dispositivos y equipos conectados dentro de la infraestructura tecnológica (Telecommunications Industry Association, 2001).

En la presente investigación, esta norma sirve como referencia técnica para el diseño del cableado estructurado que soportará los sistemas de videovigilancia, control de acceso, alarmas y la plataforma de gestión unificada del pabellón universitario, asegurando una infraestructura de red ordenada, escalable y compatible con los requerimientos de seguridad electrónica (Telecommunications Industry Association, 2001).

ANSI/TIA-569: La norma ANSI/TIA-569 corresponde a un estándar internacional orientado al diseño y construcción de espacios y canalizaciones para infraestructuras de telecomunicaciones en edificaciones comerciales e institucionales. Su finalidad es establecer criterios técnicos para la adecuada distribución del cableado y de los elementos de conectividad dentro de una infraestructura de red (Telecommunications Industry Association, 2015).

Esta norma contempla aspectos relacionados con ductos, canaletas, bandejas portacables, rutas de cableado, cuartos de telecomunicaciones y espacios destinados a equipos de comunicaciones, permitiendo que las instalaciones sean organizadas, seguras y escalables. Asimismo, busca facilitar el mantenimiento, la administración y futuras ampliaciones de la infraestructura tecnológica (Telecommunications Industry Association, 2015).

En el contexto del presente proyecto, la norma ANSI/TIA-569 sirve como referencia para el diseño de las canalizaciones y espacios destinados de los sistemas de videovigilancia, control de acceso y alarmas dentro del pabellón.

IEC 62642: Sistemas de Alarma y Detección de Intrusión

La norma IEC 62642 establece lineamientos técnicos para los sistemas de alarma contra intrusión y asalto utilizados en aplicaciones de seguridad electrónica. Su finalidad es definir criterios relacionados con el diseño, funcionamiento, desempeño e integración de dispositivos destinados a la detección de accesos no autorizados y eventos que comprometan la seguridad de las instalaciones (International Electrotechnical Commission, 2022).

Esta norma contempla especificaciones aplicables a paneles de alarma, sensores de movimiento, contactos magnéticos, dispositivos de señalización y mecanismos de comunicación utilizados en sistemas de detección de intrusión. Asimismo, establece criterios relacionados con niveles de seguridad, confiabilidad, supervisión de eventos y capacidad de respuesta ante incidentes (International Electrotechnical Commission, 2022).

La IEC 62642 también promueve la interoperabilidad y correcto funcionamiento de los componentes que integran los sistemas de alarma, considerando aspectos relacionados con transmisión de señales, monitoreo de eventos y protección frente a intentos de manipulación o fallas del sistema (International Electrotechnical Commission, 2022).

En la presente investigación, la norma IEC 62642 sirve como referencia técnica para el diseño del subsistema de alarmas de intrusión del pabellón universitario, contribuyendo a la definición de criterios para la selección e integración de sensores, paneles de control y mecanismos de generación de alertas dentro del sistema de seguridad inteligente propuesto.

IEC 60839: Sistemas Electrónicos de Seguridad e Integración

La norma IEC 60839 establece lineamientos generales para los sistemas electrónicos de seguridad y alarmas utilizados en aplicaciones de protección y supervisión. Su propósito es proporcionar criterios técnicos para el diseño, integración, operación y evaluación de sistemas destinados a la detección de eventos de seguridad, monitoreo y control de instalaciones

(International Electrotechnical Commission, 2020).

Esta norma contempla aspectos relacionados con sistemas de videovigilancia, control de acceso, detección de intrusión, monitoreo de alarmas y plataformas de gestión de seguridad, promoviendo la interoperabilidad y funcionamiento coordinado de los diferentes subsistemas de seguridad electrónica (International Electrotechnical Commission, 2020).

Asimismo, la IEC 60839 establece criterios orientados a garantizar la confiabilidad, disponibilidad y continuidad operativa de los sistemas electrónicos de seguridad, considerando mecanismos de supervisión, transmisión de eventos, generación de alertas y administración centralizada de la información (International Electrotechnical Commission, 2020).

La norma también considera aspectos relacionados con la integración de dispositivos y la gestión de eventos de seguridad dentro de infraestructuras tecnológicas, permitiendo una administración más eficiente de los sistemas implementados (International Electrotechnical Commission, 2020).

En la presente investigación, la IEC 60839 sirve como referencia técnica para la integración de los subsistemas de videovigilancia, control de acceso y alarmas dentro de la plataforma de gestión unificada propuesta para el pabellón universitario, contribuyendo a garantizar un funcionamiento coordinado y eficiente del sistema de seguridad inteligente.

ONVIF (Open Network Video Interface Forum)

ONVIF (Open Network Video Interface Forum) es un estándar internacional orientado a la interoperabilidad de dispositivos de seguridad física basados en redes IP, tales como cámaras de videovigilancia, grabadores de video, sistemas de control de acceso y plataformas de gestión de seguridad. Su finalidad es permitir la integración y comunicación entre equipos de distintos fabricantes mediante protocolos estandarizados (ONVIF, 2023).

Este estándar define especificaciones relacionadas con la transmisión de video,

configuración de dispositivos, control de eventos, autenticación y descubrimiento automático de equipos dentro de la red. Gracias a ello, los sistemas compatibles con ONVIF pueden intercambiar información y operar de manera integrada, facilitando la administración centralizada de los diferentes subsistemas de seguridad (ONVIF, 2023).

Asimismo, ONVIF contribuye a mejorar la escalabilidad y flexibilidad de las infraestructuras de seguridad electrónica, evitando la dependencia de un único fabricante y permitiendo la incorporación futura de nuevos dispositivos compatibles dentro de la misma plataforma tecnológica (ONVIF, 2023).

En la presente investigación, el estándar ONVIF sirve como referencia para garantizar la interoperabilidad entre las cámaras IP, dispositivos de seguridad y la plataforma de gestión unificada propuesta para el pabellón universitario, favoreciendo la integración y supervisión centralizada de los subsistemas de videovigilancia, alarmas y control de acceso.

2.2.7. Normas Técnicas Nacionales

Norma Técnica EM.020: Instalaciones de Telecomunicaciones

La Norma Técnica EM.020 del Reglamento Nacional de Edificaciones del Perú establece los lineamientos para el diseño e implementación de instalaciones de telecomunicaciones en edificaciones, incluyendo infraestructura para transmisión de datos, redes de comunicación y sistemas de seguridad electrónica. Esta norma contempla aspectos relacionados con canalizaciones, cableado, espacios técnicos y distribución de servicios tecnológicos dentro de las edificaciones(Ministerio de Vivienda, Construcción y Saneamiento, 2018).

En el contexto de la presente investigación, la norma EM.020 sirve como referencia para el diseño de la infraestructura de telecomunicaciones que soporta el sistema integrado de seguridad electrónica, considerando la instalación de cableado estructurado, cámaras de videovigilancia, dispositivos de control de acceso y sistemas de alarma, garantizando una

adecuada organización, conectividad y escalabilidad de la solución propuesta(Ministerio de Vivienda, Construcción y Saneamiento, 2018).

Ley N.º 29090 y el Reglamento Nacional de Edificaciones

La Ley N.º 29090, Ley de Regulación de Habilitaciones Urbanas y de Edificaciones, establece el marco normativo para la ejecución, supervisión y regularización de edificaciones en el territorio peruano. Esta ley tiene como finalidad garantizar que las edificaciones cumplan condiciones adecuadas de seguridad, habitabilidad y funcionalidad, considerando criterios técnicos y normativos aplicables a la infraestructura física (Ministerio de Vivienda, Construcción y Saneamiento, 2020).

En complemento, el Reglamento Nacional de Edificaciones (RNE) constituye el conjunto de normas técnicas que regulan el diseño, construcción y acondicionamiento de edificaciones en el Perú. El RNE establece disposiciones relacionadas con seguridad, instalaciones eléctricas, infraestructura de telecomunicaciones, accesibilidad y condiciones técnicas que deben considerarse durante la planificación y desarrollo de proyectos de infraestructura (Ministerio de Vivienda, Construcción y Saneamiento, 2020).

Asimismo, el Reglamento Nacional de Edificaciones contempla criterios orientados a garantizar la seguridad de las personas y la adecuada integración de instalaciones tecnológicas dentro de las edificaciones, permitiendo que los sistemas implementados mantengan condiciones adecuadas de funcionamiento y compatibilidad con la infraestructura existente (Ministerio de Vivienda, Construcción y Saneamiento, 2020).

En la presente investigación, la Ley N.º 29090 y el Reglamento Nacional de Edificaciones sirven como referencia normativa para el diseño de la infraestructura del sistema de seguridad inteligente del pabellón universitario, considerando aspectos relacionados con la instalación de dispositivos tecnológicos, canalizaciones, cableado, condiciones de seguridad

y adecuación de los espacios destinados al monitoreo y operación de los subsistemas de seguridad electrónica.

El Código Nacional de Electricidad (CNE)

El Código Nacional de Electricidad (CNE) constituye el conjunto de disposiciones técnicas que regulan las instalaciones eléctricas en el Perú, estableciendo criterios orientados a garantizar la seguridad de las personas, la protección de los equipos y el correcto funcionamiento de los sistemas eléctricos. Su finalidad es asegurar que las instalaciones eléctricas sean diseñadas e implementadas bajo condiciones adecuadas de seguridad, confiabilidad y eficiencia (Ministerio de Energía y Minas del Perú, 2006).

El CNE contempla lineamientos relacionados con la distribución eléctrica, protección contra sobrecargas y cortocircuitos, sistemas de puesta a tierra, canalizaciones, tableros eléctricos y alimentación de equipos tecnológicos. Asimismo, establece requisitos para la instalación de conductores, dispositivos de protección y mecanismos destinados a reducir riesgos eléctricos dentro de las edificaciones (Ministerio de Energía y Minas del Perú, 2006).

Además, el Código Nacional de Electricidad incluye criterios aplicables a infraestructuras de telecomunicaciones y sistemas electrónicos, permitiendo que los equipos conectados mantengan condiciones adecuadas de operación y protección frente a fallas eléctricas o variaciones de energía (Ministerio de Energía y Minas del Perú, 2006).

En la presente investigación, el Código Nacional de Electricidad sirve como referencia técnica para el diseño de la alimentación eléctrica y protección de los dispositivos que conforman el sistema de seguridad inteligente del pabellón universitario, incluyendo cámaras IP, switches PoE, servidores, sistemas de monitoreo y equipos de control de acceso, contribuyendo a garantizar una infraestructura eléctrica segura y confiable.

Norma Técnica Peruana ISO/IEC 27001

La Norma Técnica Peruana ISO/IEC 27001 establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI). Su finalidad es proteger la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de controles de seguridad orientados a la gestión de riesgos y protección de los activos de información (Instituto Nacional de Calidad, 2014).

Esta norma proporciona un marco de referencia para identificar amenazas, vulnerabilidades y riesgos relacionados con la información y los sistemas tecnológicos, permitiendo establecer medidas de control para reducir posibles incidentes de seguridad. Asimismo, promueve la definición de políticas, procedimientos y mecanismos de protección orientados a garantizar la seguridad de la información dentro de las organizaciones (Instituto Nacional de Calidad, 2014).

La ISO/IEC 27001 también contempla aspectos relacionados con el control de accesos, gestión de incidentes, protección de redes, respaldo de información y monitoreo de los sistemas tecnológicos, contribuyendo a fortalecer la seguridad de las infraestructuras digitales y servicios asociados (Instituto Nacional de Calidad, 2014).

En la presente investigación, la Norma Técnica Peruana ISO/IEC 27001 sirve como referencia para el establecimiento de criterios de seguridad aplicables a la infraestructura tecnológica y a la gestión de la información generada por los sistemas de videovigilancia, control de acceso y monitoreo del pabellón universitario, contribuyendo a la protección de los datos y al fortalecimiento de la seguridad integral del sistema propuesto.

2.2.8. Reglamentación Nacional

Decreto Legislativo N.º 1218

El Decreto Legislativo N.º 1218 regula el uso de cámaras de videovigilancia y de tecnologías especiales para la seguridad ciudadana en el Perú, estableciendo disposiciones orientadas a fortalecer las acciones de prevención, supervisión y control en espacios públicos y privados. Su finalidad es promover el uso adecuado de sistemas de videovigilancia como herramientas de apoyo para la seguridad y prevención de incidentes (Presidencia de la República del Perú, 2015).

Este decreto establece lineamientos relacionados con la instalación y utilización de cámaras de videovigilancia, conservación de grabaciones, acceso a la información registrada y colaboración con las autoridades competentes en situaciones vinculadas a la seguridad. Asimismo, promueve la implementación de mecanismos tecnológicos que contribuyan al monitoreo y supervisión de ambientes donde puedan presentarse riesgos que afecten la integridad de las personas o bienes (Presidencia de la República del Perú, 2015).

Además, el Decreto Legislativo N.º 1218 contempla la necesidad de que los sistemas de videovigilancia mantengan condiciones adecuadas de funcionamiento, almacenamiento y protección de la información recopilada, considerando medidas orientadas a preservar la seguridad y confidencialidad de los registros generados (Presidencia de la República del Perú, 2015).

En la presente investigación, el Decreto Legislativo N.º 1218 sirve como referencia normativa para el diseño del sistema de videovigilancia propuesto para el pabellón universitario, contribuyendo al establecimiento de criterios relacionados con el monitoreo, almacenamiento de grabaciones y supervisión de incidentes dentro de la infraestructura académica.

Directiva N.º 01-2020-JUS/DGTAIPD

La Directiva N.º 01-2020-JUS/DGTAIPD, emitida por la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos del Perú, establece disposiciones para el tratamiento de datos personales mediante sistemas de videovigilancia. Su finalidad es garantizar que la recopilación, almacenamiento, acceso y uso de imágenes y datos obtenidos a través de cámaras de seguridad se realicen respetando los principios de protección de datos personales establecidos en la normativa peruana (Ministerio de Justicia y Derechos Humanos, 2020).

La directiva establece lineamientos relacionados con la instalación de cámaras de videovigilancia, deber de información a los usuarios, control de acceso a las grabaciones, conservación de registros, medidas de seguridad y restricciones sobre el uso de los datos recopilados. Asimismo, dispone que las entidades deben implementar mecanismos orientados a prevenir el acceso no autorizado, alteración, pérdida o uso indebido de la información generada por los sistemas de videovigilancia (Ministerio de Justicia y Derechos Humanos, 2020).

En la presente investigación, la Directiva N.º 01-2020-JUS/DGTAIPD sirve como referencia normativa para el diseño de políticas, procedimientos y medidas de seguridad relacionadas con el tratamiento de los datos generados por los sistemas de videovigilancia y control de acceso del pabellón universitario, contribuyendo al cumplimiento de las disposiciones de protección de datos personales aplicables al sistema de seguridad inteligente propuesto.

Autoridad Nacional de Protección de Datos Personales (ANPD)

La Autoridad Nacional de Protección de Datos Personales (ANPD) es el órgano del Ministerio de Justicia y Derechos Humanos del Perú encargado de supervisar y garantizar el cumplimiento de la normativa relacionada con la protección de datos personales. Su función principal consiste en velar por el tratamiento adecuado de la información personal recopilada por entidades públicas y privadas, promoviendo el respeto a los derechos fundamentales de privacidad y protección de datos (Autoridad Nacional de Protección de Datos Personales, 2023).

La ANPD establece lineamientos y criterios aplicables al tratamiento de datos obtenidos mediante sistemas tecnológicos, incluyendo sistemas de videovigilancia, control de acceso biométrico y plataformas digitales de monitoreo. Asimismo, supervisa el cumplimiento de las disposiciones relacionadas con la recopilación, almacenamiento, acceso, conservación y seguridad de los datos personales (Autoridad Nacional de Protección de Datos Personales, 2023).

Además, esta entidad promueve la implementación de medidas orientadas a garantizar la confidencialidad, integridad y disponibilidad de la información, así como la prevención de accesos no autorizados, pérdida o uso indebido de los datos recopilados por los sistemas de seguridad electrónica (Autoridad Nacional de Protección de Datos Personales, 2023).

En la presente investigación, la ANPD sirve como referencia institucional para el establecimiento de criterios relacionados con la protección y tratamiento de los datos generados por los sistemas de videovigilancia y control de acceso del pabellón universitario, contribuyendo al cumplimiento de las disposiciones legales aplicables a la seguridad de la información y protección de datos personales.

Ley N.° 29733 – Ley de Protección de Datos Personales

La Ley N.° 29733 tiene como finalidad garantizar la protección de los datos personales y regular su tratamiento, almacenamiento y uso por parte de entidades públicas y privadas. Esta normativa resulta relevante en los sistemas de seguridad electrónica debido a que tecnologías como la videovigilancia y el control de acceso biométrico recopilan información que permite identificar a las personas(Congreso de la República del Perú, 2011).

En los sistemas de videovigilancia, las imágenes captadas por las cámaras constituyen datos personales, mientras que en los sistemas de control de acceso los registros biométricos, como huellas dactilares o reconocimiento facial, son considerados datos sensibles y requieren mayores medidas de protección.

La ley establece principios relacionados con la seguridad, confidencialidad y finalidad del tratamiento de datos, por lo que el diseño del sistema de seguridad debe contemplar mecanismos que permitan restringir accesos no autorizados, proteger la información almacenada y garantizar el uso adecuado de los datos recopilados(Congreso de la República del Perú, 2011).

Asimismo, la aplicación de esta normativa contribuye a que la propuesta del sistema de seguridad electrónica considere aspectos de privacidad y protección de la información dentro del entorno universitario.

Documentación técnica para el diseño de sistemas de seguridad electrónica

El Ministerio de Economía y Finanzas del Perú (MEF) establece pautas orientadas a mejorar la elaboración de expedientes técnicos, promoviendo una adecuada planificación, coordinación y definición de los componentes necesarios para la ejecución de proyectos de infraestructura y sistemas tecnológicos. Estas pautas buscan reducir deficiencias técnicas, interferencias y modificaciones durante la etapa de implementación, contribuyendo a una

ejecución más eficiente de los proyectos (Ministerio de Economía y Finanzas del Perú, 2020).

Asimismo, el MEF señala la importancia de desarrollar expedientes técnicos completos y debidamente sustentados, considerando estudios, especificaciones técnicas, planos, presupuestos y criterios normativos que permitan garantizar la viabilidad y correcta ejecución de las soluciones propuestas (Ministerio de Economía y Finanzas del Perú, 2020).

En el contexto de la presente investigación, estas pautas sirven como referencia para la elaboración de la documentación técnica asociada al diseño del sistema de seguridad inteligente del pabellón universitario, incluyendo la definición de requerimientos, arquitectura tecnológica, distribución de dispositivos, infraestructura de red, especificaciones técnicas y criterios necesarios para una futura implementación del sistema.

2.2.9. Arquitectura de Analítica de Video Basada en Inteligencia Artificial (Deep Learning)

El sistema propuesto integra soluciones de analítica de video automatizada basadas en algoritmos de aprendizaje profundo (*Deep Learning*). Esta infraestructura permite la transición de un esquema de videovigilancia pasivo hacia un modelo proactivo y automatizado, reduciendo drásticamente la tasa de falsas alarmas provocadas por factores ambientales (variaciones climáticas, ráfagas de viento, lluvia, cambios de iluminación) o fauna urbana, optimizando la eficiencia operativa del Centro de Monitoreo (NOC/SOC).

Módulos Tecnológicos y Funciones Inteligentes Consolidadas

El diseño técnico aprovecha las capacidades de procesamiento en el borde (*Edge AI*) mediante la convergencia de las tecnologías líderes del mercado (*AcuSense / Motion Detection 2.0* de Hikvision y *SMD Plus / IVS / WizMind* de Dahua). Los módulos analíticos parametrizados se estructuran bajo las siguientes funciones core:

- **Filtrado Inteligente de Objetos y Movimiento Evolucionado (AcuSense / SMD Plus):** Módulos algorítmicos diseñados para clasificar y discriminar vectores de movimiento en la escena. El sistema analiza los mapas de píxeles dinámicos e ignora de manera automática el movimiento de follaje, lluvia o animales, activando la grabación y la transmisión de alertas prioritarias en el flujo principal (*Main-stream*) únicamente ante la detección y confirmación de siluetas correspondientes a **seres humanos o vehículos**, logrando una reducción de hasta el 90 % en falsas alarmas operativas.

- **Protección Perimetral Avanzada e Inteligente (IVS):** Implementación de algoritmos geométricos virtuales que monitorean de forma continua dos eventos críticos sobre la escena: el *Cruce de Línea Virtual* (detección bidimensional con sentido paramétrico) y la *Intrusión en Área Prohibida* (análisis poligonal de N lados). El sistema evalúa el porcentaje de permanencia, dirección y escala del objeto para validar la amenaza de forma automatizada, descartando elementos irrelevantes del entorno.

- **Estructuración de Metadatos de Video y Búsqueda Forense:** Los dispositivos perimetrales analizan y desglosan las siluetas capturadas en vectores de características cualitativas (atributos), indexándolos inmediatamente en la base de datos del servidor de grabación. Permite clasificar de forma automatizada atributos humanos (género, rango de edad, uso de anteojos, gorros o mascarillas) y de vestimenta/accesorios (tipo de prenda superior/inferior, patrones de color en espacio RGB, uso de cascos de seguridad y presencia de mochilas o bolsos). Esta indexación viabiliza consultas booleanas complejas en el VMS para localizar objetivos en segundos.

- **Detección y Reconocimiento Facial en Tiempo Real:** Algoritmo de detección de puntos de referencia faciales (*facial landmarks*) que extrae las características biométricas del rostro y las contrasta de manera instantánea contra bases de

datos locales autorizadas para la verificación de identidad y el control de accesos institucionales.

- **Seguimiento Inteligente Automatizado (WizTracking / Smart Tracking):** Mecanismo de control dinámico diseñado para cámaras domo PTZ (*Pan-Tilt-Zoom*). Al activarse una regla perimetral (intrusión o cruce de línea), el algoritmo toma el control de los servomotores de la cámara de forma autónoma, modificando el azimut, la elevación y el plano óptico para seguir la trayectoria del objetivo en movimiento, manteniéndolo centrado y en alta resolución dentro de la escena.

- **Conteo de Personas (People Counting):** Analítica estadística que genera un registro bidireccional exacto del flujo peatonal en tiempo real. Contabiliza los ingresos, salidas y permanencia neta de personas dentro de áreas específicas, sirviendo como una herramienta automatizada para el control estricto de aforos y gestión de evacuación civil.

- **Mapeo de Calor (*Heat Mapping*):** Algoritmo de acumulación temporal de movimiento que calcula y representa gráficamente mediante un espectro cromático (gradiente de colores cálidos a fríos) las zonas con mayor densidad de tránsito estático o dinámico de personas, aportando datos de valor logístico y análisis de uso de los espacios comunes del pabellón.

Capítulo 3

Metodología de Recolección de Información

3.1. Recolección de Información

3.1.1. Encuestas

Objetivo de la encuesta

Recolectar información sobre la situación actual de la seguridad en el pabellón, conocer la percepción de los usuarios respecto a las condiciones de seguridad existentes, y registrar cualquier incidente o problema relacionado con la seguridad que haya ocurrido, con el fin de identificar necesidades de mejora.

Instrumento

Número de preguntas: El cuestionario estuvo conformado por un total de 12 preguntas.

Tipo de preguntas: Se diseñaron distintos tipos de ítems, seleccionados en función

del tipo de variable a evaluar:

- Preguntas cerradas dicotómicas (Sí/No), orientadas a variables categóricas nominales.
- Ítems con escala tipo Likert, adecuados para medir actitudes, opiniones o niveles de acuerdo (p. ej., "¿Cómo calificaría...?").
- Preguntas abiertas, empleadas para recolectar datos cualitativos que complementen la información cuantitativa (p. ej., "Describa brevemente...").
- Preguntas de opción múltiple con selección múltiple, utilizadas para recoger información más específica y variada.

3.1.2. Validez y confiabilidad:

Para garantizar la validez de contenido del instrumento, se aplicaron dos estrategias fundamentales,en primer lugar, se realizaron entrevistas exploratorias de carácter informal con seis participantes, lo que permitió identificar elementos clave del fenómeno de estudio desde la perspectiva de los involucrados. Esta etapa inicial sirvió como insumo para el diseño preliminar del cuestionario.

En segundo lugar, se aplicó el **Juicio de Expertos** como técnica fundamental de validación de contenido. Para este proceso, se seleccionó a tres (03) docentes especialistas de la Escuela Profesional de Ingeniería Informática y de Sistemas, a quienes se les entregó la **Matriz de Operacionalización de Variables** junto con el diseño preliminar del cuestionario. Esto permitió a los evaluadores contrastar técnicamente la alineación de los ítems con los objetivos de la investigación,Como se muestra en el anexo E.

Cada docente evaluó los reactivos en cuanto a su claridad, pertinencia y adecuación, plasmando sus sugerencias, correcciones y recomendaciones en las **Fichas de Observaciones**, las cuales fueron validadas y suscritas mediante sus respectivas firmas. Posteriormente, se

realizó el procesamiento de estas recomendaciones, incorporando minuciosamente cada una de las observaciones proporcionadas por los expertos para refinar, corregir y consolidar la versión definitiva del cuestionario.

La confiabilidad del instrumento se sustenta en el proceso de diseño y validación. La claridad en la redacción, la coherencia entre ítems y variables, y el uso de un lenguaje accesible contribuyen a la consistencia de las respuestas. Adicionalmente, se elaboró una matriz de consistencia, incluida en el Anexo B que evidencia la congruencia entre los objetivos, las variables y los ítems evaluados.

3.1.3. Aplicación

El cuestionario fue aplicado de forma mixta, tanto presencial como virtual, mediante la plataforma Google Forms. La mayoría de los participantes completaron el instrumento de manera autoadministrada; sin embargo, en algunos casos puntuales se brindó apoyo durante la aplicación, leyendo las preguntas sin modificar su contenido ni estructura, manteniendo así el carácter estructurado del cuestionario. El modelo de encuesta aplicado se presenta en el Anexo A, mientras que el registro digitalizado de las encuestas aplicadas y sus respectivas respuestas se encuentra disponible en el siguiente enlace:

`https://drive.google.com/drive/folders/1-tQggVXTA1Ms_WbRJ9bcl6VBUr3UL18Z?usp=sharing`

3.2. Resultados de la Encuesta

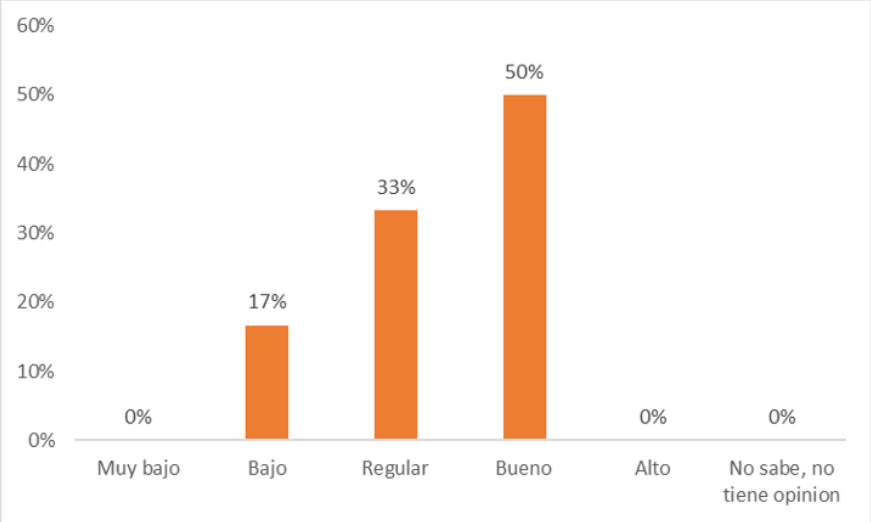
3.2.1. Resultados por Grupo de Encuestados

Pregunta 1

¿Cómo calificaría el nivel de seguridad actual del pabellón, considerando aspectos como la vigilancia, respuesta ante incidentes, el control de accesos y la detección de intrusos?

Personal administrativo

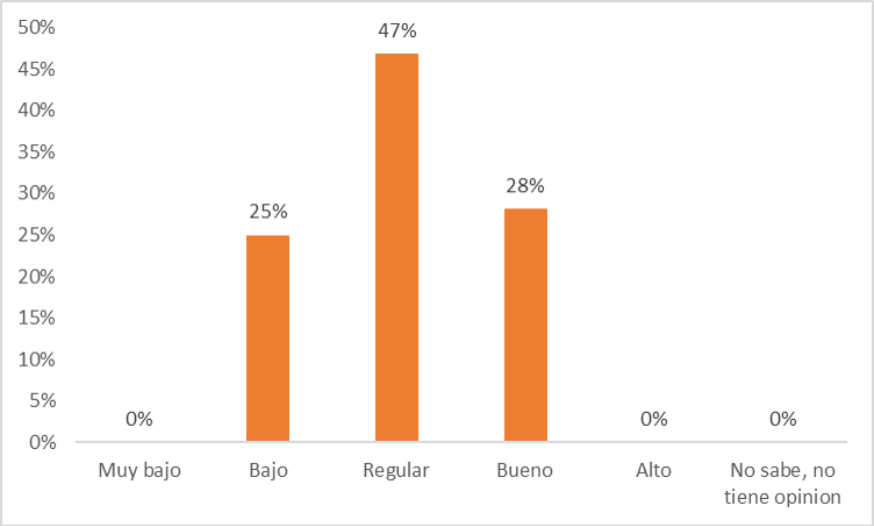
Figura 3.1: *Nivel de seguridad del pabellón según el personal administrativo.*



En el caso de los administrativos, los resultados muestran una distribución más crítica: un 50 % considera que la percepcion de seguridad es bueno, un 33 % regulat y solo un 17 % bajo. Esto indica que, desde la perspectiva administrativa, las medidas de seguridad no son percibidas como plenamente efectivas.

Docentes

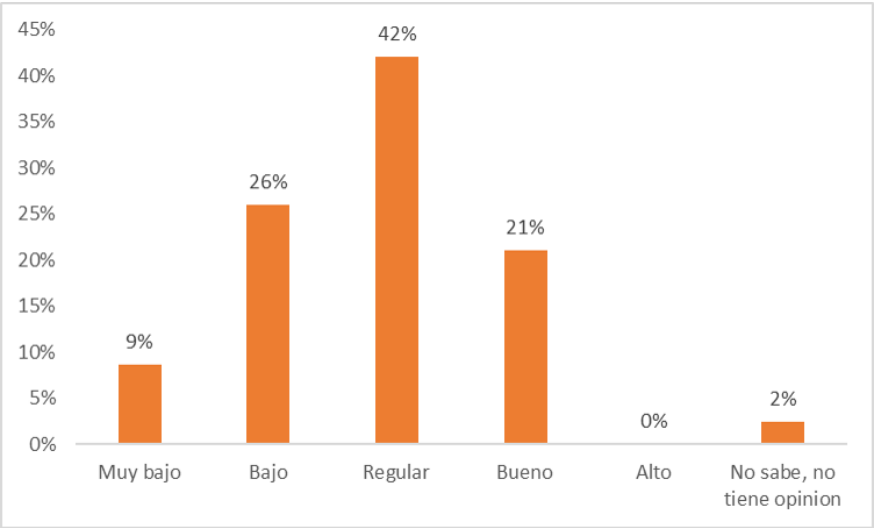
Figura 3.2: *Nivel de seguridad del pabellón según los docentes.*



La mayoría de los docentes percibe un nivel de seguridad regular en el pabellón (47 %), seguido por un 28 % que lo considera bueno y un 25 % que lo califica como bajo, lo que refleja una percepción moderada con margen de mejora en las medidas de seguridad.

Estudiantes

Figura 3.3: *Nivel de seguridad del pabellón según los estudiantes.*



La mayoría de los encuestados percibe el nivel de seguridad del pabellón como regular (42 %), seguido de un 26 % que lo considera bajo y un 21 % que lo califica como bueno.

Solo un 9 % lo percibe muy bajo y un 2 % no tiene opinión, lo que evidencia una percepción predominantemente intermedia con cierta tendencia a la insatisfacción respecto a la seguridad actual.

Análisis comparativo

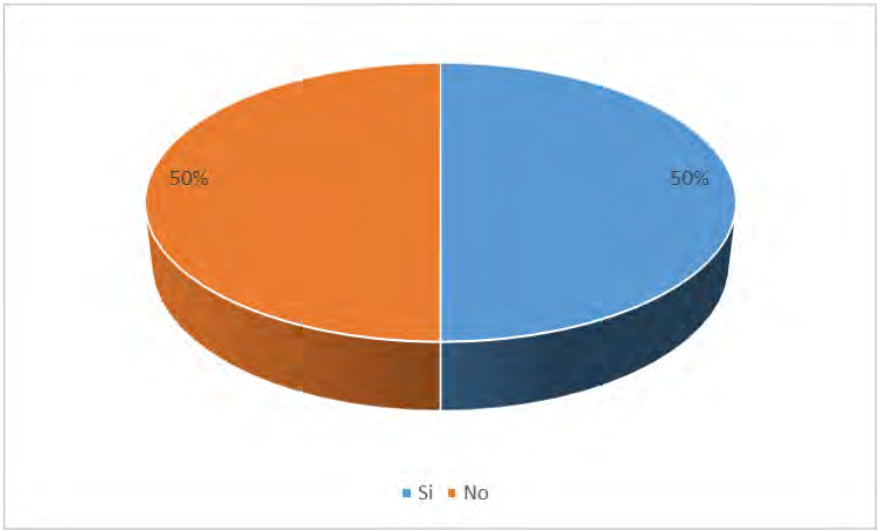
En general, los resultados muestran que la percepción del nivel de seguridad del pabellón es moderada, con una tendencia positiva entre el personal administrativo, mientras que docentes y estudiantes mantienen una valoración regular con ciertos niveles de insatisfacción, evidenciando la necesidad de reforzar las medidas de seguridad.

Pregunta 2

¿Ha sido víctima o conoce algún caso sobre incidentes de seguridad como perdidas de sus pertenencias, robos, mal uso o daño a la infraestructura del pabellón?

Personal administrativo

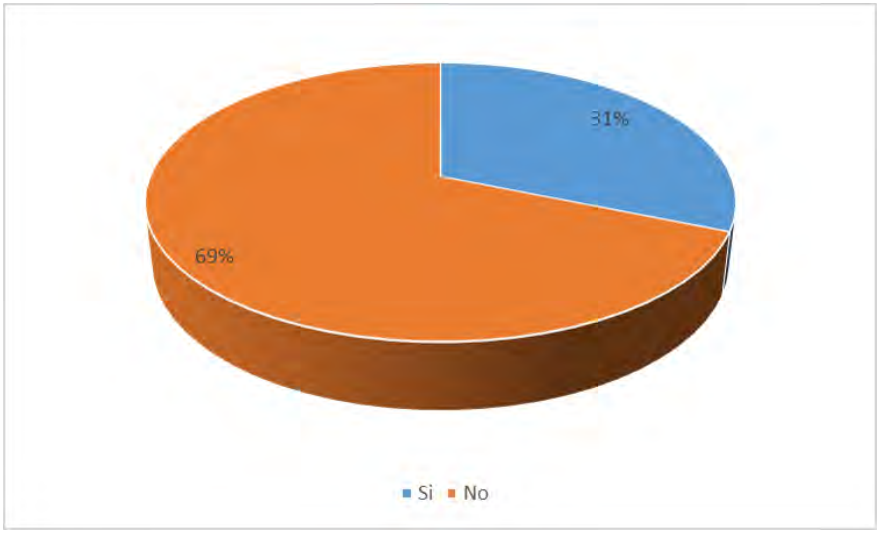
Figura 3.4: *Incidentes de seguridad según el personal administrativo.*



En el caso del personal administrativo, los resultados revelan una división equitativa: la mitad ha sido víctima o conoce incidentes relacionados con pérdidas, robos o daños en el pabellón, mientras que la otra mitad no ha experimentado ni conoce situaciones similares. Esto refleja que los eventos de inseguridad son percibidos como una realidad existente, aunque no generalizada entre todos los administrativos.

Docentes

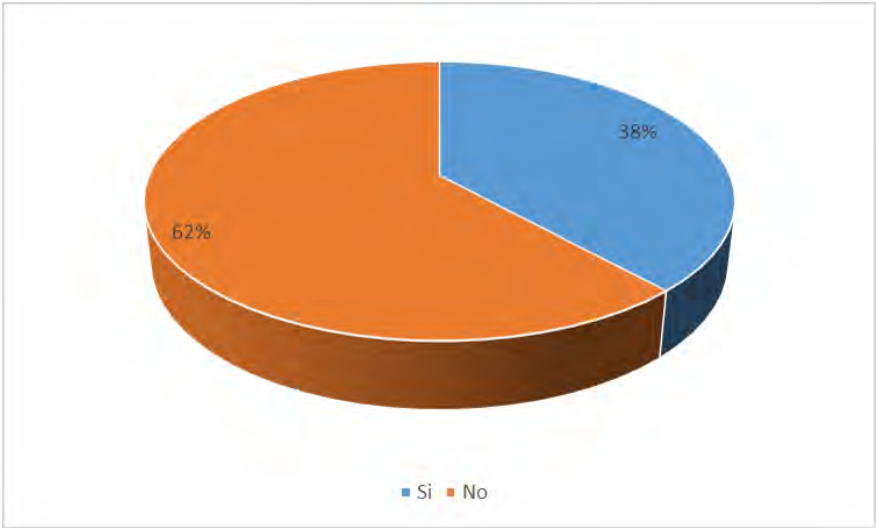
Figura 3.5: *Incidentes de seguridad según los docentes.*



En el caso de los docentes, la mayoría (69 %) no ha sido víctima ni conoce casos de incidentes de seguridad, mientras que un 31 % sí ha tenido o conoce experiencias relacionadas. Esto sugiere que, aunque existen situaciones de inseguridad, estas no son frecuentes entre el personal docente y podrían estar más focalizadas en determinados contextos o momentos.

Estudiantes

Figura 3.6: *Incidentes de seguridad según los estudiantes.*



En el caso de los estudiante, la mayoria (62 %), experimentó o conoce algun incidente de seguridad dentro del pabellón y un 38 % no conoce ni sufrio un incidente, lo que nos da a entender que los estudiantes estan mas propensos a sufrir ese tipo d eincidentes relacionados con la seguridad.

Análisis comparativo

En general, los resultados nos indican que si existen incidentes de seguridad dentro del pabellón y se presentan con mayor frecuencia entre los estudiantes, mientras que en los docentes y personal administrativo la percepción de estos eventos es mucho menor o equilibrada. Esto indica que los grupos con mayor permanencia y movilidad dentro del pabellón (como los estudiantes) están más expuestos a situaciones de pérdida, robo o daño, a diferencia del personal administrativo, que reporta menor incidencia de estos casos

Pregunta 3

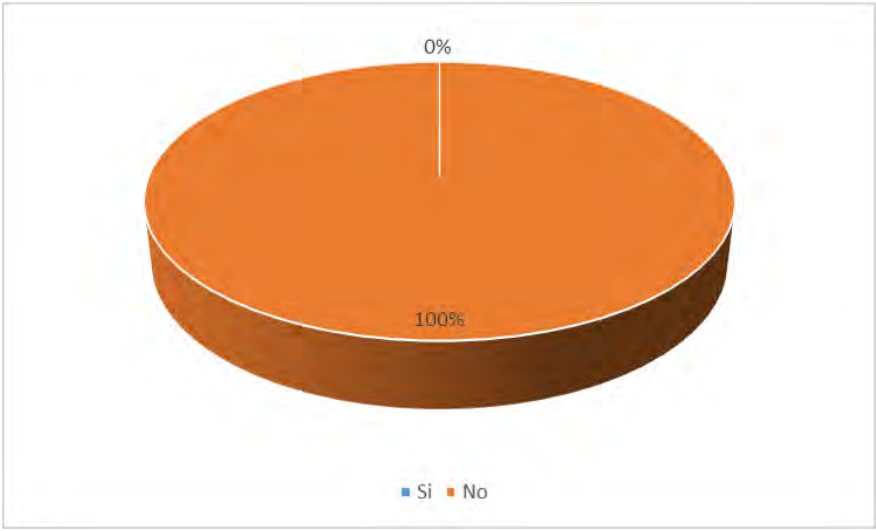
¿Tiene conocimiento de algún incidente relacionado con el ingreso no autorizado a algún ambiente del pabellón?

Tabla 3.1: *Casos reportados de incidentes de seguridad en el pabellón.*

Tipo de incidente	**Descripción o ejemplos reportados**	**Grupos que lo mencionan**	**Frecuencia estimada**
Pérdida de objetos personales	Celulares, audífonos, cargadores, USB, billeteras, casacas, mouse.	Estudiantes, Docentes, Administrativos	Alta
Daños a infraestructura o mobiliario	Mesas rotas, cerraduras dañadas, vidrios rotos, sillas malogradas.	Estudiantes, Administrativos	Media
Robo de equipos o materiales	Proyectores, cortinas, materiales de limpieza, laptop.	Estudiantes, Docentes, Administrativos	Baja
Vandalismo	Pintarrajeado o graffitis en paredes y puertas.	Estudiantes, Docentes	Media
Acceso no autorizado o mal uso de ambientes	Ingreso de personas ajenas, uso inadecuado de laboratorios o aulas.	Docentes, Administrativos	Baja
Suciedad o desorden en espacios comunes	Restos de bebidas, basura o materiales inapropiados en aulas.	Administrativos, Estudiantes	Baja

Personal administrativo

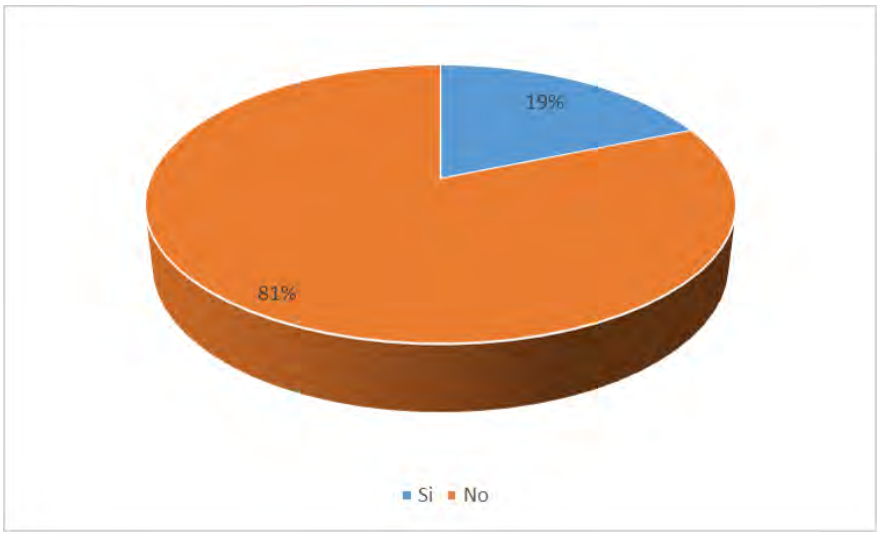
Figura 3.7: *Incidentes de ingreso no autorizado según administrativos.*



En el caso del personal administrativo, la totalidad de los encuestados (6 personas) indicó no haber presenciado ni tenido conocimiento de ingresos no autorizados a los ambientes del pabellón. Esto refleja que, desde su perspectiva, este tipo de incidentes no se ha presentado o no constituye un problema perceptible en su entorno laboral.

Docentes

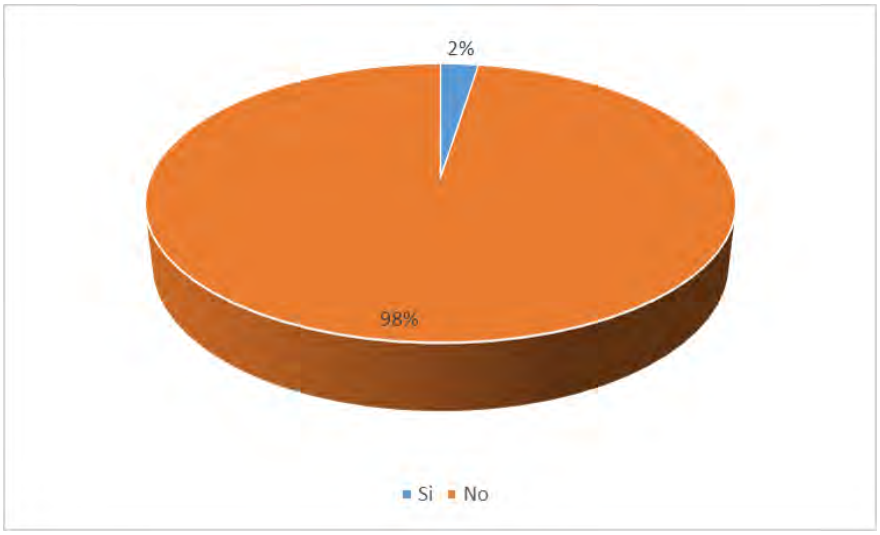
Figura 3.8: *Incidentes de ingreso no autorizado según docentes.*



En el caso de los docentes, la mayoría (81 %) señaló no tener conocimiento de incidentes relacionados con ingresos no autorizados a los ambientes del pabellón, mientras que un 19 % manifestó haber presenciado o conocido algún caso de este tipo. Este resultado sugiere que, si bien existen situaciones aisladas de acceso indebido, la percepción general entre los docentes es que estos incidentes no son frecuentes, lo que podría reflejar un nivel de control aceptable en el acceso a las instalaciones académicas.

Estudiantes

Figura 3.9: *Incidentes de ingreso no autorizado según estudiantes.*



La mayoría de los encuestados percibe el nivel de seguridad del pabellón como regular (42 %), seguido de un 26 % que lo considera bajo y un 21 % que lo califica como bueno. Solo un 9 % lo percibe muy bajo y un 2 % no tiene opinión, lo que evidencia una percepción predominantemente intermedia con cierta tendencia a la insatisfacción respecto a la seguridad actual.

Análisis comparativo

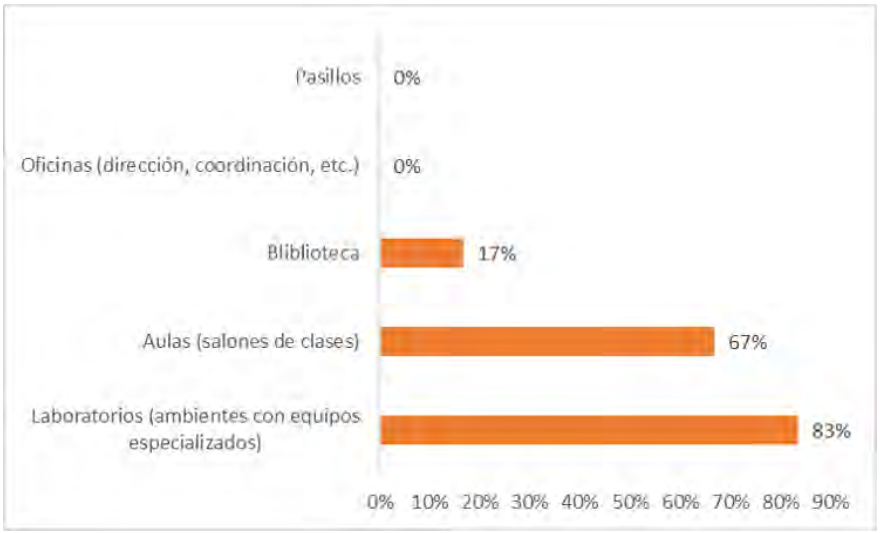
En terminos generales los resultados evidencian que los eventos de acceso no autorizado son poco frecuentes o no perceptibles para la comunidad universitaria, lo que podría asociarse a la existencia de un control razonable en el ingreso a los espacios académicos. No obstante, la pequeña proporción de docentes que sí reportó conocer estos casos sugiere la conveniencia de mantener medidas preventivas y reforzar la supervisión de accesos en determinadas zonas o horario

Pregunta 4

¿Qué áreas considera más vulnerables en términos de riesgo de incidentes de seguridad? Cabe precisar que los porcentajes se basan en un total de seis participantes y corresponden a respuestas múltiples, dado que algunos encuestados señalaron más de un ambiente.

Personal administrativo

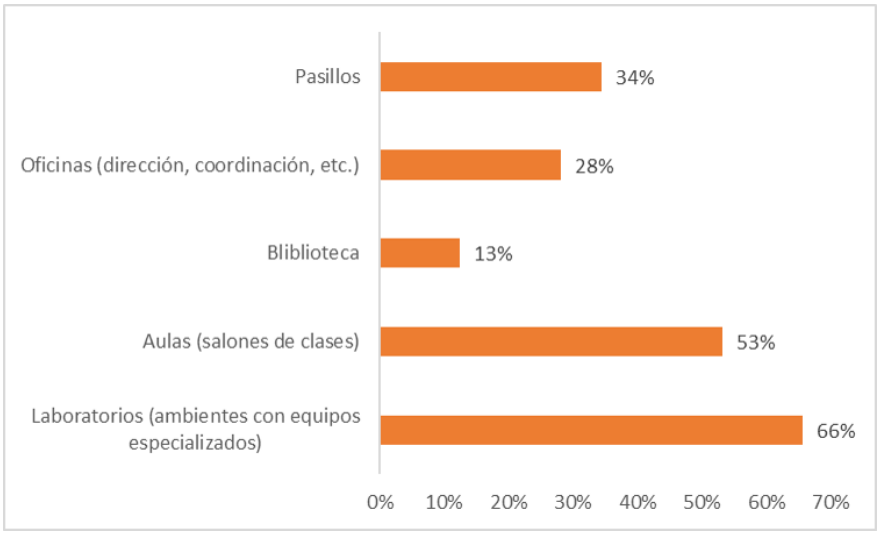
Figura 3.10: *Areas vulnerables según el personal administrativo.*



Respecto a las áreas consideradas más vulnerables a incidentes de seguridad, la mayoría del personal administrativo identificó a los laboratorios (83 %) como los espacios de mayor riesgo, seguidos de las aulas (67 %) y, en menor medida, la biblioteca (17 %). Estos resultados evidencian que los laboratorios son percibidos como los entornos más expuestos a pérdidas, robos o daños, posiblemente debido a la presencia de equipos de valor y al uso compartido de dichos espacios.

Docentes

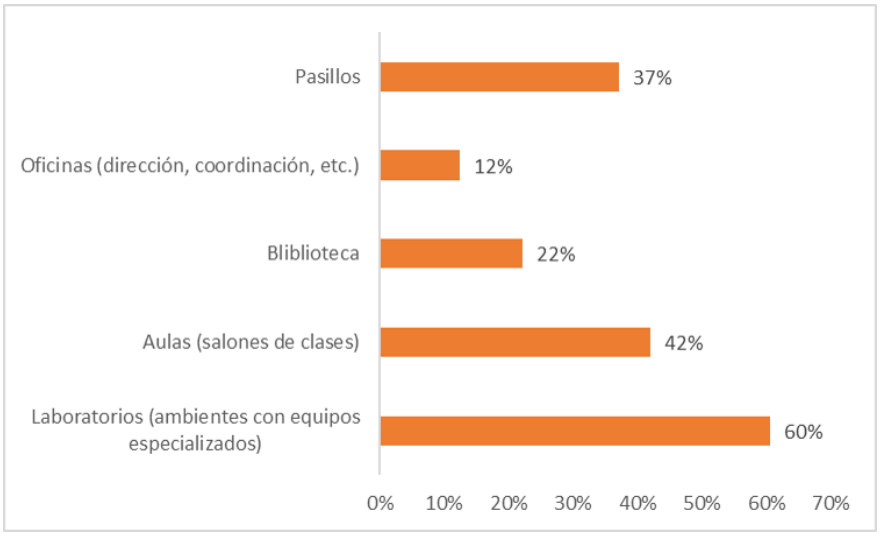
Figura 3.11: *Areas vulnerables según los docentes.*



En el caso de los docentes, los resultados muestran que los laboratorios (66 %) son considerados los espacios más vulnerables a incidentes de seguridad, seguidos de las aulas (53 %) y los pasillos (34 %). En menor medida, se mencionaron las oficinas (28 %) y la biblioteca (13 %). La percepción de mayor vulnerabilidad en los laboratorios podría estar asociada al valor de los equipos y materiales, así como al uso compartido de estos ambientes, mientras que las aulas y pasillos representan zonas de mayor tránsito y exposición dentro del pabellón.

Estudiantes

Figura 3.12: *Areas vulnerables según los estudiantes.*



En el caso de los estudiantes, los laboratorios (60 %) se perciben como las áreas más vulnerables a incidentes de seguridad, seguidos de las aulas (42 %) y los pasillos (37 %). En menor proporción se mencionaron la biblioteca (22 %) y las oficinas (12 %). Esto evidencia que los estudiantes asocian la vulnerabilidad con los espacios donde existe mayor circulación de personas y equipos de valor, especialmente en los laboratorios.

Análisis comparativo

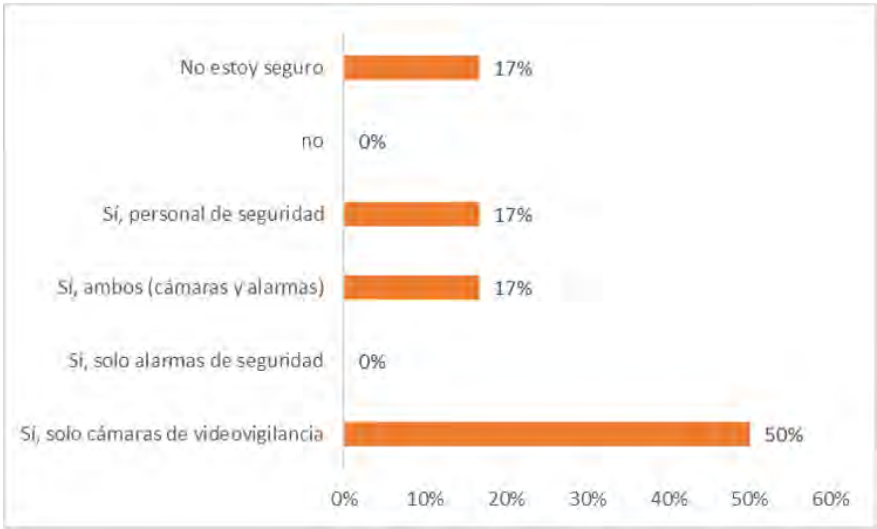
En los tres grupos se identifica a los laboratorios como las áreas más vulnerables a incidentes de seguridad (83 % en administrativos, 66 % en docentes y 60 % en estudiantes). Las aulas también presentan un nivel medio de vulnerabilidad, mientras que la biblioteca, oficinas y pasillos registran porcentajes menores. En conjunto, esto indica que los espacios con mayor uso y equipos de valor requieren mayor control y supervisión.

Pregunta 5

¿Conoce los sistemas de seguridad implementados actualmente en el pabellón como cámaras o alarmas? Conviene aclarar que la base para los porcentajes es de seis participantes en total, y que corresponden a respuestas múltiples, dado que algunos encuestados indicaron varios ambientes.

Personal administrativo

Figura 3.13: *Reconocimiento de sistemas de seguridad según administrativos.*

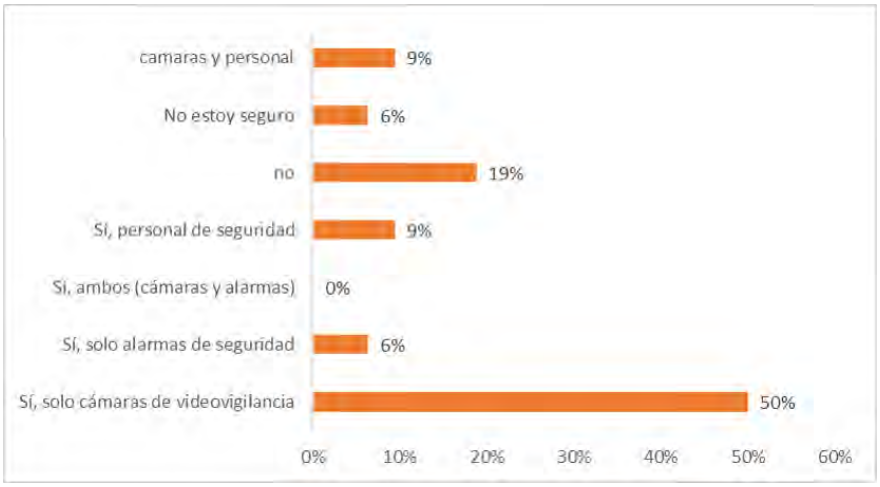


En el grupo de administrativos, las respuestas evidencian que los sistemas más reconocidos son las cámaras de seguridad (50 %), seguidas por la mención conjunta de cámaras y alarmas (17 %) y la presencia de personal de seguridad (17 %). Un 17 % indicó no

estar seguro de las medidas implementadas. Dado que la pregunta fue de opción múltiple, los resultados reflejan la frecuencia con que se mencionan los sistemas, mostrando que las cámaras son el elemento más identificado dentro del pabellón.

Docentes

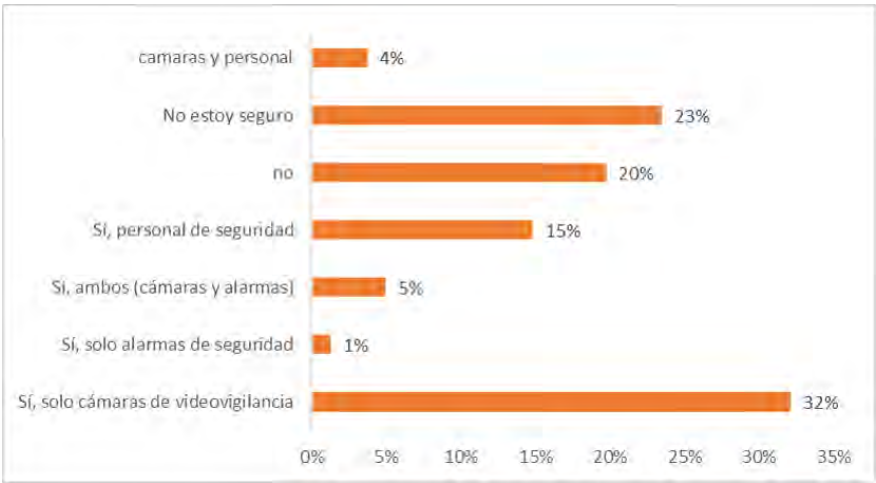
Figura 3.14: *Reconocimiento de sistemas de seguridad según los docentes.*



En el caso de los docentes, el 50 % identificó la existencia de cámaras de seguridad, mientras que un 9 % mencionó la presencia de personal de seguridad y otro 9 % la combinación de cámaras y personal. En menor medida, un 6 % señaló las alarmas, y un porcentaje similar no está seguro de los sistemas implementados. Además, un 19 % indicó no conocer ningún sistema de seguridad. En conjunto, se evidencia que las cámaras son el medio más reconocido, aunque persiste un nivel limitado de conocimiento general sobre las medidas existentes en el pabellón.

Estudiantes

Figura 3.15: *Reconocimiento de sistemas de seguridad según los estudiantes.*



En el grupo de estudiantes, el 32 % señaló conocer la presencia de cámaras de seguridad, mientras que un 15 % mencionó personal de seguridad y un 5 % identificó la existencia conjunta de cámaras y alarmas. En menor proporción, un 4 % indicó cámaras y personal de seguridad, y solo un 1 % mencionó alarmas. Por otro lado, un 20 % manifestó no conocer ningún sistema y un 23 % no está seguro de su existencia. En general, se observa que el reconocimiento de los sistemas de seguridad es bajo, predominando el conocimiento de las cámaras sobre otros mecanismos de protección.

Análisis comparativo

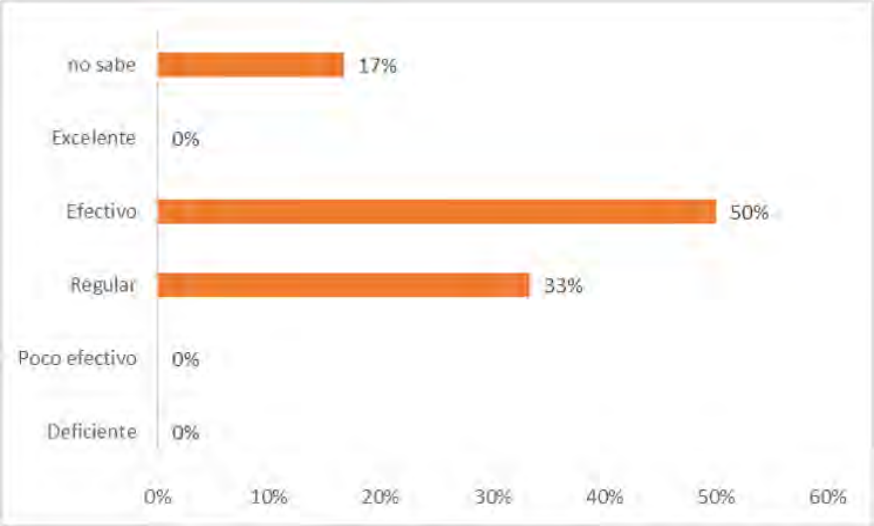
En los tres grupos encuestados, las cámaras de seguridad son el sistema más reconocido dentro del pabellón. Los administrativos (50 %) y docentes (50 %) presentan un nivel similar de conocimiento, mientras que entre los estudiantes (32 %) el reconocimiento es menor. En general, los otros sistemas como alarmas o personal de seguridad son mencionados en porcentajes reducidos, y una proporción importante de encuestados indica no estar seguro o no conocer las medidas implementadas. Esto evidencia una percepción limitada y desigual del sistema de seguridad existente, centrada principalmente en las cámaras.

Pregunta 5.1

¿Cómo calificaría su efectividad de los sistemas de seguridad? Cabe recalcar que la valoración de la efectividad se refiere a los sistemas de seguridad que cada encuestado señaló en la pregunta anterior

Personal administrativo

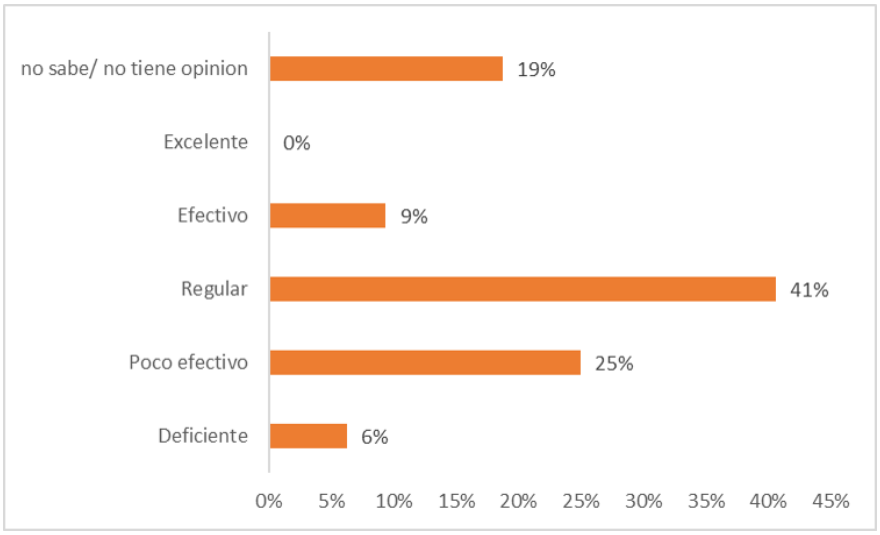
Figura 3.16: *Efectividad de los sistemas de seguridad según administrativos*



En el grupo de administrativos, el 50 % considera que los sistemas de seguridad son efectivos, mientras que un 33 % los califica como regulares y un 17 % no sabe o no opina. En conjunto, la mayoría percibe que las medidas implementadas cumplen adecuadamente su función, aunque una parte significativa mantiene una valoración intermedia, lo que sugiere oportunidades de mejora en su funcionamiento o visibilidad.

Docentes

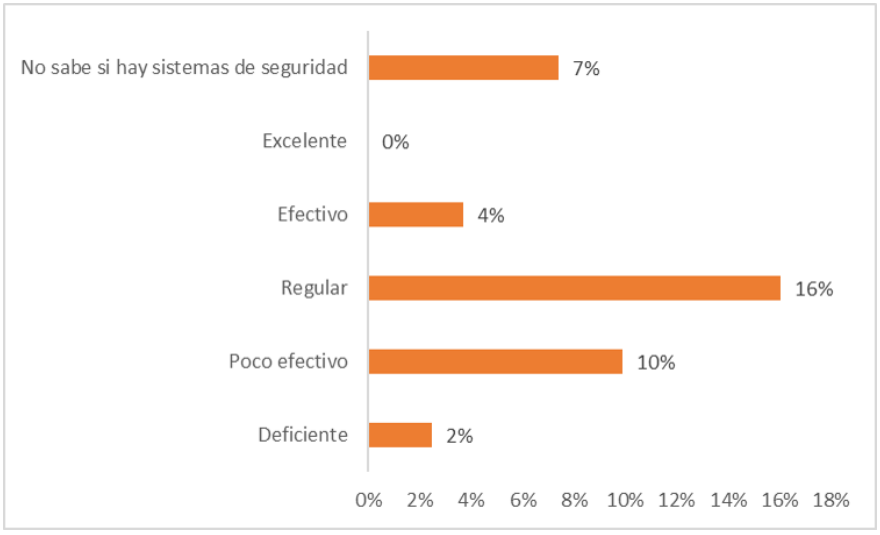
Figura 3.17: *Efectividad de los sistemas de seguridad según los docentes.*



En el grupo de docentes, el 41 % califica los sistemas de seguridad como regulares, mientras que un 25 % los considera poco efectivos y solo un 9 % los percibe como efectivos. Además, un 19 % no tiene opinión y un 6 % los evalúa como deficientes. En conjunto, la mayoría presenta una percepción moderada o crítica, lo que refleja cierta insatisfacción con la efectividad de las medidas de seguridad implementadas en el pabellón.

Estudiantes

Figura 3.18: *Efectividad de los sistemas de seguridad según el personal según los estudiantes.*



En el caso de los estudiantes, el 16 % califica los sistemas de seguridad como regulares, un 10 % los considera poco efectivos y un 4 % los percibe como efectivos. Por otro lado, el 7 % no tiene opinión y un 2 % los evalúa como deficientes. En general, la mayoría muestra una percepción neutral o baja, evidenciando limitada confianza en la eficacia de las medidas de seguridad.

Análisis comparativo

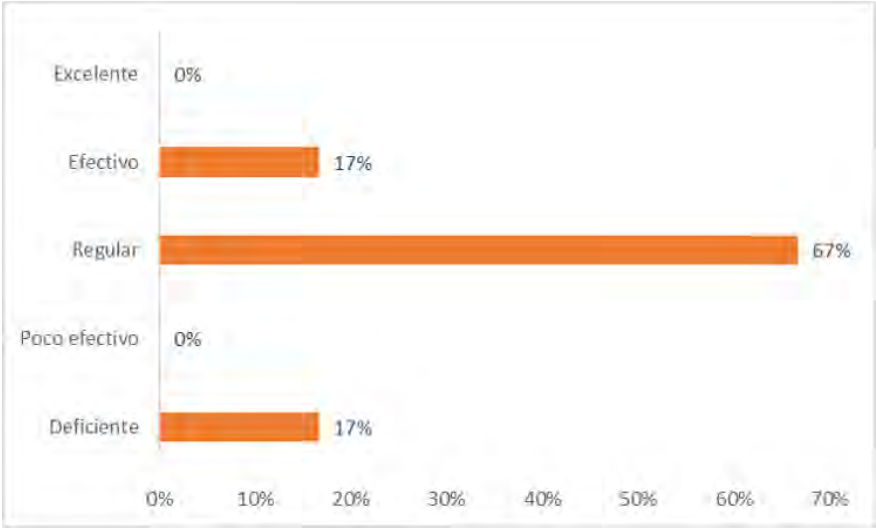
Al comparar los tres grupos, se observa que los administrativos son quienes mejor valoran la efectividad de los sistemas de seguridad, con un 50 % que los considera efectivos. En cambio, los docentes y estudiantes presentan percepciones más moderadas o críticas, predominando las calificaciones de "regular" o "poco efectivo". En conjunto, esto refleja que, aunque las medidas actuales son reconocidas y valoradas positivamente por el personal administrativo, persiste una percepción de mejora necesaria entre docentes y estudiantes respecto a su desempeño y alcance.

Pregunta 6

¿Cuál es su opinión sobre la suficiencia de los mecanismos de control de acceso?

Personal administrativo

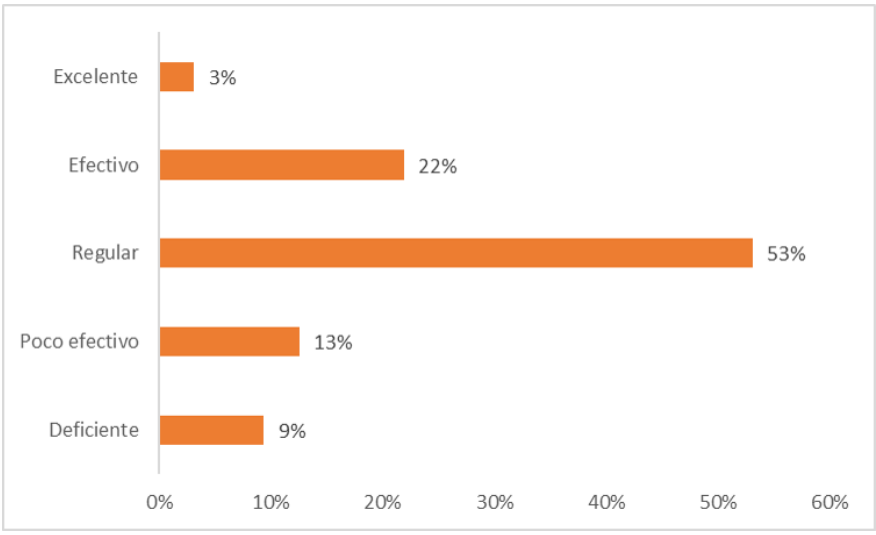
Figura 3.19: *Suficiencia de los controles de acceso según el personal administrativo.*



En el grupo de administrativos, la mayoría de los encuestados 67 % considera que los mecanismos de control de acceso son regulares, mientras que un 17 % los califica como efectivos y otro 17 % como deficientes. Estos resultados reflejan una percepción intermedia respecto a la suficiencia de los controles implementados, lo que sugiere la necesidad de fortalecer las medidas de acceso para mejorar la seguridad en el pabellón.

Docentes

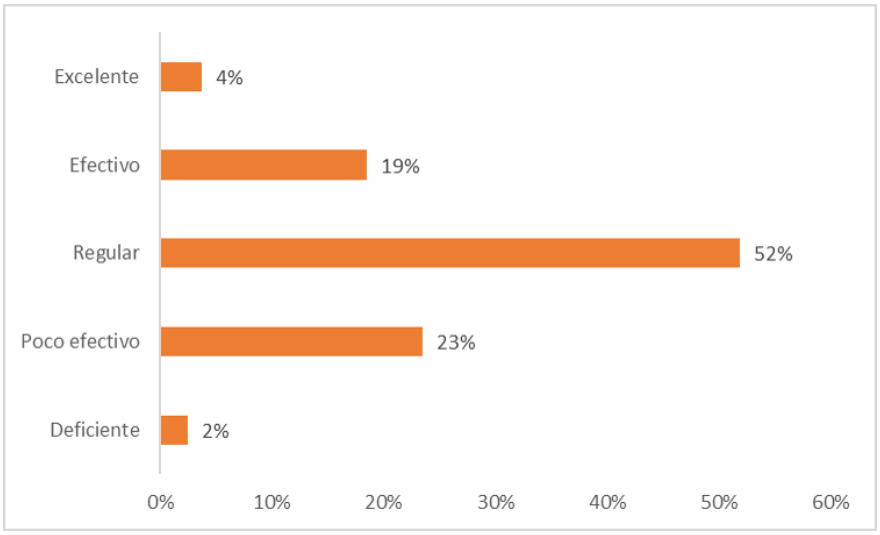
Figura 3.20: *Suficiencia de los controles de acces según los docentes.*



En el grupo de docentes, la mayoría 53 % califica los mecanismos de control de acceso como regulares, mientras que un 22 % los considera efectivos y un 13 % poco efectivos. En menor medida, un 9 % los percibe como deficientes y un 3 % como excelentes. En conjunto, los resultados reflejan una valoración predominantemente intermedia, lo que sugiere que, si bien existen mecanismos de control, aún se perciben oportunidades de mejora en su eficacia y alcance.

Estudiantes

Figura 3.21: *Suficiencia de los controles de acces según los estudiantes.*



En el grupo de estudiantes, la mayoría (52 %) califica los mecanismos de control de acceso como regulares, mientras que un 19 % los considera efectivos y un 23 % poco efectivos. En menor proporción, un 4 % los valora como excelentes y un 2 % como deficientes. En conjunto, predomina una percepción moderada, que refleja una confianza parcial en los mecanismos de control y evidencia la necesidad de fortalecer las medidas existentes.

Análisis comparativo

En los tres grupos encuestados predomina la percepción de que los mecanismos de control de acceso son regulares, con porcentajes similares entre administrativos (67 %),

docentes (53 %) y estudiantes (52 %). Solo una minoría los considera efectivos, lo que indica una valoración intermedia respecto a su suficiencia.

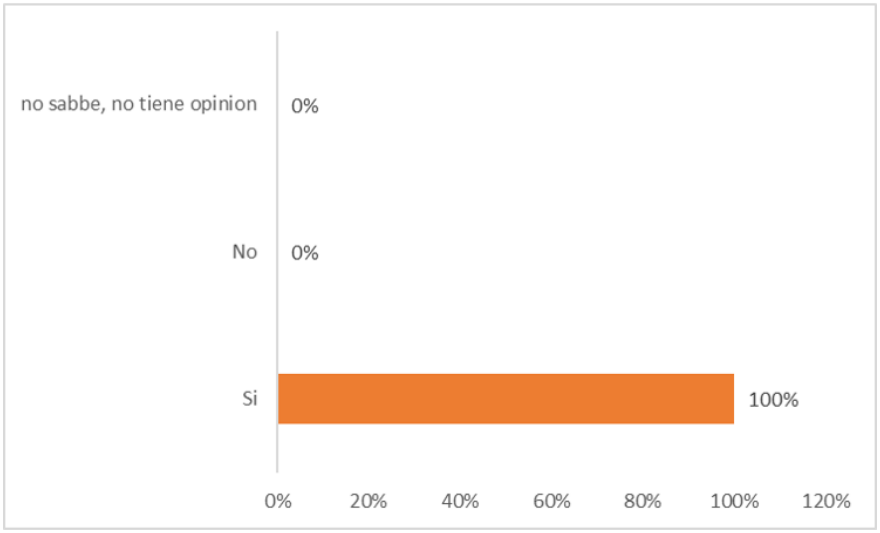
En general, los resultados sugieren que, aunque existen mecanismos implementados, estos no son percibidos como totalmente adecuados. Por ello, se recomienda reforzar las medidas de control y supervisión para mejorar la seguridad en los diferentes ambientes del pabellón

Pregunta 7

¿Considera que un sistema de seguridad basado en dispositivos inteligentes podría mejorar la seguridad?

Personal administrativo

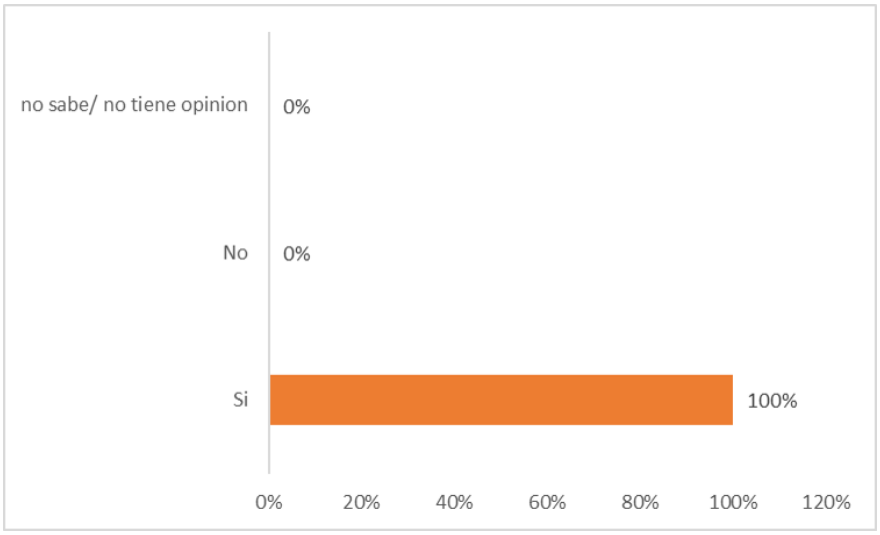
Figura 3.22: *Percepción sobre la seguridad inteligente según personal administrativo*



En el grupo de administrativos, la totalidad (100 %) considera que la implementación de un sistema de seguridad basado en dispositivos inteligentes contribuiría a mejorar la seguridad. Este resultado evidencia una percepción completamente positiva y un consenso generalizado sobre la utilidad y eficacia potencial de este tipo de tecnologías en el entorno institucional.

Docentes

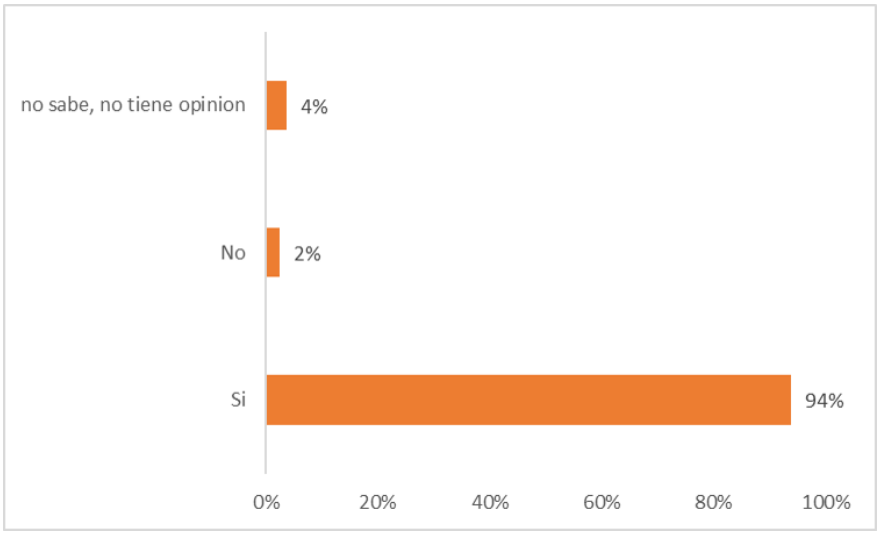
Figura 3.23: *Percepción sobre la seguridad inteligente según docentes.*



De igual manera, el 100 % de los docentes comparte esta percepción positiva, lo que evidencia un consenso general entre ambos grupos respecto al impacto favorable que tendría la implementación de este tipo de sistemas en la seguridad del entorno universitario.

Estudiantes

Figura 3.24: *Percepción sobre la seguridad inteligente según estudiantes.*



Por su parte, entre los estudiantes predomina también una opinión favorable: el 94 % respondió afirmativamente, mientras que un 2 % no lo considera así y un 4 % no tiene una

opinión definida.

Análisis comparativo

La comparación entre los tres grupos revela un alto grado de coincidencia en la percepción sobre el potencial de los sistemas de seguridad inteligentes. Tanto administrativos como docentes manifiestan unanimidad (100 %) en su valoración positiva, mientras que los estudiantes, aunque presentan un ligero margen de desacuerdo (2 %) y de indecisión (4 %), mantienen una tendencia claramente favorable (94 %).

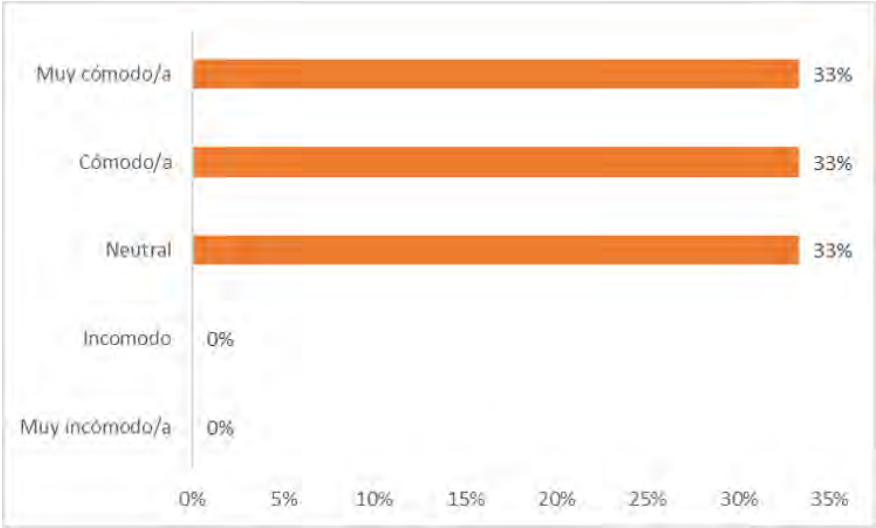
Estos resultados evidencian una percepción general de confianza en las tecnologías inteligentes como herramienta para mejorar la seguridad institucional. La mínima diferencia observada en el grupo estudiantil podría asociarse a un menor conocimiento técnico o menor involucramiento directo con los sistemas de seguridad, sin que ello afecte la valoración positiva global.

Pregunta 8

¿Qué tan cómodo/a se sentiría usando identificación biométrica para acceder a áreas restringidas?

Personal administrativo

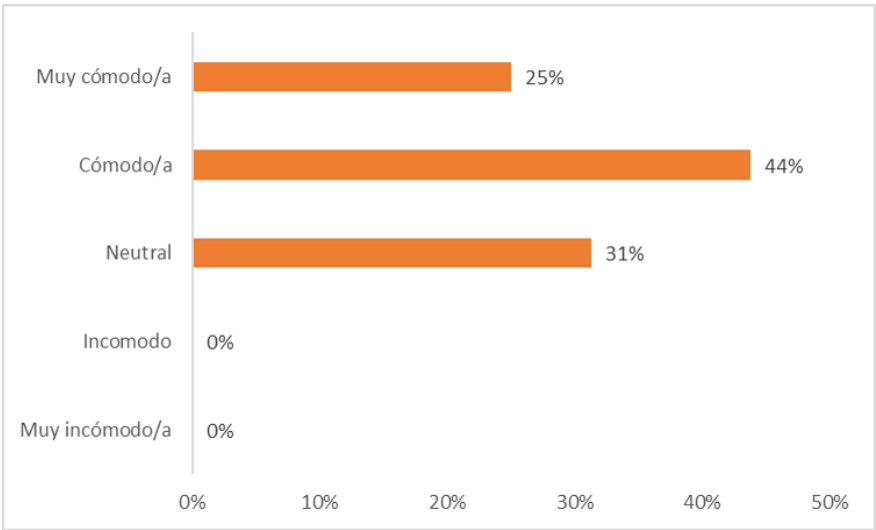
Figura 3.25: *Comodidad conla identificación biométrica según personal administrativo.*



En el grupo de administrativos, las opiniones se encuentran equilibradas: el 33 % se sentiría muy cómodo, otro 33 % cómodo y el 33 % restante mantiene una posición neutral frente al uso de identificación biométrica para acceder a áreas restringidas. Esto indica que, si bien existe una disposición favorable hacia la tecnología biométrica, aún hay cierto grado de reserva o expectativa en torno a su implementación.

Docentes

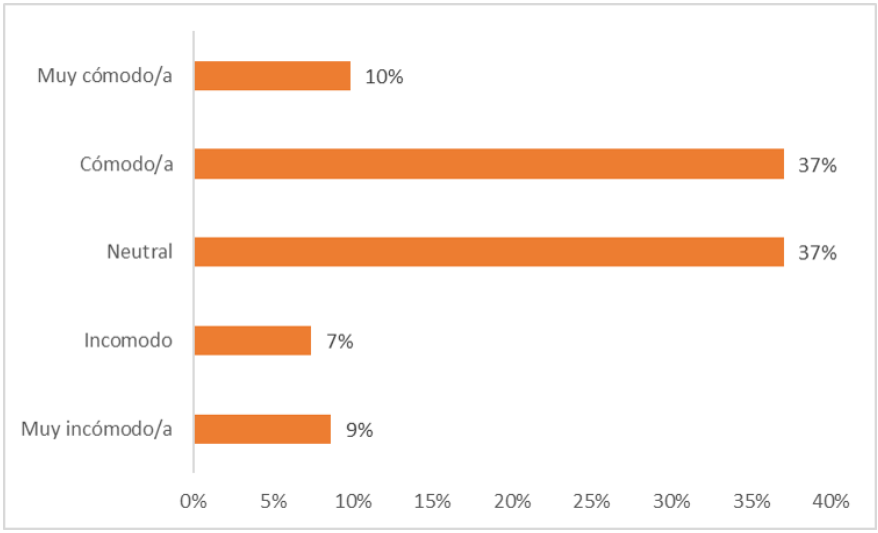
Figura 3.26: *Comodidad conla identificación biométrica según docentes.*



En el grupo de administrativos, las respuestas se distribuyen equitativamente: un 33 % se sentiría muy cómodo, otro 33 % cómodo y el 33 % neutral. Esto refleja una actitud moderadamente favorable hacia el uso de la biometría, aunque con cierta prudencia. En el caso de los docentes, el 25 % manifiesta sentirse muy cómodo, el 44 % cómodo y el 31 % neutral, lo que también evidencia una tendencia positiva, pero sin un consenso pleno.

Estudiantes

Figura 3.27: *Comodidad conla identificación biométrica según estudiantes.*



En el grupo de administrativos, las opiniones se dividen equitativamente: un 33 % se sentiría muy cómodo, otro 33 % cómodo y el 33 % neutral frente al uso de identificación biométrica para acceder a áreas restringidas. De manera similar, entre los docentes predomina una tendencia positiva, con un 25 % que se sentiría muy cómodo, un 44 % cómodo y un 31 % neutral, lo que evidencia una aceptación mayoritaria, aunque sin unanimidad.

En cuanto a los estudiantes, el 10 % manifestó sentirse muy cómodo, el 37 % cómodo, el 37 % neutral, el 7 % incómodo y el 9 % muy incómodo. Esta distribución muestra percepciones más diversas, con una mayoría moderadamente favorable, pero también con una proporción minoritaria que expresa incomodidad ante el uso de la biometría.

Análisis comparativo

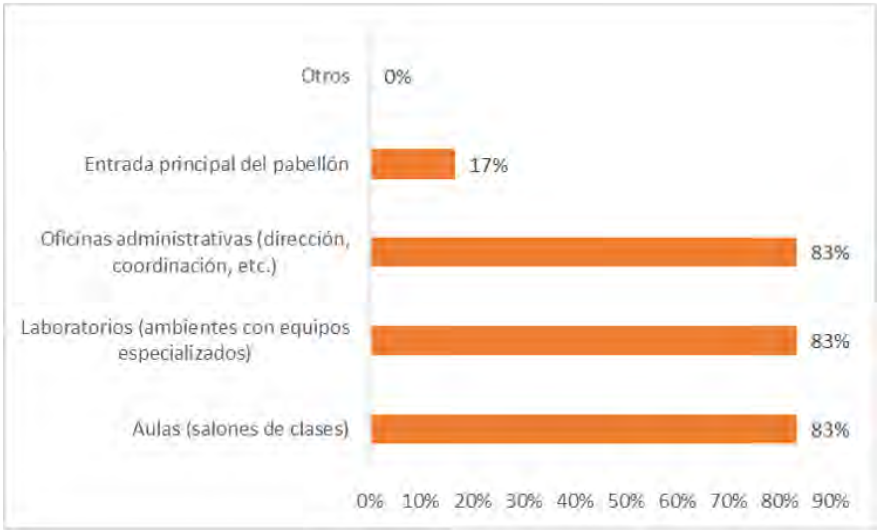
La comparación entre los tres grupos revela una tendencia general de aceptación hacia el uso de identificación biométrica, aunque con distintos niveles de confianza. Administrativos y docentes presentan valoraciones más positivas y equilibradas, mientras que los estudiantes muestran mayor dispersión en sus respuestas. Esto podría relacionarse con diferencias en la familiaridad o en la percepción de privacidad asociada al uso de datos biométricos. En conjunto, los resultados reflejan que la biometría es vista mayormente como una medida viable y segura, pero que aún requiere estrategias de sensibilización y confianza para su adopción plena.

Pregunta 9

¿En qué ambientes considera que debería implementarse un sistema de control de acceso?

Personal administrativo

Figura 3.28: *Ambientes que requieren sistemas de control de acceso según personal administrativo*

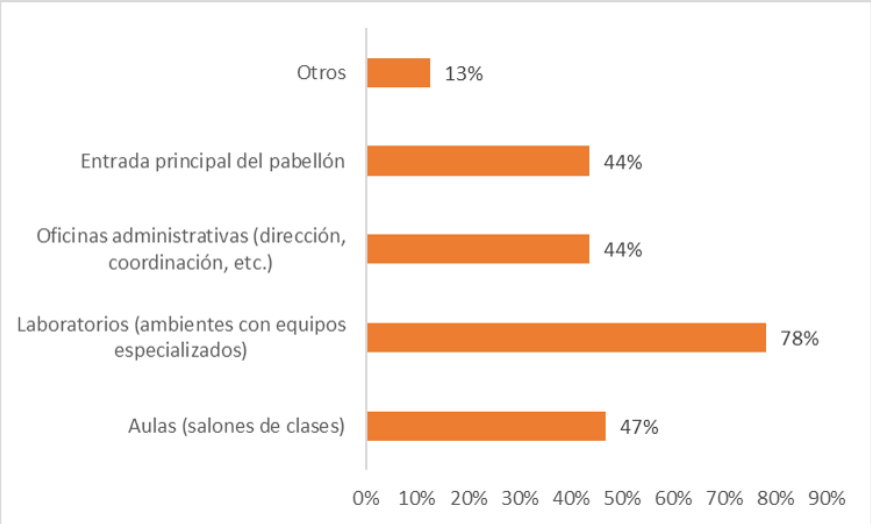


Los resultados muestran que los encuestados consideran que el sistema de control de acceso debería implementarse principalmente en oficinas administrativas (83 %), laboratorios

(83 %) y aulas (83 %), mientras que un porcentaje menor lo sugiere para la entrada principal (17 %). Esto evidencia una mayor preocupación por restringir el acceso en los espacios donde se realizan actividades académicas y administrativas sensibles

Docentes

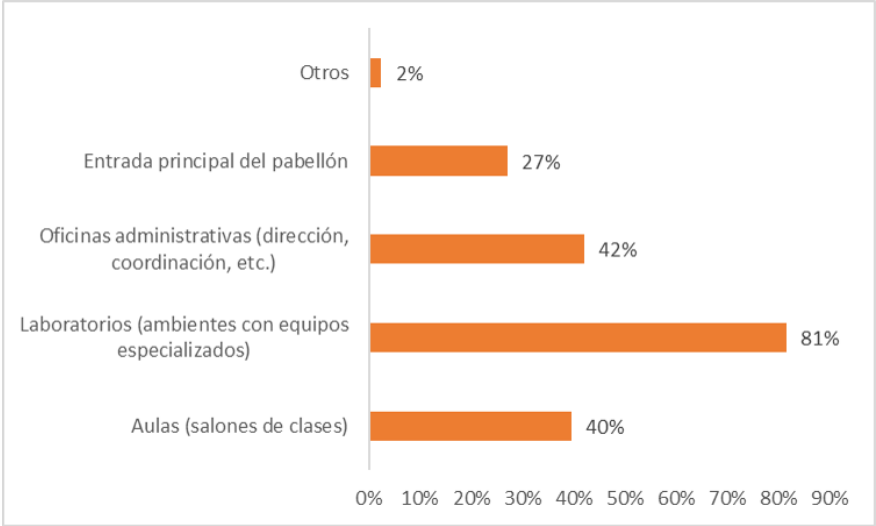
Figura 3.29: *Ambientes que requieren sistemas de control de acceso según docentes.*



En el grupo de docentes, los resultados muestran que el 78 % considera que el sistema de control de acceso debería implementarse en los laboratorios, seguido por las aulas (47 %), la entrada principal (44 %) y las oficinas administrativas (44 %). Además, un 13 % sugiere otros espacios, como los cubículos de docentes. Esto refleja una mayor preocupación por proteger las zonas donde se realizan actividades académicas y de investigación.

Estudiantes

Figura 3.30: *Ambientes que requieren sistemas de control de acceso según estudiantes.*



En el grupo de estudiantes, la mayoría (81 %) considera que el sistema de control de acceso debería instalarse en los laboratorios, seguidos por las oficinas administrativas (42 %) y las aulas (40 %). Un 27 % opina que también debería aplicarse en la entrada principal, mientras que un 2 % sugiere otros espacios, como los círculos de estudio. Estos resultados evidencian que los estudiantes priorizan la seguridad en los laboratorios, donde se manejan equipos y materiales especializados.

Análisis comparativo

En general, los tres grupos coinciden en que los laboratorios son los espacios donde resulta más necesario implementar un sistema de control de acceso. Los administrativos también priorizan las oficinas y aulas, los docentes distribuyen su atención entre varios ambientes, incluyendo la entrada principal y cubículos docentes, mientras que los estudiantes centran su interés en los laboratorios y, en menor medida, en las oficinas y aulas.

Pregunta 10

¿Qué componentes considera más importantes para un nuevo sistema de seguridad?

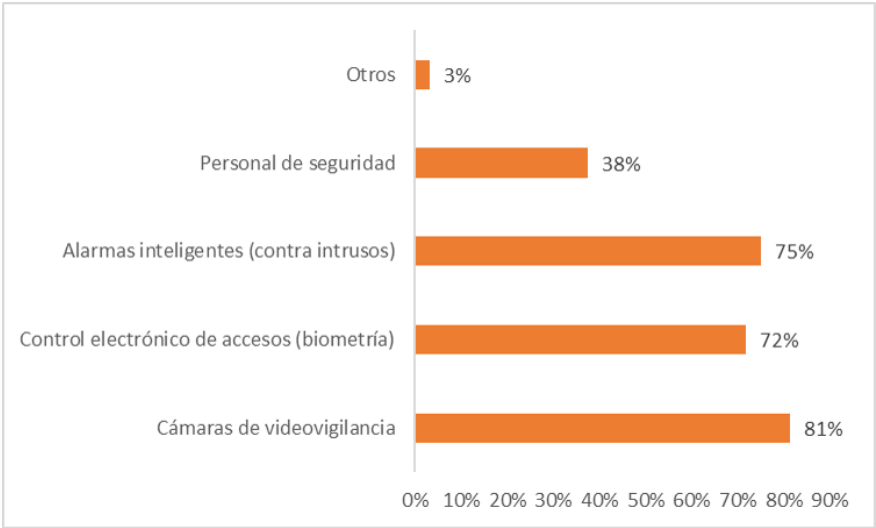
Personal administrativo

Figura 3.31: *Componentes más importantes para un sistema de seguridad según administrativoS.*

En el grupo administrativo, los resultados muestran que las cámaras de videovigilancia son consideradas el componente más importante (100 %), seguidas por las alarmas inteligentes (83 %) y el control electrónico de accesos (67 %). En menor medida, se valora la presencia de personal de seguridad (33 %). Esto refleja una clara preferencia por soluciones tecnológicas que fortalezcan la vigilancia y el control de los espacios.

Docentes

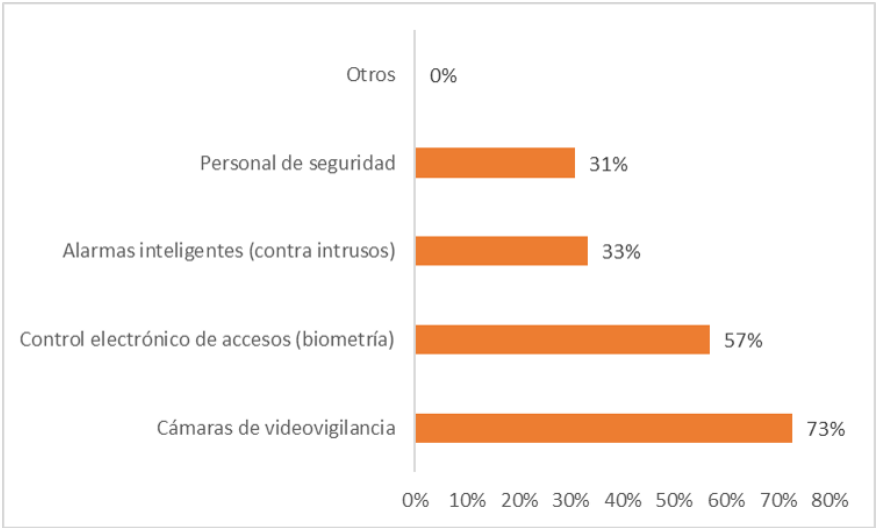
Figura 3.32: *Componentes más importantes para un sistema de seguridad segun docentes.*



En el grupo de docentes, los resultados indican que las cámaras de videovigilancia (81 %) son consideradas el componente más importante del sistema de seguridad, seguidas por las alarmas inteligentes (75 %) y el control electrónico de accesos (72 %). Un 38 % valora la presencia de personal de seguridad, mientras que un 3 % menciona otros elementos, como la identificación del personal o un sistema de seguridad integral. Esto muestra una preferencia general por tecnologías que mejoren la vigilancia y el control, complementadas por la presencia humana.

Estudiantes

Figura 3.33: *Componentes más importantes para un sistema de seguridad según estudiantes.*



En el grupo de estudiantes, los resultados muestran que las cámaras de videovigilancia (73 %) son consideradas el componente más importante del sistema de seguridad, seguidas por el control electrónico de accesos (57 %). En menor medida, se valoran las alarmas inteligentes (33 %) y la presencia de personal de seguridad (31 %). Esto refleja una inclinación hacia el uso de herramientas tecnológicas que brinden mayor control y monitoreo dentro del entorno universitario.

Análisis comparativo

De manera general, los tres grupos coinciden en que las cámaras de videovigilancia son el componente más importante dentro de un sistema de seguridad, al considerarlas esenciales para la supervisión y el registro de actividades. Tanto administrativos como docentes y estudiantes priorizan este elemento por su capacidad para disuadir incidentes y apoyar la detección de riesgos en tiempo real.

Sin embargo, se observan diferencias en la valoración de otros componentes. Los administrativos otorgan mayor relevancia a las alarmas inteligentes y al control electrónico de accesos, los docentes muestran una preferencia equilibrada entre estos tres elementos

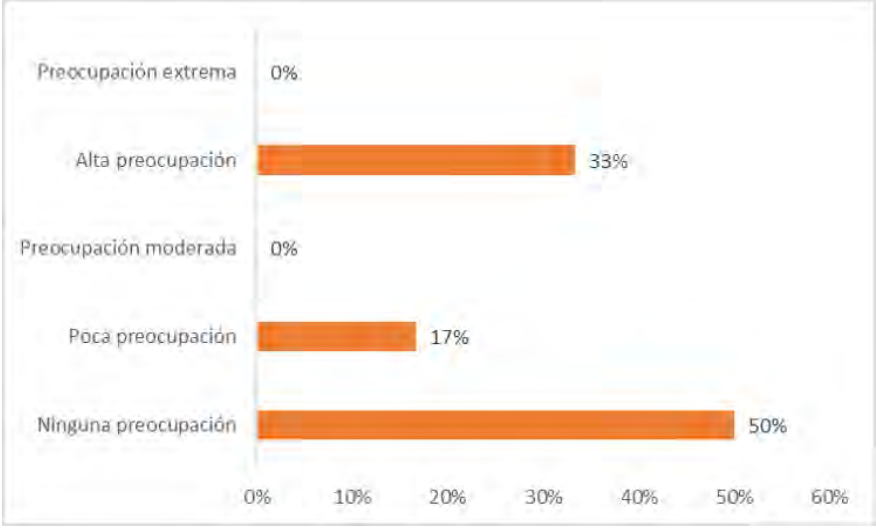
tecnológicos, mientras que los estudiantes dan más peso al control de accesos, dejando en segundo plano las alarmas y el personal de seguridad. En conjunto, los resultados evidencian una tendencia hacia la automatización y digitalización de la seguridad, destacando el papel complementario del recurso humano.

Pregunta 11

¿Cuál es su nivel de preocupación respecto a la privacidad de sus datos personales al interactuar con sistemas de videovigilancia o control de acceso?

Personal administrativo

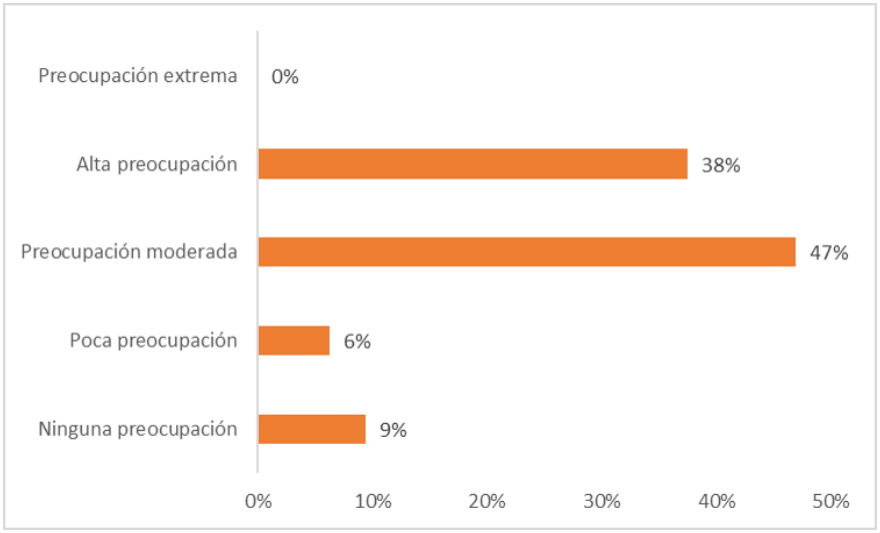
Figura 3.34: *Preocupación sobre la privacidad de los datos personales según administrativos.*



Los resultados muestran que la mitad (50 %) no manifiesta preocupación respecto a la privacidad de sus datos personales al interactuar con sistemas de videovigilancia o control de acceso. Un 33 % presenta un alto nivel de preocupación, mientras que un 17 % muestra poca preocupación. Esto indica que, aunque una parte de los estudiantes es consciente de los riesgos asociados al manejo de sus datos, la mayoría percibe estos sistemas como seguros o no considera que representen una amenaza directa a su privacidad.

Docentes

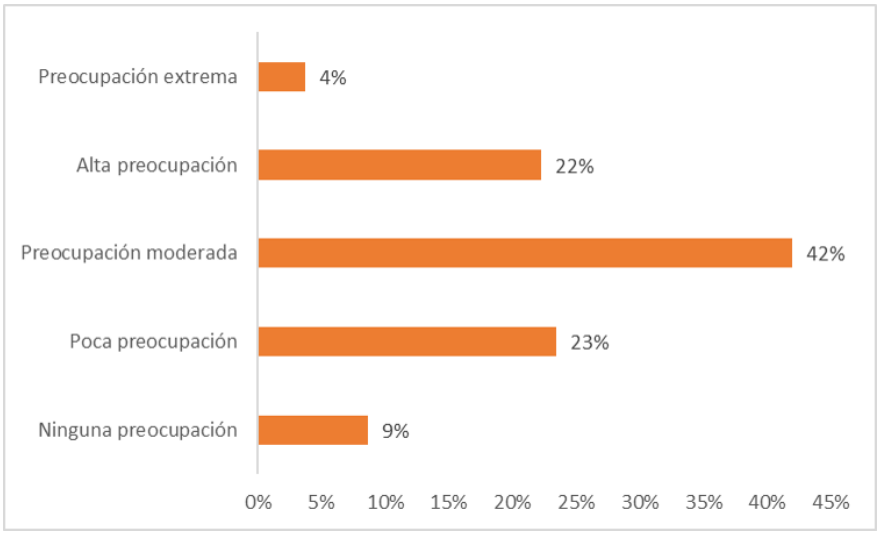
Figura 3.35: *Preocupación sobre la privacidad de los datos personales según docentes.*



En el grupo de docentes, los resultados evidencian que la mayoría (47 %) manifiesta una preocupación moderada por la privacidad de sus datos personales al interactuar con sistemas de videovigilancia o control de acceso. Un 38 % presenta un alto nivel de preocupación, mientras que solo un pequeño porcentaje expresa poca (6 %) o ninguna preocupación (9 %). Esto refleja una actitud más cautelosa por parte de los docentes, quienes muestran mayor sensibilidad frente al uso y protección de su información personal.

Estudiantes

Figura 3.36: *Preocupación sobre la privacidad de los datos personales según estudiantes.*



En el grupo de estudiantes, los resultados muestran que la mayoría (42 %) presenta una preocupación moderada respecto a la privacidad de sus datos personales al interactuar con sistemas de videovigilancia o control de acceso. Un 22 % manifiesta alta preocupación y un 4 % una preocupación extrema, mientras que el resto expresa poca (23 %) o ninguna preocupación (9 %). Esto evidencia una percepción equilibrada, donde la mayoría reconoce cierto nivel de riesgo, aunque sin considerarlo alarmante.

Análisis comparativo

De forma comparativa, los tres grupos muestran diferentes niveles de preocupación frente a la privacidad de sus datos personales. Los docentes son quienes presentan una actitud más cautelosa, con predominio de una preocupación moderada o alta, lo que refleja mayor conciencia sobre los posibles riesgos del tratamiento de información personal.

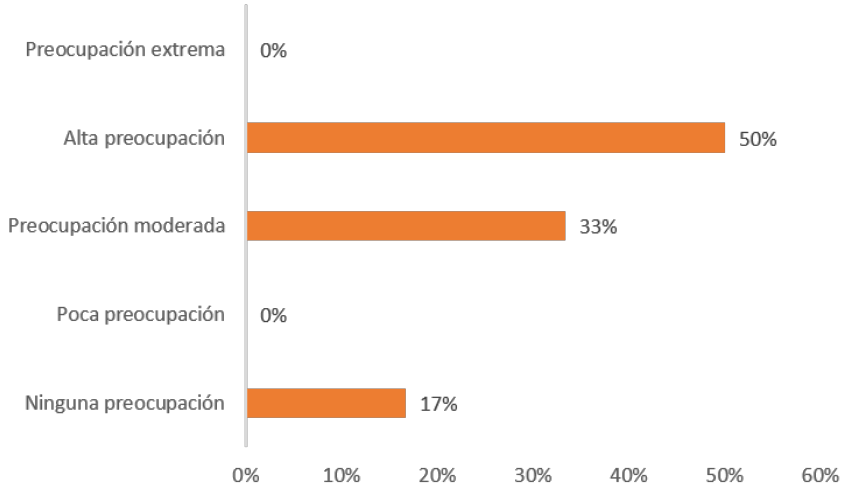
Por su parte, los estudiantes muestran una postura más equilibrada, donde predomina la preocupación moderada, aunque también existe un sector con baja o nula preocupación, lo que sugiere confianza o desconocimiento sobre el tema. En cambio, los administrativos tienden a mostrar menor inquietud, considerando los sistemas de videovigilancia y control de acceso como herramientas necesarias para la seguridad más que como una amenaza a la privacidad.

Pregunta 12

¿Qué nivel de confianza le genera la forma en que se gestiona sus datos personales recopilados mediante los sistemas de seguridad en general, en cuanto a su recolección, uso, almacenamiento y protección?

Personal administrativo

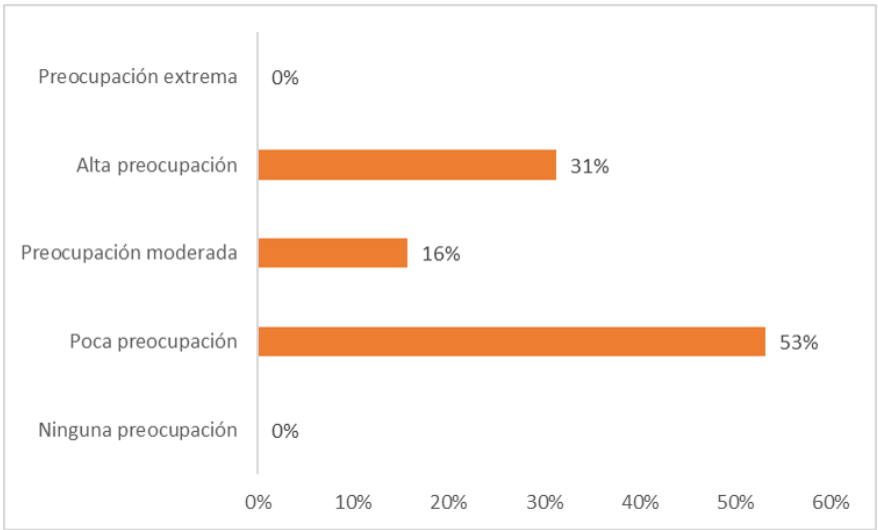
Figura 3.37: *Confianza en la gestión de datos personales según personal administrativo.*



En el grupo administrativo, los resultados muestran que la mitad (50 %) expresa un alto nivel de confianza en la gestión de sus datos personales recopilados por los sistemas de seguridad, mientras que un 33 % manifiesta una confianza moderada y un 17 % indica ninguna confianza. Esto sugiere que, aunque la mayoría percibe una gestión adecuada de la información, aún existe un sector que mantiene ciertas dudas sobre la protección y el uso de sus datos personales.

Docentes

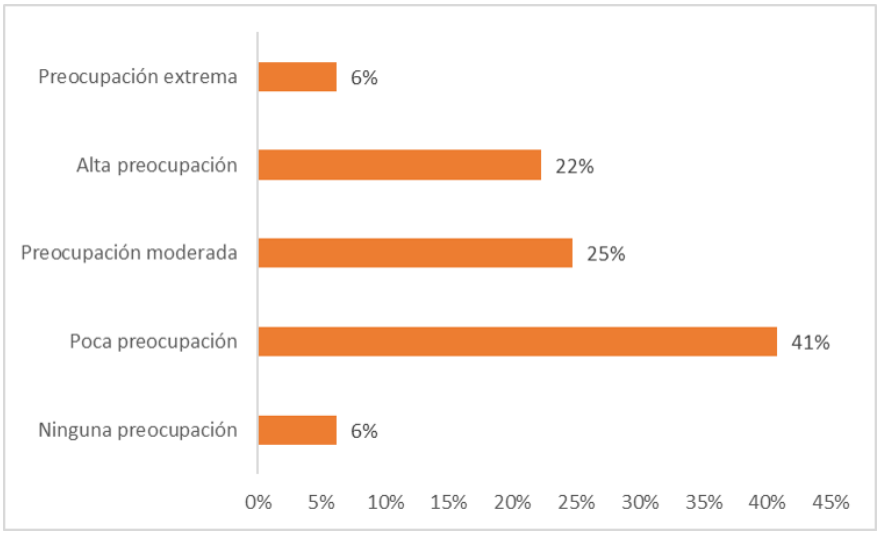
Figura 3.38: *Confianza en la gestión de datos personales según docentes.*



En el grupo de docentes, los resultados indican que la mayoría (53 %) muestra poca confianza en la forma en que se gestionan sus datos personales recopilados por los sistemas de seguridad. Un 31 % expresa alta confianza, mientras que un 16 % mantiene una confianza moderada. Esto refleja una percepción más reservada por parte de los docentes, quienes, en general, parecen mostrar cierta incertidumbre sobre el manejo y la protección de su información personal.

Estudiantes

Figura 3.39: *Confianza en la gestión de datos personales según estudiantes.*



En el grupo de estudiantes, los resultados muestran que la mayoría (41 %) presenta poca confianza en la forma en que se gestionan sus datos personales por los sistemas de seguridad. Un 25 % manifiesta una confianza moderada, mientras que un 22 % expresa alta confianza. En los extremos, un 6 % indica confianza total y otro 6 % refleja ninguna confianza. En conjunto, estos resultados evidencian una percepción dividida, aunque con una tendencia general hacia la desconfianza parcial en los procesos de recolección y protección de datos personales.

Análisis comparativo

Comparativamente, los administrativos muestran mayor confianza en la gestión de sus datos personales, mientras que los docentes reflejan mayor desconfianza y cautela frente al manejo de su información. Los estudiantes mantienen una posición intermedia, con predominio de poca confianza. En conjunto, se observa que, aunque los sistemas de seguridad son valorados, persisten dudas sobre la protección y el uso adecuado de los datos recopilados.

Capítulo 4

Analisis del Entorno y Requisitos del Sistema

4.1. Contexto General del Pabellón

4.1.1. Identificación de Activos y Caracterización de Ambientes

El pabellón de la Escuela Profesional de Ingeniería Informática y de Sistemas se encuentra ubicado en el campus universitario de la Universidad Nacional de San Antonio Abad del Cusco. Cuenta con aulas, laboratorios, oficinas administrativas y espacios comunes, donde se desarrollan actividades académicas y técnicas con equipos de valor considerable.

A fin de identificar los espacios prioritarios para la implementación del sistema de seguridad inteligente, se realizó un inventario general de los ambientes distribuidos por piso. La siguiente tabla detalla las aulas, laboratorios, oficinas y el equipamiento tecnológico presente en cada nivel del pabellón.

Tabla 4.1: *Distribución de ambientes y equipos por piso del pabellón de Ingeniería*

Piso	Ambiente	Cantidad	Equipos estimados
1.er	Aulas de clase	5	5 proyectores, 1 ap
	Centro federado	1	1router
	Deposito de Limpieza	1	suministros de limpieza
	Sala de uso multiple	1	muebles
2.º	Aulas de clase	4	4 proyectores
	Laboratorio de informática	1	18 PCs
	Bilbioteca virtual	1	4 PCs
	Biblioteca	1	3 PCs,
	Deposito de libros	1	3 PCs,
3.er	Laboratorio de informática	10	50 PCs, 1 servidor
	Oficinas	4	3 PCs, documentos
	Sala de uso multiple	1	muebles
4.º	Cubiculos docentes	5	31 PCs, 1 proyector
	Laboratorio de informática	1	13 PCs, 1 servidor
	Oficina de coordinación	2	2 PCs, documentos
	Circulo de estudios	2	1 laptop, 1 router
	Sala de uso multiple	1	1 pantalla interactiva, 2 monitores, 1 AP

4.1.2. Evaluación de las Medidas de Seguridad Física y Electrónica Existentes

El pabellón de Ingeniería presenta las siguientes condiciones de seguridad:

- **Cobertura de sistemas:**
  - Videovigilancia limitada al tercer piso (3 cámaras IP)
  - Videovigilancia limitada al cuarto piso (7 camaras analogicas)
  - 4 sensores de alarma y una sirena ubicados en el cuarto piso

Actualmente, el pabellón dispone de un sistema de seguridad electrónica integrado por videovigilancia, sensores de alarma y una central de monitoreo, cuya operatividad es deficiente. La cobertura de cámaras es limitada, lo que restringe el monitoreo continuo de los espacios comunes y laboratorios; además, la falta de sistemas de respaldo de energía compromete la continuidad del servicio ante fallas eléctricas.

La mayor vulnerabilidad radica en la gestión de accesos, la cual se realiza de forma

manual mediante el préstamo de llaves físicas y el llenado de hojas de registro. Al no existir un encargado específico para esta labor, el proceso pierde rigurosidad, eliminando cualquier posibilidad de control y auditoría eficiente sobre quién ingresa a los ambientes del pabellón.

Esta falta de control se extiende al sistema de alarmas, el cual no es operado directamente por el personal responsable de la infraestructura. Como único complemento, se cuenta con el soporte de vigilancia física externa mediante rondas aleatorias del personal de seguridad general de la Universidad Nacional de San Antonio Abad del Cusco.

4.1.3. Percepción de los Usuarios Sobre la Seguridad

Nivel de seguridad percibido

Los resultados de la encuesta muestran que la situación actual es percibida mayoritariamente como regular, lo que evidencia que las condiciones existentes solo satisfacen de manera parcial los requerimientos esperados. Asimismo, una proporción significativa de los encuestados considera que el estado actual es bajo o muy bajo, lo que refleja la presencia de deficiencias en los mecanismos de seguridad y gestión implementados.

En contraste, solo una parte de la comunidad califica la situación como buena, mientras que no se registra ninguna valoración que la considere alta, lo cual pone de manifiesto la ausencia de un nivel óptimo de desempeño. En conjunto, estos resultados confirman que la situación actual presenta limitaciones estructurales y operativas, justificando la necesidad de diseñar un sistema integrado de seguridad electrónica, orientado a mejorar el monitoreo, el control de accesos y la respuesta ante incidentes en la Escuela Profesional de Ingeniería Informática y de Sistemas.

Tabla 4.2: *Percepción del nivel de seguridad del pabellón*

Respuesta	**Porcentaje (%)**
Muy Bajo	6 %
Bajo	25 %
Regular	43 %
Bueno	24 %
No sabe, no tiene opinion	2 %
Total	**100 %**

Experiencias personales de incidentes

Los resultados de la encuesta evidencian que una parte de la comunidad sí ha experimentado incidentes relacionados con la seguridad, lo que confirma la existencia de situaciones de riesgo dentro de la institución. Sin embargo, la mayoría de los encuestados manifiesta no haber vivido directamente este tipo de eventos, lo cual sugiere que los incidentes no afectan de manera uniforme a todos los miembros.

Aun así, la presencia de experiencias personales vinculadas a incidentes de seguridad pone de manifiesto la necesidad de fortalecer los mecanismos de prevención, monitoreo y respuesta, con el fin de reducir la ocurrencia de estos eventos y mejorar la percepción de seguridad en la Escuela Profesional de Ingeniería Informática y de Sistemas.

Tabla 4.3: *Experiencias personales sobre incidentes de seguridad*

Respuesta	**Porcentaje**
Sí	37 %
No	63 %
Total	100 %

Evaluación de sistemas actuales

Los resultados de la encuesta evidencian que la situación actual se caracteriza predominantemente por un nivel regular de efectividad, lo que indica que las medidas existentes cumplen solo de manera parcial con los objetivos de seguridad establecidos. Asimismo, una parte de los encuestados considera que el sistema actual es deficiente o poco efectivo, reflejando limitaciones en la prevención, detección y respuesta ante incidentes.

En contraste, solo un grupo reducido percibe las medidas como efectivas o excelentes, lo cual demuestra que el nivel de desempeño aún no alcanza un estándar óptimo. En conjunto, estos resultados confirman que la situación actual presenta debilidades operativas y tecnológicas, lo que justifica la necesidad de implementar un sistema integrado de seguridad electrónica que permita mejorar la eficiencia y confiabilidad de la gestión de la seguridad en la institución.

Tabla 4.4: *Percepción de la efectividad de la situación actual*

Respuesta	**Porcentaje**
Deficiente	5 %
Poco efectivo	19 %
Regular	53 %
Efectivo	19 %
Excelente	3 %
Total	100 %

4.1.4. Panorama Actual de la Gestión de Protección de Datos Personales

Se evaluó la gestión institucional de la protección de datos personales, considerando aspectos organizativos, normativos y técnicos. El diagnóstico evidenció que la institución no cuenta con políticas formalizadas ni con un área específica responsable de la gestión integral de la seguridad y protección de datos a nivel institucional.

En cuanto a medidas técnicas, la seguridad se sustenta principalmente en controles perimetrales básicos, como un firewall institucional. Otras acciones relacionadas con la seguridad de la información y el tratamiento de datos personales son gestionadas de manera descentralizada por cada dependencia, sin lineamientos ni procedimientos estandarizados. Esta situación refleja una gestión fragmentada, lo que limita el control, seguimiento y cumplimiento normativo en los procesos que involucran información sensible.

El análisis se apoyó en información cualitativa obtenida mediante consultas técnicas al personal institucional, realizadas de manera exploratoria, con la finalidad de identificar el estado actual de la gestión de protección de datos personales y las medidas de seguridad existentes.

4.1.5. Identificación de Brechas y Necesidades de Seguridad

A partir del análisis de campo, observaciones realizadas y los resultados de la encuesta aplicada a los usuarios del pabellón de Ingeniería Informática y de Sistemas, se identificaron diversas carencias en los aspectos relacionados con la seguridad física, tecnológica y organizativa. Estas deficiencias reflejan la necesidad de implementar una solución integrada y tecnológica para mejorar las condiciones actuales.

*1. Deficiencias en el control de acceso físico Se evidenció que las aulas del primer piso permanecen abiertas sin ningún tipo de control, lo que permite el ingreso libre de

personas, generando riesgos para los usuarios y el equipamiento. Actualmente, no se dispone de un sistema de control electrónico de accesos en laboratorios, oficinas o almacenes. La gestión basada exclusivamente en llaves físicas, sin un protocolo definido ni personal dedicado exclusivamente a su manejo, representa una debilidad significativa.

*2. Vigilancia y supervisión insuficiente Las áreas comunes del pabellón, como pasillos y accesos secundarios, presentan cobertura limitada de vigilancia. Los ambientes con equipamiento de alto valor, incluyendo laboratorios, salas de servidores y oficinas administrativas, cuentan con poca o nula supervisión, lo que los expone a posibles pérdidas materiales o accesos no autorizados.

*3. Limitaciones en los sistemas tecnológicos existentes Aunque existen cámaras de videovigilancia y un sistema de alarmas instalado, se identificó que su operación no es óptima. La cobertura de cámaras es parcial y algunas presentan fallas en calidad de imagen o conectividad. En cuanto al sistema de alarmas, el encargado no maneja directamente su operación, lo que evidencia la necesidad de capacitación, señalización adecuada y protocolos claros de uso.

*4. Ambientes desprotegidos y riesgos para elementos personales Los casilleros y áreas de almacenamiento de los usuarios se encuentran sin supervisión ni protección adicional. Esta situación genera percepción de inseguridad y ha motivado reportes de pérdidas de pertenencias. No se cuenta con un sistema o procedimiento formal para el registro y recuperación de objetos extraviados.

*5. Ausencia de un sistema de seguridad integrado Los componentes del sistema de seguridad funcionan de manera independiente, sin una plataforma central que permita su gestión conjunta. Esta falta de integración limita la capacidad de monitoreo en tiempo real, la coordinación ante incidentes y la generación de registros históricos de eventos, reduciendo la efectividad del sistema en general.

*6. Falta de procedimientos documentados No existen protocolos claros para la operación de los sistemas, el registro de incidencias o la respuesta ante emergencias, lo que dificulta la supervisión y control del entorno.

*7. Vulnerabilidades identificadas En resumen, las principales vulnerabilidades del sistema de seguridad del pabellón son:

- Cobertura de cámaras insuficiente, limitando la supervisión de los ambientes.
- Equipos sin respaldo energético, aumentando el riesgo ante cortes de electricidad.
- Registro de accesos de manera manual, sin trazabilidad centralizada.
- Falta de personal dedicado al control de accesos.
- Ausencia de integración entre videovigilancia, alarmas y control de accesos.
- Mantenimiento irregular de los equipos tecnológicos existentes.
- Áreas críticas y equipamiento de alto valor sin supervisión constante.
- Falta de procedimientos documentados para operación, registro de incidencias y respuesta ante emergencias.

4.2. Definición de Requerimientos del Sistema de Videovigilancia

Requerimientos Funcionales

- **RF-SV-01:** El subsistema debe permitir el flujo de video y monitoreo en tiempo real de todas las cámaras IP proyectadas en el pabellón.
- **RF-SV-02:** El subsistema debe incluir analíticas de detección de movimiento configurables por rangos de horarios no operativos.

- **RF-SV-03:** El subsistema debe incorporar analíticas de detección de intrusión automáticas en zonas críticas (laboratorios y salas técnicas).
- **RF-SV-04:** El subsistema debe permitir el despliegue de perímetros analíticos mediante cruce de línea virtual en los accesos del edificio.
- **RF-SV-05:** El subsistema debe procesar analíticas de merodeo (loitering) para alertar sobre permanencias inusuales en áreas sensibles.
- **RF-SV-06:** El subsistema debe incluir analíticas para la detección de objetos abandonados en vías de evacuación o la remoción de activos fijos.
- **RF-SV-07:** El subsistema debe prever la capacidad técnica de reconocimiento facial analítico sobre flujos de video específicos, conforme a la normativa de datos personales.

Requerimientos No Funcionales

- **RNF-SV-01:** La arquitectura de captura de video debe garantizar un régimen de operación continuo 24/7.
- **RNF-SV-02:** Los flujos de video y el almacenamiento local de evidencias deben estar protegidos mediante protocolos de cifrado de datos.
- **RNF-SV-03:** El dimensionamiento de las cámaras y del nvr debe admitir códecs de compresión avanzados (H.265 o superior) para optimizar el ancho de banda y el espacio en disco.

4.3. Definición de Requerimientos del Sistema de Alarmas de Intrusión

Requerimientos Funcionales

- **RF-SA-01:** El subsistema debe procesar señales de intrusión provenientes de sensores de movimiento (PIR).
- **RF-SA-02:** El subsistema debe activar salidas físicas de alerta sonora (sirenas) al confirmarse una intrusión o apertura forzada.
- **RF-SA-03:** El subsistema debe permitir el armado y desarmado del perímetro tanto de manera manual (teclados/credenciales) como por programación de horarios automáticos del pabellón.
- **RF-SA-04:** El subsistema debe mapear zonas independientes de alarma para discriminar con precisión el origen exacto del disparo de emergencia.

Requerimientos No Funcionales

- **RNF-SA-01:** El tiempo de procesamiento y propagación de la señal desde el sensor hasta el panel central no debe superar un segundo.
- **RNF-SA-02:** Los dispositivos centrales de alarma deben incluir un respaldo de energía por batería (UPS) que asegure una autonomía ante cortes eléctricos.
- **RNF-SA-03:** El subsistema debe almacenar localmente un histórico de eventos de armado, desarmado y fallas.

4.4. Definición de Requerimientos del Sistema de Control de Acceso

Requerimientos Funcionales

- **RF-CA-01:** El subsistema debe restringir o permitir el ingreso a las áreas protegidas únicamente mediante la validación de credenciales autorizadas (biometría, tarjetas o

contraseñas).

- **RF-CA-02:** El subsistema debe registrar cronológicamente cada intento de acceso (exitoso y fallido), detallando fecha, hora, punto de lectura e identidad.
- **RF-CA-03:** El subsistema debe permitir la estructuración de perfiles de usuario y privilegios de acceso basados en horarios y zonas específicas.
- **RF-CA-04:** El subsistema debe ejecutar bloqueos temporales automáticos en las lectoras tras registrar intentos fallidos consecutivos de autenticación.

Requerimientos No Funcionales

- **RNF-CA-01:** El tiempo de verificación de la credencial y la liberación física de la cerradura no debe superar los 2 segundos.
- **RNF-CA-02:** La base de datos local de control de accesos debe conservar los registros históricos de tránsito por un período mínimo de 12 meses para fines de auditoría.
- **RNF-CA-03:** La controladora de acceso debe poseer memoria no volátil para seguir operando y validando usuarios localmente de forma independiente si pierde conexión con el servidor.

4.5. Definición de Requerimientos de la Plataforma de Gestión Unificada

Requerimientos Funcionales

- **RF-PGU-01:** La plataforma debe centralizar de manera lógica la gestión y datos del subsistema de videovigilancia, alarmas y control de accesos bajo un único entorno de software.

- **RF-PGU-02:** La plataforma debe ejecutar la correlación lógica de eventos entre los subsistemas (ej. vincular la apertura forzada de una puerta controlada con el despliegue automático del flujo de la cámara más cercana).
- **RF-PGU-03:** El sistema debe centralizar, priorizar y unificar las notificaciones y alarmas críticas enviadas desde todos los terminales periféricos en una única consola de eventos.
- **RF-PGU-04:** La plataforma debe proveer una bitácora unificada de auditoría que registre de forma segura las acciones y tiempos de respuesta de los operadores ante incidentes.

Requerimientos No Funcionales

- **RNF-PGU-01:** La arquitectura de la plataforma debe basarse en protocolos estandarizados y abiertos para garantizar la interoperabilidad con dispositivos IoT de múltiples fabricantes.
- **RNF-PGU-02:** El núcleo de software debe implementar seguridad de la información con perfiles basados en roles y cifrado en tránsito para proteger la base de datos unificada de auditorías.
- **RNF-PGU-03:** El diseño lógico debe permitir la escalabilidad modular de la plataforma, posibilitando la adición de nuevos nodos periféricos o subsistemas sin degradar el rendimiento general.

4.6. Definición de Requerimientos del Centro de Control y Monitoreo

Requerimientos Funcionales

- **RF-CCM-01:** Las estaciones de trabajo deben permitir la operación ininterrumpida y concurrente de la plataforma de gestión unificada y el monitoreo de los sistemas de seguridad.

- **RF-CCM-02:** El equipamiento gráfico de las estaciones de trabajo debe admitir la decodificación y visualización simultánea de múltiples flujos de video sobre una matriz multimonitor.

Requerimientos No Funcionales

- **RNF-CCM-01:** El hardware seleccionado para el centro de control (servidores, GPUs, terminales) debe estar clasificado para soportar ciclos de trabajo continuo 24/7 bajo alta demanda de datos de red.

- **RNF-CCM-02:** El diseño físico y la ubicación de las estaciones de control del operador deben respetar criterios de ergonomía visual y operativa para mitigar la fatiga laboral en jornadas extendidas.

- **RNF-CCM-03:** El espacio físico proyectado para el centro de control debe poseer infraestructura de energía estabilizada y climatización constante para asegurar la correcta operación del equipamiento crítico.

Capítulo 5

Diseño del Sistema de Seguridad

5.1. Marco Normativo y Estándares

El diseño del sistema de seguridad electrónica se fundamenta en el cumplimiento de la legislación peruana vigente y estándares técnicos nacionales e internacionales aplicables a los sistemas de videovigilancia, control de acceso, alarmas de intrusión, infraestructura de red y protección de datos personales.

- ISO/IEC 62676-4:2015. Sistemas de videovigilancia para aplicaciones de seguridad. Parte 4: Directrices de aplicación.
- IEEE 802.3af-2003. Power over Ethernet (PoE).
- ANSI/TIA-568.2-D:2018. Estándar de cableado de telecomunicaciones de par trenzado balanceado.
- ANSI/TIA-569-E:2019. Rutas y espacios de telecomunicaciones para edificios comerciales.
- IEC 62642-1:2017. Sistemas de alarma y detección de intrusión.
- IEC 60839-11-1:2013. Sistemas electrónicos de seguridad. Sistemas de control de acceso electrónico.

- ONVIF Profile S. Especificación para la interoperabilidad de dispositivos de videovigilancia IP.
- NTP ISO/IEC 27001:2022. Sistemas de gestión de seguridad de la información.
- Ley N.° 29090 y Reglamento Nacional de Edificaciones (RNE), versión vigente consultada.
- Código Nacional de Electricidad – Utilización, edición vigente consultada.
- Norma Técnica EM.020: Instalaciones de Telecomunicaciones, versión vigente consultada.
- Decreto Legislativo N.° 1218 (2015). Medidas para el fortalecimiento de la seguridad ciudadana mediante el uso de cámaras de videovigilancia.
- Directiva N.° 01-2020-JUS/DGTAIPD (2020). Tratamiento de datos personales mediante sistemas de videovigilancia.

5.2. Diseño del Sistema de Videovigilancia

5.2.1. Criterios Técnicos para la Determinación de la Ubicación de Cámaras

La ubicación de las cámaras en el pabellón de Ingeniería Informática y de Sistemas fue definida mediante un análisis técnico y arquitectónico orientado a maximizar la cobertura visual, reducir puntos ciegos y proteger áreas críticas con equipos tecnológicos de alto valor. Los dispositivos fueron distribuidos estratégicamente en accesos, pasillos, escaleras y zonas de tránsito, considerando factores como iluminación, obstáculos estructurales, ángulos de visión y continuidad del monitoreo.

Para el diseño del sistema de videovigilancia se estableció una resolución base de 4 megapíxeles (4MP), debido a su equilibrio entre calidad de imagen, almacenamiento. A fin de verificar el cumplimiento de los objetivos operativos, se realizó un análisis de densidad de píxeles basado en los criterios DORI (Detección, Observación, Reconocimiento e Identificación) definidos en la norma ISO/IEC 62676-4.

Cálculo de Densidad de Píxeles

El cálculo de la densidad de píxeles (D) en el plano horizontal se define mediante la relación entre la resolución horizontal de la cámara (R_h) y el ancho del campo de visión (W) en el punto de interés:

$$D = \frac{R_h}{W} \tag{5.1}$$

Considerando que las cámaras propuestas poseen una resolución de **4 Megapíxeles**, cuyas dimensiones son 2560×1440 píxeles, se procede a validar el cumplimiento de los niveles DORI.

Validación para el Nivel de Reconocimiento

Según la norma ISO/IEC 62676-4, el nivel de Reconocimiento requiere una densidad mínima de 125 px/m. Para determinar el ancho máximo de cobertura (W_{max}) que permite este nivel, despejamos la fórmula:

$$W_{max} = \frac{2560 \text{ px}}{125 \text{ px/m}} = 20{,}48 \text{ m} \tag{5.2}$$

Interpretación: Dado que los pasillos de circulación del proyecto poseen un ancho promedio de entre 2.5 y 4 metros, el uso de cámaras de 4MP garantiza un nivel de calidad superior al de reconocimiento, acercándose a los estándares de *Identificación* (>250 px/m)

en áreas críticas.

Tabla 5.1: *Niveles DORI aplicados a cámaras de 4MP*

Nivel Operativo	**Requerimiento (px/m)**	**Ancho Máximo de Escena (m)**
Detección	25	102.40 m
Observación	62	41.29 m
Reconocimiento	125	20.48 m
Identificación	250	10.24 m

5.2.2. Nomenclatura del Sistema de Videovigilancia

Para la identificación de las cámaras del sistema de videovigilancia, se ha definido la siguiente estructura de codificación:

FORMATO:

CCTV-[PISO]-[TIPO]-[N°]

Donde:

- **CCTV**: Corresponde al sistema de videovigilancia.
- **PISO**: Indica el nivel donde se ubica la cámara (P1, P2, P3, P4.).
- **TIPO**: Representa el tipo de cámara (domo=D, tubo=T , ptz=PTZ).
- **N°**: Número correlativo asignado a cada cámara.

5.2.3. Cuadro de Distribución y Ubicación de Dispositivos de Videovigilancia

Tabla 5.2: *Distribución de cámaras IP*

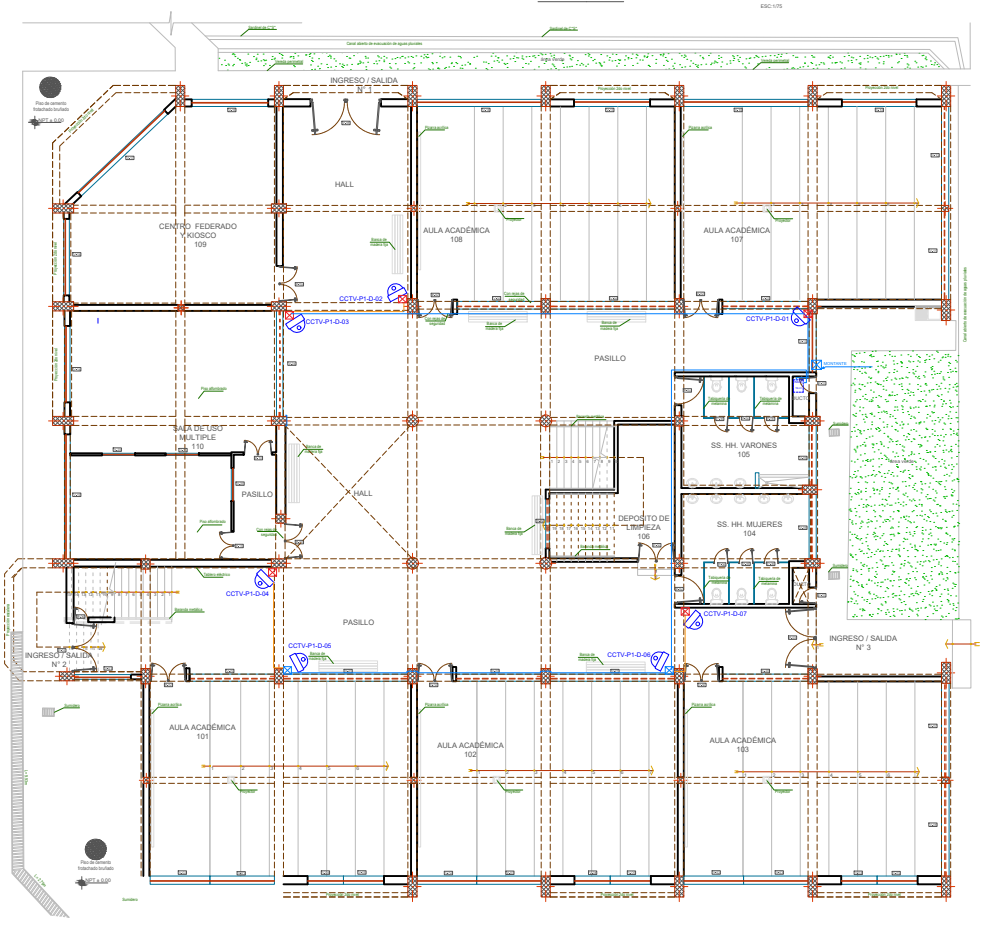
Ubicación	**Descripción**	**Cantidad**	**Observaciones**
Primer piso	Zonas comunes	7	Pasillos, gradas y sala de lectura
Segundo piso	Zonas comunes	8	Pasillos y gradas
Tercer piso	Zonas comunes	9	Pasillos y gradas
Tercer piso	Zona exterior	3	Pasillos y gradas
Cuarto piso	Zonas comunes	7	Pasillos, gradas y sala de monitoreo

Total de cámaras: 34

5.2.4. Plano de Distribución Física del Sistema de Videovigilancia por Nivel

PLANO DE DISTRIBUCION DE CAMARAS DE SEGURIDAD
PRIMER NIVEL

ESC:1/75



N M

LEYENDA

SIMBOLO	DESCRIPCION
	CAMARA IP POE TIPO DOMO ANTIVANDALICA
	CAMARA IP POE TIPO TUBO ANTIVANDALICA
	CAMARA IP POE TIPO DOMO PTZ ANTIVANDALICA
	CAJA DE PASO METALICO 10"X10"X4"
	CAJA DE PASO METALICO 3"X3"X2"
	TUBERIA CONDUIT EMT 1 2"
	TUBERIA CONDUIT EMT 1/2"
	RACK DE COMUNICACIONES

UNIVERSIDAD DE SAN ANTONIO ABAD DEL CUSCO

CARRERA: INGENIERIA INFORMATICA Y DE SISTEMAS

PLANO: PLANO DE UBICACIÓN DE CÁMARAS DE SEGURIDAD - PRIMER NIVEL

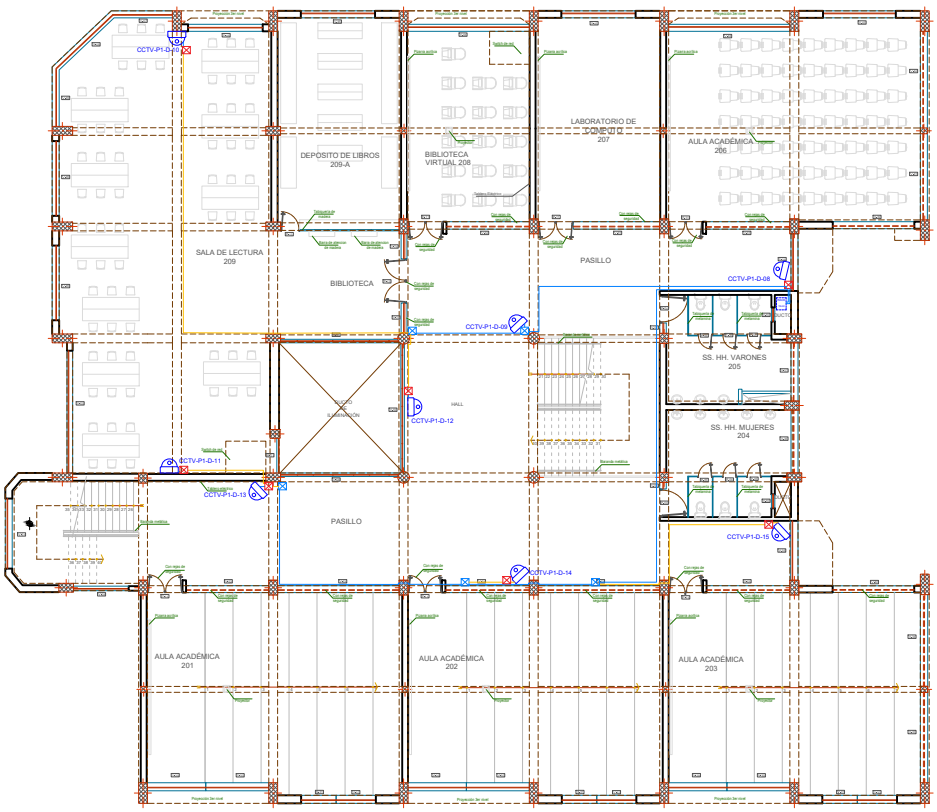
ASESOR: Ing.	
Alumno	CUSCO
Departamento	CUSCO
FECHA:	06/03/2020
Cusco, Marzo del 2020	

LAMINA: P-01

IE - 01

PLANO DE DISTRIBUCION DE CAMARAS DE SEGURIDAD
SEGUNDO NIVEL

ESC:1/75



LEYENDA

SIMBOLO	DESCRIPCION
	CAMARA IP POE TIPO DOMO ANTIVANDALICA
	CAMARA IP POE TIPO TUBO ANTIVANDALICA
	CAMARA IP POE TIPO DOMO PTZ ANTIVANDALICA
	CAJA DE PASO METALICO 10"X10"X4"
	CAJA DE PASO METALICO 3"X3"X2"
	TUBERIA CONDUIT EMT 1 ½"
	TUBERIA CONDUIT EMT 1/2"
	RACK DE COMUNICACIONES

UNIVERSIDAD DE SAN ANTONIO ABAD DEL CUSCO

FACULTAD: INGENIERIA INFORMATICA Y DE SISTEMAS

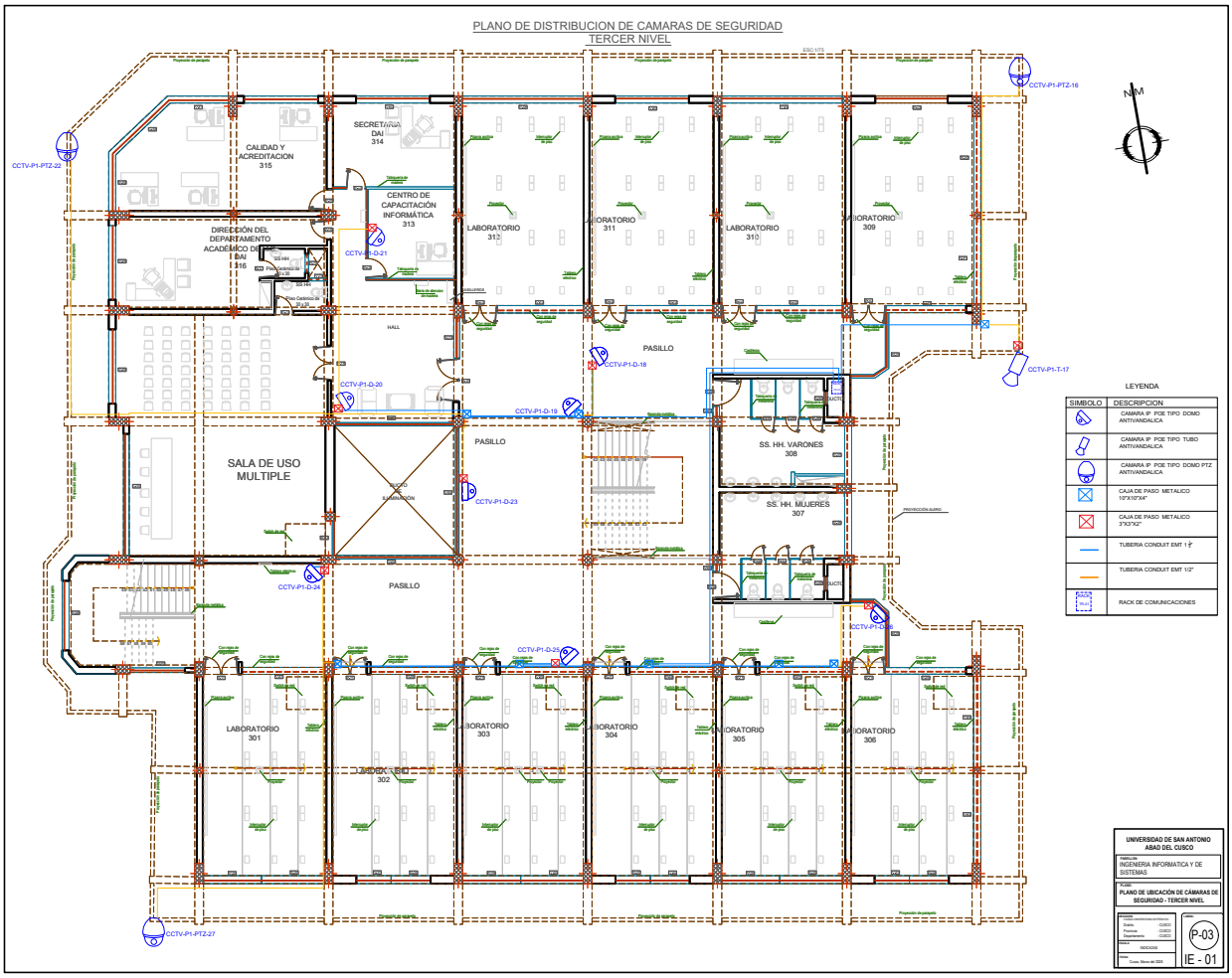
PLANO: PLANO DE UBICACIÓN DE CÁMARAS DE SEGURIDAD - SEGUNDO NIVEL

Distrito	: CUSCO
Provincia	: CUSCO
Departamento	: CUSCO
Escala	: 1/75
Fecha	: Cusco, Marzo del 2024

P-02

IE - 01

PLANO DE DISTRIBUCION DE CAMARAS DE SEGURIDAD
TERCER NIVEL



LEYENDA

SIMBOLO	DESCRIPCION
	CAMARA IP POE TIPO DOMO ANTIVANDALICA
	CAMARA IP POE TIPO TUBO ANTIVANDALICA
	CAMARA IP POE TIPO DOMO PTZ ANTIVANDALICA
	CAJA DE PASO METALICO 10"X10"X4"
	CAJA DE PASO METALICO 3"X3"X2"
	TUBERIA CONDUIT EMT 1"
	TUBERIA CONDUIT EMT 1/2"
	RACK DE COMUNICACIONES

UNIVERSIDAD DE SAN ANTONIO ABAD DEL CUSCO

FACULTAD: INGENIERIA INFORMATICA Y DE SISTEMAS

PLANO: PLANO DE UBICACIÓN DE CÁMARAS DE SEGURIDAD - TERCER NIVEL

UBICACION: Distrito : CUSCO, Provincia : CUSCO, Departamento : CUSCO

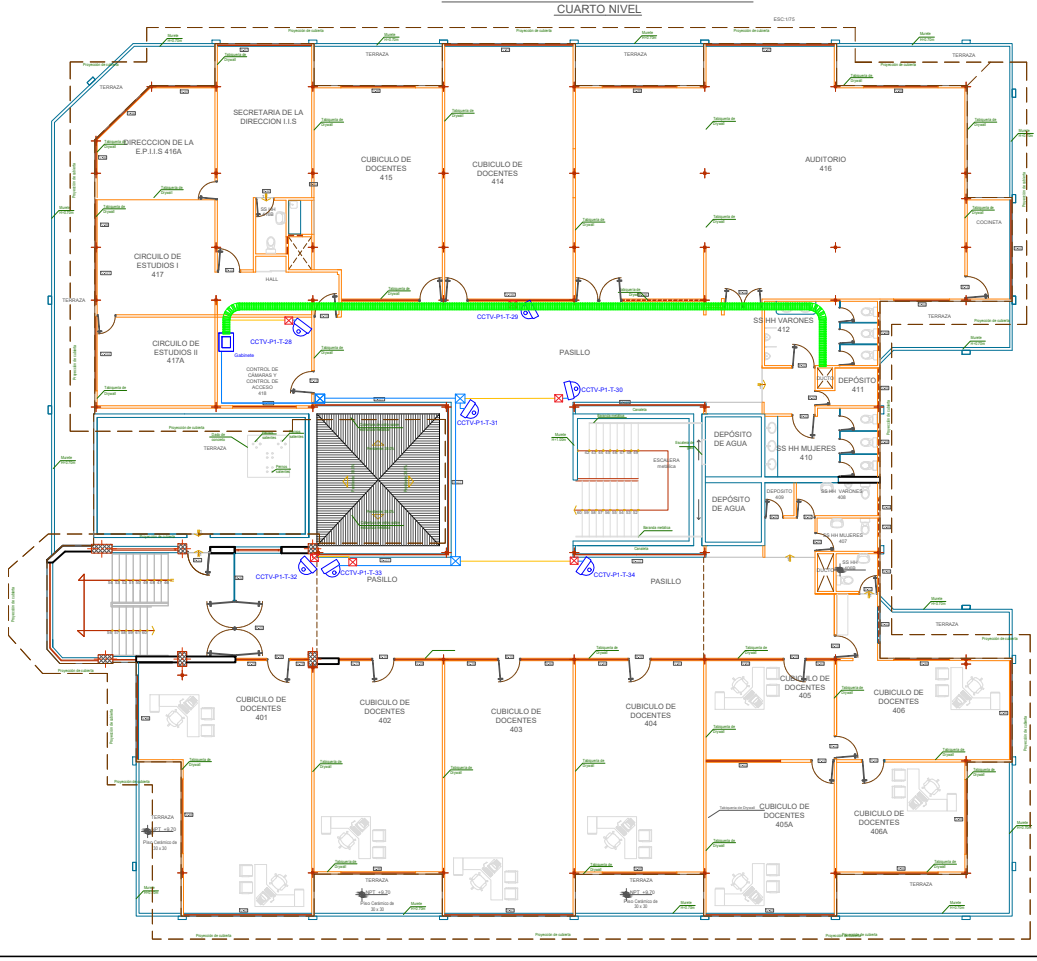
ESCALA: INDICADAS

FECHA: Cusco, Marzo del 2024

LAMINA: P-03

IE - 01

PLANO DE DISTRIBUCION DE CAMARAS DE SEGURIDAD
CUARTO NIVEL



LEYENDA

SIMBOLO	DESCRIPCION
	CAMARA IP POE TIPO DOMO ANTIVANDALICA
	CAMARA IP POE TIPO TUBO ANTIVANDALICA
	CAMARA IP POE TIPO DOMO PTZ ANTIVANDALICA
	CAJA DE PASO METALICO 10"X10"X4"
	CAJA DE PASO METALICO 3"X3"X2"
	TUBERIA CONDUIT EMT 1 ø"
	TUBERIA CONDUIT EMT 1/2"
	GABINETE RACKEABLE
	BANDEJA TIPO REGILLA

UNIVERSIDAD DE SAN ANTONIO ABAD DEL CUSCO

FACULTAD: INGENIERIA INFORMATICA Y DE SISTEMAS

PLANO: PLANO DE UBICACIÓN DE CÁMARAS DE SEGURIDAD - CUARTO NIVEL

Dibujo	: CUSCO
Revisado	: CUSCO
Aprobado	: CUSCO
Escala	: 1/50/100
Fecha	: Enero, Marzo del 2024

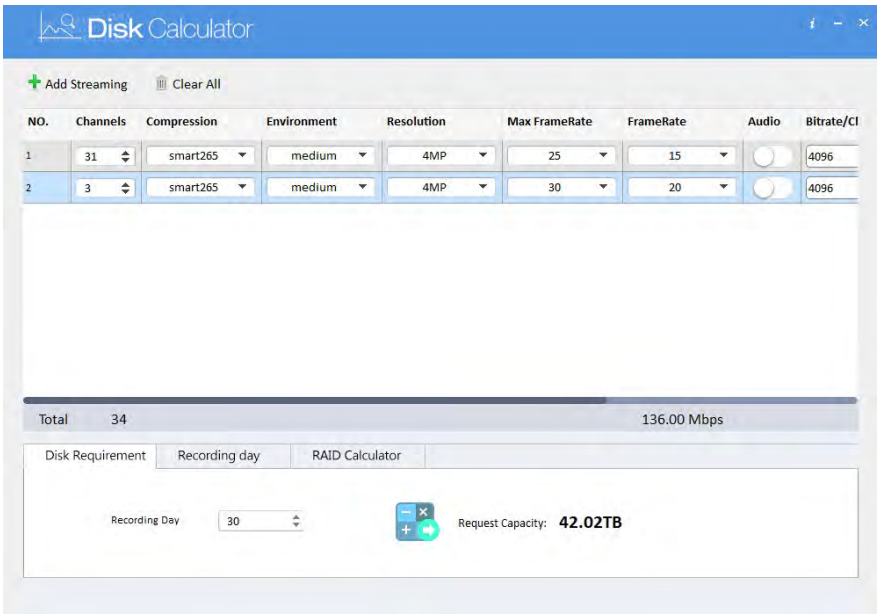
P-04

IE - 01

5.2.5. Dimensionamiento del Sistema de Almacenamiento de Video

Para el dimensionamiento del sistema de almacenamiento de video, se utilizó la herramienta Disk Calculator del software Toolbox, desarrollado por el fabricante Dahua. Esta herramienta permite estimar la capacidad de almacenamiento requerida en función de parámetros, garantizando un dimensionamiento adecuado de los discos duros del sistema.

Figura 5.1: *Calculo de almacenamiento*



Definición y valores de los parámetros de configuración

- **Channels (Canales):** Según la cantidad real de cámaras del sistema 31 cámaras fijas , 3 camaras PTZ).
- **Compression (Compresión):** Se ha implementado el estándar de compresión **H.265 / Smart H.265**, el cual permite optimizar el uso del almacenamiento mediante una mayor eficiencia en la codificación de video, sin comprometer significativamente la calidad de la imagen.
- **Environment (Entorno):** Se ha establecido en **Medium (medio)**, ya que este nivel corresponde a un escenario de actividad moderada, coherente con la dinámica

de tránsito de personas en entornos institucionales.

- **Resolution (Resolución): 4MP:** se considero la resolucion para las camras fijas y ptz
- **Max Frame Rate:** Corresponde a la máxima cantidad de cuadros por segundo que puede soportar el dispositivo, estableciéndose en **25 fps**para camaras fijas ya que permite subir FPS si hay moviemientoo eventos. **30 fps** para camaras PTZ , necesita mas fluidez y mejor respuesta en panel/zoom
- **Audio:** Se ha establecido en estado **desactivado**,dado que no se contempla el uso de audio en las cámaras de videovigilancia, debido a consideraciones legales relacionadas con la protección de datos personales, así como al principio de proporcionalidad, priorizando el uso de video como medio suficiente para la supervisión y registro de eventos en el sistema de seguridad
- **Bitrate/Ch (Tasa de bits por canal):**

  4MP: 4096 Kbps asegura que la densidad de pixeles tenga la profundidad de bits necesaria para realizar zoom digital sin perder evidencia critica).
- **Recording Day (Días de grabación):** Se ha establecido un periodo de almacenamiento de **30 días**, en concordancia con las prácticas comunes en sistemas de videovigilancia y en cumplimiento de la normativa vigente en materia de protección de datos personales, la cual establece un rango de conservación recomendado entre 30 y 60 días. Este periodo garantiza la disponibilidad de información para la verificación, análisis y seguimiento de incidentes de seguridad.
- **Request Capacity (Capacidad requerida):** El dimensionamiento del almacenamiento, determinó una capacidad requerida de 42.02.31 TB para un periodo de retención de 30 días.

Para garantizar la integridad de la evidencia videográfica y la continuidad operativa del sistema, se definió la configuración de almacenamiento bajo los siguientes criterios técnicos:

- **Capacidad Teórica Requerida (C_{req}):** El software de dimensionamiento de almacenamiento determinó un requerimiento inicial de **42.02 TB**, considerando un periodo de retención de 30 días, la resolución configurada, la tasa de bits y la cantidad total de cámaras proyectadas para el sistema de videovigilancia.

- **Configuración de Redundancia (RAID 5):** Se ha seleccionado un arreglo *RAID 5* para proporcionar tolerancia a fallos y asegurar la disponibilidad de la información ante la falla de un disco duro. La capacidad útil (C_u) se calcula mediante la relación:

$$C_u = (n - 1) \times S$$

  Donde n representa el número de discos instalados y S la capacidad nominal de cada unidad. Esta arquitectura permite mantener la operación del sistema sin pérdida de datos ante la falla de una unidad física.

- **Especificación de Hardware:** Se propone la implementación de cinco (5) unidades de disco duro de 12 TB cada una:

  - **Capacidad Bruta Total:**

$$5 \times 12 \text{ TB} = 60 \text{ TB}$$

  - **Capacidad Útil Real (C_u):**

$$(5 - 1) \times 12 \text{ TB} = 48 \text{ TB}$$

- **Conclusión Técnica:** La capacidad útil disponible de **48 TB** supera el requerimiento calculado de **42.02 TB**, proporcionando un margen de reserva aproximado del **14.2 %**. Este excedente permite compensar el espacio utilizado por el sistema de archivos, la sobrecarga del arreglo RAID y futuras ampliaciones relacionadas con incrementos en la calidad de grabación o incorporación de nuevas cámaras.

5.2.6. Especificaciones Técnicas de los Componentes Principales del Sistema de Videovigilancia

Tabla 5.3: *Especificaciones técnicas recomendadas de la cámaras*

Característica	**Especificación**
Tipo	IP – Domo
Resolución	4 MP (2560×1440)
Visión nocturna	IR 30 m
Compresión	H.265+
Compatibilidad	ONVIF
Conectividad	Ethernet
Alimentación	PoE
Protección	IP67+IK10 antivandálica

Tabla 5.4: *Especificaciones técnicas del videograbador*

Característica	**Especificación**
Número de canales	64 canales IP
Resolución	4MP en todos los canales
Ancho de banda de entrada	$\geq$ 256 Mbps
Compresión	H.265+
Almacenamiento	5 HDD SATA
Salidas de video	HDMI y VGA
Compatibilidad	ONVIF

Tabla 5.5: *Especificaciones técnicas del switch principal*

Característica	**Especificación recomendada**
Tipo	Administrable (Layer 3)
Montaje	Rackeable

Tabla 5.6: *Especificaciones técnicas del switch PoE*

Característica	**Especificación recomendada**
Número de puertos	8-16 GIGA
Estándar PoE	802.3af (PoE) y 802.3at (PoE+)
Potencia por puerto	Hasta 30 W por puerto (802.3at)
Montaje	Rackeable

Tabla 5.7: *Especificaciones técnicas del cable UTP Cat6*

Característica	**Especificación**
Tipo de cable	UTP Categoría 6
Material del conductor	Cobre sólido (100 % cobre)
Calibre del conductor	23 AWG
Estructura interna	4 pares trenzados
Revestimiento (chaqueta)	LSZH

5.3. Diseño del Sistema de Control de Acceso

5.3.1. Criterios Técnicos para la Ubicación de Dispositivos de Control de Acceso

La ubicación de los dispositivos del sistema de control de acceso ha sido definida en función del nivel de criticidad de las áreas, el tipo de uso de los ambientes y los requerimientos de seguridad del pabellón.

En ese sentido, se ha determinado que la implementación de controles de acceso se realizará únicamente en ambientes que requieren restricción y control del ingreso, tales como laboratorios, oficinas administrativas y áreas sensibles, excluyendo las aulas de dictado regular, debido a su carácter de acceso libre durante los horarios académicos.

Los principales criterios considerados son los siguientes:

- **Nivel de criticidad del ambiente:** Se prioriza la instalación en laboratorios y oficinas donde se resguardan equipos, información o recursos sensibles.
- **Control de acceso restringido:** Se implementan dispositivos en ambientes donde el ingreso debe estar limitado únicamente a personal autorizado, como docentes,

administrativos o estudiantes registrados.

- **Flujo de personas:** No se consideran las aulas de uso común debido a su alto flujo de estudiantes y necesidad de acceso libre durante las actividades académicas.
- **Protección de activos:** Se busca evitar el acceso no autorizado a equipos tecnológicos, materiales de laboratorio y documentación institucional.
- **Ubicación estratégica:** Los dispositivos se instalan en puntos de ingreso principales (puertas), garantizando el control efectivo de entrada y salida.
- **Integración con otros sistemas:** La ubicación de los dispositivos considera su integración con el sistema de videovigilancia y el sistema de alarmas, permitiendo una gestión centralizada de la seguridad.

Políticas de autenticación y gestión de usuarios

El acceso a los ambientes restringidos, tales como laboratorios y oficinas administrativas, será gestionado únicamente por personal autorizado, incluyendo docentes y personal administrativo. Para la autenticación de usuarios, se ha definido el uso de tecnologías combinadas, priorizando el uso de tarjetas de proximidad (RFID) por su rapidez y facilidad de uso. De manera complementaria, se implementará la autenticación biométrica mediante huella digital, con el fin de reforzar la seguridad del sistema y evitar el uso indebido de credenciales. El uso de doble método de autenticación permitirá mejorar el control de accesos en áreas críticas, garantizando que únicamente usuarios registrados puedan ingresar a dichos ambientes. Asimismo, la gestión de credenciales será administrada por el personal responsable del sistema, quienes tendrán la facultad de registrar, modificar o revocar accesos según los perfiles de usuario establecidos.

5.3.2. Nomenclatura del Sistema de Control de Acceso

Para la identificación de los dispositivos del sistema de control de acceso, se ha definido la siguiente estructura de codificación:

FORMATO:

CA-[PISO]-[N°]

Donde:

- **CA**: Corresponde a control de acceso.
- **PISO**: Indica el nivel donde se ubica el dispositivo (P1, P2, P3, P4.).
- **N°**: Número correlativo asignado a cada dispositivo.

Asignación de control de acceso por ambiente y rol de usuario

Tabla 5.8: *Control de acceso propuesto – Segundo piso*

Ubicación	**Descripción**	**Cantidad**	**Rol autorizado**
Amb. 207	Laboratorio de cómputo	1	Docentes responsables
Amb. 208	Biblioteca virtual	1	Personal administrativo
Amb. 209	Biblioteca	1	Personal autorizado

Tabla 5.9: *Control de acceso propuesto – Tercer piso*

Ubicación	**Descripción**	**Cantidad**	**Rol autorizado**
Amb. 301-306	Laboratorios	6	Docentes responsables
Amb. 309-312	Laboratorios	4	Docentes responsables
Amb. 313	Centro de capacitación	1	Personal autorizado
Amb. 314	Secretaría DAI	1	Personal administrativo
Amb. 316	DAI	1	Personal administrativo

Tabla 5.10: *Control de acceso propuesto – Cuarto piso*

Ubicación	**Descripción**	**Cantidad**	**Rol autorizado**
Cubículos docentes	Área docente	8	Docentes
Auditorio	Área de uso múltiple	1	Administración / Seguridad
Secretaría de coordinación	Área administrativa	1	Personal administrativo
Coordinación	Área administrativa	1	Personal administrativo
Sala de cámaras	Infraestructura crítica	1	Personal autorizado

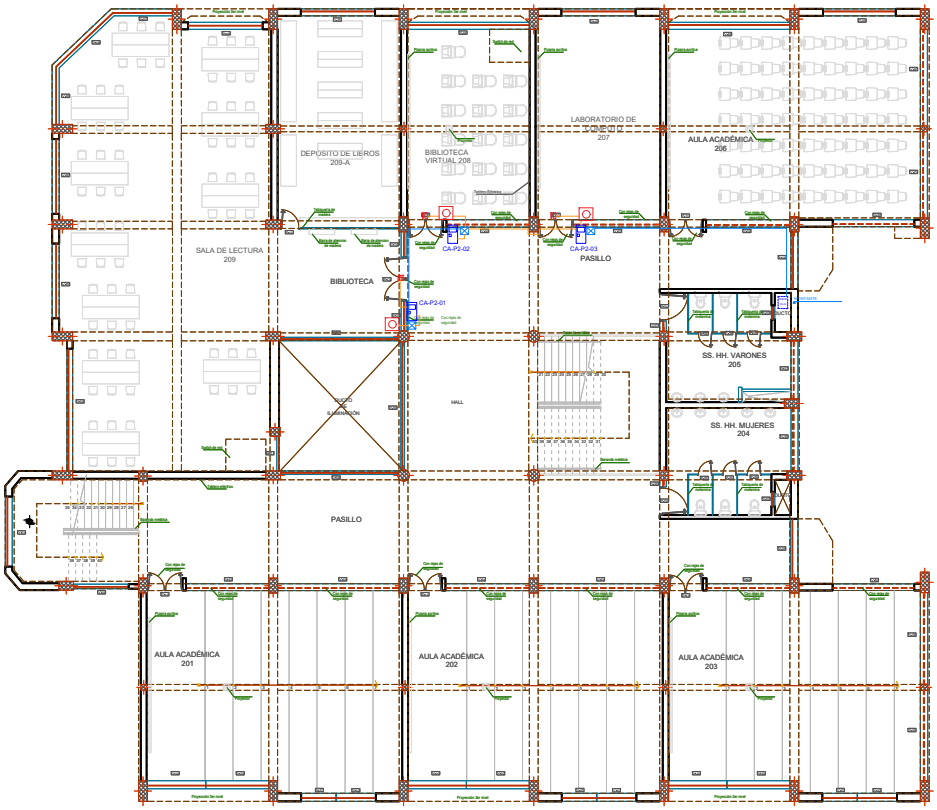
Tabla 5.11: *Resumen de controles de acceso propuestos por piso*

Piso	**Cantidad de controles de acceso**
Segundo piso	3
Tercer piso	13
Cuarto piso	12
Total	**28**

5.3.3. Plano de Distribución Física del Sistema de Control de Acceso por Nivel

PLANO DE DISTRIBUCION DEL CONTROL DE ACCESO
SEGUNDO NIVEL

ESC:1/75



LEYENDA

SIMBOLO	DESCRIPCION
	CONTROL IDENTIFICADOR DOMO ANTIVANDALICA
	TABLERO GABINETE 600X400X150
	CERRADURA MAGNETICA ANTIVANDALICA
	CAJA DE PASO METALICO 10"X10"X4"
	BOTON DE SALIDA
	TUBERIA CONDUIT EMT 1"
	TUBERIA CONDUIT EMT 1/2"
	RACK DE COMUNICACIONES

UNIVERSIDAD DE SAN ANTONIO ABAD DEL CUSCO

INGENIERIA INFORMATICA Y DE SISTEMAS

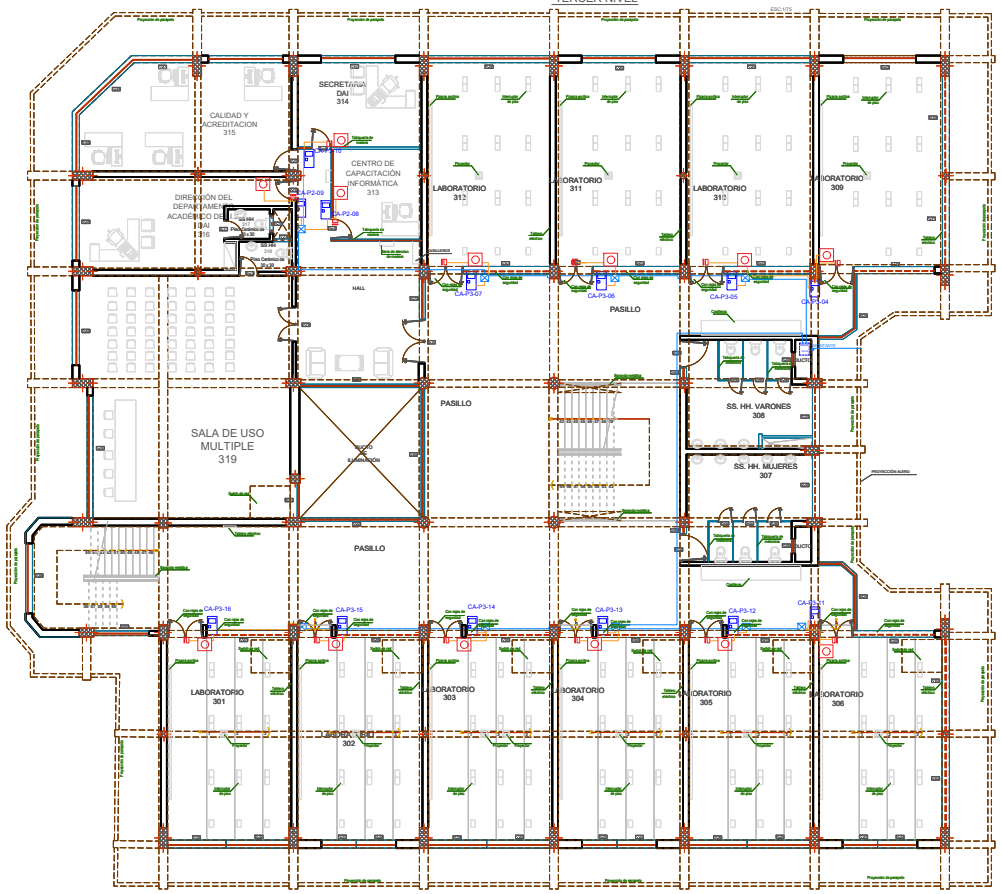
PLANO DE UBICACIÓN DE CONTROL DE ACCESO - SEGUNDO NIVEL

Cusco, Marzo del 2024

P-05

IE - 01

PLANO DE DISTRIBUCION DEL CONTROL DE ACCESO
TERCER NIVEL



LEYENDA

SIMBOLO	DESCRIPCION
	CONTROL D/S/TRECEIRO DOMO ANTIVANDALICA
	TABLERO GABINETE 600X400X150
	CERRADURA MAGNETICA ANTIVANDALICA
	CAJA DE PASO METALICO 10"X10"X6"
	BOTON DE SALIDA
	TUBERIA CONDUIT EMT 1"
	TUBERIA CONDUIT EMT 1/2"
	RACK DE COMUNICACIONES

UNIVERSIDAD DE SAN ANTONIO ABAD DEL CUSCO

FACULTAD: INGENIERIA INFORMATICA Y DE SISTEMAS

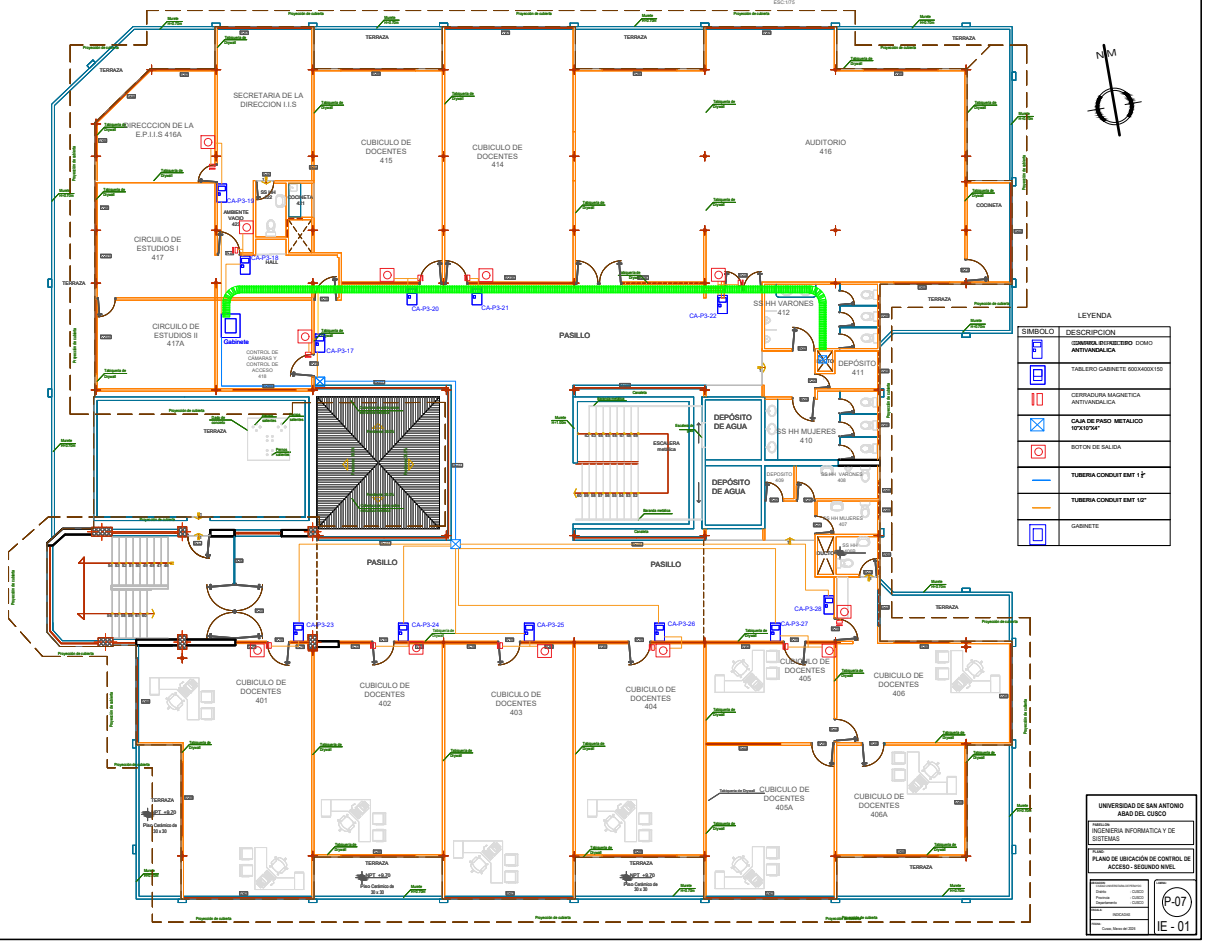
PLANO: PLANO DE UBICACIÓN DE CONTROL DE ACCESO - SEGUNDO NIVEL

Distrito	: CUSCO
Provincia	: CUSCO
Departamento	: CUSCO
Escala	: 1/50
Fecha	: Cusco, Marzo del 2024

P-06

IE - 01

PLANO DE DISTRIBUCION DEL CONTROL DE ACCESO
CUARTO NIVEL



LEYENDA

SIMBOLO	DESCRIPCION
	CONTROL ECO RECEIBRO DOMO ANTIVANDALICA
	TABLERO GABINETE 600X400X150
	CERRADURA MAGNETICA ANTIVANDALICA
	CAJA DE PASO METALICO 10"X10"X4"
	BOTON DE SALIDA
	TUBERIA CONDUIT EMT 1"
	TUBERIA CONDUIT EMT 1/2"
	GABINETE

UNIVERSIDAD DE SAN ANTONIO ABAD DEL CUSCO

INGENIERIA INFORMATICA Y DE SISTEMAS

PLANO DE UBICACIÓN DE CONTROL DE ACCESO - SEGUNDO NIVEL

P-07

IE - 01

5.3.4. Especificaciones Técnicas de los Dispositivos de Control de Acceso

Tabla 5.12: *Especificaciones tecnicas deL control de acceso*

Caracteristica	**Especificacion recomendada**
Tipo de dispositivo	Huella y tarjeta.
Lectura de tarjetas RFID	distancia de lectura aproximada 2 a 5 cm.
Salida	rele NO/NC para control de cerradura
Conectividad	TCP/IP; RS-485
Compatibilidad	Compatible con cerradura de 12 VDC
Salida	rele NO/NC para control de cerradura
Pantalla	Si

5.4. Diseño del Sistema de Detección y Alarma de Intrusión

5.4.1. Criterios Técnicos para la Ubicación de los Dispositivos de Detección

Para el diseño del sistema de alarmas, se establecen criterios técnicos orientados a la correcta ubicación de los sensores de detección, considerando que se emplearán únicamente sensores de movimiento. Asimismo, se ha definido que estos dispositivos serán instalados exclusivamente en ambientes que resguarden bienes de valor, debido a que los accesos estarán protegidos mediante el sistema de control de acceso.

Los criterios técnicos considerados son los siguientes:

- **Cobertura efectiva del área:** Los sensores de movimiento deben ubicarse de manera

que cubran completamente el ambiente, evitando zonas muertas o sin detección.

- **Altura de instalación:** Se recomienda instalar los sensores a una altura aproximada entre 2.2 m y 2.5 m, de acuerdo con las especificaciones del fabricante, para garantizar un desempeño óptimo.
- **Orientación del sensor:** Los sensores deben orientarse hacia las zonas de posible tránsito de personas, priorizando accesos internos, pasillos y áreas de circulación dentro del ambiente.
- **Evitar interferencias:** No se deben ubicar cerca de fuentes de calor (aires acondicionados, luminarias, equipos electrónicos) o corrientes de aire que puedan generar falsas alarmas.
- **Línea de visión despejada:** Se debe asegurar que no existan obstáculos como mobiliario, divisiones o estructuras que bloqueen el campo de detección del sensor.
- **Protección contra manipulación:** Los sensores deben instalarse en ubicaciones que dificulten su sabotaje o manipulación por personas no autorizadas.
- **Cobertura en puntos críticos:** Se prioriza la instalación en ambientes que contengan equipos de alto valor, como laboratorios, salas de servidores o áreas administrativas sensibles.
- **Integración con otros sistemas:** La ubicación debe considerar su integración con el sistema de monitoreo central, facilitando la supervisión y gestión de eventos.

5.4.2. Cuadro de Distribución de Dispositivos del Sistema de Alarma

En el primer piso no se contempla la instalación de sistemas de control de acceso, al tratarse de áreas de uso común y circulación abierta.

Tabla 5.13: *Distribución del sistema de alarmas – Segundo piso*

Ubicación	**Descripción**	**Tipo de dispositivo**	**Cantidad**
Amb. 207	Laboratorio de cómputo	Sensor PIR	1
Amb. 208	Biblioteca virtual	Sensor PIR	1

Tabla 5.14: *Distribución del sistema de alarmas – Tercer piso*

Ubicación	**Descripción**	**Tipo de dispositivo**	**Cantidad**
Amb. 301-312	Laboratorios	Sensor PIR	12

Tabla 5.15: *Distribución del sistema de alarmas – Cuarto piso*

Ubicación	**Descripción**	**Tipo de dispositivo**	**Cantidad**
Sala de cámaras	Infraestructura crítica	Sensor PIR	1

Tabla 5.16: *Distribución del sistema de alarmas – Sirenas*

Ubicación	**Cantidad**	**Observación**
Ducto de iluminación (interior del pabellón)	1	Sirena interior para alerta audible interna
Exterior del pabellón	1	Sirena exterior para disuasión y alerta perimetral

Tabla 5.17: *Resumen del sistema de alarmas propuesto*

Elemento	**Cantidad**
Sensores PIR – Segundo piso	2
Sensores PIR – Tercer piso	12
Sensores PIR – Cuarto piso	1
Total de sensores PIR	**15**
Sirena interior	1
Sirena exterior	1
Total de sirenas	**2**

5.4.3. Nomenclatura del Sistema de Alarmas

Estructura general de nomenclatura

La nomenclatura del sistema de alarmas se define mediante una estructura estandarizada que permite identificar de manera única cada dispositivo dentro de la infraestructura. La estructura es la siguiente:

FORMATO:

ALM-[PISO]-[TIPO]-[N°]

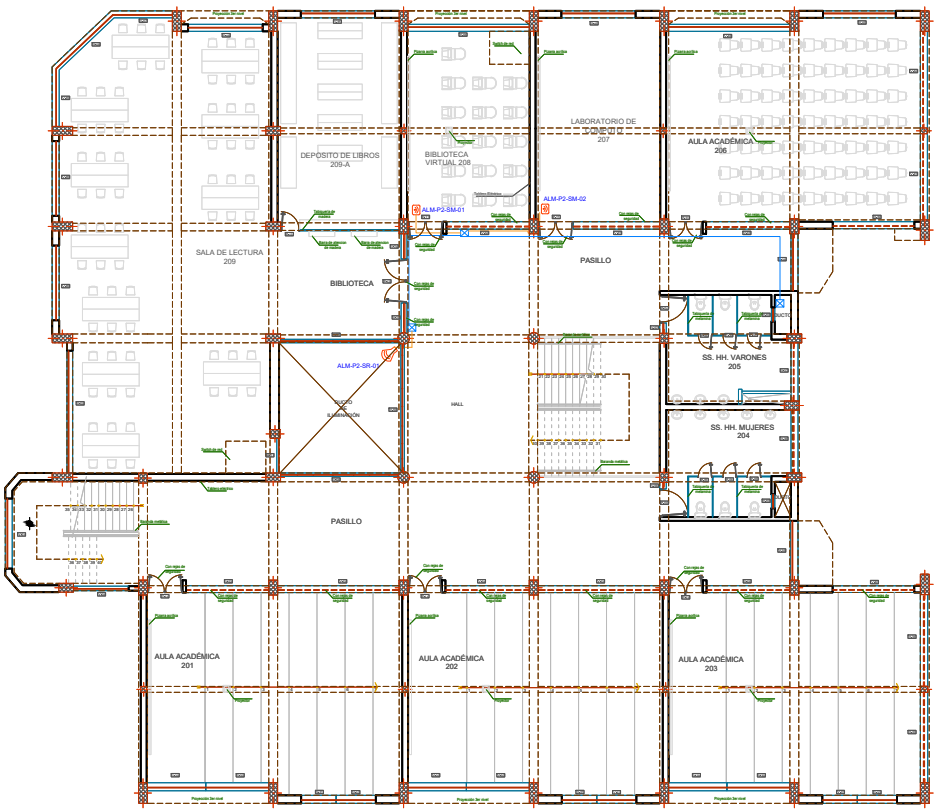
Donde:

- **ALM**: Corresponde al sistema de alarmas.
- **PISO**: Indica el nivel donde se ubica el dispositivo (P1, P2, P3, etc.).
- **TIPO**: Representa el tipo de dispositivo dentro del sistema de alarmas (SM: sensor de movimiento, SI: sirena, CP: panel de control, KP: teclado).
- **N°**: Número correlativo asignado a cada dispositivo.

5.4.4. Plano de Distribución Física del Sistema de Alarma por Nivel

PLANO DE DISTRIBUCION DE LA ALARMA ANTIRROBO
SEGUNDO NIVEL

ESC:1/75



LEYENDA

SIMBOLO	DESCRIPCION
	SENSOR DE MOVIMIENTO
	CAJA DE PASO METALICO 10"X10"X6"
	CAJA DE PASO METALICO 3"X3"X2"
	TUBERIA CONDUIT EMT 1"
	TUBERIA CONDUIT EMT 1/2"

UNIVERSIDAD DE SAN ANTONIO ABAD DEL CUSCO

INGENIERIA INFORMATICA Y DE SISTEMAS

PLANO DE UBICACIÓN DE ALARMA ANTIRROBO - SEGUNDO NIVEL

Distrito : CUSCO
Provincia : CUSCO
Departamento : CUSCO

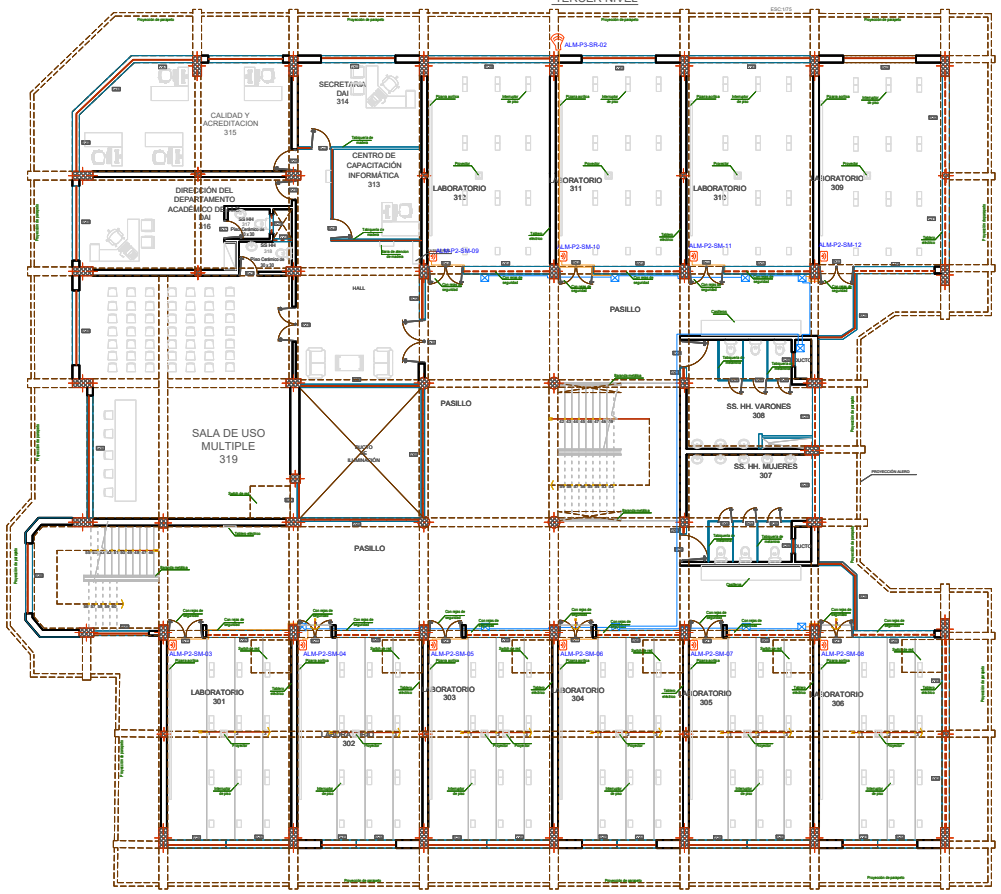
Escala : 1/50

Fecha : Cusco, Marzo del 2024

P-08

IE - 01

PLANO DE DISTRIBUCION DE LA ALARMA ANTIRROBO
TERCER NIVEL



LEYENDA

SIMBOLO	DESCRIPCION
	SENSOR DE MOVIMIENTO
	CAJA DE PASO METALICO 10"X10"X4"
	CAJA DE PASO METALICO 3"X3"X2"
	TUBERIA CONDUIT EMT 1"
	TUBERIA CONDUIT EMT 1/2"
	GABINETE RACKEABLE

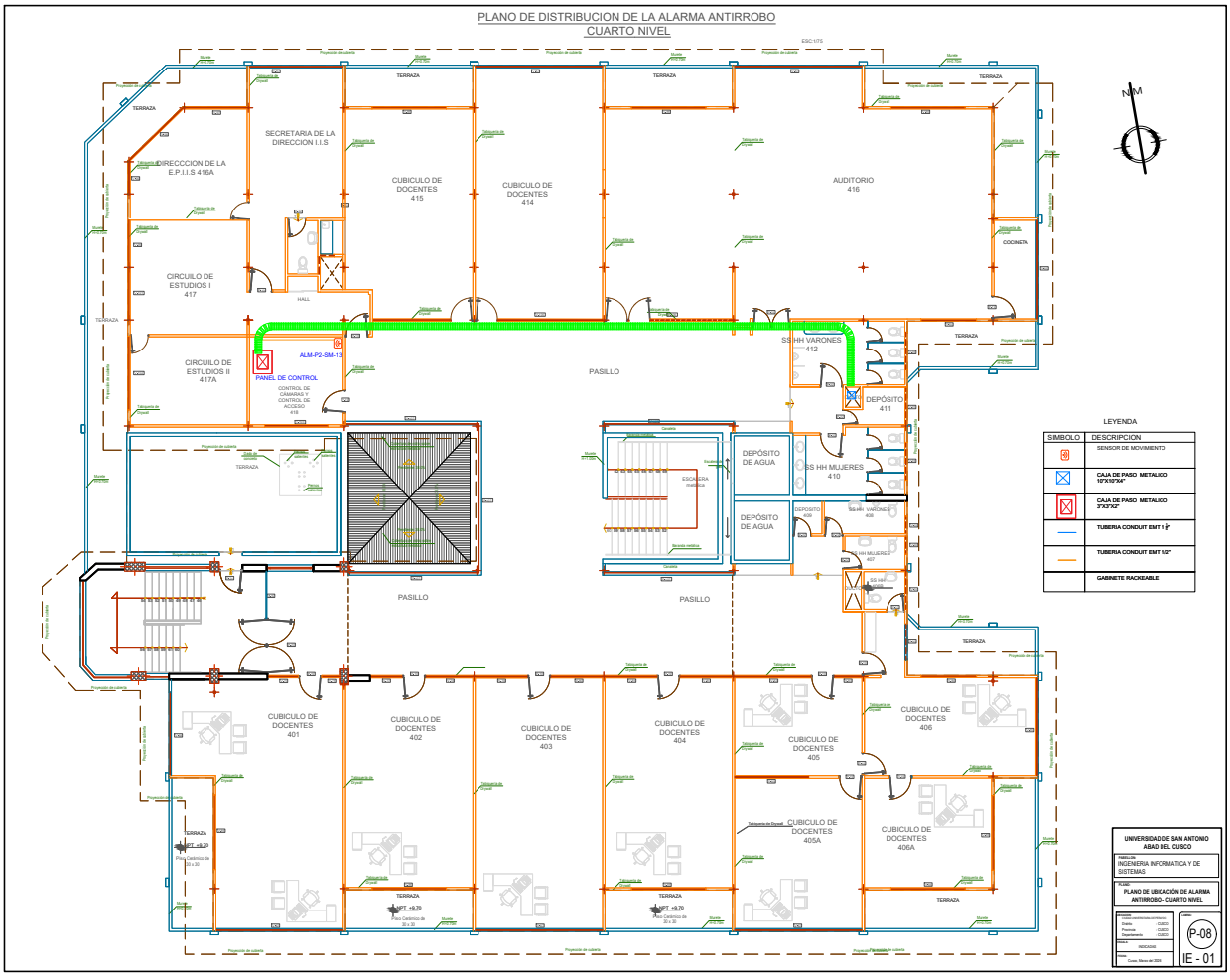
UNIVERSIDAD DE SAN ANTONIO ABAD DEL CUSCO

INGENIERIA INFORMATICA Y DE SISTEMAS

PLANO DE UBICACIÓN DE ALARMA ANTIRROBO - TERCER NIVEL

P-08

IE - 01


PLANO DE DISTRIBUCION DE LA ALARMA ANTIRROBO
CUARTO NIVEL
ESC:1/75
SECRETARIA DE LA DIRECCION I.I.S
DIRECCCION DE LA E.P.I.I.S 416A
CUBICULO DE DOCENTES 415
CUBICULO DE DOCENTES 414
AUDITORIO 416
COCINETA
CIRCUILO DE ESTUDIOS I 417
CIRCUILO DE ESTUDIOS II 417A
HALL
PANEL DE CONTROL
ALM-P2-SM-13
CONTROL DE CAMARAS Y CONTROL DE ACCESO 418
PASILLO
SS HH VARONES 412
DEPÓSITO 411
DEPÓSITO DE AGUA
SS HH MUJERES 410
ESCALERA
DEPÓSITO 409
SS HH VARONES 408
SS HH MUJERES 407
CUBICULO DE DOCENTES 401
CUBICULO DE DOCENTES 402
CUBICULO DE DOCENTES 403
CUBICULO DE DOCENTES 404
CUBICULO DE DOCENTES 405
CUBICULO DE DOCENTES 405A
CUBICULO DE DOCENTES 406
CUBICULO DE DOCENTES 406A
TERRAZA
LEYENDA
SIMBOLO
DESCRIPCION
SENSOR DE MOVIMIENTO
CAJA DE PASO METALICO 10"X10"X4"
CAJA DE PASO METALICO 3"X3"X2"
TUBERIA CONDUIT EMT 1"
TUBERIA CONDUIT EMT 1/2"
GABINETE RACKEABLE
UNIVERSIDAD DE SAN ANTONIO ABAD DEL CUSCO
INGENIERIA INFORMATICA Y DE SISTEMAS
PLANO DE UBICACIÓN DE ALARMA ANTIRROBO - CUARTO NIVEL
P-08
IE - 01

5.4.5. Especificaciones Técnicas del Sistema de Alarma

Tabla 5.18: *Especificaciones técnicas del panel de alarma*

Característica	**Especificación**
Zonas cableadas	16 zonas
Comunicación	Ethernet y módulo GSM o LTE
Batería de respaldo	Si

Tabla 5.19: *Especificaciones técnicas de la sirena electrónica*

Característica	**Especificación**
Tipo	Interna o externa
Potencia sonora	110 a 120 dB
Consumo	200 a 400 mA
Protección IP	IP54 para exteriores
Material	ABS o metal resistente

Tabla 5.20: *Especificaciones técnicas del sensor PIR*

Característica	**Especificación**
Tipo	Infrarrojo pasivo (PIR)
Cobertura	10 a 12 m, 90 a 110 grados
Sensibilidad	Ajustable

Tabla 5.21: *Especificaciones técnicas del cableado para alarmas*

Característica	**Especificación**
Tipo de cable	Cable dúplex o multipar para alarmas
Calibre para sensores hline Calibre para sirena y panel	22 AWG 18 AWG
Norma	CL2 o FPLR (según NEC)
Revestimiento	Libre de halógenos

5.5. Diseño de la Plataforma de Gestión Unificada

El diseño de la plataforma lógica constituye el núcleo de integración del sistema, donde se define la inteligencia operativa y la administración centralizada de los recursos de seguridad.

5.5.1. Arquitectura de Gestión y Control de Acceso

Se diseña una estructura de administración basada en roles, permitiendo la segregación de funciones de acuerdo con la normativa de protección de datos:

- **Perfil Administrador:** Acceso total a la configuración del sistema, gestión de usuarios y auditoría de *logs*.
- **Perfil Operador:** Monitoreo en tiempo real, gestión de alarmas y visualización de eventos recientes, con restricciones para la eliminación de registros.

Lógica de Integración y Eventos Vinculados

La unificación de los subsistemas se basa en un motor de reglas condicionales de tipo *If-This-Then-That* (IFTTT). Se diseñan los siguientes escenarios lógicos:

- **Vinculación de Video:** Ante la activación de un sensor de intrusión o un cruce de línea analítico, el software ejecutará un *Video Pop-up* prioritario en la estación de control.

Interfaz de Visualización Situacional

A diferencia de los planos arquitectónicos de ubicación, la plataforma integrará mapas electrónicos dinámicos (*E-Maps*). Estos mapas permiten:

- La georreferenciación lógica de cada nodo de red en los diferentes niveles del pabellón.
- La interacción táctil o mediante puntero para el control de domos PTZ y la apertura remota de accesos autorizados.
- Retroalimentación visual mediante cambio de estados (color) de los íconos de dispositivos ante fallas de conexión o alertas activas.

Gestión de la Continuidad y Trazabilidad

El software implementará un módulo de *Audit Trail* (Pista de Auditoría) inalterable, el cual registrará cada acción realizada por los usuarios del sistema. Este diseño asegura que cualquier consulta a la base de datos de video sea trazable, garantizando la cadena de custodia de la información y la transparencia en la gestión de la seguridad del pabellón.

5.6. Centro de Control y Monitoreo

El Centro de control y monitoreo constituye el núcleo operativo del sistema integrado de seguridad electrónica, permitiendo la supervisión, control y gestión centralizada de los subsistemas de videovigilancia, control de acceso y alarmas electrónicas.

El centro de monitoreo estará ubicado dentro del pabellón, en un ambiente destinado

exclusivamente para tal fin, desde donde se realizará la supervisión en tiempo real de las diferentes áreas mediante una estación de trabajo equipada con un computador, monitores y software de gestión unificada.

Para el presente diseño, se considera la integración de 28 cámaras fijas y 3 cámaras PTZ, distribuidas estratégicamente en el pabellón.

Objetivo del centro de monitoreo

Garantizar la vigilancia continua, la detección oportuna de incidentes y una respuesta eficiente ante eventos de seguridad, mediante una infraestructura tecnológica adecuada y la integración centralizada de los distintos subsistemas.

5.6.1. Infraestructura del centro de monitoreo

Componentes principales

- **Estación de monitoreo:** Computadora de alto rendimiento con software de gestión unificada.
- **Sistema de visualización:** Implementación de cuatro monitores para la supervisión simultánea de los sistemas integrados.
- **Joystick PTZ:** Dispositivo para el control manual de cámaras PTZ.
- **Sistema de alimentación:** UPS para respaldo energético y protección de los equipos.

Distribución de Monitores

Se propone la siguiente distribución de monitores para optimizar la supervisión operativa del sistema de seguridad:

- **Monitor 1:** Visualización de hasta 16 cámaras fijas correspondientes a accesos principales, pasillos y áreas comunes.
- **Monitor 2:** Visualización de las 15 cámaras fijas restantes instaladas en aulas, oficinas y ambientes complementarios.
- **Monitor 3:** Supervisión dedicada de las 3 cámaras PTZ y de cámaras críticas ubicadas en laboratorios, zonas restringidas y áreas de alto valor.
- **Monitor 4:** Plataforma unificada de gestión de seguridad, destinada al monitoreo de alarmas, control de acceso, eventos del sistema y reproducción de grabaciones.

Esta distribución permite organizar adecuadamente la información visual del sistema, reduciendo la saturación operativa del personal de monitoreo y facilitando la atención de eventos críticos en tiempo real.

5.6.2. Diseño Físico del Centro de Monitoreo

El ambiente destinado al centro de monitoreo contará con acceso restringido únicamente al personal autorizado. La disposición de los equipos considerará criterios ergonómicos que permitan al operador mantener visibilidad directa de todos los monitores.

Asimismo, se recomienda considerar las siguientes condiciones:

- Escritorio tipo consola para múltiples monitores.
- Ubicación de monitores a nivel de la línea de visión del operador.
- Iluminación adecuada y control de reflejos.
- Ventilación y condiciones ambientales controladas.

Funcionamiento operativo

El operador realizará la supervisión continua de las cámaras, priorizando las zonas críticas del pabellón. Ante la detección de un incidente, podrá utilizar el joystick PTZ para realizar seguimiento de eventos, acceder a grabaciones y gestionar alertas provenientes de los sistemas integrados.

Asimismo, el sistema permitirá la supervisión de accesos autorizados y no autorizados, así como la visualización de notificaciones generadas por sensores y dispositivos de seguridad.

Criterios técnicos de diseño

- **Escalabilidad:** Posibilidad de incorporar nuevos dispositivos en el futuro.
- **Disponibilidad:** Respaldo energético mediante UPS.
- **Seguridad:** Acceso restringido y control de usuarios.
- **Interoperabilidad:** Compatibilidad entre subsistemas y dispositivos.
- **Usabilidad:** Interfaz amigable y operación eficiente.

Consideraciones finales

El diseño propuesto para el Centro de Control y Monitoreo permite una supervisión eficiente de los sistemas integrados de seguridad electrónica, garantizando condiciones adecuadas para el monitoreo continuo, la gestión centralizada de eventos y la futura escalabilidad del sistema.

Especificaciones Técnicas del Sistema del Centro de Control y Monitoreo

La estación de monitoreo permitirá la supervisión centralizada de las cámaras IP, eventos de control de acceso, alarmas y reproducción de grabaciones del sistema de seguridad inteligente.

Tabla 5.22: *Especificaciones de la Workstation de Monitoreo*

Componente	**Especificación**
Procesador	Intel Core i7 de 12ª generación o superior
Memoria RAM	32 GB DDR4
Almacenamiento	SSD NVMe de 1 TB
Tarjeta gráfica	GPU dedicada con soporte para múltiples monitores
Conectividad	Puerto Ethernet Gigabit
Puertos de video	HDMI y DisplayPort múltiples

Tabla 5.23: *Distribución y especificaciones de monitores*

Monitor	**Tamaño**	**Resolución**	**Función**
Monitor 1	27” LED	Full HD 1920x1080	Visualización de hasta 16 cámaras fijas
Monitor 2	27” LED	Full HD 1920x1080	Visualización de las 15 cámaras fijas restantes
Monitor 3	27” LED	Full HD 1920x1080	Supervisión de cámaras PTZ y cámaras críticas
Monitor 4	27” LED	Full HD 1920x1080	Plataforma unificada de alarmas, control de acceso, eventos y reproducción de grabaciones

La distribución propuesta permite organizar adecuadamente la información visual del sistema, facilitando la supervisión en tiempo real y mejorando la capacidad de respuesta ante incidentes.

5.7. Lineamientos Técnicos Generales

En el presente apartado se establecen los criterios técnicos generales aplicables a los sistemas de videovigilancia, control de acceso y alarmas, con el fin de garantizar una implementación segura, eficiente y estandarizada de la infraestructura tecnológica del pabellón.

- **Respaldo eléctrico:** Los equipos críticos del sistema deberán contar con respaldo energético mediante sistemas de alimentación ininterrumpida (UPS), garantizando la continuidad operativa ante interrupciones del suministro eléctrico.
- **Altura de instalación:** Los dispositivos serán instalados a alturas adecuadas que permitan optimizar su funcionamiento y reducir riesgos de manipulación no autorizada.
- **Sistema de puesta a tierra:** Los equipos y componentes metálicos de la infraestructura deberán conectarse al sistema de puesta a tierra, con el fin de brindar protección frente a sobretensiones y descargas eléctricas.
- **Escalabilidad de la infraestructura:** La infraestructura tecnológica será diseñada considerando capacidad de crecimiento para futuras ampliaciones de los sistemas de seguridad electrónica.
- **Normativas técnicas:** La implementación deberá cumplir con las normas técnicas aplicables a cableado estructurado, instalaciones eléctricas y sistemas de seguridad electrónica.

5.7.1. Diseño del Cableado Estructurado

En esta sección se describe la infraestructura de cableado estructurado propuesta para soportar las comunicaciones del sistema de seguridad inteligente, considerando criterios

de organización, disponibilidad y escalabilidad conforme a los lineamientos de la norma ANSI/TIA/EIA-568-B.1.

Cableado Horizontal

- **Tipo de cable:** Se empleará cable de par trenzado no blindado (UTP) Categoría 6. Este estándar proporciona un ancho de banda de hasta 1 Gbps y una frecuencia de 250 MHz, características suficientes para soportar la transmisión de video IP, eventos de control de acceso y señales del sistema de alarmas, además de permitir futuras ampliaciones de la infraestructura.

- **Conexión de dispositivos hacia los switches:** La interconexión se realizará mediante una topología de estrella, donde cada dispositivo final se conectará de forma independiente al switch de acceso correspondiente. Esta configuración facilita el aislamiento de fallas y mejora la administración de la red.

- **Distribución del cableado:** El tendido de cables se realizará mediante tuberías conduit y bandejas portacables instaladas en el pabellón.

- **Distancias máximas de transmisión:** De acuerdo con el estándar ANSI/TIA-568, las tiradas de cable UTP no superarán los 90 metros entre el switch y el dispositivo final, garantizando la integridad de la señal y el correcto funcionamiento de los equipos PoE.

- **Alimentación mediante Power over Ethernet (PoE):** Se utilizarán switches con tecnología PoE (IEEE 802.3af/at), permitiendo transmitir datos y alimentación eléctrica a través del mismo cable UTP hacia cámaras IP y lectores biométricos, reduciendo la necesidad de fuentes de alimentación locales.

Backbone de Comunicaciones

La infraestructura de backbone permitirá concentrar el tráfico generado por los subsistemas de videovigilancia, control de acceso y alarmas hacia el rack principal de telecomunicaciones.

- **Interconexión de dispositivos y áreas:** La red permitirá integrar los equipos instalados en los diferentes ambientes del pabellón con el centro de monitoreo y administración del sistema de seguridad.
- **Convergencia hacia el rack principal:** Los enlaces de comunicación convergerán hacia un rack principal ubicado en un ambiente protegido del pabellón. En este gabinete se instalarán los switches principales, el NVR y los equipos de respaldo eléctrico.
- **Capacidad del backbone:** El backbone será dimensionado considerando el tráfico simultáneo generado por las cámaras IP, lectores biométricos y paneles de alarma, asegurando capacidad suficiente para la operación estable del sistema y futuras ampliaciones.
- **Priorización del tráfico de seguridad:** Se contempla la implementación de mecanismos de Calidad de Servicio (QoS) en los equipos de red, priorizando el tráfico asociado a video, eventos de alarma y control de acceso. Entre los mecanismos considerados se incluyen la clasificación de tráfico mediante DSCP, segmentación por VLAN y colas de prioridad para aplicaciones críticas.

Canalizaciones y Rutas de Cableado

- **Canalizaciones:** Se implementará un sistema de canalización basado en tuberías metálicas y bandejas portacables. El dimensionamiento de los ductos considerará un factor máximo de llenado del 40 %, facilitando la ventilación y futuras ampliaciones

del cableado.

- **Rutas de distribución:** Las trayectorias del cableado seguirán recorridos accesibles y ordenados, aprovechando los ductos técnicos y cielos rasos existentes en el pabellón, evitando curvaturas excesivas que puedan afectar el desempeño del cable UTP.
- **Protección física:** Los conductores y puntos de conexión permanecerán protegidos mediante canalizaciones cerradas y accesorios de instalación, reduciendo el riesgo de daños mecánicos o manipulación no autorizada.
- **Separación entre energía y datos:** Para minimizar interferencias electromagnéticas, se mantendrá separación física entre las canalizaciones de datos y las líneas eléctricas de potencia. En los cruces inevitables, estos se realizarán en ángulo recto.
- **Facilidad de mantenimiento y expansión:** El sistema de canalización permitirá la inspección y mantenimiento de los conductores mediante cajas de paso estratégicamente ubicadas, además de considerar capacidad disponible para futuras ampliaciones.

Rack y Patch Panel

- **Ubicación del rack:** Se instalará un gabinete de telecomunicaciones en un ambiente seguro y ventilado del pabellón, destinado a centralizar la infraestructura de comunicaciones y seguridad electrónica.
- **Organización de equipos:** Los equipos activos serán distribuidos de forma ordenada dentro del rack, ubicando switches y dispositivos de gestión en las unidades superiores, mientras que los equipos de mayor peso se colocarán en la parte inferior del gabinete.
- **Patch panels:** Se implementarán patch panels Categoría 6 para la terminación del cableado horizontal. Esto facilitará la administración de conexiones y reducirá el desgaste de los puertos de los switches.

- **Switches PoE:** La infraestructura contará con switches PoE capaces de suministrar alimentación eléctrica a cámaras IP y lectores biométricos directamente desde el rack principal.

- **Administración y etiquetado:** El rack contará con organizadores horizontales y verticales para el manejo del cableado. Asimismo, se aplicará la norma ANSI/TIA-606-B para la identificación y etiquetado de cables, puertos y dispositivos de red.

Segmentación de Red mediante VLAN

La arquitectura de red propuesta contempla la segmentación lógica de los subsistemas de seguridad electrónica mediante redes de área local virtuales (VLAN), con la finalidad de mejorar la administración, seguridad y rendimiento de la infraestructura de comunicaciones del pabellón.

- **Separación lógica de los subsistemas:** Se implementará la segmentación de la red utilizando VLANs, permitiendo aislar el tráfico correspondiente a los sistemas de videovigilancia, control de acceso y alarmas. Esta separación lógica evita interferencias con la red administrativa o académica de la institución y garantiza que el funcionamiento de los sistemas de seguridad no se vea afectado por otros servicios de la red del pabellón.

- **Organización de la infraestructura de seguridad:** La segmentación permitirá agrupar los dispositivos según su función dentro del sistema de seguridad, facilitando la administración de cámaras IP, lectores biométricos, paneles de alarma, estaciones de monitoreo y servidores de gestión. Asimismo, posibilita la asignación ordenada de direccionamiento IP estático, mejorando el control y monitoreo de los dispositivos desde la plataforma de gestión unificada.

- **Seguridad de red y control de acceso:** Con el propósito de reforzar la seguridad

de la infraestructura, se aplicarán mecanismos de protección a nivel de capa 2, tales como port security en los switches administrables, restringiendo la conexión únicamente a dispositivos autorizados. Además, se deshabilitarán los puertos no utilizados y se establecerán políticas de acceso que limiten la administración de cámaras, NVR y servidores únicamente al personal autorizado desde el centro de monitoreo.

- **Reducción de congestión y optimización del tráfico:** La segmentación mediante VLAN permite reducir el alcance del tráfico de difusión (broadcast), evitando que las comunicaciones generadas por otros equipos del pabellón afecten el rendimiento de los sistemas de seguridad electrónica. Esto resulta especialmente importante para el sistema de videovigilancia IP, debido a consumo de ancho de banda requerido para la transmisión de video en alta resolución.

Firewall Perimetral

Se propone la incorporación de un firewall perimetral como mecanismo de seguridad lógica encargado de controlar y filtrar el tráfico de red entre la infraestructura interna del pabellón y las redes externas, permitiendo proteger los dispositivos del sistema de videovigilancia, control de acceso y alarmas frente a accesos no autorizados y posibles amenazas informáticas.

5.8. Presupuesto Referencial

5.9. Matriz de Trazabilidad Normativa

Tabla 5.24: *Listado de Equipos de Videovigilancia*

Descripción	**Cantidad**	**PU**	**Subtotal**
Nvr 64 canales	1	S/ 13,910.00	S/ 13,910.00
Cámara domo ip 4mp	30	S/ 635.00	S/ 19,050.00
Cámara tubo ip 4mp	1	S/ 620.00	S/ 620.00
Cámara ptz ip 4mp	3	S/ 2,225.00	S/ 6,675.00
Plug rj45 cat6 x100und	1	S/ 115.00	S/ 115.00
Cable utp cat6 rollo	5	S/ 780.00	S/ 3,900.00
Disco duro 12tb	5	S/ 2,775.00	S/ 13,875.00
Switch 16 puertos poe	4	S/ 1,165.00	S/ 4,660.00
Switch 8 puerto	1	S/ 558.00	S/ 558.00
Ups 4 tomas 600w	1	S/ 340.00	S/ 340.00
Patch panel cat6	4	S/ 225.00	S/ 900.00
Organizador horizontal 1ru	4	S/ 50.00	S/ 200.00
Patch cord 2m cat6	34	S/ 15.00	S/ 510.00
Power rack 8 tomas 15a	5	S/ 540.00	S/ 2,700.00
Materiales extras			S/ 12,572.00
Subtotal			**S/ 80,585.00**

Tabla 5.25: *Listado de Equipos de Sistema de Alarma*

Descripción	**Cantidad**	**PU**	**Subtotal**
Panel de alarma	1	S/ 1,056.00	S/ 1,056.00
Sensor pir	13	S/ 95.00	S/ 1,235.00
Sirena interior	1	S/ 287.00	S/ 287.00
Sirena exterior	1	S/ 287.00	S/ 287.00
Teclado	1	S/ 129.00	S/ 129.00
Cable de alarma rollo	2	S/ 400.00	S/ 800.00
Cable utp cat6 x metro	20	S/ 2.50	S/ 50.00
Plug rj45 cat6 x100und	1	S/ 115.00	S/ 115.00
Materiales extras	1		S/ 3,695.00
Subtotal			**S/ 7,654.00**

Tabla 5.26: *Listado de Equipos de Control de Acceso*

Descripción	**Cantidad**	**PU**	**Subtotal**
Cerradura 270kg	28	S/ 120.00	S/ 3,360.00
Botón de salida	28	S/ 65.00	S/ 1,820.00
Control de acceso	28	S/ 670.00	S/ 18,760.00
Switch 8p poe giga	1	S/ 725.00	S/ 725.00
Switch 16p poe giga	2	S/ 1,165.00	S/ 2,330.00
Patch panel cat6	3	S/ 225.00	S/ 675.00
Organizador horizontal 1ru	3	S/ 50.00	S/ 150.00
Cable de alarma rollo	1	S/ 400.00	S/ 400.00
Cable utp cat6 rollo	3	S/ 570.00	S/ 1,710.00
Plug rj45 cat6 x100und	1	S/ 115.00	S/ 115.00
Patch cord 2m cat6	28	S/ 15.00	S/ 420.00
Power rack 8 tomas 15a	3	S/ 540.00	S/ 1,620.00
Materiales extras	1		S/ 10,707.00
Subtotal			**S/ 42,792.00**

Tabla 5.27: *Listado de Materiales Compartidos*

Descripción	**Cantidad**	**PU**	**Subtotal**
Switch admi capa 3 24p	1	S/ 5,847.00	S/ 5,847.00
Ups rackable 3kva	4	S/ 2,899.00	S/ 11,596.00
Rack de piso 24ru	3	S/ 600.00	S/ 1,800.00
Gabinete de piso 18ru	1	S/ 1,610.00	S/ 1,610.00
Bandeja de rejilla	40	S/ 131.00	S/ 5,240.00
Materiales extras	1		S/ 3,992.00
Subtotal			**S/ 30,085.00**

Tabla 5.28: *Resumen general del presupuesto*

Descripción	**Subtotal**
Sistema de videovigilancia	S/ 80,585.00
Sistema de control de acceso	S/ 42,792.00
Sistema de alarmas	S/ 7,654.00
Materiales compartidos	S/ 30,085.00
Servicio de instalación y configuración	S/ 25,000.00
Total global del proyecto	**S/ 186,116.00**

Tabla 5.29: Matriz de trazabilidad normativa de los requerimientos técnicos

Requerimiento técnico	**Norma de referencia**	**Aplicación en el diseño**
Resolución mínima de 4 MP para cámaras IP.	ISO/IEC 62676	La resolución fue determinada mediante el análisis DORI para garantizar niveles adecuados de detección, observación, reconocimiento e identificación.
Interoperabilidad entre cámaras IP, NVR y plataforma de gestión.	ONVIF	Los dispositivos seleccionados cumplen estándares abiertos para garantizar compatibilidad e integración.
Alimentación eléctrica mediante PoE.	IEEE 802.3af	Permite suministrar energía y datos a través del mismo cable de red.
Cableado estructurado categoría 6.	ANSI/TIA-568	Define las características mínimas del medio de transmisión utilizado por el sistema.
Diseño de canalizaciones y rutas de cableado.	ANSI/TIA-569	Establece criterios para rutas y espacios destinados a telecomunicaciones.
Etiquetado e identificación de la infraestructura.	ANSI/TIA-568	Documentación e identificación de los enlaces de telecomunicaciones.
Implementación de sensores de intrusión en laboratorios.	IEC 62642	Define los criterios generales para sistemas de detección de intrusión.
Integración de subsistemas de videovigilancia, alarmas y control de acceso.	IEC 60839	Sustenta la arquitectura de un sistema electrónico de seguridad integrado.
Control de acceso mediante huella dactilar y tarjeta de proximidad.	IEC 60839	Define los requisitos generales para sistemas electrónicos de control de acceso.
Conservación de grabaciones por 30 días.	D. Leg. 1218 y Directiva N.º 01-2020-JUS/DGTAIPD	La capacidad de almacenamiento fue dimensionada para cumplir los requerimientos de videovigilancia institucional.
Protección de datos biométricos y registros de acceso.	Directiva N.º 01-2020-JUS/DGTAIPD	Se consideran medidas para el tratamiento de datos personales obtenidos por sistemas biométricos.
Respaldo eléctrico con autonomía mínima de una hora.	Código Nacional de Electricidad	Garantiza continuidad operativa ante interrupciones del suministro eléctrico.
Instalación de infraestructura de telecomunicaciones del sistema.	Norma EM.020	Cumplimiento de los requisitos nacionales para instalaciones de telecomunicaciones.

Capítulo 6

Documentos de Gestión y Procedimientos

6.1. Marco Estratégico y Normativo

6.1.1. Ámbito de Aplicación

La presente estructura de gestión está orientada a las áreas, actores y procesos involucrados en la implementación, operación y administración de los sistemas de seguridad electrónica del pabellón de Ingeniería Informática y de Sistemas. Su alcance comprende tanto los aspectos técnicos de ingeniería como los lineamientos normativos vinculados al tratamiento de datos personales.

Esta gestión aplica específicamente a los siguientes subsistemas integrados:

- Sistema de videovigilancia.
- Sistema de control de accesos.
- Sistema de alarmas.

6.1.2. Fundamento Normativo

El tratamiento de datos personales y la operación de los sistemas de seguridad electrónica propuestos se sustentan en la normativa peruana vigente en materia de protección de datos personales y videovigilancia:

Ley N.° 29733 – Ley de Protección de Datos Personales: Establece los principios, derechos, obligaciones y condiciones aplicables al tratamiento de datos personales, incluyendo la protección de información sensible.

Decreto Supremo N.° 003-2013-JUS: Aprueba el Reglamento de la Ley N.° 29733 y desarrolla las medidas jurídicas, organizativas y técnicas que deben implementarse para garantizar la seguridad de los datos personales.

Directiva N.° 01-2020-JUS/DGTAIPD: Establece disposiciones para el tratamiento de datos personales mediante sistemas de videovigilancia, incluyendo aspectos relacionados con el deber de información, conservación de grabaciones y atención de derechos ARCO.

6.2. Gestión de Datos Personales y Análisis de Riesgos

6.2.1. Identificación y Clasificación de Datos Personales

En el marco de la implementación del sistema integral de seguridad, se identifican los datos personales tratados por los subsistemas de videovigilancia, control de accesos y alarmas. Esta identificación permite definir medidas de protección acordes con el nivel de sensibilidad de la información.

Los datos tratados incluyen información de identificación, datos biométricos considerados sensibles y registros derivados de la operación del sistema.

Tabla 6.1: *Matriz de identificación de datos personales*

Sistema	**Tipo de dato**	**Categoría**	**Sensibilidad**	**Finalidad**
Videovigilancia	Imagen de personas	Dato personal	Medio	Supervisión y seguridad
Videovigilancia	Rasgos faciales (analítica)	Dato biométrico	Alto	Identificación
Videovigilancia	Ubicación y desplazamiento	Dato de comportamiento	Medio	Control de áreas
Videovigilancia	Fecha y hora de grabación	Dato indirecto	Bajo	Trazabilidad
Control de acceso	Nombre y apellidos	Dato personal	Medio	Identificación
Control de acceso	DNI / código institucional	Dato personal	Medio	Validación de usuario
Control de acceso	Huella dactilar	Dato biométrico	Alto	Autenticación
Control de acceso	Reconocimiento facial	Dato biométrico	Alto	Autenticación
Control de acceso	Tarjeta RFID / credencial	Dato identificador	Medio	Acceso físico
Control de acceso	Registro de accesos (logs)	Dato de comportamiento	Medio	Auditoría y control
Sistema de alarmas	Eventos de activación	Dato de seguridad	Bajo	Detección de incidentes
Sistema de alarmas	Usuario que activa/desactiva	Dato personal	Medio	Responsabilidad operativa
Sistema de alarmas	Ubicación del sensor	Dato indirecto	Bajo	Gestión del sistema
Sistema de alarmas	Historial de incidencias	Dato derivado	Medio	Análisis de seguridad

6.2.2. Análisis de Riesgos en el Tratamiento de Datos

El tratamiento de datos personales dentro de los sistemas de seguridad electrónica implica riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de la información. Los datos biométricos y los registros de comportamiento presentan un mayor nivel de criticidad, por lo que requieren controles de protección reforzados.

Niveles de Impacto

- **Impacto bajo:** Consecuencias mínimas y fácilmente reversibles.
- **Impacto medio:** Afectación parcial de la privacidad o del funcionamiento del sistema.

- **Impacto alto:** Posibilidad de accesos indebidos, vulneraciones significativas o afectación importante a la seguridad.
- **Impacto muy alto:** Compromiso de datos altamente sensibles o irreversibles, como los datos biométricos.

Matriz de Riesgos

Tabla 6.2: *Matriz de riesgos en el tratamiento de datos personales*

Tipo de dato	**Riesgo identificado**	**Impacto**	**Medidas de protección**
Imágenes	Acceso no autorizado a grabaciones	Alto	Control de acceso, cifrado y registro de accesos
Datos biométricos	Robo o filtración de datos sensibles	Muy alto	Cifrado fuerte, almacenamiento seguro y acceso restringido
Registros de acceso	Uso indebido de información de usuarios	Medio	Políticas de acceso y auditoría de logs
Datos de comportamiento	Seguimiento indebido de personas	Medio	Anonimización parcial y limitación de uso
Credenciales (RFID, claves)	Suplantación de identidad	Alto	Autenticación segura y renovación de credenciales
Eventos de alarmas	Manipulación o eliminación de registros	Medio	Integridad de datos y copias de seguridad
Logs del sistema	Exposición de información sensible	Medio	Restricción de acceso y almacenamiento seguro

6.3. Políticas de Seguridad y Privacidad

6.3.1. Políticas de Privacidad y Seguridad desde el Diseño

Con el propósito de garantizar una infraestructura tecnológica segura y alineada con la normativa vigente en materia de protección de datos personales y seguridad de la información, se establecen los siguientes lineamientos:

1. **Minimización y protección de datos:** Recopilar únicamente la información estrictamente necesaria para fines de seguridad institucional. En caso de compartir material audiovisual con terceros que no requieran la identificación directa de personas, se deberá aplicar técnicas de anonimización o difuminado de elementos identificables.

2. **Plazos de conservación:** Las grabaciones de videovigilancia se conservarán por un periodo de 30 a 60 días, salvo que exista una investigación o procedimiento en curso. Los datos biométricos serán eliminados al finalizar la relación institucional del usuario, conforme al principio de finalidad.

3. **Aislamiento de infraestructura crítica:** Los sistemas de seguridad electrónica operarán en redes segmentadas mediante VLAN dedicadas y protegidas mediante mecanismos de seguridad perimetral, como firewalls.

4. **Trazabilidad y control administrativo:** El acceso a la plataforma de gestión unificada requerirá credenciales individuales y autenticación multifactor (MFA), manteniendo registros de auditoría para garantizar la trazabilidad de las operaciones realizadas.

5. **Restricción en espacios sensibles:** Se prohíbe la captura de imágenes o datos en ambientes que puedan comprometer la privacidad y dignidad de las personas, conforme a la normativa de protección de datos personales.

6.3.2. Protocolo para el Ejercicio de Derechos ARCO

Con la finalidad de garantizar el control de los usuarios sobre sus datos personales, se establece el siguiente procedimiento:

- **Gestión de solicitudes:** Las solicitudes deberán presentarse ante la Mesa de Partes de la Facultad y dirigirse al responsable del tratamiento de datos.

- **Acreditación de identidad:** Será obligatoria la presentación del Documento Nacional de Identidad (DNI).
- **Solicitudes relacionadas con videovigilancia:** El usuario deberá indicar fecha, hora aproximada y ubicación de la cámara.
- **Plazos de atención:** Las solicitudes serán atendidas conforme a los plazos establecidos en el Reglamento de la Ley N.° 29733.

6.4. Manual de Procedimientos Operativos

6.4.1. Gestión de Incidentes en Videovigilancia

Clasificación de Incidentes

Tabla 6.3: *Clasificación de Incidentes de Seguridad*

Nivel	**Descripción**	**Acción inmediata**
Nivel 1 (Bajo)	Fallas técnicas menores o conductas inusuales sin riesgo.	Registro en bitácora y monitoreo preventivo.
Nivel 2 (Medio)	Intentos de intrusión, vandalismo o disputas en áreas comunes.	Aviso a supervisión y despliegue de personal físico.
Nivel 3 (Alto)	Robo, incendio, agresiones o intrusión confirmada.	Comunicación inmediata a autoridades y preservación de evidencia.

Detección y Seguimiento

Ante la identificación de un evento sospechoso, el operador deberá:

1. Seleccionar la cámara con mejor ángulo de visualización y activar grabación de alta resolución.

2. Realizar seguimiento mediante cámaras adyacentes para mantener continuidad visual.

3. Priorizar la captura de rasgos físicos, vestimenta y otros elementos relevantes.

Gestión de Evidencia y Cadena de Custodia

Para preservar la validez de la evidencia audiovisual:

- Extraer grabaciones desde cinco minutos antes hasta cinco minutos después del incidente.
- Exportar el material en formato nativo con mecanismos de verificación de integridad.
- Registrar fecha, hora, cámara y motivo de extracción.

Procedimiento ante Fallas del Sistema

En caso de pérdida de señal o fallos en almacenamiento:

- Notificar al área técnica.
- Incrementar rondas de vigilancia física.
- Registrar el periodo de indisponibilidad del sistema.

6.4.2. Gestión del Sistema de Control de Accesos

Eventos de Seguridad y Respuesta Operativa

Alerta de puerta forzada

1. Verificar la cámara más cercana al acceso comprometido.

2. Confirmar posible intrusión y coordinar apoyo de seguridad.

3. Revisar daños en cerraduras o electroimanes.

Acceso denegado o tarjeta no válida

1. Verificar si existe intento de ingreso forzado.

2. En caso de reiteración, validar identidad mediante supervisión.

Manejo de Credenciales

- **Reporte de extravío:** Toda tarjeta reportada como perdida deberá ser bloqueada inmediatamente.
- **Uso indebido:** El préstamo de credenciales deberá registrarse como incidencia administrativa.

Fallas y Contingencias

Tabla 6.4: *Contingencias ante fallas del sistema de acceso*

Fallo detectado	**Acción de contingencia**
Lectora no reconoce tarjetas	Verificar si el problema corresponde a la tarjeta o al dispositivo y reportar a mantenimiento.
Puerta no asegura correctamente	Asignar vigilancia física temporal hasta la reparación.
Corte de energía	Verificar el modo seguro de funcionamiento de la chapa eléctrica conforme al protocolo institucional.

6.4.3. Gestión del Sistema de Alarmas

Tipos de Alertas y Respuesta

Alarma de intrusión

1. Verificar la zona activada.

2. Confirmar el evento mediante videovigilancia.

3. Coordinar respuesta de seguridad y comunicación a autoridades.

Fallo de batería o sabotaje

1. Identificar el origen del fallo.

2. Reportar inmediatamente al área técnica.

6.5. Continuidad Operativa y Mantenimiento

6.5.1. Verificación Operativa Diaria

Al inicio de cada jornada, el operador deberá verificar el estado general de funcionamiento de los dispositivos de seguridad.

Tabla 6.5: *Checklist de verificación de equipos de seguridad*

Punto a revisar	**Estado (SI / NO)**
¿El panel de alarmas presenta errores o alertas?	
¿El flujo de video de las cámaras es estable y continuo?	
¿Las puertas con control de acceso funcionan correctamente?	
¿El botón de pánico se encuentra operativo y accesible?	

6.5.2. Gestión de Servicios de Terceros

Las actividades de instalación, mantenimiento o soporte técnico realizadas por empresas externas deberán ejecutarse bajo controles de seguridad que permitan proteger la infraestructura tecnológica y la información gestionada por los sistemas de seguridad electrónica.

Toda intervención externa deberá ser previamente autorizada por el área responsable del sistema, registrando la fecha, hora, personal involucrado y actividades a realizar. Asimismo, las empresas proveedoras deberán cumplir las políticas institucionales relacionadas con seguridad de la información y protección de datos personales.

Para trabajos realizados por terceros, se establecen las siguientes medidas:

- Los técnicos deberán utilizar accesos temporales restringidos, limitados únicamente a los recursos necesarios para la actividad asignada.
- Toda intervención será supervisada por personal del área de TI o por el responsable del sistema de seguridad electrónica.
- Será obligatoria la firma de acuerdos de confidencialidad y compromisos de no divulgación de información sensible.
- Se restringirá el acceso a grabaciones, bases de datos biométricas y configuraciones críticas del sistema, salvo autorización expresa.
- Toda modificación realizada sobre dispositivos, servidores o configuraciones deberá quedar registrada en una bitácora de mantenimiento.
- Finalizada la intervención, se deberán deshabilitar los accesos temporales otorgados al personal externo.

6.6. Instrumentos de Control y Verificación

6.6.1. Checklist de Cumplimiento de Seguridad

Tabla 6.6: *Lista de verificación de controles de seguridad y privacidad*

Ítem de verificación	**Estado**
¿Los sistemas cuentan con cifrado de almacenamiento y transmisión?	SI / NO
¿Existen avisos de videovigilancia visibles?	SI / NO
¿Se registran automáticamente las exportaciones de video?	SI / NO
¿El software se encuentra actualizado con parches de seguridad?	SI / NO
¿Existe consentimiento para el tratamiento de datos biométricos?	SI / NO

6.6.2. Modelo de Aviso de Privacidad

Para garantizar el derecho de información de los usuarios, se diseñó la señalética obligatoria tomando como base la Directiva N.° 01-2020-JUS/DGTAIP. Sin embargo, debido a que el formato original de la norma empleaba un pictograma de dron, este fue adaptado gráficamente sustituyéndolo por una cámara fija y optimizando el color amarillo de seguridad para ajustarse estrictamente a la naturaleza del hardware y entorno del proyecto. El diseño final propuesto se presenta en el Anexo C.

6.6.3. Formato de Consentimiento Informado (Datos Biométricos)

Yo, _____, con DNI _____, autorizo de manera libre e inequívoca a la institución para el tratamiento de mis datos biométricos con la única finalidad de gestión de accesos a ambientes controlados, bajo las medidas de seguridad técnicas descritas en el

manual de gestión de la facultad.

6.6.4. Bitácora Unificada de Incidentes

Este formato centraliza los eventos de los subsistemas de Videovigilancia, Accesos y Alarmas en un registro único, facilitando el control operativo diario.

Tabla 6.7: *Registro General de Incidentes de Seguridad*

Fecha y Hora	.....
Sistema	(Video / Acceso / Alarma): .....
Ubicación	(Ej. Laboratorio, Entrada, Pasillo): .....
Descripción del Evento	....
Acción Realizada	....
Referencia	(ID de Video o Log de Acceso): .....
Operador	Firma: .....

6.6.5. Checklist de Cumplimiento de Privacidad

Lista de verificación interna para evaluar el cumplimiento del tratamiento adecuado de datos personales

Tabla 6.8: *Lista de verificación de controles de seguridad y privacidad*

Ítem de verificación	**Cumplimiento**
Se ha identificado al responsable y encargado del tratamiento.	SI / NO
Se cuenta con documento de consentimiento para el uso de datos biométricos.	SI / NO
Existe un aviso de privacidad visible en zonas con cámaras de videovigilancia.	SI / NO
Los sistemas cuentan con medidas de seguridad técnicas (cifrado, contraseñas, logs).	SI / NO
Se ha capacitado al personal que opera los sistemas de seguridad.	SI / NO
Se ha definido un tiempo máximo de conservación para grabaciones o registros.	SI / NO
Existe un canal de atención para solicitudes de derechos ARCO.	SI / NO
El software utilizado está actualizado y cumple con políticas de protección de datos.	SI / NO
Hay respaldo de información y mecanismos para respuesta ante incidentes.	SI / NO
Se han firmado contratos con proveedores con cláusulas de protección de datos.	SI / NO

Formato: Registro de Cadena de Custodia de Evidencia

1. Datos generales de la evidencia

Tipo de evidencia: _____

Descripción de la evidencia: _____

Subsistema de origen: Videovigilancia / Control de acceso / Alarmas

Código de identificación: _____

2. Datos del levantamiento

Fecha: _____ Hora: _____

Ubicación: _____

Responsable del levantamiento: _____

Cargo: _____

3. Detalle del evento

Tipo de incidente: _____

Descripción del hecho:

_____

_____

_____

4. Observaciones

_____

_____

_____

5. Registro de transferencia de custodia

Entregado por	Cargo	Recibido por	Cargo	Fecha	Hora	Motivo

6. Responsables finales

Responsable del registro: _____

Firma: _____

Capítulo 7

Resultados

7.1. Análisis de resultados obtenidos

Los resultados obtenidos evidencian que el objetivo general de la investigación fue cumplido, al diseñarse un sistema integrado de seguridad electrónica basado en IoT para la Escuela Profesional de Ingeniería Informática y de Sistemas, orientado al monitoreo continuo, la gestión eficiente de accesos y la respuesta oportuna ante incidentes. Asimismo, se alcanzaron los objetivos específicos mediante el diseño de un sistema de videovigilancia inteligente, un sistema de alarmas de intrusión y detección de emergencias, y un sistema de control de accesos inteligente, los cuales se integran en una plataforma de gestión de seguridad unificada. Finalmente, como aporte complementario, se elaboró una guía de tratamiento de datos personales que incorpora criterios legales, técnicos y organizativos, fortaleciendo el enfoque responsable y normativo del sistema de seguridad propuesto.

7.2. Discusión de resultados respecto a los antecedentes

El análisis e interpretación de los resultados obtenidos en esta investigación permiten contrastar la propuesta tecnológica para el pabellón de la Escuela Profesional de Ingeniería

Informática y de Sistemas de la UNSAAC frente a los antecedentes del marco referencial. A continuación, se discuten los hallazgos en función de las ventajas técnicas, la escala del diseño y el valor metodológico y normativo aportado por esta tesis.

7.2.1. Escala de Cobertura y Optimización Teórica frente a Casos de Estudio

En lo relativo al diseño de la cobertura de videovigilancia y la mitigación de puntos ciegos, los resultados de esta investigación demuestran una optimización en la distribución tridimensional de los dispositivos de campo. Al contrastar este hallazgo con el primer antecedente desarrollado por Báez Buelvas (2019), se evidencia que este último validó los principios de distancia focal y campo de visión (FOV) en un entorno reducido de solo 9 cámaras para 6 laboratorios en un plano estrictamente horizontal.

La presente tesis **supera técnicamente dicha escala de diseño**, al proyectar un sistema integrado de mayor complejidad que abarca entre 27 y 32 cámaras distribuidas volumétricamente en múltiples pisos (niveles 3 y 4 del pabellón), pasadizos y accesos principales. De este modo, se demuestra que la modelación geométrica previa no solo es válida para espacios confinados como los de Báez Buelvas, sino que es escalable a infraestructuras educativas de gran envergadura sin perder eficiencia en la resolución de captura.

Por otra parte, respecto al impacto de la tecnología en los índices de inseguridad, el diagnóstico de esta investigación dialoga con el trabajo de **?** (**?**) para la Ciudad de México. Mientras que **?** plantea a nivel macro-social que los sistemas de videovigilancia son insuficientes si no se resuelven brechas políticas y educativas estructurales, esta investigación **operativiza esa limitación teórica desde la ingeniería práctica**. En lugar de delegar la efectividad del sistema a variables sociológicas abstractas, la presente propuesta mitiga el factor de insuficiencia tecnológica mediante el diseño explícito de protocolos de respuesta

rápida unificados para el operador del centro de monitoreo local (NOC/SOC), aterrizando con éxito el concepto de seguridad activa al micro-entorno universitario.

7.2.2. Dimensionamiento, Escalabilidad y Adaptación del Entorno Operativo

Al evaluar la arquitectura del Centro de Monitoreo y la infraestructura de red, se realizó un contraste crítico con el antecedente de Perez Morris (2016) en una instalación minera. Perez Morris reportó un diseño con serias restricciones de escalabilidad (limitado al 25 %) debido a un cuello de botella en el servidor de grabación de 2TB y un sobredimensionamiento innecesario en los switches de agregación frente a su troncal de fibra.

En contraste, **esta tesis corrigió dichos errores de dimensionamiento logrando una arquitectura más eficiente y escalable**. Mediante el cálculo matemático del flujo de bits (bitrate) y la adopción de códecs de compresión modernos como H.265, se dimensionó un sistema de almacenamiento masivo y una topología de red capaces de soportar la concurrencia de hasta 32 cámaras en alta definición de forma continua, optimizando el presupuesto de hardware y evitando el desperdicio de ancho de banda reportado en el entorno minero.

Asimismo, la integración mulisubsistema (CCTV IP, alarmas y biometría) se analizó frente al informe técnico de Gonzales Rodriguez (2024) para la Caja Cusco. Si bien los resultados de esta tesis coinciden con Gonzales Rodriguez en que las plataformas de gestión unificada (VMS) reducen drásticamente la latencia de las alarmas, **existe una diferencia sustancial en el enfoque del entorno operativo**. El modelo de Gonzales Rodriguez responde a un entorno financiero ultra-restrictivo regulado por la SBS, inviable para una universidad pública. Esta investigación adaptó con éxito los criterios de alta disponibilidad y redundancia bancaria a un contexto de educación superior de libre tránsito, logrando equilibrar la rigurosidad de la protección de activos con la fluidez logística y peatonal que

exige la comunidad de la UNSAAC.

7.2.3. Soporte en Estándares Físicos de Telecomunicaciones

En el ámbito de la capa física de comunicaciones, los cálculos de atenuación, ancho de banda y rendimiento de streams de video de esta propuesta **se apoyan sólidamente en los criterios técnicos** validados por Sibitanga and Toaquiza (2017) en Ecuador. Al igual que los autores demostraron que la certificación de redes LAN bajo normas ANSI/TIA/EIA 568 reduce drásticamente la pérdida de paquetes en laboratorios de software, esta tesis adopta estrictamente las normas TIA/EIA 568 y 569 para el diseño de las canalizaciones y espacios técnicos del pabellón. Esto garantiza inmunidad contra la interferencia electromagnética (EMI) del entorno académico y asegura la estabilidad a largo plazo del tráfico de datos de seguridad, validando que el cumplimiento de estándares internacionales es la base obligatoria de cualquier sistema integrado de ingeniería.

7.2.4. Operativización de la Gobernanza Tecnológica y Privacidad

Finalmente, el tratamiento de información sensible constituye el principal eje diferenciador y de mejora metodológica de esta tesis. Al contrastar la propuesta con el antecedente internacional de Lyon (2022), se observa que el autor aborda la vigilancia contemporánea desde una perspectiva puramente sociológica y filosófica, advirtiendo sobre los riesgos éticos de la captura masiva de datos y la falta de marcos de justicia social, pero sin proponer mecanismos de ingeniería para resolverlo.

Esta tesis **supera la naturaleza puramente descriptiva de dicho antecedente al operativizar la gobernanza de datos en el plano legal-técnico peruano**. Mediante la implementación transversal de la Ley N.° 29733 (Ley de Protección de Datos Personales en el Perú) en el modelo conceptual del sistema, se diseñaron soluciones prácticas:

máscaras de privacidad automatizadas en el VMS, cifrado de plantillas biométricas y flujos procedimentales para salvaguardar los derechos ARCO y el consentimiento informado de usuarios y docentes. Con esto se demuestra de forma inédita que es viable diseñar un sistema de seguridad electrónica robusto para el pabellón de la UNSAAC sin incurrir en la vigilancia invasiva que denuncia el autor.

Conclusiones

1. Se diseñó un sistema integrado de seguridad electrónica basado en tecnologías IoT para el pabellón de Ingeniería Informática y de Sistemas, integrando videovigilancia, control de acceso y sistemas de alarma, conforme a los requerimientos de seguridad y la normativa aplicable.

2. Se diseñó un sistema de videovigilancia que considera criterios técnicos de cobertura, ubicación estratégica de cámaras y capacidad de integración con otros subsistemas, lo que permite el monitoreo continuo de ambientes críticos y la optimización de la gestión de eventos. Esta propuesta contribuye a fortalecer la vigilancia tanto en áreas comunes como en ambientes restringidos, incrementando los niveles de seguridad y control.

3. Se diseñó un sistema de control de accesos que regula el ingreso a los ambientes restringidos mediante mecanismos de autenticación adecuados, integrando criterios de seguridad, trazabilidad y gestión de usuarios. Esto permite contar con registros confiables de los accesos y mejorar el control sobre el uso de los espacios y recursos institucionales.

4. El sistema de alarmas fue concebido a partir del análisis de riesgos del pabellón, incorporando sensores de movimiento y dispositivos de alerta sonora que facilitan la detección temprana de accesos no autorizados y la activación oportuna de mecanismos de respuesta ante incidentes.

5. Todos los subsistemas propuestos se articulan mediante una plataforma de gestión de seguridad unificada que centraliza el monitoreo e integra dispositivos, mejorando la eficiencia operativa y optimizando la toma de decisiones ante eventos críticos.

6. Se elaboraron los documentos de gestión y procedimientos para el tratamiento de los datos personales generados por los sistemas de seguridad, alineados con la normativa vigente, lo que garantiza un uso responsable de la información y refuerza la viabilidad, legalidad y sostenibilidad del sistema diseñado.

Recomendaciones

1. Se recomienda ejecutar la instalación física y configuración lógica del sistema propuesto, validando el hardware seleccionado, la ubicación de los periféricos y el almacenamiento calculado.

2. Se sugiere realizar pruebas de estrés en condiciones operativas reales y horas punta para evaluar el subsistema de control de accesos. Esto permitirá medir métricas críticas como los tiempos de la autenticación, tasas de error y el impacto directo en el flujo de los estudiantes hacia los laboratorios.

3. Se recomienda desarrollar escenarios controlados para calibrar la sensibilidad de los sensores de movimiento y verificar los tiempos de respuesta ante eventos de intrusión. Asimismo, se debe evaluar su integración operativa con los protocolos de evacuación y alertas sonoras del pabellón.

4. Se sugiere el desarrollo de un software a medida basado en el modelo de integración propuesto, orientando los trabajos futuros hacia la automatización inteligente de procesos institucionales.

5. Se recomienda establecer revisiones periódicas de los documentos de gestión, formatos de consentimiento e instrumentos para el ejercicio de los derechos ARCO. Este proceso es indispensable para asegurar el alineamiento continuo con el reglamento vigente.

Trabajos Futuros

- Extender el diseño propuesto hacia un modelo integral de seguridad para campus universitarios, incorporando la protección y supervisión de estacionamientos, accesos vehiculares y peatonales, áreas deportivas, áreas comunes y demás espacios institucionales mediante tecnologías de seguridad electrónica.

- Investigar y desarrollar funciones inteligentes orientadas a entornos educativos que permitan mejorar la prevención, detección y gestión de incidentes de seguridad mediante el uso de analítica de datos e inteligencia artificial.

- Evaluar mecanismos avanzados de ciberseguridad para la protección de dispositivos IoT y de la información procesada por los sistemas de videovigilancia y control de acceso.

- Realizar estudios comparativos entre diferentes tecnologías biométricas, tales como reconocimiento facial, reconocimiento de iris y huella dactilar, con la finalidad de determinar su viabilidad técnica y operativa en entornos universitarios.

Bibliografía

Autoridad Nacional de Protección de Datos Personales (2023). Protección de datos personales en sistemas de videovigilancia. Ministerio de Justicia y Derechos Humanos del Perú.

Báez Buelvas, D. M. (2019). Implementación de un sistema de video vigilancia a través de cámaras de seguridad para los laboratorios de la facultad de ingeniería electrónica. Tesis de pregrado, Universidad Santo Tomás, Tunja, Colombia.

Congreso de la República del Perú (2011). Ley n.° 29733, ley de protección de datos personales. Diario Oficial El Peruano.

Congreso de la República del Perú (2015). Decreto legislativo n.° 1218 que regula el uso de las cámaras de videovigilancia. Publicado en el Diario Oficial El Peruano el 24 de junio de 2015.

Gonzales Rodriguez, E. J. (2024). Implementación de los sistemas de seguridad electrónica (sistemas de alarmas, cctv, y control de acceso) en los locales nuevos de la entidad financiera caja cusco.

Hernández-Sampieri, R. and Mendoza Torres, C. P. (2023). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill Interamericana, Ciudad de México, 2 edition.

IEEE Standards Association (2003). Ieee 802.3af-2003: Power over ethernet (poe).

Inria Chile and Baccelli, E. (2021). Libro blanco n°05. internet de las cosas (iot): Retos sociales y campos de investigación científica en relación con la iot. Libro blanco, Inria Chile / Instituto Francés de Investigación en Ciencias y Tecnologías Digitales, Santiago, Chile.

Instituto Nacional de Calidad (2014). *NTP ISO/IEC 27001: Sistema de Gestión de Seguridad de la Información*. Instituto Nacional de Calidad (INACAL).

International Electrotechnical Commission (2020). Iec 60839: Alarm and electronic security systems. `https://webstore.iec.ch/publication/67862`. [Recuperado el 11-05-2026].

International Electrotechnical Commission (2022). Iec 62642: Alarm systems – intrusion and hold-up systems. `https://webstore.iec.ch/publication/22973`. [Recuperado el 11-05-2026].

ISO/IEC (2014). *ISO/IEC 62676: Video Surveillance Systems*. International Organization for Standardization.

Lyon, D. (2022). Surveillance. *Internet Policy Review*, 11(4).

Ministerio de Economía y Finanzas del Perú (2020). Pautas para elaborar un expediente técnico más eficiente. url: https://www.mef.gob.pe/contenidos/inv_publica/docs/capacitaciones. [recuperado el 11-04-2025].

Ministerio de Energía y Minas del Perú (2006). *Código Nacional de Electricidad*.

Ministerio de Justicia y Derechos Humanos (2020). Directiva n.° 01-2020-jus/dgtaipd para el tratamiento de datos personales mediante sistemas de videovigilancia. Resolución Directoral N.° 02-2020-JUS/DGTAIPD.

Ministerio de Vivienda, Construcción y Saneamiento (2018). Norma técnica em.020: Instalaciones de telecomunicaciones. Resolución Ministerial N.° 400-2018-VIVIENDA, Reglamento Nacional de Edificaciones, Perú. Consultado el 25 de mayo de 2026.

Ministerio de Vivienda, Construcción y Saneamiento (2020). Reglamento nacional de edificaciones. Gobierno del Perú.

Norman, T. L. (2014). *Integrated Security Systems Design: A Complete Reference for Building Enterprise-Wide Digital Security Systems*. Butterworth-Heinemann, Boston, USA, 2 edition.

ONVIF (2023). Onvif: Open network video interface forum. Recuperado el 26 de noviembre de 2024.

Perez Morris, C. T. (2016). Diseño de un sistema de seguridad electrónica con monitoreo centralizado para protección de una instalación minera. Recuperado de repositorio institucional PUCP.

Presidencia de la República del Perú (2015). Decreto legislativo n.º 1218, decreto legislativo que regula el uso de las cámaras de videovigilancia.

Sibitanga, D. A. C. and Toaquiza, L. N. P. (2017). Cualificación y certificación de la red lan con cableado estructurado basado en normas internacionales ansi/tia/eia 568-b2, en el laboratorio de investigación de ingeniería de software, en el año 2017.

Telecommunications Industry Association (2001). Ansi/tia/eia-568-b.1: Commercial building telecommunications cabling standard.

Telecommunications Industry Association (2015). *ANSI/TIA-569-D: Telecommunications Pathways and Spaces*. TIA.

Glosario de Términos

IoT (Internet de las Cosas): Paradigma tecnológico que permite la interconexión de dispositivos físicos a través de Internet para intercambiar información y ejecutar acciones automatizadas.

Sistema Integrado de Seguridad Electrónica: Conjunto de tecnologías y dispositivos que operan de manera coordinada para proteger personas, bienes e infraestructura.

Videovigilancia: Sistema basado en cámaras que permite la supervisión y registro de actividades en áreas específicas.

Control de Acceso: Mecanismo que restringe o autoriza el ingreso de personas a determinadas áreas según permisos establecidos.

Identificación Biométrica: Método de autenticación basado en características físicas o conductuales únicas de una persona.

Sensor de Movimiento: Dispositivo capaz de detectar la presencia o desplazamiento de personas dentro de un área determinada.

Contacto Magnético: Sensor utilizado para detectar la apertura o cierre de puertas y ventanas.

Alarma: Sistema diseñado para generar alertas ante eventos de riesgo o accesos no autorizados.

CCTV: Circuito Cerrado de Televisión utilizado para el monitoreo y grabación de imágenes con fines de seguridad.

Plataforma de Gestión Unificada: Software que permite supervisar y administrar de forma centralizada los diferentes subsistemas de seguridad.

Riesgo: Probabilidad de ocurrencia de un evento que pueda afectar la seguridad de personas, bienes o instalaciones.

Vulnerabilidad: Debilidad existente en una infraestructura, proceso o sistema que puede ser aprovechada para generar un incidente de seguridad.

Seguridad Electrónica: Conjunto de tecnologías destinadas a prevenir, detectar y responder ante amenazas que afecten personas, bienes e instalaciones.

Anexo A: Cuestionario aplicado

Estimado(a) participante:

Lo(a) invitamos a responder esta encuesta que tiene como objetivo recolectar información sobre la situación actual de la seguridad en el pabellón de Ingeniería Informática y de Sistemas. Sus respuestas serán tratadas de manera confidencial, utilizándose únicamente para fines académicos.

¡Agradezco de antemano su valioso aporte!

Información general

Rol:
☐ Estudiante
☐ Docente
☐ Administrativo

1. ¿Cómo calificaría el nivel de seguridad actual del pabellón, considerando aspectos como la vigilancia, respuesta ante incidentes, el control de accesos y la detección de intrusos?

☐ Muy bajo
☐ Bajo
☐ Regular
☐ Bueno
☐ Alto
☐ No sabe / No tiene opinión

2. ¿Ha sido víctima o conoce algún caso sobre incidentes de seguridad como perdidas de sus pertenencias, robos, mal uso o daño a la infraestructura del pabellón?

☐ Sí ☐ No
Si su respuesta fue "Sí", describa brevemente el incidente:

……

……

……

……

3. ¿Tiene conocimiento de algún incidente relacionado con el ingreso no autorizado a algún ambiente del pabellón?

☐ Sí ☐ No
Si su respuesta fue "Sí", describa brevemente el incidente:

……

……

……

……

……

4. ¿Qué áreas considera más vulnerables en cuanto al riesgo de incidentes de seguridad? (Puede marcar más de una opción)

☐ Laboratorios (ambientes con equipos especializados)
☐ Aulas (salones de clases)
☐ Biblioteca
☐ Oficinas (dirección, coordinación, etc.)
☐ Pasillos
☐ Otros: ……..

5. ¿Tiene conocimiento de la existencia de sistemas de seguridad actualmente instalados en el pabellón?

☐ Sí, solo cámaras de videovigilancia
☐ Sí, solo alarmas de seguridad
☐ Sí, ambos (cámaras y alarmas)
☐ Sí, personal de seguridad
☐ No
☐ No estoy seguro

Si respondió Sí, ¿cómo calificaría su efectividad?

☐ Deficiente
☐ Poco efectivo
☐ Regular
☐ Efectivo
☐ Excelente

6. ¿Cómo evalúa la eficiencia del mecanismo actual de control de acceso a los ambientes del pabellón, en particular el uso y gestión de llaves?

☐ Deficiente
☐ Poco efectivo
☐ Regular
☐ Efectivo
☐ Excelente

7. ¿Considera que un sistema de seguridad basado en dispositivos inteligentes podría mejorar la seguridad del pabellón?

☐ Sí
☐ No
☐ No sabe / No tiene opinión

8. ¿Qué tan cómodo/a se sentiría usando identificación biométrica (huella, rostro) para acceder a ambientes con acceso autorizado?

☐ Muy incómodo/a
☐ Incómodo/a
☐ Neutral
☐ Cómodo/a
☐ Muy cómodo/a

9. ¿En qué ambientes del pabellón considera que debería implementarse un sistema de control de acceso (por ejemplo, con huellas digitales, reconocimiento facial, etc.)?

(Puede marcar más de una opción)

☐ Aulas (salones de clases)
☐ Laboratorios (ambientes con equipos especializados)
☐ Oficinas administrativas (dirección, coordinación, etc.)
☐ Entrada principal del pabellón
☐ Otros (especifique): ……

10. ¿Qué componentes considera más importantes para incluir en un nuevo sistema de seguridad?

(Marque todas las opciones que considere relevantes)

☐ Cámaras de videovigilancia
☐ Control electrónico de accesos (biometría)
☐ Alarmas inteligentes (contra intrusos)
☐ Personal de seguridad
☐ Otros: ……

11. ¿Cuál es su nivel de preocupación respecto a la privacidad de sus datos personales al interactuar con sistemas de videovigilancia o control de acceso?

☐ Ninguna preocupación
☐ Poca preocupación
☐ Preocupación moderada
☐ Alta preocupación
☐ Preocupación extrema

12. ¿Qué nivel de confianza le genera la forma en que se gestiona sus datos personales recopilados mediante los sistemas de seguridad en general, en cuanto a su recolección, uso, almacenamiento y protección?"

☐ Confianza total
☐ Confianza parcial
☐ Indiferente / Sin opinión
☐ Desconfianza parcial
☐ Desconfianza total

13. ¿Desea agregar algún comentario, sugerencia o recomendación relacionada con la seguridad del pabellón? (Opcional)

……
……
……
……
……

Anexo B: Matriz de operacionalización de variables

Tabla 7.1: *Matriz de operacionalización*

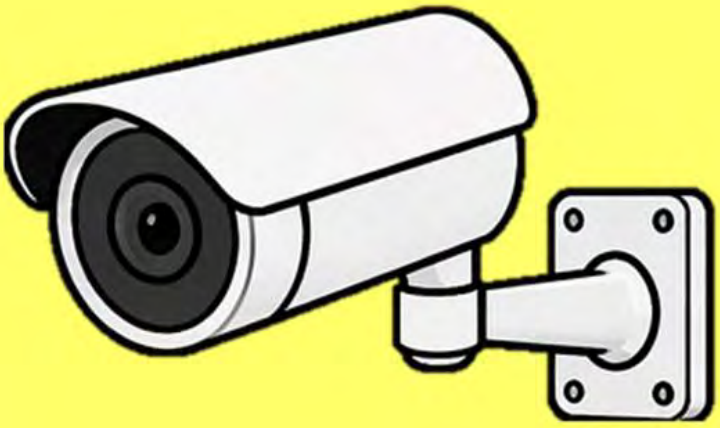
Variable	**Dimensión**	**Indicador**	**Ítem de encuesta**
Percepción actual de seguridad	Nivel percibido de seguridad	Calificación de la seguridad del pabellón	Pregunta 1
	Experiencia personal	Incidentes de seguridad vividos o presenciados	Pregunta 2
	Conocimiento de incidentes	Información de ingresos no autorizados	Pregunta 3
	Áreas vulnerables	Áreas percibidas como más inseguras	Pregunta 4:

Variable	**Dimensión**	**Indicador**	**Ítem de encuesta**
	Conocimiento de sistemas existentes	Conocimiento de existencia de sistemas de seguridad actuales	Pregunta 5
	Percepción de efectividad	Evaluación de la efectividad de los sistemas actuales	Pregunta 5 segunda parte
	Suficiencia de control de acceso	Satisfacción con los mecanismos actuales de control de acceso	Pregunta 6
Aceptación de un sistema de seguridad inteligente (IoT)	Valoración sobre la tecnología	Percepción de mejora con dispositivos inteligentes	Pregunta 7
	Aceptación de la biometría	Nivel de comodidad con el uso de identificación biométrica	Pregunta 8
	Áreas prioritarias de control	Ambientes críticos donde se debería implementar el sistema	Pregunta 9

Variable	**Dimensión**	**Indicador**	**Ítem de encuesta**
	Componentes deseados del sistema	Preferencia por tecnologías específicas	Pregunta 10
	Percepción de privacidad	Nivel de preocupación sobre la privacidad de los datos personales	Pregunta 11
	Confianza en la gestión de datos personales	Confianza en la gestión de los datos personales por los sistemas de seguridad	Pregunta 12
Información adicional cualitativa	Comentarios y sugerencias	Observaciones cualitativas del encuestado	Pregunta 13

Anexo C: Cartel Informativo

ZONA VIDEOVIGILADA



LEY DE PROTECCIÓN DE DATOS PERSONALES - Ley N° 29733

PUEDE EJERCITAR SUS DERECHOS ANTE:

TITULAR DEL BANCO DE DATOS Y DIRECCIÓN

LUGAR DÓNDE PUEDE OBTENER LA INFORMACIÓN CONTENIDA EN EL ARTÍCULO 18 DE LA LPDP

Anexo D: Carteles Adicionales

CONTROL DE ACCESO

BIOMÉTRICO

AUTORIZACIÓN DE INGRESO:
El ingreso a este laboratorio requiere validación obligatoria de identidad mediante huella dactilar o tarjeta.

- Todo acceso lícito queda registrado en la bitácora del sistema.
- El ingreso no autorizado o intento de sabotaje reportará una alerta inmediata al Centro de Monitoreo del Pabellón.

PROTECCIÓN DE DATOS:
Sus características biométricas se procesan únicamente para fines de autenticación local e intransferible.

PULSE PARA SALIR

[NOTA OPERATIVA]

Presione el pulsador para liberar el seguro magnético de la puerta. La cerradura se abrirá durante.

Anexo E: Revisión Encuesta

Cusco, 13 de Mayo del 2025

Dr. Edwin Carrasco Poblete
Escuela Profesional de Ingeniería Informática y de Sistemas

Asunto: Solicito revisión de cuestionario

Por medio de la presente, me dirijo a usted para solicitarle de manera cordial su apoyo en **la revisión del cuestionario que he elaborado como parte del proyecto de tesis** titulado "Diseño de un Sistema Integrado de Seguridad Electrónica Basado en IoT para el Pabellón de Ingeniería Informática y de Sistemas de la UNSAAC".

Agradeceré mucho que pueda brindarme sus observaciones, recomendaciones o ajustes que considere necesarios para optimizar la claridad, relevancia y estructura de las preguntas.

Quedo a su disposición para cualquier aclaración adicional que requiera.

Agradezco de antemano su tiempo y disposición para apoyarme en este proceso.

Adjunto:

1. Matriz de Operacionalización de Variables.

2.Cuestionario.

3. Formato de revisión.

Atentamente,

Roxana Hermoza Cusi
DNI: 47993578

FORMATO DE REVISION DEL CUESTIONARIO

NOMBRE DEL INSTRUMENTO:	**Cuestionario sobre la seguridad en el pabellón de IIS**
FINALIDAD DEL CUESTIONARIO:	**Recolectar información sobre la situación actual de la seguridad en el pabellón, conocer la percepción de los usuarios respecto a las condiciones de seguridad existentes, y registrar cualquier incidente o problema relacionado con la seguridad que haya ocurrido, con el fin de identificar necesidades de mejora.**
TÍTULO DE LA TESIS:	**"Diseño de un sistema integrado de seguridad electrónica basado en tecnologías IoT para el pabellón de Ingeniería Informática y de Sistemas de la UNSAAC"**
Bachiller: Roxana Hermoza Cusi Código: 111180 **Asesor: Dr. Rony Villafuerte Serna**	
DATOS DEL REVISOR:	EDWIN CARRASCO POBLETE
CARGO / ROL:	DOCENTE

CONCLUSIONES Y SUGERENCIAS:

1) Incluir opciones razonables en cada pregunta v.g. preg. 01
2) Preg 05 - considerar personal de seg.
3) Preg 06 - mejorar escala de respuestas
4) Preg 08 - ———"———
5) Preg 10 - Discriminar procesos de dispositivos
6) Considerar aspectos de privacidad en encuesta.

FIRMA:

Cusco, 13 de Mayo del 2025

Dr. Dennis Iván Candia Oviedo
Director del departamento académico
Escuela Profesional de Ingeniería Informática y de Sistemas

Asunto: Solicito revisión de cuestionario

Por medio de la presente, me dirijo a usted para solicitarle de manera cordial su apoyo **en la revisión del cuestionario que he elaborado como parte del proyecto de tesis** titulado "Diseño de un Sistema Integrado de Seguridad Electrónica Basado en IoT para el Pabellón de Ingeniería Informática y de Sistemas de la UNSAAC".

Agradeceré mucho que pueda brindarme sus observaciones, recomendaciones o ajustes que considere necesarios para optimizar la claridad, relevancia y estructura de las preguntas.

Quedo a su disposición para cualquier aclaración adicional que requiera.

Agradezco de antemano su tiempo y disposición para apoyarme en este proceso.

Adjunto:

1. Matriz de Operacionalización de Variables.

2.Cuestionario.

3. Formato de revisión.

Atentamente,

Roxana Hermoza Cusi
DNI: 47993578

FORMATO DE REVISION DEL CUESTIONARIO

NOMBRE DEL INSTRUMENTO:	**Cuestionario sobre la seguridad en el pabellón de IIS**
FINALIDAD DEL CUESTIONARIO:	**Recolectar información sobre la situación actual de la seguridad en el pabellón, conocer la percepción de los usuarios respecto a las condiciones de seguridad existentes, y registrar cualquier incidente o problema relacionado con la seguridad que haya ocurrido, con el fin de identificar necesidades de mejora.**
TÍTULO DE LA TESIS:	**"Diseño de un sistema integrado de seguridad electrónica basado en tecnologías IoT para el pabellón de Ingeniería Informática y de Sistemas de la UNSAAC"**

Bachiller: Roxana Hermoza Cusi Código: 111180
Asesor: Dr. Rony Villafuerte Serna

DATOS DEL REVISOR:	Dennis J. Condio
CARGO / ROL:	Director de Dpto.

CONCLUSIONES Y SUGERENCIAS:

Los indicados de manera verbal.
/ Limitar a 2 variables (Dep. e Indepnd.)

FIRMA:

Términos de Referencia (TDR)

1. Denominación de la Contratación

Contratación de servicios especializados para el suministro, instalación, configuración, integración y puesta en marcha del **Sistema Integrado de Videooperación, Control de Acceso Biométrico y Alarma de Intrusión** para el Pabellón de la Escuela Profesional de Ingeniería Informática y de Sistemas de la Universidad Nacional de San Antonio Abad del Cusco (UNSAAC).

2. Finalidad Pública

La presente contratación busca mitigar las vulnerabilidades físicas críticas identificadas en la infraestructura del pabellón, salvaguardando la integridad de los activos tecnológicos de los laboratorios y garantizando un entorno seguro para la comunidad universitaria. Esto se logrará mediante la implementación de una solución de ingeniería centralizada que optimice los recursos de red y cumpla estrictamente con el marco legal peruano de protección de la privacidad.

3. Objetivos de la Contratación

- **Objetivo General:** Implementar un sistema integrado de seguridad electrónica y videovigilancia unificado en un centro de monitoreo local dentro del pabellón de la Escuela Profesional de Ingeniería Informática y de Sistemas - UNSAAC.

- **Objetivos Específicos:**

  - Desplegar la infraestructura de campo (cámaras IP de alta resolución, lectoras biométricas, sensores analógicos/digitales y cableado estructurado) conforme al análisis de cobertura de los niveles del pabellón.
  - Equipar y configurar el Centro de Monitoreo optimizando el hardware para la decodificación y almacenamiento masivo de flujos de video.
  - Configurar las políticas de seguridad de la información y tratamiento de datos personales de acuerdo a la normativa nacional vigente.

4. Alcance y Características Técnicas del Servicio

El contratista será responsable del suministro completo, instalación y configuración de los siguientes componentes, los cuales interactúan bajo el modelo conceptual de la solución:

A. Subsistema de Videovigilancia (CCTV IP)

- Instalación de cámaras IP distribuidas estratégicamente (cobertura en pasadizos, accesos principales, laboratorios y áreas críticas de los niveles 3 y 4 del pabellón).
- Configuración de flujos de video optimizados (códecs de compresión H.265 o equivalentes) para garantizar que el consumo de ancho de banda y el almacenamiento en el servidor principal se alineen con los cálculos de ingeniería del proyecto.
- Configuración de máscaras de privacidad en zonas que puedan vulnerar el derecho a la intimidad de los usuarios dentro de las instalaciones universitarias.

B. Subsistema de Control de Acceso Biométrico

- Suministro e instalación de terminales de lectura biométrica en los puntos de control definidos (laboratorios especializados y áreas administrativas).

- Integración de los dispositivos a cerraduras electromecánicas y cableado de señales de estado de puerta.

- Configuración de la base de datos centralizada de usuarios en estricto cumplimiento de la **Ley N.° 29733 (Ley de Protección de Datos Personales en el Perú)**, asegurando que los datos biométricos (huellas, facciones) sean cifrados y tratados únicamente bajo consentimiento expreso.

C. Subsistema de Alarma e Intrusión

- Despliegue de paneles de alarma, sensores de movimiento (PIR), y sirenas de alta potencia.

- Vinculación lógica de las alertas de intrusión con el sistema de video, de modo que ante un evento de alarma se genere un encuadre automático (pop-up) en las estaciones de monitoreo.

D. Equipamiento del Centro de Monitoreo

- **Servidores y Almacenamiento:** Configuración del servidor de grabación con arreglos de discos (RAID) calculados para el almacenamiento continuo de las filmaciones por el tiempo mínimo que exija la ley.

- **Estaciones de Trabajo (Workstations):** Configuración del hardware de procesamiento (CPU y GPU dedicada) para la gestión fluida del software de gestión unificada (VMS), garantizando la visualización en tiempo real en la matriz de monitores instalada.

5. Cumplimiento Normativo y Seguridad de la Información

Debido a la naturaleza de los datos capturados por el sistema (imágenes de video y plantillas biométricas), el contratista está obligado a:

- Implementar mecanismos técnicos que garanticen el ejercicio de los **Derechos ARCO** (Acceso, Rectificación, Cancelación y Oposición) por parte de los usuarios.
- Configurar perfiles de usuario con contraseñas seguras y niveles de acceso restringidos para el personal de operaciones, asegurando la confidencialidad de las grabaciones.
- Entregar los formatos y plantillas de consentimiento informado que la universidad utilizará para el tratamiento legítimo de los datos personales recopilados.

6. Perfil del Proveedor y Personal Técnico

- **Del Proveedor:** Persona jurídica especializada en la integración de sistemas de seguridad electrónica, redes de datos o telecomunicaciones, con experiencia comprobada en proyectos similares en el sector público o privado.
- **Del Personal Técnico:** El equipo asignado en campo debe contar con ingenieros de sistemas, electrónica o redes certificados formalmente por las marcas de los fabricantes del software y hardware de red propuesto.

7. Plazo y Lugar de Ejecución

- **Lugar:** Pabellón de la Escuela Profesional de Ingeniería Informática y de Sistemas de la UNSAAC, Ciudad Universitaria de Perayoc, Cusco.
- **Plazo:** El plazo total para la ejecución e integración de todo el sistema será de [indicar número, ej. 60 o 90] días calendario, computados a partir del día siguiente de la firma del contrato formal.

8. Entregables e Hitos de Pago

El servicio se dividirá en tres (03) entregables obligatorios sujetos a la conformidad del área técnica correspondientes a la universidad:

- **Entregables 1 (Plan e Ingeniería de Detalle):** Presentación del plan de trabajo definitivo, cronograma gantt detallado y diagramas físicos finales de canalización y ubicación de equipos en planos actualizados.
- **Entregable 2 (Instalación Física de Campo):** Despliegue completo del cableado estructurado, canaletas, tuberías, instalación física de cámaras, lectoras biométricas, sensores, y el montaje de los racks e infraestructura en el Centro de Monitoreo.
- **Entregable 3 (Configuración, Pruebas y Cierre):** Sistema completamente integrado y operativo en el software de gestión. Se incluirán las pruebas de conectividad y estrés de ancho de banda, configuración de políticas de privacidad, entrega de manuales técnicos, planos y capacitación técnica al personal operador designado por la UNSAAC.