UNIVERSIDAD DEL PACÍFICO | Escuela de Postgrado

“Ausencia de mecanismos y sistemas de seguridad digital en los equipos informáticos de la Dirección de Investigación Criminal (DIRINCRI) de la PNP, 2024 - 2025”

Trabajo de investigación presentado
para optar al Grado Académico de
Magíster en Gestión Pública

Presentado por:
Ernan Ananias Guevara Bazan
Gilmar Yin Rique Florentini
Luis Alberto Casos Flores
Paulo Cesar Avila Romero
Aldo Evaristo Valverde Obregon

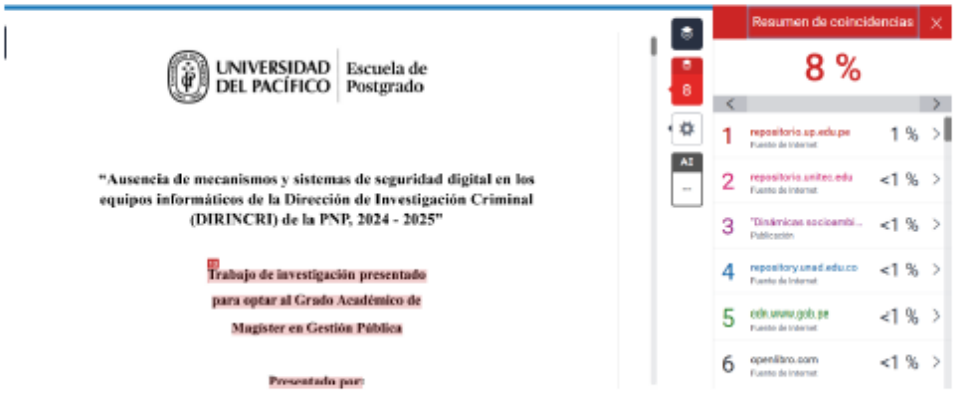
Asesor: César Manuel Bazán Ramírez
0009-0003-4898-6083

Lima, diciembre de 2025

Anexo III. Reporte de Evaluación Antiplagio

UNIVERSIDAD DEL PACÍFICO | Escuela de Postgrado

A través del presente, Juan Carlos Ubillús Ramírez deja constancia que el trabajo de investigación titulado "Ausencia de mecanismos y sistemas de seguridad digital en los equipos informáticos de la Dirección de Investigación Criminal (DIRINCRI) de la PNP, 2024 - 2025" presentado por Eman Ananias GUEVARA BAZAN, de acuerdo con el D.N.I. 09582645, Gilmar Yin RIQUE FLORENTINI de acuerdo con el D.N.I. 08668411, Luis Alberto CASOS FLORES, de acuerdo con el D.N.I. 08132702, Paulo Cesar AVILA ROMERO, de acuerdo con el D.N.I 07477453 y Aldo Evaristo VALVERDE OBREGON, de acuerdo con el D.N.I 43291447 para optar al Grado de Magíster en Gestión Pública), fue sometido al análisis del sistema antiplagio turnitin el 20 de octubre de 2026, dando el siguiente resultado:



20 de octubre de 2026.

Juan Carlos Ubillús Ramírez
Jefe Académico

Dedicatoria

Dedicamos este trabajo a quienes, con su ejemplo y compromiso silencioso, nos recuerdan que la búsqueda de la verdad constituye también una forma de servicio a la sociedad. A nuestras familias, por su paciencia constante y por acompañarnos en cada etapa de estudio y responsabilidad. A nuestros maestros y superiores, cuya orientación y exigencia fortalecieron nuestra convicción de que la investigación rigurosa es un pilar esencial para la justicia. Que este esfuerzo académico contribuya a fortalecer y retribuir el apoyo incondicional que hemos recibido.

Agradecimiento

Expresamos nuestro agradecimiento a quienes contribuyeron, de diversas maneras, a la concreción de este trabajo de investigación. Reconocemos especialmente a los docentes y asesores de la Escuela de Posgrado de la Universidad del Pacífico, cuya orientación académica y exigencia metodológica permitieron encausar con mayor claridad cada etapa del estudio. Del mismo modo, valoramos la disposición institucional de la Dirección de Investigación Criminal de la Policía Nacional del Perú, por facilitar el acceso a información y experiencias que enriquecieron el análisis desarrollado. Finalmente, agradecemos a compañeros y colegas que, desde su experiencia profesional, compartieron opiniones y observaciones que ayudaron a fortalecer el contenido del trabajo.

Resumen Ejecutivo

El presente trabajo de investigación tuvo como objetivo comprender las limitaciones de los mecanismos de seguridad digital en las unidades estudiadas de la DIRINCRI y sus posibles implicancias para la protección de la evidencia digital y la eficiencia de la investigación criminal durante el periodo 2024-2025.

Se empleó un enfoque mixto, con alcance exploratorio y descriptivo. El componente cualitativo comprendió la revisión documental y trece entrevistas semiestructuradas: once a policías y dos a expertos civiles. Las transcripciones se analizaron mediante ATLAS.ti. En el componente cuantitativo se aplicó un cuestionario de doce ítems con escala Likert a 83 efectivos policiales, seleccionados mediante muestreo no probabilístico por conveniencia, según su disponibilidad. Las entrevistas y encuestas se realizaron en 2025.

Los resultados muestran percepciones diversas sobre las condiciones de seguridad digital. El 66,27 % de los encuestados expresó acuerdo o total acuerdo con la afirmación de que los equipos no cuentan con protección suficiente para evitar accesos no autorizados. Respecto de la ausencia de reglas claras, el acuerdo alcanzó el 42,17 %, y sobre la insuficiente orientación o capacitación, el 48,19 %. La presencia de respuestas neutrales y de desacuerdo impide afirmar un consenso absoluto sobre estas carencias. Los hallazgos describen al grupo participante y no acreditan representatividad estadística poblacional ni, por sí solos, deficiencias técnicas o relaciones causales.

Se propone implementar gradualmente una solución institucional de gestión y monitoreo de eventos de seguridad (SIEM), articulada con procedimientos de acceso, respuesta a incidentes, trazabilidad y custodia digital. El piloto operaría en un horario institucional aprobado, con personal designado y formado. Su ampliación y la interoperabilidad quedarían sujetas a evaluación técnica, autorizaciones y disponibilidad de recursos.

La viabilidad financiera permanece condicionada, pues los costos son aproximaciones académicas que requieren validación mediante información económica documentada. Las mejoras previstas en detección, trazabilidad y gestión de incidentes deberán comprobarse mediante el piloto, sin presentarlas como resultados ya obtenidos.

Palabras clave: seguridad digital institucional, evidencia digital, SIEM, investigación criminal, DIRINCRI.

Abstract

This study aimed to understand the limitations of digital security mechanisms in the DIRINCRI units examined and their potential implications for the protection of digital evidence and the efficiency of criminal investigations during 2024–2025.

A mixed-methods approach with an exploratory and descriptive scope was employed. The qualitative component comprised a documentary review and thirteen semi-structured interviews with eleven police officers and two civilian experts. The transcripts were analyzed using ATLAS.ti. For the quantitative component, a twelve-item questionnaire with a Likert response scale was administered to 83 police officers selected through non-probability convenience sampling based on their availability. The interviews and surveys were conducted in 2025.

The results reveal diverse perceptions of digital security conditions. Among respondents, 66.27% agreed or strongly agreed that their computers lacked sufficient protection against unauthorized access. Agreement with the statement concerning the absence of clear rules reached 42.17%, while agreement regarding insufficient guidance or training reached 48.19%. Neutral and dissenting responses preclude claims of unanimous agreement on these shortcomings. The findings describe the participating group and do not establish statistical representativeness of the population or, by themselves, technical deficiencies or causal relationships.

The study proposes the gradual implementation of an institutional Security Information and Event Management (SIEM) solution, coordinated with procedures for access control, incident response, traceability, and digital evidence custody. The pilot would operate during approved institutional hours with designated, trained personnel. Expansion and interoperability would depend on technical assessment, authorization, and resource availability.

Financial feasibility remains conditional because the costs are academic estimates requiring validation through documented economic information. The anticipated improvements in detection, traceability, and incident management must be assessed through the pilot and should not be presented as outcomes already achieved.

Keywords: institutional digital security, digital evidence, SIEM, criminal investigation, DIRINCRI.

Índice de contenidos

Dedicatoria iv
Agradecimiento v
Resumen ejecutivo vi
Abstract v
Índice de figuras x
Índice de tablas xi
Índice de anexos xii
Capítulo 1. Problematizar 1
1.1. Selección inicial 1
1.2. Contexto Normativo Institucional 1
1.3. Descripción del problema 2
Capítulo 2: Explorar 12
2.1 Definición del desafío de solución 12
2.2. Análisis del desafío institucional 14
2.2 Generación de ideas y evaluación de alternativas 15
2.2.1. Generación de ideas 15
2.2.2. Métodos y hallazgos 16
2.2.3. Evaluación de alternativas 31
Capítulo 3: Proponer 35
3.1. Propuesta de solución: Conceptualización y fundamentos de la solución tecnológica 35
3.1.1. Características generales 35
3.1.2. Sustento institucional y estratégico de la propuesta 37
3.1.3. Descripción de la propuesta de solución 37
3.2. Evaluación de la propuesta: Valoración funcional, estratégica y operativa de la propuesta 38
3.2.1. Testeo de efectividad del concepto de solución 39
3.3. Ruta de implementación 39
3.3.1. Identificación de tareas críticas de implementación 39
3.3.2. Hoja de ruta de la implementación 40
3.3.3. Gobernanza de datos e interoperabilidad del ecosistema SIEM–SOC institucional 42
Capítulo 4: Conclusiones y recomendaciones 48
4.1. Conclusiones 48
4.2. Recomendaciones 49

Bibliografía 50
Anexos 57

Índice de figuras

Figura 1: *Ciclo de funcionamiento de sistemas de trazabilidad de los eventos digitales*.....4

Figura 2: *Vulnerabilidades cibernéticas en entornos industriales por ausencia de sistemas de monitoreo continuo* 5

Figura 3: *Empleo de sistemas de correlación de eventos y detección temprana de eventos maliciosos en la PNP* 10

Figura 4: *Nube de palabras sobre conceptos asociados a ciberseguridad institucional en la DIRINCRI (2024-2025)* 24

Figura 5: *Cadena de valor público relacionado con la implementación del SIEM* 39

Figura 6: *Arquitectura institucional de seguridad digital y gestión de evidencias* 47

Índice de tablas

Tabla 1: *Principales incidentes de ciberseguridad en la Policía Nacional del Perú (2019-2025)* 7

Tabla 2: *Definición del desafío* 14

Tabla 3: *Matriz de experiencias comparadas* 16

Tabla 4: *Matriz fortalecida de rigor metodológico del componente cualitativo y su articulación con la matriz de consistencia* 18

Tabla 5: *Consistencia interna y estadísticos descriptivos por dimensión (n = 83)* 21

Tabla 6: *Matriz Multicriterio de Priorización de Alternativas Proyecto SIEM-DIRINCRI PNP (Enfoque Invierte.pe) Priorización de alternativas mediante ponderación simple* 22

Tabla 6-A: *Análisis de sensibilidad de la priorización de alternativas según el peso de la viabilidad financiera* 23

Tabla 7: *Distribución porcentual de las percepciones sobre reglas, protección de equipos, capacitación y recursos para la seguridad digital en las unidades estudiadas* 26

Tabla 8: *Distribución porcentual de percepciones sobre las implicancias operativas, jurídicas y sociales derivadas de la falta de monitoreo y trazabilidad digital en la DIRINCRI (2024-2025)* 28

Tabla 9: *Percepción del personal sobre las estrategias institucionales y alternativas tecnológicas para fortalecer la ciberseguridad y la gobernanza digital en la DIRINCRI (2024-2025)* 30

Tabla 10: *Evaluación de alternativas para la implementación de una solución tecnológica de monitoreo y gestión de eventos de seguridad digital* 32

Tabla 11: *Evaluación de factores críticos y acciones estratégicas para la implementación de una solución integral de seguridad digital en la DIRINCRI-PNP* 38

Tabla 12: *Matrices de Alternativas, costos y evaluación de sostenibilidad* 40

Índice de anexos

Anexo 1: Matriz de Consistencia 57

Anexo 2: Bosquejo de proyecto de inversión pública 58

Anexo 3: Ruta propuesta para la implementación gradual del SIEM 63

Anexo 4: Matriz de vinculación de la propuesta con instrumentos de gestión pública y la cadena de valor del servicio policial 65

Anexo 5: Matriz de indicadores propuestos, líneas de base pendientes, metas y fuentes de verificación 66

Anexo 6: Matriz de variables críticas y Benchmarks referenciales para estimación Clase II–III de costos SIEM (híbrido) 68

Anexo 7: Matriz de Registro de riesgos y plan de respuesta del Proyecto SIEM–DIRINCRI (Enfoque Invierte.pe) 70

Anexo 8: Mapa de Cumplimiento en Protección de Datos, Gobierno Digital y Calidad de Servicio 71

Proyecto SIEM–DIRINCRI (Enfoque Invierte.pe) 71

Anexo 9: Matriz de Cadena de valor del proyecto SIEM-DIRINCRI 72

Anexo 10: Guía de entrevistas 74

Anexo 11: Perfil de entrevistados clave del componente cualitativo 78

Anexo 12: Matriz de codificación cualitativa 79

Anexo 13: Cuestionario Likert 80

Anexo 14: Ficha Técnica de la Encuesta 82

Anexo 15: Paneaux fotográfico 84

Anexo 16: Matriz de actores estratégicos para la implementación del SIEM en la DIRINCRI bajo enfoque de poder/interés 86

Anexo 17: Propuesta de procedimiento de gobernanza de datos e interoperabilidad 87

Gobernanza de Datos e Interoperabilidad del Ecosistema SIEM-SOC Institucional - DIRINCRI 87

Anexo 18: Plan Estratégico de Gestión del Cambio y Sensibilización Institucional 93

Anexo 19: Mapa de Empatía del usuario institucional 98

Anexo 20: Secuencia visual del Storyboard 99

Capítulo 1. Problematizar

1.1. Selección inicial

La carencia de mecanismos y sistemas de seguridad digital revela serias limitaciones en la planificación estratégica de la PNP respecto al cumplimiento de los objetivos establecidos en el IV Pilar "Nuestra TIC" del Plan Estratégico Mariano Santos al 2030. Esta brecha tecnológica debilita la capacidad de la DIRINCRI para anticiparse a ciberataques, detectar anomalías en tiempo real y proteger la evidencia digital vinculada a investigaciones criminales de alta sensibilidad.

1.2. Contexto Normativo Institucional

El marco normativo vigente refuerza esta necesidad. La Constitución Política del Perú de 1993 establece como deber del Estado garantizar la seguridad nacional, lo que tácitamente incluye a la seguridad digital. A ello se suma la Ley Nro. 30096 de 22 de octubre de 2013 sobre delitos informáticos. Que obliga a las instituciones, a proteger sus sistemas y datos frente a amenazas.

El Plan Estratégico de Capacidades de la PNP al 2030 Mariano Santos Mateos (MS30) define como pilar "Nuestra TIC" a la modernización y resiliencia de los entornos digitales para garantizar la seguridad nacional. Identifica además la necesidad de fortalecer la infraestructura tecnológica y la ciberdefensa.

La Ley de la Policía Nacional (Decreto Legislativo 1267 de 16 de diciembre de 2016) establece que la institución está llamada a preservar el orden interno, proteger a las personas y hacer cumplir las leyes. Por eso, incluye la investigación y el combate de la delincuencia como parte de su misión fundamental. En esa línea de ideas, el Decreto Supremo 026-2017-IN de 15 de octubre de 2017 establece que la DIRINCRI "es el órgano especializado, de carácter técnico y sistémico, normativo y operativo; responsable de prevenir, combatir, investigar y denunciar los delitos en el marco de la lucha contra la delincuencia y el crimen organizado" (p .52).

El Texto Único Ordenado de la Ley Nro. 32069, publicado el 24JUN2024 y vigente desde el 22ABR2025, regula las contrataciones del Estado y, entre ellas, la adquisición de bienes y servicios tecnológicos, asegurando que estos procesos se desarrollen con criterios de eficiencia, transparencia y valor público. A su vez, el Decreto Legislativo Nro. 1412, promulgado el 13 de diciembre de 2018, y su reglamento aprobado por el Decreto Supremo Nro. 029-2021-PCM, con la modificatoria introducida por el Decreto Supremo Nro. 098-2025-

PCM del 1 de agosto de 2025, establecen que las entidades públicas tienen la obligación de garantizar la seguridad de la información, la protección de los datos y la continuidad de los servicios digitales en el marco del Gobierno Digital.

De manera complementaria, la Política Nacional de Transformación Digital, aprobada mediante el Decreto Supremo Nro. 157-2021-PCM del 24 de septiembre de 2021, dispone la incorporación de soluciones tecnológicas modernas, seguras e interoperables como condición indispensable para alcanzar los objetivos institucionales y contribuir al cumplimiento de las metas nacionales vinculadas con la innovación, la eficiencia administrativa y la confianza ciudadana en los servicios del Estado. El marco legal vigente fundamenta la necesidad de que la DIRINCRI se modernice mediante herramientas tecnológicas de última generación. La normativa y su reglamento exigen a la institución investigar con rigor, preservar adecuadamente las evidencias y coordinar en tiempo real, funciones que solo pueden cumplirse con sistemas informáticos actuales, seguros y eficientes.

Por otro lado, la normativa vigente evidencia con claridad la urgencia de que la DIRINCRI modernice su infraestructura tecnológica, incorporando herramientas avanzadas de ciberseguridad que superen las limitaciones de los sistemas actualmente disponibles. En ese contexto, la adopción de soluciones informáticas orientadas al monitoreo, detección y respuesta ante incidentes digitales deja de ser una alternativa técnica para convertirse en una obligación institucional derivada del marco legal vigente. Sin el respaldo de sistemas informáticos modernos, seguros y dotados de capacidades automatizadas de defensa y control, dichas funciones resultan imposibles de cumplir de manera eficiente.

1.3. Descripción del problema

En este estudio, la seguridad digital institucional se aborda mediante la protección de información, los controles de acceso, la trazabilidad de actuaciones y la gestión de incidentes. El análisis comprende tanto las herramientas tecnológicas como las responsabilidades, los procedimientos y las capacidades del personal vinculadas con el manejo de información de investigación criminal.

No se limita a herramientas tecnológicas. También abarca políticas, procesos, talento humano y cultura organizacional. Su alcance incluye la infraestructura tecnológica, los datos, los usuarios, los procesos internos y la interoperabilidad con otras entidades, asegurando la continuidad y resiliencia institucional (Flores et al., 2021)

En el contexto policial, implica garantizar la protección de evidencias digitales y la confianza en la información procesada. La experiencia demuestra que reducir la ciberseguridad a medidas aisladas genera vulnerabilidades estructurales. Por el contrario, su gestión integral fortalece la gobernanza digital y la eficiencia operativa. Así, la ciberseguridad se consolida como un componente esencial para la modernización institucional y la confianza pública (Malaver, 2024).

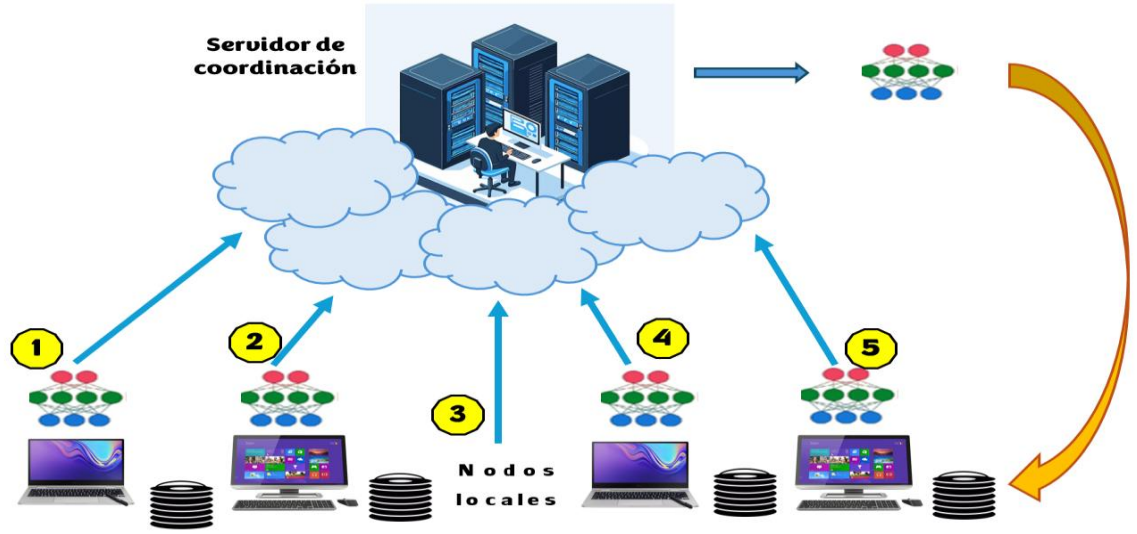
En este contexto, se hace indispensable que la institución cuente con sistemas de ciberseguridad capaces de recopilar, analizar y correlacionar en tiempo real la información generada por sus aplicaciones, servidores, dispositivos y usuarios. Dichas herramientas permiten obtener una visión integral del entorno informático, facilitando la identificación de comportamientos anómalos y la detección oportuna de amenazas. De esta forma, la DIRINCRI podría anticiparse a los incidentes que comprometen su infraestructura digital y responder de manera coordinada ante posibles intrusiones o vulneraciones.

Asimismo, disponer de mecanismos que aseguren la trazabilidad de los eventos digitales y generen alertas tempranas constituye un requisito esencial para garantizar la transparencia y la integridad de la información institucional. Estos sistemas no solo fortalecen la capacidad operativa frente a riesgos tecnológicos, sino que también contribuyen al cumplimiento de las normas sobre protección de datos y al refuerzo de la confianza pública en las plataformas digitales de la Policía Nacional del Perú. La consolidación de una cultura de monitoreo permanente y detección preventiva se convierte, por tanto, en una condición necesaria para la seguridad y legitimidad de la gestión policial en la era digital.

Esta carencia permite que actores maliciosos aprovechen vulnerabilidades ocultas, accediendo a información confidencial o poniendo en riesgo la integridad de los sistemas. Este proyecto de investigación argumenta que, sin una arquitectura de seguridad sustentada en estas herramientas, las infraestructuras informáticas permanecen expuestas a amenazas constantes y de alto impacto. En otras palabras, que seguirán “hackeando” a la PNP.

Figura 1

Ciclo de funcionamiento de sistemas de trazabilidad de los eventos digitales



Nota. La figura ilustra el ciclo operativo de monitoreo de amenazas e infiltraciones, mostrando cómo se articulan sus componentes para detectar, correlacionar y responder ante incidentes. Tomado de Truong et al. (2021).

Machín y Gazapo (2020) en un estudio sobre seguridad digital dentro del entorno europeo, sobre todo en España, muestran que la falta de mecanismos de protección digital constituye una amenaza directa para la estabilidad operativa y jurídica de las instituciones públicas. Además, advierten que la carencia de estrategias de seguridad digital integrales en los organismos estatales ha incrementado las vulnerabilidades estructurales, generando un terreno fértil para ataques persistentes y de difícil detección. La falta de monitoreo, además, obstaculiza los procesos de análisis forense posteriores a un incidente, lo que complica la identificación de responsables y limita la posibilidad de corregir fallos de manera efectiva.

El estudio técnico elaborado por el Parlamento Europeo (2021) documentó que la ausencia de políticas efectivas de ciberdefensa en Irlanda y Bélgica facilitó ataques de ransomware y accesos no autorizados a infraestructuras críticas, paralizando temporalmente servicios de salud y plataformas gubernamentales. La carencia de estos mecanismos priva a las instituciones de una supervisión continua y de la posibilidad de correlacionar eventos de seguridad, lo que retrasa la detección temprana de amenazas. En Irlanda, por ejemplo, el ataque de *ransomware*[1], dirigido contra el sistema nacional de salud en 2021 dejó al descubierto la fragilidad de sus redes; mientras que en Bélgica se produjeron intrusiones en plataformas gubernamentales que carecían de “respuestas automatizadas eficaces”.

[1] Modalidad delictiva en la cual, se utiliza un programa informático malicioso que bloquea el acceso a la información mediante técnicas de cifrado, con el objetivo de extorsionar a la víctima a cambio de liberar sus datos (Ávila Niño, 2023).

En el estudio realizado por Gonzales, Gonzales y Díaz (2021), se destaca que la falta de mecanismos de vigilancia digital constante en entornos industriales de Madrid ha propiciado un contexto vulnerable frente a ciberataques de alta complejidad. La carencia de monitoreo continuo y de mecanismos eficaces para la correlación de eventos limita significativamente la capacidad de detectar anomalías en tiempo real. Esto favorece la diseminación de programas informáticos malicioso, comúnmente denominado *malware*. Entre estos, el *phishing* ocupa un lugar destacado como técnica de fraude digital orientada a inducir a las personas a revelar información sensible, como contraseñas, datos bancarios o números de tarjetas de crédito, mediante estrategias de engaño cuidadosamente diseñadas. El estudio enfatizó que, sin una arquitectura de seguridad sustentada en estas herramientas, las infraestructuras industriales permanecen expuestas a amenazas constantes y de alto impacto.

Figura 2

Vulnerabilidades cibernéticas en entornos industriales por ausencia de sistemas de monitoreo continuo



Nota. La ilustración representa el impacto de no contar con sistemas de correlación y detección de eventos maliciosos en infraestructuras industriales, destacando la exposición a *malware* y técnicas de *phishing*. Adaptado a partir del estudio de Gonzales, Gonzales y Díaz (2021).

Villafani (2025) señala que, en el último año, cerca del 19% de los 10,000 ciberataques registrados en la Unión Europea tuvieron como blanco directo a entidades de la administración pública. A partir de datos proporcionados por la Agencia de la Unión Europea para la Ciberseguridad (ENISA), se advierte que la ausencia de sistemas de medidas de seguridad digital en organismos estatales ha sido un elemento clave en el aumento de vulnerabilidades, facilitando incidentes como las brechas de seguridad y los ataques de denegación de servicio. En una línea similar, Snider et al. (2021) subrayan que la débil implementación de marcos de

protección digital en entidades gubernamentales de Estados Unidos constituye una falla crítica en el deber de diligencia frente a la protección de activos tecnológicos estratégicos.

En Chile, persiste una brecha estructural en materia de ciberseguridad estatal, caracterizada por escasa inversión en protección digital, fragmentación normativa y una limitada capacidad de respuesta institucional frente a incidentes de alto impacto, sumada a la debilidad de las políticas públicas en la región, ha colocado a este y varios países latinoamericanos en un escenario de elevada vulnerabilidad frente a amenazas persistentes. De acuerdo con los indicadores del *Global Cybersecurity Index (GCI) y el National Cyber Security Index* (NSCI), gran parte de los Estados de la región exhiben bajos niveles de preparación frente a incidentes digitales, lo que limita sus capacidades de detección, reacción y recuperación. Esta deficiencia normativa y tecnológica favorece que los ciberdelincuentes aprovechen las brechas existentes en infraestructuras críticas, afectando tanto al ámbito estatal como al privado. La ausencia de sistemas de monitoreo y correlación de eventos limita la capacidad de las instituciones para mantener una vigilancia activa sobre su infraestructura digital y reconocer de manera temprana los patrones que anteceden a un ataque cibernético.

Esta deficiencia retrasa la contención de incidentes y amplifica el impacto de las amenazas. A ello, se suma la escasa inversión en programas de ciberinteligencia y la fragmentación institucional – factores que incrementan la exposición frente a riesgos digitales persistentes. En consecuencia, y tal como advierte Aguilar Antonio (2021), mientras no se consolide una estrategia regional articulada en materia de seguridad digital, la resiliencia tecnológica continuará siendo un desafío pendiente para América Latina.

En el mismo contexto regional, se ha señalado que la ausencia de sistemas de correlación de datos y de seguridad digital en los entornos institucionales, representa un factor de alto riesgo para la salvaguarda de los activos digitales. Tal como advierte la literatura especializada revisada en los párrafos anteriores, esta carencia impide un monitoreo constante y la correlación efectiva de incidentes. Lo que facilita que las amenazas pasen inadvertidas hasta convertirse en ataques de gran escala.

Entre los años 2019 y 2025, la Policía Nacional del Perú (PNP) se ha visto expuesta a diversos ciberataques que han dejado al descubierto serias limitaciones en la protección de sus activos digitales. Uno de los episodios más críticos fue la sustracción masiva de información del Sistema de Denuncias Policiales (SIDPOL), ejecutada por el hacker conocido como “Gatito FBI_NZ”.

Este actor logró obtener más de 80 GB de datos sensibles, entre ellos denuncias, registros vehiculares e información personal que posteriormente fueron comercializados en la *dark web*. Según el propio atacante, el acceso se produjo mediante credenciales legítimas adquiridas en canales clandestinos como Telegram y WhatsApp. Lo que refleja la inexistencia de controles tecnológicos avanzados para identificar accesos no autorizados y frenar la exfiltración de información. Aunque el caso se hizo público el 4 de agosto de 2025, los ataques se venían gestando de manera sistemática desde el 2019 (Retamozo, 2025).

A este hecho se sumó la vulneración de la base de datos de la Dirección de Inteligencia de la PNP perpetrada el 7 de agosto de 2025, en la que se expusieron identidades de agentes, planes operativos y órdenes reservadas. Aunque en un inicio se atribuyó a un ataque externo, posteriormente se confirmó que la filtración fue interna y ejecutada por personal con acceso autorizado (Chuquín, 2025).

Tabla 1

Principales incidentes de ciberseguridad en la Policía Nacional del Perú (2019-2025)

Año	Tipo de incidente	Sistema afectado	Volumen comprometido	Mecanismo de acceso
2019	Accesos no autorizados iniciales	SIDPOL	No cuantificado	Credenciales filtradas
2021	Escaneo masivo de infraestructura	Red privada de datos policiales	36,000 intentos/seg	Reconocimiento automatizado
2023	Vulneración de registros vehiculares	Sistema de Registro Vehicular	~15 GB	Exfiltración progresiva
2024	Contratación irregular de servicios	Infraestructura de telecomunicaciones	Riesgo sistémico	Falta de blindaje contractual
2025	Sustracción masiva de datos	SIDPOL	>80 GB	Credenciales legítimas compradas
2025	Restricción de acceso por 5 años	Base de datos de denuncias	Total, del sistema	Resolución institucional

Nota. La tabla resume los principales eventos de ciberseguridad que afectaron a la Policía Nacional del Perú entre 2019 y 2025, destacando el caso del hacker "Gatito FBI_NZ" y la progresiva exposición de activos digitales críticos. Fuentes: Elaboración propia tomado de Retamozo (2025) y Correo (2025).

Como medida de contención orientada a mitigar los efectos del ciberataque, la PNP dispuso restringir durante cinco años el acceso público a sus bases de datos, alegando la necesidad de preservar la seguridad ciudadana y el orden interno frente a posibles nuevas vulneraciones. Si bien la decisión puede entenderse como preventiva, ha generado cuestionamientos por limitar la transparencia y el escrutinio social en la gestión de información

pública. De no adoptarse una política integral de ciberseguridad con herramientas digitales adecuadas con protocolos de "respuesta y formación especializada", la institución continuará expuesta a incidentes que comprometen tanto a la institución como a la ciudadanía (Correo, 2025).

La investigación sobre la ausencia de herramientas informáticas especializadas para la protección digital en la Dirección de Investigación Criminal (DIRINCRI) de la Policía Nacional del Perú (PNP) se fundamenta en la urgente necesidad de cerrar la brecha de ciberseguridad que persiste en las instituciones del Estado. Esta brecha ha quedado en evidencia a través de los reiterados ciberataques y vulneraciones de datos ocurridos en los últimos años, los que han puesto de manifiesto las limitaciones estructurales en materia de monitoreo, detección y respuesta ante incidentes digitales.

La DIRINCRI, concentra investigaciones vinculadas al crimen organizado, la extorsión, el secuestro, los homicidios y los delitos informáticos, por ello, administra información de alta sensibilidad cuyo resguardo constituye un deber jurídico y estratégico. La ausencia de herramientas informáticas y sistemas de correlación de eventos que aseguren la integridad y autenticidad de los datos compromete la validez probatoria de la evidencia digital y debilita la confianza ciudadana en la administración de justicia. En este trabajo, el fortalecimiento de la seguridad digital se plantea como una necesidad de gestión institucional que debe evaluarse junto con las capacidades operativas, los procedimientos de preservación de evidencia y los recursos disponibles (Rojas, 2025).

Los diagnósticos internos realizados en distintas dependencias de la PNP evidencian que la institución carece de sistemas integrales de ciberseguridad, lo que incluye ausencia de gestión centralizada de eventos de seguridad. En el caso específico de la DIRINCRI, la carencia de estas herramientas refleja un vacío crítico, conforme se detalla:

- La Inspectoría General identificó ausencia de gobernanza digital, falta de protocolos de incidentes y nula gestión de riesgos estructurada.
- En el Departamento de Producción de Inteligencia en Asuntos Sociales se encontró que no existe una directiva específica de protección de datos personales ni indicadores de seguridad. Lo que expone información sensible.

- La División de Ciberseguridad de la DIRTIC advirtió la fragmentación de funciones y ausencia de políticas institucionales unificadas, proponiendo incluso la creación de una Dirección General de Ciberseguridad dentro de la PNP.

- La Dirección de Criminalística reportó que no existen planes formales de respuesta a incidentes ni protocolos claros para la protección de datos forenses, lo que afecta la cadena de custodia digital.

- Finalmente, algunos avances parciales en otras áreas de la PNP (como la existencia de comités de ciberseguridad o convenios externos) son insuficientes, pues se trata de procesos aislados, sin estandarización institucional[2].

Además, se identifica ausencia de liderazgo institucional en ciberseguridad y fragmentación de funciones que generan vulnerabilidad. Esta escasa cultura organizacional y resistencia al cambio limitan la adopción de buenas prácticas. El déficit de personal especializado y la formación informal reducen la capacidad técnica de respuesta. Los procesos administrativos lentos limitan la adquisición de tecnología sumado a la falta de integración con estándares internacionales como ISO/IEC 27032, 27001 y NIST debilitan la protección digital.

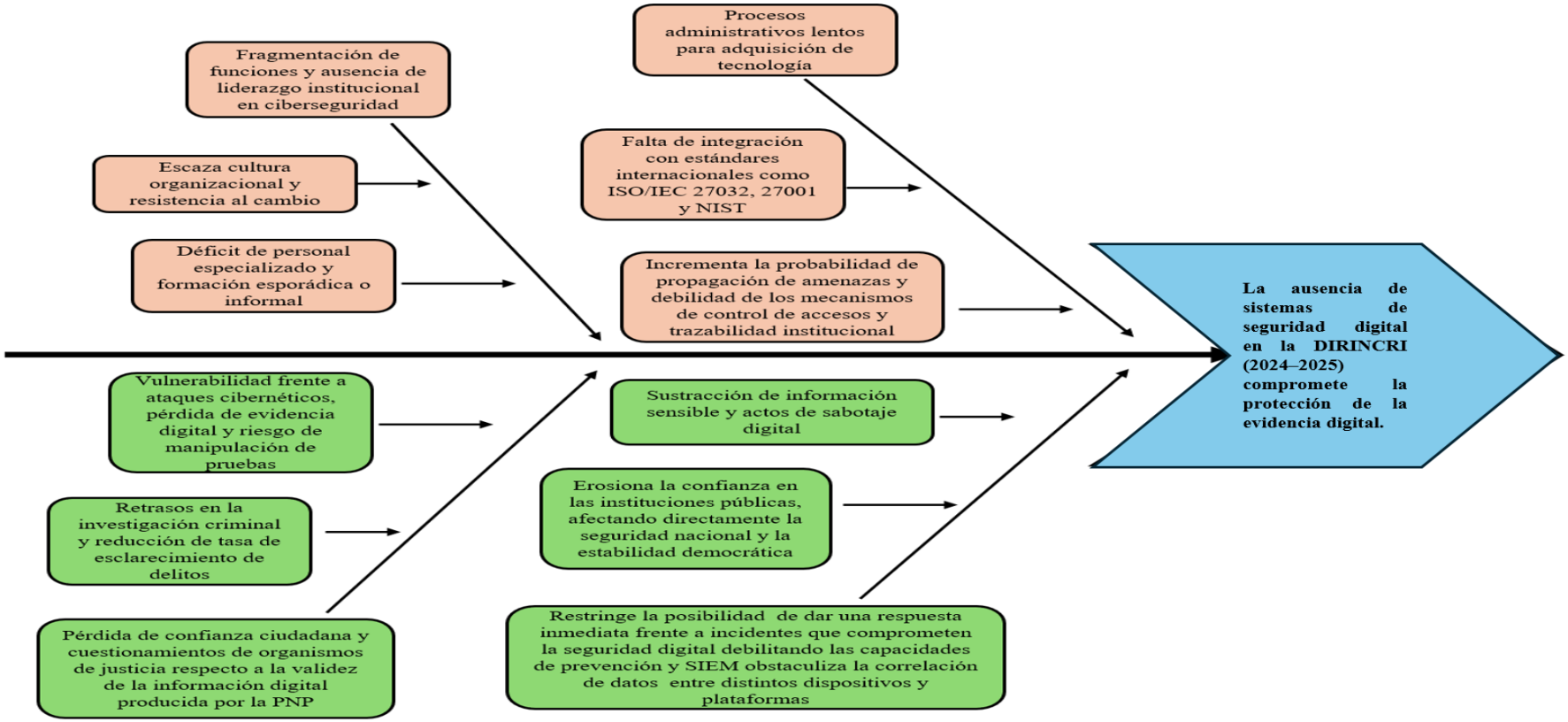
Consecuentemente, esto incrementa la propagación de amenazas y la fragilidad de los mecanismos de control de accesos y trazabilidad. Además, se compromete la validez de la evidencia digital, la eficiencia de la investigación criminal y la confianza ciudadana en la PNP (Aguilar Antonio, 2021).

Sobre la identificación del usuario e impacto en el ciudadano, los usuarios directos como la DIRINCRI resultarían más afectados ante un eventual ataque cibernético. La falta de sistemas de detección temprana de ciberamenazas debilita la capacidad de detectar intrusiones o accesos indebidos, comprometiendo la seguridad de las investigaciones. Los beneficiarios finales son los ciudadanos, quienes terminan siendo afectados por: 1) demoras en la resolución de casos de criminalidad organizada y delitos informáticos, 2) Incremento de la percepción de inseguridad, y 3) Menor credibilidad en la PNP como garante de la investigación criminal.

[2] Información obtenida con el llenado de la "Plantilla de Brechas sobre Seguridad Digital", del XCII Curso de Capacitación en Inteligencia Policial de la Dirección de Inteligencia de la Policía Nacional del Perú 2025.

Figura 3

Empleo de sistemas de correlación de eventos y detección temprana de eventos maliciosos en la PNP



Nota: La figura muestra las causas y consecuencias clave para implementar el uso de sistemas adecuados para la seguridad digital en la PNP. Elaboración propia.

Finalmente, los elementos críticos, que se han identificado como *supuestos o desafíos* son:

- ***Brechas estructurales:*** ausencia de gobernanza central, carencia de procesos unificados y déficit de herramientas de protección avanzadas.
- ***Recursos humanos***: falta de formación continua y limitada especialización en ciberseguridad.
- ***Sistemas administrativos***: lentitud en los procesos de adquisición bajo el SEACE y limitada articulación con sistemas presupuestales.
- ***Ruta técnica***: no existen protocolos de integración tecnológica ni de respuesta a incidentes, lo que impide la implementación de sistemas de detección y prevención temprana de ciberataques de forma estandarizada.
- ***Ruta estratégica***: escasa priorización en los instrumentos de planificación institucional (PEI–PNP, PEI–MININTER) y poca articulación con la Política de Modernización del Estado.
- ***Supuestos críticos***: apoyo sostenido de la alta dirección policial, disponibilidad de presupuesto, y cooperación con actores externos públicos y privados.

En suma, la ausencia de mecanismos integrales de seguridad digital en la Dirección de Investigación Criminal de la PNP revela una vulnerabilidad estructural que trasciende el ámbito tecnológica y constituye una obligación estratégica para la institución policial. Estas soluciones (Ej. herramientas informáticas avanzadas y sistemas de monitoreo, detección y trazabilidad de eventos) no solo garantizan la integridad y trazabilidad de la información, sino que también refuerzan la transparencia en la gestión pública y aseguran el respeto a los derechos fundamentales en el entorno digital (López Velásquez et al., 2023).

No se trata únicamente de cerrar brechas tecnológicas, sino de consolidar un modelo de gobernanza digital que sitúe a la Policía Nacional del Perú a la altura de los estándares internacionales de ciberseguridad, en cumplimiento de su deber constitucional de proteger la vida, la seguridad y la libertad de las personas.

En consecuencia, se plantea como imperativo incorporar sistemas de ciberseguridad y monitoreo permanente dentro de una estrategia institucional de defensa orientada a la prevención, la respuesta oportuna y la resiliencia cibernética.

Capítulo 2: Explorar

2.1 Definición del desafío de solución

La Dirección de Investigación Criminal (DIRINCRI-PNP) atraviesa una brecha estructural en materia de seguridad digital, que afecta directamente su capacidad operativa frente a los desafíos del entorno digital. La ausencia de una solución tecnológica que le permita monitorear, correlacionar y gestionar de manera integrada los eventos de seguridad informática limita la detección oportuna de amenazas, dificulta el análisis articulado de incidentes y restringe la trazabilidad de acciones policiales. La carencia compromete la protección de activos digitales y debilita la eficacia investigativa frente a organizaciones criminales sofisticadas. En consecuencia, se configura un riesgo institucional tanto operativo como reputacional

La situación actual responde a causas interrelacionadas: ausencia de protocolos unificados de seguridad digital, limitada interoperabilidad entre sistemas y dificultades en el intercambio de información. Estas carencias se agravan por la escasa cultura de ciberseguridad y el déficit de personal especializado, lo que reduce la capacidad de respuesta ante amenazas cada vez más sofisticadas. Finalmente, los procedimientos administrativos lentos y fragmentados para adquirir tecnología obstaculizan la modernización oportuna de la infraestructura crítica, manteniendo vulnerabilidades institucionales.

Las consecuencias afectan el desempeño institucional y la confianza pública: la pérdida o manipulación de evidencias compromete investigaciones y la vulneración de bases de datos expone información sensible, debilitando la protección policial y generando cuestionamientos de la ciudadanía.

2.1.1 Enfoque en usuarios directos y beneficiarios finales

La Ficha 01 se desarrolla a partir del diagnóstico institucional y de las actividades de manejo de información descritas en el estudio. Sus dificultades se presentan como necesidades y riesgos identificados, sin atribuir a ciudadanos opiniones que no fueron recogidas. Los usuarios directos son el personal investigador y quienes administran, supervisan o preservan información digital; los operadores fiscales y judiciales intervienen como usuarios relacionados de los productos de investigación.

Los beneficiarios finales son las personas cuyos datos, denuncias y evidencias se gestionan durante las investigaciones: agraviados, denunciantes, testigos e

investigados. La protección debe considerar tanto la seguridad de la información como la privacidad y las garantías de todas las personas involucradas.

Campo de la Ficha 01	Aplicación al estudio
Usuarios directos y relacionados	Investigadores, custodios y personal técnico de DIRINCRI; DIRTIC como soporte institucional. Ministerio Público y Poder Judicial reciben información conforme a competencias y autorizaciones.
Actividades e interacciones	Registrar y consultar información; documentar accesos; preservar y remitir archivos; reportar incidentes; coordinar soporte y atención de alertas.
Espacios y materiales	Equipos, redes, aplicaciones, repositorios y registros institucionales. El inventario, número de activos y capacidad de almacenamiento se determinarán antes del piloto.
Dificultades y efectos	Controles heterogéneos y dificultades percibidas para seguir accesos o modificaciones. Pueden originar trabajo adicional, exposición de datos o problemas de autenticidad, sujetos a verificación por caso.
Beneficiarios finales	Personas afectadas por delitos y personas involucradas en investigaciones. Beneficio esperado: resguardo de datos y mayor confiabilidad del servicio de investigación.
Verificación futura	Medir completitud de registros de custodia y tiempos de atención; recoger experiencia del usuario interno. Evaluar reclamos vinculados a datos mediante instrumentos específicos, sin confundirlos con confianza ciudadana general.

El enfoque en el usuario se complementa con un Mapa de Empatía del usuario institucional y un Storyboard de la interacción propuesta con el SIEM, desarrollados en los Anexos 19 y 20. Ambos se elaboraron durante la revisión del trabajo a partir de las transcripciones aportadas del levantamiento de 2025 y de las 83 respuestas de encuesta registradas entre el 11 y el 15 de noviembre de ese año. El mapa sintetiza necesidades y dificultades expresadas por los participantes, sin representar a una persona específica ni atribuir emociones no documentadas. Las opiniones de especialistas de otras dependencias se emplean como perspectiva relacionada y no se equiparan automáticamente a experiencias de DIRINCRI.

El Storyboard distingue las dificultades descritas en el diagnóstico de las actuaciones previstas para una implementación futura. Representa cómo el registro de eventos, el análisis de alertas y la preservación de evidencia podrían contribuir a proteger la información de las personas involucradas en investigaciones. No reproduce un incidente real ni acredita resultados de un SIEM implementado. Las referencias a confianza ciudadana expresan opiniones de participantes institucionales; no constituyen una medición directa de satisfacción de los beneficiarios finales.

Frente a este panorama, los factores críticos de intervención se orientan a fortalecer la gestión institucional de riesgos, consolidar una arquitectura tecnológica interoperable,

promover la formación de capacidades humanas especializadas en ciberseguridad y optimizar la asignación presupuestal bajo un enfoque de resultados. Solo mediante la articulación de estos componentes será posible transitar hacia un ecosistema digital resiliente, capaz de sostener la integridad de las investigaciones y la legitimidad institucional frente a los desafíos de la era tecnológica. En ese marco, la siguiente tabla transforma el problema de esta investigación en desafío de gestión pública.

Tabla 2

Definición del desafío

Problema de gestión publica	Desafío de Gestión Publica
Ausencia de mecanismos y sistemas de seguridad digital en los equipos informáticos de la Dirección de Investigación Criminal (DIRINCRI) de la PNP, 2024 – 2025.	¿Cómo puede la DIRINCRI fortalecer la protección y trazabilidad de la información y evidencia digital, así como su capacidad de detectar y atender incidentes, con capacidades institucionales sostenibles?

Nota. La tabla relaciona el problema identificado en la DIRINCRI durante el periodo 2024-2025 con un desafío orientado a proteger la información y evidencia digital, mejorar su trazabilidad y fortalecer la atención de incidentes con capacidades institucionales sostenibles. Elaboración propia a partir del diagnóstico del estudio.

En consecuencia, el desafío consiste en diseñar y adoptar una solución que fortalezca la gobernanza digital, garantice la supervisión continua de la infraestructura y permita una reacción institucional más eficiente ante amenazas cada vez más sofisticadas.

2.2. Análisis del desafío institucional

La Dirección de Investigación Criminal enfrenta un escenario crítico por la ausencia de herramientas que integren el monitoreo y correlación de eventos de seguridad digital. Esto impide detectar comportamientos inusuales, dificulta la lectura articulada de incidentes y compromete la trazabilidad de las actuaciones policiales. Más allá de lo tecnológico, la situación refleja una vulnerabilidad institucional que afecta la investigación criminal y la confianza ciudadana, al debilitar la protección de activos digitales y la eficacia frente a organizaciones cada vez más sofisticadas.

El origen de la problemática radica en la falta de protocolos unificados de seguridad digital, lo que genera vacíos normativos y deja al personal sin guía clara frente a incidentes. A ello se suma la limitada interoperabilidad entre sistemas policiales, que dificulta el flujo de información y retrasa el análisis. La escasa formación en ciberseguridad y la fragmentación de funciones agravan la vulnerabilidad institucional. Finalmente, los procesos de contratación pública, lentos y poco articulados, impiden adquirir soluciones tecnológicas acordes a las necesidades operativas de la DIRINCRI.

El Informe N.º 289-2025-DIRREHUM-PNP/DIVABL-DEPACAS.SCAS, del 14 de noviembre de 2025, comunica que entre 2021 y 2024 no hubo ingresos por asimilación ni contratos CAS en carreras de sistemas, informática y ciberseguridad. Sin embargo, en 2025 se incorporaron tres profesionales de dichas especialidades, asignados al Departamento de Sistematización de la Información de la Carrera Policial de la DIVSICPAL-DIRREHUM PNP.

2.2 Generación de ideas y evaluación de alternativas

2.2.1. Generación de ideas

El proceso de generación de ideas partió de la revisión de incidentes ocurridos dentro de la PNP y del análisis de la literatura especializada sobre ciberseguridad en organizaciones públicas. Se identificaron prácticas comunes en instituciones que han logrado proteger sus activos digitales mediante sistemas capaces de recolectar y procesar registros en tiempo real, correlacionar eventos relevantes y producir alertas automáticas para reducir riesgos. El estudio de experiencias internacionales muestra que la modernización tecnológica requiere liderazgo institucional, normativas claras y una cultura organizacional orientada a la gestión de riesgos. Estos insumos permiten visualizar alternativas progresivas y sostenibles para la DIRINCRI

La literatura especializada destaca que la resiliencia digital institucional depende de la capacidad de las entidades públicas para monitorear eventos de seguridad en tiempo real. Según la *European Union Agency for Cybersecurity* (ENISA, 2024), los sistemas SIEM constituyen el eje central de la defensa cibernética, pues consolidan registros, detectan patrones anómalos y emiten alertas automáticas ante actividades sospechosas.

La revisión de experiencias comparadas permite identificar funciones y condiciones de implementación pertinentes para la propuesta: gestión de datos, definición de responsabilidades, selección de fuentes de eventos y evaluación de capacidades. La Tabla 3 desarrolla estos aportes y sus límites de transferencia a DIRINCRI. Las experiencias externas no acreditan mejoras efectivamente obtenidas en la institución ni sustituyen la evaluación del piloto.

La experiencia latinoamericana sugiere que la combinación de marcos normativos actualizados, capacitación continua y soluciones SIEM integradas genera entornos más seguros, especialmente en organizaciones policiales o judiciales. La incorporación de inteligencia artificial (IA) y aprendizaje automático (*machine learning*) en estas plataformas

ha permitido predecir ataques y priorizar vulnerabilidades críticas, otorgando valor estratégico a la información. La tabal 3 resume la experiencias revisadas.

Tabla 3

Matriz de experiencias comparadas

Dimensión de análisis	Variables	Gestión de datos policiales	Tecnología SIEM
Fuente verificable	Documento	Hollywood et al. (2024), RAND, RRA108-22	González-Granadillo et al. (2021), Sensors, 21(14), 4759
Naturaleza	Alcance	Agenda de investigación sobre gobernanza y gestión de datos en organizaciones policiales	Revisión de funciones, tendencias y limitaciones de SIEM en infraestructuras críticas
Aplicación a DIRINCRI	Aporte	Ordenar roles, calidad de datos y necesidades de implementación	Definir fuentes de eventos, correlación y requisitos de integración
Presupuesto	Evidencia disponible	No se utiliza como fuente de precios de DIRINCRI	No se utiliza como presupuesto ni cotización de la propuesta
Resultados	Límite de transferencia	No acredita mejora cuantificada en DIRINCRI	No acredita reducción del 42 % ni una implementación concreta en Europol
Personal	Condición de adaptación	Responsables de datos y coordinación con usuarios investigadores	Administración técnica y analistas con competencias acreditadas
Normativa	Condición de adaptación	Compatibilizar gobernanza con competencias y protección de datos peruanas	Verificar tratamiento de datos, acceso remoto, almacenamiento y custodia
Sostenibilidad	Riesgo de transferencia	Diferencias de estructura, recursos y procesos entre instituciones	Volumen de eventos y costo recurrente dependen del entorno local
Lección	Decisión aplicable	Formalizar gobernanza antes de ampliar intercambios	Validar un piloto antes del despliegue y de comprometer cobertura continua

***Nota*.** Se sustituyen los casos institucionales con montos, marcas y resultados no acreditados por referencias documentales identificables: Hollywood et al. (2024) y González-Granadillo et al. (2021). La comparación extrae condiciones de adaptación; no presenta esas publicaciones como evaluaciones de un SIEM instalado en la Policía de Colombia o Europol ni extrapola resultados a DIRINCRI.

2.2.2. Métodos y hallazgos

El proceso de exploración de alternativas se sustentó en una estrategia metodológica integral que combinó análisis documental con información empírica de actores vinculados a la problemática. Se revisaron estudios científicos (2021-2025), informes internacionales y documentos institucionales sobre modernización tecnológica, gobernanza digital y soluciones de monitoreo policial avanzado.

Se emplearon técnicas cualitativas y cuantitativas para comprender las percepciones y experiencias de los participantes. El componente cualitativo comprendió trece entrevistas semiestructuradas: once a efectivos policiales y dos a expertos civiles vinculados con el tema de investigación. Las transcripciones fueron analizadas mediante ATLAS.ti para organizar los

segmentos relevantes y las categorías analíticas. Los perfiles de los participantes se presentan en el Anexo 11 y la matriz de codificación cualitativa, en el Anexo 12.

Tabla 4

Matriz fortalecida de rigor metodológico del componente cualitativo y su articulación con la matriz de consistencia

Criterio de rigor	Articulación con la matriz de consistencia	Aplicación operativa en el estudio	Evidencia verificable	Aporte para sustentación
Credibilidad	Correspondencia entre los problemas, los objetivos específicos y las categorías de ciberseguridad institucional, implicancias operativas y jurídicas, y estrategias de gobernanza digital.	Análisis de entrevistas semiestructuradas a 13 participantes: 11 policías y 2 expertos civiles, considerando sus experiencias y conocimientos relacionados con el tema investigado.	Transcripciones de las 13 entrevistas, registros del procesamiento en ATLAS.ti y fragmentos de respuestas que sustentan las interpretaciones. La nube de palabras se conserva como recurso complementario de visualización.	Permite examinar la correspondencia entre los testimonios, las categorías analíticas y los hallazgos presentados.
Transferibilidad	Delimitación del contexto institucional y del periodo de estudio 2024–2025, en relación con los problemas y objetivos de investigación.	Descripción de los perfiles de los participantes, sus funciones y su relación con la seguridad de la información y la investigación criminal, preservando su identificación mediante códigos en la presentación académica.	Caracterización del contexto, perfiles de los entrevistados y descripción de las condiciones institucionales a las que se refieren sus respuestas.	Proporciona información para valorar la pertinencia de los hallazgos en contextos similares, sin atribuirles generalización estadística.
Dependencia	Correspondencia entre los objetivos específicos, la guía de entrevista y el procedimiento de análisis cualitativo.	Organización y procesamiento de las 13 entrevistas en ATLAS.ti, manteniendo la relación entre los registros originales y los resultados expuestos.	Transcripciones y registros del análisis disponibles para su cotejo. La presentación final conserva la nube de palabras y no incluye las redes semánticas.	Facilita la revisión del procedimiento analítico y la identificación de los documentos que sustentan los resultados.
Confirmabilidad	Vinculación de las interpretaciones con las categorías	Fundamentación de los hallazgos mediante testimonios identificados por códigos,	Fragmentos de entrevistas y su correspondencia con las interpretaciones	Permite distinguir la evidencia aportada por los participantes de la interpretación del equipo

	de la matriz de consistencia y con las respuestas de los participantes.	considerando coincidencias y discrepancias entre las respuestas.	desarrolladas. La nube de palabras constituye un apoyo visual y no sustituye el examen del contenido de los testimonios.	investigador y de la propuesta tecnológica.

Nota. Elaboración propia a partir de los criterios de credibilidad, transferibilidad, dependencia y confirmabilidad de Lincoln y Guba (1985), adaptados al componente cualitativo del estudio. La matriz presenta los criterios de rigor del componente cualitativo y su articulación con la matriz de consistencia. Se analizaron en ATLAS.ti entrevistas correspondientes a 13 participantes: 11 policías y 2 expertos civiles. Las redes semánticas fueron retiradas de la presentación final por indicación del asesor; se conservó la nube de palabras como recurso visual complementario. Esta visualización no demuestra por sí sola relaciones entre categorías, saturación ni causalidad. La revisión de los hallazgos se sustenta en las transcripciones y los registros del análisis.

Alcance metodológico y trazabilidad de los datos

El estudio integra evidencia documental, entrevistas y una encuesta de percepciones con alcance exploratorio y descriptivo. El contexto institucional comprende el periodo 2024–2025, mientras que las entrevistas y encuestas corresponden al levantamiento realizado en 2025. La revisión posterior corrige cálculos, precisiones metodológicas e interpretaciones, sin modificar las respuestas originales ni atribuir al periodo investigado información obtenida posteriormente.

El componente cualitativo comprendió trece participantes: once policías y dos civiles expertos en el tema. Las transcripciones se analizaron mediante ATLAS.ti para organizar el contenido e interpretar las experiencias y valoraciones relacionadas con las categorías del estudio. La nube de palabras se conserva como un recurso visual complementario; por sí sola no demuestra causalidad, frecuencia de incidentes ni saturación de las categorías. Los hallazgos de las entrevistas se circunscriben a las experiencias de los participantes y no se presentan como porcentajes de la población policial.

Se empleó un muestreo no probabilístico por conveniencia, en el que participaron 83 efectivos policiales según su disponibilidad durante la aplicación de la encuesta. Los resultados describen las percepciones del grupo encuestado, sin que se acredite representatividad estadística respecto del conjunto de efectivos de las unidades estudiadas ni de toda la DIRINCR. La selección no se realizó mediante un procedimiento aleatorio sobre un padrón de personal elegible. Por ello, no corresponde atribuir a los resultados un nivel de confianza del 95 % ni un margen de error del 5 %, ni afirmar su representatividad estadística respecto de toda la DIRINCRI o del conjunto de efectivos de las unidades estudiadas. La disponibilidad pudo influir en la composición del grupo encuestado y constituye una limitación para generalizar los hallazgos.

Se administró un cuestionario de opinión de doce ítems, con una escala de respuesta de cinco niveles: 1, totalmente en desacuerdo; 2, en desacuerdo; 3, neutro; 4, de acuerdo; y 5, totalmente de acuerdo. El instrumento recogió las percepciones de los participantes sobre las limitaciones del monitoreo de seguridad digital, la importancia de proteger la información y la evidencia digital, y la necesidad de implementar mecanismos institucionales de protección. Sus respuestas expresan valoraciones del personal encuestado y no constituyen, por sí mismas, una medición técnica de la frecuencia de incidentes o del estado de seguridad de los equipos informáticos.

Las frecuencias, porcentajes, medias y desviaciones estándar describen las respuestas de los 83 participantes. El alfa de Cronbach aporta evidencia de consistencia interna de las puntuaciones obtenidas en este grupo, sin acreditar por sí solo la validez del instrumento ni la representatividad de la muestra. La trazabilidad del análisis se sustenta en la conservación de la base de respuestas, las transcripciones y los registros del procesamiento efectuado. Para sostener la denominación de diseño exploratorio secuencial, debe documentarse, además, que la fase cualitativa precedió y orientó la fase cuantitativa; mientras esa relación no se acredite, no corresponde afirmarla como una característica verificada del estudio.

Los resultados cuantitativos se presentan como estadísticas descriptivas de los 83 participantes. Los coeficientes alfa de Cronbach (α), las medias y las desviaciones estándar de la Tabla 5 fueron recalculados a partir de las respuestas individuales de la base original. Las medias y desviaciones estándar muestrales corresponden a los promedios de respuesta de cada participante por dimensión y para el instrumento total. No se utilizaron porcentajes redondeados para estos cálculos ni se realizaron comparaciones inferenciales entre grupos.

$$\alpha = \frac{n}{n-1}\left(1 - \frac{\sum_{i=1}^{n} V_i}{V_T}\right)$$

Fórmula: Donde:

n = número de ítems de la escala.

Vi = varianza de cada ítem.

VT = varianza total de la suma de los ítems.

Tabla 5

Consistencia interna y estadísticos descriptivos por dimensión (n = 83)

Dimensión	k	Media	Desv. Est.	Alfa (α)
OE1	4	3.648	1.094	0.746
OE2	4	3.855	1.048	0.790
OE3	4	4.298	1.015	0.933
Instrumento total	12	3,934	0,916	0.906

***Nota*.** Elaboración propia a partir de las 83 respuestas individuales de la encuesta aplicada en 2025. Las medias y desviaciones estándar muestrales se calcularon sobre el promedio de respuestas de cada participante en cada dimensión y en el instrumento total. Escala Likert de 1 (totalmente en desacuerdo) a 5 (totalmente de acuerdo). El alfa de Cronbach se calculó con las respuestas individuales a los ítems. Los resultados se presentan con tres decimales.

El instrumento presentó un alfa de Cronbach global de 0,906, calculado a partir de las respuestas individuales de los 83 participantes. Por dimensión, los coeficientes fueron de 0,746 para OE1, 0,790 para OE2 y 0,933 para OE3. Las medias y desviaciones estándar de los promedios individuales fueron, respectivamente, M = 3,648 y DE = 1,094; M = 3,855 y DE = 1,048; y M = 4,298 y DE = 1,015. Estos resultados aportan evidencia de consistencia interna de las puntuaciones en el grupo estudiado. El mayor coeficiente de OE3 expresa una mayor relación entre sus ítems, sin demostrar por sí solo uniformidad de opiniones. La consistencia interna no acredita estabilidad temporal, validez del instrumento ni representatividad de la muestra. Los estadísticos descriptivos deben interpretarse junto con la distribución de las respuestas.

La Tabla 6 presenta una matriz académica de priorización de alternativas para la propuesta SIEM-DIRINCRI, mediante ponderación simple de criterios de idoneidad, impacto, factibilidad técnica, viabilidad financiera, deseabilidad y disrupción organizacional. Sus puntajes permiten comparar las alternativas bajo los supuestos del estudio, pero no acreditan por sí mismos sostenibilidad financiera ni constituyen una evaluación de inversión aprobada. El análisis de sensibilidad y las condiciones presupuestales se desarrollan a continuación.

Tabla 6

Matriz Multicriterio de Priorización de Alternativas Proyecto SIEM-DIRINCRI PNP (Enfoque Invierte.pe) Priorización de alternativas mediante ponderación simple

Criterio	Peso	A1: Modelo actual	A2: SaaS + SOC híbrido	A3: On-premise más SOC propio
Idoneidad	0.25	2	5	4
Impacto	0.20	2	5	4
Factibilidad técnica	0.15	4	4	3
Viabilidad financiera	0.15	5	3	2
Deseabilidad	0.15	2	4	3
Disrupción organizacional	0.10	4	3	2
Puntaje total ponderado	1.00	2.95	4.20	3.20

***Nota*.** Puntaje = suma de peso x calificación. Escala: 1 a 5; en disrupción organizacional una nota mayor representa menor dificultad de adopción. Pesos originales: 0,25; 0,20; 0,15; 0,15; 0,15; 0,10. Los totales corregidos son A1 = 2,95; A2 = 4,20; A3 = 3,20. Su carácter analítico exige validación por las áreas responsables antes de una decisión de gasto.

Análisis de sensibilidad y condición presupuestal

El peso financiero de 0,15 refleja la priorización original de adecuación e impacto, pero no resulta suficiente para acreditar asequibilidad. Para probar su efecto, se modifica solo ese peso a f y se redistribuyen proporcionalmente los otros cinco: nuevo peso = peso original x (1 - f) / 0,85. Las calificaciones permanecen constantes. Los escenarios no constituyen una nueva consulta a expertos.

Con f = 0,15, A2 aventaja a A1 en 1,25 puntos. Con f = 0,40 la ventaja se reduce a 0,2941. A1 y A2 empatan cuando f = 0,4785 aproximadamente; por encima, A1 obtiene mayor puntaje. A2 conserva el primer lugar en los escenarios de 0,25 y 0,40, pero la preferencia no es incondicional. El riesgo R4 mantiene nivel 6, rojo, y exige acreditar recursos para implementación y operación antes de contratar.

La puerta de decisión para A2 requiere costo total validado, previsión de gasto recurrente, dotación mínima, aprobación de la arquitectura y reglas de protección de datos. Si alguna condición no se cumple, corresponde ajustar el alcance del piloto o reevaluar alternativas; un puntaje mayor no sustituye la factibilidad presupuestal.

Tabla 6-A

Análisis de sensibilidad de la priorización de alternativas según el peso de la viabilidad financiera

Peso financiero	A1	A2	A3
0.15	2.9500	4.2000	3.2000
0.25	3.1912	4.0588	3.0588
0.40	3.5529	3.8471	2.8471
0.50	3.7941	3.7059	2.7059

Nota. Elaboración propia a partir de los pesos y calificaciones de la Tabla 6. Para cada escenario, el peso financiero se fija en f y los demás pesos se redistribuyen proporcionalmente mediante la expresión: peso original x (1 - f) / 0,85. Las calificaciones permanecen constantes y los resultados se presentan con cuatro decimales. A1: modelo actual; A2: SaaS + SOC híbrido; A3: infraestructura local (*on-premise*) con SOC propio. Los escenarios son analíticos y no acreditan disponibilidad presupuestal.

2.2.2.1. Hallazgos y resultados

En el marco de la investigación aplicada titulada “Ausencia de mecanismos y sistemas de seguridad digital en los equipos informáticos de la Dirección de Investigación Criminal (DIRINCRI) de la PNP, 2024 - 2025”, resulta indispensable comprender cómo se manifiestan conceptual y operativamente, los principales factores que condicionan la madurez institucional en ciberseguridad. La categoría definida como

Ciberseguridad institucional permite identificar, con mayor precisión, las brechas que impactan directamente en la confiabilidad de los procesos de investigación criminal y en la protección de los activos digitales estratégicos que la DIRINCRI gestiona a diario.

Desde una perspectiva de gestión pública orientada a resultados, la identificación de patrones, conceptos emergentes y términos recurrentes resulta vital, pues permite priorizar inversiones, orientar decisiones estratégicas y sustentar técnicamente la necesidad de incorporar capacidades institucionales permanentes en materia de vigilancia digital. La nube de palabras analizada constituye, por ello, un insumo metodológico relevante: sintetiza la percepción de los actores, revela la direccionalidad de los problemas y aporta evidencia cualitativa clave para comprender por qué la seguridad informática sigue siendo un componente vulnerable dentro de los procesos policiales de investigación.

Figura 4

Nube de palabras sobre conceptos asociados a ciberseguridad institucional en la DIRINCRI (2024-2025)



Nota. Elaboración propia basada en el procesamiento cualitativo de términos vinculados a riesgos, capacidades, brechas y necesidades institucionales en materia de seguridad digital. Generado con el software de análisis cualitativo ATLAS.ti.

La ausencia de mecanismos de seguridad digital en la DIRINCRI refleja un problema estructural que combina debilidades tecnológicas, organizacionales y humanas. La nube de palabras evidencia que la principal carencia es la falta de un sistema de vigilancia constante que garantice integridad, disponibilidad y trazabilidad de la información policial. En un contexto donde la criminalidad organizada emplea

tecnologías avanzadas, la institución necesita sistemas de correlación y análisis que anticipen y neutralicen amenazas.

La reiterada aparición de conceptos como amenazas, vulnerabilidad, filtraciones y ataques confirma que la exposición actual compromete activos digitales y el valor probatorio de la evidencia. Este riesgo afecta la confiabilidad de las investigaciones y la legitimidad de los procesos judiciales. Además, el factor humano resulta esencial para la sostenibilidad de cualquier estrategia de ciberseguridad. Palabras como capacitación, concientización, competencias y liderazgo muestran que el fortalecimiento del talento institucional es indispensable. La solución requiere equilibrar sistemas robustos con personal altamente calificado.

Para la construcción de la nube de palabras y el análisis de redes semánticas mediante el software de análisis cualitativo ATLAS.ti, se incorporarán como fuentes de información las transcripciones de las entrevistas realizadas a especialistas, conforme a la muestra definida. A partir de dichas transcripciones se realizará el proceso de codificación de los segmentos más relevantes, asignando códigos que posteriormente se agruparán en categorías analíticas vinculadas con los objetivos del estudio. Este procedimiento permitirá identificar patrones conceptuales y relaciones entre factores institucionales, normativos y tecnológicos asociados a la problemática de la seguridad digital en la DIRINCRI de la PNP. Los resultados del análisis se representarán gráficamente mediante redes semánticas, las cuales facilitarán la interpretación de los factores que inciden en la ausencia de mecanismos y sistemas de seguridad digital en los equipos informáticos de dicha unidad policial.

Orientado a explorar los factores institucionales, normativos y tecnológicos vinculados con la ausencia de mecanismos y sistemas de seguridad digital en la DIRINCRI de la PNP, el análisis cualitativo permitirá organizar la información obtenida de los especialistas en categorías temáticas que evidencien las principales condiciones que inciden en la problemática estudiada.

El análisis de redes semánticas permitirá identificar las relaciones conceptuales entre los factores institucionales, normativos y tecnológicos asociados a la problemática de la seguridad digital en la DIRINCRI. A partir de la codificación de las entrevistas, se buscará determinar cómo aspectos como la gestión institucional, las limitaciones presupuestales, la infraestructura tecnológica disponible y los marcos normativos vigentes influyen en la implementación de mecanismos formales de seguridad digital. Asimismo, el análisis permitirá explorar la forma en que estas condiciones pueden

incidir en la adopción de soluciones tecnológicas de monitoreo y gestión de incidentes de seguridad, tales como sistemas de gestión de eventos e información de seguridad (SIEM). De igual modo, se analizará la existencia de posibles brechas en la gobernanza institucional de los activos digitales, incluyendo factores organizacionales y de capacidades técnicas del personal que podrían afectar la adecuada protección de la información vinculada a las investigaciones criminales.

El análisis cualitativo realizado mediante ATLAS.ti, basado en la codificación y categorización de las entrevistas a especialistas, se integrará con la información cuantitativa obtenida a través del cuestionario con escala Likert. Los datos estadísticos serán procesados en una hoja de cálculo de Microsoft Excel, lo que permitirá organizar y describir las tendencias de las respuestas de los participantes. La articulación de ambas fuentes de información facilitará un análisis complementario del problema de investigación, integrando la perspectiva interpretativa del análisis cualitativo con los patrones identificados en los datos cuantitativos. Este procedimiento metodológico permitirá aproximarse de manera más completa al objeto de estudio, como se sintetiza en la tabla 7.

Tabla 7

Distribución porcentual de las percepciones sobre reglas, protección de equipos, capacitación y recursos para la seguridad digital en las unidades estudiadas

Descripción de la pregunta	Totalmente en desacuerdo	En desacuerdo	Neutro	De acuerdo	Totalmente de acuerdo
En la unidad donde trabajo no existen reglas claras o procedimientos para proteger la información digital	24%	2%	31%	8%	34%
Considero que los equipos de cómputo que utilizamos no cuentan con la seguridad necesaria para evitar el acceso no autorizado	13%	0%	20%	12%	54%
En la DIRINCRI no se brinda suficiente orientación o capacitación sobre cómo proteger los datos que manejamos	19%	7%	25%	12%	36%
La falta de recursos o apoyo técnico limita la instalación de programas o sistemas que mejoren la seguridad digital	10%	4%	19%	11%	57%

Nota. Elaboración propia a partir de las 83 respuestas válidas por ítem de la encuesta aplicada en 2025. Los porcentajes de las categorías se presentan redondeados a números enteros; por ello, sus totales pueden diferir del 100 %. Los porcentajes agrupados de la interpretación se calcularon directamente a partir de las frecuencias originales.

La Tabla 7 muestra percepciones diversas entre los 83 efectivos encuestados sobre las condiciones institucionales relacionadas con la seguridad digital. Ante la afirmación

de que en su unidad no existen reglas claras o procedimientos para proteger la información digital, las categorías «de acuerdo» y «totalmente de acuerdo» suman un 42 %, mientras que un 31 % respondió de manera neutral y un 26 % manifestó desacuerdo o total desacuerdo. Esta distribución no permite afirmar una percepción compartida por todos los participantes sobre la ausencia de reglas. La neutralidad se considera por separado y no se interpreta como acuerdo ni como desacuerdo.

Respecto de la afirmación de que los equipos de cómputo no cuentan con la seguridad necesaria para evitar accesos no autorizados, el acuerdo y el total acuerdo suman un 66 %, frente a un 20 % de respuestas neutrales y un 13 % de desacuerdo o total desacuerdo. En cuanto a la insuficiente orientación o capacitación para proteger los datos, el acuerdo y el total acuerdo alcanzan un 48 %, la neutralidad representa un 25 % y el desacuerdo o total desacuerdo suman un 26 %. Por tanto, aunque una parte de los encuestados percibe limitaciones de capacitación, no corresponde afirmar un una absoluto sobre esta carencia.

Finalmente, ante la afirmación de que la falta de recursos o apoyo técnico limita la instalación de programas o sistemas de seguridad digital, la Tabla 7 muestra percepciones diversas entre los 83 efectivos encuestados. Ante la afirmación de que en su unidad no existen reglas claras o procedimientos para proteger la información digital, 35 participantes expresaron acuerdo o total acuerdo (42,17 %), 26 respondieron de manera neutral (31,33 %) y 22 manifestaron desacuerdo o total desacuerdo (26,51 %). Esta distribución no permite afirmar una percepción compartida por todos los participantes sobre la ausencia de reglas. La neutralidad se interpreta de forma independiente.

Respecto de la protección insuficiente de los equipos frente al acceso no autorizado, 55 participantes expresaron acuerdo o total acuerdo (66,27 %), 17 respondieron de manera neutral (20,48 %) y 11 manifestaron desacuerdo o total desacuerdo (13,25 %). En cuanto a la insuficiente orientación o capacitación, las respuestas fueron 40 de acuerdo o total acuerdo (48,19 %), 21 neutrales (25,30 %) y 22 de desacuerdo o total desacuerdo (26,51 %). Aunque una parte del grupo percibe limitaciones de capacitación, los resultados no acreditan consenso absoluto.

Finalmente, 56 participantes expresaron acuerdo o total acuerdo con que la falta de recursos o apoyo técnico limita la instalación de programas o sistemas de seguridad digital (67,47 %); 16 respondieron de manera neutral (19,28 %) y 11 manifestaron desacuerdo o total desacuerdo (13,25 %). Los porcentajes agrupados se calcularon

directamente desde las frecuencias originales, con 83 respuestas por ítem. Estos resultados describen percepciones del grupo encuestado y no acreditan, por sí solos, deficiencias técnicas, disponibilidad presupuestal ni relaciones causales.

A continuación, la Tabla 8 presenta las percepciones de los participantes sobre las posibles implicancias operativas, jurídicas y sociales relacionadas con el monitoreo y la trazabilidad digital en la investigación criminal. Su interpretación distingue las valoraciones del personal encuestado de la comprobación técnica o jurídica de esas implicancias; asimismo, las respuestas sobre confianza ciudadana expresan la opinión de los efectivos participantes y no una medición directa de las opiniones de la ciudadanía.

Tabla 8

Distribución porcentual de percepciones sobre las implicancias operativas, jurídicas y sociales derivadas de la falta de monitoreo y trazabilidad digital en la DIRINCRI (2024-2025)

Descripción de la pregunta	Totalmente en desacuerdo	En desacuerdo	Neutro	De acuerdo	Totalmente de acuerdo
La falta de control digital hace difícil saber quién accedió o modificó un archivo de una investigación	10%	5%	28%	12%	46%
Considero que no existe un seguimiento adecuado sobre el uso de la información digital en las investigaciones	14%	1%	24%	19%	41%
Cuando no se protege bien la información, se pone en riesgo la validez de la evidencia en el proceso judicial	11%	4%	19%	12%	54%
La ausencia de medidas de seguridad digital afecta la confianza de los ciudadanos en el trabajo policial	7%	5%	22%	17%	49%

Nota. Elaboración propia a partir de las 83 respuestas válidas por ítem de la encuesta aplicada en 2025. Los porcentajes de las categorías se presentan redondeados a números enteros; por ello, sus totales pueden diferir del 100 %. Los porcentajes agrupados de la interpretación se calcularon directamente a partir de las frecuencias originales.

La tabla 8 permite identificar tendencias en la percepción del personal policial respecto a las implicancias operativas, jurídicas y sociales asociadas a la ausencia de mecanismos de monitoreo digital en los procesos de investigación criminal. La Tabla 8 recoge las percepciones de los 83 participantes sobre las posibles implicancias operativas, jurídicas y sociales de las limitaciones del monitoreo digital. Al agrupar «de acuerdo» y «totalmente de acuerdo», 48 participantes consideran que la falta de control dificulta identificar quién accedió o modificó un archivo de investigación (57,83 %); 50 perciben un seguimiento insuficiente del uso de la información (60,24 %); y 55

consideran que una protección insuficiente puede poner en riesgo la validez de la evidencia en el proceso judicial (66,27 %). Asimismo, 55 participantes relacionan la ausencia de medidas de seguridad digital con posibles afectaciones a la confianza ciudadana (66,27 %). Estas respuestas expresan valoraciones del personal encuestado: no demuestran incidentes específicos, invalidez jurídica de evidencias ni cambios efectivamente medidos en la confianza de los ciudadanos.

Orientado a identificar estrategias institucionales y alternativas tecnológicas para el fortalecimiento de la ciberseguridad y de la gobernanza digital en la DIRINCRI, en concordancia con las buenas prácticas internacionales y la normativa peruana vigente, el análisis cualitativo permitirá examinar las propuestas y criterios técnicos señalados por los especialistas entrevistados. A partir del proceso de codificación y categorización desarrollado mediante el software ATLAS.ti, se organizarán los segmentos relevantes de las entrevistas en categorías analíticas relacionadas con herramientas tecnológicas, modelos de gestión de seguridad de la información y estrategias institucionales de fortalecimiento.

Este procedimiento permitirá explorar la pertinencia de diversas alternativas tecnológicas y organizacionales orientadas a mejorar la capacidad institucional de monitoreo, detección y respuesta frente a incidentes de seguridad digital. En este contexto, el análisis considerará tecnologías y prácticas reconocidas en el ámbito de la ciberseguridad, tales como sistemas de gestión de eventos e información de seguridad (SIEM), mecanismos de autenticación multifactor, gestión de identidades digitales, procedimientos de análisis forense digital y enfoques de arquitectura de seguridad basados en principios como *Zero Trust*, así como el uso de técnicas de integridad de datos como el *hashing* y otras soluciones emergentes orientadas a reforzar la trazabilidad y protección de la información.

De igual modo, el análisis incorporará factores organizacionales vinculados con la gestión institucional de la ciberseguridad, tales como la definición de roles y responsabilidades, el liderazgo institucional, la planificación estratégica y el fortalecimiento de las capacidades del personal encargado de la gestión de incidentes de seguridad digital.

La interpretación cualitativa se complementará con la información cuantitativa obtenida mediante la aplicación de un cuestionario con escala Likert. Los datos serán

organizados y procesados en una hoja de cálculo de Microsoft Excel, permitiendo describir tendencias en las percepciones del personal policial respecto a las condiciones de seguridad digital y a la necesidad de implementar mecanismos tecnológicos e institucionales de protección de los activos digitales. La integración de ambas fuentes de información facilitará una aproximación analítica más completa al fenómeno estudiado, conforme se sintetiza en la tabla 9.

Tabla 9

Percepción del personal sobre las estrategias institucionales y alternativas tecnológicas para fortalecer la ciberseguridad y la gobernanza digital en la DIRINCRI (2024-2025)

Descripción de la pregunta	Totalmente en desacuerdo	En desacuerdo	Neutro	De acuerdo	Totalmente de acuerdo
Sería útil que todo el personal reciba capacitación básica sobre cómo proteger la información en los equipos de cómputo	4%	2%	14%	10%	70%
La creación de un área especializada que supervise la seguridad digital mejoraría la protección de los datos	4%	6%	16%	14%	60%
Contar con programas que registren automáticamente las actividades en los equipos ayudaría a mejorar la seguridad	6%	4%	18%	12%	60%
Creo que la DIRINCRI debería modernizar sus sistemas informáticos para evitar riesgos de pérdida o filtración de información	4%	2%	12%	13%	69%

Nota. Elaboración propia a partir de las 83 respuestas válidas por ítem de la encuesta aplicada en 2025. Los porcentajes de las categorías se presentan redondeados a números enteros; por ello, sus totales pueden diferir del 100 %. Los porcentajes agrupados de la interpretación se calcularon directamente a partir de las frecuencias originales.

La tabla 9 permite identificar tendencias en la percepción del personal policial respecto a las estrategias institucionales y alternativas tecnológicas orientadas al fortalecimiento de la ciberseguridad en la DIRINCRI. La Tabla 9 muestra una valoración favorable de las estrategias propuestas entre los 83 participantes. Al agrupar «de acuerdo» y «totalmente de acuerdo», 66 consideran útil que el personal reciba capacitación básica en protección de información (79,52 %); 62 valoran favorablemente la creación de un área especializada que supervise la seguridad digital (74,70 %); 60 consideran útiles los programas de registro automático de actividades (72,29 %); y 68 respaldan la modernización de los sistemas informáticos para prevenir riesgos de pérdida o filtración de información (81,93 %). Estos resultados orientan la evaluación de alternativas y necesidades de formación, pero no acreditan la eficacia de una solución implementada ni justifican, por sí solos, una decisión de contratación. La utilidad

atribuida a la capacitación tampoco equivale a afirmar que todos los participantes consideran insuficiente la formación existente.

Previo al proceso de evaluación, resulta pertinente identificar las principales alternativas tecnológicas disponibles dentro de la familia de soluciones SIEM (*Security Information and Event Management*), considerando que el capítulo desarrolla como propuesta general la implementación de un sistema institucional de monitoreo y gestión de eventos de ciberseguridad para la DIRINCRI.

En el ámbito de la ciberseguridad institucional, las soluciones SIEM suelen clasificarse en distintas modalidades según su arquitectura tecnológica, modelo de despliegue y nivel de integración con otros sistemas de seguridad. Entre las alternativas más utilizadas se encuentran: SIEM basado en infraestructura local (*on-premise*), que permite a la institución mantener el control directo de la infraestructura y de los datos sensibles; SIEM en la nube (*cloud-based*), que ofrece escalabilidad y reducción de costos de infraestructura; SIEM híbrido, que combina capacidades locales y servicios en la nube para optimizar la gestión de eventos de seguridad; y SIEM gestionado o *SOC-as-a-Service*, en el cual parte del monitoreo y análisis de eventos es realizado por proveedores especializados.

Cada una de estas alternativas presenta ventajas y limitaciones en términos de seguridad de la información, costos de implementación, capacidad de integración con sistemas existentes y sostenibilidad operativa. Por ello, en el siguiente apartado se realiza una evaluación comparativa considerando criterios de idoneidad técnica, impacto institucional, deseabilidad social, factibilidad presupuestal y sostenibilidad, con el propósito de determinar la opción más adecuada para el contexto operativo y normativo de la DIRINCRI de la Policía Nacional del Perú.

2.2.3. Evaluación de alternativas

Al evaluar las alternativas identificadas se consideraron criterios como idoneidad técnica, impacto institucional, deseabilidad social, factibilidad presupuestal y sostenibilidad. Las opciones menos complejas (como herramientas aisladas de antivirus o monitoreo puntual), no responden a la necesidad de análisis integral ni ofrecen mecanismos de trazabilidad confiables. Por el contrario, las soluciones que permiten consolidar registros, correlacionar eventos relevantes y generar alertas tempranas se alinean con los estándares actuales de gobierno digital y seguridad de la información. La alternativa priorizada es la Implementación del Sistema Institucional de Gestión y Monitoreo de Eventos de Ciberseguridad (SIEM-PNP).

Tabla 10

Evaluación de alternativas para la implementación de una solución tecnológica de monitoreo y gestión de eventos de seguridad digital

Alternativa tecnológica	Idoneidad técnica	Impacto institucional	Factibilidad presupuestal	Sostenibilidad operativa	Valoración general
SIEM On-Premise (infraestructura local)	Alto nivel de control sobre datos y registros; mayor capacidad de personalización e integración con sistemas internos.	Alto impacto en la gestión de seguridad digital al centralizar registros y mejorar la trazabilidad de eventos.	Requiere inversión inicial elevada en infraestructura, licencias y personal especializado.	Alta sostenibilidad si se dispone de personal técnico permanente y mantenimiento institucional.	Alta
SIEM en la nube (Cloud SIEM)	Escalabilidad y actualización permanente del sistema; menor necesidad de infraestructura local.	Impacto significativo en la capacidad de monitoreo y detección temprana de incidentes.	Inversión inicial moderada basada en modelo de suscripción; reduce costos de hardware.	Dependencia de proveedores externos y de conectividad institucional estable.	Media-Alta
SIEM híbrido (infraestructura local + nube)	Combina control institucional sobre datos sensibles con capacidades analíticas de la nube.	Alto impacto institucional al permitir monitoreo flexible y mayor capacidad de correlación de eventos.	Inversión moderada; combina infraestructura propia con servicios externos.	Alta sostenibilidad si se gestiona adecuadamente la interoperabilidad tecnológica.	Muy alta
SIEM gestionado (SOC-as-a-Service)	Monitoreo continuo realizado por especialistas externos con tecnologías avanzadas.	Mejora rápida de capacidades de respuesta ante incidentes sin necesidad de crear estructura interna compleja.	Costos operativos periódicos; menor inversión inicial en infraestructura.	Dependencia de proveedores y limitaciones en el control directo de los datos institucionales.	Media

Nota. La valoración se realiza considerando criterios de idoneidad técnica, impacto institucional, factibilidad presupuestal y sostenibilidad operativa en el contexto de las necesidades de seguridad digital de la Dirección de Investigación Criminal (DIRINCRI) de la Policía Nacional del Perú. Elaboración propia.

2.2.3.1. Acciones clave sobre elementos críticos

El análisis de la problemática permitió identificar un conjunto de elementos críticos que obstaculizan la capacidad institucional de la DIRINCRI para gestionar de manera efectiva la seguridad digital. Abordar estos factores requiere plantear acciones estratégicas que no solo atiendan las brechas tecnológicas, sino también los aspectos organizacionales, normativos y culturales que influyen en la respuesta institucional. La primera acción esencial es establecer un marco de gobernanza digital claro, con

responsabilidades, líneas de reporte y protocolos frente a incidentes tecnológicos. Esto ordena procesos internos, reduce la fragmentación funcional y asegura decisiones coherentes. El objetivo es garantizar una gestión institucional orientada a resultados en materia digital.

El segundo elemento crítico es fortalecer las capacidades humanas, pues la falta de personal especializado y la escasa formación continua limitan el uso de herramientas avanzadas de monitoreo y trazabilidad digital. Se requieren programas en tres niveles: capacitación operativa para usuarios finales, diplomados para personal técnico y analistas de seguridad, y certificaciones profesionales para especialistas estratégicos. Estos procesos deben fomentar una cultura organizacional que valore la seguridad digital como parte de la labor diaria, asegurando sostenibilidad y eficacia en la gestión institucional.

Mientras se consolidan las capacidades institucionales, puede evaluarse la incorporación de especialistas civiles para reforzar de inmediato la ciberseguridad y el análisis digital. Si es temporal, se canalizaría mediante contratación CAS; si es permanente, correspondería un proceso de asimilación. Esta alternativa permitiría transferir conocimiento especializado al personal policial y acelerar el uso de herramientas tecnológicas previstas. La literatura especializada coincide en que la tecnología solo tiene impacto real cuando existe capital humano con competencias adecuadas.

Un aspecto crítico son los procesos administrativos y contractuales regulados por la Ley de Contrataciones del Estado. La lentitud, la falta de estandarización en los términos de referencia y la débil articulación entre áreas generan retrasos en la adopción de soluciones tecnológicas. Se requieren mecanismos de contratación más eficientes, con expedientes técnicos que definan claramente requerimientos, interoperabilidad, métricas de desempeño y garantías mínimas de continuidad. Esta acción permitirá reducir sobrecostos, evitar adquisiciones inadecuadas y asegurar que las herramientas tecnológicas respondan a las necesidades reales de la unidad.

La investigación evidenció la necesidad de fortalecer la ruta técnica de integración, dado que la DIRINCRI opera con infraestructura heterogénea y poco articulada. Es indispensable estandarizar procesos de interoperabilidad, establecer protocolos para el registro y correlación de eventos, y desarrollar mecanismos de

comunicación entre sistemas como SIDPOL, RENIEC, Ministerio Público y DIRTIC-PNP. Estas medidas permitirán construir una arquitectura digital coherente y facilitar la trazabilidad en cada fase de la investigación criminal.

Finalmente, la ruta estratégica exige alinear la modernización digital con instrumentos de gestión como el PEI-PNP, el PEI del MININTER y la Política Nacional de Transformación Digital. Esto asegura sostenibilidad presupuestal, respaldo político y prioridad de Estado para su implementación a largo plazo. Además, la articulación con la SEGDI-PCM y organismos internacionales garantiza estándares adecuados de ciberseguridad, interoperabilidad y gobernanza institucional.

Estas acciones muestran que la solución tecnológica no es un fin aislado, sino parte de un proceso integral que articula gobernanza, capital humano, gestión administrativa, interoperabilidad y planificación estratégica que posibilitará cerrar brechas y orientar a la DIRINCRI hacia un modelo de seguridad digital robusto, sostenible y acorde al entorno contemporáneo.

Capítulo 3: Proponer

3.1. Propuesta de solución: Conceptualización y fundamentos de la solución tecnológica

La propuesta consiste en implementar gradualmente un Sistema Institucional de Gestión y Monitoreo de Eventos de Ciberseguridad, basado en tecnología SIEM, en la DIRINCRI. Su alcance inicial comprenderá las unidades, activos y fuentes de eventos que se seleccionen mediante un inventario y una evaluación de criticidad, capacidades operativas y recursos disponibles.

El sistema permitiría centralizar registros, correlacionar eventos y generar alertas para apoyar la detección y atención de incidentes. La oportunidad de respuesta dependerá del horario aprobado, la disponibilidad de analistas, la calidad de los registros y los procedimientos de escalamiento. El monitoreo puede contribuir a documentar actuaciones y preservar información, pero no garantiza por sí solo autenticidad, admisibilidad ni valor probatorio de la evidencia.

La articulación con DIRTIC y otras entidades se desarrollará conforme a sus competencias, autorizaciones y acuerdos aplicables. Los estándares técnicos se utilizarán como orientación para diseñar controles y procedimientos, sin atribuir a la propuesta certificaciones o integraciones ya ejecutadas.

La evaluación económica distinguirá los costos iniciales y los gastos recurrentes de implementación, operación y mantenimiento. Los importes utilizados son aproximaciones para la comparación académica de alternativas; deberán revisarse mediante dimensionamiento técnico e información económica documentada. La clasificación presupuestal y contable corresponderá a las áreas competentes.

La propuesta no acredita financiamiento aprobado. El PIA y el PIM son instrumentos presupuestarios y no constituyen fuentes de financiamiento por sí mismos. Antes de ejecutar o contratar, deberán identificarse la fuente, la disponibilidad de recursos y la previsión de operación y mantenimiento, así como determinarse la aplicabilidad del sistema de inversiones. En consecuencia, la viabilidad financiera permanece condicionada.

3.1.1. Características generales

La propuesta plantea implementar gradualmente un Sistema Institucional de Gestión y Monitoreo de Eventos de Ciberseguridad, basado en tecnología SIEM, en la DIRINCRI. Su

fase inicial comprenderá fuentes de eventos seleccionadas a partir del inventario técnico, la criticidad de los activos y las capacidades disponibles. La incorporación de otros equipos, servidores y aplicaciones quedará condicionada a los resultados del piloto y a la disponibilidad de recursos.

El sistema generará alertas automáticas ante actividades que cumplan las reglas de detección configuradas. Su análisis y atención se efectuarán conforme al horario aprobado, los responsables designados y los procedimientos de escalamiento. La captura automatizada de eventos se diferenciará de la atención humana, sin presumir una cobertura operativa permanente.

La solución incorporará controles para fortalecer la trazabilidad y preservar la integridad de los registros que puedan resultar relevantes para una investigación. Su utilización como evidencia requerirá procedimientos documentados de preservación, acceso, exportación y cadena de custodia; la implementación del SIEM no garantiza por sí sola su valor probatorio. Las coordinaciones e integraciones institucionales se definirán conforme a las competencias, autorizaciones y condiciones técnicas correspondientes.

La evaluación económica distingue desembolso inicial y gasto recurrente. Para la modalidad A2, las suscripciones y licencias anuales se registran como gasto operativo en el modelo de costos, evitando duplicarlas como inversión inicial y renovación del mismo periodo. La clasificación presupuestal y contable definitiva será determinada por las áreas competentes según el objeto de la contratación y el tratamiento de los activos.

Los montos presentados son aproximaciones utilizadas para la comparación académica de alternativas. Para obtener información económica verificable se requería documentación técnica que el equipo investigador no logró reunir durante el desarrollo del estudio. Por esta limitación, no se dispone de cotizaciones ni de un estudio de mercado que permitan validar los importes consignados. Estos valores no constituyen un presupuesto aprobado y deberán revisarse mediante el dimensionamiento técnico y la obtención de información económica documentada antes de cualquier decisión de contratación.

El PIA y el PIM son instrumentos presupuestarios, no fuentes de financiamiento por sí mismos. La propuesta no acredita una asignación aprobada. Antes de comprometer gasto, las áreas competentes deberán identificar la fuente de financiamiento, la disponibilidad de recursos y la previsión de operación y mantenimiento para los años previstos. Asimismo, deberán determinar la aplicabilidad del sistema de inversiones y la modalidad de contratación

correspondiente; el bosquejo académico del Anexo 2 no equivale a una inversión formulada, viable o aprobada.

La contratación y ampliación del servicio quedarán condicionadas a la validación técnica y económica, la disponibilidad de personal competente y la acreditación de recursos. Si estas condiciones no se cumplen, se ajustará el alcance del piloto o se reevaluarán las alternativas.

3.1.2. Sustento institucional y estratégico de la propuesta

La propuesta de implementar un sistema SIEM en la DIRINCRI-PNP se fundamenta en el *Pilar IV "Nuestra TIC" del Modelo Mariano Santos 2030 (MS30)*, que impulsa la modernización tecnológica policial mediante interoperabilidad, infraestructura digital segura y estandarización de procesos. Este pilar, recogido en el PEI 2025-2030 del Ministerio del Interior, se materializa en la Acción Estratégica Institucional AEI.8.1, destinada al fortalecimiento institucional de la PNP. En este marco, el PEI establece que los proyectos tecnológicos deben contribuir a mejorar las capacidades del Sistema de TIC Institucional, posicionando la propuesta como coherente con las prioridades estratégicas sectoriales y policiales. Asimismo, el Objetivo Estratégico Institucional OEI.8 refuerza la iniciativa al promover proyectos tecnológicos financiados oportunamente, evidenciando que la incorporación de un SIEM responde a una política institucional formal orientada a incrementar la eficiencia operativa y la seguridad de la información.

Desde el enfoque de planificación por resultados, el proyecto se articula con unidades responsables como la DIRTIC-PNP, la División de Infraestructura y la División de Talento Humano, que intervienen tanto en la incorporación de tecnologías como en la capacitación del personal. Además, la propuesta se integra a la cadena de valor público: aporta infraestructura y talento humano en los insumos, introduce monitoreo y correlación de eventos en los procesos, entrega evidencia íntegra y alertas tempranas como productos, y genera resultados que optimizan el desempeño institucional y fortalecen la confianza ciudadana. Esta secuencia lógica, alineada con el PEI, asegura una implementación gradual, sostenible y ajustada a los estándares internacionales de seguridad, consolidando la modernización tecnológica de la Policía Nacional hacia el 2030.

3.1.3. Descripción de la propuesta de solución

La propuesta plantea implementar un sistema institucional de monitoreo y gestión de eventos digitales en la DIRINCRI, capaz de supervisar, analizar y correlacionar en tiempo real

los incidentes de seguridad. Este sistema funcionará como eje articulador de la seguridad digital, fortaleciendo la protección de activos críticos y mejorando la coordinación con las áreas responsables de ciberseguridad. Al integrar fuentes como servidores, bases de datos, aplicaciones y equipos de usuario, generará una visión completa del entorno digital y se alineará con estándares internacionales como ISO/IEC 27032, ISO 27001 y NIST SP 800-137, garantizando compatibilidad con lineamientos del Gobierno Digital.

Asimismo, la solución incorpora un componente formativo y organizacional que facilitará su adopción por parte del personal, asegurando que las capacidades técnicas se acompañen de una cultura institucional orientada a la prevención y respuesta efectiva. Con ello, se busca consolidar una estrategia integral que no solo refuerce la seguridad digital, sino que también promueva la sostenibilidad operativa y la resiliencia institucional frente a incidentes, fortaleciendo la capacidad de la DIRINCRI para enfrentar los desafíos del entorno tecnológico contemporáneo.

3.2. Evaluación de la propuesta: Valoración funcional, estratégica y operativa de la propuesta

El proceso de evaluación permitió determinar la pertinencia y potencial de la solución frente a los desafíos identificados. Esta evaluación integró el testeo conceptual, la valoración técnica y la revisión de criterios asociados a la deseabilidad, la factibilidad y la viabilidad institucional.

Tabla 11

Evaluación de factores críticos y acciones estratégicas para la implementación de una solución integral de seguridad digital en la DIRINCRI-PNP

Elemento crítico	Supuesto o desafío	Acción clave
Brechas estructurales	Fragmentación tecnológica y ausencia de protocolos unificados.	Elaborar la Política Institucional de Ciberseguridad de la DIRINCRI y adoptar el SIEM-PNP como eje operativo.
Recursos humanos	Falta de personal especializado y resistencia al cambio.	Capacitar a los analistas mediante convenios con la SEGDI-PCM y universidades nacionales.
Sistemas administrativos	Procedimientos lentos de adquisición tecnológica.	Incluir el proyecto SIEM-PNP en el Plan Anual de Contrataciones (PAC) 2026.
Ruta técnica	Falta de integración con otras direcciones policiales.	Implementar conectores API con los sistemas SIDPOL, RENIEC y MP.
Ruta estratégica	Escasa articulación con la Política Nacional de Transformación Digital.	Alinear el SIEM-PNP con los objetivos del Plan Mariano Santos 2030 (“Nuestra TIC”).
Supuestos críticos	Apoyo de la Alta Dirección y sostenibilidad presupuestal.	Formalizar el proyecto como programa prioritario de modernización institucional.

Nota. La tabla resume los principales factores estructurales, humanos, administrativos y estratégicos que inciden en la viabilidad de la propuesta de fortalecimiento de la seguridad digital institucional. Asimismo, identifica los desafíos y las acciones clave requeridas para la implementación progresiva de la solución tecnológica en el marco de la modernización policial. Elaboración propia.

3.2.1. Testeo de efectividad del concepto de solución

El análisis integrado de entrevistas y encuesta permite reconocer necesidades percibidas de protección de información, seguimiento de accesos, capacitación y coordinación institucional. Las respuestas presentan diferencias entre participantes, especialmente respecto de la claridad de los procedimientos y la suficiencia de la capacitación. Los testimonios aportan elementos para interpretar posibles riesgos operativos y probatorios, mientras que la encuesta describe las valoraciones de los 83 efectivos participantes. Esta evidencia orienta la pertinencia de evaluar un piloto SIEM, pero no demuestra causalidad, eficacia de una solución implementada ni cambios en la confianza ciudadana. La efectividad del concepto deberá comprobarse durante el piloto mediante indicadores y registros previamente definidos.

Figura 5

Cadena de valor público relacionado con la implementación del SIEM



Nota. La figura representa el proceso estructurado de la cadena de valor público en la implementación del SIEM, y la gestión de evidencia digital, desde la infraestructura y el personal capacitado (insumos), pasando por actividades operativas como monitoreo, detección y auditoría (procesos), hasta la generación de productos como alertas y reportes, que contribuyen a resultados institucionales como investigaciones confiables y mayor confianza ciudadana. Elaboración propia.

3.3. Ruta de implementación

3.3.1. Identificación de tareas críticas de implementación

La implementación del sistema SIEM en la DIRINCRI-PNP iniciará con la recopilación de los conocimientos, actitudes y prácticas de expertos en ciberseguridad. Lo que permitirá construir un diagnóstico realista sobre las capacidades institucionales. Este insumo será clave para mapear activos digitales, redes y flujos de datos sensibles, asegurando que la solución responda a necesidades concretas. Según Menon (2024),

omitir esta fase crítica puede generar desviaciones presupuestales y vulnerabilidades operativas, afectando la eficacia del proyecto desde su origen.

Durante el desarrollo, se diseñarán procesos de integración entre sistemas institucionales y operativos, normalizando datos y definiendo alertas para la toma de decisiones. Se establecerá un plan de capacitación para personal técnico y administrativo, fortaleciendo la gobernanza colaborativa. *Boston Consulting Group* (2024) advierte que la ausencia de un plan maestro con hitos claros y estructura de gobernanza sólida es una causa recurrente de sobrecostos y fallas en proyectos tecnológicos del sector público.

La sostenibilidad dependerá de un mecanismo de contratación eficiente, con criterios técnicos y de gestión que orienten la selección de proveedores y el cumplimiento de hitos. Se definirán *KPIs* como interoperabilidad y estabilidad del servicio para medir el impacto. Además, se realizarán pruebas piloto y auditorías técnicas, siguiendo un enfoque iterativo que garantice mejoras continuas. Yan y Lyu (2023) destacan que los proyectos exitosos vinculan gobernanza adaptativa, control de calidad y gestión del conocimiento en todas sus fases.

3.3.2. Alternativas y costos

Tabla 12

Matrices de Alternativas, costos y evaluación de sostenibilidad

Matriz de Alternativas

Alternativa	Descripción	Ventajas	Desventajas
1. Continuidad sin inversión	No se implementan mecanismos adicionales.	Costo cero.	No resuelve la brecha; aumenta riesgos operativos y jurídicos.
2. Monitoreo básico	Herramientas aisladas sin correlación.	Reduce parcialmente riesgos.	No garantiza trazabilidad; escalabilidad limitada.
3. SIEM institucional (recomendada)	Plataforma integral con SOC.	Monitoreo 24/7; trazabilidad verificable; interoperabilidad; valor público.	Mayor costo inicial; requiere capacitación.

Matriz de Costos

Tipo de gasto	Rubro	Detalle	Costo estimado
CAPEX	Hardware SIEM	Clúster + storage	USD. 40,000 - 100,000
	Software	Licencias SIEM anuales	USD. 30,000 - 80,000
	Infraestructura	Racks, UPS, climatización	USD. 50,000 - 150,000
OPEX	Licencias	Renovación anual	USD. 20,000 – 60,000

	Soporte	Mesa de ayuda + monitoreo anual	USD. 40,000 – 100,000
	Capacitación	Certificaciones (por participante)	USD. 1,000 – 5,000

Matriz de Evaluación de Sostenibilidad

Dimensión	Descripción	Nivel esperado
Técnica	Actualizaciones, soporte, escalabilidad	Alto
Financiera	Disponibilidad PIA/PIM	Medio–alto
Institucional	Gobernanza digital operativa	Alto

La hoja de ruta del Anexo 3 es prospectiva. Los años consignados corresponden al cronograma referencial originalmente propuesto y no acreditan ejecución en 2025 o 2026. Antes de implementar el piloto, la programación deberá actualizarse a partir de su aprobación y de los recursos y capacidades disponibles. Las líneas de base de MTTD, tiempos de atención y trazabilidad no se encuentran acreditadas para 2025; deberán obtenerse registros comparables antes de evaluar mejoras.

La referencia a estándares orienta los controles propuestos y no implica certificación. Toda coordinación externa, integración o revisión técnica dependerá de las competencias, acuerdos y autorizaciones aplicables. Las metas numéricas se mantienen como referencias provisionales de planificación y deben revisarse después de medir la línea de base.

3.3.3. Gestión del cambio y dotación para el piloto

El componente tiene un responsable operativo de DIRINCRI y un enlace técnico de DIRTIC. Antes de iniciar, ambas áreas validarán inventario de competencias, carga de trabajo y horas disponibles. La propuesta de dotación no representa personal ya asignado. El informe histórico de incorporaciones a DIRREHUM no acredita disponibilidad especializada en DIRINCRI.

Para la planificación inicial se propone una dotación de cinco personas con dedicación documentada, sujeta a validación según el volumen de eventos, la carga de alertas y el horario del piloto con dedicación documentada: un administrador técnico en DIRTIC, dos analistas para triage y sustitución dentro del horario del piloto, un responsable operativo de supervisión y un custodio designado. La supervisión puede integrarse a una función existente si se acredita tiempo; la administración técnica y la exportación probatoria se segregan. Se requiere un suplente de custodia formalmente designado. Las funciones de análisis avanzado y soporte externo se incluyen solo si existe capacidad propia o servicio contratado.

El piloto operará inicialmente en horario institucional aprobado, con protocolo de aviso y escalamiento fuera de horario. Cinco personas no sustentan una cobertura 24/7. Para ampliarla se calcularán horas de cobertura divididas entre horas netas disponibles por analista, ajustando descansos, licencias, capacitación y simultaneidad requerida. Recursos humanos y presupuesto deberán validar la dotación antes de ofrecer ese nivel de servicio. La propuesta no presupone la disponibilidad de un SOC

de nivel 4 de madurez. El nivel inicial deberá determinarse mediante una evaluación documentada, identificando el modelo y los criterios utilizados. La ampliación de capacidades se condicionará a los resultados del piloto, la competencia demostrada del personal, la disponibilidad de soporte especializado y la previsión presupuestal de operación

Las actividades de formación, sensibilización y seguimiento se desarrollan en el Plan Estratégico de Gestión del Cambio y Sensibilización Institucional, incorporado como anexo del trabajo. En los meses 1-2 se identifican brechas de competencias y se sensibiliza a jefaturas y usuarios sobre finalidad, privacidad y canales de ayuda. En meses 3-4, el personal técnico recibe formación en ingesta, reglas, accesos, triage y custodia. En meses 7-9 se realizan ejercicios guiados y se recoge retroalimentación; el refuerzo se mantiene trimestralmente tras la aceptación. Las certificaciones se seleccionan por funciones y costo, sin asumir que una credencial sustituye la práctica supervisada.

El presupuesto del componente incluye horas de personal y reemplazos, facilitación, materiales, entornos de práctica, evaluaciones y tasas de certificación cuando correspondan. Su monto se incorpora al costo anual validado. Los indicadores son cobertura de formación = participantes que completan / personal objetivo x 100; competencia demostrada = aprobados en ejercicios / evaluados x 100; adopción = usuarios que aplican el protocolo / usuarios observados x 100. Las metas propuestas son 100 % del personal del piloto formado antes de operar y 80 % de aprobación práctica inicial, con refuerzo y nueva evaluación para quienes no alcancen el criterio.

La jefatura operativa revisará mensualmente barreras, consultas y cumplimiento; documentará acuerdos y protegerá la confidencialidad del personal. El riesgo R3 mantiene nivel 6, rojo, por insuficiente capacitación; R5 mantiene nivel 4, amarillo, por resistencia al cambio. Los niveles son evaluaciones de riesgo del equipo y se revisarán con evidencias de capacitación y adopción.

3.3.4. Costeo y medición inicial de resultados

Antes de solicitar precios se definirá número de fuentes, EPS y GB/día medidos, retención por categoría, almacenamiento activo y de respaldo, usuarios, conectores autorizados, conectividad y horario del servicio. Cada precio debe registrar proveedor o fuente pública, fecha, moneda, impuestos, unidad, vigencia y exclusiones. Se

compararán ofertas con igual alcance y se incorporarán personal, soporte, capacitación, continuidad y salida del proveedor.

El costo total para un horizonte de tres años se estimará como desembolso inicial más gasto operativo del primer año y gastos recurrentes de los años segundo y tercero, evitando duplicar licencias o servicios. Se presentarán escenarios de volumen medido bajo, central y alto; sus porcentajes de crecimiento se justificarán mediante registros del piloto. Los importes del documento anterior se retiran por no contar con trazabilidad de precios incorporada; no se sustituyen por cotizaciones inventadas.

El piloto registrará un periodo inicial de 90 días, ampliable si el número de incidentes es insuficiente. El MTTD se calculará como suma de diferencias entre instante de inicio verificable del incidente e instante de detección, dividida entre incidentes con ambos tiempos válidos. Si se desconoce el inicio, se informará la demora desde el primer evento observable con otra denominación. Se publicarán número de casos válidos, exclusiones, media y mediana.

Para evitar ambigüedad, el indicador de atención se denomina tiempo medio desde detección hasta contención inicial: suma de esas diferencias / incidentes con ambos tiempos. La resolución definitiva se medirá por separado. Los relojes se sincronizarán y cada incidente tendrá identificador, gravedad, fuente, responsable y cierre documentado. Los ejercicios simulados se reportarán separados de incidentes reales.

La trazabilidad completa se medirá como evidencias del alcance auditado con registros de identificación, preservación, transferencia y recepción completos / total de evidencias auditadas x 100. La capacitación y la integración tendrán denominadores definidos en un padrón y un inventario fechados. Las metas de los Anexos 3 y 5 son provisionales, no líneas de base observadas ni garantías de desempeño.

3.3.5. Gobernanza de datos e interoperabilidad del ecosistema SIEM–SOC institucional

Desde la lógica de un proyecto de inversión en sistemas informáticos, la gobernanza de datos del SIEM–SOC en la DIRINCRI no puede reducirse a “guardar logs”; supone diseñar una arquitectura que oriente quién genera datos, quién los custodia, quién los explota y bajo qué reglas se comparten con otras entidades del

sistema de justicia. La investigación permitió señalar que la solución debe alinearse con el marco del Gobierno Digital peruano (D. Leg. 1412, D.S. 029-2021-PCM, D.S. 157-2021-PCM y D.S. 098-2025-PCM) y con la ruta estratégica del PEI-PNP y el MS30, en particular el pilar IV "Nuestra TIC", que exige infraestructura moderna, interoperable y orientada a valor público.

Arquitectura de datos y catálogo institucional de logs

Para la propuesta se plantea una arquitectura que comprenda ingesta de eventos, normalización de formatos, almacenamiento protegido y análisis mediante reglas de correlación. Su diseño deberá especificar un catálogo institucional de registros con fuentes, metadatos mínimos, responsables y plazos de conservación. El alcance, los mecanismos de integración y la capacidad de almacenamiento se determinarán mediante el inventario y las pruebas del piloto.

En términos operativos, el catálogo debe alinearse con modelos internacionales de gestión de eventos de seguridad, donde el SIEM actúa como "sistema nervioso" institucional al centralizar información heterogénea y aplicar reglas de correlación. Esto fortalece la respuesta a incidentes y las auditorías internas y externas, garantizando trazabilidad y confiabilidad (López Velásquez et al., 2023). En el caso de la DIRINCRI, se complementa con indicadores como MTTD, MTTR y porcentaje de evidencias con trazabilidad completa, que permiten conectar la arquitectura de datos con resultados observables en la gestión de riesgos y en la cadena de custodia digital, consolidando así la seguridad y eficiencia operativa.

Roles, controles de acceso y cifrado

La gobernanza de datos del SIEM requiere un modelo de roles claramente definido, donde los propietarios de datos (DIRINCRI, DIRTIC-PNP y entidades asociadas) aseguren la gestión de registros internos y compartidos; los custodios operativos mantengan el catálogo de logs y la calidad de la información; y los usuarios autorizados (analistas, jefes operativos, órganos de control) actúen bajo perfiles diferenciados. Este esquema debe sustentarse en un control de accesos basado en roles (RBAC), aplicando principios de mínimo privilegio y segregación de funciones, junto con autenticación robusta y registro exhaustivo de

operaciones. Sin estas responsabilidades claras y trazabilidad, la calidad e integridad de los datos se vuelve meramente declarativa (Hollywood et al., 2024).

En materia de seguridad criptográfica, el modelo plantea cifrado en tránsito mediante TLS y en reposo con AES-256, además de funciones de hash y sellos de tiempo para garantizar integridad y no repudio en los logs incorporados a expedientes fiscales o judiciales. Las directrices de NIST y ISO/IEC 27037 destacan que preservar evidencia digital exige controles técnicos y registros detallados de cada transferencia o análisis (Guttman et al., 2022). En la DIRINCRI, cada exportación hacia laboratorios forenses o al Ministerio Público debe acompañarse de actas digitales, huellas criptográficas y registros automáticos en la cadena de custodia, asegurando validez probatoria y legitimidad institucional.

Interoperabilidad y conectores/API con SIDPOL, RENIEC y Ministerio Público

La integración propuesta con SIDPOL deberá evaluarse según sus posibilidades técnicas, competencias y autorizaciones aplicables. Si se habilitan registros de auditoría pertinentes, el SIEM podría apoyar el seguimiento de accesos y modificaciones y la identificación de patrones de uso inusual. Esta funcionalidad constituye una posibilidad de diseño; no se presenta como integración ejecutada ni como reducción de filtraciones ya comprobada.

Para RENIEC, la integración se articula mediante la Plataforma de Autenticación ID Perú, registrando cada invocación de servicios de verificación de identidad y certificados digitales en el catálogo de logs, vinculándolos al expediente de investigación correspondiente (Registro Nacional de Identificación y Estado Civil, s. f.). Respecto al Ministerio Público, los conectores deben permitir inicialmente el intercambio seguro de evidencia digital y reportes dentro de canales cifrados, evolucionando hacia esquemas de interoperabilidad semántica con ontologías comunes. La literatura sobre sistemas semánticos interoperables en administraciones públicas destaca que este modelo facilita la minería de información y la coordinación interinstitucional (Spyropoulos y Tsiantos, 2025).

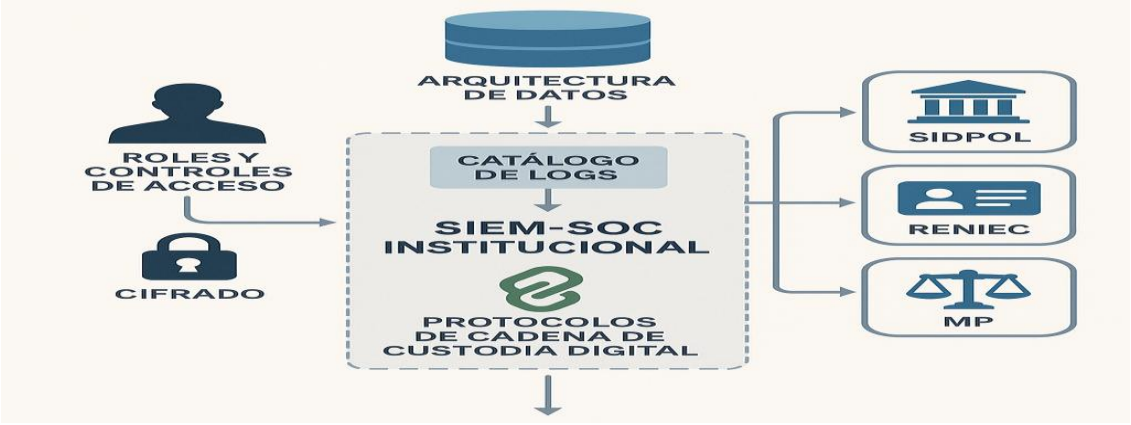
Cadena de custodia digital y valor probatorio

La gobernanza de datos en el SIEM-SOC resulta crítica para sostener la cadena de custodia digital, ya que la ausencia de monitoreo y trazabilidad expone a la DIRINCRI a riesgos de integridad y cuestionamientos procesales. Por ello, la arquitectura debe alinearse con lineamientos de preservación de evidencia y normativa de gobierno digital, registrando automáticamente cada acción relevante como captura, traslado, análisis y entrega al fiscal. La investigación internacional muestra que los modelos más avanzados combinan registros detallados, sellos de tiempo, firmas electrónicas y, en algunos casos, *blockchain* para reforzar la inmutabilidad de los datos (Nath et al., 2024).

Aunque la propuesta inicial no requiere *blockchain*, sí incorpora principios como el uso sistemático de hashes, trazas firmadas digitalmente y repositorios con controles estrictos de acceso. De este modo, la información generada por el SIEM se convierte en insumo robusto para peritajes y audiencias judiciales. Además, la cadena de custodia digital se articula con la cadena de valor público del proyecto: insumos tecnológicos y personal capacitado, procesos de monitoreo y auditoría, productos como reportes y expedientes trazables, y resultados como investigaciones confiables y mayor transparencia. La relación entre estos productos y las mejoras del servicio deberá evaluarse durante la implementación mediante indicadores previamente definidos; no se presenta como un resultado ya demostrado por el estudio.

Figura 6

Arquitectura institucional de seguridad digital y gestión de evidencias



Nota: Diagrama funcional del sistema SIEM-SOC aplicado a entidades estatales. Integra cifrado, control de acceso y protocolos de custodia digital. Elaboración propia.

Capítulo 4: Conclusiones y recomendaciones

4.1. Conclusiones

El estudio identificó percepciones de limitaciones relacionadas con la protección de los equipos informáticos, la claridad de los procedimientos, la capacitación y los recursos para la seguridad digital en las unidades comprendidas en la investigación. Las respuestas de los 83 efectivos encuestados muestran valoraciones heterogéneas, particularmente respecto de las reglas y la capacitación, por lo que no permiten afirmar un consenso absoluto sobre estas carencias. Los hallazgos orientan la revisión de las condiciones institucionales de protección de la información, pero no constituyen una evaluación técnica exhaustiva ni permiten generalizar los resultados a toda la DIRINCRI o a la Policía Nacional del Perú.

El análisis realizado permite identificar riesgos potenciales para los procesos de investigación criminal asociados a las limitaciones del monitoreo y la trazabilidad digital. Las dificultades para registrar accesos y modificaciones, verificar la integridad de los archivos y reconstruir el uso de la información pueden dificultar la documentación de su manejo y conservación. Estos hallazgos sustentan la necesidad de evaluar y fortalecer los controles correspondientes, sin acreditar que se hayan producido alteraciones de evidencia, afectaciones concretas de la cadena de custodia o pérdida de valor probatorio en casos determinados.

Las percepciones recogidas respaldan considerar una estrategia de fortalecimiento de la seguridad digital que articule herramientas tecnológicas, capacitación y responsabilidades institucionales definidas. La valoración favorable de recibir

capacitación básica debe distinguirse de la percepción de que la capacitación existente es insuficiente, pues ambas afirmaciones evalúan aspectos diferentes. El estudio orienta la identificación de brechas de competencias y la evaluación de capacidades especializadas; la eventual creación de una unidad o la asignación de estas funciones a órganos existentes requiere verificar competencias, disponibilidad de personal, recursos y organización institucional. Las mejoras previstas deberán comprobarse durante la implementación y evaluación del piloto.

La alternativa A2 obtiene 4,20 puntos frente a 2,95 de A1 y 3,20 de A3 bajo la ponderación original corregida. El análisis de sensibilidad muestra que la preferencia cambia si el peso financiero supera aproximadamente 0,4785. La alternativa propuesta constituye una opción de implementación gradual cuya viabilidad financiera permanece condicionada. Los costos referenciales permiten una comparación preliminar, pero no acreditan asequibilidad ni financiamiento disponible. Su ejecución requiere validar los importes, acreditar recursos para implementación, operación y mantenimiento, y verificar la dotación y capacidad técnica. Las mejoras en detección y trazabilidad constituyen resultados esperados que deberán comprobarse mediante el piloto.

4.2. Recomendaciones

Se recomienda fortalecer la gobernanza institucional de la ciberseguridad en la DIRINCRI, mediante la creación de un Consejo de Ciberseguridad encargado de conducir estratégicamente la gestión de riesgos digitales e incorporar esta materia como prioridad en la planificación institucional y en la programación multianual de inversiones. Asimismo, resulta necesario actualizar y estandarizar la normativa interna sobre seguridad digital, acompañándola de un diagnóstico técnico que identifique vulnerabilidades en equipos, redes y servicios. Como complemento, debe elaborarse una Guía de Buenas Prácticas para usuarios, orientada a reducir errores humanos y promover hábitos seguros en el manejo de la información institucional.

Para reducir las implicancias operativas y jurídicas derivadas de la falta de monitoreo digital, se recomienda implementar mecanismos de auditoría y registro automático de actividades en sistemas críticos, que permitan fortalecer la trazabilidad de la información y la cadena de custodia de la evidencia digital. Esta medida debe complementarse con programas de capacitación en evidencia digital y procedimientos

forenses, de modo que el personal policial comprenda la relevancia jurídica de la gestión de información digital y adopte prácticas alineadas a estándares.

Con el propósito de fortalecer la ciberseguridad institucional, conforme a las buenas prácticas internacionales, se recomienda implementar de manera progresiva un sistema institucional de monitoreo y gestión de eventos de ciberseguridad (SIEM), iniciando con una fase piloto que permita validar su funcionamiento, capacidad operativa y reglas de correlación de eventos. Este proceso debe complementarse con la creación o fortalecimiento de una unidad especializada en seguridad digital, así como con programas permanentes de capacitación técnica para el personal responsable.

Se recomienda incorporar la implementación del SIEM institucional como un componente estratégico dentro de la planificación de la DIRINCRI, asegurando su articulación con los sistemas de información utilizados en la investigación criminal y con las entidades del sistema de justicia. Para garantizar su sostenibilidad, el proyecto debe contar con financiamiento multianual, mecanismos de supervisión técnica y procesos de actualización tecnológica, de modo que la institución fortalezca la protección de la evidencia digital y mejore su capacidad de respuesta frente a los riesgos del entorno digital.

Bibliografía

Aguilar Antonio, J. M. (2020). La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas. *Revista de Estudios en Seguridad Internacional, 6*(2), 17-43. https://doi.org/10.18847/1.12.2

Aguilar Antonio, J. M. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. *Estudios Internacionales, 53*(198), 169–197. https://doi.org/10.5354/0719-3769.2021.57067

Ávila Niño, F. Y. (2023). Ransomware, una amenaza latente en Latinoamérica. *InterSedes, 24*(49), 92–119. https://www.scielo.sa.cr/pdf/is/v24n49/2215-2458-is-24-49-092.pdf

Bernardo, B. M. V., São Mamede, H., Barroso, J. M. P., & dos Santos, V. M. P. D. (2024). Data governance & quality management—Innovation and breakthroughs across different fields. *Journal of Innovation & Knowledge, 9*(4), Artículo 100598. https://doi.org/10.1016/j.jik.2024.100598

Bozzini, M., Prifti, K., Galeazzi, A., & Manenti, F. (2023). Capex Opex robust optimization: A software for well-founded economic estimations and process optimization. *Chemical Engineering Transactions, 99*, 619–624. https://doi.org/10.3303/CET2399104

Brezavšček, A., & Baggia, A. (2025). Recent trends in information and cyber security maturity assessment: A systematic literature review. *Systems, 13*(1), Artículo 52. https://doi.org/10.3390/systems13010052

Cabrera Vargas, J., Lujano Suaña, Y., & Vargas Salazar, I. Y. (2023). Determinantes de la eficiencia del gasto de capital: Caso gobiernos locales de principales ciudades en Perú, 2021. *Transdisciplinary Human Education, 6*(11), 1-15. https://doi.org/10.55364/the.Vol6.Iss11.154

Carvalho, M., Sá, F., & Bernardino, J. (2025). Evaluation of the impact of AES encryption on query read performance across Oracle, MySQL, and SQL Server databases. *Cryptography, 9*(4), Artículo 77. https://doi.org/10.3390/cryptography9040077

Chourasiya, L., Khatri, S., Lilhore, U. K., Simaiya, S., Alroobaea, R., Baqasah, A. M., Alsafyani, M., & Khan, M. (2025). Advanced system log analyzer for anomaly detection and cyber forensic investigations using LSTM and transformer networks. *Journal of Cloud Computing, 14*(1), Artículo 60. https://doi.org/10.1186/s13677-025-00789-y

Chuquín, R. (2025, 7 de septiembre). Eduardo Pérez Rocha, exdirector de la Policía Nacional del Perú: “Una filtración es más grave que un hackeo”. *Correo*.

https://diariocorreo.pe/edicion/lima/eduardo-perez-rocha-exdirector-de-la-policia-nacional-del-peru-una-filtracion-es-mas-grave-que-un-hackeo-noticia/

Decreto Legislativo N.º 1412. (2018, 13 de septiembre). Decreto Legislativo que aprueba la Ley de Gobierno Digital. *Diario Oficial El Peruano*. https://cdn.www.gob.pe/uploads/document/file/353216/decreto-legislativo-que-aprueba-la-ley-de-gobierno-digital-decreto-legislativo-n-1412-1691026-1.pdf

Decreto Supremo N.º 009-2025-EF. (2025, 22 de enero). Decreto Supremo que aprueba el Reglamento de la Ley N.º 32069, Ley General de Contrataciones Públicas. *Diario Oficial El Peruano*. https://www.gob.pe/institucion/mef/normas-legales/6401561-009-2025-ef

Decreto Supremo N.º 016-2024-JUS. (2024, 30 de noviembre). Decreto Supremo que aprueba el Reglamento de la Ley N.º 29733, Ley de Protección de Datos Personales. *Diario Oficial El Peruano*. https://epdoc2.elperuano.pe/EpPo/VistaNLSE.asp?Referencias=MjM0OTY1My0xMjAyNDExMzA%3D

Decreto Supremo N.º 029-2021-PCM. (2021, 19 de febrero). Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N.º 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo. *Diario Oficial El Peruano*. https://cdn.www.gob.pe/uploads/document/file/1680865/DS%20029-2021-PCM.pdf.pdf

Decreto Supremo N.º 085-2023-PCM. (2023, 28 de julio). Decreto Supremo que aprueba la Política Nacional de Transformación Digital al 2030. *Diario Oficial El Peruano*. https://www.gob.pe/institucion/pcm/normas-legales/4471543-085-2023-pcm

Decreto Supremo N.º 098-2025-PCM. (2025, 1 de agosto). Decreto Supremo que modifica el Reglamento del Decreto Legislativo N.º 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, aprobado por Decreto Supremo N.º 029-2021-PCM. *Diario Oficial El Peruano*. https://busquedas.elperuano.pe/dispositivo/NL/2423580-2

European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Forero-Corba, W., & Negre Bennasar, F. (2024). Técnicas y aplicaciones del Machine Learning e Inteligencia Artificial en educación: una revisión sistemática. *RIED-Revista Iberoamericana de Educación a Distancia, 27*(1), 209-253. https://doi.org/10.5944/ried.27.1.37491

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors, 21*(14), Artículo 4759. https://doi.org/10.3390/s21144759

Grebe, M., Lyon, V., Harnisch, M., Chatterjee, A., Kok, S. A., & Brock, J. (2024, 13 de noviembre). *Most large-scale tech programs fail—Here's how to succeed*. Boston Consulting Group. https://www.bcg.com/publications/2024/most-large-scale-tech-programs-fail-how-to-succeed

Guttman, B., White, D. R., & Walraven, T. (2022). *Digital evidence preservation: Considerations for evidence handlers* (NIST IR 8387). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8387

Hollywood, J. S., Woods, D., Peterson, S., Vermeer, M. J. D., & Jackson, B. A. (2024). *Using data governance and data management in law enforcement: Building a research*

agenda that includes strategy, implementation, and needs for innovation (RR-A108-22). RAND Corporation. https://doi.org/10.7249/RRA108-22

Ley N.º 30096. (2013, 22 de octubre). Ley de Delitos Informáticos. *Diario Oficial El Peruano*. https://busquedas.elperuano.pe/dispositivo/NL/1003117-1

Ley N.º 32069. (2024, 24 de junio). Ley General de Contrataciones Públicas. *Diario Oficial El Peruano*. https://www.gob.pe/institucion/csjpuentepiedra-ventanilla/normas-legales/7901277-32069-0

Lincoln, Y., & Guba, E. (1985). *Naturalistic inquiry*. SAGE Publications

López Velásquez, J. M., Martínez Monterrubio, S. M., Sánchez Crespo, L. E., & Garcia Rosado, D. (2023). Systematic review of SIEM technology: SIEM-SC birth. *International Journal of Information Security, 22*(3), 691-711. https://doi.org/10.1007/s10207-022-00657-9

Machín, N., & Gazapo, M. (2016). La ciberseguridad como factor crítico en la seguridad de la Unión Europea. *Revista UNISCI*, (42), 47–68. https://www.redalyc.org/pdf/767/76747805002.pdf

Malaver Sagastegui, L. S. (2024). *Impacto del gobierno digital en la seguridad ciudadana en la ciudad de Trujillo-2024* [Tesis de maestría, Universidad César Vallejo]. Repositorio Institucional de la Universidad César Vallejo. https://hdl.handle.net/20.500.12692/153769

Menon, S. (2024). Best practices and implementation challenges in effective project management. *International Business Research, 17*(2), 66–74. https://doi.org/10.5539/ibr.v17n2p66

Nath, S., Summers, K., Baek, J., & Ahn, G.-J. (2024). Digital evidence chain of custody: Navigating new realities of digital forensics. En *2024 IEEE 6th International*

Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA) (pp. 11–20). IEEE. https://doi.org/10.1109/TPS-ISA62245.2024.00012

Neville, A. (2021, junio). *Los ciberataques recientes y la estrategia de ciberseguridad de la UE para la década digital* (PE 690.639). Servicio de Estudios del Parlamento Europeo. https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/690639/EPRS_ATA(2021)690639_ES.pdf

Redacción Diario Correo. (2025, 17 de septiembre). Policía Nacional esconde su base de datos por cinco años. *Correo*. https://diariocorreo.pe/politica/policia-nacional-esconde-su-base-de-datos-por-cinco-anos-noticia/

Registro Nacional de Identificación y Estado Civil. (s. f.). *ID Perú: Plataforma de Autenticación Nacional*. https://identidad.reniec.gob.pe/id-peru

Retamozo, C. (2025, 4 de agosto). Ciberataque expone a miles en Perú: "Gatito FBI" roba datos y denuncias a la PNP para venderlos en la dark web. *La República*. https://larepublica.pe/sociedad/2025/08/04/ciberataque-expone-a-miles-en-peru-gatito-fbi-roba-datos-y-denuncias-a-la-pnp-para-venderlos-en-la-dark-web-lrtmae-112748

Rojas Berríos, M. (2025, 20 de abril). Menos del 30% de los peruanos confía en la Policía Nacional del Perú: "Llamamos al 105 y nunca responden". *Infobae*. https://www.infobae.com/peru/2025/04/20/pnp-menos-del-30-de-los-peruanos-confia-en-la-policia-nacional-del-peru-llamamos-al-105-y-nunca-responden/

Snider, K. L. G., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity, 7*(1), Artículo tyab019. https://doi.org/10.1093/cybsec/tyab019

Spyropoulos, A. Z., & Tsiantos, V. (2025). Interoperable semantic systems in public administration: AI-driven data mining from law-enforcement reports. *Computers, 14*(9), Artículo 376. https://doi.org/10.3390/computers14090376

Truong, N., Sun, K., Wang, S., Guitton, F., & Guo, Y. (2021). Privacy preservation in federated learning: An insightful survey from the GDPR perspective. *Computers & Security, 110*, Artículo 102402. https://doi.org/10.1016/j.cose.2021.102402

Vaca, P. A., & Dulce-Villarreal, E. R. (2024). Blockchain para asegurar la integridad y trazabilidad en la cadena de custodia de evidencia digital en informática forense: un estudio de mapeo sistemático. *TecnoLógicas, 27*(60), Artículo e3049. https://doi.org/10.22430/22565337.3049

Villafani, F. (2025, 10 de abril). *Ciberataques en la UE: 10.000 en el último año, el 19% contra la Administración*. Universidad de Navarra. https://www.unav.edu/web/global-affairs/ciberataques-en-la-ue-10.000-en-el-ultimo-ano-el-19-contra-la-administracion

Yan, Y.-C., & Lyu, S.-J. (2023). Can e-government reduce local governments' financial deficits?——Analysis based on county-level data from China. *Government Information Quarterly, 40*(3), Artículo 101812. https://doi.org/10.1016/j.giq.2023.101812

Anexos

Anexo 1: Matriz de Consistencia

Título de la investigación: Ausencia de mecanismos y sistemas de seguridad digital en los equipos informáticos de la Dirección de Investigación Criminal (DIRINCRI) de la PNP, 2024 - 2025

PROBLEMAS	OBJETIVOS	CATEGORIA	SUBCATEGORIAS	METODO
Problema general ¿De qué manera la ausencia de mecanismos y sistemas de seguridad digital en los equipos informáticos de la Dirección de Investigación Criminal (DIRINCRI) de la Policía Nacional del Perú durante los años 2024–2025 incide en la protección de la evidencia digital y en la eficiencia de la investigación criminal? **Problemas específicos** • ¿Qué factores institucionales, normativos y tecnológicos explican la falta de implementación de mecanismos y sistemas de seguridad digital en la DIRINCRI de la PNP? • ¿Cómo afecta la carencia de sistemas de monitoreo, detección y trazabilidad digital a la gestión de evidencia criminal y a la confianza ciudadana en la labor policial? • ¿Qué estrategias institucionales y alternativas tecnológicas podrían fortalecer la ciberseguridad y la gobernanza digital en la DIRINCRI, conforme a las buenas prácticas internacionales y la normativa peruana vigente?	**Objetivo general** Comprender cómo la ausencia de mecanismos y sistemas de seguridad digital en los equipos informáticos de la Dirección de Investigación Criminal (DIRINCRI) de la Policía Nacional del Perú durante los años 2024–2025 incide en la protección de la evidencia digital y en la eficiencia de la investigación criminal. **Objetivos específicos** • Explorar los factores institucionales, normativos y tecnológicos que han condicionado la falta de implementación de mecanismos y sistemas de seguridad digital en la DIRINCRI de la PNP. • Interpretar las implicancias operativas, jurídicas y sociales derivadas de la carencia de sistemas de monitoreo, detección y trazabilidad digital en los procesos de investigación criminal. • Identificar estrategias institucionales y alternativas tecnológicas orientadas al fortalecimiento de la ciberseguridad y la gobernanza digital en la DIRINCRI, conforme a las buenas prácticas internacionales y la normativa peruana vigente.	**Ciberseguridad institucional**	**Gestión institucional y normativa de la seguridad digital.** **Implicancias operativas y jurídicas de la carencia de ciberseguridad.** **Estrategias y herramientas para el fortalecimiento de la gobernanza digital**.	**Tipo de investigación** Aplicada **Enfoque de investigación** Mixto **Diseño de investigación** Exploratorio secuencial **Método de investigación** Deductivo-inductivo **Participantes** (10) Expertos en Ciberseguridad e informática policiales. (02) Expertos en Ciberseguridad e informática policiales civiles. **Técnicas** Entrevista Encuesta (usuario terminal) **Instrumentos** Guía de entrevista Cuestionario Likert

Anexo 2: Bosquejo de proyecto de inversión pública

Implementación del Sistema Integrado de Monitoreo y Gestión de Eventos de Seguridad Digital (SIEM) para la DIRINCRI-PNP

1. Nombre del Proyecto

"Mejoramiento del servicio de investigación criminal mediante la implementación de un Sistema Institucional de Gestión y Monitoreo de Seguridad Digital (SIEM) en la DIRINCRI–PNP"

2. Planteamiento del problema

La Dirección de Investigación Criminal carece actualmente de mecanismos tecnológicos para monitorear accesos, registrar trazabilidad digital y detectar incidentes en tiempo real, lo que genera vulnerabilidad en la integridad de la evidencia digital y afecta la eficiencia de las investigaciones. El documento institucional evidencia que estas brechas obedecen a factores normativos, presupuestales y operativos que han impedido la adopción de soluciones modernas de seguridad digital, exponiendo a la institución a pérdidas de información, filtraciones y cuestionamientos probatorios.

Esta situación configura un problema público: la ineficacia del servicio de investigación criminal debido a la ausencia de un sistema integral de monitoreo y correlación de eventos digitales.

3. Objetivo del Proyecto

Objetivo General del PIP

Mejorar la capacidad institucional de la DIRINCRI para proteger la evidencia digital y fortalecer la eficiencia de la investigación criminal mediante la implementación de una plataforma SIEM con monitoreo continuo, trazabilidad verificable e interoperabilidad con entidades del sistema de justicia.

4. Población Objetivo y Población Beneficiaria

- ***Población objetivo***: Unidades investigativas de la DIRINCRI que manejan evidencia digital (Secuestros, Extorsiones, Robos, Alta Complejidad, etc.).

- ***Población beneficiaria***: La ciudadanía, el sistema de justicia penal, operadores policiales y fiscales, debido al incremento de la confiabilidad probatoria y a la reducción de impunidad.

5. Alineamiento Estratégico

Conforme a los Lineamientos para la Eficacia del MEF, el proyecto se articula con:

- El PEI–PNP, que prioriza fortalecer la investigación criminal y modernizar capacidades tecnológicas.
- El MS30 – Pilar IV "Nuestra TIC", que exige plataformas digitales resilientes, interoperables y seguras.
- La Política Nacional de Transformación Digital, que obliga a garantizar la integridad y trazabilidad de los datos públicos.
- El documento institucional identifica esta brecha como crítica para la protección de la evidencia digital y la transparencia investigativa.

6. Alternativas de Solución

Basado en el análisis institucional y normativo, se identifican tres alternativas:

Alternativa 1: Continuidad sin inversión

- No se propone implementar mecanismos adicionales.
- Mantiene la vulnerabilidad actual y profundiza el problema.

Alternativa 2: Implementación parcial de herramientas de monitoreo básico

- Soluciones aisladas sin correlación ni centralización.
- Reduce levemente la brecha, pero no garantiza trazabilidad probatoria.

Alternativa 3: Implementación integral de un SIEM institucional con SOC interno (Alternativa de Inversión)

- Plataforma SIEM con almacenamiento centralizado, reglas de correlación y monitoreo 24/7.
- SOC institucional, interoperabilidad con SIDPOL, RENIEC y Ministerio Público.
- Contempla gobernanza, capacitación y sostenibilidad.

Esta alternativa es la recomendada, pues responde a la naturaleza del servicio público y genera valor público sostenible.

7. Componentes del Proyecto

7.1. Infraestructura

- Acondicionamiento del Centro de Datos para albergar el clúster SIEM y el SOC.
- Instalación eléctrica, UPS, racks, climatización.

7.2. Equipamiento

- Servidores de alto rendimiento (nodos SIEM).
- Storage con retención mínima de 24 meses.
- Sensores de red, colectores, firewalls complementarios.
- Consolas para analistas SOC.

7.3. Desarrollo de capacidades

- Capacitación especializada (Security, CySA, CHFI, ISO 27001).
- Talleres de manejo de incidentes y cadena de custodia digital.
- Sensibilización institucional en buenas prácticas digitales.

7.4. Capacidad institucional

- Implementación del Consejo de Ciberseguridad de la DIRINCRI.
- Desarrollo de la Guía Institucional de Buenas Prácticas Informáticas.
- Adquisición de software especializado SIEM.
- Diseño del catálogo institucional de logs y arquitectura de datos.

7.5. Estudios

- Estudio de preinversión.
- Análisis de brechas de ciberseguridad.
- Estudios de impacto en procesos investigativos.

8. Costos Estimados y Naturaleza del Gasto

CAPEX (Inversión)

- Hardware SIEM, storage, sensores: alto componente de inversión inicial.
- Infraestructura de soporte y adecuación de centros de datos.

OPEX (Operación y Mantenimiento)

- Renovación de licencias.
- Soporte especializado 24/7.
- Capacitación continua.
- Actualización de reglas de correlación e inteligencia de amenazas.

Los lineamientos del MEF enfatizan que la sostenibilidad depende del financiamiento de operación y mantenimiento a lo largo de la vida útil del proyecto.

9. Análisis de Sostenibilidad

La sostenibilidad se sustenta en tres dimensiones:

- Técnica: soporte continuo, personal especializado, escalabilidad del SIEM.
- Institucional: creación del Consejo de Ciberseguridad; integración con PEI/POI; políticas internas.
- Financiera: asignación en el PIA, PIM y programación multianual de inversiones.

10. Beneficios del Proyecto (Valor Público)

El proyecto genera beneficios operativos, jurídicos y sociales:

- Protección de la evidencia digital y fortalecimiento de la cadena de custodia.
- Reducción de riesgos de filtración, manipulación o pérdida de información.
- Incremento de la eficiencia investigativa y del tiempo de respuesta ante incidentes.
- Mejora de la coordinación con el Ministerio Público y entidades del sistema de justicia.
- Mayor transparencia institucional y recuperación de la confianza ciudadana.

El valor público se enmarca en la lógica MEF de proyectos orientados al cierre de brechas y mejora de servicios esenciales.

11. Indicadores de Desempeño

Producto

- "Plataforma SIEM instalada y operativa."
- "Consejo de Ciberseguridad implementado."

Resultado Inmediato

- Reducción del MTTD (tiempo medio de detección).
- Incremento de evidencias con trazabilidad verificable.

Resultado Final

- Investigaciones más eficientes y confiables.
- Reducción de riesgos de exclusión probatoria.

12. Evaluación de Impacto Esperado

Siguiendo los lineamientos del MEF, el proyecto contribuye al impacto nacional al:

- Fortalecer la investigación criminal.
- Mejorar la competitividad del Estado frente a delitos informáticos.
- Elevar la capacidad institucional para responder a amenazas digitales emergentes.

13. Recomendación Final

La implementación del SIEM debe declararse prioritaria dentro de la cartera de inversiones del sector Interior, al tratarse de un proyecto integral orientado al cierre de una brecha crítica y con repercusión directa en la seguridad ciudadana y la administración de justicia. Su adopción genera un valor público significativo y fortalece la confianza en la Policía Nacional como garante de la investigación criminal y la protección de derechos fundamentales.

Anexo 3: Ruta propuesta para la implementación gradual del SIEM

Etapa	Periodo referencial de la propuesta original	Responsables propuestos, sujetos a validación	Acciones principales	Indicadores e hitos propuestos: situación inicial, metas y condiciones de validación	Seguimiento y verificación
1. Identificación de la necesidad y diagnóstico técnico	2025, trimestres I-II.	DIRINCRI y DIRTIC-PNP.	Delimitar las unidades, activos y fuentes de información comprendidos en la propuesta. Revisar inventarios, controles existentes, competencias y registros de incidentes. Elaborar y validar el diagnóstico técnico y operativo.	**Activos inventariados:** situación inicial pendiente de verificación; meta propuesta de 100 % de los activos del alcance aprobado. **Diagnóstico:** informe documentado y validado. **MTTD:** línea de base no determinada; definir el protocolo de medición y comprobar la disponibilidad de registros. Meta temporal pendiente de validación.	Inventario de activos y fuentes; informe de diagnóstico; registro de brechas; protocolo de medición y acta de validación.
2. Formulación de requerimientos y evaluación de condiciones de implementación	2025, trimestres III-IV.	DIRTIC-PNP, DIRINCRI y áreas competentes de administración y presupuesto.	Elaborar los requerimientos técnicos y operativos. Definir almacenamiento, accesos, custodia, soporte y personal. Obtener información económica documentada y verificar recursos para implementación, operación y mantenimiento. Determinar los requisitos y actuaciones institucionales aplicables.	**Hitos:** requerimientos validados; estimación de costo total sustentada; requisitos aplicables verificados; disponibilidad de recursos acreditada antes de comprometer gasto. Estos hitos no se presentan como actividades ya realizadas.	Documentos técnicos; información económica de respaldo; lista de comprobación de requisitos; informes de personal y presupuesto; constancias de aprobación correspondientes.
3. Contratación de la solución y servicios necesarios	2026, trimestres I-II.	Áreas competentes de contratación, administración y presupuesto, con participación técnica de DIRTIC-PNP y DIRINCRI.	Desarrollar las actuaciones de contratación que correspondan, una vez cumplidas las condiciones técnicas y presupuestales. Incluir obligaciones de implementación, soporte, capacitación, seguridad y aceptación.	**Hitos:** convocatoria, evaluación, adjudicación y formalización contractual, según el procedimiento aplicable. **Condición:** alcance y costo validados, recursos acreditados y responsabilidades definidas.	Expediente de contratación; registros de evaluación; contrato; entregables y mecanismos de seguimiento contractual.
4. Implementación piloto en unidades seleccionadas	2026, trimestre III, a 2027, trimestre I.	DIRINCRI y DIRTIC-PNP, con personal formalmente designado.	Integrar las fuentes aprobadas, configurar reglas y accesos, probar alertas y procedimientos de custodia, y capacitar al personal.	**MTTD y MTTR:** líneas de base no determinadas; metas temporales pendientes de validación. **Trazabilidad:** línea de base pendiente	Pruebas de integración; registros de alertas e incidentes; bitácoras; controles de integridad y

			Operar en el horario autorizado. Registrar incidentes y evaluar el desempeño del piloto.	de evaluación documentada; meta preliminar propuesta de 60 % de las evidencias evaluadas, sujeta a validación. **Formación:** 100 % del personal del piloto formado antes de operar.	custodia; registros de formación; informe de evaluación del piloto.
5. Expansión progresiva y consolidación operativa	2027, trimestre II, a 2028, trimestre IV.	DIRINCRI, DIRTIC-PNP y áreas competentes de personal y presupuesto.	Ampliar a las unidades del alcance aprobado según los resultados del piloto y la disponibilidad de recursos. Consolidar protocolos, formación, soporte y seguimiento. Validar capacidades antes de ampliar horarios o cobertura.	**Unidades integradas:** línea de base pendiente de inventario; meta preliminar de 80 % del alcance aprobado al cuarto trimestre de 2028. **Formación:** 100 % del personal designado formado antes de asumir funciones. **Incidentes tratados conforme al protocolo:** línea de base pendiente de revisión; meta preliminar de 70 %, sujeta a validación.	Inventario de fuentes integradas; pruebas y actas de aceptación; registros de formación; revisión de incidentes; informes de capacidad operativa y disponibilidad presupuestal.
6. Evaluación, sostenibilidad y mejora continua	2029-2030.	DIRINCRI, DIRTIC-PNP y áreas competentes de administración, presupuesto y evaluación.	Revisar el desempeño, actualizar reglas y controles, mantener soporte y evaluar continuidad y recuperación. Ajustar metas con evidencia del piloto y de la operación. Seleccionar un modelo de evaluación de madurez y aplicar su diagnóstico inicial.	**MTTD y MTTR:** metas por definir con las mediciones y resultados del piloto. **Trazabilidad:** meta preliminar de 95 % de las evidencias evaluadas, sujeta a validación. **Madurez:** nivel objetivo pendiente de definición según el modelo seleccionado y la evaluación inicial.	Informes de desempeño; registros de mantenimiento; revisión de trazabilidad; pruebas de recuperación y respaldo; evaluación de madurez; acuerdos de mejora y previsión de recursos.

Nota. Elaboración propia. Los periodos corresponden al cronograma referencial originalmente propuesto y no acreditan ejecución, contratación ni asignación presupuestal. La ruta deberá reprogramarse antes de su implementación, según las aprobaciones, recursos y capacidades disponibles. No se dispone de una línea de base verificable del tiempo medio de detección (MTTD); por ello, su valor inicial y sus metas temporales quedan pendientes de medición y validación. Las demás situaciones iniciales pendientes deberán verificarse mediante registros documentados. Las metas numéricas consignadas son propuestas preliminares sujetas a validación. Cada indicador requerirá definir su alcance, fórmula, fuentes, periodo de medición y responsable; los indicadores temporales deberán precisar sus marcas de inicio y final. Las fuentes de seguimiento previstas deberán comprobarse antes de utilizarlas.

Anexo 4: Matriz de vinculación de la propuesta con instrumentos de gestión pública y la cadena de valor del servicio policial

Instrumento oficial y componente	Brecha oficial relevante	Manifestación en DIRINCRI (evidencia del diagnóstico)	Eslabón de cadena de valor impactado	Indicador de línea base y monitoreo
MS30 (Pilar IV "Nuestra TIC") / Ruta PEI-PNP	Infraestructura TIC moderna, segura e interoperable; monitoreo continuo y trazabilidad de información crítica.	Limitaciones en monitoreo, detección y trazabilidad; necesidad de catálogo institucional de logs y plataforma unificada (SIEM) para correlación y tableros.	Procesos (monitoreo, detección, auditoría) y Productos (alertas, reportes correlacionados, evidencia digital íntegra).	MTTD, MTTR; % evidencias con trazabilidad; disponibilidad del SIEM/SOC.
Política Nacional de Modernización al 2030 (gestión por resultados y centrada en personas)	Servicios y bienes públicos sustentados en evidencia; decisiones orientadas a resultados medibles y experiencia del usuario.	Riesgo operativo y probatorio que afecta la calidad del servicio de investigación criminal y la confianza ciudadana.	Resultados (investigación más eficiente y transparente) e Impacto (confianza ciudadana).	% casos con evidencia digital válida; reducción de incidentes críticos; percepción de confianza (cuando corresponda).
Gobierno Digital (D. Leg. 1412 y Reglamento DS 029-2021-PCM)	Gobernanza digital, interoperabilidad y seguridad digital con indicadores de desempeño; trazabilidad y registros confiables.	Necesidad de interoperabilidad con MP/PJ y registro auditable de eventos; repositorio central de logs y controles de acceso.	Insumos (lineamientos y roles), Procesos (gobernanza/gestión de incidentes) y Productos (protocolos, tableros).	% incidentes tratados conforme a protocolo; % unidades integradas; madurez digital institucional.
PEI MININTER 2025–2030 y POI/POI Multianual (programación y seguimiento)	Objetivos y acciones para fortalecer la gestión institucional, transformación digital y calidad del servicio; seguimiento mediante indicadores.	Hoja de ruta con metas e hitos; exigencia de línea base documentada para MTTD/MTTR y trazabilidad probatoria.	Insumos (financiamiento, personal, infraestructura) y Procesos (implementación y operación SIEM).	% recursos asignados; % personal capacitado; % unidades integradas; MTTD/MTTR.

Nota. La matriz vincula el problema público con brechas reconocibles en instrumentos de gestión y normas de gobierno digital. El objetivo es dejar explícito qué parte del servicio policial se afecta, qué eslabón de la cadena de valor se interviene y qué indicadores permiten medir la línea de base y el cambio durante la implementación del SIEM. Elaboración propia.

Anexo 5

Matriz de indicadores propuestos, líneas de base pendientes, metas y fuentes de verificación

Aspecto por evaluar o fortalecer	Instrumento de gestión pública relacionado	Vinculación estratégica propuesta	Indicador, línea de base, meta y verificación
Disponibilidad de registros para medir los tiempos de detección de incidentes de seguridad digital.	MS30, Pilar IV "Nuestra TIC"; instrumentos de gobierno digital relacionados con seguridad y gobernanza.	Fortalecer el monitoreo y la gestión de la seguridad de la información.	**Indicador:** tiempo medio de detección (MTTD). **Línea de base:** no determinada; pendiente de medición. **Meta:** pendiente de definición y validación. **Verificación prevista:** registros de incidentes con marcas temporales contrastables y bitácoras; registros del SIEM cuando esté disponible.
Registro y medición estandarizada de la respuesta y contención de incidentes.	Instrumentos de gobierno digital y modernización de la gestión pública.	Mejorar la gestión de incidentes y el seguimiento de la respuesta institucional.	**Indicador:** tiempo medio de respuesta (MTTR), previa definición del inicio y final de la medición. **Línea de base:** no determinada. **Meta:** pendiente de validación técnica según el horario, alcance y capacidad del piloto. **Verificación prevista:** tickets de incidentes, bitácoras y registros de las acciones realizadas.
Documentación de la trazabilidad de la evidencia digital y de los controles de integridad y custodia.	MS30, Pilar IV; instrumentos de gobierno digital relacionados con seguridad e interoperabilidad.	Fortalecer los procedimientos de trazabilidad, integridad y custodia digital.	**Indicador:** porcentaje de evidencias evaluadas que cumplen los criterios de trazabilidad definidos. **Línea de base:** no determinada; pendiente de evaluación documentada. **Metas preliminares propuestas:** 60 % en una etapa intermedia y 95 % en la etapa final, sujetas a validación. **Verificación prevista:** registros de custodia, accesos, integridad, sellos de tiempo y auditorías.
Integración de las fuentes de información de las unidades comprendidas en el alcance aprobado.	PEI y POI aplicables; MS30, en lo relacionado con modernización tecnológica.	Articular capacidades tecnológicas y fortalecer la gestión de la información.	**Indicador:** porcentaje de unidades del alcance aprobado que cumplen los criterios de integración definidos. **Línea de base:** pendiente de inventario. **Meta preliminar propuesta:** 80 % al cuarto trimestre de 2028, sujeta a validación del cronograma. **Verificación prevista:** inventario de unidades y

			fuentes, pruebas de ingesta de registros y actas de aceptación.
Formación del personal designado para operar y supervisar el piloto.	Instrumentos de modernización y gestión del talento institucional.	Fortalecer las competencias técnicas y la cultura de seguridad digital.	**Indicador:** porcentaje del personal objetivo del piloto que completa la formación prevista. **Línea de base:** pendiente de verificación de registros de capacitación. **Meta propuesta:** 100 % del personal del piloto formado antes de iniciar operaciones, conforme al apartado 3.3.3. **Verificación prevista:** relación de personal designado, registros de asistencia, constancias de formación y evaluaciones prácticas.

Nota. Elaboración propia. Las vinculaciones estratégicas son propuestas analíticas y deberán contrastarse con los instrumentos institucionales aplicables; no se presentan como transcripciones oficiales de objetivos o acciones estratégicas. El estudio no acredita líneas de base numéricas para los indicadores consignados. Las fuentes de verificación describen los registros que deberán utilizarse, sin afirmar que todos estén actualmente disponibles. Las metas son propuestas de planificación sujetas a validación técnica, operativa y presupuestal. En los indicadores porcentuales deberán definirse el numerador, el denominador, los criterios de cumplimiento y el periodo de medición.

Anexo 6: Matriz de variables de dimensionamiento y estimaciones referenciales de costos del SIEM

Categoría	Variable / Componente	Descripción técnica	Supuesto o estimación referencial pendiente de validación
Variables críticas de costeo	EPS (Eventos por segundo)	Volumen de eventos procesados por segundo; determina capacidad de correlación y licenciamiento.	Modelo enterprise tarifado por bloques de 1,000 EPS.
	Volumen diario en GB	Cantidad de datos ingeridos por día; impacta licencias SaaS y almacenamiento.	Licenciamiento SaaS por GB/día ingerido.
	Periodo de retención (12-36 meses)	Tiempo de conservación de logs en almacenamiento activo o frío.	• Storage empresarial: USD 20-50 por TB/mes; • Nube fría: USD 10-25 por TB/mes.
	Modalidad (SaaS vs On-prem)	Arquitectura de despliegue que impacta CAPEX/OPEX y escalabilidad.	SaaS: OPEX mensual; On-prem: inversión inicial más mantenimiento.
	Modelo SOC (propio, MDR, híbrido)	Esquema operativo de monitoreo y respuesta ante incidentes.	Servicio MDR: USD 8 000–25 000 mensuales como aproximación académica no validada. El costo del modelo híbrido deberá estimarse según alcance, horario y capacidades propias; no se acredita una reducción porcentual.
	Integraciones externas	Conectores y APIs con SIDPOL, RENIEC, MP u otros sistemas.	Costos variables según complejidad técnica.
	Nivel de servicio (SLA 8x5 vs 24x7)	Disponibilidad contractual y tiempos máximos de respuesta.	SLA 24/7 incrementa costos respecto a 8x5.
Estimaciones académicas de costos	Licenciamiento SIEM SaaS	Modelo de cobro por volumen ingerido o por EPS.	• USD 100-300 por GB/día/mes; • USD 1,000–3,000 por 1,000 EPS/mes.
	Capacitación especializada	Formación técnica y certificaciones del equipo SOC.	• Certificaciones: USD 800-2,000 por persona; • Talleres: USD 3,000-10,000 por grupo de participantes.

Nota. Elaboración propia. Los montos son estimaciones preliminares referenciales. El equipo investigador no logró obtener los requisitos necesarios para acceder a información económica que permitiera validarlos mediante cotizaciones o un estudio de mercado. Los importes se utilizan exclusivamente para la comparación académica de alternativas y no acreditan disponibilidad presupuestal ni viabilidad financiera.

Anexo 7: Matriz de Registro de riesgos y plan de respuesta del Proyecto SIEM–DIRINCRI (Enfoque Invierte.pe)

Código	Riesgo identificado	Prob.	Impacto	Nivel	Semáforo	Dueño	Mitigación	Control trimestral	Vinculación PEI
R1	Subestimación del volumen real de eventos	3	3	9	🔴	Unidad TIC / Proyecto	Medición piloto y ajuste en expediente técnico	Revisión trimestral de crecimiento de logs	OEI Transformación Digital
R2	Dependencia tecnológica del proveedor	2	3	6	🔴	Oficina de Abastecimiento	Cláusula de transferencia y documentación obligatoria	Auditoría contractual trimestral	OEI Fortalecimiento institucional
R3	Insuficiente capacitación interna	3	2	6	🔴	DIRINCRI / DIRREHUM / DIREDOC	Plan formal de capacitación certificada	Evaluación trimestral de competencias	OEI Profesionalización
R4	Insuficiencia presupuestal PIM	2	3	6	🔴	Oficina de Presupuesto	Validar el alcance y el costo total mediante información económica documentada; identificar la fuente de financiamiento y acreditar recursos para implementación, operación y mantenimiento. Condicionar la contratación y	Seguimiento PIA-PIM trimestral	OEI Sostenibilidad financiera

							ampliación al cumplimiento de estas condiciones		
R5	Resistencia al cambio organizacional	2	2	4	🟡	Jefatura operativa	Gestión del cambio y sensibilización	Encuesta interna semestral	OEI Modernización del servicio
R6	Falsos positivos elevados	2	2	4	🟡	Equipo SOC	Ajuste progresivo de reglas de correlación	Reporte técnico trimestral	OEI Mejora del servicio investigativo

Nota. La escala utilizada corresponde a una matriz probabilidad–impacto (1=bajo, 2=medio, 3=alto). El nivel de riesgo resulta del producto de ambas variables. Semaforización: verde (1-2), amarillo (3-4) y rojo (6-9). En el presente registro no se visualizan riesgos en categoría verde, lo que evidencia que las brechas identificadas mantienen una exposición institucional relevante que requiere intervención estructural. La vinculación al PEI 2025-2030 permite asegurar coherencia estratégica y seguimiento presupuestal en el marco del PIA/PIM y del enfoque Invierte.pe. Elaboración propia.

Anexo 8: Mapa de Cumplimiento en Protección de Datos, Gobierno Digital y Calidad de Servicio

Proyecto SIEM–DIRINCRI (Enfoque Invierte.pe)

Requisito normativo	Control institucional proyectado	Evidencia verificable	Nivel actual de cumplimiento (diagnóstico)	Riesgo mitigado
D. Leg. 1412 - Gobierno digital	Implementación de SIEM con monitoreo centralizado y trazabilidad integral.	Reportes automatizados y bitácoras consolidadas.	🟡 Parcial (existen controles dispersos, sin sistema centralizado)	Fragmentación y pérdida de información crítica.
D.S. 029-2021-PCM - Interoperabilidad segura	Integración mediante APIs seguras, autenticación fuerte y segregación de accesos.	Registros de integración y logs auditables.	🔴 Bajo (no existe interoperabilidad estructurada con monitoreo unificado)	Accesos no autorizados y fuga de información.
Ley 29733 - Protección de datos personales	Control de acceso basado en roles (RBAC) y principio de minimización.	Matriz de perfiles y registros de acceso.	🟡 Parcial (controles administrativos sin trazabilidad automatizada)	Vulneración de datos sensibles.

Integridad de evidencia digital	Cifrado en tránsito y reposo, sellado de tiempo y registros inmutables.	Certificados digitales y logs firmados.	🔴 Bajo (no se evidencia sistema institucional de sellado de tiempo centralizado)	Impugnación probatoria por alteración.
Norma Técnica de Calidad de Servicios	SLA contractuales y medición de desempeño (MTTD, MTTR, disponibilidad).	Reportes trimestrales de KPIs.	🔴 Bajo (no existen indicadores institucionales formalizados de desempeño digital)	Deficiencia en la prestación del servicio.
Ley 32069 - Gestión por desempeño contractual	Indicadores verificables vinculados a metas institucionales.	Informe de evaluación de desempeño del proveedor.	🟡 Parcial (aún no implementado por tratarse de fase precontractual)	Ineficiencia operativa o incumplimiento contractual.

Nota. El nivel actual de cumplimiento se ha estimado con base en el análisis cualitativo y documental realizado en la investigación. La ausencia de categorías en verde refleja la existencia de brechas estructurales en gobernanza digital, trazabilidad y medición del desempeño, lo que justifica la intervención mediante el Proyecto de Inversión SIEM-DIRINCRI. Los controles señalados deberán acreditarse formalmente durante la fase de ejecución conforme al marco de Gobierno Digital y la Ley 32069. Elaboración propia.

Anexo 9: Matriz de Cadena de valor del proyecto SIEM-DIRINCRI

(Formato compatible con Invierte.pe y con una narrativa clara orientada a valor público)

Eslabón de la cadena	Descripción del aporte al servicio de investigación criminal	Indicadores asociados	Responsables
INSUMOS	Financiamiento; equipamiento SIEM; infraestructura TIC; talento humano; lineamientos normativos; conectividad institucional; soporte de DIRTIC; validación SEGDI.	% de recursos asignados; disponibilidad de infraestructura; personal designado.	DIRINCRI, DIRTIC-PNP, MEF, SEGDI.
PROCESOS	Instalación del SIEM; integración con SIDPOL/RENIEC/MP; diseño de reglas de correlación; monitoreo 24/7; gestión de incidentes; gobernanza digital; capacitación; auditorías.	MTTD; MTTR; % de unidades integradas; % personal capacitado.	DIRINCRI-SOC, DIRTIC-PNP, proveedor SIEM.
PRODUCTOS	SIEM funcional; SOC operativo; catálogo de logs; protocolos de cadena de custodia; dashboards tácticos; alertas tempranas; evidencia digital trazable.	% SIEM implementado; % evidencia trazable; disponibilidad del SOC.	DIRINCRI-SOC; Unidades investigativas.
RESULTADOS	Investigación criminal más eficiente, transparente y soportada en evidencia digital íntegra; reducción de incidentes; decisiones policiales oportunas.	% casos con evidencia digital válida; reducción de incidentes críticos.	DIRINCRI; Ministerio Público.

IMPACTO (VALOR PÚBLICO)	Mayor confianza ciudadana; reducción de impunidad; fortalecimiento del sistema de justicia; modernización institucional.	Variación de percepción ciudadana; tasa de sentencias efectivas; nivel de madurez digital.	PNP; MININTER; Sistema de Justicia.

Nota. La cadena de valor demuestra que el proyecto no solo incorpora tecnología, sino que transforma la forma en que la DIRINCRI investiga, documenta y sostiene casos complejos. Los insumos correctos generan procesos modernos, que producen evidencia digital sólida y resultados investigativos confiables, lo que finalmente construye valor público a través de una justicia más eficiente y una policía más transparente. Elaboración propia.

Anexo 10: Guía de entrevistas

Guía de entrevista

Especialistas en seguridad digital con conocimientos en informática - personal policial

Investigación: Ausencia de mecanismos y sistemas de seguridad digital en los equipos informáticos de la Dirección de Investigación Criminal (DIRINCRI) de la PNP, 2024 - 2025.

Objetivo de la investigación: Comprender cómo la ausencia de mecanismos y sistemas de seguridad digital en los equipos informáticos de la Dirección de Investigación Criminal (DIRINCRI) de la Policía Nacional del Perú durante los años 2024–2025 incide en la protección de la evidencia digital y en la eficiencia de la investigación criminal.

I. DATOS GENERALES

Código de Entrevistado : ……..
Cargo : ……..
Lugar : ……..
Hora : ……..
Fecha : ……..
Entrevistador : ……..

II. INTERROGANTES

OE. 1: Explorar los factores institucionales, normativos y tecnológicos que han condicionado la falta de implementación de mecanismos y sistemas de seguridad digital en la DIRINCRI de la PNP.

1. Desde su experiencia profesional, ¿qué factores considera que han limitado la adopción de mecanismos avanzados de seguridad digital dentro de la DIRINCRI?
2. ¿De qué manera influyen las normas y políticas institucionales vigentes en la capacidad de la PNP para implementar tecnologías de ciberseguridad?
3. ¿Qué barreras técnicas o estructurales identifica actualmente para integrar sistemas de monitoreo y correlación de eventos (como SIEM) en la DIRINCRI?

OE. 2: Interpretar las implicancias operativas, jurídicas y sociales derivadas de la carencia de sistemas de monitoreo, detección y trazabilidad digital en los procesos de investigación criminal.

4. ¿Cómo considera que la falta de sistemas de monitoreo y trazabilidad digital afecta la validez probatoria de la evidencia digital en una investigación policial?
5. ¿Qué impactos operativos o institucionales ha podido observar cuando no existen mecanismos de detección temprana frente a ciberamenazas internas o externas?

6. Desde su perspectiva, ¿cómo percibe la ciudadanía o la comunidad digital la capacidad de respuesta de la PNP ante incidentes cibernéticos?

OE. 3: Identificar estrategias institucionales y alternativas tecnológicas orientadas al fortalecimiento de la ciberseguridad y la gobernanza digital en la DIRINCRI, conforme a las buenas prácticas internacionales y la normativa peruana vigente.

7. ¿Qué estrategias o acciones institucionales considera prioritarias para fortalecer la ciberseguridad en la DIRINCRI?
8. ¿Qué tipo de tecnologías o soluciones digitales considera más adecuadas para elevar los niveles de seguridad y trazabilidad institucional?
9. ¿Qué rol deberían desempeñar la capacitación especializada y la cooperación con organismos externos en la consolidación de una cultura de ciberseguridad dentro de la PNP?

CIERRE:

10. ¿Qué recomendación o reflexión personal podría compartir sobre la importancia de fortalecer la seguridad digital en una institución policial como la DIRINCRI, considerando los desafíos actuales del entorno tecnológico?

Guía de entrevista

Especialistas en seguridad digital con conocimientos en informática - especialistas civiles

Investigación: Ausencia de mecanismos y sistemas de seguridad digital en los equipos informáticos de la Dirección de Investigación Criminal (DIRINCRI) de la PNP, 2024 - 2025.

Objetivo de la investigación: Comprender cómo la ausencia de mecanismos y sistemas de seguridad digital en los equipos informáticos de la Dirección de Investigación Criminal (DIRINCRI) de la Policía Nacional del Perú durante los años 2024-2025 incide en la protección de la evidencia digital y en la eficiencia de la investigación criminal.

III. DATOS GENERALES

Código de Entrevistado : ……..
Cargo : ……..
Lugar : ……..
Hora : ……..
Fecha : ……..
Entrevistador : ……..

IV. INTERROGANTES

OE. 1: Explorar los factores institucionales, normativos y tecnológicos que han condicionado la falta de implementación de mecanismos y sistemas de seguridad digital en la DIRINCRI de la PNP.

11. Desde su perspectiva como especialista en ciberseguridad, ¿cuáles cree que son los principales factores institucionales o de gestión pública que dificultan se incorpore sistemas modernos de seguridad digita?
12. ¿De qué manera las normas o políticas estatales actuales favorecen o limitan la capacidad de las instituciones públicas —como la PNP— para aplicar tecnologías de ciberseguridad?
13. Considerando su experiencia ¿Qué obstáculos técnicos, presupuestales o estructurales podrían impedir que una institución del estado utilice herramientas de monitoreo digital y análisis de incidentes informáticos?

OE. 2: Interpretar las implicancias operativas, jurídicas y sociales derivadas de la carencia de sistemas de monitoreo, detección y trazabilidad digital en los procesos de investigación criminal.

14. Desde su experiencia profesional, ¿de qué manera considera que la ausencia de sistemas de monitoreo y trazabilidad digital puede influir en la confiabilidad o validez de la evidencia empleada en las investigaciones policiales?
15. En su opinión, ¿qué consecuencias operativas o institucionales suelen generarse cuando las entidades públicas no cuentan con mecanismos adecuados para detectar y responder oportunamente ante incidentes o amenazas digitales?
16. Desde una mirada ciudadana o social, ¿cómo cree que la población percibe la capacidad de la PNP para enfrentar los delitos informáticos o responder ante situaciones que comprometen la seguridad digital del Estado?

OE. 3: Identificar estrategias institucionales y alternativas tecnológicas orientadas al fortalecimiento de la ciberseguridad y la gobernanza digital en la DIRINCRI, conforme a las buenas prácticas internacionales y la normativa peruana vigente.

17. Desde su experiencia profesional en seguridad digital, ¿qué estrategias institucionales considera prioritarias para mejorar la ciberseguridad y la protección de la información en entidades públicas como la DIRINCRI?
18. En su opinión, ¿qué herramientas o soluciones tecnológicas serían más adecuadas para fortalecer la trazabilidad, el control y la protección de los datos en los procesos de investigación criminal?
19. ¿Qué importancia atribuye a la capacitación continua y a la cooperación con entidades académicas, tecnológicas o internacionales en la creación de una cultura institucional de ciberseguridad dentro de la PNP?

CIERRE:

20. ¿Finalmente, ¿qué reflexión o recomendación personal podría compartir respecto a la necesidad de fortalecer la seguridad digital en una institución pública como la policial Nacional del Perú y en específico, como la DIRINCRI, considerando los desafíos actuales y futuros del entorno tecnológico?

Anexo 11: Perfil de entrevistados clave del componente cualitativo

Código	Perfil profesional	Experiencia relevante	Rol en el análisis
E1	Especialista en ciberseguridad pública	Implementación de controles ISO/IEC 27001	Análisis normativo
E2	Arquitecto de sistemas	Integración de SIEM en sector público	Evaluación técnica
E3	Consultor en gobierno digital	Gobernanza y transformación digital	Estrategia institucional
E4	Analista SOC	Gestión de incidentes	Detección y respuesta
E5, 6 Y 7	Oficial investigador	Gestión de evidencia digital	Impacto operativo
E8	Suboficial investigador	Manejo de archivos institucionales	Trazabilidad
E9	Jefe de unidad	Supervisión operativa	Impacto institucional
E10	Experto en derecho informático	Validez probatoria digital	Dimensión jurídica
E11	Ingeniero en redes	Infraestructura tecnológica	Factibilidad técnica
E12	Especialista en capacitación TIC	Formación institucional	Cultura organizacional
E12	Ingeniero de Sistemas	Supervisión operativa y gestión de incidentes	Detección y respuesta

Nota. La selección de entrevistados respondió a un muestreo intencional por conveniencia de acuerdo con el criterio experto, priorizando experiencia en ciberseguridad, investigación de delitos informáticos y manejo de plataformas digitales.

Anexo 12:

Matriz de codificación cualitativa

Categoría principal	Subcategoría	Evidencia recurrente
Gobernanza tecnológica	• Ausencia de política clara • Débil articulación interinstitucional	• Falta de lineamientos internos definidos • Limitaciones de coordinación tecnológica estatal
Riesgo operativo y probatorio	• Falta de trazabilidad • Vulnerabilidad ante accesos no autorizados	• Dificultad para acreditar cadena de custodia digital • Ausencia de registros automatizados (logs)
Cultura organizacional	• Capacitación insuficiente • Baja priorización presupuestal	• Formación reactiva y no preventiva • Competencia con otras necesidades operativas
Estrategia tecnológica	• Necesidad de SIEM/SOC • Implementación progresiva	• Consenso técnico transversal • Modelo escalonado considerado viable

Nota. Las categorías emergieron del proceso de codificación abierta y axial realizado con apoyo de ATLAS.ti, permitiendo identificar patrones recurrentes y relaciones conceptuales entre dimensiones analíticas.

Anexo 13: Cuestionario Likert

Cuestionario

Grado jerárquico:

Tiempo de servicio en la PNP: **Tiempo de servicio en la unidad:**

Encuesta sobre "ausencia de mecanismos y sistemas de seguridad digital en los equipos informáticos de la Dirección de Investigación Criminal (DIRINCRI) de la PNP, 2024 - 2025"

El objetivo de la investigación es comprender cómo la ausencia de mecanismos y sistemas de seguridad digital en los equipos informáticos de la Dirección de Investigación Criminal (DIRINCRI) de la Policía Nacional del Perú durante los años 2024-2025 incide en la protección de la evidencia digital y en la eficiencia de la investigación criminal.

Se desea conocer su opinión acerca del tema según las siguientes opciones: 1(Totalmente en desacuerdo), 2(En desacuerdo), 3(Neutro), 4(De acuerdo), 5(Totalmente de acuerdo)

OE 1: Explorar los factores institucionales, normativos y tecnológicos que han condicionado la falta de implementación de mecanismos y sistemas de seguridad digital en la DIRINCRI de la PNP.					
Preguntas	**Totalmente en desacuerdo**	**En desacuerdo**	**Neutro**	**De acuerdo**	**Totalmente de acuerdo**
En la unidad donde trabajo no existen reglas claras o procedimientos para proteger la información digital					
Considero que los equipos de cómputo que utilizamos no cuentan con la seguridad necesaria para evitar el acceso no autorizado					
En la DIRINCRI no se brinda suficiente orientación o capacitación sobre cómo proteger los datos que manejamos					
La falta de recursos o apoyo técnico limita la instalación de programas o sistemas que mejoren la seguridad digital					
OE. 2: Interpretar las implicancias operativas, jurídicas y sociales derivadas de la carencia de sistemas de monitoreo, detección y trazabilidad digital en los procesos de investigación criminal					

La falta de control digital hace difícil saber quién accedió o modificó un archivo de una investigación					
Considero que no existe un seguimiento adecuado sobre el uso de la información digital en las investigaciones					
Cuando no se protege bien la información, se pone en riesgo la validez de la evidencia en el proceso judicial					
La ausencia de medidas de seguridad digital afecta la confianza de los ciudadanos en el trabajo policial					
OE. 3: Identificar estrategias institucionales y alternativas tecnológicas orientadas al fortalecimiento de la ciberseguridad y la gobernanza digital en la DIRINCRI, conforme a las buenas prácticas internacionales y la normativa peruana vigente.					
Sería útil que todo el personal reciba capacitación básica sobre cómo proteger la información en los equipos de cómputo					
La creación de un área especializada que supervise la seguridad digital mejoraría la protección de los datos					
Contar con programas que registren automáticamente las actividades en los equipos ayudaría a mejorar la seguridad					
Creo que la DIRINCRI debería modernizar sus sistemas informáticos para evitar riesgos de pérdida o filtración de información					

Anexo 14

Ficha Técnica de la Encuesta

Nombre del instrumento: Cuestionario sobre ausencia de mecanismos y sistemas de seguridad digital en los equipos informáticos de la Dirección de Investigación Criminal (DIRINCRI) de la PNP, 2024-2025.

Objetivo del instrumento: Recoger información empírica sobre cómo la ausencia de mecanismos y sistemas de seguridad digital incide en la protección de la evidencia digital y en la eficiencia de la investigación criminal.

Dimensiones: OE1: Factores institucionales, normativos y tecnológicos (4 ítems). OE2: Implicancias operativas, jurídicas y sociales (4 ítems). OE3: Estrategias institucionales y alternativas tecnológicas (4 ítems).

Tipo de instrumento: Cuestionario estructurado con escala Likert de cinco puntos.

Escala de medición: 1 = Totalmente en desacuerdo; 2 = En desacuerdo; 3 = Neutro; 4 = De acuerdo; 5 = Totalmente de acuerdo.

Número total de ítems: 12 ítems distribuidos en tres dimensiones.

Población de Interés: Personal policial de las unidades especializadas comprendidas en el estudio: DIVINROB, DIVINHOM, DIVINSE y la unidad correspondiente a DIVINDAT, considerando su cambio de denominación institucional en 2025.

Tamaño de muestra: 83 efectivos policiales participantes.

Tipo de muestreo: No probabilístico por conveniencia.

Procedimiento de selección: Participaron los efectivos policiales que estuvieron disponibles durante los momentos de aplicación de la encuesta. La selección fue no probabilística por conveniencia y no se realizó mediante un procedimiento aleatorio.

Nivel de confianza: No corresponde declarar un nivel de confianza para la generalización poblacional, debido al procedimiento de selección empleado.

Error máximo permitido: No corresponde declarar un margen de error de muestreo probabilístico.

Confiabilidad del instrumento: Alfa de Cronbach global (α) = 0.906, indicando consistencia interna excelente. OE1 α = 0.746; OE2 α = 0.790; OE3 α = 0.933.

Validez de contenido: Juicio de expertos en gestión pública, metodología de investigación y seguridad digital institucional.

Procesamiento estadístico: Análisis descriptivo (media y desviación estándar) y análisis de consistencia interna (α de Cronbach y correlación ítem-total corregida).

Consideraciones éticas: Participación voluntaria, confidencialidad garantizada y uso exclusivo para fines académicos.

Alcance de los resultados: Los resultados describen las percepciones de los 83 efectivos encuestados. No se acredita representatividad estadística respecto del conjunto de efectivos de las unidades estudiadas ni de toda la DIRINCRI.

pro

Anexo 15: Paneaux fotográfico



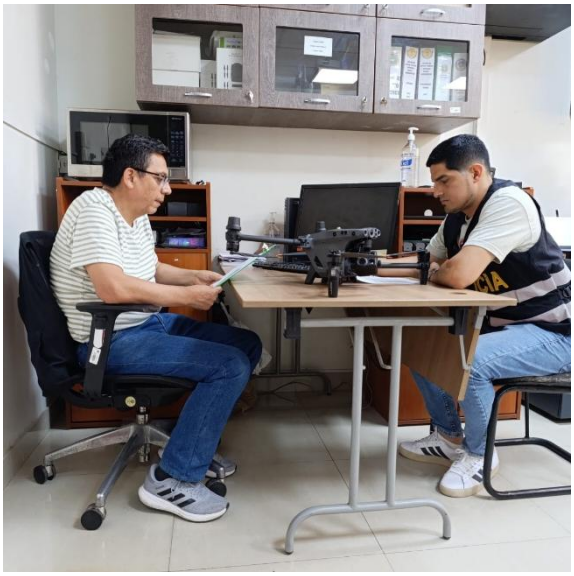
Entrevista May. S. PNP Ronald PEÑA CARRASCO



Entrevista S3 PNP Edinson LIZANA MEDINA



Entrevista SS PNP Percy CLAVIJO CAMPOS



Entrevista S1 PNP Luis VEGA VALENZUELA

Anexo 16: Matriz de actores estratégicos para la implementación del SIEM en la DIRINCRI bajo enfoque de poder/interés

Actor Institucional	Nivel de Poder	Nivel de Interés	Clasificación Estratégica	Tácticas de Integración	Riesgos Asociados	Estrategias de Mitigación
DIRTIC–PNP	Alto	Alto	Aliado estratégico clave	Participación desde fase de formulación (ficha técnica INVIERTE.PE); liderazgo técnico en especificaciones; comité técnico permanente; gobernanza compartida del SOC	Resistencia técnica por sobrecarga operativa; conflictos de competencia funcional	Definir matriz RACI; resolución interna de competencias; presupuesto específico para soporte post-implementación
SEGDI–PCM	Alto	Medio-Alto	Aliado normativo	Validación temprana de arquitectura; alineamiento con Política Nacional de Transformación Digital; interoperabilidad con PIDE	Observaciones por incumplimiento de estándares de seguridad o arquitectura digital	Talleres de pre-validación técnica; adopción de estándares ISO/IEC 27001 y NIST
Ministerio Público (MP)	Alto	Alto	Aliado estratégico funcional	Convenios de interoperabilidad; protocolos de evidencia digital; mesas técnicas conjuntas	Cuestionamiento de cadena de custodia digital; nulidad probatoria	Incorporación de fiscal especializado en diseño de protocolos; auditorías forenses externas
Poder Judicial (PJ)	Alto	Medio	Neutral de alto poder	Socialización de beneficios probatorios; capacitaciones sobre evidencia digital	Resistencia jurisprudencial; desconocimiento técnico	Programas de capacitación judicial; difusión de buenas prácticas internacionales
RENIEC	Medio-Alto	Medio	Neutral colaborativo	Convenio de interoperabilidad de datos; protocolos de seguridad y trazabilidad	Restricciones de acceso por protección de datos personales	Acuerdos de nivel de servicio (SLA); cumplimiento Ley de Protección de Datos
OGA / OPP (Órgano General de Administración / Oficina de Planeamiento y Presupuesto)	Alto	Medio	Actor crítico de viabilidad financiera	Inclusión del proyecto en Programación Multianual de Inversiones; sustento costo-beneficio; análisis CAPEX/OPEX	Observaciones presupuestales; recortes fiscales; retrasos en certificación	Estudio de mercado robusto; evaluación costo-efectividad; estructuración modular del proyecto

Nota. La matriz de poder/interés ha sido elaborada conforme al enfoque de gestión de *stakeholders* aplicado a proyectos tecnológicos bajo el marco de INVIERTE.PE. La clasificación responde al nivel de influencia normativa, presupuestal y operativa de cada actor en la implementación del SIEM en la DIRINCRI. Su finalidad es anticipar riesgos institucionales y definir estrategias de integración y gobernanza digital sostenible. Elaboración propia.

Anexo 17: Propuesta de procedimiento de gobernanza de datos e interoperabilidad

Gobernanza de Datos e Interoperabilidad del Ecosistema SIEM-SOC Institucional - DIRINCRI

I. Objeto

Proponer reglas para la arquitectura de datos, controles de acceso, cifrado y remisión de información del ecosistema SIEM-SOC. Su finalidad es fortalecer integridad, confidencialidad, disponibilidad y trazabilidad. La admisibilidad y valoración de evidencia corresponden a las autoridades competentes; el sistema no garantiza validez jurídica automática.

II. Alcance

Ámbito propuesto, sujeto a aprobación institucional:

- DIRINCRI (Jefatura y Unidades de Investigación operativas).
- DIRTIC PNP (ente rector TICs).
- Personal de las áreas de seguridad digital institucional.
- Oficiales operativos encargados de cadena de custodia digital.
- Proveedores tecnológicos contratados.
- Órganos de control interno.

III. Base normativa

El presente procedimiento se sustenta en el siguiente marco normativo:

a. Normativa constitucional

Constitución Política del Perú:

- Art. 2 inc. 6: Derecho a la protección de datos personales.
- Art. 159: Función constitucional del Ministerio Público.
- Art. 166: Finalidad constitucional de la Policía Nacional del Perú.

b. Normativa legal interna

- Decreto Legislativo Nro. 1267 - Ley de la Policía Nacional del Perú.
- Decreto Legislativo Nro. 1412 - Ley de Gobierno Digital.
- Ley Nro. 29733, Ley de Protección de Datos Personales. Para el tramo anterior al 31 de marzo de 2025, considerar el reglamento entonces aplicable; desde esa fecha, el aprobado por el Decreto Supremo Nro. 016-2024-JUS.
- Ley Nro. 30096 - Ley de Delitos Informáticos.
- Ley Nro. 30077 - Ley contra el Crimen Organizado (uso de técnicas especiales).
- Ley Nro. 27444 - Ley del Procedimiento Administrativo General.
- Ley Nro. 32069, Ley General de Contrataciones Públicas, y Reglamento aprobado por el Decreto Supremo Nro. 009-2025-EF, con las modificaciones aplicables al momento de ejecutar.
- Decreto Legislativo Nro. 1252 - Sistema Nacional de Programación Multianual y Gestión de Inversiones (Invierte.pe).

c. Normativa reglamentaria y directivas

- Política Nacional de Transformación Digital.

- Lineamientos de Interoperabilidad del Estado - PCM.
- Directivas de la Secretaría de Gobierno y Transformación Digital (SGTD-PCM).
- Directivas internas de seguridad de la información de la PNP.
- Directiva de Cadena de Custodia Digital del Ministerio Público (cuando corresponda).

d. Normativa procesal

Código Procesal Penal de 2004:

- Artículos relativos a cadena de custodia.
- Principio de legalidad probatoria.
- Exclusión de prueba ilícita.

Jurisprudencia sobre integridad y autenticidad de evidencia digital.

e. Estándares internacionales

- ISO/IEC 27001: Sistema de Gestión de Seguridad de la Información.
- ISO/IEC 27002: Controles de seguridad.
- ISO/IEC 27032: Estándar internacional que proporciona directrices para mejorar la ciberseguridad, abordando aspectos técnicos y colaborativos en un entorno digital.
- ISO/IEC 27037: Identificación, recolección y preservación de evidencia digital.
- NIST SP 800-92: Log Management.
- NIST SP 800-137: Continuous Monitoring.
- Convenio de Budapest sobre Ciberdelincuencia.

f. Incorporación de normativa en el procedimiento

- ***Control de acceso basado en roles (RBAC)***

  Sustento:

  ✓ D. Leg. 1412 (Gobierno Digital).
  ✓ ISO/IEC 27001, controles de acceso según la edición que se adopte; no se atribuye una numeración de control sin precisar la versión.
  ✓ Ley 29733 (Protección de Datos).

  Control propuesto sujeto a aprobación interna y asignación formal de responsabilidades.

- ***Principio del mínimo privilegio***

  Sustento:

  ✓ ISO/IEC 27002.
  ✓ NIST SP 800-53.
  ✓ Ley 30096 (Delitos Informáticos - acceso indebido).

- Cifrado TLS y AES

  Sustento:

  ✓ ISO/IEC 27001 (Criptografía).
  ✓ NIST FIPS 197 (AES).
  ✓ Lineamientos SGTD-PCM sobre seguridad digital.
  ✓ Ley 29733 (Protección de datos sensibles).

- ***Sellos de tiempo y Hash en exportaciones a MP/PJ***
  Sustento:
  - ✓ Código Procesal Penal (cadena de custodia).
  - ✓ ISO/IEC 27037.
  - ✓ Ley 27269 (Firmas y Certificados Digitales).
  - ✓ Principio de autenticidad y no repudio probatorio.

- ***Auditorias y bitácoras***
  Sustento:
  - ✓ Ley 27785 (Sistema Nacional de Control).
  - ✓ ISO/IEC 27001, controles de registro y monitoreo según la edición adoptada.
  - ✓ NIST SP 800-92 (Gestión de logs).

- ***Cláusula de cumplimiento normativo***
  Este anexo es una propuesta académica de procedimiento y no una norma vigente. Su aprobación, ámbito y mecanismos de supervisión deben definirse por los órganos competentes. Las eventuales responsabilidades se determinan conforme al ordenamiento aplicable y al debido procedimiento; el anexo no crea infracciones ni sanciones.

- Enfoque de gestión pública en Invierte.pe
  Desde la perspectiva de inversión pública:
  - ✓ El procedimiento propone controles de operación; su sostenibilidad requiere recursos y personal acreditados.
  - ✓ Reduce riesgo de observaciones por Contraloría.
  - ✓ Busca alineamiento con el marco de gobierno digital.
  - ✓ Contribuye a la trazabilidad; no garantiza admisibilidad ni valoración probatoria.

Matriz RACI propuesta para coordinación institucional

R ejecuta; A responde por la decisión o entrega; C es consultado; I es informado. Cada actividad tiene una sola A. La matriz es una propuesta para validación contra competencias formales; no modifica el ROF ni atribuye obligaciones a entidades externas. La aprobación institucional debe identificar responsables nominales y suplencias.

Actividad	DIRTIC	DIRINCRI	Custodio	Administración
Infraestructura conectividad y soporte	A/R	C	I	C
Configuración técnica accesos y respaldos	A/R	C	C	I
Priorizar y validar reglas de detección	R	A	C	I
Triage escalamiento y atención operativa	C	A/R	I	I
Preservación y registro de evidencia	C	A	R	I
Remisión autorizada a MP o PJ	C	A	R	I
Contratación y disponibilidad de gasto	C	R	I	A
Conformidad operativa del piloto	R	A	C	C

- ***Clasificación de roles***

Rol	Competencia	Nivel de Acceso
Administrador SIEM	Configuración técnica	Privilegios mínimos por función; acceso auditado y segregado de custodia
Analista SOC N1	Monitoreo	Lectura y alertas
Analista SOC N2	Investigación técnica	Lectura y correlación avanzada
Supervisor SOC	Validación	Validación y escalamiento
Oficial Cadena Custodia	Exportación probatoria	Exportación cifrada con firma
Usuario Investigativo	Consulta por caso	Acceso restringido

IV. Cifrado y Protección de Datos

1.1. Cifrado de Tránsito

- Toda comunicación entre SIEM y sistemas externos (SIDPOL, RENIEC, MP, PJ) deberá utilizar TLS 1.3 o superior.[3]
- Certificados digitales emitidos por autoridad certificadora reconocida por el Estado.

1.2. Cifrado en reposo

- Bases de datos, almacenamiento de logs y respaldos deberán emplear AES-256.[4]
- Gestión de claves mediante HSM[5] o servicio equivalente certificado.

1.3. Integridad de Logs

- Implementación de hash SHA-256 para verificación de integridad.
- Logs inmutables con almacenamiento WORM (*Write Once Read Many*).

V. Gobernanza de Logs

a. Clasificación de logs por criticidad (alta, media, baja).
b. Los plazos de retención se aprobarán por categoría, finalidad y obligación aplicable, considerando minimización y preservación de evidencia. No se impone un plazo uniforme de cinco años sin sustento.
c. Indexación automatizada.
d. Trazabilidad completa de consultas y modificaciones.

VI. Protocolo de Interoperabilidad y Exportación a MP/PJ

6.1. Requisitos técnicos obligatorios

Toda exportación de evidencia digital deberá:

- Generar hash criptográfico SHA-256 verificable.
- Incorporar sello de tiempo certificado (TSA).

[3] **TLS 1.3** es la última versión del protocolo de seguridad *Transport Layer Security* (TLS), diseñado para mejorar la seguridad y el rendimiento de las conexiones en Internet. Introduce un proceso de enlace más eficiente, reduciendo el número de viajes de ida y vuelta entre cliente y el servidor, lo que resulta en conexiones más rápidas y menos propensas a fallos.

[4] **AES 256**, que significa Estándar de Cifrado Avanzado (*Advanced Encryption Standard*), es un algoritmo de cifrado adoptado por el gobierno de los Estados Unidos en 2001. AES-256 utiliza una clave de 256 bits, lo que proporciona un nivel extremadamente alto de seguridad.

[5] **Los HSM** son dispositivos físicos especializados que aseguran que las claves estén fuera del entorno del software vulnerable, protegiendo así los activos digitales más críticos de una organización.

- Incorporar firma digital del responsable conforme al marco aplicable y a los medios institucionales disponibles.
- Transmitirse mediante canal cifrado TLS.
- Generar acta digital de remisión.

6.2. Registro de exportaciones (Bitácora Obligatoria)

El sistema registrará automáticamente:

- Usuario exportador.
- Fecha y hora exacta.
- Identificador único del caso.
- Hash generado.
- Entidad destinataria.
- Confirmación de recepción.

Las bitácoras serán:

- Inmutables.
- Auditables.
- Conservadas según la política de retención aprobada y las necesidades de preservación del caso.

VII. Auditoría y Control

7.1. Auditoría técnica

- Auditoría interna semestral del SIEM.
- Pruebas de penetración anual.
- Verificación de cumplimiento ISO/IEC 27001.

7.2. Auditoría probatoria

- Validación conjunta con fiscal designado.
- Simulacros de exportación probatoria.
- Revisión de cadena de custodia digital.

7.3. Reportes

- Informe trimestral de incidentes.
- Informe anual de desempeño y trazabilidad.
- Reporte de cumplimiento a SGTD-PCM.

VIII. Gestión de riesgos

Riesgo	Impacto	Medida Correctiva
Acceso indebido	Alto	MFA más monitoreo de sesiones privilegiadas
Filtración de datos	Alto	AES-256 más DLP
Nulidad probatoria	Alto	Hash, preservación y registro de custodia; no garantiza admisibilidad automática
Manipulación interna	Medio-Alto	Logs inmutables más revisión cruzada

IX. Responsabilidad funcional

La evaluación de incumplimientos y responsabilidades corresponderá a los órganos competentes, conforme a normas vigentes y debido procedimiento.

X. Consideraciones desde Invierte.pe

El presente anexo propone controles complementarios para una implementación futura. No acredita expediente técnico aprobado, sostenibilidad financiera ni validez probatoria automática.

- Sostenibilidad operativa.
- Cumplimiento normativo.
- Protección de valor probatorio.
- Generación de valor público mediante evidencia digital íntegra.

Anexo 18: Plan Estratégico de Gestión del Cambio y Sensibilización Institucional

1. Finalidad y condición de la propuesta

El plan organiza la preparación del personal para adoptar los procedimientos y herramientas asociados al SIEM en la DIRINCRI. Busca que el despliegue tecnológico se acompañe de comprensión de su finalidad, capacidades prácticas y cambios sostenibles en el trabajo cotidiano. Constituye una propuesta del trabajo de investigación, sujeta a aprobación, asignación de responsables y financiamiento.

El diagnóstico del trabajo identifica necesidades de capacitación y resistencia al cambio. Estas condiciones orientan el plan, pero los porcentajes de la encuesta histórica no se convierten en una línea de base de adopción del piloto. Antes de iniciar, se verificará el personal objetivo y se medirán sus competencias, preocupaciones y prácticas. La ausencia de participación no se interpretará automáticamente como resistencia: puede obedecer a carga laboral, turnos, acceso o falta de información.

2. Objetivo general y objetivos específicos

Objetivo general: preparar y acompañar al personal comprendido en el piloto para aplicar los procedimientos del SIEM, mediante sensibilización, formación por funciones, participación y seguimiento de la adopción.

Objetivos específicos: identificar y atender barreras de adopción; explicar responsabilidades y alcances del monitoreo institucional; desarrollar competencias operativas verificables; establecer acompañamiento durante el piloto; y evaluar resultados para decidir ajustes o expansión.

3. Alcance y criterios de actuación

El alcance inicial comprende las jefaturas y usuarios de las unidades seleccionadas para el piloto, los analistas, el responsable operativo, el custodio y el administrador técnico vinculado a DIRTIC. La nómina y las funciones se validarán antes de iniciar. La extensión a otras unidades dependerá de los resultados y de la capacidad disponible.

La ejecución respetará las competencias institucionales y la protección de información sensible. Los ejercicios utilizarán datos sintéticos o anonimizados previamente autorizados. La evaluación de aprendizaje será distinta del seguimiento disciplinario. Las consultas se atenderán sin exponer innecesariamente al personal; cualquier irregularidad se tramitará mediante los canales competentes.

4. Responsabilidades y participación del personal

La jefatura competente de DIRINCRI actuará como patrocinador propuesto: solicitará la aprobación del plan, definirá prioridades, facilitará horas de formación y resolverá barreras que excedan al equipo del piloto. La asignación concreta se formalizará antes de ejecutar actividades.

El responsable operativo del piloto coordinará el plan, mantendrá el padrón de participantes, consolidará el cronograma y presentará el informe mensual. El enlace de DIRTIC validará contenidos técnicos, requisitos de acceso y ejercicios. El custodio revisará los contenidos relacionados con preservación y trazabilidad de la evidencia digital.

Las áreas competentes de capacitación, recursos humanos, administración y presupuesto intervendrán según sus atribuciones: validarán perfiles y horas disponibles, tramitarán actividades formativas y revisarán costos y mecanismos de contratación o cooperación. No se presupone la creación de una nueva oficina ni una reasignación de competencias.

Cada unidad del piloto propondrá un referente operativo con tiempo disponible. Este recogerá dudas, acompañará el uso inicial de los procedimientos y comunicará dificultades al coordinador. No sustituirá al analista de seguridad ni autorizará accesos o decisiones de custodia.

5. Diagnóstico de barreras y comunicación

En los meses 1-2 se aplicará un cuestionario breve al personal del padrón y se realizarán conversaciones por función. Se explorarán claridad de responsabilidades, carga de trabajo, confianza en el tratamiento de datos, experiencia digital y disponibilidad para capacitarse. Los resultados se registrarán de forma agregada; no se atribuirán percepciones a personas identificables en los informes generales.

Se mantendrá un registro de barreras con descripción, evidencia, responsable, acción, plazo y estado. Por ejemplo, la falta de tiempo se abordará con horas protegidas y recuperación; la dificultad técnica, con práctica y apoyo; y las dudas sobre monitoreo, con explicación de finalidad, permisos, límites y canales de consulta. Las mejoras sugeridas se evaluarán y se comunicará su aceptación o rechazo motivado.

La comunicación inicial explicará qué cambiará, por qué, a quién corresponde cada tarea y cómo solicitar apoyo. Habrá una sesión para jefaturas, una sesión por grupo operativo y un instructivo breve por función. Durante el piloto se comunicarán ajustes y resultados agregados mensualmente, sin divulgar configuraciones sensibles ni detalles de incidentes.

6. Formación progresiva y verificación de competencias

Se propone que la formación necesaria para operar sea obligatoria para el personal asignado al piloto, una vez aprobada por la autoridad competente. La obligatoriedad deberá acompañarse de horas programadas, acceso a materiales, cobertura de turnos y recuperación; no puede depender exclusivamente del tiempo personal del participante.

Nivel inicial de sensibilización

Dirigido a todo el personal del piloto. Comprende finalidad del SIEM, responsabilidades, protección de información, reporte de incidentes y solicitud de ayuda. Se propone una duración inicial de cuatro horas, ajustable al diagnóstico. El producto será una ficha de responsabilidades y una evaluación mediante situaciones breves.

Nivel operativo por funciones

Para usuarios y jefaturas: ocho horas propuestas sobre reporte, uso del protocolo, escalamiento y decisiones dentro de sus competencias. Para analistas y personal técnico: veinticuatro horas propuestas sobre ingesta, reglas, clasificación inicial de alertas, accesos y registro de actuaciones. Para custodia: doce horas propuestas sobre identificación, preservación, transferencia y documentación de evidencia. Quienes acumulen funciones recibirán los módulos pertinentes sin duplicar contenidos comunes.

Nivel especializado y capacitación universitaria

Tras identificar brechas específicas, se evaluará formación especializada y certificaciones pertinentes para administración, análisis de incidentes o evidencia digital. Se podrá proponer cooperación o contratación con universidades y entidades competentes. Antes de seleccionar una oferta se verificará la entidad, el programa, las horas, el instrumento de evaluación y el documento que efectivamente otorga.

Una constancia universitaria de capacitación y una certificación profesional acreditan resultados diferentes. No se presentarán como equivalentes ni se afirmará acreditación universitaria o profesional sin comprobarla. La participación y el financiamiento dependerán de pertinencia funcional, requisitos, disponibilidad y autorización.

Evaluación práctica y recuperación

Antes de operar sin acompañamiento, cada participante resolverá un ejercicio correspondiente a su función. La rúbrica propuesta evalúa identificación del evento, aplicación del protocolo, registro, escalamiento y protección de la evidencia cuando corresponda. El criterio inicial será al menos 80 % del puntaje y cumplimiento de todos los pasos críticos definidos antes del ejercicio. Quien no lo alcance recibirá refuerzo y nueva evaluación; no desempeñará autónomamente la tarea crítica hasta demostrar competencia.

7. Cronograma y recursos para la ejecución

Programación vinculada a la hoja de ruta

Meses 1-2: validar participantes, responsabilidades y horas disponibles; medir competencias y barreras; ejecutar sensibilización; elaborar el registro de barreras y el plan de formación. Productos: padrón, diagnóstico inicial, mensajes por función y cronograma aprobado.

Meses 3-4: desarrollar formación operativa y técnica, ajustar instructivos y practicar con datos autorizados. Productos: registros de asistencia, materiales, rúbricas y resultados. La adquisición del SIEM conserva los meses 5-6 de la ruta; si aún no existe entorno técnico, la preparación utilizará casos y simulaciones, sin afirmar experiencia sobre una plataforma no disponible.

Meses 5-6: verificar preparación para el piloto, organizar recuperación y validar soporte. La evaluación específica de la plataforma se completará cuando el entorno esté

disponible. Productos: relación de personal habilitado por función y pendientes de recuperación. Si no se cumplen las condiciones, se reprogramará el inicio operativo.

Meses 7-9: acompañar el piloto, realizar ejercicios guiados, observar aplicación de procedimientos y revisar barreras mensualmente. Productos: informes de adopción, acciones de mejora y evaluación del piloto. Desde el mes 10: decidir expansión condicionada y mantener refuerzo trimestral tras la aceptación.

Recursos y estimación del costo

Se requerirán horas de participantes y facilitadores, reemplazos cuando sean necesarios, materiales, ambiente de formación, entorno de práctica, soporte, evaluaciones y costos de programas o certificaciones autorizados. No se fija un monto sin fuentes verificables. El costo se incorporará al presupuesto del proyecto evitando duplicar rubros de capacitación ya registrados.

El costo por actividad se calculará mediante cantidades y precios unitarios documentados. Las horas de personal se registrarán separadamente de los desembolsos adicionales; solo se monetizarán cuando exista un criterio institucional validado. Cada precio externo identificará proveedor o fuente, fecha, moneda, impuestos, alcance y vigencia. Se distinguirán necesidades iniciales y recurrentes.

Condiciones para iniciar la operación

Antes de operar se verificará aprobación, padrón, responsabilidades, disponibilidad de personal, formación completada, evaluación práctica, canales de ayuda y entorno autorizado. Los incumplimientos se documentarán y elevarán a la autoridad competente; las metas temporales no justificarán omitir requisitos de seguridad o competencia.

8. Indicadores y metas propuestas

Las siguientes metas son parámetros de planificación sujetos a validación; no representan resultados obtenidos. El coordinador registrará numerador, denominador, fecha de corte, fuente y exclusiones. Las tasas se presentarán junto con los números absolutos para facilitar su interpretación.

Cobertura de formación: participantes del padrón que completan los módulos obligatorios / personal del padrón obligado a cursarlos x 100. Meta propuesta: 100 % antes de asumir funciones operativas. Fuente: padrón y registros de conclusión; corte previo al inicio y ante nuevas incorporaciones.

Competencia inicial: participantes que superan la evaluación práctica / participantes evaluados x 100. Meta propuesta: al menos 80 % en la primera evaluación. Como condición de operación autónoma, cada persona deberá aprobar los criterios de su función después del refuerzo necesario. Fuente: rúbricas y actas de evaluación.

Adopción: actuaciones observadas que cumplen todos los pasos aplicables del protocolo / actuaciones observadas evaluables x 100. Meta provisional: al menos 80 % al cierre del mes 9. El método de selección y número de actuaciones se definirán antes de medir. Si no

hay casos reales suficientes, se reportarán ejercicios por separado y no se estimará adopción real a partir de ellos.

Atención de barreras: acciones de respuesta concluidas dentro del plazo acordado / acciones cuyo plazo vence en el periodo x 100. Meta provisional: al menos 80 % mensual. El cierre requerirá evidencia y validación con la unidad afectada. Registrar también barreras nuevas, reiteradas y pendientes; el cierre administrativo no acredita por sí solo un cambio cultural.

9. Seguimiento y gestión de riesgos

El coordinador presentará un informe mensual al patrocinador con participación, aprendizaje, adopción, barreras, recursos y decisiones pendientes. Una caída de resultados originará revisión de causas y acciones correctivas, no atribución automática de culpa. Se revisarán los riesgos R3 de capacitación y R5 de resistencia al cambio junto con el registro de riesgos del proyecto, sin modificar su valoración únicamente por haber realizado una charla.

El cierre del piloto documentará productos, resultados, limitaciones y ajustes requeridos. La decisión de expansión considerará competencias demostradas, disponibilidad de soporte y recursos, cumplimiento de procedimientos y barreras pendientes. Los registros conservarán evidencia de lo ejecutado y permitirán distinguir las actividades propuestas de las efectivamente realizadas.

10. Sustento y articulación con el trabajo

El plan es elaboración propia, sustentada en el diagnóstico y la propuesta del trabajo. Se articula con el apartado 3.3.3, la ruta del Anexo 3 y los riesgos del Anexo 7. Sus metas y actividades son propuestas sujetas a validación institucional.

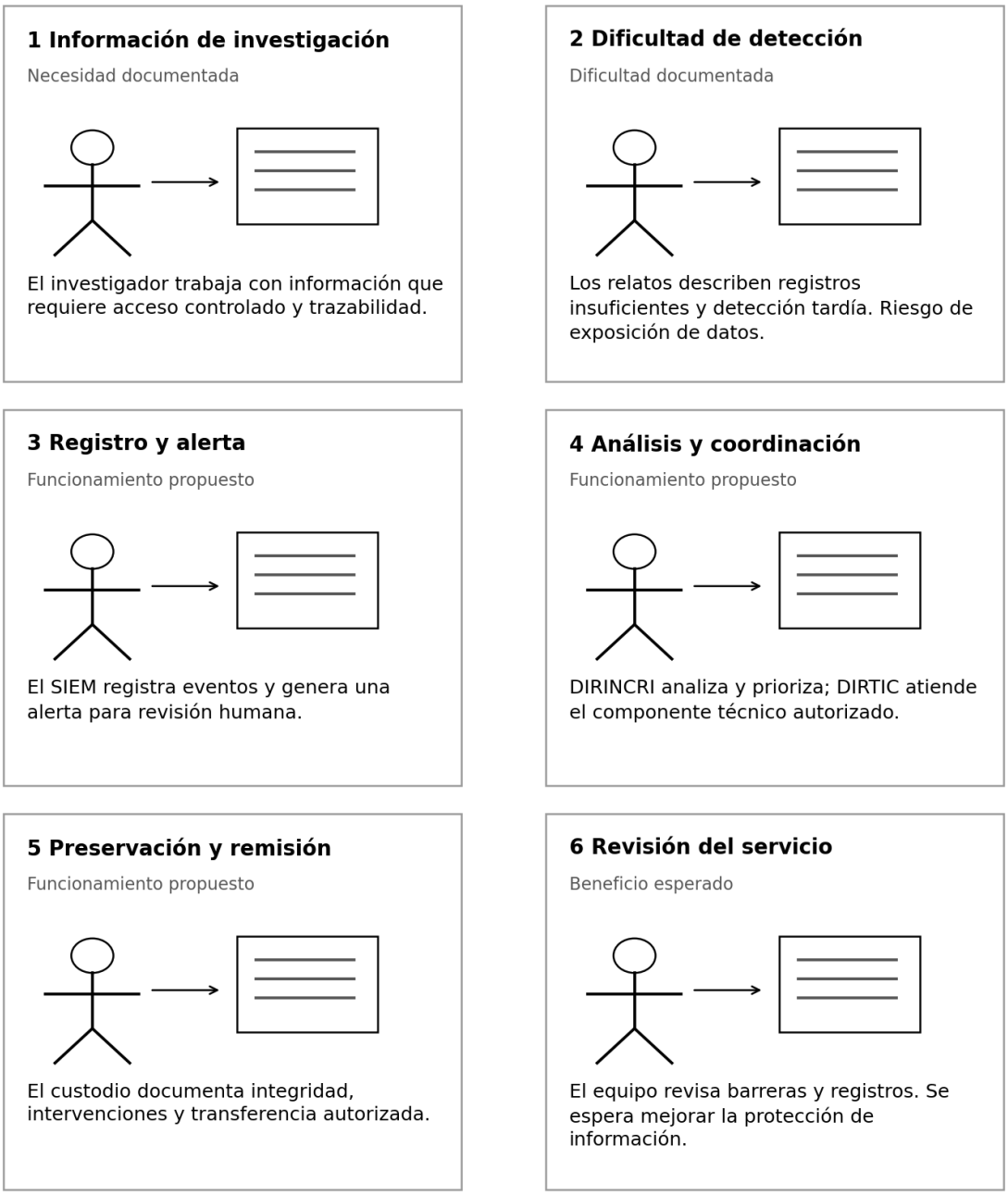
Anexo 19 Mapa de Empatía del usuario institucional

Perfil compuesto: personal que gestiona información de investigación y requiere apoyo técnico para protegerla y conservar su trazabilidad. Ámbito: necesidades del usuario institucional, interpretadas con apoyo de especialistas relacionados. Base: testimonios aportados de 2025 y encuesta institucional; no es un retrato psicológico ni un mapa del ciudadano.

Dimensión	Síntesis sustentada y fuente
Qué expresa	Requiere capacitación continua, monitoreo y coordinación operativa y técnica. G001, G004 y G005, OE3.
Qué observa o describe	Describe infraestructura insuficiente, sistemas heterogéneos y restricciones de recursos. G001, G004 y G005, OE1.
Qué escucha o recibe	G004 refiere normas y recomendaciones de auditoría con límites presupuestales para su ejecución. Entorno referido, no generalizado. G004, OE1.
Qué hace o necesita hacer	Necesita reconstruir actuaciones, identificar accesos y conservar registros. Tareas requeridas; no observación de cumplimiento. G001 y G005, OE2.
Qué piensa y qué le preocupa	Prioriza protección y continuidad. G007 refiere inseguridad y desconfianza del personal ante incidentes; no representa a toda la muestra. G007, OE2.
Dificultades y esfuerzos	Dificultades de detección y registro de acceso, modificación y transferencia. G001 y G005, OE2.
Necesidades y resultados deseados	Formación por funciones, registros confiables, roles claros y apoyo sostenible. Resultado esperado: protección y actuaciones verificables. G001 y G005, OE3.

Nota. Elaboración propia mediante síntesis analítica de testimonios. Las fuentes y el contraste cuantitativo se detallan en la matriz de trazabilidad. Los beneficiarios finales son las personas cuya información se gestiona; sus experiencias y emociones no fueron recogidas directamente en los archivos aportados.

Anexo 20 Secuencia visual del Storyboard



Nota. Escenario compuesto elaborado a partir del diagnóstico de 2025. Las acciones del SIEM son propuestas futuras; no se representa un incidente real ni satisfacción ciudadana medida. El sustento de cada escena se desarrolla a continuación.

Anexo 20 Storyboard del servicio propuesto para el usuario institucional

Escenario ilustrativo: un investigador trabaja con información digital de una investigación y requiere identificar una actividad sospechosa y preservar los registros pertinentes. La secuencia combina necesidades documentadas en 2025 con acciones futuras propuestas. No corresponde a un caso real observado ni constituye evidencia de ejecución del sistema.

Escena 1 Trabajo con información de una investigación

Actor: usuario investigador. Interacción: consulta y gestiona información digital mediante herramientas institucionales. Necesidad: identificar quién accede y qué actuaciones se realizan. Sustento: G001, OE2, describe la importancia de registros de acceso, modificación y transferencia. La encuesta incluye preguntas sobre seguimiento del uso de información y dificultad para identificar accesos. La escena concreta es una construcción ilustrativa.

Escena 2 Dificultad para advertir o reconstruir una actividad sospechosa

Actor: investigador con apoyo técnico. Dificultad del diagnóstico: los especialistas describen detección tardía, registros insuficientes y problemas para reconstruir hechos. Sustento: G005, OE1 y OE2; G010, OE2. No se asigna a este escenario una filtración, víctima o tiempo de respuesta real. Consecuencia posible para el beneficiario final: exposición de información, formulada como riesgo.

Escena 3 Registro y generación de alerta mediante el SIEM

Actor: administrador técnico y analista. Interacción propuesta: integrar fuentes autorizadas, correlacionar eventos y registrar una alerta para su revisión. Sustento de la necesidad: G005, OE3, propone SIEM y herramientas de auditoría; G010, OE3, plantea centralización de logs y alertas. Condiciones: inventario, reglas validadas, accesos autorizados y capacidad técnica. La generación de una alerta no demuestra por sí sola la comisión de un delito.

Nota. Escenas 1-2: necesidades y dificultades documentadas, representadas mediante un escenario compuesto. Escena 3 y siguientes: funcionamiento futuro propuesto. El SIEM contribuye al monitoreo; no sustituye la investigación, la adquisición forense ni los procedimientos de custodia.

Anexo 20 Continuación del Storyboard

Escena 4 Análisis operativo y coordinación técnica

Actor: analista operacional de DIRINCRI y enlace de DIRTIC. Interacción propuesta: clasificar la alerta, comprobar su contexto, documentar actuaciones y escalar según protocolo. DIRINCRI prioriza la atención operativa; DIRTIC atiende el componente técnico dentro de las competencias que se validen. Sustento: G001, OE1, refiere limitada articulación entre áreas; G005, OE1 y OE3, plantea responsabilidades y gestión de incidentes. La distribución se vincula con la matriz RACI del Anexo 17.

Escena 5 Preservación y transferencia documentada

Actor: custodio y personal autorizado. Interacción propuesta: identificar los registros pertinentes, preservar su integridad, documentar quién interviene y transferirlos por canales autorizados cuando corresponda. Sustento: G001 y G005, OE2, señalan riesgos de trazabilidad; G010, OE2, diferencia dificultades de investigación y pérdida de datos volátiles. El sistema apoyaría la trazabilidad, pero no garantiza admisibilidad ni valoración probatoria automática.

Escena 6 Revisión del servicio y protección de los beneficiarios

Actor: responsable operativo, equipo técnico y usuario investigador. Interacción propuesta: revisar registros, barreras, cumplimiento y necesidades de formación; documentar mejoras y limitaciones. Sustento: G004 y G005, OE3, proponen capacitación y cooperación. Beneficio esperado para agraviados, denunciantes, testigos e investigados: menor exposición de su información y mayor posibilidad de verificar actuaciones. No se afirma una mejora ya medida en seguridad, confianza o satisfacción ciudadana.

Qué deberá verificarse durante la implementación

Experiencia institucional: facilidad de uso, claridad de roles, barreras y formación requerida. Desempeño: completitud de registros de custodia y tiempos de atención medidos con definiciones y denominadores previos. Perspectiva ciudadana: recoger directamente experiencias mediante un instrumento específico y condiciones de confidencialidad; los testimonios de especialistas no sustituyen ese levantamiento.

Nota. Elaboración propia basada en el diagnóstico de 2025 y en la propuesta del trabajo. Las escenas expresan una secuencia diseñada para comunicar necesidades y respuestas institucionales; no son fotografías, observaciones de campo ni resultados de un piloto ejecutado.

Matriz de trazabilidad de los dos instrumentos

El componente cualitativo comprendió trece entrevistas realizadas en 2025 a once efectivos policiales y dos expertos civiles, cuyas transcripciones fueron analizadas mediante ATLAS.ti. El archivo G011 se conserva con su encabezado corregido, por lo que se retira la exclusión consignada en la versión anterior. La matriz siguiente identifica los testimonios específicos que sustentan el Mapa de Empatía y el Storyboard; no constituye un listado completo de las trece entrevistas. La correspondencia entre los códigos, los archivos de transcripción y los participantes debe mantenerse consistente con el registro del análisis y con los perfiles del Anexo 11. Las fechas que no figuren en las transcripciones deberán cotejarse con los registros originales; la identificación del levantamiento como correspondiente a 2025 se sustenta en la información proporcionada por el equipo investigador.

Contenido	Fuente y ubicación	Uso
Recursos y articulación	G001, OE1, preguntas sobre factores y barreras.	Mapa; escenas 1 y 4.
Normas y auditorías	G004, OE1, pregunta sobre normas y políticas.	Mapa, entorno referido.
Logs y detección	G005, OE1, barreras; OE2, impactos; OE3, tecnologías.	Mapa; escenas 2 y 3.
Inseguridad y desconfianza del personal	G007, OE2, pregunta sobre impactos operativos.	Mapa, preocupación referida; no prevalencia.
Trazabilidad y datos volátiles	G001 y G005, OE2, validez; G010, OE2, validez e impactos.	Escena 5; conservar diferencias entre testimonios.
Capacitación y cooperación	G004 y G005, OE3, pregunta sobre capacitación.	Mapa; escena 6.

Contraste cuantitativo de la encuesta

Fuente: DATA SOBRE ESTADÍSTICA.xlsx, hoja Respuestas de formulario 1, filas 2-84. Se verificaron 83 registros, 12 ítems y ausencia de respuestas vacías o fuera del intervalo 1-5. La correspondencia de la escala se toma del cuestionario del trabajo: 1-2 desacuerdo, 3 neutralidad y 4-5 acuerdo. Los siguientes resultados suman respuestas 4 y 5; describen al grupo participante.

Capacitación insuficiente, ítem 3: 40/83 (48,2 %). Dificultad para identificar acceso o modificación, ítem 5: 48/83 (57,8 %). Utilidad de capacitación básica, ítem 9: 66/83 (79,5 %). Utilidad de registro automático, ítem 11: 60/83 (72,3 %). Estas opiniones contrastan necesidades del mapa; no acreditan incidentes, emociones, causalidad ni satisfacción ciudadana.

La transcripción G010 contiene una valoración distinta sobre la relación entre monitoreo y validez probatoria; se conserva esa divergencia y no se presenta unanimidad. La elaboración posterior de los instrumentos no cambia el año del levantamiento ni incorpora nuevas entrevistas o encuestas.