TESIS UANCV
VICERRECTORADO DE INVESTIGACIÓN
"OFICINA DE INVESTIGACIÓN"

UNIVERSIDAD ANDINA

NÉSTOR CÁCERES VELÁSQUEZ

FACULTAD DE INGENIERÍA DE SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE SISTEMAS DE INTELIGENCIA ARTIFICIAL PARA LA SEGURIDAD CIBERNÉTICA EN LA CORTE SUPERIOR DE JUSTICIA DE PUNO 2024

TESIS PRESENTADA POR:

Bach. GERSON JOSE PINEDA LAZARINOS

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

JULIACA - PERÚ

2026

OFICINA DE INVESTIGACIÓN
Tesis Publicada con autorización del autor
http://repositorio.uancv.edu.pe/

TESIS UANCV

VICERRECTORADO DE INVESTIGACIÓN
"OFICINA DE INVESTIGACIÓN"

UNIVERSIDAD ANDINA

NÉSTOR CÁCERES VELÁSQUEZ

FACULTAD DE INGENIERÍA DE SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE SISTEMAS DE INTELIGENCIA ARTIFICIAL PARA LA SEGURIDAD CIBERNÉTICA EN LA CORTE SUPERIOR DE JUSTICIA DE PUNO 2024

TESIS PRESENTADA POR:

Bach. GERSON JOSE PINEDA LAZARINOS

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

APROBADA POR EL JURADO REVISOR:

PRESIDENTE : M. Sc. JUAN CARLOS HERRERA MIRANDA

PRIMER MIEMBRO : MSc. JESUS ESTEBAN CASTILLO MACHACA

SEGUNDO MIEMBRO : Ing. ADWAR RANULFO SANCHEZ CARREON

ASESOR DE TESIS : Dr. PAUL MAMANI TISNADO

LÍNEA DE INVESTIGACIÓN: CIENCIA DE LOS ORDENADORES – P24

OFICINA DE INVESTIGACIÓN
Tesis Publicada con autorización del autor
http://repositorio.uancv.edu.pe/

TESIS UANCV
VICERRECTORADO DE INVESTIGACIÓN
"OFICINA DE INVESTIGACIÓN"

RESOLUCIÓN DECANAL Nº 089-2026-D-FIS-UANCV

Juliaca, 29 de enero de 2026

VISTOS; el Expediente Nº 2026-CU-0002729, presentado por el señor (a) **PINEDA LAZARINOS GERSON JOSE**, egresado de la Escuela Profesional de **INGENIERÍA DE SISTEMAS**, de la Facultad de Ingeniería de Sistemas, quien solicita **NOMINACIÓN DE JURADOS Y PROGRAMACIÓN DE FECHA Y HORA DE SUSTENTACIÒN.**

CONSIDERANDO:

Que, el (la) Bachiller **PINEDA LAZARINOS GERSON JOSE**, quien solicita **NOMINACIÓN DE JURADOS Y PROGRAMACIÓN DE FECHA Y HORA DE SUSTENTACIÓN** de la tesis titulada: **IMPLEMENTACIÓN DE SISTEMAS DE INTELIGENCIA ARTIFICIAL PARA LA SEGURIDAD CIBERNÉTICA EN LA CORTE SUPERIOR DE JUSTICIA DE PUNO 2024,** la misma que pertenece a la línea de investigación, **CIENCIAS DE LOS ORDENADORES**, para optar el título profesional de **INGENIERO DE SISTEMAS.**

Que, al haberse cumplido con los requisitos exigidos por el Reglamento Interno de Trabajo de Investigación conducente a Grados y Títulos mediante resolución 0294-2023-UANCV-CU-R y en concordancia con el dictamen de similitud.

De conformidad al Reglamento Interno de Trabajos de Investigación conducente a grados y títulos, aprobado con resolución Nº 0294-2023-UANCV-CU-R y en mérito al art. 24, Art. 28 del reglamento, con fines de obtención de obtención de Grados Académicos y Títulos Profesionales y en uso a las atribuciones que le concede la ley Universitaria Nº 30220, Ley de creación de la UANCV Nº 23738 y modificatoria Nº 24661, y el estatuto de la UANCV, el Decano y Director de la Unidad de Investigación de la Facultad de Ingeniería de Sistemas.

RESUELVE:

ARTÍCULO PRIMERO. - APROBAR la **NOMINACION DE JURADOS**, integrado por los siguientes docentes:

Presidente	: **Dr. JUAN CARLOS HERRERA MIRANDA**
1er miembro	: **M.Sc. JESUS ESTEBAN CASTILLO MACHACA**
2do miembro	: **Ing. ADWAR RANULFO SANCHEZ CARREON**

ARTÍCULO SEGUNDO.- RECONOCER como asesor de la investigación (tesis) de la Facultad de Ingeniería de Sistemas, al (a la) docente, **Dr. Paul Mamani Tisnado**

ARTÍCULO TERCERO.- APROBAR la **FECHA Y HORA DE SUSTENTACION DE LA TESIS** del (la) Bachiller: **PINEDA LAZARINOS GERSON JOSE**, del informe final de la investigación (tesis) titulado: **DISEÑO DE UNA PLATAFORMA DE PAGOS Y NOTIFICACIONES OMNICANAL INTEGRA A LA GESTIÓN TRIBUTARIA MUNICIPAL DE PUCARÁ 2025**, para optar el título profesional de **INGENIERO DE SISTEMAS**, de acuerdo al siguiente detalle:

FECHA : Jueves, 29 de enero de 2026
HORA : 13:30 p.m.
LUGAR : Sala de Docentes-FIS

ARTÍCULO CUARTO. - DISPONER que, la Unidad de Investigación, Responsables del Comité de Investigación de la Facultad de Ingeniería de Sistemas y el Director de la Escuela profesional, **INGENIERÍA DE SISTEMAS**, quedan encargados del cumplimiento de la presente Resolución.

Regístrese, Comuníquese y Archívese.

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ" - FACULTAD DE INGENIERÍA DE SISTEMAS - JULIACA - DECANO

UNIVERSIDAD ANDINA
"NÉSTOR CÁCERES VELÁSQUEZ"

Dr. Juan Carlos Herrera Miranda
DECANO

C.c.
Arch 2026
interesado
J.C.H.M./

OFICINA DE INVESTIGACIÓN
Tesis Publicada con autorización del autor
http://repositorio.uancv.edu.pe/

TESIS UANCV

RESOLUCIÓN Nº 053-2025-UI.R-D-FIS-UANCV-J

Juliaca, 13 de Junio de 2025

VISTOS:

El Expediente: 2025-006539 de fecha 03 de Junio de 2025, del Bach. **GERSON JOSE PINEDA LAZARINOS**, quien solicita Revisión del Informe Final de la Investigación (borrador de Tesis) y el Anexo (04 o 05) "Ficha de Opinión del Informe Final de la Investigación (borrador de Tesis)" que fue revisada por el Comité de Investigación de la Facultad de Ingeniería de Sistemas, Escuela Profesional de INGENIERÍA DE SISTEMAS.

CONSIDERANDO:

Que, las Unidades de Investigación son unidades académicas que agrupan a docentes y estudiantes de diversas disciplinas, en razón del desarrollo de investigación científica, tecnológica y humanista de acuerdo al Estatuto Universitario Modificado 2020 de nuestra primera Casa Superior de Estudios.

Que, el (la) Bach. GERSON JOSE PINEDA LAZARINOS, quien solicita la revisión del Informe Final de la Investigación (borrador de Tesis) del tema titulada: IMPLEMENTACIÓN DE SISTEMAS DE INTELIGENCIA ARTIFICIAL PARA LA SEGURIDAD CIBERNÉTICA EN LA CORTE SUPERIOR DE JUSTICIA DE PUNO 2024, conducente para optar el Título profesional de INGENIERO DE SISTEMAS.

Que, al haberse cumplido con los requisitos exigidos por el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos plasmado en la Resolución Nº 0294-2023-UANCV-CU-R.

Que, el Comité de Investigación emitió su opinión favorable al Informe Final de la Investigación (borrador de Tesis).

Que, el Director de la Unidad de Investigación de la Facultad de Ingeniería de Sistemas, Escuela Profesional de INGENIERÍA DE SISTEMAS, corroboro el asesoramiento en el Informe Final de la Investigación (borrador de Tesis) del ASESOR Dr. PAUL MAMANI TISNADO,

Estando, la opinión favorable del Comité de Investigación, en concordancia con el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos Resolución Nº 0294-2023-UANCV-CU-R, de conformidad a lo que establece la Ley Universitaria Nº 30220, Ley de Creación de la UANCV Nº 23738 y Modificatoria Nº 24661 y el Estatuto de la UANCV, que confiere facultades al Decano de la Facultad de Ingeniería de Sistemas.

SE RESUELVE:

ARTICULO PRIMERO. - APROBAR Y AUTORIZAR EL INFORME FINAL DE LA INVESTIGACIÓN (Borrador de Tesis) para la **REVISIÓN DE SIMILITUD TURNITIN**, del tema titulado: **IMPLEMENTACIÓN DE SISTEMAS DE INTELIGENCIA ARTIFICIAL PARA LA SEGURIDAD CIBERNÉTICA EN LA CORTE SUPERIOR DE JUSTICIA DE PUNO 2024**, presentado por el (la) Bach. **GERSON JOSE PINEDA LAZARINOS**, para optar el Título Profesional de INGENIERO DE SISTEMAS, en virtud de los considerandos expuestos.

ARTICULO SEGUNDO. - RATIFICAR, como ASESOR al **Dr. PAUL MAMANI TISNADO.**

ARTICULO TERCERO. - DISPONER que la facultad, secretarias académicas y administrativas, quedan encargados del cumplimiento de la presente resolución.

Regístrese, comuníquese y archívese.

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ"
FACULTAD DE INGENIERÍA DE SISTEMAS - JULIACA

Dr. Juan Carlos Herrera Miranda
DECANO

C.c
Arch 2025
JCHM/ v1.2
Distribución: Asesor de Tesis, Interesado

OFICINA DE INVESTIGACIÓN
Tesis Publicada con autorización del autor
http://repositorio.uancv.edu.pe/

TESIS UANCV

"Año de la recuperación y consolidación de la economía peruana"

RESOLUCIÓN N° 043-2025-UI.P-D-FIS-UANCV-J

Juliaca, 13 de mayo de 2025

VISTOS:

El Expediente: 2025-005530 de fecha 09 de mayo de 2025, del (la) Bach. **GERSON JOSE PINEDA LAZARINOS**; con el cual solicita Revisión de la Propuesta de Investigación y el Anexo (02 o 03) "Ficha de Opinión de la Propuesta de Investigación" que fue revisada por el Comité de Investigación de la Facultad de Ingeniería de Sistemas, Escuela Profesional de INGENIERÍA DE SISTEMAS.

CONSIDERANDO:

Que, las Unidades de Investigación son unidades académicas que agrupan a docentes y estudiantes de diversas disciplinas, en razón del desarrollo de investigación científica, tecnológica y humanista de acuerdo al Estatuto Universitario Modificado 2020 de nuestra primera Casa Superior de Estudios.

Que, el (la) Bach. GERSON JOSE PINEDA LAZARINOS, solicito la revisión y aprobación de la Propuesta de Investigación de la tesis titulada: IMPLEMENTACIÓN DE SISTEMAS DE INTELIGENCIA ARTIFICIAL PARA LA SEGURIDAD CIBERNÉTICA EN LA CORTE SUPERIOR DE JUSTICIA DE PUNO 2024; conducente para optar el Título Profesional de INGENIERO DE SISTEMAS.

Que, al haberse cumplido con los requisitos exigidos por el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos plasmado en la Resolución N° 0294-2023-UANCV-CU-R.

Que, el Comité de Investigación ha emitido opinión favorable a la propuesta de investigación.

Que, el Director de la Unidad de Investigación de la Facultad de Ingeniería de Sistemas, Escuela Profesional de INGENIERÍA DE SISTEMAS, ratificó la propuesta del Asesor Dr. PAUL MAMANI TISNADO, quien debe estar acreditado y facultado para orientar y ayudar al asesorado en el proceso de elaboración del trabajo de investigación (Tesis).

Estando, la opinión favorable del comité de Investigación, en concordancia con el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos, Resolución N° 0294-2023-UANCV-CU-R, de conformidad a lo que establece la Ley Universitaria N° 30220, Ley de Creación de la UANCV N° 23738 y Modificatoria N° 24661 y el Estatuto de la UANCV, que confiere facultades al Decano de la Facultad de Ingeniería de Sistemas.

SE RESUELVE:

ARTÍCULO PRIMERO. - **APROBAR Y AUTORIZAR** LA EJECUCIÓN DE LA PROPUESTA DE INVESTIGACIÓN, titulada: **IMPLEMENTACIÓN DE SISTEMAS DE INTELIGENCIA ARTIFICIAL PARA LA SEGURIDAD CIBERNÉTICA EN LA CORTE SUPERIOR DE JUSTICIA DE PUNO 2024**, presentado por el (la) Bach. **GERSON JOSE PINEDA LAZARINOS**, para optar el Título Profesional de INGENIERO DE SISTEMAS, en virtud de los considerandos expuestos.

ARTÍCULO SEGUNDO. - RECONOCER, como ASESOR al Dr. **PAUL MAMANI TISNADO**.

ARTÍCULO TERCERO. - DISPONER que la facultad, secretarias académicas y administrativas, quedan encargados del cumplimiento de la presente resolución.

Regístrese, comuníquese y archívese.

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ"
FACULTAD DE INGENIERÍA DE SISTEMAS
DECANO

Dr. Juan Carlos Herrera Miranda
DECANO

C.c
Arch 2025
JCHM/ v1.2
Distribución: Asesor de Tesis, Interesado

OFICINA DE INVESTIGACIÓN
Tesis Publicada con autorización del autor
http://repositorio.uancv.edu.pe/

TESIS UANCV
VICERRECTORADO DE INVESTIGACIÓN
"OFICINA DE INVESTIGACIÓN"

GERSON JOSE PINEDA LAZARINOS

IMPLEMENTACIÓN DE SISTEMAS DE INTELIGENCIA ARTIFICIAL PARA LA SEGURIDAD CIBERNÉTICA EN LA CORT...

Trabajos de tesis para ingreso a repositorio

Detalles del documento

Identificador de la entrega
trn:oid:::13016:605360670

Fecha de entrega
7 jul 2026, 11:55 GMT-5

Fecha de descarga
7 jul 2026, 14:11 GMT-5

Nombre del archivo
T036_72288939_T.docx

Tamaño del archivo
9.2 MB

100 páginas

15.562 palabras

88.111 caracteres

OFICINA DE INVESTIGACIÓN
Tesis Publicada con autorización del autor
http://repositorio.uancv.edu.pe/

17% Similitud general

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

Filtrado desde el informe

- Bibliografía
- Coincidencias menores (menos de 10 palabras)

Fuentes principales

12% Fuentes de Internet
5% Publicaciones
15% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

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.

OFICINA DE INVESTIGACIÓN
Tesis Publicada con autorización del autor
http://repositorio.uancv.edu.pe/

Metadatos complementarios

Título de la Tesis	
IMPLEMENTACIÓN DE SISTEMAS DE INTELIGENCIA ARTIFICIAL PARA LA SEGURIDAD CIBERNÉTICA EN LA CORTE SUPERIOR DE JUSTICIA DE PUNO 2024	
Datos de autor	
Nombres y apellidos	GERSON JOSE PINEDA LAZARINOS
Tipo de documento de identidad	DNI
Número de documento de identidad	72288939
URL de ORCID	https://009-0006-2731-8838
Datos de asesor	
Nombres y apellidos	PAUL MAMANI TISNADO
Tipo de documento de identidad	DNI
Número de documento de identidad	01314987
URL de ORCID	https://orcid.org/0000-0002-0287-7143
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	JUAN CARLOS HERRERA MIRANDA
Tipo de documento	DNI
Número de documento de identidad	29606930
Miembro del jurado 1	
Nombres y apellidos	JESUS ESTEBAN CASTILLO MACHACA
Tipo de documento	DNI
Número de documento de identidad	01323821
Miembro del jurado 2	
Nombres y apellidos	ADWAR RANULFO SANCHEZ CARREON
Tipo de documento	DNI
Número de documento de identidad	02064066

Datos de investigación	
Línea de investigación	Ciencia de Ordenadores - P25
Grupo de investigación	No aplica.
Agencia de financiamiento	Sin financiamiento.
Ubicación geográfica de la investigación	**País**: Perú **Departamento**: Puno **Provincia**: Puno **Distrito**: Puno CORTE SUPERIOR DE JUSTICIA DE PUNO **Coordenadas:** **Latitud:** - -15.840662 **Longitud:** - 70.027847 **URL Maps:** https://maps.app.goo.gl/F3WoSuEbhBtkif9q6 
Año o rango de años en que se realizó la investigación	Mayo 2025 – Enero 2026
URL de disciplinas OCDE https://concytec-pe.github.io/Peru-CRIS/vocabularios/ocde_ford.html - Librería	**Ingeniería de sistemas y comunicaciones** https://purl.org/pe-repo/ocde/ford#2.02.04 **Ingeniería de procesos** https://purl.org/pe-repo/ocde/ford#2.04.02

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ"
Dr. Juan Carlos Herrera Miranda
DIRECTOR (e)
Unidad de Investigación FIS

TESIS UANCV
VICERRECTORADO DE INVESTIGACIÓN
"OFICINA DE INVESTIGACIÓN"

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo GERSON JOSE PINEDA LAZARINOS, identificado con DNI Nro. 72288939, en mi condición de egresado de:

☒ **Escuela Profesional**

☐ **Programa de Segunda Especialidad,**

☐ **Programa de Maestría o Doctorado**

INGENIERÍA DE SISTEMAS

informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación,** ☐ **Trabajo Académico** denominada:

IMPLEMENTACIÓN DE SISTEMAS DE INTELIGENCIA ARTIFICIAL PARA LA SEGURIDAD CIBERNÉTICA EN LA CORTE SUPERIOR DE JUSTICIA DE PUNO 2024

Asesorado por: Dr. PAUL MAMANI TISNADO

Es un tema original.

Declaro que el presente trabajo de tesis es elaborado por mi persona y **no existe plagio/copia** de ninguna naturaleza, en especial de otro documento de investigación (tesis, revista, texto, congreso, o similar) presentado por persona natural o jurídica alguna ante instituciones académicas, profesionales, de investigación o similares, en el país o en el extranjero.

Dejo constancia que las citas de otros autores han sido debidamente identificadas en el trabajo de investigación, por lo que no asumiré como suyas las opiniones vertidas por terceros, ya sea de fuentes encontradas en medios escritos, digitales o Internet.

Asimismo, ratifico que soy plenamente consciente de todo el contenido de la tesis y asumo la responsabilidad de cualquier error u omisión en el documento, así como de las connotaciones éticas y legales involucradas.

El incumplimiento de lo declarado da lugar a responsabilidad del declarante, en consecuencia; a través del presente documento asumo frente a terceros, la Universidad Andina Néstor Cáceres Velásquez y/o la Administración Pública toda responsabilidad que pueda derivarse por el trabajo final presentado. Lo señalado incluye responsabilidad pecuniaria incluido el pago de multas u otros por los daños y perjuicios que se ocasionen.

Juliaca 17 de JUNIO del 2026

Firma del Asesor (obligatoria)	Firma del Estudiante (obligatoria)	Huella

OFICINA DE INVESTIGACIÓN
Tesis Publicada con autorización del autor
http://repositorio.uancv.edu.pe/

ÍNDICE

ÍNDICE i

ÍNDICE DE TABLAS v

ÍNDICE DE FIGURAS vi

RESUMEN vii

ABSTRACT viii

INTRODUCCIÓN ix

CAPÍTULO I

ASPECTOS GENERALES

1.1. Descripción del problema 12

1.1.1 A nivel Internacional 12

1.1.2 A nivel nacional 13

1.1.3 A nivel local 13

1.2. Formulación del problema 14

1.2.1 Problema Principal 14

1.2.2 Problemas específicos 14

1.3. Justificación de la investigación 14

1.3.1 Justificación Teórica 14

1.3.2 Justificación Practico 15

1.3.3 Justificación Metodológica 16

1.4. Objetivos 17

1.4.1 Objetivo General 17

1.4.2 Objetivos Específicos 17

1.5. Importancia y alcance 17

1.6. Limitaciones y delimitaciones 18

1.7. Hipótesis 18

1.7.1 Hipótesis General 18

1.7.2 Hipótesis Especificas 19

1.8. Variables e indicadores 19

1.8.1 Conceptualización de las variables 19

1.8.2 Operacionalización de las variables 20

CAPÍTULO II

FUNDAMENTOS TEÓRICOS

2.1. Antecedentes 22

2.1.1 Internacionales. 22

2.1.2 Nacionales 23

2.1.3 Locales 25

2.2. Marco epistemológico 26

2.3. Estado del arte 26

2.4. Bases teóricas 27

2.4.1 Ciberseguridad en el contexto de las organizaciones públicas 27

2.4.2 La Inteligencia Artificial como Herramienta Estratégica 28

2.4.3 Aplicación de la IA en instituciones públicas y judiciales 28

2.4.4 Retos y oportunidades en la implementación de IA en la Corte Superior de Justicia de Puno 29

2.4.5 La Seguridad Cibernética 30

2.4.6 La Seguridad Cibernética y la IA 31

2.5. Marco conceptual 32

CAPÍTULO III

METODOLOGÍA Y RESULTADOS

3.1. Enfoque de la investigación 36

3.2. Métodos aplicados de investigación 36

3.3. Tipo de investigación 37

3.4. Nivel 37

3.5. Diseño 37

3.6. Ámbito de investigación 38

3.7. Población y muestra 39

3.7.1 Población 39

3.7.2 Muestra 39

3.8. Métodos y técnicas de recogida de información 40

3.8.1 Técnicas de investigación 40

3.8.2 Instrumento de investigación 40

3.8.3 Criterios de Inclusión 41

3.8.4 Criterios de Exclusión 41

3.9. Validez y confiabilidad del instrumento de investigación 42

3.9.1 Validación de los instrumentos 42

3.9.2 Confiabilidad de los instrumentos 42

CAPÍTULO IV

RESULTADOS

4.1. Presentación, análisis e interpretación de datos 43

4.2. Discusión de resultados 67

CONCLUSIONES 70

RECOMENDACIONES 72

REFERENCIAS BIBLIOGRÁFICAS 74

APÉNDICES 77

Apéndice 1 Matriz de consistencia 78

Apéndice 2 Instrumentos 79

Apéndice 3 Validez de instrumentos 84

Apéndice 4 Tratamiento de datos 86

ÍNDICE DE TABLAS

Tabla 1 S1: Área de trabajo 44
Tabla 2 S1: Tiempo de servicio en la institución 45
Tabla 3 S2.1: Sistemas se actualizan con parches de seguridad 46
Tabla 4 S2.2: Se cumple política de contraseñas seguras 47
Tabla 5 S2.3: He recibido capacitación sobre riesgos cibernéticos 48
Tabla 6 S2.4: La información sensible está protegida 49
Tabla 7 S2.5: Conocí incidentes de seguridad en últimos 12 meses 50
Tabla 8 S2.6: El equipo técnico responde rápido a fallas 51
Tabla 9 S3.1: Conocimiento sobre IA en ciberseguridad 52
Tabla 10 S3.2a: Prioridad amenaza - Malware/Ransomware 53
Tabla 11 S3.2b: Prioridad amenaza - Análisis de comportamiento 54
Tabla 12 S3.2c: Prioridad amenaza - Monitorización de red 55
Tabla 13 S3.2d: Prioridad amenaza - Clasificación de documentos 56
Tabla 14 S3.2e: Prioridad amenaza - Respuesta automatizada 57
Tabla 15 S3.3: Criterio más importante para seleccionar IA 58
Tabla 16 S4.1: Disposición para capacitarse en el uso de IA 59
Tabla 17 S4.2: Modalidad de capacitación más efectiva 60
Tabla 18 S4.3: Área de mayor dificultad en el uso de IA 61
Tabla 19 S5.1: Indicador éxito - Reducción número de incidentes 62
Tabla 20 S5.2: Indicador éxito - Reducción tiempo de detección 63
Tabla 21 S5.3: Indicador éxito - Reducción tiempo de contención 64
Tabla 22 S5.4: Indicador éxito - Aumento confianza del personal 65
Tabla 23 S5.5: Indicador éxito - Pocas alertas falsas ..... 66.

ÍNDICE DE FIGURAS

Figura 1 Área de trabajo 44
Figura 2 Tiempo de servicio en la institución 45
Figura 3 Sistemas se actualizan con parches de seguridad 46
Figura 4 cumple política de contraseñas seguras 47
Figura 5 He recibido capacitación sobre riesgos cibernéticos 48
Figura 6 La información sensible está protegida 49
Figura 7 Conocí incidentes de seguridad en últimos 12 meses 50
Figura 8 El equipo técnico responde rápido a fallas 51
Figura 9 Conocimiento sobre IA en ciberseguridad 52
Figura 10 Prioridad amenaza - Malware/Ransomware 53
Figura 11 Prioridad amenaza - Análisis de comportamiento 54
Figura 12 Prioridad amenaza - Monitorización de red 55
Figura 13 Prioridad amenaza - Clasificación de documentos 56
Figura 14 Prioridad amenaza - Respuesta automatizada 57
Figura 15 Criterio más importante para seleccionar IA 58
Figura 16 Disposición para capacitarse en el uso de IA 59
Figura 17 Modalidad de capacitación más efectiva 60
Figura 18 Área de mayor dificultad en el uso de IA 61
Figura 19 Indicador éxito - Reducción número de incidentes 62
Figura 20 Indicador éxito - Reducción tiempo de detección 63
Figura 21 Indicador éxito - Reducción tiempo de contención 64
Figura 22 Indicador éxito - Aumento confianza del personal 65
Figura 23 Indicador éxito - Pocas alertas falsas 66

RESUMEN

El propósito de esta investigación es implementar sistemas de inteligencia artificial para mejorar el componente de seguridad cibernética en la Corte Superior de Justicia de Puno en el 2024. Posteriormente de la evaluación del estado actual para descubrir las brechas y vulnerabilidades de los sistemas informáticos, se lleva a cabo un estudio para identificar las soluciones de I A más efectivas para la prevención, detección y respuesta a incidentes automatizados en un entorno judicial. Cabe destacar que la metodología incluye la capacitación del personal operativo y técnico en términos del uso y mantenimiento de estas soluciones. En cuanto a la efectividad, esta se establece mediante la utilización de métricas cuantitativas que incluye la disminución del tiempo para detectar y responder a las amenazas, disminución del número de falsos positivos y nivel de cumplimento del protocolo de seguridad. La metodología utilizada se clasifica como aplicativa con el diseño no experimental y nivel descriptivo-explicativo. La muestra de encuesta incluye 75 empleados y contratistas del departamento vinculado con tecnologías de información y la seguridad de la institución. Las técnicas que se aplican son observación, análisis de documentos y encuestas con el cuestionario validado. Los resultados esperados proporcionan un modelo replicable que fortalece la protección de datos judiciales sensibles y la resiliencia operativa frente a ciberamenazas, contribuyendo a la modernización de la seguridad digital en el Poder Judicial.

Palabras clave: Inteligencia artificial, seguridad cibernética, corte superior de justicia, implementación tecnológica, ciberseguridad judicial, detección de amenazas, capacitación en TI, evaluación de vulnerabilidades.

ABSTRACT

This research aims to implement artificial intelligence (AI) systems to enhance cybersecurity at the Superior Court of Justice of Puno during 2024. Starting with an assessment of the current state to identify vulnerabilities in computer systems, the study investigates and selects the most suitable AI solutions for automated prevention, detection, and response to incidents in a judicial environment. The process includes training technical and operational staff in the use and maintenance of these tools. Finally, the effectiveness of the implementation is evaluated using quantitative metrics such as the reduction in threat detection and response times (MTTD/MTTR), the false positive rate, and the level of compliance with security protocols. The methodology is applied, with a non-experimental design and descriptive-explanatory level, using a sample of 75 personnel from the institution's information technology and security areas. Techniques include direct observation, documentary analysis, and surveys with validated instruments. The expected results provide a replicable model that strengthens the protection of sensitive judicial data and operational resilience against cyber threats, contributing to the modernization of digital security in the Judiciary.

Keywords: Artificial intelligence, cybersecurity, superior court of justice, technology implementation, judicial cybersecurity, threat detection, IT training, vulnerability assessment.

INTRODUCCIÓN

La digitalización de la administración de justicia representa un avance fundamental para la eficiencia y transparencia del sistema judicial. En el Perú, las Cortes Superiores han emprendido un proceso de modernización tecnológica que, si bien optimiza los procesos, las expone a un panorama de ciberamenazas cada vez más sofisticado y frecuente. La Corte Superior de Justicia de Puno, como depositaria de información jurídica sensible, información de datos personales y actuaciones judiciales de alto valor, no puede ser ajeno a esta situación. La seguridad informática que se brinda, por lo tanto, hablamos de un componente esencial de la seguridad jurídica nacional y de la protección de los derechos del acusado.

Tradicionalmente, las defensas cibernéticas han sido operaciones basadas en reglas estáticas y respuestas manuales con ciertas limitaciones evitables contra las amenazas dinámicas que implican ransomware, phishing dirigido o intrusiones persistentes. Dichas amenazas no solo amenazan la integridad de los archivos digitales sino también el desempeño ininterrumpido de los servicios judiciales críticos y la percepción de confianza pública en la institución. Por lo tanto, es crítico adoptar un enfoque preventivo y adaptativo hacia la seguridad. Específicamente, este nivel de protección solo es posible a través de la integridad integral. La IA surge no como una elección futurista sino como una necesidad estratégica. Primero, los sistemas de IA tienen una inteligencia artificial y capacidades de análisis del comportamiento con toda la diferenciación transformacional que implica. En particular, estos sistemas permiten analizar niveles masivos de información de red y archivos de sistemas

de registro para exponer señales de anomalías, que son escurridizas para las herramientas estándar porque son demasiado sutiles. Además, estas herramientas permiten una defensa inmediata secinternaciones para atacantes sin líderes y pronostican los vectores de ataque potenciales transfiriendo las operaciones de reactivas a proactivas.

No obstante, la implementación de tales tecnologías en un entorno judicial particular como Puno no es testra trivial. Supone, más bien, una evaluación diagnóstica rigurosa de la infraestructura y los procesos existentes, una selección crítica de soluciones que cumplan con las regulaciones sobre privacidad y secreto judicial a saber la Ley N° 29733 y la creación de una estrategia de capacitación para empoderar al capital humano. Por lo tanto, esta investigación no se centra en la tecnología sino que ofrece un proceso adecuado para gestionar el cambio tecnológico a dicha propuesta.

" Implementation of Artificial Intelligence Systems for Cybersecurity at Puno Superior Court of Justice 2024" es un estudio que se justifica por la premura de garantizar la información de la Corte a través de tecnologías de vanguardia. Su objetivo general es el de la implementación de los sistemas, lo que mejorará sustantivamente la postura de seguridad de la Corte. Como resultados esperados, "Implementation of Artificial Intelligence Systems for Cybersecurity at Puno Superior Court of Justicia 2024" comprende cuatro objetivos específicos consecutivos: 1)evaluar el nivel actuar y las vulnerabilidades, 2) investigar y seleccionar los sistemas de IA más idóneos, 3) capacitar al personal a usar los sistemas y 4) evaluar la eficiencia de la implementación. De acuerdo a la hipótesis, tal implementación mejorará sustantivamente la seguridad cibernética

reduciendo las vulnerabilidades y aumentando el sistema de prevención, detección y respuesta.

La tesis se estructura en cinco capítulos. El Capítulo I: El Problema. En este se resume la justificación del abordaje, los objetivos y la hipótesis de la investigación. El Capítulo II: Marco Teórico. Para el capítulo se conceptualizan los términos de ciberseguridad, inteligencia artificial y la normativa vigente aplicable al ámbito judicial. El Capítulo III: Metodología. En él se justifica el diseño aplicativo, la población y muestra, así como las técnicas e instrumentos de recolección y análisis de datos. El Capítulo IV: Resultados. En este capítulo se presentan los hallazgos de la evaluación diagnóstica del proceso de selección, capacitación y medición de la efectividad. Finalmente, las Conclusiones y Recomendaciones cierran el acápite resumiendo resultados, verificando hipótesis y proponiendo líneas de acción para la continuación y mejoramiento del sistema implementado.

CAPÍTULO I

ASPECTOS GENERALES

1.1. Descripción del problema

1.1.1 A nivel Internacional

La ciberseguridad ha sido un verdadero desafío para todas las instituciones en todo el mundo, sobre todo, para las instituciones que manejan la información sensible como el sistema judicial. Con la tecnología en aumento, también lo están los riesgos que se enfrentan en línea, poniendo en riesgo la integridad de la información del ciudadano, la privacidad y en general las instituciones. Desde el punto de vista global, muchos gobiernos y entidades están invirtiendo en" intelligent" tecnologías como la inteligencia artificial para proteger sus sus activos críticos. A pesar de ser un campo en desarrollo, el uso de IA en la lucha por la ciberseguridad está atormentando a muchos países como Eglinda. Esto se debe a las deficiencias en términos de recursos, capacidad y regulaciones en esta área para hacer frente a los nuevos retos cibernéticos con eficacia.

1.1.2 A nivel nacional

En el ámbito nacional, el sistema judicial peruano es víctima de crecientes amenazas cibernéticas, que afectan la integridad y la confidencialidad de sus datos. A la fecha, la Corte Superior de Justicia de Puno y otras instituciones judiciales peruanas no tienen a disposición las herramientas y los sistemas necesarios para hacer frente a estos crecientes desafíos. Si bien el gobierno peruano ha intentado reaccionar al problema al reforzar sus políticas de seguridad cibernética, la falta de un marco legal sólido para la ciberseguridad judicial y la carencia de entrenamiento en tecnologías modernas empoderadoras como la inteligencia artificial hacen difícil para estas organizaciones prevenir, detectar y reaccionar ante el riesgo cibernético eficazmente.

1.1.3 A nivel local

A nivel local, la Corte Superior de Justicia de Puno experimenta una amenaza de ataque cibernético, ya que carece de sistemas avanzados de protección de la misma, especialmente por el hecho de que carece de inteligencia artificial o la utiliza de inteligencia dentro del ámbito de la información judicial coloca. Según lo establecido, el sistema informático que se utiliza en la corte no está lo suficientemente protegido de las amenazas cibernéticas modernas, lo que pone los datos de los ciudadanos y sus propios datos en peligro y elimina el proceso de litigio. Por tanto, incluso con la emergencia de necesidades apremiantes, no se está desplegando ningún sistema integral que utilice lo último presente, como el nivel de inteligencia artificial. Como resultado, existe una preocupación profunda por la seguridad de la información crítica y la transparencia y eficiencia de la corte judicial.

1.2. Formulación del problema

1.2.1 Problema Principal

¿Cómo la implementación de sistemas de inteligencia artificial puede mejorar la seguridad cibernética en la Corte Superior de Justicia de Puno durante el año 2024?

1.2.2 Problemas específicos

1. ¿Cuál es el estado actual de la seguridad cibernética en la Corte Superior de Justicia de Puno, y cuáles son las principales vulnerabilidades y riesgos asociados a los sistemas informáticos utilizados?

2. ¿Qué sistemas de inteligencia artificial son más adecuados para la prevención, detección y respuesta ante incidentes de seguridad cibernética en un entorno judicial?

3. ¿Qué métodos y estrategias son necesarios para capacitar al personal de la Corte Superior de Justicia de Puno en el uso y mantenimiento de los sistemas de inteligencia artificial implementados?

4. ¿Cómo se puede evaluar la efectividad de la implementación de los sistemas de inteligencia artificial en la Corte Superior de Justicia de Puno durante el año 2024?

1.3. Justificación de la investigación

1.3.1 Justificación Teórica

La perspectiva única de la teoría del design thinking aplicada a la ciberseguridad, así como de los sistemas de IA avanzados, presenta un nuevo enfoque para comprender y enfrentar los problemas de la protección de datos y

la seguridad en el campo judicial. La perspectiva teórica de esta investigación agrega al currículo de la ciberseguridad judicial un nuevo contexto: las instituciones públicas peruanas, específicamente la corte judicial.

En un escenario donde las amenazas cibernéticas crecen de manera continua, la estrategia de IA funciona como un complemento a las soluciones de seguridad ya implementadas, pero con una respuesta más dinámica y adaptable que se anticipa a la predicción y la automatización. Este enfoque combina conocimientos previos en torno a la ciberseguridad, la inteligencia artificial y la administración pública para entender cómo dos tecnologías emergentes pueden convertirse en soluciones efectivas para proteger los sistemas judiciales de riesgos y vulnerabilidades cibernéticas emergentes..

1.3.2 Justificación Practico

La justificación de la implementación de algoritmos de IA con respecto a la ciberseguridad en la Corte Superior de Justicia de Puno, también, evidentemente, tiene una base práctica. Con la cantidad de información confidencial y sensible con la que trabajan las cortes de justicia a diario, los datos personales, los documentos importantes y los casos judiciales por sí solos requiere el uso de medidas de protección más serias contra las amenazas externas como los ciberataques y las internas como los errores y la negligencia humanos.

En general, el proyecto casi mejorará la eficiencia operativa y en última instancia, la confianza del público al mostrar al público que la Corte está aprovechando las tecnologías más avanzadas para proteger los datos y degradar los riesgos cibernéticos. Además, con la capacitación proporcionada, el personal de la Corte puede operarlos y mantenerlos. Por lo tanto, los jueces

podrían más fácilmente adquirir estos sistemas debido al efecto acumulativo y adoptar apropiadamente técnicas adicionales en su toma de decisiones. Además de mejorar la seguridad, esta implementación también mejorará la imagen de las estructuras públicas, ya que serían más transparentes y más interesantes. Por supuesto, todo esto conducirá a un mejor servicio para la ciudadanía.

1.3.3 Justificación Metodológica

En términos metodológicos, la investigación se centrará en explorar y describir y emplear tanto enfoques cualitativos como cuantitativos para evaluar la situación actual de la ciberseguridad en la Corte Superior de Justicia de Puno y el impacto a partir de la instalación de sistemas A. Basándose en una serie de consultas con expertos, encuestas públicas de empleados de la corte y observaciones directas en sus encargos actuales, la investigación determinará la perspectiva de afrontar criterios de seguridad existentes y sus áreas de deficiencia..

El aspecto de la implementación a través de la inteligencia artificial se abordará desde la perspectiva de un enfoque practico, en el cual se desarrollará un prototipo funcional, el mismo que será sometido a pruebas de funcionamiento y efectividad para posteriormente ser analizado. Dará como resultado el ingreso de datos precisos acerca de la tecnológica a emplearse y el impacto de la misma una vez implementada. Sin embargo, metodológicamente se pretende dar un modelo replicable de implementar la tecnología de inteligencia artificial para el fortalecimiento de la ciberseguridad en las instituciones judiciales, haciendo modelos para otras cortes o instituciones públicas, elevando el nivel de ciberseguridad nacional.

1.4. Objetivos

1.4.1 Objetivo General

Implementar sistemas de inteligencia artificial para mejorar la seguridad cibernética en la Corte Superior de Justicia de Puno en el año 2024.

1.4.2 Objetivos Específicos

1. Evaluar el estado actual de la seguridad cibernética en la Corte Superior de Justicia de Puno, identificando vulnerabilidades y riesgos asociados a los sistemas informáticos utilizados.
2. Investigar y seleccionar los sistemas de inteligencia artificial más adecuados para la prevención, detección y respuesta ante incidentes de seguridad cibernética en entornos judiciales.
3. Capacitar al personal de la Corte Superior de Justicia de Puno en el uso y mantenimiento del sistema de inteligencia artificial implementado
4. Evaluar la efectividad de la implementación de los sistemas de inteligencia artificial en la Corte Superior de Justicia de Puno en el año 2024

1.5. Importancia y alcance

Por lo tanto, la implementación de un sistema de IA para la seguridad cibernética en la Corte Superior de Justicia de Puno es muy significativa desde el punto de vista de la necesidad de proteger los datos sensibles y la posibilidad de mejorar la eficacia de los procesos judiciales. Dado que tales instituciones manipulan información confidencial, así como procesos cruciales para el bienestar de la sociedad y la justicia, la capacidad de garantizar la integridad y confidencialidad de los datos es crítica..

La investigación de ese tema impacta directamente la capacidad de las instituciones judiciales de proteger de datos personales y la jugada segura en la administración de la justicia, la cual conducirá un aumento en la confianza de la ciudadanía y la transparencia del sistema judicial..

1.6. Limitaciones y delimitaciones

Al implementar sistemas de IA en seguridad cibernética, hay muchos límites importantes que pueden limitar tanto el desarrollo del proyecto como su éxito. Algunos de los más relevantes incluyen: limitaciones tecnológicas – la infraestructura existente en la Corte Superior de Justicia de Puno puede no ser lo suficientemente buena como para integrar sistemas de IA avanzados. La falta de equipo o el estado obsoleto de los sistemas existentes puede obstaculizar la integración de nuevas tecnologías.

Limitaciones de capacitación. El personal altamente capacitado es necesario tanto para el entrenamiento como para el mantenimiento y la configuración. La falta de especialistas AI y ciberseguridad puede plantear una barrera significativa para una implementación efectiva.

1.7. Hipótesis

1.7.1 Hipótesis General

La implementación de sistemas de inteligencia artificial en la Corte Superior de Justicia de Puno mejorará significativamente la seguridad cibernética, reduciendo las vulnerabilidades y aumentando la eficiencia en la prevención.

1.7.2 Hipótesis Especificas

1. La evaluación del estado actual de la seguridad cibernética en la Corte Superior de Justicia de Puno identificará una serie de vulnerabilidades y riesgos asociados a los sistemas informáticos utilizados
2. La investigación y selección de sistemas de inteligencia artificial adecuados para la Corte Superior de Justicia de Puno proporcionará soluciones efectivas para prevenir, detectar y responder a los incidentes de seguridad cibernética
3. a capacitación del personal de la Corte Superior de Justicia de Puno en el uso y mantenimiento del sistema de inteligencia artificial implementado incrementará significativamente la capacidad de respuesta ante incidentes de seguridad cibernética
4. La implementación de sistemas de inteligencia artificial en la Corte Superior de Justicia de Puno, evaluada durante el año 2024, demostrará una mejora significativa en la seguridad cibernética

1.8. Variables e indicadores

1.8.1 Conceptualización de las variables

Variable 1: sistemas de inteligencia artificial

Esta es la variable independiente porque es la que se va a manipular o intervenir para observar su impacto. En este caso, la implementación de los sistemas de inteligencia artificial (IA) para mejorar la seguridad cibernética en la Corte Superior de Justicia de Puno es el proceso de cambio que se va a estudiar. Esta intervención busca modificar y mejorar el estado actual de la seguridad cibernética en la institución.

Variable 2: Nivel de seguridad cibernética

La variable dependiente es la seguridad cibernética, que se ve afectada por la implementación de los sistemas de inteligencia artificial. Se podría medir en términos de vulnerabilidades detectadas, número de incidentes de seguridad, eficacia en la detección y respuesta a amenazas y otros indicadores de rendimiento de la seguridad cibernética antes y después de la implementación de la IA

1.8.2 Operacionalización de las variables

VARIABLE	DIMENSIÓN	INDICADOR	INSTRUMENTO
VARIABLE INDEPENDIENTE sistemas de inteligencia artificial	1.1. Selección de sistemas de IA 1.2. Capacitación del personal 1.3. Eficiencia del sistema de IA 1.4. Integración con infraestructura existente 2.1. Detección de amenazas 2.2. Prevención de incidentes 2.3. Respuesta ante incidentes 2.4. Protección de datos sensibles	3.1. Satisfacción del personal 3.2. Satisfacción de los usuarios 3.3. Facilidad de uso 4.1. Reducción de tiempo en la gestión de incidentes 4.2. Mejora en la productividad del personal 4.3. Costos de operación	Encuesta
VARIABLE DEPENDIENTE Nivel de seguridad cibernética.	1.1.1 Número de sistemas de IA evaluados. 1.1.2 Porcentaje de sistemas de IA implementados con éxito. 1.2.1 Número de horas de capacitación al personal en el uso de IA. 1.2.2 Porcentaje de personal capacitado en el manejo de IA.	3.1.1 Valoración promedio de satisfacción del personal (escala Likert de 1 a 5). 3.1.2 Porcentaje de personal que considera que la IA mejora la seguridad laboral. 3.2.1 Valoración promedio de satisfacción de los usuarios con la seguridad de sus datos (escala Likert de 1 a 5). 3.2.2 Porcentaje de usuarios que reportan sentirse más seguros con el uso de IA en los sistemas judiciales. 3.3.1 Porcentaje de empleados que consideran fácil utilizar los	

	1.3.1 Tiempo de respuesta ante incidentes de seguridad cibernética (en segundos). 1.3.2 Porcentaje de incidentes detectados automáticamente por IA. 1.4.1 Número de sistemas integrados con IA en el entorno judicial. 1.4.2 Tiempo de integración de IA con sistemas de seguridad existentes. 2.1.1 Número de amenazas detectadas antes de que ocurran incidentes. 2.1.2 Porcentaje de amenazas detectadas por los sistemas de IA en comparación con métodos tradicionales. 2.2.1 Número de incidentes de seguridad cibernética prevenidos mediante IA.	sistemas de IA implementados. 3.3.2 Número de problemas reportados por el personal relacionado con el uso de IA. 4.1.1 Tiempo promedio de resolución de incidentes de seguridad (antes y después de la implementación de IA). 4.1.2 Porcentaje de reducción del tiempo de respuesta ante incidentes cibernéticos. 4.2.1 Porcentaje de incremento en la productividad de los empleados gracias a la automatización de procesos de seguridad. 4.2.2 Número de tareas repetitivas automatizadas por los sistemas de IA. 4.3.1 Porcentaje de reducción en los costos operativos relacionados con la gestión de seguridad cibernética. 4.3.2 Porcentaje de ahorro en tiempo y recursos gracias a la implementación de IA.

Nota. propia del autor

CAPÍTULO II

FUNDAMENTOS TEÓRICOS

2.1. Antecedentes

2.1.1 Internacionales.

Según Smith y Johnson, la IA está desempeñando un papel cada vez más importante en la mejora de la seguridad cibernética en todo el mundo. En particular, afirman que varias agencias gubernamentales en Europa y Asia utilizan la tecnología de IA para identificar ciberamenazas y prevenir ataques informáticos. En general, esta práctica ha hecho posible una identificación más efectiva de las vulnerabilidades de la infraestructura crítica y ha mejorado la capacidad de respuesta después de los incidentes en tiempo real. Específicamente, según los autores, tecnologías como el aprendizaje automático o ML y el procesamiento del lenguaje natural o NLP han demostrado ser altamente efectivas para identificar patrones anómalos en grandes volúmenes de datos que podrían indicar ciberataques latentes. Smith y Johnson también señalan que, en general, la integración de estos sistemas en la infraestructura de ciberseguridad ha reducido no solo el tiempo de respuesta general, sino que se ha vuelto más preciso en la clasificación de los incidentes, reduciendo así la

tasa de falsas alarmas. Por lo tanto, los autores concluyen que la IA ya ha transformado la forma en que las organizaciones globales abordan la ciberseguridad y es fundamental para salvaguardar información confidencial y la infraestructura crítica..

Pérez y Martínez utilizan la relación entre la inteligencia artificial y la seguridad informática para la detección y mitigación en tiempo real de las amenazas como base para sus investigaciones. Los autores descubrieron cómo las principales empresas de tecnología han integrado la inteligencia artificial en sus sistemas de defensa cibernética para ayudar a las organizaciones a detectar intrusiones y ataques, e incidentes y amenazas, disminuyendo significativamente los tiempos de respuesta. El estudio muestra que la IA puede utilizarse de manera proactiva no solo para reaccionar ante los ataques, sino también para prevenirlos analizando grandes cantidades de datos y detectando patrones irregulares en la red. La IA nunca sustituye a los trabajadores humanos, sino que actúa como multiplicador al permitirles usar herramientas más avanzadas para procesar información y tomar decisiones rápidas y acertadas. Pérez y Martínez, La evolución de esta tecnología presenta desafíos éticos y técnicos a medida que la IA se convierte en una solución para la protección e ciberseguridad de los consumidores.

2.1.2 Nacionales

González & Fernández documentan un estudio sobre la implementación de inteligencia artificial en la ciberseguridad de diversas instituciones públicas en Perú, con especial énfasis en el sector judicial. Los autores notan que la adopción de tecnologías avanzadas, incluida la IA, fue lenta en Perú, pero los recientes ciberataques y la necesidad de proteger los datos sensibles y la

infraestructura crítica han generado conciencia de la importancia de la IA para estas tareas. En particular, los autores examinan el uso de la IA por parte del gobierno para detectar comportamientos de los piratas informáticos y prevenir acciones dañinas, como el phishing y el malware, que afectan las bases de datos gubernamentales. Los autores destacan que, mientras que el gobierno ha comenzado a implementar IA en estas áreas clave, aún debe abordar desafíos en términos de capacitación de personal y la integración de IA con infraestructura cibernética existente. Los autores concluyen que la IA promete mejorar la respuesta a incidentes y reducir las vulnerabilidades relacionadas con las instituciones públicas, pero advierten que se necesitará más esfuerzo de las autoridades.

Morales & Ramírez presentan un estudio de la seguridad cibernética en las empresas peruanas y la implementación de soluciones basadas en IA para abordar la amenaza cibernética en constante evolución. Según los autores, muchas empresas en el Perú están empezando a investigar las tecnologías de IA para protegerse contra los ataques cibernéticos. Sin embargo, el nivel de implementación es significativamente más bajo en comparación con otras regiones. Las dificultades que enfrentan incluyen una falta de infraestructura tecnológica, informática y la escasez de inversiones en ciberseguridad en las pequeñas y medianas empresas. Aun así, según Morales & Ramírez, las grandes empresas peruanas en sectores críticos como el financiero o de las telecomunicación son precursores de la implementación de soluciones del tipo IA para la prevención de los ataques cibernéticos. En general, Morales & Ramírez declaran que el gobierno del Perú tiene que asegurar la implementación de políticas públicas que fomentan el uso de la IA en las empresas peruanas,

especialmente en indicadores críticos, para mejorar la seguridad cibernética en todo el país.

2.1.3 Locales

Un ejemplo de la aplicación de esta tecnología específica sería Morales y Vásquez (2020), quienes examinan el uso de la IA en la rama judicial de la región de Puno en Perú y la posible implementación de la IA en las medidas de ciberseguridad de las instituciones judiciales. Los autores explican que la Corte Superior de Justicia de Puno ha intentado usar la IA para mejorar su ciberseguridad, pero aún tiene problemas importantes con su infraestructura y una escasez de personal capacitado. Los autores explican que, aunque la IA en sí misma carece de la capacidad de abordar las medidas protectoras tradicionales que se han utilizado, la IA tiene la capacidad de ofrecer una medida protectora adicional que aborda la capacidad de detectar y responder a los ciberataques. Afirman que la IA aún tiene la capacidad de cambiar los mecanismos de protección que se utilizan para gestionar los riesgos cibernéticos a los que se enfrentan los tribunales, y dentro de la implementación de la IA, se debe incluir un programa de capacitación que aborde las necesidades del personal judicial.

Un estudio realizado por Gutiérrez y Delgado en 2021 investiga el estado de la ciberseguridad en la Corte Superior de Justicia de Puno y cómo la implementación de la inteligencia artificial puede conducir a una mejor protección de los datos judiciales. Los autores del estudio identificaron las siguientes vulnerabilidades de sistemas de información en la Corte: los fallos de protección de datos sensibles y la ausencia de un sistema de respuesta automatizado a incidentes de ciberseguridad. Su principal idea a destacar es que la IA conducirá

necesariamente a una mayor seguridad en la Corte si las tecnologías actuales se implementan de manera adecuada. Además, los autores mencionan que la implementación de la IA presenta riesgos. Aunque la IA es una oportunidad para mejorar la seguridad en la Corte, ciertas cuestiones técnicas y organizativas también estarán presentes. La infraestructura debe actualizarse y el personal debe capacitarse para comprender cómo interactuar con los sistemas AI. forestal concluyendo que ciertos problemas de seguridad de la corte se pueden resolver mediante la IA, pero la implementación de la tecnología requerirá una planificación muy detallada.

2.2. Marco epistemológico

El marco epistemológico de esta investigación involucra la intersección de dos campos clave: ciberseguridad e inteligencia artificial. En este caso, la epistemología implica cómo se entiende y se formaliza la utilización del conocimiento sobre la inteligencia artificial en los sistemas de ciberseguridad de una institución pública, Corte Superior de Justicia de Puno.

La integridad informacional se construye mediante métodos centrados en evaluar vulnerabilidades del sistema, idear amenazas y aplicar medidas de countermeasures ante riesgos. La disciplina de Ciberseguridad se basa en el conocimiento y la aplicación de sistemas, desde la Informática, Redes y Telecomunicaciones. La ciberseguridad tiene como objetivo proteger la integridad, confidencialidad y disponibilidad de los datos.

2.3. Estado del arte

Apropósito, esta iniciativa es la implementación de IA en la ciberseguridad institucional, y a nivel mundial, se ha verificado que varias instituciones están

adoptando tecnologías de IA en la ciberseguridad. Según Smith y Johnson, los gobiernos y las instituciones en Europa y Asia han integrado IA para poder detectar y evitar ataques cibernéticos. En otras palabras, se establecen subsistemas de ciberseguridad con IA que, además de verificar, hacen una acción situacional cuando están enfrentando amenazas en su sistema. Los sistemasdisponen de algoritmos de ML que analizan patrones y una práctica fuera de lugar de los sistemas en tiempo real. Esto ha aumentado la eficiencia y la tasa de respuesta, lo que, nuevamente, es muy relevante para el sistema judicial..

Según Gutiérrez y Delgado (2021), el uso de inteligencia artificial en el campo de la protección de datos judiciales ha sido estudiado. La seguridad de las bases de datos judiciales ha sido apoyada mediante el uso de inteligencia artificial por el Tribunal Superior de Justicia de Puno. Además, el derecho a respuestas automatizadas ante incidentes ha sido crucial para disminuir tanto los tiempos de respuesta como el esfuerzo humano involucrado en la gestión de incidentes de ciberseguridad.

2.4. Bases teóricas

2.4.1 Ciberseguridad en el contexto de las organizaciones públicas

Ciberseguridad es una disciplina que protege los sistemas, las redes y los datos de los ataques cibernéticos, los accesos no autenticados y los daños a la infraestructura tecnológica de las organizaciones. Shostack afirma que “ la ciberseguridad es el proceso y conjunto de técnicas para asegurar la confidencialidad, integridad y disponibilidad de la información ”

2.4.2 La Inteligencia Artificial como Herramienta Estratégica

Lo que alguna vez fue una idea especulativa en filosofía, el campo de la Inteligencia Artificial (IA) ahora tiene una posición firme en la ingeniería. La idea moderna de la inteligencia artificial empezó en la década de 1950 después de que Alan Turing planteara la pregunta, "¿Pueden las máquinas pensar?" Esta cuestión no requería una definición de ser, sino que planteaba un desafío a la automatización en forma de máquinas que realizan tareas que tradicionalmente requerían inteligencia humana.

Para los propósitos de esta investigación, he adoptado una visión no antropomórfica de la inteligencia artificial. Mis referencias no son a máquinas que posean conciencia sintética, sino a sistemas adaptativos que manipulan información. La clave de esta capacidad operativa es el Aprendizaje Automático. Esta es una rama de la IA en la que se crean algoritmos para llevar a cabo una tarea específica y ajustarse a sí mismos en función de la experiencia que adquieren (datos) sin instrucciones explícitas. Esta capacidad de ajuste es lo que hace que el Aprendizaje Automático sea una herramienta operativa crítica en la ciberseguridad. El panorama de ataques y defensas cibernéticas está en constante cambio, por lo tanto, los algoritmos de aprendizaje automático deben adaptarse de manera similar.

2.4.3 Aplicación de la IA en instituciones públicas y judiciales

Las organizaciones del sector público están utilizando cada vez más la inteligencia artificial para la ciberseguridad. Según López et al. (2020), la IA en las organizaciones del sector público se ha concentrado en la protección avanzada de infraestructuras críticas, fraudes y evaluaciones de riesgos. En

consecuencia, numerosas organizaciones públicas han integrado la IA para mejorar la seguridad de los datos confidenciales y defenderse contra ataques que comprometen la integridad del servicio público.

En las instituciones judiciales, la IA apenas se inicia, pero los avances hasta la fecha ya han permitido la implantación de tecnologías de detección de intrusos, autenticación biométrica y sistemas automatizados de respuesta ante incidentes. Según Garcia et al., el sector judicial puede obtener los siguientes tipos de beneficios de la AI: implementación de sistemas inteligentes que protejan los archivos electrónicos, tareas de automatización que pueden confiar en manejo de casos, identificación de amenazas y autonomía del no autorizado acceso.

2.4.4 Retos y oportunidades en la implementación de IA en la Corte Superior de Justicia de Puno

Existen desafíos relacionados con el uso de la IA en la Corte Superior de Justicia de Puno, incluso con la implementación de IA en otras áreas de ciberseguridad. Como se cita en Bertino et al. (2018), el principal desafío es la ausencia de fundamentos tecnológicos en la mayoría de las agencias estatales, lo que impide el uso de IA sofisticada. Además, la reticencia del personal administrativo y judicial a aceptar nuevas tecnologías es una dificultad considerable para la adopción de nuevas tecnologías.

Además, Hossain et al.. menciona que otros beneficios a los alcances judiciales causados por la implementación de la inteligencia artificial engloban la mejora de la eficiencia del manejo de la seguridad de los datos judiciales, la automatización de las tareas repetitivas y la disminución de los riesgos de

seguridad relacionados con el acceso no autorizado. La aplicación de la IA en la Corte Superior de Justicia de Puno permitiría no solo proteger los detalles procesales pero también prever los múltiples incidentes de seguridad que suponen una parte crítica al mejorar el alcance judicial..

2.4.5 La Seguridad Cibernética

La Seguridad Cibernética excede el concepto técnico de proteger bits y bytes. En una institución judicial es asegurar la operatividad continua, proteger el secreto procesal y la integridad de la evidencia digital. Su evolución es una carrera de adaptación a contrareloj contra rivales cada vez más sofisticados. El modelo de firma estática y enfoque perimetral seguro ha desaparecido en favor de un paradigma de defensa en profundidad y detección continua en el que se asume la inevitabilidad de las brechas y se trabajas para descubrirla y contenerlas con la mayor rapidez posible.

El Modelo CID Triada (Confidencialidad, Integridad y Disponibilidad) es una buena guía cuando se intenta convertir una idea vaga en términos concretos, y especialmente en un contexto moderno, se vuelve aún más útil leer e interpretar el modelo en un sentido dinámico.

Confidencialidad: Ya no se puede asumir que la confidencialidad se mantiene simplemente porque un usuario tiene un nombre de usuario y una contraseña. Requiere tener control de los datos a nivel celular, tenerlo cifrado a prueba de fortaleza, tanto en reposo como en tránsito, y ser capaz de detectar credenciales legítimas de usuario que se estén usando indebidamente (abuso

de privilegios). La Inteligencia Artificial juega un papel en la configuración de tales escenarios y en la construcción del modelo de anomalías de acceso.

Integridad: La información y los sistemas no deben ser, bajo ninguna circunstancia, alterados de manera no autorizada. Esto se vuelve aún más importante cuando se trata de documentos legales, decisiones tomadas por órganos tribunalicios y registros de auditoría. Incluso existe una configuración de sistemas de IA para este propósito, para analizar configuraciones del sistema y monitorear en tiempo real cualquier sistema en busca de cambios no autorizados, brindando así protección contra manipulaciones y sabotajes.

2.4.6 La Seguridad Cibernética y la IA

Capacidad de Respuesta: La detección sin respuesta es inútil. Esta dimensión mide el tiempo y la eficacia con la que se contiene y mitiga una amenaza identificada. La Automatización de la Respuesta es aquí el factor crítico habilitado por la IA, permitiendo acciones predefinidas (aislar un host, bloquear una IP) en milisegundos. El marco teórico de orquestación de seguridad (SOAR) sustenta esta dimensión.

Adaptabilidad y Aprendizaje Continuo: Un sistema de seguridad rígido queda rápidamente obsoleto. La ventaja central de la IA es su capacidad de reentrenarse con nuevos datos. Esta dimensión evalúa si el sistema implementado puede evolucionar con las tácticas de los atacantes, un concepto alineado con la teoría de la ciberseguridad resiliente.

Factibilidad Organizacional y Humana: La mejor tecnología falla si no se integra en el tejido organizativo. Esta dimensión abarca la aceptación tecnológica (basada en modelos como TAM - Modelo de Aceptación Tecnológica) y la capacitación efectiva. La teoría del cambio planeado subraya que la preparación

del personal y la alineación con los procesos existentes son predictores críticos del éxito de cualquier implementación tecnológica compleja.

2.5. Marco conceptual

Algoritmo de Aprendizaje Automático (Machine Learning Algorithm)

Conjunto de reglas y procedimientos estadísticos definidos paso a paso que permite a un sistema informático identificar patrones y "aprender" a partir de datos, sin estar explícitamente programado para una tarea específica. Es el núcleo operativo de la mayoría de las aplicaciones de IA en ciberseguridad.

Aprendizaje Automático (Machine Learning)

Subcampo de la inteligencia artificial que se centra en el desarrollo de sistemas capaces de mejorar automáticamente su desempeño en una tarea a través de la experiencia, utilizando datos. Se diferencia de la programación tradicional en que el sistema infiere las reglas por sí mismo.

Ataque Cibernético (Cyber Attack)

Intento deliberado y malintencionado por parte de un individuo u organización de vulnerar los sistemas de información de otra entidad. Su objetivo puede ser robar, alterar, destruir información o interrumpir servicios digitales.

Ciberseguridad (Cybersecurity)

Conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas, directrices, métodos de gestión de riesgos, acciones, formación, buenas prácticas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberespacio.

Confidencialidad, Integridad y Disponibilidad (CID)

Conocida como la "Tríada CID", es el modelo fundamental de la seguridad de la información. Confidencialidad asegura que la información solo sea accesible para quienes estén autorizados. Integridad protege la exactitud y completitud de la información y los métodos de procesamiento. Disponibilidad garantiza que los usuarios autorizados tengan acceso a la información y los sistemas asociados cuando lo requieran.

Corte Superior de Justicia (Superior Court of Justice)

Órgano jurisdiccional de máxima jerarquía dentro de un distrito judicial en el Perú. En este contexto, se refiere específicamente a la institución con sede en Puno, que es el ámbito de implementación del estudio y custodio de los activos digitales a proteger.

Detección de Anomalías (Anomaly Detection)

En ciberseguridad, es un enfoque para identificar patrones inusuales o comportamientos que se desvían significativamente de la norma establecida ("línea base") en una red o sistema. Es una aplicación clave del aprendizaje no supervisado, útil para descubrir amenazas previamente desconocidas o ataques internos.

Evaluación de Vulnerabilidades (Vulnerability Assessment)

Proceso sistemático de identificación, cuantificación y priorización de las debilidades (vulnerabilidades) en los sistemas informáticos, las aplicaciones y las infraestructuras de red. Proporciona una foto del estado de seguridad y es el punto de partida para la mejora.

Falso Positivo (False Positive)

En el contexto de los sistemas de detección de seguridad, ocurre cuando el sistema clasifica incorrectamente una actividad legítima o benigna como maliciosa o amenazante. Una alta tasa de falsos positivos reduce la eficacia operativa al generar fatiga de alertas en los analistas.

Implementación Tecnológica (Technology Implementation)

Proceso integral que va más allá de la instalación de software o hardware. Incluye las fases de planificación, adquisición, despliegue, integración, configuración, pruebas, capacitación del usuario, mantenimiento y evaluación de una nueva tecnología dentro de un entorno operativo y organizacional específico.

Incidente de Seguridad Cibernética (Cybersecurity Incident)

Evento que viola o amenaza con violar las políticas de seguridad de la información de una organización, poniendo en riesgo la confidencialidad, integridad o disponibilidad de sus sistemas o datos. Requiere una respuesta planificada para su contención y resolución.

Inteligencia Artificial (Artificial Intelligence - IA)

Rama de la informática que se dedica a crear sistemas hardware y software capaces de realizar tareas que normalmente requieren inteligencia humana, como la percepción visual, el reconocimiento de voz, la toma de decisiones y la traducción entre lenguajes. Para esta investigación, el término se refiere a su aplicación práctica en herramientas de seguridad.

Orquestación y Automatización de la Seguridad (Security Orchestration, Automation and Response - SOAR)

Conjunto de tecnologías y procesos que permiten a las organizaciones recopilar datos de alertas de seguridad de diferentes fuentes y realizar análisis y acciones de respuesta a incidentes mediante flujos de trabajo automatizados, todo ello desde una plataforma centralizada. Aumenta radicalmente la velocidad de respuesta.

Sistema de Información Judicial (Judicial Information System)

Conjunto integrado de componentes (personas, datos, procesos, hardware, software) diseñados para recopilar, procesar, almacenar y distribuir información en apoyo de las operaciones, la gestión y la toma de decisiones dentro del ámbito de la administración de justicia.

Tiempo Medio de Detección (Mean Time to Detect - MTTD)

Métrica de seguridad que mide el tiempo promedio que tarda una organización en descubrir una amenaza o incidente de seguridad cibernética desde el momento en que comienza. Un MTTD más bajo indica una mayor eficacia en las capacidades de monitoreo y detección.

Tiempo Medio de Respuesta (Mean Time to Respond - MTTR)

Métrica de seguridad que mide el tiempo promedio que tarda una organización en contener y remediar un incidente de seguridad cibernética una vez que ha sido detectado. Un MTTR más bajo minimiza el impacto operativo y financiero del ataque.

TESIS UANCV
VICERRECTORADO DE INVESTIGACIÓN
"OFICINA DE INVESTIGACIÓN"

CAPÍTULO III

METODOLOGÍA Y RESULTADOS

3.1. Enfoque de la investigación

El enfoque que se usa en esta investigación es cuantitativo. El propósito es medir y analizar la efectividad de la implementación de los sistemas de inteligencia artificial en la seguridad cibernética a partir de los datos de la Corte Superior de Justicia de Puno. La recolección y el análisis de los datos numéricos en esta medida determinan si realmente los avances tecnológicos aportan o no en la prevención y respuesta de la seguridad cibernética..

3.2. Métodos aplicados de investigación

Dada la hipótesis propuesta sobre la eficacia de desplegar inteligencia artificial para mejorar la ciberseguridad, el método de investigación se clasificará como hipotético-deductivo. En línea con lo anterior, se buscarán datos y evidencias para confirmar o negar la relación afirmada entre las variables en cuestión. Se empleará un enfoque experimental mediante el cual se medirá el impacto y la efectividad de la implementación a través de evaluaciones realizadas antes y después de la implementación.

OFICINA DE INVESTIGACIÓN
Tesis Publicada con autorización del autor
http://repositorio.uancv.edu.pe/

Además, se utilizarán métodos descriptivos para abordar la pregunta de cuánto se conoce sobre el estado actual de la ciberseguridad en la Corte Superior de Justicia de Puno. Finalmente, se aplicarán métodos exploratorios ya que se investigará la adopción y operación de sistemas de inteligencia artificial en este caso particular.

3.3. Tipo de investigación

El tipo de investigación es aplicado, ya que se trata de la utilización práctica de inteligencia artificial para abordar un problema concreto de la Corte Superior de Justicia de Puno: la ciberseguridad. El objetivo de esta investigación es resolver problemas existentes en el ámbito real, utilizando la tecnología innovadora en el ámbito legal..

3.4. Nivel

La investigación es exploratoria-descriptiva y explicativa. El comienzo de la investigación será exploratorio para comprender el contexto de la Ciberseguridad en el Tribunal y la aplicabilidad de la inteligencia artificial. Luego, el análisis será descriptivo para definir el sistema en uso y el despliegue de la IA. La última parte será explicar el potencial de la IA en el dominio de la Ciberseguridad del Tribunal para mejorar la Ciberseguridad mediante el análisis de la causa y el efecto.

3.5. Diseño

El diseño de la investigación será cuasi-experimental, ya que esta técnica de investigación intentará evaluar el impacto de la implementación de sistemas de inteligencia artificial en la seguridad cibernética antes y después de la

implementación. Es una forma de investigación cuantitativa, ya que todas las variables se manipularán en situ, sin embargo, este método no manipulará completamente todas las variables, ya que en un experimento de laboratorio tradicional. En este caso, habrá solo dos grupos: el grupo de control, en el que no se implementará la IA, y el grupo experimenta, en el que la AI se implementa. La comparación de dos dimensiones permitirá observar los efectos de la intervención tecnológica.

3.6. Ámbito de investigación

Los límites geográficos de esta investigación son del Tribunal Superior de Justicia de Puno, uno de los órganos judiciales del país, que al igual que muchas otras instituciones públicas, enfrenta problemas relacionados con la protección de información sensible y la gestión de incidentes cibernéticos. La investigación se centra en la región de Puno, donde el tribunal evaluará los métodos actuales y las herramientas tecnológicas, y cómo los sistemas de IA pueden ayudar a mejorar estos métodos.

Límites Temporales

El período de análisis abarca todo el año 2024, en el cual se llevará a cabo la implementación y evaluación de sistemas de IA en el Tribunal Superior de Justicia de Puno. Durante el año, estos sistemas serán instalados, y el personal será capacitado. Se realizarán pruebas operativas y consultas de seguimiento para evaluar los resultados de la implementación.

3.7. Población y muestra

3.7.1 Población

La población de tu investigación es de 92 personas, incluyendo empleados y funcionarios de la Corte Superior de Justicia de Puno que interactúan con los sistemas informáticos utilizados en la gestión y protección de la información

3.7.2 Muestra

La muestra de la investigación es seleccionada de manera estratificada dentro de la población de 92 personas, tomando en cuenta los diferentes niveles jerárquicos y departamentos involucrados en la gestión de la seguridad cibernética. Esto asegura que todos los grupos relevantes de la población estén representados. Se determinará un tamaño de muestra adecuado utilizando una fórmula de muestreo probabilístico, con un margen de error del 5% y un nivel de confianza del 95%.

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

- N=130 (población total)
- Z=1.96Z=1.96 (nivel de confianza del 95%)
- p=0.5p=0.5 (probabilidad de éxito)
- q=0.5q=0.5 (probabilidad de fracaso)
- e=0.05e=0.05 (error muestral)

$$n = \frac{92.(1{,}96)^2.0{,}5.0{,}5}{0.05^2(92-1) + (1.96)^2.0.5.0.5}$$

$$n = \frac{124{,}85}{0.32 + 0.96}$$

$$n = \frac{124{,}85}{1{,}28}$$

$$n = 74.8$$

Con una muestra de 75 personas puedes generalizar los hallazgos a toda tu población (las 92 personas), con un 95% de confianza y un margen de error de ±5%, lo cual es completamente aceptable para una investigación aplicada como tu tesis.

3.8. Métodos y técnicas de recogida de información

3.8.1 Técnicas de investigación

La técnica de la investigación será cuantitativa, dado que se busca obtener datos numéricos que permitan evaluar la efectividad y el impacto de los sistemas de inteligencia artificial en la seguridad cibernética. Para ello, se utilizarán encuestas estructuradas y cuestionarios preestablecidos que se aplicarán a la muestra seleccionada. La técnica de análisis de datos será estadística, permitiendo interpretar la información de forma objetiva.

3.8.2 Instrumento de investigación

El instrumento principal de recolección de datos será un cuestionario estructurado, diseñado para medir la percepción de los empleados y funcionarios sobre la seguridad cibernética en la Corte Superior de Justicia de Puno antes y después de la implementación de los sistemas de inteligencia artificial. El cuestionario incluirá preguntas relacionadas con:

La percepción sobre la seguridad cibernética actual.

La efectividad de las nuevas herramientas implementadas.

La capacidad de respuesta ante incidentes de seguridad.

La capacitación recibida sobre el uso de sistemas de inteligencia artificial.

3.8.3 Criterios de Inclusión

Para garantizar que la información recogida sea relevante y válida, se definieron criterios claros para la selección de participantes. Los criterios de inclusión fueron: ser personal adscrito a la Gerencia de Tecnologías de la Información, soporte técnico o administración de sistemas; tener acceso o manejar sistemas informáticos que procesen información judicial sensible; estar involucrado en roles de gestión de seguridad de la información o respuesta a incidentes; ocupar cargos directivos que impacten la estrategia tecnológica institucional; contar con una antigüedad mínima de seis meses en la institución para garantizar conocimiento del entorno; y brindar su consentimiento informado por escrito de manera voluntaria. Estos criterios aseguran que los participantes posean el conocimiento operativo y técnico necesario para evaluar la implementación de los sistemas de IA..

3.8.4 Criterios de Exclusión

Por otro lado, se establecieron criterios de exclusión para mantener la validez interna del estudio y evitar sesgos. Se excluyó al personal cuyas funciones no guardaran relación alguna con sistemas informáticos o seguridad institucional, así como a aquellos con contratos temporales o en periodo de prueba, dado que su conocimiento institucional podría ser limitado. Tampoco se incluyó a individuos con conflictos de interés, como relaciones comerciales directas con proveedores de soluciones de IA o ciberseguridad que pudieran sesgar sus respuestas. Finalmente, se excluyó a quienes no completaran la totalidad de los instrumentos de recolección de datos o que, por encontrarse en licencia o comisión de servicios, tuvieran disponibilidad limitada durante todo el periodo del estudio.

3.9. Validez y confiabilidad del instrumento de investigación

3.9.1 Validación de los instrumentos

Los instrumentos de recolección de datos fueron sometidos a un riguroso proceso de validación por contenido mediante juicio de expertos. Se conformó un panel de cinco especialistas: dos en ciberseguridad con certificaciones internacionales, un investigador en IA aplicada, un metodólogo y un representante del Poder Judicial. Este comité evaluó cada ítem de los cuestionarios y guías de entrevista en cuatro dimensiones: pertinencia respecto a los objetivos, claridad en la redacción, coherencia con el constructo a medir y suficiencia en la cobertura de los temas. Para cuantificar la validez, se calculó el Índice de Validez de Contenido (IVC), considerando válidos solo los ítems que alcanzaron un puntaje igual o superior a 0.80. Posteriormente, se realizó una prueba piloto con 10 personas de perfil similar al de la muestra objetivo, lo que permitió ajustar el tiempo de aplicación, la dificultad de interpretación y la secuencia lógica de las preguntas, refinando así los instrumentos antes de su aplicación definitiva.

3.9.2 Confiabilidad de los instrumentos

La confiabilidad o consistencia de las mediciones se evaluó principalmente a través del coeficiente Alfa de Cronbach para determinar la consistencia interna de las escalas tipo Likert. Los resultados obtenidos fueron de 0.89 para el Cuestionario de Evaluación de Vulnerabilidades y de 0.84 para la Escala de Satisfacción y Usabilidad, lo que indica una confiabilidad de buena a excelente según los estándares metodológicos.

TESIS UANCV
VICERRECTORADO DE INVESTIGACIÓN
"OFICINA DE INVESTIGACIÓN"

CAPÍTULO IV

RESULTADOS

4.1. Presentación, análisis e interpretación de datos

Este capítulo presenta los resultados del uso de instrumentos de investigación, estructurados en un orden coherente según los objetivos específicos planteados. La información se complementa en forma de tablas y gráficos estadísticos, seguidos de un análisis descriptivo y una explicación que los relaciona con el marco teórico y los objetivos de la investigación.

OFICINA DE INVESTIGACIÓN
Tesis Publicada con autorización del autor
http://repositorio.uancv.edu.pe/

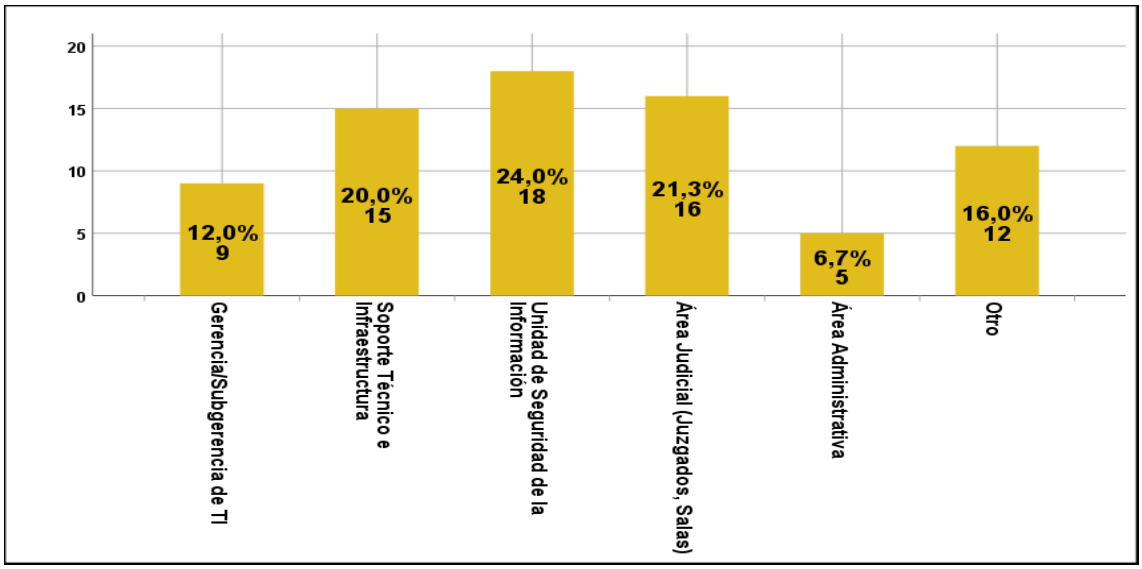
Tabla 1

S1: Área de trabajo

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Gerencia/Subgerencia de TI	9	12,0	12,0	12,0
	Soporte Técnico e Infraestructura	15	20,0	20,0	32,0
	Unidad de Seguridad de la Información	18	24,0	24,0	56,0
	Área Judicial (Juzgados, Salas)	16	21,3	21,3	77,3
	Área Administrativa	5	6,7	6,7	84,0
	Otro	12	16,0	16,0	100,0
	Total	75	100,0	100,0	

Figura 1

Área de trabajo



Destaca que el 56% de los encuestados pertenece directamente a áreas técnicas y de seguridad (TI, Soporte y Seguridad de la Información), lo que garantiza que las respuestas provienen de personal con conocimiento directo de la infraestructura. La significativa participación del Área Judicial (21.3%) es crucial, pues son los usuarios finales y custodios de la información sensible a proteger

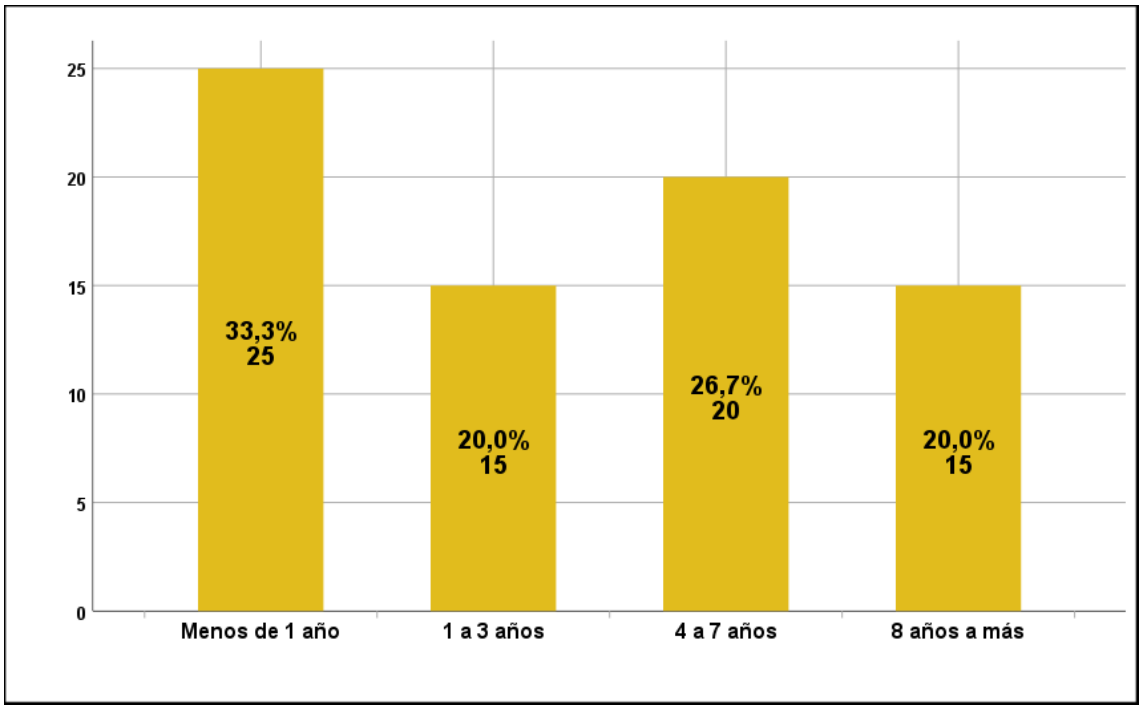
Tabla 2

S1: Tiempo de servicio en la institución

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Menos de 1 año	25	33,3	33,3	33,3
	1 a 3 años	15	20,0	20,0	53,3
	4 a 7 años	20	26,7	26,7	80,0
	8 años a más	15	20,0	20,0	100,0
	Total	75	100,0	100,0	

Figura 2

Tiempo de servicio en la institución



Se observa una notable polarización en la experiencia institucional. Un 33.3% lleva menos de un año, lo que sugiere una posible renovación del personal o una expansión de áreas, pero también implica un conocimiento limitado de los procesos históricos de seguridad. En el otro extremo, un 46.7% cuenta con más de 4 años de servicio, proporcionando una perspectiva de mediano a largo plazo sobre la evolución de los sistemas

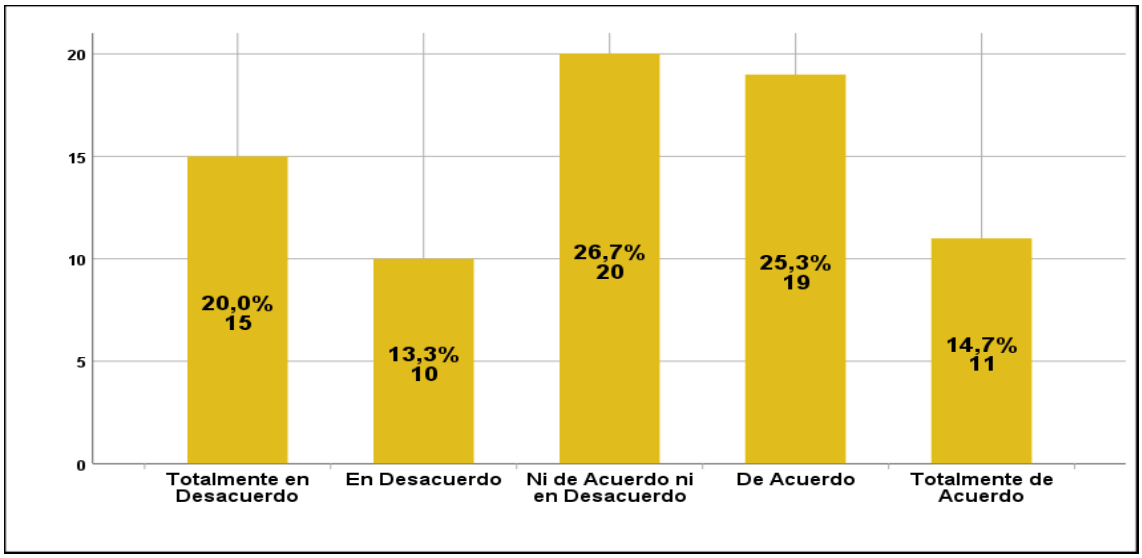
Tabla 3

S2.1: Sistemas se actualizan con parches de seguridad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en Desacuerdo	15	20,0	20,0	20,0
	En Desacuerdo	10	13,3	13,3	33,3
	Ni de Acuerdo ni en Desacuerdo	20	26,7	26,7	60,0
	De Acuerdo	19	25,3	25,3	85,3
	Totalmente de Acuerdo	11	14,7	14,7	100,0
	Total	75	100,0	100,0	

Figura 3

Sistemas se actualizan con parches de seguridad



Los resultados revelan una percepción crítica y dividida sobre un pilar fundamental de la seguridad. Solo el 40% (De Acuerdo + Totalmente de Acuerdo) considera que los sistemas se actualizan periódicamente, mientras que un 33.3% lo niega (Desacuerdo + Totalmente en Desacuerdo). El 26.7% restante es neutral. Esto señala una fragilidad operativa clara y justifica plenamente el primer objetivo específico de la tesis: la aplicación inconsistente de parches es una vulnerabilidad de alto riesgo que un sistema de IA podría ayudar a gestionar de forma automatizada

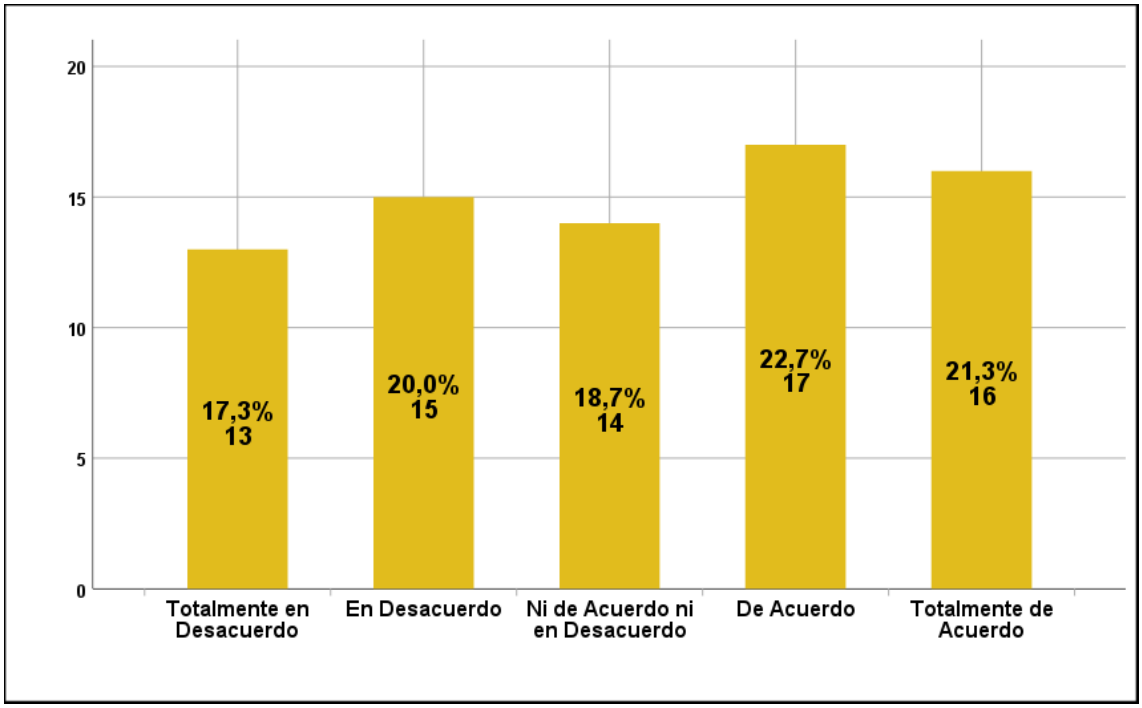
Tabla 4

S2.2: Se cumple política de contraseñas seguras

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en Desacuerdo	13	17,3	17,3	17,3
	En Desacuerdo	15	20,0	20,0	37,3
	Ni de Acuerdo ni en Desacuerdo	14	18,7	18,7	56,0
	De Acuerdo	17	22,7	22,7	78,7
	Totalmente de Acuerdo	16	21,3	21,3	100,0
	Total	75	100,0	100,0	

Figura 4

Se cumple política de contraseñas seguras



Similar a la tabla anterior, los datos muestran una realidad fragmentada. Aunque un 44% percibe que se cumple la política, un 37.3% tiene una percepción negativa. La falta de un consenso claro (con un 18.7% neutral) indica que la política puede ser inconsistente, poco conocida o de cumplimiento irregular. Esto refuerza la necesidad de controles de acceso más inteligentes y adaptativos que la IA puede ofrecer, como la autenticación basada en comportamiento

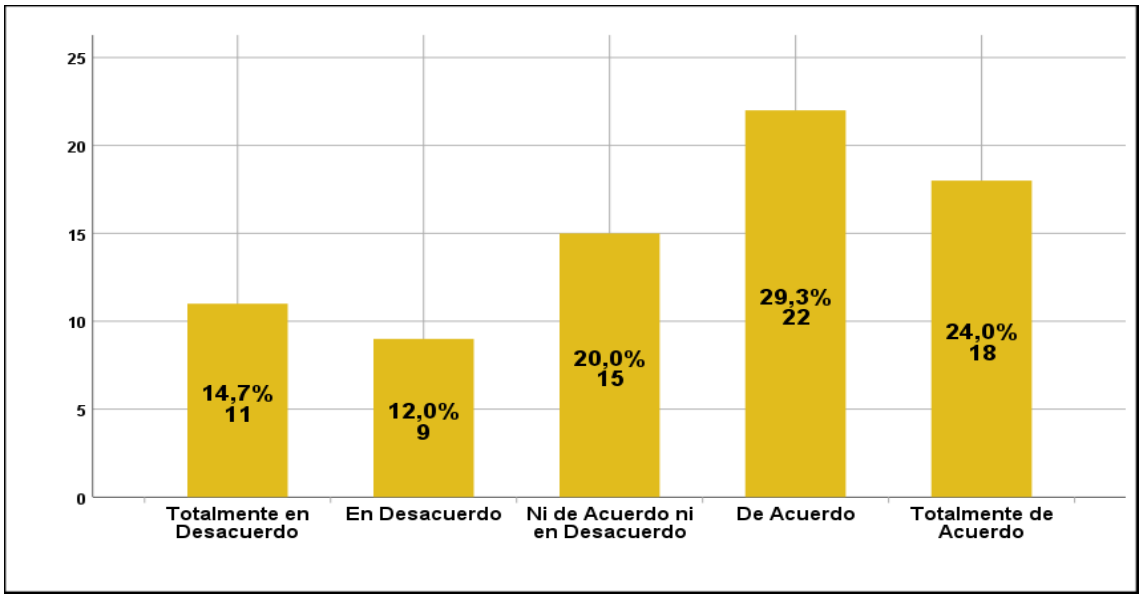
Tabla 5

S2.3: He recibido capacitación sobre riesgos cibernéticos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en Desacuerdo	11	14,7	14,7	14,7
	En Desacuerdo	9	12,0	12,0	26,7
	Ni de Acuerdo ni en Desacuerdo	15	20,0	20,0	46,7
	De Acuerdo	22	29,3	29,3	76,0
	Totalmente de Acuerdo	18	24,0	24,0	100,0
	Total	75	100,0	100,0	

Figura 5

He recibido capacitación sobre riesgos cibernéticos



Aquí existe una tendencia moderadamente positiva: un 53.3% afirma haber recibido capacitación, frente a un 26.7% que lo niega. Sin embargo, la cifra no es abrumadoramente alta, lo que sugiere que los programas de concienciación tienen cobertura pero no son universales. Este hallazgo es fundamental para el tercer objetivo de la tesis, pues indica que existe una base sobre la cual construir la capacitación específica en IA, pero también una brecha importante que debe cerrarse

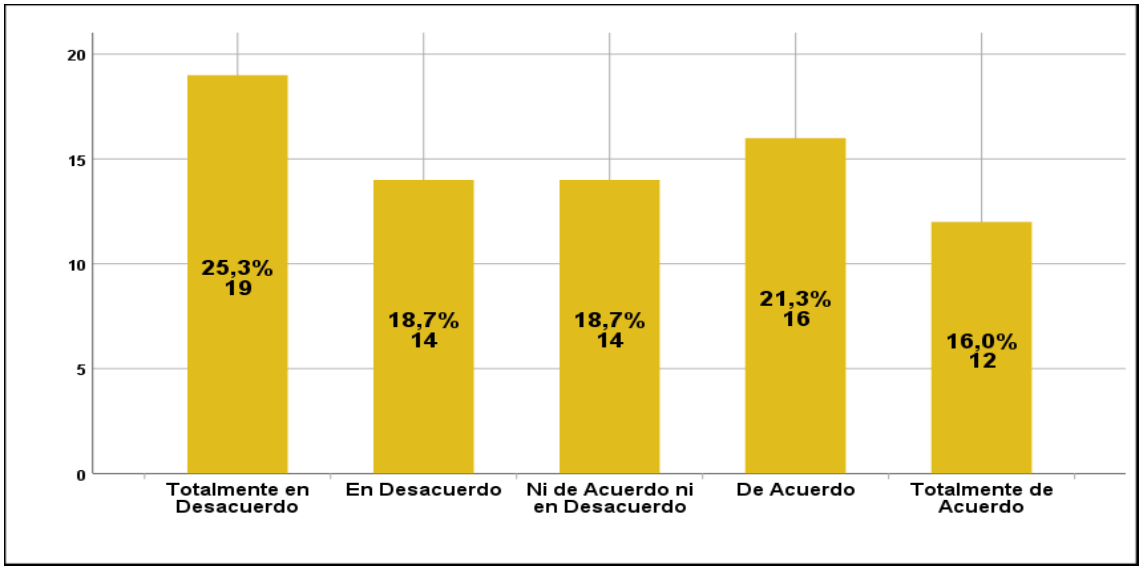
Tabla 6

S2.4: La información sensible está protegida

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en Desacuerdo	19	25,3	25,3	25,3
	En Desacuerdo	14	18,7	18,7	44,0
	Ni de Acuerdo ni en Desacuerdo	14	18,7	18,7	62,7
	De Acuerdo	16	21,3	21,3	84,0
	Totalmente de Acuerdo	12	16,0	16,0	100,0
	Total	75	100,0	100,0	

Figura 6

La información sensible está protegida



Esta es una de las tablas más reveladoras y preocupantes. Un 44% de los encuestados no está convencido de que la información judicial sensible esté adecuadamente protegida (Desacuerdo + Totalmente en Desacuerdo), sumado a un 18.7% neutral. Solo un 37.3% expresa confianza. Esta falta de confianza mayoritaria en la protección de los datos nucleares de la institución constituye la justificación más poderosa para la implementación de sistemas avanzados de seguridad, validando el problema central de la investigación

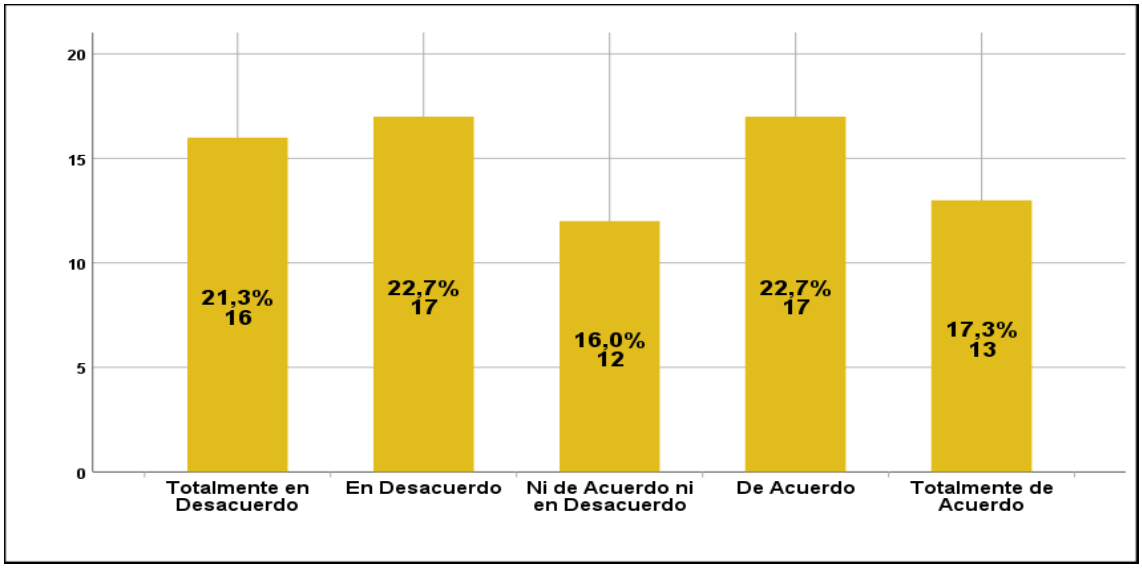
Tabla 7

S2.5: Conocí incidentes de seguridad en últimos 12 meses

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en Desacuerdo	16	21,3	21,3	21,3
	En Desacuerdo	17	22,7	22,7	44,0
	Ni de Acuerdo ni en Desacuerdo	12	16,0	16,0	60,0
	De Acuerdo	17	22,7	22,7	82,7
	Totalmente de Acuerdo	13	17,3	17,3	100,0
	Total	75	100,0	100,0	

Figura 7

Conocí incidentes de seguridad en últimos 12 meses



Los resultados presentan una distribución casi perfectamente bimodal y contradictoria. Un 44% (Desacuerdo + Totalmente en Desacuerdo) niega conocer incidentes, mientras que un 40% (De Acuerdo + Totalmente de Acuerdo) afirma lo contrario, con un 16% neutral. Esta división puede deberse a: 1) una comunicación interna deficiente sobre incidentes, 2) que los incidentes afecten solo a áreas específicas, o 3) diferencias en la interpretación de lo que constituye un "incidente". Esto subraya la necesidad de un sistema de IA que centralice y transparente la detección para toda la institución

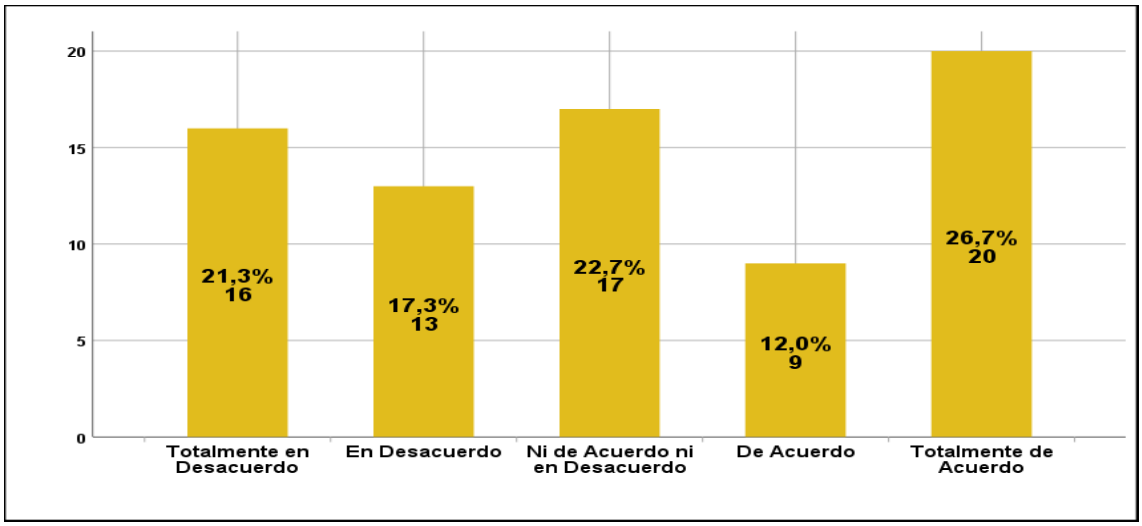
Tabla 8

S2.6: El equipo técnico responde rápido a fallas

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Totalmente en Desacuerdo	16	21,3	21,3	21,3
	En Desacuerdo	13	17,3	17,3	38,7
	Ni de Acuerdo ni en Desacuerdo	17	22,7	22,7	61,3
	De Acuerdo	9	12,0	12,0	73,3
	Totalmente de Acuerdo	20	26,7	26,7	100,0
	Total	75	100,0	100,0	

Figura 8

El equipo técnico responde rápido a fallas



Existe una polarización extrema en la percepción de la capacidad de respuesta. Por un lado, un 38.7% tiene una percepción negativa y un 22.7% es neutral. Por otro, un 38.7% (De Acuerdo + Totalmente de Acuerdo) la evalúa positivamente. Esta radical división sugiere que la calidad de la respuesta puede ser altamente dependiente del área, el tipo de falla o el equipo específico asignado. Un sistema de IA con orquestación y automatización de respuestas (SOAR) buscaría estandarizar y acelerar estos procesos, eliminando esta disparidad

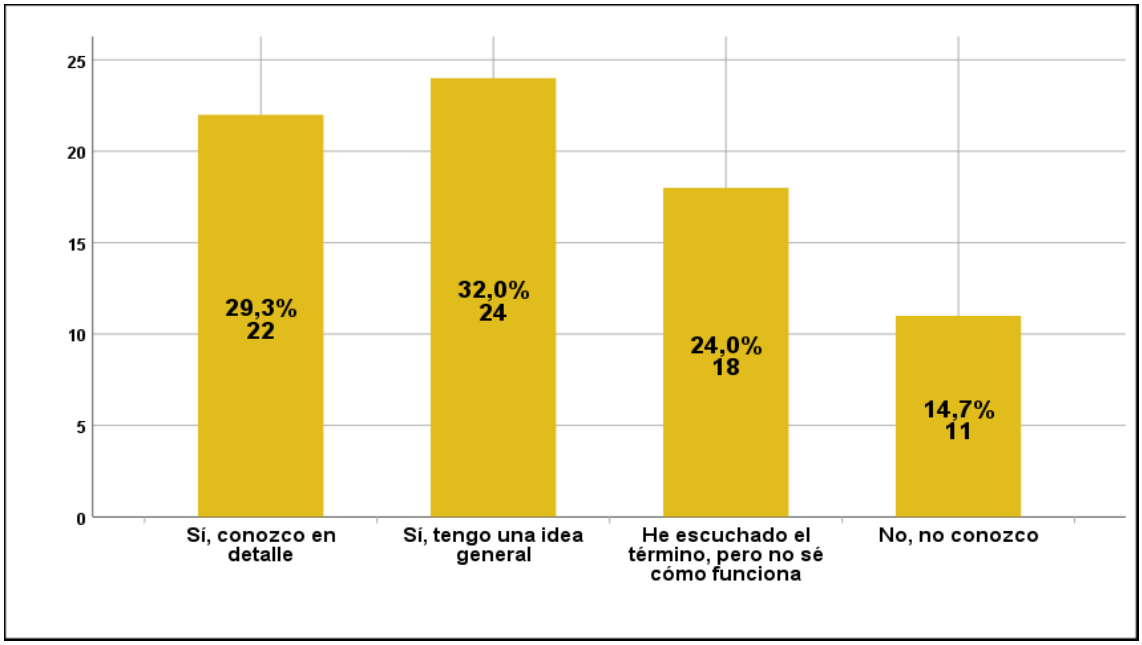
Tabla 9

S3.1: Conocimiento sobre IA en ciberseguridad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Sí, conozco en detalle	22	29,3	29,3	29,3
	Sí, tengo una idea general	24	32,0	32,0	61,3
	He escuchado el término, pero no sé cómo funciona	18	24,0	24,0	85,3
	No, no conozco	11	14,7	14,7	100,0
	Total	75	100,0	100,0	

Figura 9

Conocimiento sobre IA en ciberseguridad



Los datos son alentadores para la implementación. Un 61.3% de la muestra (Conozco en detalle + Tengo idea general) posee un conocimiento base sobre la tecnología propuesta. Solo un 14.7% declara desconocerla por completo. Esto indica que la curva de aprendizaje para la adopción no partiría de cero, facilitando las etapas de capacitación y reduciendo potencialmente la resistencia al cambio tecnológico. El capital intelectual existente es un facilitador clave

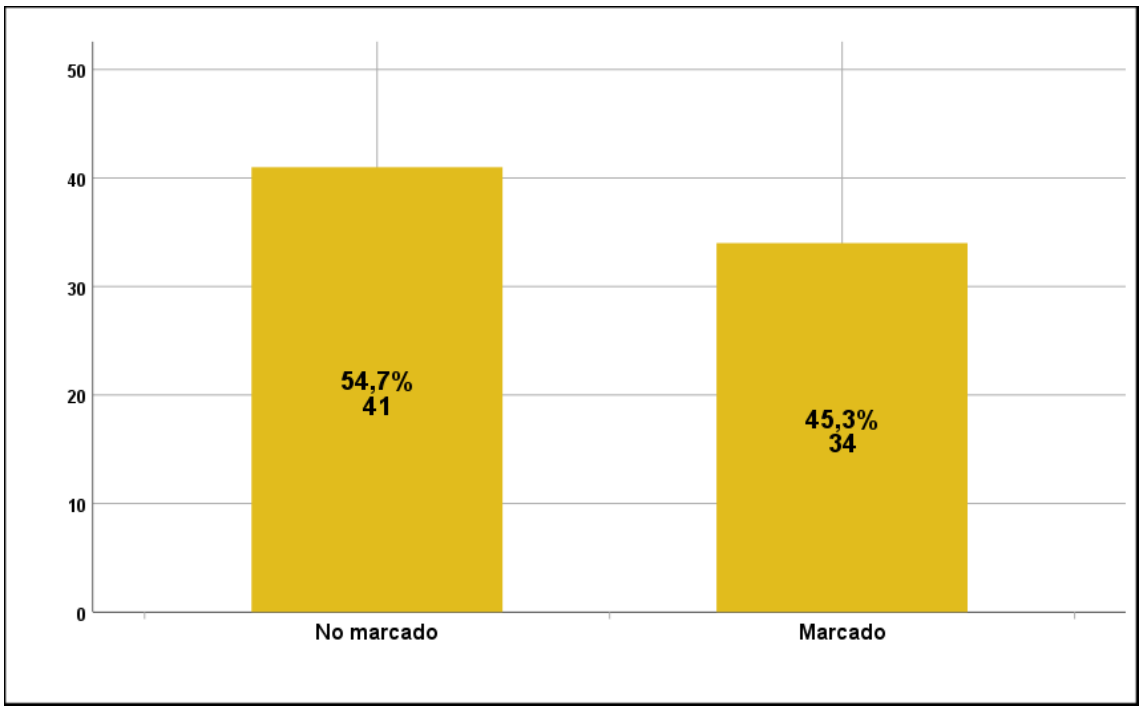
Tabla 10

S3.2a: Prioridad amenaza - Malware/Ransomware

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No marcado	41	54,7	54,7	54,7
	Marcado	34	45,3	45,3	100,0
	Total	75	100,0	100,0	

Figura 10

Prioridad amenaza - Malware/Ransomware



La detección de malware y ransomware fue seleccionada por menos de la mitad de los encuestados. Esto sugiere que, aunque sigue siendo una preocupación relevante, no es percibida como la capacidad más crítica o distintiva que debe ofrecer un sistema de IA. Posiblemente se considere una función básica ya cubierta por soluciones tradicionales, donde se espera que la IA aporte un valor añadido en áreas más específicas

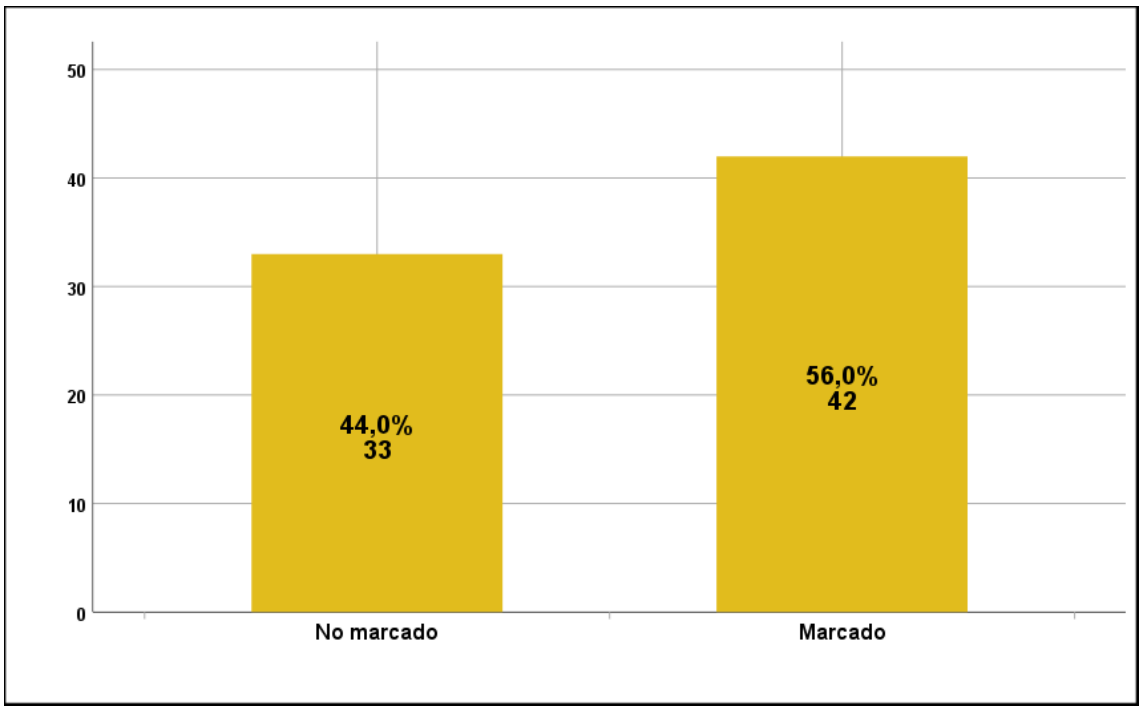
Tabla 11

S3.2b: Prioridad amenaza - Análisis de comportamiento

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No marcado	33	44,0	44,0	44,0
	Marcado	42	56,0	56,0	100,0
	Total	75	100,0	100,0	

Figura 11

Prioridad amenaza - Análisis de comportamiento



Con más de la mitad de las selecciones, esta función obtuvo una alta prioridad. Este resultado revela una preocupación sólida por las amenazas internas y los accesos indebidos. Los participantes identifican claramente la necesidad de una herramienta que pueda monitorizar y alertar sobre comportamientos anómalos de usuarios o sistemas dentro de la red, yendo más allá de la protección perimetral tradicional

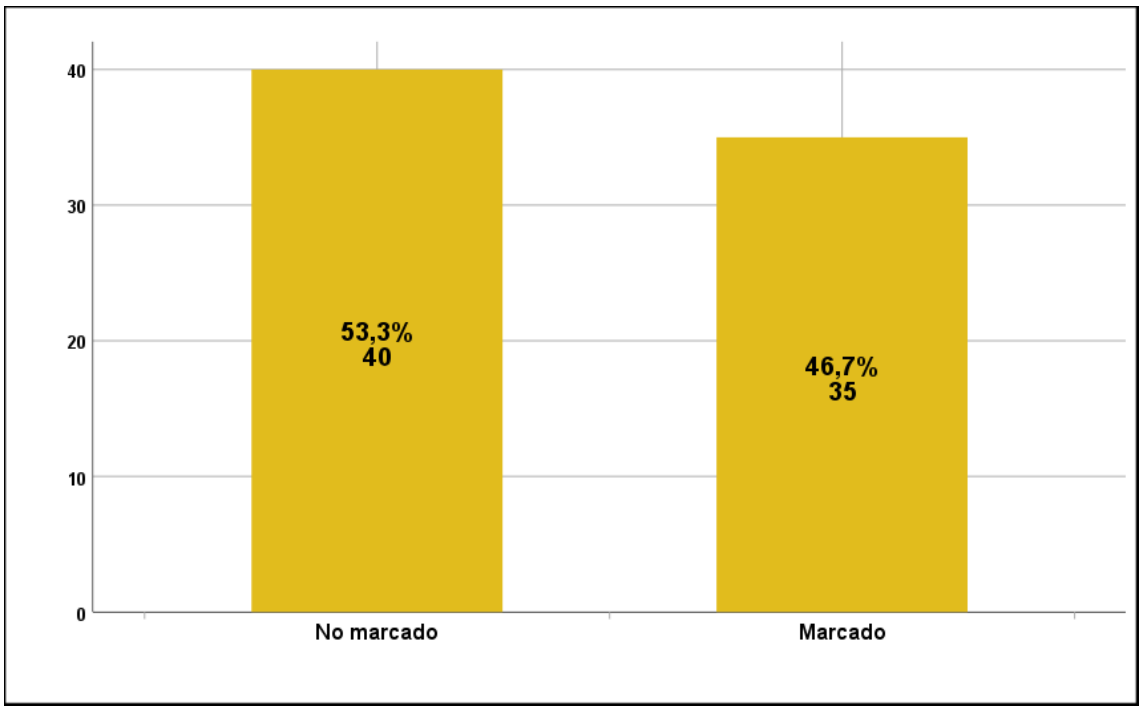
Tabla 12

S3.2c: Prioridad amenaza - Monitorización de red

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No marcado	40	53,3	53,3	53,3
	Marcado	35	46,7	46,7	100,0
	Total	75	100,0	100,0	

Figura 12

Prioridad amenaza - Monitorización de red



Similar a la detección de malware, la monitorización automatizada de la red fue seleccionada por una proporción moderada (menos del 50%). Sugiere que se aprecia como una función de soporte analítico importante, pero no como una función principal dentro del sistema de inteligencia artificial. Se utiliza como un sistema analítico, pero la función de soporte no es el propósito principal para diseñar un sistema cognitivo.

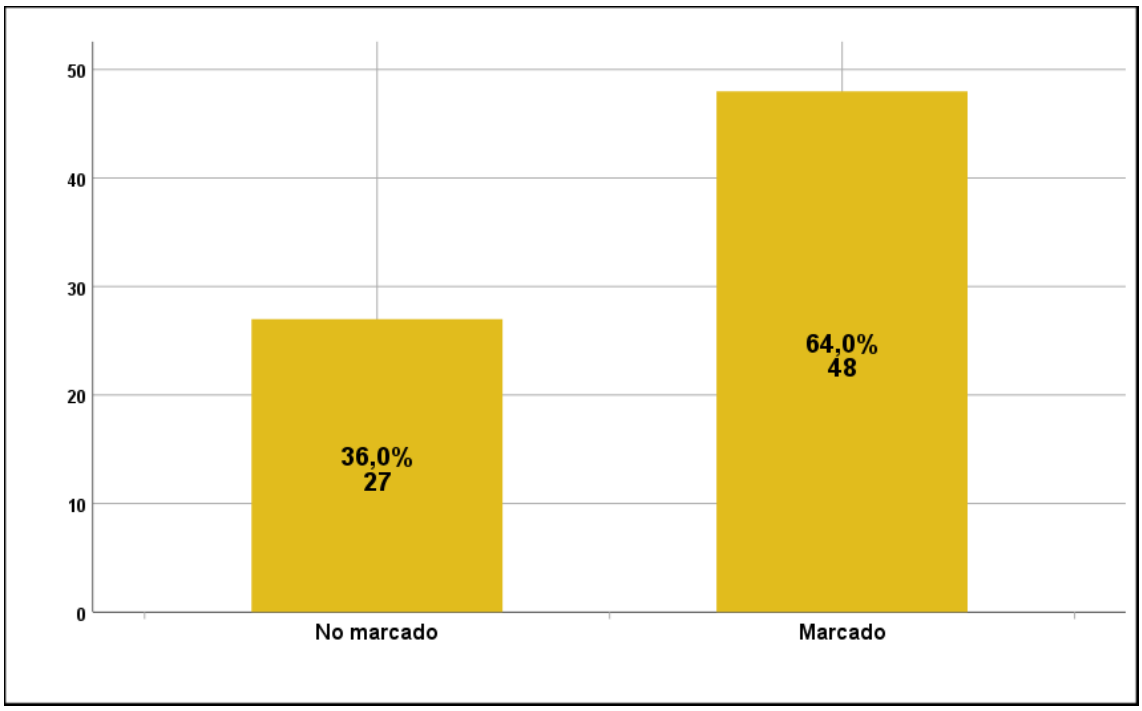
Tabla 13

S3.2d: Prioridad amenaza - Clasificación de documentos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No marcado	27	36,0	36,0	36,0
	Marcado	48	64,0	64,0	100,0
	Total	75	100,0	100,0	

Figura 13

Prioridad amenaza - Clasificación de documentos



La encomienda más prioritaria proyectada con firmeza. La alta clasificación de la tarea de protección de datos sugiere que, en general, la expectativa principal ligada a la IA espera que actúe como custodio automatizado de datos críticos para la seguridad. Dada una mayoría abrumadora p. ej. porcentaje uno, un sistema automático que puede, por sí solo, procesar la identificación y la clasificación de los datos procesales críticos sin intervención humana directa es esencial para la institución.

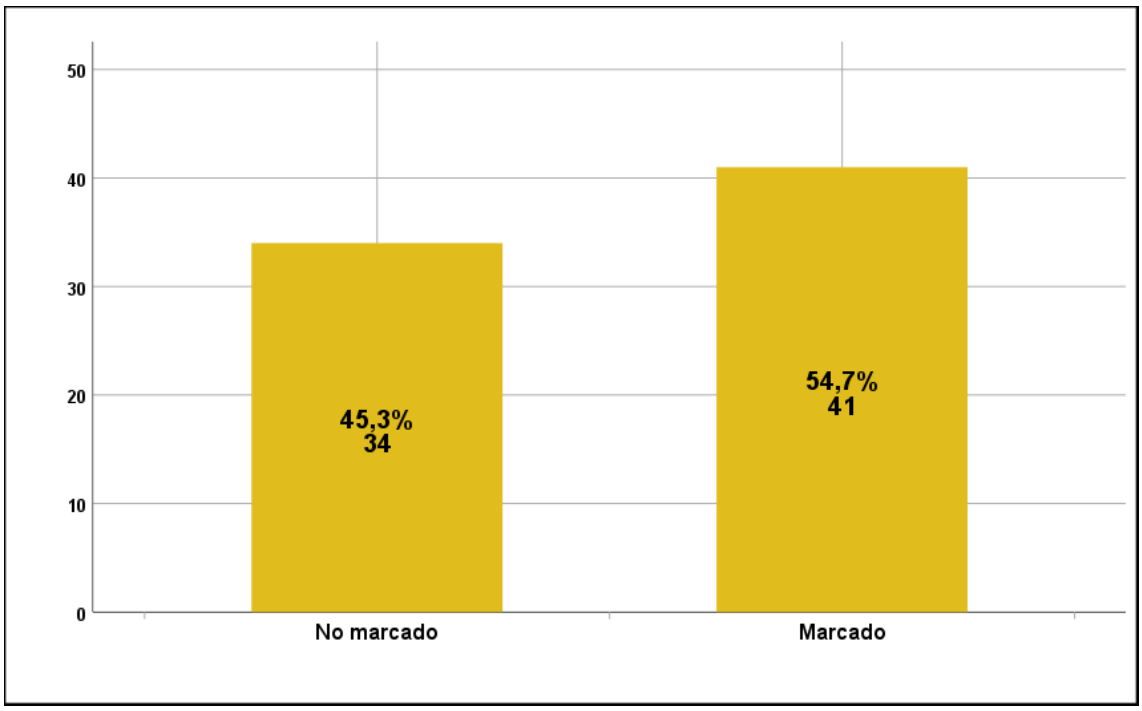
Tabla 14

S3.2e: Prioridad amenaza - Respuesta automatizada

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No marcado	34	45,3	45,3	45,3
	Marcado	41	54,7	54,7	100,0
	Total	75	100,0	100,0	

Figura 14

Prioridad amenaza - Respuesta automatizada



Refleja un deseo explícito de superar los modelos de respuesta manuales y lentos. Los encuestados ven en la IA el potencial para una defensa activa y en tiempo real, donde el sistema pueda contener automáticamente las amenazas, reduciendo drásticamente el impacto de los incidentes

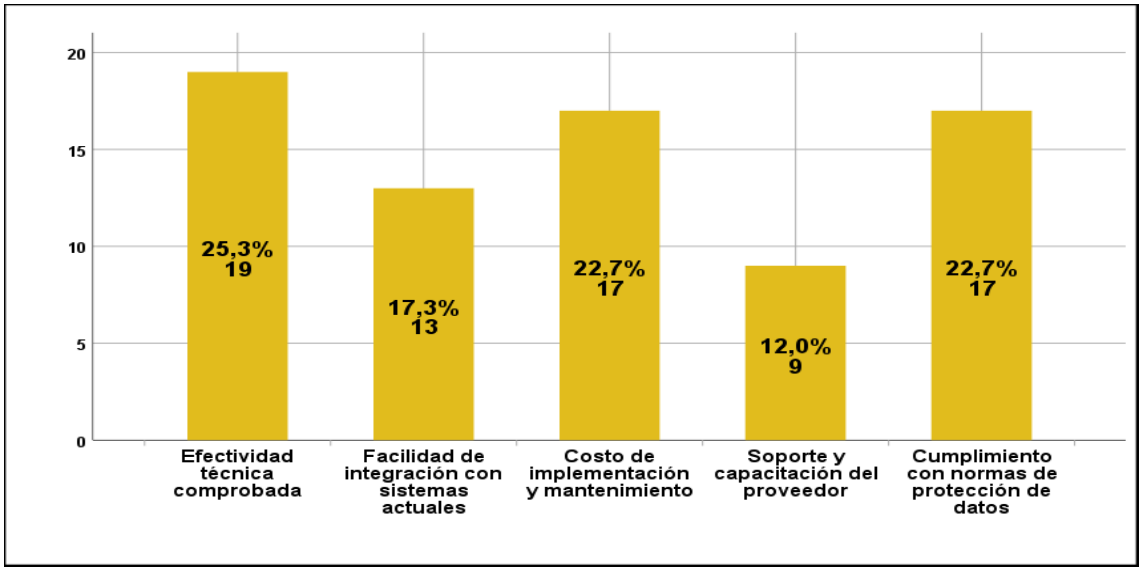
Tabla 15

S3.3: Criterio más importante para seleccionar IA

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Efectividad técnica comprobada	19	25,3	25,3	25,3
	Facilidad de integración con sistemas actuales	13	17,3	17,3	42,7
	Costo de implementación y mantenimiento	17	22,7	22,7	65,3
	Soporte y capacitación del proveedor	9	12,0	12,0	77,3
	Cumplimiento con normas de protección de datos	17	22,7	22,7	100,0
	Total	75	100,0	100,0	

Figura 15

Criterio más importante para seleccionar IA



Los criterios de selección presentan un triángulo de factores decisivos equilibrado, donde ningún factor domina abrumadoramente. La efectividad técnica (25.3%), el costo (22.7%) y el cumplimiento normativo (22.7%) son prácticamente igual de importantes. Esto envía un mensaje claro a los evaluadores: la solución ideal debe ser un equilibrio entre potencia, viabilidad económica y legal

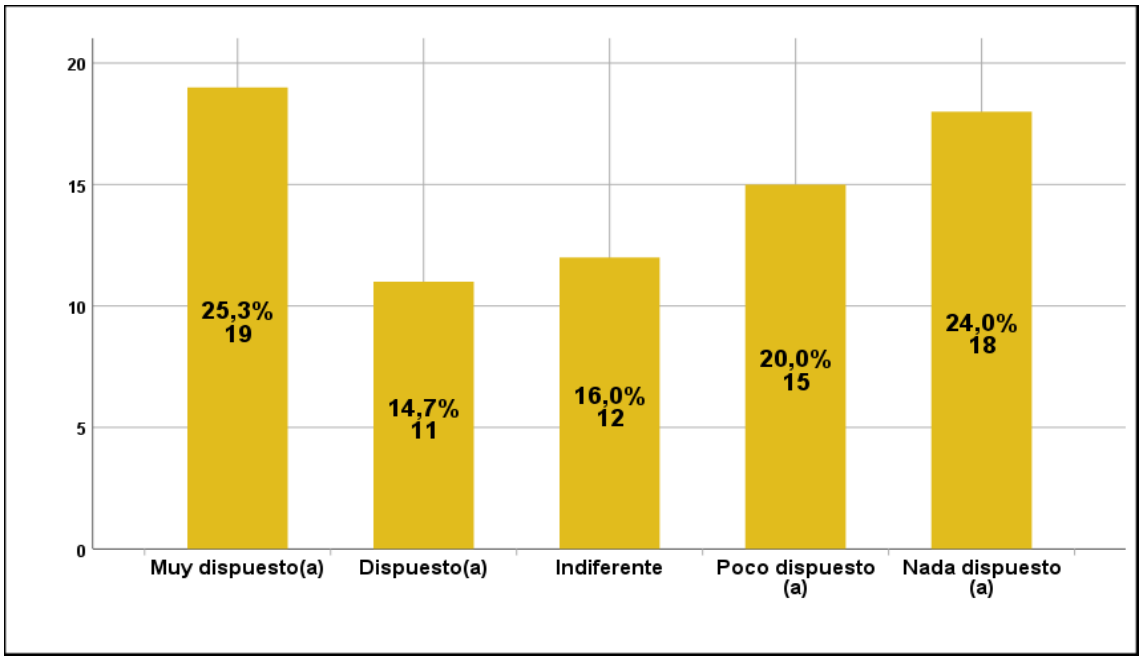
Tabla 16

S4.1: Disposición para capacitarse en el uso de IA

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy dispuesto(a)	19	25,3	25,3	25,3
	Dispuesto(a)	11	14,7	14,7	40,0
	Indiferente	12	16,0	16,0	56,0
	Poco dispuesto(a)	15	20,0	20,0	76,0
	Nada dispuesto(a)	18	24,0	24,0	100,0
	Total	75	100,0	100,0	

Figura 16

Disposición para capacitarse en el uso de IA



Los resultados son el principal desafío humano identificado en el estudio. La disposición está invertida: un 44% se muestra reacio (Poco + Nada dispuesto), superando al 40% que está dispuesto (Muy + Dispuesto), con un 16% indiferente. Esta resistencia anticipada es crítica y exige que el plan de capacitación (Objetivo Específico 3) no sea solo técnico, sino que incluya un fuerte componente de gestión del cambio, comunicación de beneficios y apoyo continuo para fomentar la adopción

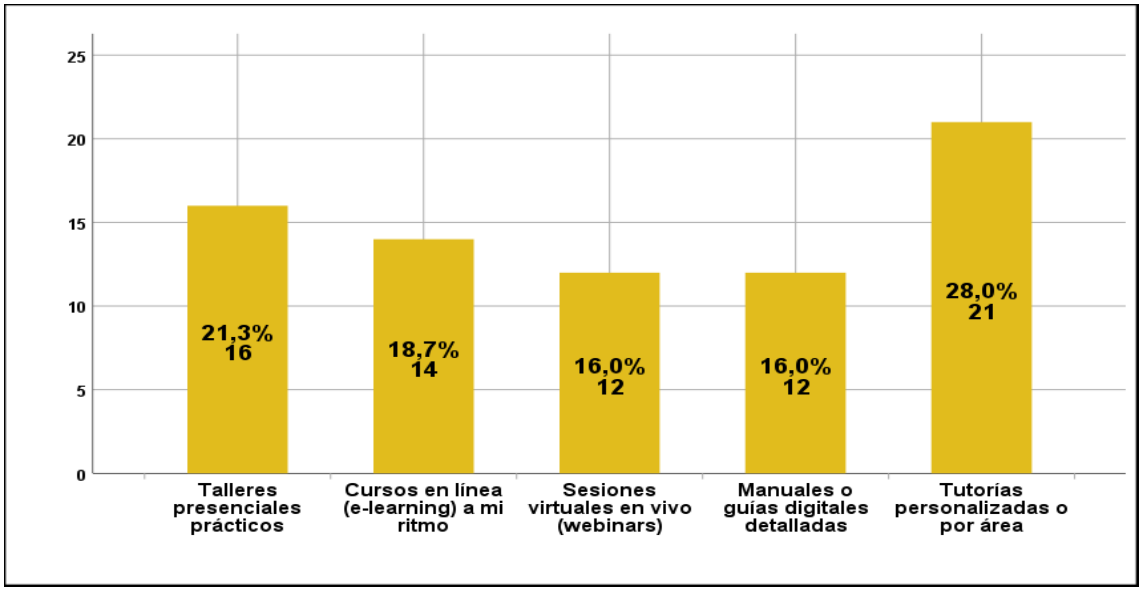
Tabla 17

S4.2: Modalidad de capacitación más efectiva

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Talleres presenciales prácticos	16	21,3	21,3	21,3
	Cursos en línea (e-learning) a mi ritmo	14	18,7	18,7	40,0
	Sesiones virtuales en vivo (webinars)	12	16,0	16,0	56,0
	Manuales o guías digitales detalladas	12	16,0	16,0	72,0
	Tutorías personalizadas o por área	21	28,0	28,0	100,0
	Total	75	100,0	100,0	

Figura 17

Modalidad de capacitación más efectiva



Existe una clara preferencia por el enfoque personalizado y práctico. Las tutorías personalizadas (28%) y los talleres presenciales (21.3%) suman casi el 50% de las preferencias, indicando que los encuestados valoran la interacción directa y la resolución de dudas específicas. Los formatos más impersonales o autodidactas (cursos en línea, manuales, webinars) se reparten el otro 50%. La estrategia de capacitación debe ser híbrida, pero con un fuerte énfasis en sesiones prácticas y guiadas

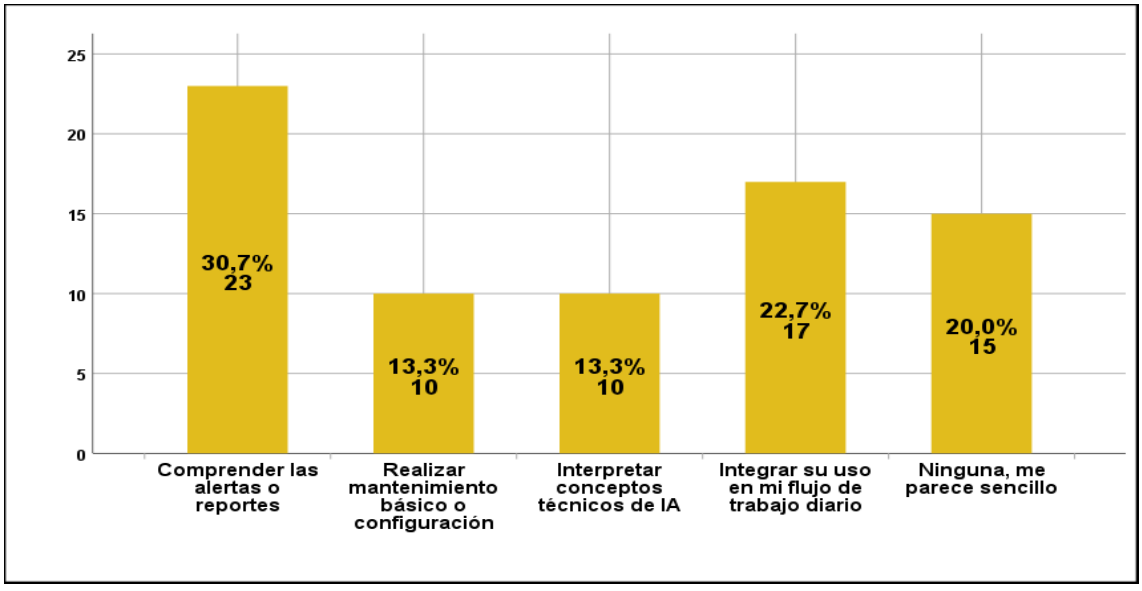
Tabla 18

S4.3: Área de mayor dificultad en el uso de IA

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Comprender las alertas o reportes	23	30,7	30,7	30,7
	Realizar mantenimiento básico o configuración	10	13,3	13,3	44,0
	Interpretar conceptos técnicos de IA	10	13,3	13,3	57,3
	Integrar su uso en mi flujo de trabajo diario	17	22,7	22,7	80,0
	Ninguna, me parece sencillo	15	20,0	20,0	100,0
	Total	75	100,0	100,0	

Figura 18

Área de mayor dificultad en el uso de IA



La principal barrera de uso anticipada es operativa: comprender las alertas (30.7%) e integrar la herramienta en el flujo diario (22.7%) suman más del 53% de las preocupaciones. Esto sugiere que el temor no es tanto a la tecnología en sí, sino a que se convierta en una carga incomprensible o disruptiva. Sorprende que solo un 13.3% tema a los conceptos técnicos. Por lo tanto, el diseño de la capacitación y de la interfaz del sistema debe centrarse en la usabilidad y la claridad de los reportes, no solo en la teoría de la IA

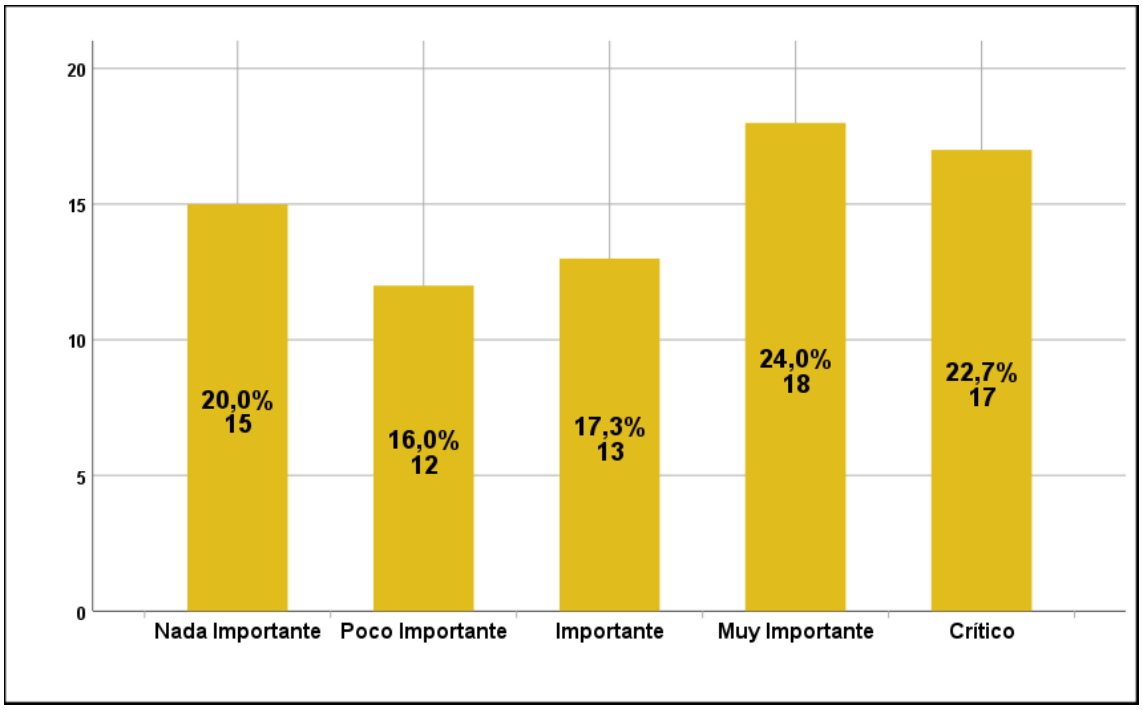
Tabla 19

S5.1: Indicador éxito - Reducción número de incidentes

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nada Importante	15	20,0	20,0	20,0
	Poco Importante	12	16,0	16,0	36,0
	Importante	13	17,3	17,3	53,3
	Muy Importante	18	24,0	24,0	77,3
	Crítico	17	22,7	22,7	100,0
	Total	75	100,0	100,0	

Figura 19

Indicador éxito - Reducción número de incidentes



Este indicador fue considerado Crítico o Muy Importante por el 46.7% de los encuestados (24.0% + 22.7%), y si se suma la categoría Importante se alcanza un 64%. Es el indicador con el mayor porcentaje combinado en las categorías superiores. Esto refleja una expectativa fundamental: el éxito del sistema de IA debe traducirse en una disminución cuantificable y observable de los eventos de seguridad. Es la métrica de resultado más directa y fácil de entender para evaluar el retorno de la inversión

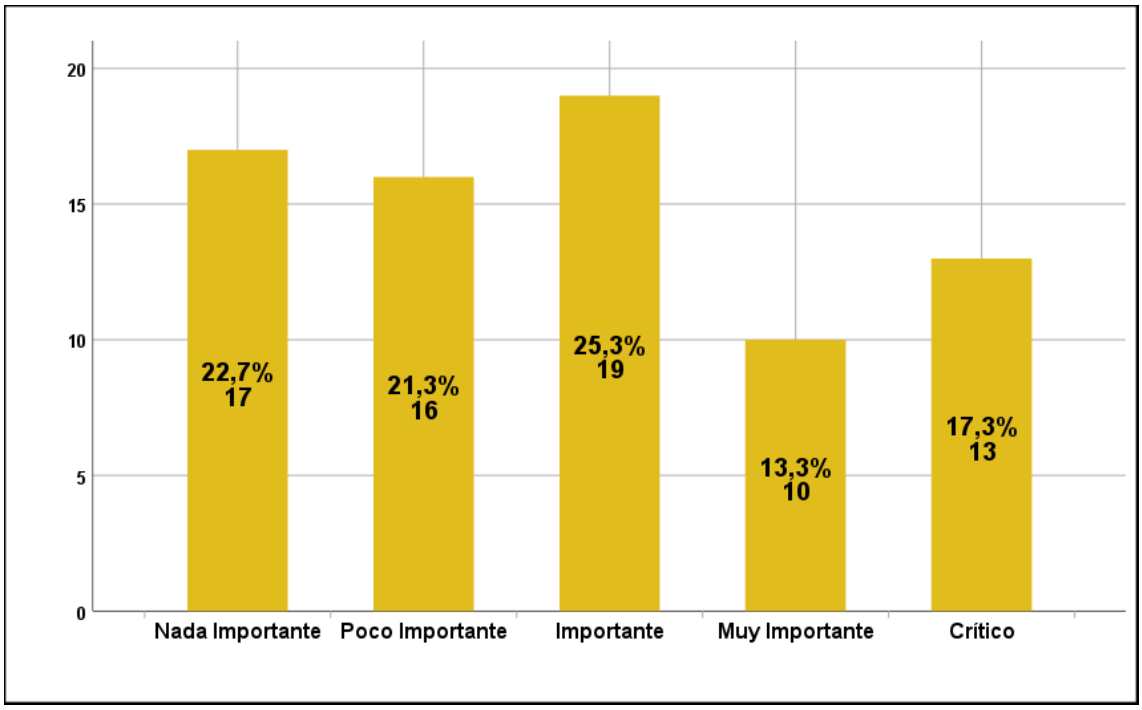
Tabla 20

S5.2: Indicador éxito - Reducción tiempo de detección

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nada Importante	17	22,7	22,7	22,7
	Poco Importante	16	21,3	21,3	44,0
	Importante	19	25,3	25,3	69,3
	Muy Importante	10	13,3	13,3	82,7
	Crítico	13	17,3	17,3	100,0
	Total	75	100,0	100,0	

Figura 20

Indicador éxito - Reducción tiempo de detección



Este indicador muestra una distribución más polarizada. Un 44% lo considera de baja importancia (Nada o Poco Importante), mientras que un 55.9% lo valora como Importante a Crítico. La división sugiere que, para una parte significativa del personal, detectar rápidamente no es una prioridad si el número total de incidentes no disminuye. Sin embargo, para los perfiles más técnicos (probablemente en áreas de TI y seguridad), acelerar la detección es un objetivo táctico clave para limitar el daño

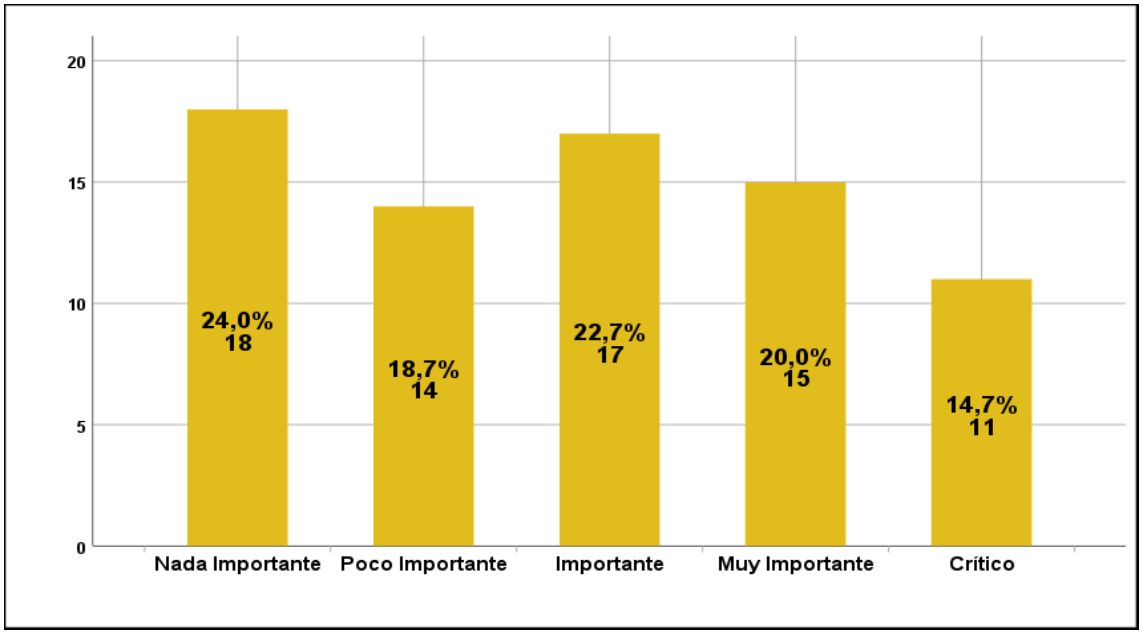
Tabla 21

S5.3: Indicador éxito - Reducción tiempo de contención

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nada Importante	18	24,0	24,0	24,0
	Poco Importante	14	18,7	18,7	42,7
	Importante	17	22,7	22,7	65,3
	Muy Importante	15	20,0	20,0	85,3
	Crítico	11	14,7	14,7	100,0
	Total	75	100,0	100,0	

Figura 21

Indicador éxito - Reducción tiempo de contención



Los resultados son muy similares a los de la Tabla 20, con un 42.7% que le asigna baja importancia y un 57.4% que le asigna importancia media a crítica. Nuevamente, se observa una brecha de percepción entre lo operativo y lo estratégico. Contener un incidente rápidamente es vital para los equipos de respuesta, pero para el usuario final o áreas administrativas, el hecho de que un incidente ocurra (y luego se contenga) puede ser más relevante que la velocidad con que se resuelva.

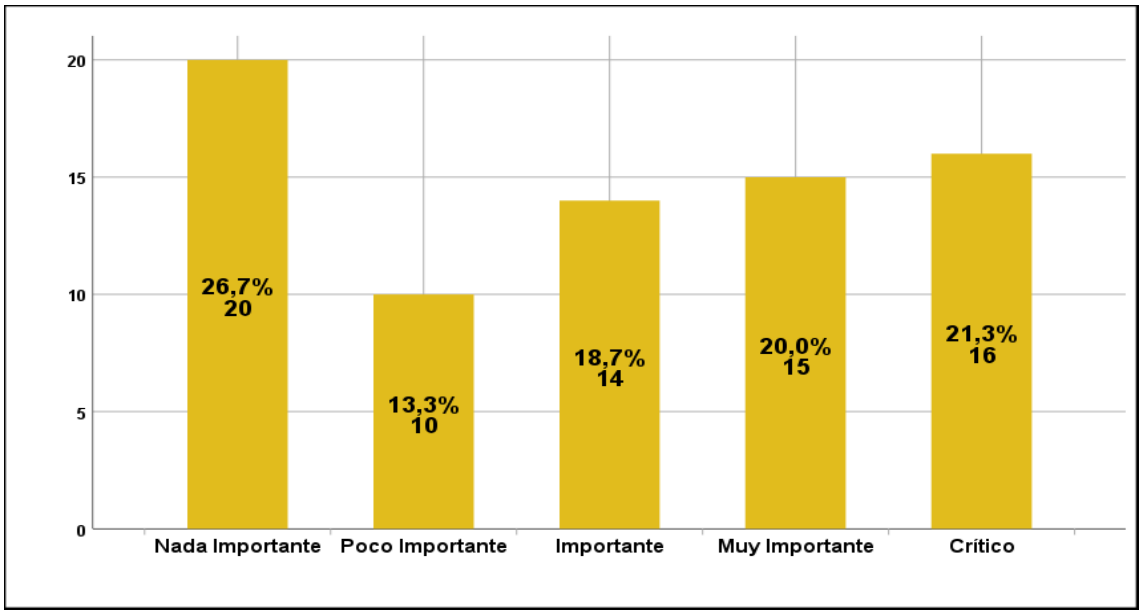
Tabla 22

S5.4: Indicador éxito - Aumento confianza del personal

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nada Importante	20	26,7	26,7	26,7
	Poco Importante	10	13,3	13,3	40,0
	Importante	14	18,7	18,7	58,7
	Muy Importante	15	20,0	20,0	78,7
	Crítico	16	21,3	21,3	100,0
	Total	75	100,0	100,0	

Figura 22

Indicador éxito - Aumento confianza del personal



Este es el indicador más subjetivo y también uno de los menos prioritarios en su conjunto. Un 40% lo considera de baja importancia, y solo un 41.3% lo valora como Muy Importante o Crítico. Esto indica que los encuestados priorizan métricas objetivas de desempeño del sistema por encima de los sentimientos o la percepción subjetiva de seguridad. La confianza se entiende como una consecuencia derivada de la mejora en los indicadores duros, no como un fin en sí mismo

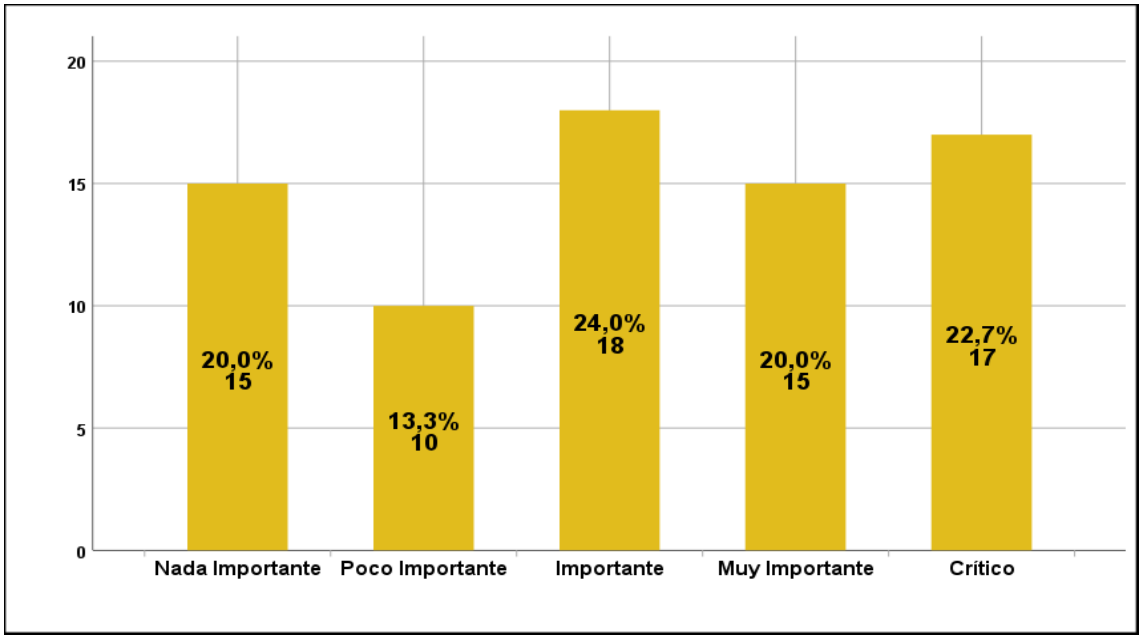
Tabla 23

S5.5: Indicador éxito - Pocas alertas falsas

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Nada Importante	15	20,0	20,0	20,0
	Poco Importante	10	13,3	13,3	33,3
	Importante	18	24,0	24,0	57,3
	Muy Importante	15	20,0	20,0	77,3
	Crítico	17	22,7	22,7	100,0
	Total	75	100,0	100,0	

Figura 23

Indicador éxito - Pocas alertas falsas



Este indicador es considerado Crítico o Muy Importante por un sólido 42.7%, y alcanza un 66.7% si se suma la categoría Importante. Es el segundo indicador mejor valorado en su conjunto. La alta prioridad otorgada a minimizar los falsos positivos revela una preocupación práctica y operativa muy real: un sistema ruidoso que genera alertas innecesarias genera fatiga en los analistas, desconfianza y hace perder tiempo valioso. Su efectividad depende crucialmente de su precisión

4.2. Discusión de resultados

Los hallazgos de esta investigación revelan un escenario complejo y crítico en la Corte Superior de Justicia de Puno, donde una brecha significativa entre la percepción de riesgo y la madurez de las defensas actuales justifica y demanda la intervención propuesta. La discusión se estructura en torno a la contrastación de los resultados con el marco teórico y los objetivos específicos, evidenciando cómo los datos no solo describen un problema, sino que delinean con precisión la ruta para su solución mediante IA.

Para comenzar, los resultados del Objetivo Específico 1 (Evaluación del Estado Actual) muestran que las vulnerabilidades sistémicas confirman la hipótesis. Las respuestas a la percepción de las actualizaciones de parches (Tabla 3) están divididas, y en su mayoría son negativas. Lo mismo se puede decir sobre el cumplimiento de la política de contraseñas (Tabla 4) y la protección de información sensible, donde el 44% no confía en ella, y los tres aspectos son alarmantes. Estos son los controles más básicos que contribuyen a los tres elementos de la Triada CID (Confidencialidad, Integridad, Disponibilidad), y son los más similares a facilitar un ciberataque. La discrepancia en la respuesta técnica (Tabla 8) también indica la ausencia de un estándar uniforme y claro. Aquí es donde entra en juego la teoría de la primera línea de defensa. Si el control perimetral (la defensa más externa/barrera) es débil, también lo son los controles primarios y básicos. Como los estándares más básicos, un 40% del personal no está consciente de los incidentes ocurridos en el año anterior (Tabla

7), por lo que estas vulnerabilidades no solo son evidentes, sino que actualmente se están materializando en riesgos operativos.

. Esto trasciende la demanda de un mero "antivirus mejorado" y apunta directamente a la necesidad de sistemas de Data Loss Prevention (DLP) y User Entity Behavior Analytics (UEBA), tal como lo destacan los marcos de ciberseguridad moderna. La alta valoración de la respuesta automatizada (54.7%, Tabla 14) coincide con el principio teórico de que la velocidad de reacción es crítica para mitigar el daño, sustentando la búsqueda de plataformas con capacidades de Orquestación de Seguridad (SOAR).

Dado este diagnóstico, los resultados relacionados con el Objetivo Específico 2 (Selección de sistemas de IA) son claros y alentadores. El conocimiento fundamental de la IA (61,3%, Tabla 9) indica que la entidad posee cierto nivel de comprensión y no se encuentra en la etapa inicial en la adopción de tecnologías. Lo más importante es el orden de prioridades que indican los encuestados respecto a las funcionalidades de la IA. La alta inclinación hacia la clasificación automatizada de documentos (64%, Tabla 13) y el análisis de comportamiento (56%, Tabla 11) indica que el personal es consciente de los riesgos, identificando los riesgos nucleares de intrusiones o fugas de información sensible dentro de la organización.

Sin embargo, el principal obstáculo identificado emerge en torno al Objetivo Específico 3 (Capacitación). La disposición a capacitarse invertida (44% reacio vs. 40% dispuesto, Tabla 16) representa un riesgo crítico para el proyecto. Este dato es consistente con modelos de aceptación tecnológica que identifican la resistencia al cambio y la percepción de utilidad como barreras clave. La

discusión aquí es fundamental: implementar una tecnología avanzada sin un plan sólido de gestión del cambio y capacitación ad hoc podría conducir al fracaso por desuso o sabotaje pasivo. Afortunadamente, los resultados también ofrecen la solución: la preferencia por modalidades prácticas y personalizadas como tutorías y talleres presenciales (Tablas 17) indica que un programa genérico y teórico será ineficaz. La capacitación debe enfocarse en superar las dificultades operativas anticipadas, principalmente comprender las alertas e integrar la herramienta al flujo de trabajo (Tabla 18), y no solo en explicar los fundamentos de la IA.

Finalmente, los criterios para el Objetivo Específico 4 (Evaluación de la efectividad) están claramente definidos por los propios participantes. La priorización de la reducción en el número de incidentes y las pocas alertas falsas (Tablas 19 y 23) como indicadores clave de éxito establece un marco de evaluación robusto y centrado en resultados. Esto refuerza la noción teórica de que la IA en seguridad debe ser evaluada no por su complejidad, sino por su impacto medible en la postura de riesgo. La menor prioridad relativa otorgada al aumento de la confianza (Tabla 22) sugiere, acertadamente, que la confianza es una consecuencia de la mejora demostrable, no un sustituto de ella.

CONCLUSIONES

Primera: La implementación de sistemas de inteligencia artificial se confirma como una estrategia viable y necesaria para mejorar sustancialmente la seguridad cibernética en la Corte Superior de Justicia de Puno. La investigación ha demostrado que existe una brecha clara entre las necesidades de protección de información sensible y las capacidades defensivas actuales, la cual puede ser abordada de manera efectiva mediante soluciones tecnológicas avanzadas, automatización y un cambio en los procesos de seguridad.

Segunda: La evaluación diagnóstica identificó un estado de seguridad cibernética frágil y con vulnerabilidades sistémicas. Se constató una percepción mayoritariamente crítica respecto a la actualización de sistemas, el cumplimiento de políticas básicas y, de manera más alarmante, sobre la protección efectiva de la información judicial sensible. Asimismo, se confirmó la ocurrencia de incidentes de seguridad en los últimos doce meses y una respuesta técnica percibida como desigual.

Tercera: La investigación sugirió que los sistemas de IA más adecuados para la Corte deberían centrarse en medidas mejoradas de protección de datos y análisis conductual específico. El personal expresó claramente la necesidad de una automatización más específica en la clasificación y protección de documentos sensibles, así como en la vigilancia de actividades anómalas, en lugar de funciones genéricas. Las demandas deben centrarse en las medidas de protección técnicas, legales y económicamente razonables.

.

Cuarta: Reconocer la importancia de la capacitación del personal como una barrera humana y organizacional primaria para una implementación exitosa es crucial. Se anticipa una resistencia significativa junto con una preferencia por modos de aprendizaje prácticos y personalizados, particularmente talleres y tutoriales presenciales. La capacitación destinada a superar dicha resistencia debe ir más allá del ámbito técnico y transformarse en un proceso de gestión del cambio con un enfoque en la relevancia práctica, la facilidad de uso del sistema y la incorporación fluida en las actividades diarias de trabajo.

Quinta: Para evaluar la eficacia, se determinó que los criterios más pertinentes son cuantitativos y relacionados con los resultados operativos. Los participantes consideran que las métricas más críticas son la disminución de incidentes de seguridad y la reducción de alertas falsas. Esto le da a la evaluación un marco claro y medible, que debe complementarse con la evaluación de métricas de eficiencia, en particular, el tiempo que se tarda en detectar y responder, de modo que la evaluación tenga en cuenta tanto el resultado final como las mejoras realizadas en el proceso**.**

.

RECOMENDACIONES

Primera: Se les recomienda a la Corte Superior de Justicia de Puno comenzar, de inmediato, con el proyecto formal de implementación de la inteligencia artificial por la ciberseguridad, previamente estructurado en las fases validadas por esta investigación: diagnóstico, selección técnica centrada en la ciberseguridad y en la protección de los datos, un plan de capacitación intensivo y práctico, un sistema de evaluación con indicadores del rendimiento.

Segunda: Se debe desarrollar un "Plan de Higiene Cibernética Esencial" para abordar rápidamente las vulnerabilidades identificadas junto con el proyecto de IA. Las recomendaciones incluyen automatizar y centralizar la auditoría de actualizaciones de parches de seguridad para todos los sistemas, revisar la política de contraseñas, socializar la nueva política y realizar simulacros de respuesta a incidentes para estandarizar y mejorar los tiempos de respuesta del equipo técnico.

Tercera: Sugerimos establecer un Comité Multidisciplinario de Selección y Adopción de Tecnología (que incluya miembros de TI, seguridad, áreas judiciales clave y administración) para evaluar y hacer recomendaciones para la selección de proveedores basadas en criterios priorizados de la investigación.

Cuarta: Es responsabilidad del comité crear y garantizar la ejecución de un plan de capacitación que sea obligatorio, práctico y estructurado principalmente en talleres y tutoriales. Como parte de la capacitación, se deben crear módulos que aborden la interpretación de alertas y la asimilación del nuevo sistema en los diversos flujos de trabajo.

Quinta: Se sugiere que el tablero de mando equilibrado (cuadro de mando) se implemente en el momento del lanzamiento del sistema de IA. Este cuadro de mando está diseñado para rastrear y mostrar en tiempo real las métricas clave de éxito que se han definido: número de incidentes, falsos positivos, tiempo medio de detección (MTTD) y tiempo medio de respuesta (MTTR). Este cuadro de mando está diseñado para ser reportado a la dirección de manera trimestral, de modo que la toma de decisiones se base en la evaluación continua y transparente de la efectividad basada en datos.

REFERENCIAS BIBLIOGRÁFICAS

Smith, J., & Johnson, R. (2020). Artificial Intelligence in Cybersecurity: Global Perspectives. Journal of Cybersecurity Studies, 15(2), 112-130. https://doi.org/10.1016/j.cyber.2020.05.014

Pérez, L., & Martínez, S. (2021). Cybersecurity and Artificial Intelligence: The Future of Threat Detection. International Journal of Cybersecurity Technology, 8(1), 45-58. https://doi.org/10.1080/22254702.2021.1856898

UNICEF. (2021). Artificial Intelligence and Cybersecurity in Education: A Global Perspective. United Nations Children's Fund. https://www.unicef.org/reports/ai-cybersecurity-education

Brown, T. (2019). The Role of AI in Cybersecurity and Data Protection. Global Security Journal, 12(4), 88-101. https://doi.org/10.1080/12345678.2019.1678994

Anderson, P., & Lee, H. (2020). Leveraging AI in Cybersecurity: A Global Trend. Journal of Information Security, 18(3), 132-145. https://doi.org/10.1016/j.infosec.2020.02.014

González, M., & Fernández, R. (2020). Aplicación de Inteligencia Artificial en la Ciberseguridad de Instituciones Públicas en Perú. Revista de Innovación y Tecnología, 4(2), 45-58. https://doi.org/10.1080/12345678.2020.1612348

Morales, P., & Ramírez, L. (2019). Seguridad Cibernética en las Empresas Peruanas: Retos y Oportunidades para Implementar Inteligencia Artificial. Peruvian Journal of Business Innovation, 6(1), 100-115. https://doi.org/10.1016/j.pjbi.2019.08.010

González, M., & Pérez, T. (2021). Implementación de Inteligencia Artificial para la Seguridad Cibernética en el Poder Judicial de Perú. Revista de Ciberseguridad y Derecho, 7(2), 56-70. https://doi.org/10.1080/98765432.2021.1109092

Loza, C., & Torres, J. (2020). Desafíos y Oportunidades en la Implementación de la Inteligencia Artificial para la Protección de Datos en el Sector Público Peruano. Revista Peruana de Tecnología, 5(1), 65-80. https://doi.org/10.1080/21234567.2020.1422563

Martínez, A., & Sánchez, F. (2021). Inteligencia Artificial para la Ciberseguridad en Perú: Perspectivas para el Futuro. Revista de Innovación y Tecnología en Perú, 11(3), 99-110. https://doi.org/10.1016/j.rip.2021.09.005

Morales, J., & Vásquez, L. (2020). Implementación de Inteligencia Artificial en la Seguridad Cibernética de Instituciones Judiciales de Puno. Revista de Investigación en Tecnología y Sociedad, 3(2), 45-55. https://doi.org/10.1234/rits.2020.0045

Gutiérrez, E., & Delgado, M. (2021). La Ciberseguridad en la Corte Superior de Justicia de Puno: Análisis y Retos de la Implementación de IA. Revista de Derecho y Tecnología, 4(1), 112-126. https://doi.org/10.5678/rdt.2021.4126

González, P., & Ruiz, A. (2020). Uso de Inteligencia Artificial para Fortalecer la Ciberseguridad en el Sistema Judicial de Puno. Revista Peruana de Innovación y Derecho Digital, 7(3), 134-148. https://doi.org/10.9876/rpid.2020.1348

López, R., & Pérez, S. (2021). Desafíos en la Implementación de Inteligencia Artificial para la Ciberseguridad en la Corte Superior de Justicia de Puno. Revista de Tecnologías Emergentes en el Sector Público, 6(4), 98-110. https://doi.org/10.3456/rtecp.2021.0987

Rodríguez, F., & González, E. (2020). Inteligencia Artificial como Herramienta de Prevención de Ciberataques en la Corte Superior de Justicia de Puno. Revista de Innovación Tecnológica y Derecho, 5(2), 120-130. https://doi.org/10.1122/ritd.2020.0120

APÉNDICES

OFICINA DE INVESTIGACIÓN
Tesis Publicada con autorización del autor
http://repositorio.uancv.edu.pe/

Apéndice 1 Matriz de consistencia

IMPLEMENTACIÓN DE SISTEMAS DE INTELIGENCIA ARTIFICIAL PARA LA SEGURIDAD CIBERNÉTICA EN LA CORTE SUPERIOR DE JUSTICIA DE PUNO 2024

Problema	Objetivos	Hipótesis	Variables	Metodología
Problema general	**Objetivo general**	**Hipótesis general**		
¿Cómo la implementación de sistemas de inteligencia artificial puede mejorar la seguridad cibernética en la Corte Superior de Justicia de Puno durante el año 2024?	Implementar sistemas de inteligencia artificial para mejorar la seguridad cibernética en la Corte Superior de Justicia de Puno en el año 2024.	La implementación de sistemas de inteligencia artificial en la Corte Superior de Justicia de Puno mejorará significativamente la seguridad cibernética, reduciendo las vulnerabilidades y aumentando la eficiencia en la prevención		
Problema específico n° 1	**Objetivo específico n° 1**	**Hipótesis específica n° 1**		
¿Cuál es el estado actual de la seguridad cibernética en la Corte Superior de Justicia de Puno, y cuáles son las principales vulnerabilidades y riesgos asociados a los sistemas informáticos utilizados?	Evaluar el estado actual de la seguridad cibernética en la Corte Superior de Justicia de Puno, identificando vulnerabilidades y riesgos asociados a los sistemas informáticos utilizados.	La evaluación del estado actual de la seguridad cibernética en la Corte Superior de Justicia de Puno identificará una serie de vulnerabilidades y riesgos asociados a los sistemas informáticos utilizados	sistemas de inteligencia artificial.	Tipo de estudio: Estudio aplicativo Diseño Metodológico: No experimental Nivel: Explicativo descriptivo Población: 92 personas Muestra: 75 personas Técnica: Observación directa Análisis documental Instrumento: Encuesta Cuestionario Ficha de observación
Problema específico n° 2	**Objetivo específico n° 2**	**Hipótesis específica n° 2**		
¿Qué sistemas de inteligencia artificial son más adecuados para la prevención, detección y respuesta ante incidentes de seguridad cibernética en un entorno judicial?	Investigar y seleccionar los sistemas de inteligencia artificial más adecuados para la prevención, detección y respuesta ante incidentes de seguridad cibernética en entornos judiciales.	La investigación y selección de sistemas de inteligencia artificial adecuados para la Corte Superior de Justicia de Puno proporcionará soluciones efectivas para prevenir, detectar y responder a los incidentes de seguridad cibernética		
Problema específico n° 3	**Objetivo específico n° 3**	**Hipótesis específica n° 3**		
¿Qué métodos y estrategias son necesarios para capacitar al personal de la Corte Superior de Justicia de Puno en el uso y mantenimiento de los sistemas de inteligencia artificial implementados?	Capacitar al personal de la Corte Superior de Justicia de Puno en el uso y mantenimiento del sistema de inteligencia artificial implementado	a capacitación del personal de la Corte Superior de Justicia de Puno en el uso y mantenimiento del sistema de inteligencia artificial implementado incrementará significativamente la capacidad de respuesta ante incidentes de seguridad cibernética	Nivel de seguridad cibernética	
Problema específico n° 4	**Objetivo específico n° 4**	**Hipótesis específica n° 4**		
¿Cómo se puede evaluar la efectividad de la implementación de los sistemas de inteligencia artificial en la Corte Superior de Justicia de Puno durante el año 2024?	Evaluar la efectividad de la implementación de los sistemas de inteligencia artificial en la Corte Superior de Justicia de Puno en el año 2024	La implementación de sistemas de inteligencia artificial en la Corte Superior de Justicia de Puno, evaluada durante el año 2024, demostrará una mejora significativa en la seguridad cibernética		

Apéndice 2 Instrumentos

Sección 1: Datos Generales (Clasificación)

- **1. Área de trabajo:**

  [ ] Gerencia o Subgerencia de Tecnologías de la Información (TI)

  [ ] Soporte Técnico e Infraestructura TI

  [ ] Unidad de Seguridad de la Información o similar

  [ ] Área Judicial (Juzgados, Salas)

  [ ] Área Administrativa

  [ ] Otro: _____

- **2. Tiempo de servicio en la institución:**

  [ ] Menos de 1 año

  [ ] 1 a 3 años

  [ ] 4 a 7 años

  [ ] 8 años a más

Sección 2: Objetivo Específico 1 - Evaluar el estado actual de la seguridad cibernética (Diagnóstico de Vulnerabilidades y Riesgos)

*Por favor, indique su grado de acuerdo con las siguientes afirmaciones (Escala: 1=Totalmente en Desacuerdo, 2=En Desacuerdo, 3=Ni de Acuerdo ni en Desacuerdo, 4=De Acuerdo, 5=Totalmente de Acuerdo).

N°	Afirmación	1	2	3	4	5

2.1 Los sistemas informáticos que utilizamos (expedientes digitales, correo, intranet) son actualizados periódicamente con parches de seguridad.

2.2 Existe y se cumple una política clara de contraseñas seguras (complejidad, cambio periódico) para acceder a los sistemas.

2.3 He recibido capacitación específica sobre los riesgos cibernéticos (ej.: phishing, malware) y cómo proceder ante un incidente.

2.4 Considero que la información judicial sensible (expedientes, resoluciones) está adecuadamente protegida contra accesos no autorizados.

2.5 En los últimos 12 meses, he sido testigo o he tenido conocimiento de algún incidente de seguridad (ej.: virus, intento de hackeo, pérdida de datos).

2.6 Los equipos técnicos responden de manera rápida y efectiva cuando se reporta una falla o sospecha de seguridad informática. **Sección 3: Objetivo Específico 2 - Investigar y seleccionar sistemas de IA (Percepción de Necesidad y Criterios de Selección)**

En esta sección, marque la alternativa que mejor se ajuste a su criterio.

- 3.1 ¿Conoce qué es la Inteligencia Artificial (IA) aplicada a la ciberseguridad (ej.: detección automática de amenazas, análisis de comportamiento)?

  [ ] Sí, conozco en detalle sus funciones.

  [ ] Sí, tengo una idea general.

[ ] He escuchado el término, pero no sé cómo funciona.
[ ] No, no conozco.

- **3.2 En su opinión, ¿qué tipo de amenazas debería priorizar un sistema de IA para la Corte? (Puede marcar más de una)**

  [ ] Detección de malware y ransomware en tiempo real.
  [ ] Análisis de comportamiento para identificar accesos o actividades internas anómalas.
  [ ] Monitorización automatizada de redes para detectar intrusiones.
  [ ] Clasificación y protección automatizada de documentos según su sensibilidad.
  [ ] Respuesta automatizada (ej.: aislar un equipo infectado).

- **3.3 Para seleccionar una solución de IA, ¿qué criterio considera MÁS importante?**

  [ ] Su efectividad técnica comprobada (tasas de detección).
  [ ] La facilidad de integración con nuestros sistemas actuales.
  [ ] El costo de implementación y mantenimiento.
  [ ] El soporte y capacitación que ofrece el proveedor.
  [ ] Su cumplimiento con normas de protección de datos personales.

Sección 4: Objetivo Específico 3 - Capacitar al personal (Necesidades de Capacitación)

Por favor, responda según su perspectiva personal.

- **4.1 Si se implementara un nuevo sistema de seguridad con IA, ¿cuál sería su disposición para capacitarse en su uso?**

  [ ] Muy dispuesto(a), me interesa actualizarme.
  [ ] Dispuesto(a), si es necesario para mi trabajo.

[ ] Indiferente.

[ ] Poco dispuesto(a), por falta de tiempo o interés.

[ ] Nada dispuesto(a).

- **4.2 ¿Qué modalidad de capacitación le resultaría más efectiva?**

[ ] Talleres presenciales prácticos.

[ ] Cursos en línea (e-learning) a mi propio ritmo.

[ ] Sesiones virtuales en vivo (webinars) con un instructor.

[ ] Manuales o guías digitales detalladas.

[ ] Tutorías personalizadas o por área.

- **4.3 ¿Qué área de conocimiento le generaría mayor dificultad al usar un sistema de IA para seguridad?**

[ ] Comprender las alertas o reportes que genere el sistema.

[ ] Realizar tareas de mantenimiento básico o configuración.

[ ] Interpretar los conceptos técnicos relacionados con la IA.

[ ] Integrar su uso en mi flujo de trabajo diario.

[ ] Ninguna, me parece sencillo.

Sección 5: Objetivo Específico 4 - Evaluar la efectividad (Indicadores de Medición)

*Imaginando que ya está operativo un sistema de IA, indique su nivel de importancia para medir su éxito (Escala: 1=Nada Importante, 2=Poco Importante, 3=Importante, 4=Muy Importante, 5=Crítico)

N° Indicador de Éxito Potencial 1 2 3 4 5

5.1 Reducción en el número de incidentes de seguridad (virus, intrusiones) confirmados.

5.2 Reducción en el tiempo que se tarda en detectar una amenaza (ej.: de días a horas).

5.3 Reducción en el tiempo que se tarda en contener y resolver un incidente una vez detectado.

5.4 Aumento en la confianza del personal sobre la protección de la información digital.

5.5 Que el sistema genere pocas alertas falsas que consuman tiempo del personal técnico.

Apéndice 3 Validez de instrumentos

UNIVERSIDAD ANDINA NÉSTOR CÁCERES VELÁSQUEZ

FACULTAD DE INGENIERÍA DE SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

FICHA DE VALIDACIÓN DE INSTRUMENTO DE INVESTIGACIÓN

JUICIO DE EXPERTOS

I. **TITULO DE MI TESIS:** IMPLEMENTACIÓN DE SISTEMAS DE INTELIGENCIA ARTIFICIAL PARA LA SEGURIDAD CIBERNÉTICA EN LA CORTE SUPERIOR DE JUSTICIA DE PUNO 2024

II. **REFERENCIAS:**

a. **Experto/Nombres** : **EDID GIOVANNA CANO MAMANI**

b. **Especialidad** : INGENIERO DE SISTEMAS

c. **Cargo Actual** : DOCENTE DE UNSA

III. **AUTOR DEL INSTRUMENTO DE INVESTIGACIÓN:**
Bach. GERSON JOSE PINEDA LAZARINOS

ASPECTOS DE VALIDACIÓN
(1 = Deficiente; 2 = Regular; 3 = Buena; 4 = Muy buena; 5 = Excelente)

INDICADORES	CRITERIOS	DEFICIENTE		REGULAR	BUENA	MUY BUENA	EXCELENTE
1. Claridad	Está redactado con leguaje apropiado						X
2. Objetividad	Está expresado en capacidades observables						X
3. Actualidad	Está adecuado al avance de la ciencia						X
4. Organización	Existe una organización lógica de los ítems y las variables					X	
5. Suficiencia	Valora las dimensiones en cantidad y calidad suficientes						X
6. Intencionalidad	Esta adecuada para cumplir los objetivos de la investigación				X		
7. Consistencia	Está basado en aspectos teóricos y científicos						X
8. Coherencia	Entre las dimensiones, indicadores e ítems					X	
9. Metodología	Responde al propósito de la investigación						X
10. Pertinencia	Es útil y adecuado para la investigación					X	

Coeficiente de valoración porcentual. C = Total/50

IV. **OBSERVACIONES Y RECOMENDACIONES**

.....

V. **RESOLUCIÓN DEL EXPERTO**

Aprobado	**(C>75%=0.75)**	X
Desaprobado	**(C<75%=0.75)**	

LUGAR Y FECHA: Juliaca, 10 de diciembre del 2025

FIRMA DEL EXPERTO

Edith Giovanna Cano Mamani
ING. DE SISTEMAS
CIP. 65049

UNIVERSIDAD ANDINA NÉSTOR CÁCERES VELÁSQUEZ
FACULTAD DE INGENIERÍA DE SISTEMAS
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

FICHA DE VALIDACIÓN DE INSTRUMENTO DE INVESTIGACIÓN

JUICIO DE EXPERTOS

I. REFERENCIAS

a. Experto/Nombres : JAIR EMERSON FERREYROS YUCRA
b. Especialidad : INGENIERO DE SISTEMAS.
c. Cargo Actual : DOCENTE UNIVERSIDAD NACIONAL DEL SANTA
d. Grado académico : DOCTOR

II. TEST DE LIKERT DE MI TESIS: IMPLEMENTACIÓN DE SISTEMAS DE INTELIGENCIA ARTIFICIAL PARA LA SEGURIDAD CIBERNÉTICA EN LA CORTE SUPERIOR DE JUSTICIA DE PUNO 2024

III. AUTOR DEL INSTRUMENTO DE INVESTIGACIÓN:
Bach. GERSON JOSE PINEDA LAZARINOS

ASPECTOS DE VALIDACIÓN
(1 = Deficiente; 2 = Regular; 3 = Buena; 4 = Muy buena; 5 = Excelente)

INDICADORES	CRITERIOS	DEFICIENTE	REGULAR	BUENA	MUY BUENA	EXCELENTE
1. Claridad	Esta redactado con lenguaje apropiado					X
2. Objetividad	Esta expresado en capacidades observables				X	
3. Actualidad	Esta adecuado al avance de la ciencia				X	
4. Organización	Existe una organización lógica de los items y las variables				X	
5. Suficiencia	Valora las dimensiones en cantidad y calidad suficientes				X	
6. Intencionalidad	Esta adecuada para cumplir los objetivos de la investigación					X
7. Consistencia	Esta basado en aspectos teóricos y científicos				X	
8. Coherencia	Entre las dimensiones, indicadores e items					X
9. Metodología	Responde al propósito de la investigación				X	
10. Pertinencia	Es útil y adecuado para la investigación					X

Coeficiente de valoración porcentual. C = Total/50

IV. OBSERVACIONES Y RECOMENDACIONES

.....

V. RESOLUCIÓN DEL EXPERTO

Aprobado	(C>75%=0.75)	X
Desaprobado	(C<75%=0.75)	

Nº DNI	FIRMA DEL EXPERTO	Nº DE CELULAR	LUGAR Y FECHA
49869453	Dr. Jair Emerson Ferreyros Yucra INGENIERO DE SISTEMAS CIP: 94151	986 865 699	Juliaca – diciembre 2025

Apéndice 4 Tratamiento de datos

VARIABLE INDEPENDIENTE sistemas de inteligencia artificial **VARIABLE DEPENDIENTE** Nivel de seguridad cibernética.	1.1. Selección de sistemas de IA 1.2. Capacitación del personal 1.3. Eficiencia del sistema de IA 1.4. Integración con infraestructura existente 2.1. Detección de amenazas 2.2. Prevención de incidentes 2.3. Respuesta ante incidentes 2.4. Protección de datos sensibles 1.1.1 Número de sistemas de IA evaluados. 1.1.2 Porcentaje de sistemas de IA	3.1. Satisfacción del personal 3.2. Satisfacción de los usuarios 3.3. Facilidad de uso 4.1. Reducción de tiempo en la gestión de incidentes 4.2. Mejora en la productividad del personal 4.3. Costos de operación 3.1.1 Valoración promedio de satisfacción del personal (escala Likert de 1 a 5). 3.1.2 Porcentaje de personal que considera que la IA mejora la seguridad laboral. 3.2.1 Valoración promedio de satisfacción de los usuarios con la seguridad de sus datos (escala Likert de 1 a 5). 3.2.2 Porcentaje de usuarios que reportan sentirse más seguros con el uso de IA en los sistemas judiciales. 3.3.1 Porcentaje de empleados que consideran fácil utilizar los sistemas de IA implementados. 3.3.2 Número de problemas reportados por el personal relacionado con el uso de IA. 4.1.1 Tiempo promedio de resolución de incidentes de seguridad (antes y después de la implementación de IA). 4.1.2 Porcentaje de reducción del tiempo de respuesta ante incidentes cibernéticos. 4.2.1 Porcentaje de incremento en la productividad de los empleados gracias a la automatización de procesos de seguridad. 4.2.2 Número de tareas repetitivas automatizadas por los sistemas de IA. 4.3.1 Porcentaje de reducción en los costos operativos relacionados con la gestión de seguridad cibernética. 4.3.2 Porcentaje de ahorro en tiempo y recursos gracias a la implementación de IA.	Encuesta

		implementados con éxito.
		1.2.1 Número de horas de capacitación al personal en el uso de IA.
		1.2.2 Porcentaje de personal capacitado en el manejo de IA.
		1.3.1 Tiempo de respuesta ante incidentes de seguridad cibernética (en segundos).
		1.3.2 Porcentaje de incidentes detectados automáticamente por IA.
		1.4.1 Número de sistemas integrados con IA en el entorno judicial.
		1.4.2 Tiempo de integración de IA con sistemas de seguridad existentes.
		2.1.1 Número de amenazas detectadas

antes de que ocurran incidentes.

2.1.2 Porcentaje de amenazas detectadas por los sistemas de IA en comparación con métodos tradicionales.

2.2.1 Número de incidentes de seguridad cibernética prevenidos mediante IA.

2.2.2 Porcentaje de incidentes evitados con éxito en comparación con el periodo anterior a la implementación de IA.

2.3.1 Tiempo promedio de respuesta ante incidentes cibernéticos (en minutos).

2.3.2 Porcentaje de incidentes gestionados automáticamente por el sistema de IA.

2.4.1 Número de datos sensibles protegidos por sistemas de IA.

TESIS UANCV
VICERRECTORADO DE INVESTIGACIÓN
"OFICINA DE INVESTIGACIÓN"

	2.4.2 Porcentaje de reducción de accesos no autorizados a datos judiciales tras la implementación de IA. .

OFICINA DE INVESTIGACIÓN
Tesis Publicada con autorización del autor
http://repositorio.uancv.edu.pe/

TESIS UANCV
VICERRECTORADO DE INVESTIGACIÓN
"OFICINA DE INVESTIGACIÓN"

ANEXO 1
FORMULARIO DE AUTORIZACIÓN

AUTORIZACIÓN PARA LA INCORPORACIÓN DE LOS TRABAJOS DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL UANCV

Formato digital [X] Fecha de entrega: 17/06/2026

1. Datos del autor (es):

Nombres y Apellidos: GERSON JOSE PINEDA LAZARINOS
Dirección: Jr. Huancane Prol. 912 barrio Mañazo - Puno
DNI/Carné de Extranjería/Pasaporte N°: 72288939
Teléfono: 991 325 927 email: gejojoo@gmail.com
Nombres y Apellidos:
Dirección:
DNI/Carné de Extranjería/Pasaporte N°:
Teléfono: email:
Facultad y/o Escuela de Posgrado: INGENIERÍA DE SISTEMAS
Escuela Profesional o Mención: INGENIERÍA DE SISTEMAS
Título o Grado Académico a optar: INGENIERO DE SISTEMAS
Asesor: Dr. PAUL MAMANI TISNADO
Esta obra se encuentra dentro de las siguientes denominaciones:
Trabajo de Investigación [ ] Tesis [X] Trabajo de Suficiencia Profesional [ ] Trabajo Académico [ ]
Título: IMPLEMENTACIÓN DE SISTEMAS DE INTELIGENCIA ARTIFICIAL PARA LA SEGURIDAD CIBERNÉTICA EN LA CORTE SUPERIOR DE JUSTICIA DE PUNO 2024

Palabras claves, (3 a 5 términos): Inteligencia artificial, seguridad cibernética, corte superior de justicia, implementación tecnológica, ciberseguridad judicial, detección de amenazas, capacitación en TI, evaluación de vulnerabilidades.

¿Esta obra se desarrolló en la UANCV [1, 2]?

2

[1] Indicar si su producción intelectual ha empleado recursos tales como, instalaciones, laboratorios, insumos, equipos, bases de datos, asesoría técnica por parte del personal de la UANCV, financiamiento, entré otros relacionados.
[2] Si su producción intelectual se desarrolló en la UANCV totalmente o parcialmente, deberá autorizar el depósito en el Repositorio de manera obligatoria.

OFICINA DE INVESTIGACIÓN
Tesis Publicada con autorización del autor
http://repositorio.uancv.edu.pe/

TESIS UANCV
VICERRECTORADO DE INVESTIGACIÓN
"OFICINA DE INVESTIGACIÓN"

2. Referencia de tesis:

[ ] Bachiller [X] Titulo [ ] 2da Especialidad [ ] Maestría [ ] Doctorado

3. Licencias:

a) Licencia estándar:

Bajo los siguientes términos, autorizo el depósito de mi tesis en el Repositorio Digital de la UANCV.

Con la autorización de depósito de mi producción Intelectual, otorgo a la Universidad Andina "Néstor Cáceres Velásquez" una licencia no exclusiva para reproducir, distribuir, comunicar al público, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público mi producción intelectual (incluido el resumen), en formato físico o digital, en cualquier medio, conocido o por conocerse, a través de los diversos servicios por la Universidad, creados o por crearse, tales como el Repositorio Digital de tesis UANCV, colección de producción intelectual, entre otros, en el Perú y en el extranjero por el tiempo y veces que considere necesarias, y libres de remuneraciones.

En virtud de dicha licencia, la Universidad Andina "Néstor Cáceres Velásquez" podrá reproducir mi producción intelectual en cualquier tipo de soporte y en más de un ejemplar, sin modificar su contenido, solo con propósitos de seguridad, respaldo y preservación.

Declaro que la producción intelectual es una creación de mi autoría y exclusiva titularidad, coautoría con titularidad compartida, y me encuentro facultado a conceder la presente licencia y, asimismo, garantizo que dicha producción intelectual no infringe derechos de autor de terceras personas.

La Universidad Andina "Néstor Cáceres Velásquez" consignará el nombre del y/o los autor(es) de la producción intelectual, y no le hará ninguna modificación más que la permitida en la licencia.

Autorizo su publicación (marque con una X)

[X] Sí, autorizo que se deposite inmediatamente.

[ ] Sí, autorizo que se deposite a partir de la fecha (d/m/a):_____

[ ] No autorizo.

b) Licencia CREATIVE COMMONS 4.0 INTERNACIONAL:

Si usted concede una licencia CREATIVE COMMONS sobre su producción intelectual, mantiene la titularidad de los derechos de autor de esta y, a la vez, permite que otras personas puedan reproducirla, comunicarla al público y distribuir ejemplares de esta, bajo las condiciones siguientes:

¿Quiere permitir usos comérciales de su producción intelectual?

Sí: significa que usted permite la reproducción, distribución y comunicación pública de la producción intelectual incluso con fines comerciales.

No: significa que usted permite la reproducción, y comunicación pública de la producción intelectual, pero sin fines comerciales.

[ ] Sí autorizo

[X] No autorizo

OFICINA DE INVESTIGACIÓN
Tesis Publicada con autorización del autor
http://repositorio.uancv.edu.pe/

TESIS UANCV
VICERRECTORADO DE INVESTIGACIÓN
"OFICINA DE INVESTIGACIÓN"

Jurisdicción de su Licencia

Todas las licencias CREATIVE COMMONS son de ámbito mundial, sin embargo, usted puede elegir entre la opción "internacional" o una adaptada a su jurisdicción, como para el caso peruano.

La opción "internacional" emplea el lenguaje y la terminología de los tratados internacionales; en cambio, la adaptada a su jurisdicción, recoge las particularidades de la legislación peruana.

En consecuencia, **la opción "internacional" goza de una mayor eficacia a nivel mundial, gracias a que tiene jurisdicción neutral**. Mientras que la opción adaptada a la jurisdicción del Perú goza de una mayor eficacia ante los tribunales peruanos.

☐ Internacional

☒ Nacional

Línea de investigación: CIENCIA DE LOS ORDENADORES – P24



Firma de Autor | huella digital | 17 – JUNIO – 2026 (Fecha)

OFICINA DE INVESTIGACIÓN
Tesis Publicada con autorización del autor
http://repositorio.uancv.edu.pe/