UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO

FACULTAD DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA, INFORMÁTICA Y MECÁNICA

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

TESIS

PROPUESTA DE UN MODELO DE CIBERSEGURIDAD BASADO EN EL MARCO NIST CSF PARA LA GESTIÓN DE VULNERABILIDADES EN LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA SUNARP

PRESENTADO POR:
Br. KENNY HAROLD CARMONA CHOQUEMAMANI
Br. JEREMY AXL LAZO MENDOZA

PARA OPTAR AL TÍTULO PROFESIONAL DE INGENIERO INFORMÁTICO Y DE SISTEMAS

ASESOR:
Dr. HARLEY VERA OLIVERA

CUSCO - PERÚ

2026

Universidad Nacional de San Antonio Abad del Cusco

INFORME DE SIMILITUD

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

El que suscribe, el **Asesor** HARLEY VERA OLIVERA ..... quien aplica el software de detección de similitud al trabajo de investigación/tesistitulada: PROPUESTA DE UN MODELO DE CIBERSEGURIDAD BASADO EN EL MARCO NIST CSF PARA LA GESTIÓN DE VULNERABILIDADES EN LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA SUNARP

Presentado por: KENNY HAROLD CARMONA CHOQUEMAMANI DNI N° 72792288;
presentado por: JEREMY AXL LAZO MENDOZA DNI N°: 70374847
Para optar el título Profesional/Grado Académico de INGENIERO INFORMATICO Y DE SISTEMAS

Informo que el trabajo de investigación ha sido sometido a revisión por 2 veces, mediante el Software de Similitud, conforme al Art. 6° del ***Reglamento para Uso del Sistema Detección de Similitud en la UNSAAC*** y de la evaluación de originalidad se tiene un porcentaje de 9 **%.**

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

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

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

Cusco, 25 de AGOSTO de 20 26

Firma
Post firma Harley Vera Olivera
Nro. de DNI 72572815
ORCID del Asesor 0000-0003-2011-8797

Se adjunta:

1. Reporte generado por el Sistema Antiplagio.
2. Enlace del Reporte Generado por el Sistema de Detección de Similitud: **oid:** 27259:617157199

KENNY HAROLD - JEREMY AXL CARMONA CHOQUE...

PROPUESTA DE UN MODELO DE CIBERSEGURIDAD BASADO EN EL MARCO NIST CSF PARA LA GESTIÓN DE VULNERABILI...

Universidad Nacional San Antonio Abad del Cusco

Detalles del documento

Identificador de la entrega
trn:oid:::27259:617157199

Fecha de entrega
25 ago 2026, 3:10 p.m. GMT-5

Fecha de descarga
25 ago 2026, 6:09 p.m. GMT-5

Nombre del archivo
TESIS FINAL - JEREMY LAZO Y KENNY CARMONA.pdf

Tamaño del archivo
2.1 MB

184 páginas

40.230 palabras

228.726 caracteres

9% Similitud general

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

Filtrado desde el informe

- Bibliografía
- Texto citado
- Texto mencionado
- Coincidencias menores (menos de 8 palabras)

Exclusiones

- N.º de coincidencias excluidas

Fuentes principales

6% Fuentes de Internet
2% Publicaciones
8% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

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

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

PRESENTACIÓN

SEÑOR: DECANO DE LA FACULTAD DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA, INFORMÁTICA Y MECÁNICA DE LA UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO

SEÑOR: DIRECTOR DE LA ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

SEÑORES: DOCENTES MIEMBROS DEL JURADO

Con la conformidad del reglamento de grados y títulos de la Escuela Profesional de Ingeniería Informática y de Sistemas, ponemos a consideración el presente trabajo de tesis intitulado: **"PROPUESTA DE UN MODELO DE CIBERSEGURIDAD BASADO EN EL MARCO NIST CSF PARA LA GESTIÓN DE VULNERABILIDADES EN LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA SUNARP"** para optar al Título Profesional de **INGENIERO INFORMÁTICO Y DE SISTEMAS**.

Atentamente,

Br. Kenny Harold Carmona Choquemamani

Br. Jeremy Axl Lazo Mendoza

DEDICATORIA

Dedico el presente trabajo a Dios, por guiar mis pasos y darme la fortaleza para alcanzar esta meta. A mis padres, Jose Carmona y Edith Choquemamani, por su esfuerzo y apoyo incondicional; a mi hermana Paola Carmona, por ser un buen ejemplo; y a mi enamorada Cielo Huamanrayme, por su paciencia y confianza en mí. Asimismo, a mi Tio Richard que ya no está físicamente, pero vive en mi memoria como inspiración constante, y a todas las personas que creyeron en mí durante este proceso.

Br. Kenny Harold Carmona Choquemamani

A Dios, por guiarme en cada paso de mi vida; a mis padres, Ruddy Lazo y Ofelia Mendoza, por su amor, sacrificio y apoyo incondicional durante mi formación profesional; a mi hermano menor, Liam Lazo, por su alegría, cariño y por motivarme cada día a seguir adelante y ser un mejor ejemplo para él; y a todas las personas que creyeron en mí y me impulsaron a continuar alcanzando mis metas.

Br. Jeremy Axl Lazo Mendoza

AGRADECIMIENTO

Agradecemos a Dios por guiarnos y brindarnos la fortaleza necesaria para culminar esta importante etapa académica. A nuestros padres y familias, por su apoyo incondicional, sus enseñanzas y la motivación constante que nos impulsó a seguir adelante. Expresamos nuestro sincero agradecimiento a nuestro asesor de tesis, por su orientación, dedicación y valiosos aportes durante el desarrollo de esta investigación. Asimismo, extendemos un especial reconocimiento a los ingenieros de la Unidad de Tecnologías de la Información (UTI) de Superintendencia Nacional de los Registros Públicos (SUNARP) - Sede Cusco, por su disposición, apoyo técnico y por compartir con nosotros sus conocimientos y experiencias durante nuestras prácticas profesionales, contribuyendo significativamente a nuestra formación académica y desarrollo profesional. Finalmente, agradecemos a nuestros docentes y a todas aquellas personas que, de manera directa o indirecta, contribuyeron en la culminación de esta investigación.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ABREVIATURAS

ACL	*Access Control List*
COBIT	*Control Objectives for Information Systems and related Technology*
CPU	*Central Processing Unit*
CVSS	*Common Vulnerability Scoring System*
DBA	*Database Administrator*
FAIR	*Factor Analysis of Information Risk*
IEC	*International Electrotechnical Commission*
INSN	Instituto Nacional de Salud del Niño
IP	*Internet Protocol*
ISO	*International Organization for Standardization*
ITIL	*Information Technology Infrastructure Library*
MCGV	Modelo de Ciberseguridad para la Gestión de Vulnerabilidades
MOF	Manual de Organización y Funciones
MTTR	*Mean Time to Repair*
NIST	*National Institute of Standards and Technology*
NIST CSF	*National Institute of Standards and Technology Cybersecurity Framework*
NVR	*Network Video Recorder*
OTI	Oficina de Tecnologías de la Información
PDCA	*Plan, Do, Check, Act*
PIDE	Plataforma de Interoperabilidad del Estado
PMBOK	*Project Management Body of Knowledge*
ROF	Reglamento de Organización y Funciones
RPO	*Recovery Point Objective*
RRHH	Recursos Humanos
RTO	*Recovery Time Objective*

SGI	Sistema de Gestión de la Información
SGSI	Sistema de Gestión de Seguridad de la Información
SID	Sistema de Intermediación Digital
SIEM	*Security Information and Event Management*
SIGA	Sistema Integrado de Gestión Administrativa
SINARP	Sistema Nacional de los Registros Públicos
SOAR	*Security Orchestration, Automation and Response*
SLA	*Service Level Agreement*
SPRL	Servicio de Publicidad Registral en Línea
SUNARP	Superintendencia Nacional de los Registros Públicos
TI	Tecnologías de la Información
UPS	*Uninterruptible Power Supply*
UTI	Unidad de Tecnologías de la Información

RESUMEN

La presente investigación tuvo como objetivo adaptar e implementar un modelo de ciberseguridad basado en el *National Institute of Standards and Technology Cybersecurity Framework* (NIST CSF) para fortalecer la gestión de vulnerabilidades en la UTI de la SUNARP – Cusco, complementado con controles relacionados de la norma *International Organization for Standardization* (ISO)/*International Electrotechnical Commission* (IEC) 27001. La metodología se desarrolló bajo el enfoque del ciclo de mejora continua *Plan, Do, Check, Act* (PDCA), empleando encuestas al personal técnico, revisión documental de inventarios de activos y análisis de incidentes históricos. Los resultados evidenciaron diferencias en la frecuencia de actualización de inventarios, dependencia de proveedores externos para la atención de incidentes críticos y brechas de capacitación en ciberseguridad. A partir de este diagnóstico se diseñó un modelo que incorpora mecanismos de identificación, priorización y tratamiento de vulnerabilidades, controles de protección y monitoreo, un programa de capacitación y procedimientos de recuperación para servicios críticos. La validación mediante una aplicación piloto en un entorno controlado permitió evidenciar mejoras en los procesos de detección, respuesta y recuperación ante incidentes. Se concluye que la adaptación del NIST CSF, complementada con controles de la norma ISO/IEC 27001, constituye una alternativa viable para fortalecer la gestión de vulnerabilidades y promover la mejora continua de la ciberseguridad en la UTI de SUNARP.

Palabras clave: Ciberseguridad, NIST CSF, ISO/IEC 27001, gestión de vulnerabilidades, SUNARP, PDCA.

ABSTRACT

This research aimed to adapt and implement a cybersecurity model based on the NIST CSF to strengthen vulnerability management at the UTI of SUNARP – Cusco, complemented by related controls from the ISO/IEC 27001 standard. The methodology was developed using the PDCA continuous improvement cycle approach, employing surveys of technical staff, a review of asset inventory documents, and an analysis of historical incidents. The results revealed differences in inventory update frequency, dependence on external providers for handling critical incidents, and cybersecurity training gaps. Based on this diagnosis, a model was designed that incorporates mechanisms for identifying, prioritizing, and addressing vulnerabilities, protection and monitoring controls, a training program, and recovery procedures for critical services. Validation through a pilot application in a controlled environment demonstrated improvements in incident detection, response, and recovery processes. It is concluded that the adaptation of the NIST CSF, complemented by controls from the ISO/IEC 27001 standard, constitutes a viable alternative for strengthening vulnerability management and promoting continuous improvement of cybersecurity at the UTI of SUNARP.

Keywords: Cybersecurity, NIST CSF, ISO/IEC 27001, vulnerability management, SUNARP, PDCA.

INTRODUCCIÓN

En la actualidad, las organizaciones públicas se enfrentan a un entorno digital cada vez más complejo y dinámico, caracterizado por un crecimiento sostenido de las amenazas cibernéticas en términos de frecuencia, impacto y sofisticación (European Union Agency for Cybersecurity, 2023). La acelerada digitalización de los servicios del Estado ha incrementado de manera significativa la exposición de los sistemas de información a riesgos asociados a accesos no autorizados, pérdida de información, interrupciones operativas y afectación a la confianza ciudadana (ISO/IEC, 2022). Esta situación resulta especialmente crítica en aquellas entidades que administran información sensible y servicios esenciales para la seguridad jurídica del país.

En este contexto, la SUNARP cumple un rol estratégico al garantizar la seguridad jurídica mediante la administración de los registros públicos a nivel nacional. La continuidad, integridad y disponibilidad de sus sistemas informáticos constituyen pilares fundamentales para el adecuado funcionamiento de los servicios registrales (Presidencia del Consejo de Ministros, 2021). No obstante, el diagnóstico realizado en la UTI evidencia debilidades relevantes en la gestión de la ciberseguridad, particularmente en los procesos vinculados a la identificación, evaluación y tratamiento de vulnerabilidades en los activos tecnológicos críticos.

La gestión de vulnerabilidades es un componente esencial de la ciberseguridad, ya que permite identificar oportunamente debilidades técnicas, organizacionales y procedimentales que podrían ser explotadas por actores maliciosos (Scarfone y Mell, 2012). Sin embargo, en la UTI de SUNARP se han identificado limitaciones como inventarios de activos incompletos o desactualizados, evaluaciones de riesgos insuficientes, ausencia de mecanismos formales de priorización de vulnerabilidades y una capacidad limitada de respuesta y recuperación ante incidentes. Estas brechas incrementan la exposición de la institución a riesgos que pueden comprometer la continuidad operativa, la integridad de la información y la confianza de los usuarios en los servicios registrales (National Institute of Standards and Technology, 2018).

Diversos estudios realizados en instituciones públicas y privadas han demostrado que la adopción de marcos de ciberseguridad reconocidos internacionalmente contribuye de manera

significativa a fortalecer la gestión de riesgos y vulnerabilidades (Alshaikh, 2020b). Investigaciones desarrolladas en entidades educativas, gubernamentales y empresas en proceso de transformación digital, tales como Tomaylla Castillo y Balbin Balbin (2024) y Yánez Intriago (2022) evidencian que la aplicación del NIST CSF ha permitido mejorar la identificación de activos críticos, optimizar la priorización de vulnerabilidades, fortalecer la respuesta ante incidentes y promover una cultura organizacional orientada a la seguridad de la información (Tøndel *et al.*, 2021). Asimismo, se ha demostrado que su carácter flexible y adaptable lo convierte en una alternativa viable para organizaciones con distintos niveles de madurez en ciberseguridad, incluyendo entidades del sector público.

En este sentido, el NIST CSF se presenta como un marco idóneo para SUNARP, debido a su enfoque estructurado basado en cinco funciones fundamentales (*Identificar, Proteger, Detectar, Responder y Recuperar*) que permiten gestionar de manera integral los riesgos cibernéticos (National Institute of Standards and Technology, 2018). La aplicación de este marco no solo facilita la identificación y mitigación de vulnerabilidades, sino que también contribuye a alinear las prácticas internas con estándares internacionales y buenas prácticas ampliamente validadas en el ámbito de la seguridad de la información (ISO/IEC, 2022).

Adicionalmente, la presente investigación incorpora el ciclo de mejora continua PDCA como soporte metodológico para el diseño del modelo propuesto. Este enfoque es ampliamente utilizado en los sistemas de gestión de la seguridad de la información, ya que permite garantizar la mejora continua de los controles implementados y su adaptación frente a la evolución constante de las amenazas cibernéticas y los cambios tecnológicos, asegurando la eficacia y sostenibilidad del modelo de ciberseguridad propuesto (ISO/IEC, 2022).

En este marco, la presente tesis tiene como objetivo general diseñar un modelo de ciberseguridad basado en el NIST CSF que fortalezca la gestión de vulnerabilidades en la UTI de SUNARP. Para ello, se plantean objetivos específicos orientados al diagnóstico de la situación actual de la gestión de vulnerabilidades, la identificación de los criterios clave del NIST CSF aplicables al contexto institucional, el diseño de un esquema de priorización de vulnerabilidades, la propuesta de estrategias de capacitación para el personal y la definición de mecanismos de recuperación de los servicios críticos.

La aplicación del modelo propuesto permitirá mejorar la capacidad institucional para anticipar, gestionar y responder de manera eficiente a los incidentes de ciberseguridad, optimizar el uso de los recursos tecnológicos disponibles y fortalecer la protección de los activos informáticos críticos que sustentan la labor registral. Asimismo, la investigación busca aportar evidencia académica y práctica sobre la pertinencia del NIST CSF como marco de referencia para fortalecer la ciberseguridad en entidades públicas del Estado peruano.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la situación problemática

A nivel mundial, la ciberseguridad se ha convertido en una de las principales preocupaciones de las instituciones y gobiernos, debido a la creciente digitalización de las actividades y a la transformación tecnológica en sectores clave, como el gubernamental. En el contexto de la SUNARP, el problema social se centra en la confianza de los usuarios hacia los servicios no privados y en la protección de sus datos, aspectos fundamentales para garantizar la seguridad jurídica y la continuidad de los servicios registrales (Flores Callejas *et al.*, 2021).

La ausencia de un sistema de ciberseguridad sólido en la Oficina de Tecnologías de la Información (OTI) pone en riesgo la integridad de los registros nacionales, exponiendo a la institución a la pérdida de información sensible y a la disminución de la confianza pública. En este sentido, cualquier vulnerabilidad en la protección de los datos podría afectar negativamente la relación entre el Estado y los usuarios de los servicios registrales.

De acuerdo con la estructura orgánica de la SUNARP, la OTI forma parte de la Administración Interna. Según lo establecido en el artículo N.° 46, dicha oficina es responsable de planificar, dirigir, diseñar, implementar y mantener la operatividad de los sistemas de información, garantizando la protección, disponibilidad y confidencialidad de los datos institucionales. No obstante, si bien la OTI establece los lineamientos, políticas y estándares tecnológicos para todas las zonas registrales de la SUNARP, la UTI de la Zona Registral N.° X – Sede Cusco presenta limitaciones en la gestión operativa de vulnerabilidades y en la evaluación de riesgos cibernéticos. Esta situación constituye el objeto de estudio de la presente investigación y evidencia la necesidad de fortalecer los mecanismos de protección de los activos tecnológicos locales.

En la UTI de la Zona Registral N.° X – Sede Cusco se ha identificado la necesidad de fortalecer los procesos de identificación de vulnerabilidades en activos tecnológicos clave, tales como estabilizadores, impresoras de tinta a color, *Central Processing Unit* (CPU), computadoras, routers y switches. Esta situación incrementa la exposición de la infraestructura local de

hardware y red a riesgos de seguridad que podrían afectar la disponibilidad, integridad y confidencialidad de la información institucional. Asimismo, la deficiente evaluación y gestión de estas vulnerabilidades, sumada a la inexistencia de un inventario actualizado de los activos críticos, dificulta la adecuada administración de los riesgos. Esta situación impide la priorización eficiente de las vulnerabilidades, generando una estrategia predominantemente reactiva frente a las amenazas, en lugar de una respuesta preventiva y proactiva.

A nivel operativo, la UTI de la Zona Registral N.° X – Sede Cusco no cuenta con un enfoque formalmente estructurado para la identificación, mitigación y priorización de vulnerabilidades alineado con marcos internacionales de ciberseguridad. Aunque la OTI establece lineamientos generales para toda la institución, la gestión local de los activos tecnológicos requiere mecanismos que permitan una mejor evaluación, tratamiento y seguimiento de los riesgos asociados a las vulnerabilidades identificadas. La ausencia de un diagnóstico detallado del modelo de gestión de vulnerabilidades, la inexistencia de un sistema claro de priorización y la falta de un modelo de capacitación adecuado para el personal en la detección temprana de vulnerabilidades contribuyen a incrementar la exposición del sistema a amenazas cibernéticas.

Adicionalmente, en la UTI de la Zona Registral N.° X – Sede Cusco no se dispone de un modelo conceptual de monitoreo que permita evaluar de manera continua la efectividad de las estrategias de mitigación implementadas y de las acciones de respuesta ante incidentes de seguridad, limitando la capacidad de mejora continua frente a nuevas amenazas cibernéticas. La falta de un plan definido para identificar y priorizar los servicios críticos de *hardware* y red agrava aún más la situación, poniendo en riesgo la continuidad operativa de la SUNARP. Sin un diagnóstico exhaustivo que permita abordar de manera integral estas áreas clave, la UTI de la Zona Registral N.° X – Sede Cusco continúa expuesta a riesgos que podrían comprometer la seguridad de los activos tecnológicos, la protección de la información sensible y la continuidad de los servicios registrales. Asimismo, esta situación dificulta la adecuada gestión de incidentes de ciberseguridad en el ámbito local y limita el cumplimiento efectivo de los lineamientos establecidos por la OTI para toda la institución.

Es importante precisar el origen metodológico de los problemas y objetivos específicos de esta investigación. Estos surgieron, en primer lugar, de un diagnóstico situacional preliminar

realizado en la UTI de SUNARP – Sede Cusco, mediante entrevistas con el personal técnico y revisión documental de inventarios, bitácoras de incidentes y reportes históricos de red, que evidenció brechas concretas en la gestión de activos, la detección de fallas y la capacidad de respuesta del personal. Posteriormente, estos hallazgos preliminares se organizaron y formularon como problemas y objetivos específicos siguiendo la estructura de las cinco funciones del NIST CSF (Identificar, Proteger, Detectar, Responder y Recuperar), con el fin de operacionalizar el diagnóstico dentro de un marco reconocido y comparable con los antecedentes revisados en el capítulo II. En consecuencia, las necesidades de investigación tienen origen empírico en la realidad institucional, mientras que su estructuración responde a la lógica funcional del marco NIST CSF adoptado como referente metodológico.

1.2 Formulación del problema

1.2.1 Problema general

¿Cuál es el impacto de adaptar e implementar un modelo basado en el NIST CSF sobre los indicadores de gestión de vulnerabilidades en la UTI de SUNARP?

1.2.2 Problemas específicos

- ¿Cuáles son las deficiencias en la gestión de vulnerabilidades en la UTI de SUNARP?
- ¿Qué criterios del NIST CSF son más relevantes para fortalecer la seguridad en la gestión de vulnerabilidades en SUNARP?
- ¿De qué manera se puede optimizar la identificación, priorización y mitigación de vulnerabilidades en la UTI de SUNARP?
- ¿Cómo puede contribuir el modelo propuesto a la capacitación del personal en la identificación temprana de vulnerabilidades?
- ¿Qué mecanismos debe incluir el modelo para garantizar la recuperación eficiente de los servicios críticos en SUNARP?

1.3 Justificación de la investigación

El fortalecimiento de la ciberseguridad en la UTI de SUNARP resulta indispensable frente al incremento de amenazas cibernéticas que comprometen la integridad, disponibilidad y confidencialidad de los activos informáticos institucionales. La gestión actual de vulnerabilidades presenta limitaciones relacionadas con inventarios desactualizados, deficiencias en la evaluación de riesgos, ausencia de controles estructurados y exposición a accesos no autorizados, lo que incrementa significativamente el riesgo operativo y la probabilidad de incidentes que afecten los servicios registrales.

En este contexto, abordar la ciberseguridad desde un enfoque integral que combine el NIST CSF y la norma ISO/IEC 27001 de manera complementaria se convierte en una necesidad estratégica. La adopción del ciclo de mejora continua PDCA permite estructurar un modelo dinámico que incorpore las fases de diagnóstico, implementación, verificación y mejora continua. Las fases de *Plan* (Planificar) y *Check* (Verificar) facilitan la evaluación sistemática de la madurez de los controles y del estado real de las vulnerabilidades, mientras que las fases de *Do* (Hacer) y *Act* (Actuar) permiten aplicar soluciones concretas y optimizarlas conforme a los resultados obtenidos.

Asimismo, la incorporación del NIST CSF proporciona una estructura reconocida internacionalmente para la identificación, evaluación, mitigación y seguimiento de vulnerabilidades en activos de *hardware* y redes. Su aplicación en la Zona Registral N.° X permitirá establecer un sistema de gestión de riesgos alineado con estándares globales, fortaleciendo la protección de los servicios críticos y contribuyendo al cumplimiento de los objetivos institucionales de seguridad jurídica y continuidad operativa.

La implementación de un modelo basado en el NIST CSF no solo mejora la capacidad técnica de protección frente a incidentes de ciberseguridad, sino que también fomenta una cultura organizacional orientada a la seguridad de la información. Esto contribuye a incrementar la confianza de los usuarios, reducir los errores humanos, mejorar la detección temprana de amenazas y permitir que SUNARP se adapte de manera oportuna a nuevos escenarios de riesgo. En conjunto, estos beneficios respaldan la pertinencia y necesidad de la investigación,

justificando la propuesta como una estrategia clave para fortalecer la gestión de vulnerabilidades en la UTI.

1.4 Objetivos de la investigación

1.4.1 Objetivo general

Adaptar e implementar un modelo de ciberseguridad basado en el NIST CSF para fortalecer la gestión de vulnerabilidades y medir su impacto en la UTI de SUNARP.

1.4.2 Objetivos específicos

- Diagnosticar el estado actual de la gestión de vulnerabilidades en la UTI de SUNARP.
- Identificar los criterios clave del NIST CSF aplicables a la gestión de vulnerabilidades en SUNARP.
- Diseñar un esquema de priorización de vulnerabilidades que integre los criterios del NIST CSF.
- Proponer estrategias de capacitación orientadas a la identificación temprana de vulnerabilidades.
- Definir mecanismos de recuperación para los servicios críticos de SUNARP basados en el NIST CSF.

1.5 Delimitación de la investigación

- **Ámbito de estudio:** La presente investigación se desarrolla en la UTI de la Zona Registral N.° X – SUNARP, Sede Cusco, ubicada en la avenida Manco Inca N.° 210, donde se evidencia una creciente exposición a riesgos cibernéticos derivados de la digitalización de los procesos y de una gestión insuficiente de los activos tecnológicos. Si bien la OTI a nivel nacional establece los lineamientos institucionales en materia de tecnologías de la información y ciberseguridad, el estudio se delimita al ámbito operativo de la UTI local.

- **Delimitación temporal:** El estudio se desarrolló durante el periodo comprendido entre mayo y diciembre de 2025, lapso que comprende el diagnóstico inicial, el diseño del modelo, la ejecución del piloto de capacitación y la evaluación de resultados. Este periodo delimita el alcance de una evaluación exhaustiva y longitudinal de los procesos de ciberseguridad, que queda como línea de investigación futura.

- **Alcance:** La investigación tiene como alcance el diseño de un modelo de ciberseguridad para la gestión de vulnerabilidades basado en el NIST CSF (versión 1.1) y en los controles pertinentes de la norma ISO/IEC 27001:2022, así como su validación mediante una prueba piloto en un entorno controlado y la capacitación dirigida al personal técnico de la UTI. La propuesta incorpora los lineamientos del marco referidos a la gestión operativa de vulnerabilidades; su aplicación se realizó únicamente en dicho entorno controlado, con el propósito de evaluar su pertinencia, funcionalidad y aplicabilidad dentro de la UTI, sin que ello represente una implementación operativa a nivel institucional ni la evaluación de un Sistema de Gestión de Seguridad de la Información (SGSI) completo.

- **Limitaciones:** El acceso a la información técnica y a la infraestructura tecnológica estuvo sujeto a las autorizaciones institucionales correspondientes (Anexo H.1), lo cual pudo restringir la profundidad del diagnóstico y de las recomendaciones formuladas. En consecuencia, los resultados obtenidos son aplicables únicamente a la UTI de SUNARP – Sede Cusco y no pueden generalizarse a otras dependencias de la institución sin un análisis posterior. Asimismo, aunque el modelo contempla un programa integral de capacitación para toda la organización, en esta investigación se ejecutó una prueba piloto de capacitación dirigida a un grupo seleccionado del personal técnico de la UTI, por lo que los resultados obtenidos corresponden únicamente al entorno controlado definido para el estudio y no representan una implementación institucional completa.

CAPÍTULO II

MARCO TEÓRICO CONCEPTUAL

El presente capítulo desarrolla el marco teórico y conceptual que sustenta la propuesta de fortalecimiento de la ciberseguridad en la SUNARP, considerando su rol estratégico en la administración y protección de información registral de alcance nacional. Para ello, se analizan antecedentes internacionales y nacionales relacionados con la implementación de marcos y estándares de ciberseguridad, destacando el NIST CSF como una herramienta flexible y adecuada para organizaciones públicas. Asimismo, se abordan los conceptos fundamentales de ciberseguridad, gestión de vulnerabilidades, activos de información y tratamiento de riesgos, integrándolos con la metodología de mejora continua PDCA, con el fin de proporcionar una base teórica sólida que permita garantizar la confidencialidad, integridad y disponibilidad de la información registral que administra la SUNARP, en concordancia con sus objetivos institucionales y el marco normativo vigente.

2.1 Antecedentes

2.1.1 Antecedentes internacionales

Por su parte, Alshaikh (2020a) realizó el estudio "*Cybersecurity Risk Management Framework for Government Information Systems Based on NIST CSF*", enfocado en el fortalecimiento de la gestión de riesgos y vulnerabilidades en unidades de tecnologías de la información del sector público. La investigación evidenció que más del 60 % de las vulnerabilidades detectadas estaban relacionadas con deficiencias en capacitación del personal y ausencia de monitoreo continuo. Para ello, se diseñó un modelo basado en las cinco funciones del NIST CSF, complementado con controles de la norma ISO/IEC 27001 y procesos de evaluación periódica bajo el enfoque PDCA. Los resultados mostraron mejoras significativas en la identificación de vulnerabilidades, reducción de los tiempos de respuesta ante incidentes y estandarización de los procesos de recuperación de servicios críticos. Se concluyó que la adopción de un marco internacional integrado resulta fundamental para garantizar la seguridad, disponibilidad e integridad

de la información en instituciones gubernamentales.

Asimismo, Behl (2021) desarrolló la investigación "*Integrating National Institute of Standards and Technology (NIST) Cybersecurity Framework and ISO/IEC 27001 for Vulnerability Management in Public Sector Organizations*", cuyo objetivo fue diseñar un modelo híbrido de ciberseguridad orientado a la gestión de vulnerabilidades en entidades gubernamentales de América del Norte. El estudio identificó que la principal debilidad en las instituciones públicas era la falta de un inventario actualizado de activos, así como la dependencia de proveedores externos para la gestión de incidentes. Mediante la integración del NIST CSF con los controles de la norma ISO/IEC 27001, estructurada bajo el ciclo de mejora continua PDCA, se logró priorizar riesgos en función del impacto y la probabilidad, reduciendo en un 40 % las vulnerabilidades críticas no mitigadas. Se concluyó que la combinación de ambos marcos permitió mejorar la detección temprana de incidentes, optimizar los tiempos de respuesta y fortalecer la resiliencia operativa, destacando su aplicabilidad en organizaciones públicas con infraestructuras tecnológicas heterogéneas.

De igual manera, Yánez Intriago (2022) desarrolló la investigación "Implementación del NIST CSF en el Instituto Superior Tecnológico Sucre", en la cual aplicó el marco de ciberseguridad NIST CSF con el fin de optimizar las prácticas de seguridad informática y proteger la infraestructura crítica de dicha institución. El principal desafío identificado fue la ausencia de una estructura formal para la gestión de riesgos, pese a que ya existían medidas básicas de protección. Para ello, se emplearon las hojas de ruta del NIST CSF basadas en sus cinco funciones esenciales: Identificar, Proteger, Detectar, Responder y Recuperar. En la fase inicial se evaluó la situación actual y se elaboró un plan de intervención para minimizar los riesgos. Tras la implementación, la función Proteger alcanzó un 70.73 %, siendo la de mayor avance; la función Identificar obtuvo 66.32 %; mientras que Detectar, Responder y Recuperar alcanzaron 59.17 %, evidenciando la necesidad de mejorar la detección temprana de incidentes y la capacidad de respuesta. El investigador concluyó que la adopción del NIST CSF permitió mejorar la seguridad y gestión de riesgos, aunque aún se requiere continuar con la implementación de contramedidas para alcanzar un nivel óptimo de ciberseguridad.

2.1.2 Antecedentes nacionales

Calderon Aquiño (2022), en su investigación titulada "Modelo de Sistema de Ciberseguridad para la Gestión de Riesgo de una Empresa de Matizados de Pintura de Lima, 2022", desarrollada en una empresa dedicada a los matizados de pintura en Lima, tuvo como objetivo mejorar la gestión de riesgos cibernéticos mediante la implementación de un modelo de ciberseguridad basado en el estándar ISO 27001. El estudio, de enfoque aplicado y diseño preexperimental, evaluó 14 activos informáticos empleando la metodología del Sistema de Gestión de la Información (SGI) y la Norma ISO 27001, utilizando pruebas estadísticas T-Student y Wilcoxon para comparar los resultados pre y post implementación. Los hallazgos evidenciaron un incremento en la protección de activos del 7.88 % al 13.53 %, así como un aumento del nivel de riesgo del 9.5 % al 18.73 %. Además, la aplicación de controles de seguridad pasó de 89.38 % a 99.12 %. Se concluyó que el modelo basado en ISO 27001 fue efectivo para fortalecer la seguridad de los datos y disminuir riesgos cibernéticos, subrayando la importancia de contar con un sistema robusto de ciberseguridad y de mantener una capacitación continua ante nuevas amenazas.

Ramirez Vargas y Pereda Otero (2023) llevaron a cabo la investigación "Propuesta de implementación de un modelo de ciberseguridad para la defensa contra ataques cibernéticos en la Oficina de Estadística e Informática del Instituto Nacional de Salud del Niño (INSN) basada en NIST CSF v1.1". El estudio se desarrolló en una institución que maneja información crítica relacionada con la salud infantil y que enfrentaba vulnerabilidades en su infraestructura tecnológica, controles insuficientes ante amenazas y la ausencia de una política unificada de gestión de incidentes. Para solucionar estas deficiencias, se adoptó el NIST CSF v1.1 mediante cinco fases: formulación de la política de ciberseguridad, análisis de riesgos, evaluación de brechas, desarrollo del plan de implementación y evaluación continua. El modelo permitió mejorar la resiliencia ante ciberataques, fortalecer la protección de datos sensibles y desarrollar una cultura organizacional orientada a la seguridad. Los autores concluyeron que implementar el NIST CSF v1.1 resultó ser una estrategia efectiva para fortalecer la infraestructura tecnológica del INSN, aunque señalaron que su implementación requiere recursos significativos, recomendándose una adopción gradual especialmente en instituciones con presupuestos limitados.

Asimismo, Cordova Facundo y Rodriguez Polo (2023), en su investigación titulada "Modelo de ciberseguridad para mejorar la seguridad de la información, basada en NIST CSF en JRM Solutions Perú, 2023", aplicaron dicho modelo en una empresa que se encontraba en proceso de digitalización y que no contaba con medidas avanzadas de protección, políticas ni planes de contingencia. Mediante una evaluación de marcos de trabajo como *Project Management Body of Knowledge* (PMBOK) y el ciclo PDCA, utilizando la escala de Likert, se seleccionó el ciclo PDCA combinado con el NIST CSF como la alternativa más adecuada. Los resultados demostraron mejoras significativas en seguridad: 86 % en disponibilidad de la información, 73 % en confiabilidad y un índice de 0.756 en confidencialidad, además de un 93 % de aceptación por parte de los colaboradores. Se concluyó que el modelo basado en NIST CSF fortaleció de manera considerable la integridad, disponibilidad y confidencialidad de la información, destacando la importancia de la formación continua del personal.

De igual forma, Tomaylla Castillo y Balbin Balbin (2024) realizaron la investigación "Propuesta de Implementación del *Framework* NIST CSF 1.1 para una entidad gubernamental", cuyo objetivo fue optimizar los procesos de administración del personal en entidades públicas. No obstante, un incremento en la demanda de acceso y consulta de datos generó problemas de seguridad y disponibilidad, especialmente en la Plataforma de Interoperabilidad del Estado (PIDE). La falta de un marco estructurado de ciberseguridad ocasionaba vulnerabilidades como accesos no autorizados y riesgos a la confidencialidad e integridad de la información. Tras comparar diversos *framework*, se determinó que el NIST CSF 1.1 era el más adecuado debido a su flexibilidad y capacidad de adaptación. Su implementación permitió fortalecer la seguridad de los datos, mejorar la gestión de amenazas y garantizar la disponibilidad, confidencialidad e integridad de la información, destacando además la importancia de la capacitación y del monitoreo permanente.

2.2 Bases Teóricas

2.2.1 Ciberseguridad

En términos generales, la ciberseguridad se refiere al conjunto de medidas y tácticas implementadas para resguardar la información dentro del ciberespacio y en los sistemas informáticos interconectados, así como la infraestructura que los sustenta. Su propósito principal es garantizar la seguridad de las interacciones entre individuos y computadoras, protegiendo tanto la información como los canales de comunicación utilizados. Esto incluye prevenir accesos no autorizados, identificar amenazas y responder ante incidentes, con el fin de establecer un entorno digital seguro (Jara Fuentealba y Jorquera Cruz, 2021).

Los ataques cibernéticos se han vuelto tan frecuentes que ahora se considera una cuestión de cuándo ocurrirán, en lugar de si sucederán. Por ello, resulta fundamental que las organizaciones refuercen sus medidas de protección frente a los ciberdelincuentes, quienes buscan obtener información valiosa con fines personales. Actualmente, muchos bancos y otras entidades financieras desarrollan e implementan sistemas de seguridad avanzados para minimizar el riesgo de fraudes y amenazas cibernéticas, protegiendo así sus activos y la estabilidad institucional (Demirkan *et al.*, 2020).

Desde una perspectiva más amplia, la ciberseguridad puede entenderse como la disciplina que articula procesos, tecnologías y personas para preservar tres atributos fundamentales de la información: confidencialidad, integridad y disponibilidad. En el contexto del sector público, esta disciplina adquiere una dimensión adicional de responsabilidad institucional, en tanto la información gestionada —como los registros públicos administrados por SUNARP— constituye un bien de interés colectivo cuya afectación no solo genera pérdidas económicas, sino que compromete la confianza ciudadana en la administración estatal (Jara Fuentealba y Jorquera Cruz, 2021). Por ello, los marcos de ciberseguridad aplicados a entidades gubernamentales, como el NIST CSF, no se limitan a la protección técnica de la infraestructura, sino que incorporan una lógica de gestión continua del riesgo que vincula la gobernanza institucional con la operación técnica diaria.

2.2.2 NIST CSF

Este marco proporciona pautas a la industria, organismos del Estado y otras entidades para administrar los riesgos de ciberseguridad. Presenta una clasificación general de los resultados de seguridad cibernética, útil para cualquier organización, sin importar su tamaño, sector o nivel de desarrollo, permitiéndole entender, evaluar, priorizar y comunicar sus esfuerzos en este campo. El NIST CSF no indica métodos específicos para alcanzar estos objetivos, sino que vincula a recursos en línea que ofrecen orientación adicional sobre prácticas y controles que pueden ser implementados (NIST CSWP, 2024).

Estructura del NIST CSF

Almagro (2019) menciona que el NIST CSF tiene como objetivo guiar los esfuerzos de ciberseguridad a través de un marco que se compone de tres elementos clave: a) Núcleo del marco, b) Perfil del marco y c) Niveles de implementación. A continuación, se detallan los componentes:

Figura 1

Componentes del NIST CSF (versión 1.1): Identify, Protect, Detect, Respond y Recover

Nota. De "*NIST releases version 1.1 of its popular Cybersecurity Framework*", por Hanacek (2018).

a) *Framework Core*: Sostiene que el *Core* es un grupo de actividades y objetivos deseados en el ámbito de la ciberseguridad, organizados en categorías y está diseñado para ser fácil de usar y además funciona como un puente de comunicación entre equipos multidisciplinarios, empleando un lenguaje sencillo y accesible. El *Core* se organiza en 3 categorías: Funciones, Categorías y Subcategorías como se visualiza en la Tabla 1 Estas incluyen 5 funciones principales como se observa en la Figura 1: Identificar, Proteger, Detectar, Responder y Recuperar, que se explican de la siguiente manera:

- Identificar: La función de identificación permite a las organizaciones gestionar de forma más efectiva los riesgos de ciberseguridad que afectan a sus sistemas, personas, datos y capacidades. Al comprender el contexto del negocio y los recursos clave, pueden organizar sus esfuerzos de manera prioritaria. Esto asegura que su enfoque para la gestión de riesgos esté alineado con los objetivos empresariales, abordando primero las vulnerabilidades más críticas.
- Proteger: Se detallan las acciones de protección más efectivas para garantizar el funcionamiento ininterrumpido de los servicios en las infraestructuras tecnológicas esenciales. Esta función también abarca la capacidad de reducir las consecuencias de posibles eventos relacionados con la ciberseguridad.
- Detectar: Esta fase está dirigida al monitoreo constante con el fin de prevenir accesos no autorizados a las redes y sistemas de la empresa. Incluye la ejecución de auditorías tecnológicas periódicas y revisiones exhaustivas para identificar cualquier evento irregular. También se establece un protocolo de respuesta rápida frente a incidentes, lo que permite abordar las amenazas de manera eficiente y salvaguardar tanto la seguridad como la integridad de la información.
- Responder: Las categorías de la función de respuesta garantizan una reacción adecuada ante ciberataques y otros incidentes de ciberseguridad. Estas categorías incluyen la planificación de la respuesta, que establece protocolos claros; las comunicaciones, que aseguran una información fluida entre los equipos; el análisis, que evalúa el impacto y la naturaleza del incidente; la mitigación, que implementa ac-

ciones para reducir el daño; y las mejoras, que buscan optimizar los procesos y fortalecer la seguridad en el futuro.

- Recuperar: Restaura los servicios y sistemas afectados por incidentes de seguridad y reanudar las operaciones normales.

Tabla 1
Funciones y Categorías del NIST CSF v1.1

Función	**Categoría (Código)**	**Descripción**
Identificar	Gestión de activos (ID.AM)	Inventario y gestión de activos de *hardware*, *software*, datos y sistemas.
	Entorno empresarial (ID.BE)	Comprensión del contexto empresarial y su rol en la gestión del riesgo.
	Gobernanza (ID.GV)	Políticas, procedimientos y procesos para gobernanza y gestión de riesgos.
	Evaluación de riesgos (ID.RA)	Identificación y evaluación de riesgos para los activos organizacionales.
	Estrategia de gestión de riesgos (ID.RM)	Definición de apetito de riesgo y toma de decisiones basadas en riesgo.
	Gestión de la cadena de suministro (ID.SC)	Identificación y evaluación de riesgos asociados a terceros y proveedores.
Proteger	Control de accesos (PR.AC)	Gestión de identidades, autenticación y acceso autorizado.
	Concienciación y formación (PR.AT)	Capacitación en seguridad cibernética para empleados y partes interesadas.
	Seguridad de los datos (PR.DS)	Protección de datos conforme a políticas de seguridad y privacidad.
	Procesos y procedimientos de protección (PR.IP)	Implementación de políticas de seguridad, mantenimiento y mejora continua.

Continúa en la siguiente página

Función	Categoría (Código)	Descripción
	Mantenimiento (PR.MA)	Mantenimiento de tecnologías y sistemas según lo planificado.
	Tecnología de protección (PR.PT)	Implementación de tecnologías para proteger los activos.
Detectar	Anomalías y eventos (DE.AE)	Detección de actividad anómala y comprensión de su impacto potencial.
	Monitoreo continuo de seguridad (DE.CM)	Supervisión activa de eventos para detectar incidentes de ciberseguridad.
	Procesos de detección (DE.DP)	Procedimientos y herramientas establecidos para detectar eventos.
Responder	Planificación de la respuesta (RS.RP)	Planes de respuesta ante incidentes implementados y actualizados.
	Comunicaciones (RS.CO)	Coordinación interna y externa durante y después de un incidente.
	Análisis (RS.AN)	Evaluación de incidentes para comprender su naturaleza e impacto.
	Mitigación (RS.MI)	Contención y eliminación de incidentes de ciberseguridad.
	Mejoras (RS.IM)	Incorporación de lecciones aprendidas y mejoras post-incidente.
Recuperar	Planificación de recuperación (RC.RP)	Implementación de planes de recuperación después de incidentes.
	Mejoras (RC.IM)	Evaluación y mejora continua de los procesos de recuperación.
	Comunicaciones (RC.CO)	Coordinación con partes interesadas durante la fase de recuperación.

b) Perfil del marco: El perfil proporciona una visión clara del estado actual de las actividades

de ciberseguridad de la organización, así como del estado objetivo al que aspira alcanzar. Este perfil está orientado hacia funciones, categorías y subcategorías, además de tener en cuenta los requerimientos comerciales y los recursos de la organización. Asimismo, ayuda a las organizaciones a comprender su situación actual en términos de seguridad, permitiéndoles realizar una revisión objetiva y exhaustiva de toda la infraestructura de Tecnologías de la Información (TI). Esto no solo facilita la identificación de áreas de mejora, sino que también establece un camino claro para alinear las estrategias de ciberseguridad con los objetivos comerciales y fortalecer la protección de los activos (Almagro, 2019).

c) Niveles de implementación Estos niveles ofrecen un esquema para comprender cómo una organización percibe y aborda el riesgo en ciberseguridad. Miden el grado en que las prácticas de gestión de riesgos se alinean con las características del marco, que van desde un enfoque inicial o parcial (*Tier 1*) hasta uno completamente adaptativo (*Tier 4*). Esta clasificación muestra una evolución, pasando de respuestas reactivas y poco estructuradas a enfoques más dinámicos y basados en un análisis de riesgos más sólido. Al elegir un nivel, la organización debe tener en cuenta sus prácticas actuales, el entorno de amenazas, los requisitos legales y normativos, sus metas comerciales y las limitaciones internas, lo que contribuye a una gestión de riesgos

Justificación de la selección de las versiones normativas

La presente investigación se sustenta en el NIST CSF, versión 1.1 (National Institute of Standards and Technology, 2018), y en la norma ISO/IEC 27001:2022 (ISO/IEC, 2022). La selección de la versión 1.1 del NIST CSF, en lugar de la versión 2.0 publicada en 2024 (NIST CSWP, 2024), obedece a tres razones. Primero, la versión 1.1 constituye el marco de referencia con mayor cantidad de antecedentes documentados de aplicación en el sector público, incluyendo experiencias nacionales e internacionales comparables (Alshaikh (2020a); Tomaylla Castillo y Balbin Balbin (2024); Yánez Intriago (2022)), lo que permitió sustentar el diseño del modelo sobre casos ya validados. Segundo, el alcance definido en el numeral 1.5 circunscribe el estudio a la gestión operativa de vulnerabilidades dentro de la UTI, y no a la gobernanza institucional

integral de la ciberseguridad; por ello, la función Gobernar (*Govern*), incorporada como sexta función en la versión 2.0, excede el ámbito delimitado para esta investigación. Tercero, los aspectos de gobernanza documental y gestión de riesgos que en el NIST CSF 2.0 asumiría la función Gobernar se cubren, dentro del alcance de la UTI, mediante los controles de gestión de la norma ISO/IEC 27001:2022, evitando una duplicidad funcional entre ambos marcos.

Respecto a la norma ISO/IEC 27001, se utilizó específicamente la versión 2022 —vigente al momento de la ejecución del estudio (mayo-diciembre de 2025) y que reemplaza a la edición de 2013— por ser la versión activa y de referencia para los sistemas de gestión de seguridad de la información en el Perú, y por su compatibilidad con los lineamientos ya establecidos en el instructivo institucional de tratamiento de riesgos de SUNARP (SUNARP, 2021).

2.2.3 Activos de información

Los activos de TI son cruciales para la protección de los datos y se dividen en categorías como Datos, *Software*, *Hardware*, Redes, Soporte, Instalaciones, Personal y Servicios, siendo los datos los más valiosos. Para protegerlos, es necesario implementar estrategias de seguridad que eviten su pérdida, daño, divulgación o uso indebido, utilizando herramientas como encriptación, controles de acceso y capacitación del personal. Esto asegura la integridad, confidencialidad y disponibilidad de los datos. Además, una gestión adecuada de estos activos es esencial para cumplir con regulaciones y estándares de seguridad, lo que refuerza la resiliencia organizacional (Peñafiel, 2021).

2.2.4 Gestión de vulnerabilidades

Según Saeckel (2023), para asegurar la infraestructura tecnológica en la gestión de vulnerabilidades, es fundamental realizar escaneos regulares, comprobar los controles de la red y llevar a cabo pruebas de penetración en todos los sistemas con el fin de identificar posibles vulnerabilidades técnicas. Además, subraya la importancia de identificar las amenazas a la seguridad informática y la protección general de la información. Las vulnerabilidades técnicas deben ser clasificadas según su nivel de gravedad y abordadas de manera adecuada. La gestión de vulnerabilidades también implica evaluar el riesgo residual de aquellas vulnerabilidades que

persisten y aceptar el riesgo, siempre en consonancia con los principios establecidos. Por otro lado, Méndez Gálvez (2020) menciona que, conforme a la norma ISO/IEC 27002: 2005, una vulnerabilidad se entiende como una debilidad de un activo de información, que puede ser explotada por una o más amenazas, afectando así la integridad de los principios de seguridad. Estas vulnerabilidades, que son inherentes a los propios activos, pueden ser de tipo tecnológico, humano o procesal.

La gestión de vulnerabilidades constituye, además, un proceso cíclico y no un evento puntual: comprende la identificación sistemática de debilidades (mediante escaneos e inventarios), su clasificación según criticidad e impacto potencial, la remediación o mitigación de acuerdo con los recursos disponibles, y la verificación posterior de que las medidas aplicadas efectivamente cierran la brecha detectada (Scarfone y Mell, 2012). Esta naturaleza cíclica es la que permite integrar la gestión de vulnerabilidades con la metodología PDCA descrita en el numeral 2.2.5, en la medida en que cada fase del proceso de gestión de vulnerabilidades puede asociarse a una fase del ciclo de mejora continua.

2.2.5 Metodología de mejora continua: PDCA

La norma ISO 27001 se fundamenta en el ciclo PDCA como se observa en la Figura 2, también conocido como el ciclo de *Deming*, que impulsa la mejora continua tanto en el sistema de gestión como en los procesos individuales (NQA, 2024). De acuerdo con Betancourt (2018), este enfoque estructurado facilita la mejora constante de los procesos, productos y servicios dentro de una organización. El ciclo es iterativo, lo que significa que, una vez que se completa una ronda, la fase de planificación se reinicia, favoreciendo un perfeccionamiento constante. Por su parte, Santiago (2018) destaca que el ciclo PDCA es una metodología orientada a la mejora continua que incluye las fases de planificar, hacer, verificar y actuar.

Así mismo, Santiago (2018) indica que se le conoce también como “ciclo de control de calidad”, este método es ampliamente utilizado en control de calidad y mejora de procesos en varias industrias. A continuación, se detalla una descripción breve de cada fase:

- **Planificar:** Identificar problemas o áreas de mejora, estableciendo metas y objetivos claros. También es fundamental desarrollar un plan detallado que trace el camino hacia el

logro de estas metas, considerando estrategias y acciones específicas que guíen el proceso de la implementación.

- **Hacer:** Implementar el plan desarrollado en la fase de planificación, ejecutando las acciones y actividades previstas. Por último, es importante recopilar datos y desarrollar un seguimiento continuo durante la ejecución para evaluar el progreso y hacer ajustes en caso de ser necesario.

- **Verificar:** Verificar los resultados que se hayan obtenido de acuerdo a las metas establecidas en la fase de planificación. Evaluar la eficacia y utilidad de las acciones que se han implementado, y analizar los datos para determinar si se han logrado los resultados esperados. Este proceso de análisis permite identificar no solo los logros obtenidos, sino también áreas de mejora y oportunidades para optimizar futuras iniciativas. Además, fomenta una cultura de aprendizaje continuo dentro de la organización, asegurando que las lecciones aprendidas se integren en el plan.

- **Actuar:** Adoptar acciones correctivas y de mejora a partir de los resultados obtenidos en la fase de verificación. Cuando los objetivos han sido alcanzados, las buenas prácticas deben estandarizarse e incorporarse a los procesos institucionales; en caso contrario, se deben identificar las causas de las desviaciones y replantear las acciones necesarias. Esta fase permite consolidar el aprendizaje organizacional y reiniciar el ciclo con nuevos niveles de desempeño.

Figura 2
Plan de PDCA

Nota. Adaptado de "Ciclo de PDCA", por Gobierno Electrónico de Ecuador (s. f.). Recuperado de `https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/08/Ciclo-de-PDCA-1024x522.jpg`

2.2.6 Tratamiento de riesgos en SUNARP

La SUNARP establece que se debe realizar una evaluación anual de riesgos de seguridad, o bien cada vez que se presenten cambios en los activos de información. Además, las reuniones del equipo de trabajo relacionadas con la capacitación sobre el estudio de riesgos de protección de la información deben ser registradas en la lista de asistencia correspondiente.

2.2.7 Prueba t de Student para muestras relacionadas

La prueba t de Student para muestras relacionadas es una técnica estadística paramétrica utilizada para comparar las medias de dos mediciones realizadas sobre un mismo grupo de individuos. Su finalidad es determinar si las diferencias observadas entre las mediciones antes y después de una intervención son estadísticamente significativas, asumiendo que las diferencias siguen una distribución aproximadamente normal. Esta prueba es ampliamente empleada en investigaciones experimentales y cuasiexperimentales para evaluar el efecto de tratamientos o programas implementados (Triola, 2018), (Walpole *et al.*, 2012).

2.2.8 Prueba de Rangos con Signo de Wilcoxon

La prueba de Rangos con Signo de Wilcoxon es una técnica estadística no paramétrica utilizada para comparar dos mediciones relacionadas cuando no se cumple el supuesto de normalidad o cuando el tamaño de la muestra es reducido. Su procedimiento se basa en el análisis de los rangos asignados a las diferencias entre observaciones emparejadas, permitiendo determinar si existe un cambio significativo entre las mediciones realizadas antes y después de una intervención (Siegel y Castellan, 1995). Según Hernández Sampieri y Mendoza, esta prueba constituye una alternativa adecuada a las pruebas paramétricas en estudios aplicados con variables ordinales o muestras pequeñas (Hernández Sampieri y Mendoza Torres, 2018).

2.3 Marco conceptual

A diferencia de las bases teóricas desarrolladas en el numeral 2.2, que explican el sustento conceptual y el debate académico detrás de cada término, el presente marco conceptual reúne las definiciones operativas que se emplean de manera consistente a lo largo del desarrollo, los resultados y las conclusiones de esta investigación, con el fin de fijar un lenguaje común y evitar ambigüedades en el uso de términos técnicos afines.

2.3.1 Ciberseguridad

La ciberseguridad abarca un conjunto de prácticas y herramientas creadas para proteger la información que se genera y procesa en computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos (Lindemulder, 2024).

2.3.2 Vulnerabilidad

Las vulnerabilidades son fallos de seguridad vinculados a los activos de información de una organización (Argüezo Ramirez, 2019).

2.3.3 Activo

Se entiende por todos los recursos de TI, tanto tangibles como intangibles, que son esenciales o complementarios para alcanzar los objetivos empresariales, sin importar el formato, medio o presentación en que se generen, almacenen o utilicen (Falcon Fernández, 2021).

2.3.4 Riesgo

Se refiere a la probabilidad de que una amenaza se concrete sobre una vulnerabilidad de un activo informático, generando un impacto específico en la empresa (López Fernández, 2017).

2.3.5 Amenaza

Se entiende por amenaza a cualquier agente, circunstancia o evento con el potencial de explotar una vulnerabilidad y causar un impacto negativo sobre un activo de información, ya sea de origen humano (intencional o accidental), tecnológico o ambiental (López Fernández, 2017).

Para efectos de esta investigación, los términos anteriores se emplean de manera diferenciada: ’vulnerabilidad’ designa una debilidad latente en un activo; ’amenaza’ designa el agente o evento capaz de explotar dicha debilidad; ’riesgo’ designa la probabilidad de que una amenaza explote una vulnerabilidad y el impacto resultante; e ’incidente’ designa la materialización efectiva de un riesgo. El término ’brecha operativa’, usado en los capítulos 4 y 5, se reserva para diferencias observadas entre el estado actual de un proceso o control y el estado esperado según el NIST CSF, y no debe confundirse con ’vulnerabilidad’ técnica.

2.4 SUNARP

2.4.1 Nombre o razón social

La entidad receptora de la propuesta se denomina Superintendencia Nacional de los Registros Públicos (SUNARP), organismo público técnico, descentralizado y autónomo, adscrito al Sector Justicia del Perú.

2.4.2 Rubro

SUNARP opera en el rubro de los servicios registrales e institucionales, en cuanto a la inscripción y publicidad registral de actos, contratos, derechos y titularidades, contribuyendo directamente a la seguridad jurídica, mediante la gestión del Sistema Nacional de los Registros Públicos (SINARP).

2.4.3 SUNARP

SUNARP funge como ente rector del SINARP, encargándose de dictar políticas, normas técnico-registrales y de supervisar las inscripciones a nivel nacional, garantizando la coherencia, validez y publicidad de los registros públicos.

2.4.4 Ubicación Geográfica

Su sede institucional principal se encuentra en la Av. Primavera Nº 1878, Santiago de Surco, Lima 33, Perú. Adicionalmente, SUNARP posee una extensa red de Zonas y Oficinas Registrales a nivel nacional, lo cual asegura cobertura territorial y disponibilidad de sus servicios en diversas regiones del país.

2.4.5 Misión

La misión institucional de SUNARP se define como “inscribir y publicitar actos, contratos, derechos y titularidades de las personas de manera oportuna, inclusiva, transparente, predecible y eficiente”. En el ámbito del Sector Justicia, su visión más amplia apunta hacia un Perú donde primen el respeto a los derechos humanos, la cultura de la legalidad y la seguridad jurídica.

2.4.6 Visión

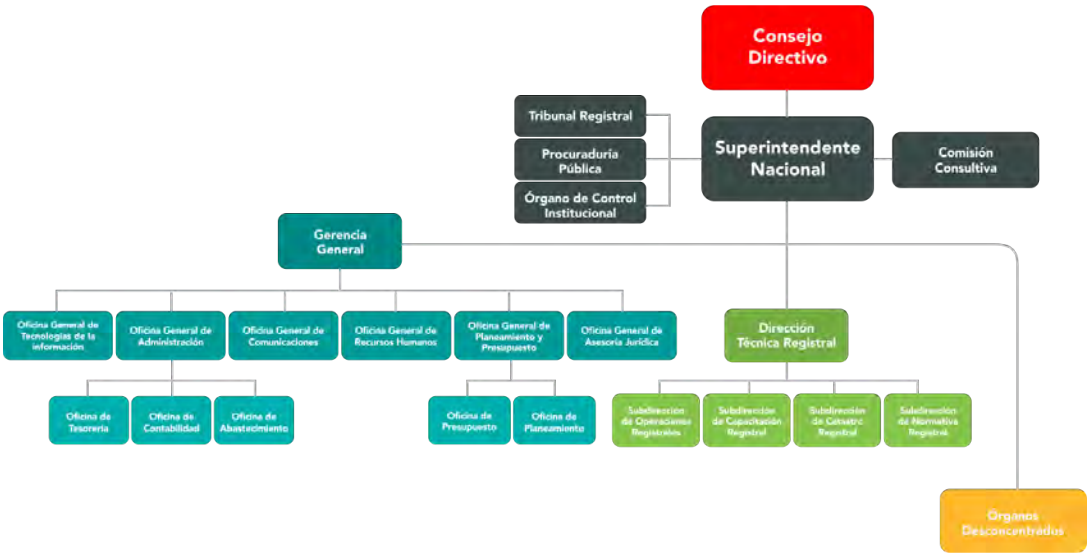
A nivel institucional, SUNARP orienta su visión hacia la prestación moderna y eficiente de sus servicios, en concordancia con los estándares del Sector Justicia y Derechos Humano.

En el caso de la Subdirección de Formación Registral, cuya misión específica es gestionar el conocimiento registral y fortalecer competencias del personal, su visión es “ser el referente

a nivel de Latinoamérica en la gestión del conocimiento y difusión del Derecho Registral".

2.4.7 *Organigrama*

Figura 3
Organigrama de SUNARP



Nota. Adaptado de "Organigrama - SUNARP", por la Superintendencia Nacional de los Registros Públicos. Recuperado de `https://www.sunarp.gob.pe/seccion/institucional/organigrama/index.html`

La estructura orgánica de SUNARP está compuesta por diversas instancias de dirección y coordinación como se muestra en la Figura 3. Entre ellas figuran el Superintendente Nacional, la Oficina de Auditoría Interna, la Secretaría General, el Tribunal Registral, las Gerencias (Administración y Finanzas; Informática; Registral; Legal; Presupuesto y Desarrollo; Catastro), además de la Escuela de Capacitación Registral y las Zonas Registrales distribuidas en todo el territorio nacional.

2.4.8 *Estructura organizacional de la gestión de tecnologías de la información*

La gestión de las tecnologías de la información en la SUNARP se desarrolla bajo un esquema centralizado de dirección y descentralizado de ejecución. A nivel institucional, la OTI es el órgano responsable de planificar, dirigir, diseñar, implementar y supervisar los sistemas

de información, la infraestructura tecnológica y los lineamientos relacionados con la seguridad de la información.

Entre sus funciones se encuentran la formulación de políticas, normas, procedimientos y estándares tecnológicos aplicables a todas las dependencias de la institución, así como la supervisión de su cumplimiento en las diferentes zonas registrales del país.

Por otro lado, las unidades de tecnologías de la información de cada zona registral son responsables de ejecutar operativamente dichos lineamientos, administrando la infraestructura tecnológica local, los activos informáticos, los servicios de red y las actividades de soporte técnico requeridas para garantizar la continuidad de los servicios institucionales.

En la Zona Registral N.° X, la UTI constituye la unidad encargada de gestionar la infraestructura tecnológica y aplicar los lineamientos establecidos por la OTI. En consecuencia, las actividades relacionadas con la identificación de vulnerabilidades, administración de activos tecnológicos, monitoreo de servicios y atención de incidentes de seguridad se desarrollan principalmente en el ámbito operativo de dicha unidad.

Por tal motivo, aunque la presente investigación toma como referencia los lineamientos institucionales definidos por la OTI, su alcance se circunscribe a la realidad operativa de la UTI de la Zona Registral N.° X – Sede Cusco, donde se analiza la gestión de vulnerabilidades y se propone la adaptación de un modelo basado en el NIST CSF.

2.4.9 Objetivos estratégicos

Según las Áreas Estratégicas de SUNARP, se identifican los siguientes objetivos:

- Consolidar a SUNARP como un sistema abierto, eficiente y eficaz en la garantía de la seguridad jurídica, reconociendo esta como un factor clave para el desarrollo nacional.
- En el ámbito institucional de Informática, evolucionar hacia una organización plenamente eficiente, moderna y democrática en cobertura, que sirva como modelo de gestión en el sector público peruano y latinoamericano.
- Desde la Subdirección de Formación Registral, fortalecer la competencia del personal registral, impulsando la excelencia en la difusión del derecho registral y su aplicación en

servicio al ciudadano.

2.4.10 Aspectos adicionales relevantes

- **Marco normativo y organización institucional:** SUNARP se constituyó legalmente mediante la Ley N° 26366 (1994) que creó el SINARP, y mediante la Resolución Suprema N° 135-2002-JUS, que aprobó su Estatuto Orgánico. Posteriormente, el Reglamento de Organización y Funciones (ROF) y el Manual de Organización y Funciones (MOF) consolidaron su funcionalidad operativa.

- **Ética y gobernanza institucional:** SUNARP cuenta con un Código de Ética aprobado mediante Resolución del Superintendente Nacional (N° 287-2002-SUNARP/SN), orientado a guiar la conducta del personal en beneficio del país y del usuario.

- **Canal digital de servicios:** SUNARP ha modernizado parte de sus procesos mediante plataformas digitales como el Servicio de Publicidad Registral en Línea (SPRL) y el Sistema de Intermediación Digital (SID), que permiten la consulta, reserva e inicio de procedimientos registrales de forma virtual, amplia y accesible.

CAPÍTULO III

METODOLOGÍA

3.1 Tipo de investigación

La presente investigación es de tipo descriptiva y aplicada. Es descriptiva porque se orienta a caracterizar y analizar detalladamente la situación actual de la gestión de vulnerabilidades en la UTI de la SUNARP, sede Cusco, así como a describir los componentes del modelo de ciberseguridad propuesto basado en el marco NIST CSF y los controles relacionados de la norma ISO/IEC 27001. Asimismo, es aplicada debido a que el modelo diseñado fue evaluado mediante un piloto en un entorno controlado, con la finalidad de comprobar su efectividad y aplicabilidad en un contexto real de trabajo institucional.

3.2 Enfoque de la investigación

La investigación presenta un **enfoque mixto (cualitativo-cuantitativo)**. Posee un fuerte componente *cualitativo* debido a que analiza la gestión de vulnerabilidades desde una perspectiva organizacional y procedimental, considerando la estructura de procesos de la UTI, las brechas normativas frente al marco NIST CSF y la percepción sociotécnica del personal.

De manera complementaria e integrada, se incorpora un enfoque *cuantitativo* de nivel descriptivo. Este componente es indispensable para establecer una línea base objetiva y evaluar la efectividad técnica del modelo a través de métricas e indicadores de rendimiento específicos, tales como *Mean Time to Repair* (MTTR), tasas porcentuales de cumplimiento de *Recovery Time Objective* (RTO), volumen de incidentes reportados en infraestructura y el rendimiento académico del personal técnico en las evaluaciones de ciberseguridad. La combinación de ambos enfoques permite mitigar los sesgos de la medición puramente subjetiva y dotar a las conclusiones de un sustento técnico verificable.

3.3 Alcance de la investigación

El alcance de la investigación es propositivo y evaluativo. Es propositivo porque desarrolla un Modelo de Ciberseguridad orientado a fortalecer la gestión de vulnerabilidades en la UTI de SUNARP, tomando como referencia el marco NIST CSF y controles específicos de la ISO/IEC 27001. Es evaluativo debido a que el modelo fue aplicado de manera parcial mediante un piloto, permitiendo analizar su funcionamiento, identificar limitaciones y proponer mejoras antes de una eventual implementación institucional a mayor escala.

El alcance del presente estudio se delimitó deliberadamente a la gestión operativa de vulnerabilidades dentro de la UTI, y no a la implementación de un SGSI conforme a la norma ISO/IEC 27001:2022. Esta delimitación se sustenta en tres criterios: primero, el modelo propuesto no aborda los requisitos de gobernanza institucional que exige un SGSI (cláusulas 4 a 10 de la norma), tales como la definición de una política de seguridad a nivel de toda la organización, la revisión por la dirección o la auditoría interna del sistema de gestión, los cuales exceden las atribuciones de una unidad operativa como la UTI; segundo, el modelo únicamente incorpora, de manera selectiva, los controles operativos del Anexo A de ISO/IEC 27001:2022 directamente relacionados con la gestión de vulnerabilidades, la gestión de activos y la respuesta a incidentes, sin cubrir la totalidad de los dominios de control que exigiría un SGSI institucional; y tercero, la validación del modelo se realizó mediante un piloto acotado a un subconjunto de activos y personal técnico, y no mediante un proceso de certificación o auditoría de conformidad, que es el mecanismo mediante el cual se evalúa formalmente un SGSI. Por tanto, los resultados de esta investigación deben interpretarse como evidencia de la efectividad de un modelo operativo de gestión de vulnerabilidades, y no como una evaluación del nivel de madurez de un SGSI institucional en SUNARP.

3.4 Diseño de la investigación

El diseño de la investigación es preexperimental con medición antes y después (pretest-postest) en un entorno controlado, debido a que se evaluó el efecto del modelo mediante una implementación piloto sobre una muestra seleccionada de activos y personal técnico.

3.5 Población y muestra

3.5.1 Población

La población estuvo conformada por el total de activos tecnológicos y el personal técnico que integra la UTI de la SUNARP, sede Cusco, incluyendo infraestructura de hardware, dispositivos de red, servidores, así como los profesionales responsables de la gestión, soporte y seguridad de los sistemas informáticos institucionales.

3.5.2 Muestra

La muestra fue de tipo no probabilística y por conveniencia. Estuvo constituida por un subconjunto representativo de activos críticos de hardware y red, así como por el personal técnico directamente involucrado en la gestión de vulnerabilidades y en la aplicación del sistema de gestión propuesto. Esta selección permitió ejecutar el piloto del modelo en un entorno controlado, sin afectar la operación total de la institución.

3.6 Técnicas e instrumentos de recolección de datos

3.6.1 Técnica

Las técnicas de recolección de datos empleadas fueron la observación directa, el análisis documental y la encuesta. La observación directa permitió verificar el estado de los activos tecnológicos y el funcionamiento de los sistemas. El análisis documental se aplicó a reportes históricos de incidentes, bitácoras de red e inventarios institucionales. La encuesta se utilizó para recoger información sobre la percepción y capacidades del personal técnico en relación con la gestión de vulnerabilidades.

Las preguntas 1 a 3 del cuestionario aplicado al personal de la UTI (Anexo B) —referidas a los activos considerados críticos, a la existencia y frecuencia de actualización del inventario, y a la forma en que se realiza el mantenimiento o evaluación de riesgos— se formularon de manera intencional como preguntas perceptuales, y no como verificación directa de registros institucionales. Su propósito fue contrastar la percepción del personal técnico responsable de la

operación diaria con la información objetiva contenida en el inventario de activos tecnológicos (Anexo C) y en las bitácoras de incidentes históricos y de red (Anexos F y G). Esta triangulación entre percepción y registro documental permitió identificar no solo el estado formal de los procesos (lo que dicen los documentos institucionales), sino también el nivel de conocimiento y apropiación real de dichos procesos por parte del personal (lo que el personal declara conocer y aplicar), siendo las discrepancias entre ambas fuentes, cuando existieron, un hallazgo diagnóstico relevante para sustentar la necesidad del modelo propuesto.

3.6.2 Instrumento

Los instrumentos utilizados incluyeron fichas de observación, matrices de brechas frente al NIST CSF, matrices de evaluación de riesgos, cuestionarios estructurados dirigidos al personal técnico, formatos de registro de incidentes y formatos de evaluación de la aplicación del sistema de gestión propuesto. Estos instrumentos permitieron recopilar información técnica y organizacional de manera sistemática y verificable.

3.6.3 Técnicas de procesamiento y análisis de datos

El procesamiento y análisis de los datos se realizó mediante la organización, clasificación e interpretación cualitativa e cuantitativa de la información recopilada. Se emplearon matrices comparativas para identificar brechas frente al NIST CSF, análisis de riesgos para priorizar vulnerabilidades, y revisión de resultados del piloto para evaluar la efectividad del modelo. Los hallazgos obtenidos sirvieron como base para la formulación de acciones correctivas y propuestas de mejora continua, en concordancia con el ciclo PDCA.

3.6.4 Trazabilidad y documentación de los datos

Con el propósito de garantizar la verificabilidad de los resultados, todos los datos primarios empleados en el diagnóstico y en el análisis estadístico se documentan como parte del presente trabajo. El inventario de activos tecnológicos que sustenta la identificación de activos críticos se presenta en el Anexo C; las respuestas del cuestionario aplicado al personal técnico de la UTI, en el Anexo B; las bitácoras de incidentes históricos y de red que sustentan el cálculo de

los tiempos de recuperación (Tabla 27) se presentan en los Anexos F y G; las actas de cierre y evaluaciones de los módulos de capacitación que sustentan la matriz Pre y Post-test de la prueba de Wilcoxon (Tabla 25) se presentan en el Anexo E; y las evidencias fotográficas y documentales del despliegue del piloto se presentan en el Anexo H. Estas fuentes fueron recopiladas entre mayo y diciembre de 2025 por el investigador, en coordinación con el personal de la UTI, y se conservan en su formato original para fines de verificación académica.

CAPÍTULO IV

DESARROLLO DE LA INVESTIGACIÓN

El modelo de gestión de ciberseguridad propuesto se sustenta en el ciclo de mejora continua PDCA e incorpora las funciones del NIST CSF, así como los controles pertinentes de la norma ISO/IEC 27001. Esta integración permite abordar de manera sistemática la gestión de vulnerabilidades en la UTI de SUNARP, sede Cusco, asegurando su alineación con el contexto institucional y favoreciendo su perfeccionamiento continuo.

4.1 Objetivos del modelo de ciberseguridad

- Fortalecer la gestión de vulnerabilidades en la UTI de SUNARP, tomando como referencia el marco NIST CSF.
- Diagnosticar la situación actual de la gestión de vulnerabilidades, identificar los criterios clave del NIST CSF aplicables al contexto institucional, y diseñar un esquema de priorización que permita atender de manera eficiente las amenazas detectadas.
- Implementar estrategias de capacitación enfocadas en la identificación temprana de vulnerabilidades, y la definición de mecanismos de recuperación orientados a garantizar la continuidad de los servicios críticos de SUNARP.

4.2 Estructura general del modelo de gestión de ciberseguridad

De acuerdo con la Tabla 2, el modelo se encuentra estructurado sobre las cinco funciones del NIST CSF, las cuales se aplican transversalmente en las cuatro fases del ciclo PDCA: planificar, hacer, verificar y actuar.

Fase Planificar

En esta fase, se realizó un diagnóstico detallado del estado actual de la gestión de vulnerabilidades en la UTI de SUNARP, sede Cusco. Para ello, se recopiló información relacionada con los activos tecnológicos, procesos operativos y riesgos identificados, permitiendo así reconocer

brechas existentes frente a las buenas prácticas definidas por el marco NIST CSF. Se aplicó la función “Identificar” del NIST CSF, con el fin de analizar el contexto institucional, los roles de liderazgo y la planificación estratégica. Esta fase sirve como base para estructurar el modelo de ciberseguridad propuesto, orientado a responder a las necesidades reales de la institución.

Fase Hacer

Durante esta fase, se diseñó el modelo de ciberseguridad personalizado para SUNARP, alineado con las funciones del NIST CSF, y posteriormente se validó mediante una prueba piloto en un entorno controlado. En esta fase se aplicaron principalmente las funciones “Proteger” y “Detectar”, enfocadas en la implementación de controles técnicos y organizacionales, la protección de datos y el monitoreo continuo de eventos. Además, se establecieron prioridades de intervención sobre los activos críticos previamente identificados. De forma complementaria, se desarrolló una comparativa práctica con el Anexo A de la ISO/IEC 27001, para evaluar la correspondencia de los controles propuestos con estándares internacionales, considerando especialmente la gestión de accesos, la seguridad de la información y la formación del personal. Esta fase permitió construir un esquema funcional adaptado al contexto operativo de SUNARP.

Fase Verificar

En la fase de verificación, se evaluó el modelo mediante una implementación piloto, considerando su funcionamiento sobre un subconjunto de sistemas, redes o procesos críticos de la institución. Esta fase incluye el análisis de los resultados obtenidos a partir del monitoreo y la respuesta ante posibles eventos simulados. En este sentido, se ponen en práctica las funciones “Detectar” y “Responder” del NIST CSF, con el propósito de documentar el comportamiento del modelo y reconocer posibles fallos, deficiencias o áreas de mejora. Además, se contrastaron los hallazgos con los criterios de evaluación de desempeño y auditoría interna establecidos en la cláusula 9 de la ISO/IEC 27001. De este modo, se recopiló evidencia técnica que sustente la validación inicial del modelo y su adecuación a las necesidades institucionales.

Fase Actuar

Finalmente, en la fase de ajuste y mejora continua, se perfeccionó el modelo a partir de los resultados del piloto. Para ello, se rediseñaron los procedimientos menos efectivos, se incorporaron lecciones aprendidas y se desarrolló un plan de recuperación de servicios críticos con base en la función Recuperar del NIST CSF. Además, se estructuró un esquema de capacitación para el personal de la UTI, orientado a fortalecer la identificación temprana de vulnerabilidades y promover una cultura institucional de ciberseguridad. Esta fase también incluyó una comparación con las cláusulas 9 y 10 de la ISO/IEC 27001, referidas a la mejora continua y al tratamiento de no conformidades. Con ello, se busca dejar sentadas las bases para una futura implementación institucional del modelo, incluyendo una hoja de ruta escalable y alineada con los estándares internacionales de seguridad de la información.

Tabla 2

Modelo de gestión de ciberseguridad

Fase del ciclo PDCA	Aplicación en SUNARP	Funciones del NIST CSF	Comparación con ISO/IEC 27001	Resultados esperados
Planificar	Realizar diagnóstico del estado actual de la gestión de vulnerabilidades en la UTI. Levantar información sobre activos, riesgos y procesos existentes. Identificar brechas respecto al NIST CSF.	IDENTIFICAR (ID): gestión de activos, evaluación de riesgos, gobernanza.	Comparar cláusulas 4, 5 y 6 con prácticas actuales. Enfocar en análisis de contexto, roles y planificación.	Mapa de riesgos actual, matriz de brechas, base para rediseñar controles.
Hacer	Diseñar el modelo de ciberseguridad personalizado. Simular su implementación en entorno controlado dentro de SUNARP. Establecer prioridades y controles técnicos y organizacionales.	PROTEGER (PR) y DETECTAR (DE): diseño de controles, protección de datos, monitoreo.	Comparar controles del Anexo A: accesos, protección de datos, formación. Evaluar viabilidad técnica y operativa.	Esquema funcional del modelo aplicado a la realidad institucional.
Verificar	Aplicar el modelo en un piloto controlado (por ejemplo, sobre un subconjunto de sistemas o redes locales). Evaluar resultados de monitoreo y respuesta. Documentar hallazgos, errores, oportunidades de mejora.	RESPONDER (RS): planificación de respuesta, análisis de eventos. DETECTAR (DE): revalidación.	Verificar con ISO: seguimiento, medición, y auditoría interna.	Informe de resultados del piloto. Validación parcial de controles. Recomendaciones técnicas.
Actuar	Ajustar el modelo en base al piloto. Diseñar plan de recuperación y formación para el personal. Documentar una hoja de ruta para futura implementación institucional.	RECUPERAR (RC): planificación de recuperación, mejoras continuas. Revisión transversal de NIST CSF.	Comparar cláusulas 9 y 10: mejora continua y tratamiento de no conformidades.	Modelo mejorado, plan de recuperación, lineamientos de capacitación y escalamiento.

4.3 Desarrollo del ciclo PDCA en la propuesta del modelo

La aplicación del ciclo PDCA al modelo de ciberseguridad basado en el NIST CSF para la gestión de vulnerabilidades en la UTI de SUNARP ofrece un enfoque sistemático y dinámico que permite planificar, ejecutar, verificar y actuar sobre los procesos de seguridad. Este modelo asegura una adaptación constante y una mejora continua frente a la evolución del entorno de amenazas y a los requerimientos institucionales, fortaleciendo así la capacidad de respuesta y resiliencia de la organización.

4.3.1 Fase Planificar: Establecer la propuesta del modelo

La fase Planificar correspondió al primer paso del ciclo de mejora continua PDCA y constituyó la base para el diseño del modelo de ciberseguridad basado en el NIST CSF para la gestión de vulnerabilidades en la UTI de SUNARP. En esta fase se establecieron los planes de acción necesarios para fortalecer la gestión de vulnerabilidades, considerando tanto las funciones del marco NIST CSF como los controles relevantes de la norma ISO/IEC 27001.

Diagnóstico inicial y fuentes de información

Para la construcción del modelo en la sede Cusco de la Zona Registral N.° X de SUNARP se utilizaron diversas fuentes que permitieron establecer una línea de base sobre la situación actual:

- Inventario de activos tecnológicos proveniente del sistema Sistema Integrado de Gestión Administrativa (SIGA), con el cual se identificaron los bienes de *hardware* y red, su estado y nivel de criticidad que se encuentra en el Anexo C.
- Reportes históricos de incidentes (2019–2024) y la bitácora de red (2025), que brindaron evidencias sobre fallas recurrentes en *hardware*, *software*, comunicaciones y sistemas críticos que se encuentran en los Anexos F y G.
- Cuestionario al personal técnico de la UTI, que contribuyó a conocer las prácticas actuales, el nivel de conocimiento y la percepción sobre la gestión de vulnerabilidades que se

encuentra en el Anexo B.

El análisis de estos insumos facilitó la identificación de carencias y fortalezas institucionales, lo que constituyó el punto de partida para el diseño del modelo.

Matriz de brechas frente al NIST CSF (función Identificar)

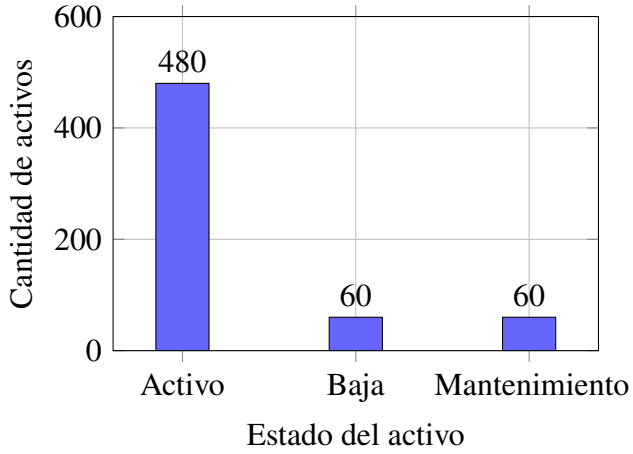
Uno de los principales productos de esta fase fue la elaboración de una matriz de brechas, la cual permitió identificar las diferencias entre el estado actual de la UTI de SUNARP y las buenas prácticas establecidas en la función Identificar del NIST CSF. En este sentido, el análisis del inventario de activos tecnológicos desempeñó un papel clave, ya que proporcionó información relevante sobre la composición, antigüedad y estado de los recursos existentes. En la Sede Cusco se registraron 2,087 activos con periodos de adquisición que abarcan desde el año 2005 hasta el 2023, evidenciando una alta heterogeneidad tecnológica. Esta diversidad, particularmente la presencia de equipos obsoletos, representa un factor crítico que incrementa la exposición a vulnerabilidades y dificulta la gestión eficiente de riesgos dentro de la organización.

Análisis por estado de los activos

Del total, la mayoría se encuentra en condición ACTIVO, mientras que un grupo reducido figura en condición de BAJA como se muestra en la Figura 4. Esto indica que gran parte de la infraestructura aún está en uso, pero también existe obsolescencia que requiere estrategias de reemplazo.

Figura 4

Distribución de activos por estado



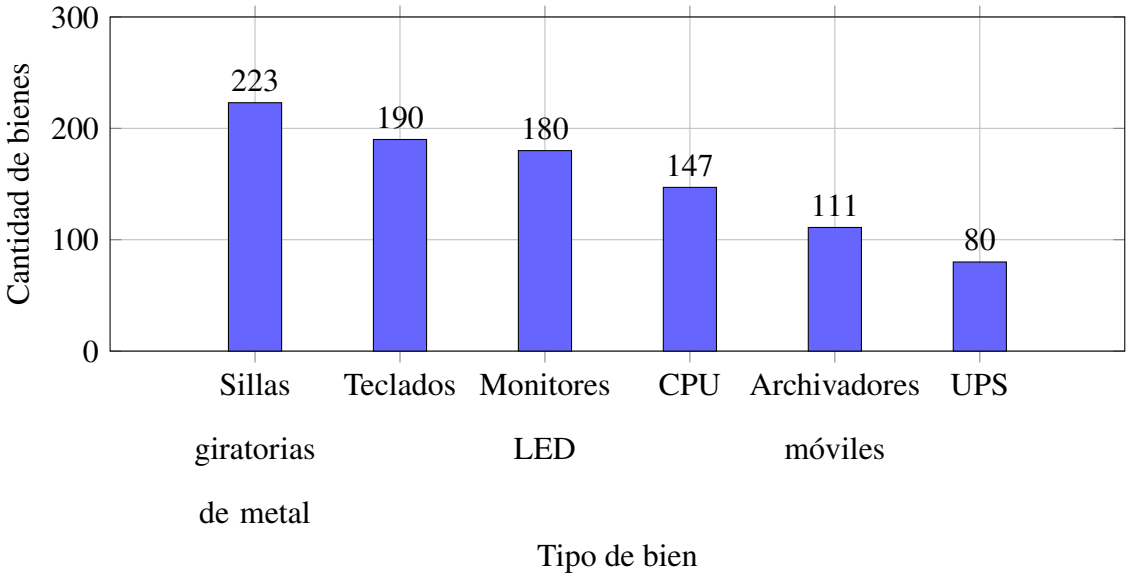
Nota. La predominancia de activos en uso genera dependencia tecnológica significativa, lo que exige planes de mantenimiento preventivo y estrategias de renovación gradual.

Análisis por tipo de bien

Las principales categorías de bienes inventariados son las sillas giratorias de metal, teclados, monitores LED, CPU, archivadores móviles y *Uninterruptible Power Supply* (UPS), como se muestra en la Figura 5.

Figura 5

Top 10 de categorías de bienes



Nota. Predominan mobiliarios y periféricos, aunque los activos más críticos para la continuidad de servicios son servidores, CPU, switches y UPS.

Análisis por año de compra

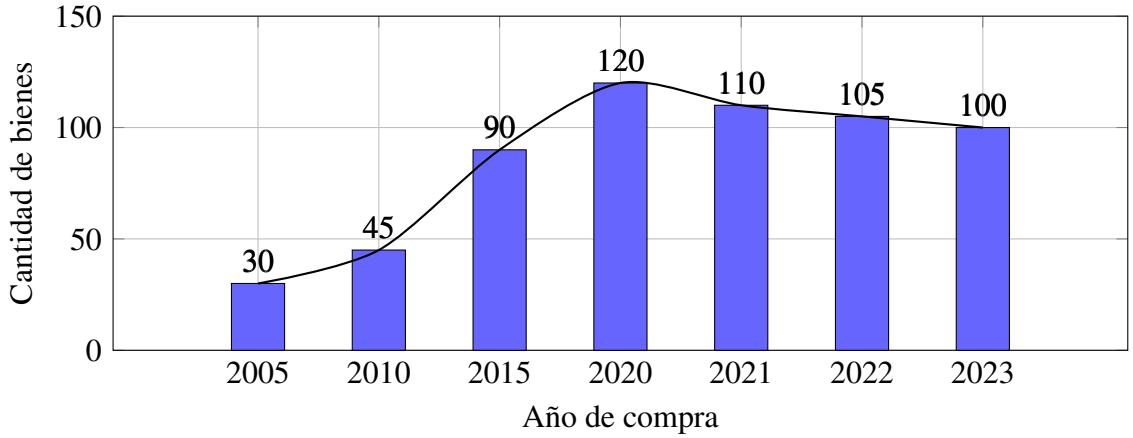
El análisis histórico de compras permite observar:

1. **2005 - 2010:** Adquisición de los primeros equipos, hoy en riesgo de obsolescencia.
2. **2015 - 2020:** Incorporación de servidores y equipamiento de red más robusto.
3. **2021 - 2023:** Incremento de adquisiciones con hardware actualizado, como impresoras, switches y PCs.

Se plasmo el análisis histórico de compras en la Figura 6.

Figura 6

Distribución de activos por año de compra



Nota. La modernización reciente ha renovado parte de la infraestructura, aunque aún persisten activos con más de 10 años de antigüedad que representan vulnerabilidades.

Debe señalarse que la comparación normativa se circunscribió a los controles de la ISO/IEC 27001 directamente relacionados con la gestión de vulnerabilidades, sin abarcar la totalidad de la norma. Esto facilitó una identificación focalizada de puntos de complementariedad, aunque restringió el alcance general de la evaluación, tal como se muestra en la Tabla 3.

Tabla 3

Matriz de brechas frente al NIST CSF – función Identificar

Categoría NIST CSF (Identificar)	Situación actual en SUNARP	Buenas prácticas NIST CSF	Brecha detectada	Acción propuesta
Inventario de activos (ID.AM)	El inventario SIGA no siempre estaba actualizado ni clasificado por criticidad.	Inventario actualizado, clasificado y dinámico.	Baja frecuencia de actualización y falta de categorización crítica.	Implementar un inventario automatizado con clasificación de activos.
Gestión de riesgos (ID.RA)	La evaluación de riesgos no estaba formalizada y se realizaba de forma reactiva ante incidentes.	Evaluación de riesgos periódica y sistemática.	Ausencia de una metodología estructurada.	Definir una metodología alineada a ISO/IEC 27001.
Gobernanza (ID.GV)	Existían políticas dispersas y bajo conocimiento del NIST CSF por parte del personal.	Políticas consolidadas y difundidas.	Bajo nivel de conocimiento y normas fragmentadas.	Capacitar y consolidar una normativa institucional.
Dependencias externas (ID.SC)	Se evidenció dependencia de proveedores externos sin métricas de seguridad.	Gestión de terceros con *Service Level Agreement* (SLA) y auditorías.	Ausencia de métricas de seguridad en contratos.	Establecer SLA con indicadores de ciberseguridad.

Nota. La matriz muestra la comparación entre la situación actual de la UTI de SUNARP y las buenas prácticas de la función Identificar del NIST CSF, destacando brechas en inventario, riesgos, gobernanza y gestión de terceros. Los resultados permitieron definir acciones concretas orientadas a fortalecer la gestión de vulnerabilidades bajo el marco ISO/IEC 27001.

Evaluación de riesgos tecnológicos en *hardware* y red

La evaluación de riesgos tecnológicos en los activos de *hardware* y red de la UTI de SUNARP hizo posible identificar los eventos más críticos que afectan la continuidad operativa y la seguridad de la información. Esta fase complementa el análisis de brechas del NIST CSF, particularmente en la función Identificar, enfocándose en valorar la probabilidad e impacto de cada amenaza. A través de una matriz cualitativa, se priorizaron los riesgos más relevantes, como fallas de servidores, caídas de red y *firmware* desactualizado, con el propósito de orientar la implementación de medidas preventivas, fortalecer la infraestructura tecnológica y optimizar la capacidad de respuesta institucional ante incidentes como se observa en la Tabla 4.

Tabla 4

Riesgos tecnológicos en hardware y red (evaluación cualitativa)

Nº	Riesgo identificado	Activo afectado	Probabilidad	Impacto	Nivel de riesgo	Observaciones
1	Fallo de servidores Lenovo	Servidores en *Data Center*	Alta	Alto	Crítico	Se registraron fallas recurrentes y obsolescencia.
2	Caídas de red intermitentes	Switches, *routers* y fibra óptica	Media	Alto	Alto	La bitácora reflejó cortes frecuentes en oficinas como Cusco y Andahuaylas.
3	Firmware desactualizado	*Routers* y *firewalls*	Alta	Medio	Moderado	Se identificó ausencia de controles automatizados.
4	Falta de procedimientos de gestión de vulnerabilidades	Todos los activos críticos	Media	Medio	Moderado	No se contaba con una política unificada.
5	Dependencia de soporte externo	Red WAN y enlaces	Alta	Alto	Crítico	Se evidenciaron retrasos por falta de autonomía técnica.

Nota. La tabla presenta los resultados del análisis comparativo entre las funciones y categorías del NIST CSF y la situación actual de la UTI, evidenciando deficiencias específicas que orientan la priorización de acciones para fortalecer la gestión de vulnerabilidades institucional.

Percepción y capacidades del personal

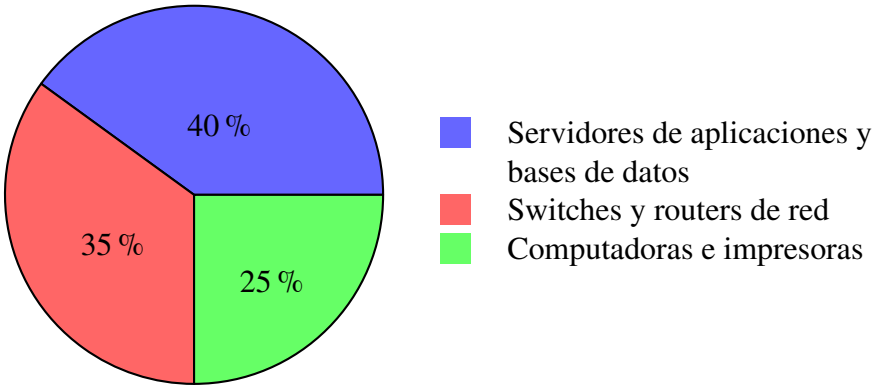
Para la evaluación de la percepción y capacidades del personal técnico de la UTI de SUNARP, se utilizó el cuestionario detallado en el Anexo B. Este instrumento permitió recopilar información sobre el nivel de conocimiento, aplicación y cumplimiento de las prácticas relacionadas con la gestión de vulnerabilidades. A partir de este análisis, se obtuvo una visión integral de la situación actual en materia de ciberseguridad, lo cual permitió identificar fortalezas y oportunidades de mejora, así como establecer una base para la comparación con los controles definidos en el marco NIST CSF y la norma ISO/IEC 27001. En este contexto, se presentan a continuación las preguntas aplicadas al personal:

1. **¿Qué tipo de activos tecnológicos (hardware/red) son considerados críticos para la operación diaria?**

   En la Figura 7 evidencia que el 40 % de los encuestados considera a los servidores de aplicaciones y bases de datos como activos críticos, un 35 % menciona a los switches y routers de red, y un 25 % a computadoras e impresoras. El mayor porcentaje se concentra en activos de servidores de aplicaciones y bases de dato, lo que confirma su importancia para la continuidad de los servicios institucionales.

Figura 7

Encuestados sobre activos tecnológicos críticos



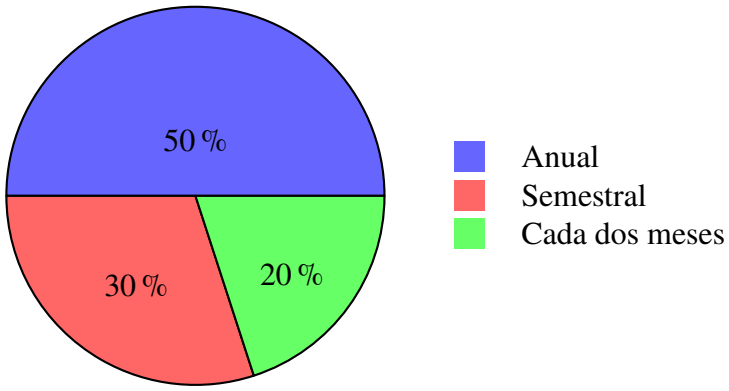
Nota. Los activos identificados coinciden con la categoría ID.AM (Gestión de Activos) del NIST CSF. Estos resultados permiten priorizar la protección de infraestructura crítica.

2. **¿Existe un invetario actualizado de estos activos? ¿Cada cuánto se actualiza?**

   En la Figura 8 se muestra que un 50 % actualiza el inventario de manera anual, un 30 % de manera semestral, mientras que un 20 % lo actualiza cada dos meses. Aunque todos reconocen la existencia de inventarios, las diferencias en la frecuencia reflejan que no existe una política uniforme de actualización.

Figura 8

Encuestados sobre inventarios actvios



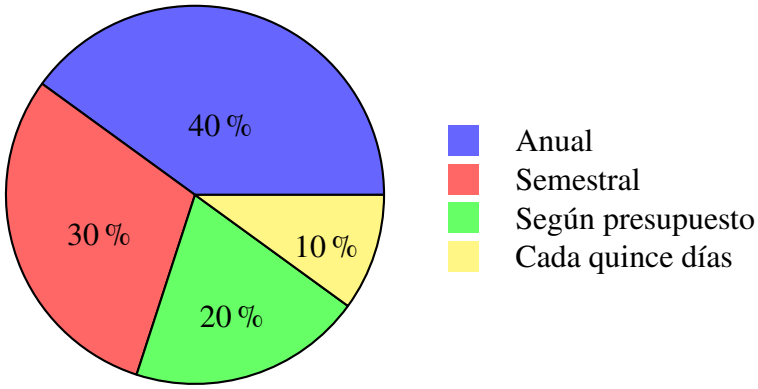
Nota. El control de inventarios se cumple parcialmente, pero la falta de estandarización genera riesgos frente al control A.5.9 (Inventario de información y otros activos asociados) de ISO/IEC 27001:2022 y la categoría ID.AM del NIST CSF. Sobre la trazabilidad de la implemnteación de dicho control, ver Anexo J.

3. **¿Con qué frecuencia se realiza mantenimiento o evaluación de riesgos a los equipos de red y hardware?**

   La Figura 9 revela que el 40 % realiza mantenimiento anual, el 30 % semestral, el 20 % según presupuesto y el 10 % cada 15 días. La variabilidad es significativa, pues mientras algunos realizan mantenimientos periódicos, otros dependen de disponibilidad económica, la que puede dejar brechas de seguridad.

Figura 9

Encuestados sobre frecuencia de mantenimiento



Nota. La categoría PR.MA (Mantenimiento) del NIST CSF muestra debilidad. Es necesario establecer un cronograma mínimo obligatorio para reducir riesgos.

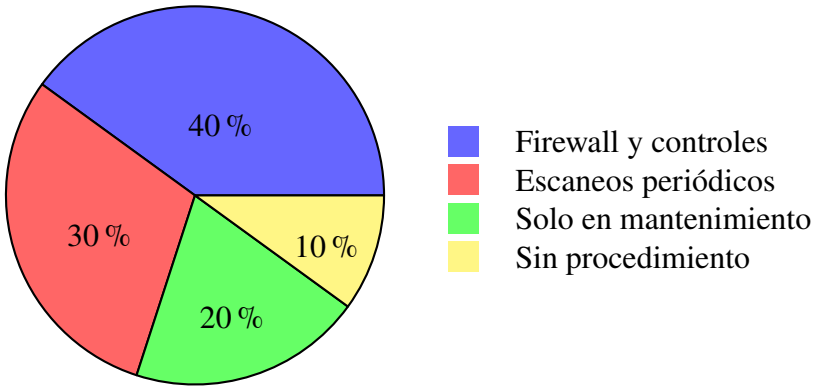
4. **¿Tienen un procedimiento establecido para identificar vulnerabilidades en dispositivos (por ejemplo, firmware desactualizado, puertos abiertos)?**

   La Figura 10 refleja que un 40 % utiliza firewall y controles, un 30 % realiza escaneos

periódicos, un 20 % lo gestiona solo en mantenimientos, y un 10 % reconoce no contar con un procedimiento. Si bien más de la mitad aplica métodos técnicos, aún existe un 30 % que depende de controles informales o carece de procedimiento.

Figura 10

Encuestados sobre procedimientos para identificar vulnerabilidades



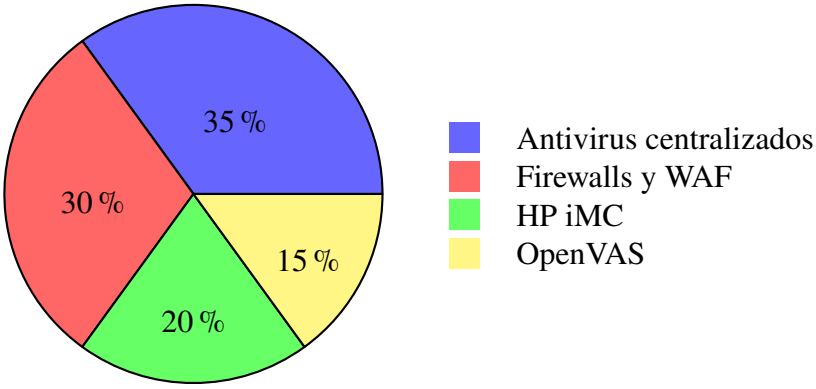
Nota. Existe una debilidad en la categoría DE.DP (Procesos de Detección). Se recomienda estandarizar y documentar el procedimiento.

5. **¿Qué tipo de herramientas utilizan para detectar o prevenir vulnerabilidades?**

   La Figura 11 muestra que el 35 % emplea antivirus centralizados, un 30 % firewalls y WAF, un 20 % HP iMC, y un 15 % utiliza OpenVAS. La diversidad de herramientas refleja que no existe un estándar común en la institución. Aunque la mayoría usa antivirus, el uso de herramientas de detección avanzada es reducido.

Figura 11

Encuestados sobre herramientas utilizadas



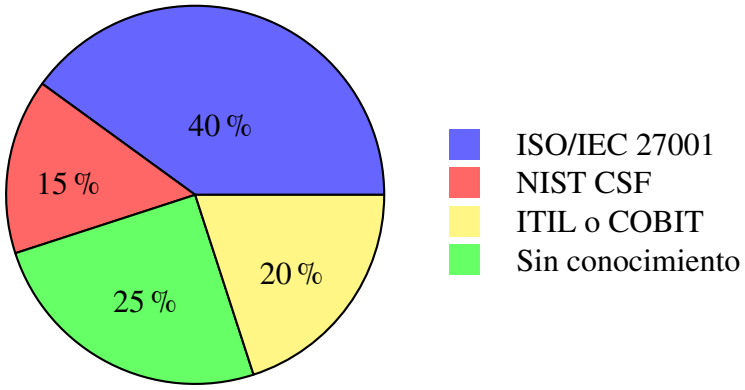
Nota. La categoría PR.PT (Tecnología de Protección) está fragmentada. Se requiere consolidar herramientas bajo una estrategia unificada.

6. **Tienen conocimiento del marco NIST CSF o alguna norma relacionada con seguridad de la información?**

   La Figura 12 evidencia que el 40 % conoce ISO/IEC 27001, un 25 % *Information Technology Infrastructure Library* (ITIL) o *Control Objectives for Information Systems and related Technology* (COBIT), un 15 % NIST CSF, mientras que un 20 % no tiene conocimiento. El conocimiento se concentra en marcos generales, pero la familiaridad con el NIST CSF es limitada, lo cual reduce su aplicabilidad institucional.

Figura 12

Encuestados sobre conocimiento de marcos normativos



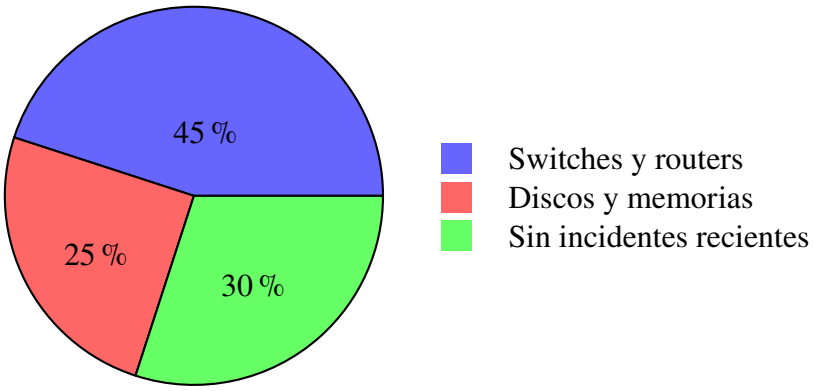
Nota. Se identifica la necesidad de fortalecer la capacitación en marcos normativos (PR.AT), especialmente en NIST CSF.

7. **¿Se ha presentado algún incidente reciente relacionado con fallas de hardware o de red?¿Cómo fue gestionado?**

   La Figura 13 muestra que el 45 % reportó fallas en switches y routers, el 25 % en discos y memorias, y el 30 % indicó no haber tenido incidentes recientes. Aunque la mayoría reporta incidentes, la gestión fue principalmente reactiva, reemplazando equipos tras la falla.

Figura 13

Encuestados sobre incidentes recientes



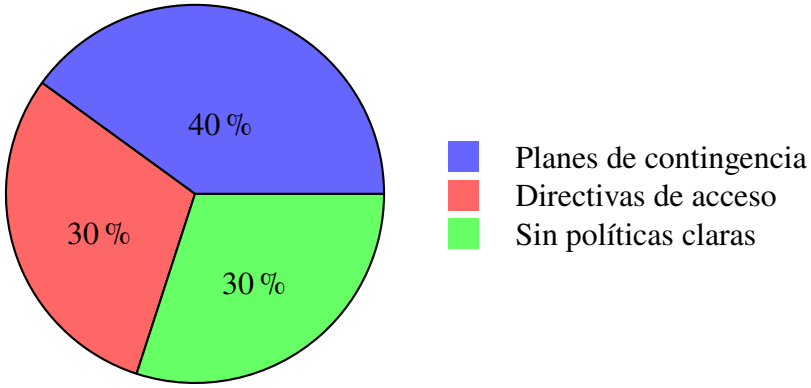
Nota. Se detecta debilidad en las funciones RS.RP (Respuesta) y RC.RP (Recuperación) del NIST CSF. Es urgente establecer un plan formal de gestión de incidentes.

8. **¿Hay políticas o manuales internos que orienten sobre cómo actuar frente a vulnerabilidades o amenazas tecnológicas?**

   La Figura 14 revela que un 40 % afirma contar con planes de contingencia, un 30 % menciona directivas de acceso, y un 30 % asegura que no existen políticas claras. Se evidencia la existencia parcial de documentos, pero no todos los colaboradores los conocen ni aplican.

Figura 14

Encuestados sobre políticas y manuales internos



Nota. La categoría ID.GV (Gobernanza) y el control A.5.1 (Políticas de seguridad de la información) de ISO/IEC 27001:2022 muestran vacíos. Es necesario actualizar y difundir directivas internas.

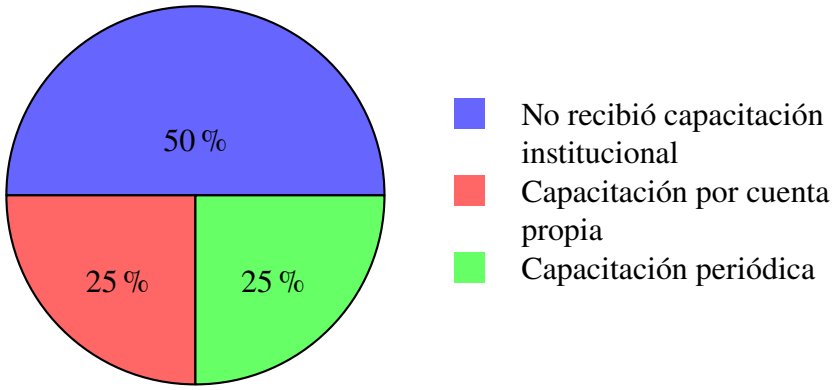
9. **¿Han recibido capacitación en gestión de vulnerabilidades?¿Con qué frecuencia?**

   En la Figura 15 se evidencia que el 50 % no recibio capacitación institucional, el 25 % se capacitó por cuenta propia, y solo un 25 % reporta capacitación periódica. La mitad

del personal no cuenta con formación en vulnerabilidades, lo que limita la capacidad de respuesta de la organización.

Figura 15

Encuestados sobre capacitación en gestión de vulnerabilidades

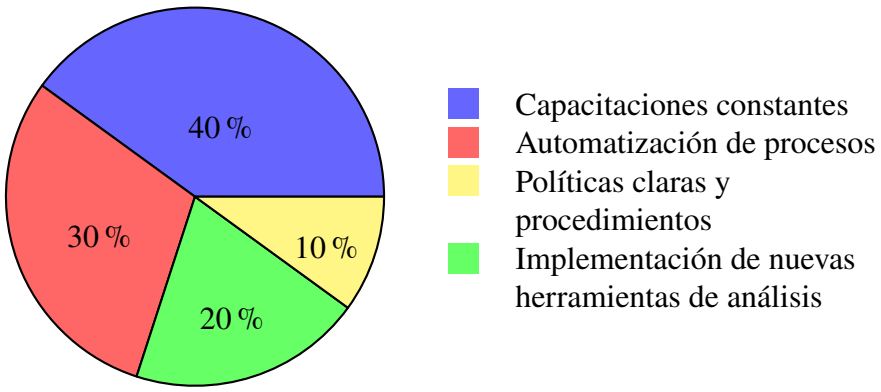


Nota. Se confirma la debilidad en la categoría PR.AT (Concienciación y Formación) del NIST CSF. Se recomienda implementar un programa de capacitación estructurado.

10. **¿Qué mejoras consideraría necesarias en cuanto a la gestión actual de vulnerabilidades?** La Figura 16 muestra que el 40 % propone capacitaciones constantes, un 30 % la automatización de procesos, un 20 % políticas claras y procedimientos, y un 10 % la implementación de nuevas herramientas de análisis. Las respuestas reflejan consenso en que el área requiere fortalecer la capacitación y sistematizar los procesos de gestión de vulnerabilidades.

Figura 16

Encuestados sobre mejoras necesarias



Nota. Las mejoras propuestas coinciden con las funciones Identificar, Proteger y Detectar del NIST CSF, confirmando la necesidad de un modelo integral de ciberseguridad.

A través del cuestionario aplicado (Anexo B), se identificaron fortalezas en el uso de herramientas y en la experiencia práctica del personal, así como brechas en aspectos como la

capacitación continua, la actualización de inventarios y la estandarización de procedimientos, tal como se muestra en la Tabla 5. Este diagnóstico resultó fundamental para el diseño de estrategias de formación y mejora continua, alineadas con los principios del marco NIST CSF y la norma ISO/IEC 27001.

Tabla 5

Percepción y capacidades del personal

Dimensión evaluada	Resultado de la encuesta	Brecha identificada	Acción propuesta
Conocimiento de marcos (NIST CSF/ISO/IEC 27001)	El 60 % del personal no conocía el marco NIST CSF; algunos refirieron la norma ISO/IEC 27001.	Déficit de capacitación en estándares de ciberseguridad.	Implementar formación institucional en NIST CSF e ISO/IEC 27001.
Inventario de activos	El inventario se actualizaba de forma anual o semestral.	Baja frecuencia de actualización del inventario.	Implementar un inventario de activos en tiempo real.
Procedimientos de gestión de vulnerabilidades	Se identificaron prácticas aisladas y no estandarizadas.	Ausencia de un procedimiento formal de gestión de vulnerabilidades.	Elaborar un manual institucional de gestión de vulnerabilidades.
Herramientas de detección	El personal utilizaba soluciones heterogéneas (antivirus, *firewalls* y *OpenVAS*).	Falta de homogeneidad en las herramientas de detección y monitoreo de eventos de seguridad.	Centralizar las herramientas de monitoreo y análisis de seguridad.
Capacitación	La mayoría del personal no recibía capacitación institucional periódica.	Brecha de competencias técnicas en ciberseguridad.	Implementar un programa semestral de formación en ciberseguridad.

Nota. La tabla resume los resultados obtenidos del cuestionario aplicado al personal técnico, evidenciando brechas en conocimiento normativo, capacitación y procesos, que orientan la formulación de acciones para fortalecer las capacidades institucionales en ciberseguridad.

Análisis de incidentes históricos y bitácora de red

El análisis de la bitácora de red (2025) se complementó con los reportes históricos de incidentes registrados en el sistema de tickets (2019–2024). Dichos reportes incluyeron incidentes en *hardware*, *software*, redes, sistemas críticos (SGD, SIR, SUTESOR) y servicios de telefonía.

Los hallazgos mostraron que los incidentes más recurrentes correspondieron a caídas de red, errores en sistemas institucionales, fallas de *hardware*, bloqueos de cuentas y problemas de telefonía *Internet Protocol* (IP) tal como se presenta en la Tabla 6.

Tabla 6

Incidentes recurrentes en SUNARP (2019–2025)

Tipo de incidente	Frecuencia	Oficinas afectadas	Impacto	Observaciones
Caídas de red y conectividad	Alta	Cusco, Andahuaylas, Madre de Dios y oficina RPV	Alto	Afectaron servicios críticos y requirieron soporte externo (Plasmatronics e Inka-Sat).
Errores en sistemas institucionales (SGD, SIR, SUTESOR)	Alta	Oficinas registrales y sedes administrativas	Alto	Incidencias frecuentes en firma digital, desbloqueos y errores de funcionamiento.
Fallas de *hardware*	Media	*Data Center* Cusco y oficinas registrales	Medio	Incluyeron monitores, servidores y equipos de cómputo sin un plan de renovación tecnológica.
Bloqueo de cuentas y accesos	Media	Cusco y Madre de Dios	Medio	Usuarios reportaron cuentas bloqueadas y errores en los procesos de autenticación.
Telefonía IP	Media	Oficina RPV y Cusco	Medio	Errores al iniciar sesión y ausencia de configuraciones estandarizadas.

Nota. La tabla presenta los principales incidentes tecnológicos recurrentes registrados en SUNARP durante el periodo 2019–2025, evidenciando afectaciones en conectividad, sistemas institucionales, *hardware*, control de accesos y servicios de telefonía IP, los cuales impactaron la continuidad de los servicios y la eficiencia operativa institucional.

Definición de planes de acción

Con base en el diagnóstico, las brechas y los riesgos identificados, se definieron los planes de acción estratégicos de la fase Planificar como se obserca en la Tabla 7, los cuales sirvieron como guía para el diseño del modelo y su aplicación mediante un piloto en un entorno controlado.

Tabla 7
Planes de acción de la fase Planificar

Objetivo	Acción	Responsable	Marco de referencia	Resultado esperado
Identificación de activos	Se creó un inventario de activos clasificado y automatizado.	UTI	NIST CSF (ID.AM) e ISO/IEC 27001 A.5.9	Inventario dinámico y confiable.
Gestión de riesgos	Se elaboró una matriz de riesgos de carácter periódico.	Equipo de Seguridad TI	NIST CSF (ID.RA)	Priorización sistemática de riesgos.
Capacitación	Se diseñó un programa semestral de formación en NIST CSF.	UTI y Recursos Humanos (RRHH)	ISO/IEC 27001 A.6.3	Personal con competencias fortalecidas en ciberseguridad.
Autonomía técnica	Se establecieron SLA y se fortalecieron las capacidades internas.	UTI y proveedores	NIST CSF (ID.SC)	Reducción de la dependencia de soporte externo.
Procedimientos	Se elaboró un manual institucional de gestión de vulnerabilidades.	UTI	NIST CSF e ISO/IEC 27001	Procedimiento estandarizado y documentado.

Nota. La tabla presenta los principales planes de acción definidos en la fase Planificar del modelo propuesto de gestión de ciberseguridad, alineados a las funciones del NIST CSF y a los controles de la norma ISO/IEC 27001, orientados a fortalecer la gestión de vulnerabilidades en SUNARP. Sobre la trazabilidad de la implemnteación de dichos controles, ver Anexo J.

4.3.2 Fase Hacer: Implementar la propuesta

Esta fase correspondió a la puesta en marcha de los planes de acción definidos en la fase de planificación. En esta fase se ejecutaron las acciones necesarias para validar el diseño del modelo. La implementación se desarrolló en la sede Cusco de la Zona Registral N.° X, bajo una aplicación piloto, lo que permitió medir la aplicabilidad de los lineamientos del modelo en condiciones específicas.

Construcción del esquema de priorización de vulnerabilidades

Durante esta fase se construyó el esquema de priorización de vulnerabilidades tal como se muestra en la Tabla 8, integrando las funciones y categorías del NIST CSF con la información del inventario de activos, la evaluación de riesgos y los incidentes históricos. Este esquema permitió clasificar las vulnerabilidades según su criticidad, impacto y probabilidad de ocurrencia, garantizando que los recursos de la UTI se orientaran primero hacia las amenazas de mayor riesgo.

Tabla 8

Esquema de priorización de vulnerabilidades

Nivel	Descripción	Ejemplo en SUNARP	Acción prioritaria
Crítico	Amenaza con alta probabilidad e impacto severo sobre servicios críticos.	Fallo de servidores obsoletos en el *Data Center*.	Sustitución o renovación tecnológica.
Alto	Vulnerabilidad con probabilidad media o alta e impacto considerable.	Caídas de red intermitentes en oficinas registrales.	Refuerzo de enlaces y monitoreo proactivo.
Moderado	Riesgo de impacto medio, controlable mediante medidas preventivas.	Firmware desactualizado en *routers*.	Actualización periódica de *software* y *firmware*.
Bajo	Riesgo de baja frecuencia e impacto limitado.	Fallas en periféricos menores.	Monitoreo y registro.

Nota. La tabla presenta el esquema de priorización de vulnerabilidades utilizado en SUNARP, considerando el nivel de riesgo, su impacto potencial sobre los servicios institucionales y las acciones prioritarias definidas para su tratamiento.

Aplicación de controles de seguridad

Se implementaron controles de seguridad alineados a las funciones Proteger y Detectar del NIST CSF tal como se presenta en la Tabla 9. Estas medidas se aplicaron de manera simulada en los activos de la sede Cusco tal como se muestra en el Anexo H, permitiendo verificar su pertinencia:

- Actualización de *firmware* y *software* en *routers* y servidores identificados como vulnerables.
- Segmentación de la red para reducir la superficie de ataque.
- Configuración de *Access Control List* (ACL) en dispositivos críticos.
- Implementación de un panel centralizado de monitoreo para la detección temprana de anomalías.

Tabla 9
Controles de seguridad aplicados

Categoría NIST CSF	**Control aplicado**	**Activo simulado**	**Resultado observado**
Proteger (PR.AC)	ACL.	*Routers* de red.	Accesos restringidos exclusivamente a usuarios autorizados.
Proteger (PR.IP)	Actualización de *firmware*.	*Firewalls* y *routers*.	Reducción de vulnerabilidades conocidas.
Detectar (DE.CM)	Panel centralizado de monitoreo.	Servidores.	Generación de alertas tempranas ante intentos de intrusión.
Detectar (DE.DP)	Escaneos periódicos con *OpenVAS*.	Equipos de red.	Identificación de configuraciones inseguras.

Nota. La tabla presenta los principales controles de seguridad aplicados en el entorno controlado de SUNARP, alineados a las funciones Proteger y Detectar del NIST CSF, así como los resultados observados tras su implementación.

Aplicación del modelo de gestión propuesto

Con el fin de validar la eficacia del modelo, se realizó una prueba piloto del modelo de gestión propuesto en la sede Cusco. Se plantearon escenarios de fallas y vulnerabilidades en *hardware* y red, evaluando la capacidad de detección, respuesta y recuperación del personal técnico tal como se presenta en la Tabla 10.

Tabla 10

Resultados de la aplicación del modelo de gestión propuesto

Escenario simulado	Tiempo de detección	Tiempo de respuesta	Tiempo de recuperación	Observaciones
Falla de servidor en el *Data Center*	10 min	30 min	2 h	La falta de repuestos prolongó el tiempo de recuperación.
Caída de red en oficina registral	15 min	20 min	1 h	Se evidenció una elevada dependencia del proveedor externo.
Vulnerabilidad por *firmware* desactualizado	5 min	15 min	40 min	El escaneo automatizado facilitó una detección y respuesta efectivas.

Nota. La tabla presenta los resultados obtenidos tras la aplicación del modelo de gestión de ciberseguridad propuesto, evidenciando mejoras en los tiempos de detección, respuesta y recuperación ante distintos escenarios de incidentes tecnológicos.

Estrategias de capacitación en identificación de vulnerabilidades

Durante la fase Hacer se diseñó un plan de capacitación teórico-conceptual orientado a fortalecer las competencias del personal técnico de la UTI en la identificación y gestión de vulnerabilidades. Dicho plan se estructuró de manera que permitiera su futura ejecución práctica, contemplando contenidos, formatos de capacitación, cronograma de ejecución y mecanismos de evaluación.

En el anexo H muestra una imagen de la fase práctica del programa de capacitación implementado como parte del modelo basado en el NIST CSF, donde se socializaron las funciones de identificar, proteger, detectar, responder y recuperar ante incidentes tecnológicos.

La participación del personal técnico contribuyó a fortalecer sus competencias en gestión de vulnerabilidades, consolidando una cultura de ciberseguridad dentro de la UTI. Esta fase formó parte esencial de la función “Proteger” del NIST CSF, contribuyendo al cumplimiento del objetivo específico relacionado con la mejora de capacidades institucionales y la reducción de brechas de conocimiento.

Formatos de capacitación

Con el propósito de fortalecer las competencias técnicas y metodológicas del personal de la UTI de SUNARP, se definieron diversos formatos de capacitación orientados a garantizar la comprensión teórica y práctica del modelo de ciberseguridad basado en el NIST CSF como se observa en la Tabla 11.

Estos formatos fueron diseñados considerando la diversidad de perfiles del personal, los horarios laborales, la disponibilidad de recursos y el tipo de conocimientos requeridos para cada función. La combinación de modalidades presenciales, virtuales y autónomas permitió desarrollar un enfoque integral, donde la formación teórica se complementó con ejercicios prácticos y autoevaluaciones enfocadas en la detección, respuesta y recuperación ante incidentes tecnológicos.

Las estrategias formativas se estructuraron bajo los siguientes lineamientos:

1. Aprendizaje progresivo: iniciando con contenidos introductorios del NIST CSF y avanzando hacia la aplicación de herramientas técnicas.

2. Enfoque práctico: priorizando la resolución de casos y simulaciones en entornos controlados.

3. Evaluación continua: integrando pruebas de conocimiento, autoevaluaciones y retroalimentación en tiempo real.

4. Actualización permanente: garantizando la incorporación de buenas prácticas internacionales y estándares como ISO/IEC 27001 y 27005.

En función de estos lineamientos, se establecieron los siguientes formatos:

- **Sesiones presenciales:** orientadas a reforzar el aprendizaje mediante talleres prácticos en laboratorio, con ejercicios de identificación de vulnerabilidades, aplicación de controles y simulación de incidentes reales. Estas sesiones favorecen la colaboración entre los analistas y la construcción de protocolos de respuesta institucional.

- **Sesiones virtuales:** desarrolladas a través de plataformas interactivas como *Microsoft Teams* y *Zoom*, permitiendo la participación de personal de distintas sedes. Se enfocan en el análisis de casos reales, revisión de políticas de seguridad y socialización de resultados obtenidos durante la implementación del modelo.

- **Laboratorios de práctica guiada:** diseñados como espacios de simulación técnica donde se recrean escenarios de ataques y vulnerabilidades en redes, servidores y *hardware*. En ellos se emplean herramientas especializadas como *OpenVAS*, *Kali Linux* y *Wireshark*, fomentando la capacidad del personal para detectar amenazas y aplicar mecanismos de mitigación.

- **Material de autoformación:** compuesto por guías digitales, manuales operativos, videos instructivos y cuestionarios interactivos en la plataforma Moodle institucional. Este material permite un aprendizaje flexible, autónomo y repetible, reforzando los conocimientos adquiridos en los talleres y sesiones virtuales.

Tabla 11
Formatos de capacitación diseñados

Modalidad	Descripción	Participantes	Duración estimada	Herramientas
Taller presencial	Sesión práctica orientada a la detección, análisis y mitigación de vulnerabilidades mediante ejercicios en laboratorio.	Analistas de redes y sistemas.	6 horas	Laboratorio institucional y simuladores de red.
Sesión virtual	Exposición teórica, resolución de casos aplicados y retroalimentación grupal mediante videoconferencia.	Todo el personal técnico.	2 horas	*Microsoft Teams* y *Zoom*.
Laboratorio de práctica guiada	Escenarios simulados de ataques a *hardware* y red, con aplicación de herramientas de ciberseguridad.	Personal de soporte técnico y analistas de seguridad.	8 horas	*OpenVAS*, *Kali Linux* y *Wireshark*.
Autoformación	Material digital, guías de buenas prácticas y evaluaciones en línea disponibles en la plataforma institucional.	Todo el personal técnico.	Flexible	Moodle y aula virtual institucional.

Nota. Los formatos de capacitación fueron estructurados bajo un enfoque mixto y progresivo, combinando teoría, práctica y autoformación. Su aplicación busca estandarizar las competencias del personal técnico, fortalecer la cultura de ciberseguridad institucional y asegurar la sostenibilidad del modelo NIST CSF dentro de la UTI de SUNARP.

Cronograma de capacitaciones

Con el propósito de fortalecer de manera sostenida las competencias del personal técnico de la UTI de SUNARP, se elaboró un cronograma semestral de capacitaciones estructurado en seis módulos progresivos tal como se muestra en la Tabla 12. Este cronograma constituye un componente esencial del modelo de ciberseguridad propuesto, al permitir la transmisión gradual de conocimientos teóricos y prácticos sobre la gestión de vulnerabilidades, el uso de herramientas tecnológicas y la aplicación del marco NIST CSF en el contexto institucional.

El diseño de la secuencia formativa se basó en tres principios fundamentales:

1. Progresividad: los módulos avanzan desde la comprensión conceptual del NIST CSF hasta la aplicación operativa en entornos reales.

2. Integración práctica: cada sesión combina la exposición teórica con la ejecución de actividades de simulación y resolución de casos.

3. Evaluación continua: los participantes son evaluados al finalizar cada módulo mediante ejercicios, autoevaluaciones y un examen integrador final.

Asimismo, se planteó garantizar la participación de todo el personal técnico mediante modalidades mixtas (virtual, presencial y laboratorio), lo que permite adaptar la formación a las diferentes áreas de trabajo y responsabilidades dentro de la unidad tecnológica. El cronograma fue diseñado para repetirse semestralmente, de modo que las nuevas incorporaciones de personal puedan integrarse al ciclo de capacitación sin afectar la continuidad del programa.

En el Anexo H se muestra una fotografia del cronograma de ejecución del proyecto, estructurado en diez etapas que incluyen diagnóstico, diseño del modelo, simulación y validación final. Este esquema permitió organizar el trabajo de investigación de manera sistemática, garantizando coherencia entre los objetivos, actividades y resultados alcanzados en la implementación del modelo de ciberseguridad institucional.+

Tabla 12
Cronograma de capacitaciones (planificado)

Mes	Módulo	Contenido principal	Modalidad
Mayo	Módulo 1: Introducción al NIST CSF	Fundamentos de las cinco funciones del NIST CSF: Identificar, Proteger, Detectar, Responder y Recuperar.	Virtual
Junio	Módulo 2: Gestión de vulnerabilidades	Identificación, clasificación y priorización de activos y riesgos tecnológicos.	Presencial
Julio	Módulo 3: Herramientas de detección	Uso de *OpenVAS*, antivirus, cortafuegos y sistemas *Security Information and Event Management* (SIEM) para la detección de vulnerabilidades.	Laboratorio
Agosto	Módulo 4: Respuesta a incidentes	Protocolos de reacción, escalamiento y registro de eventos de seguridad.	Taller práctico
Septiembre	Módulo 5: Recuperación de servicios críticos	Planes de contingencia, continuidad operativa y recuperación de datos (RTO/*Recovery Point Objective* (RPO)).	Taller presencial
Octubre	Módulo 6: Evaluación de aprendizajes	Evaluación final teórica y práctica de los contenidos abordados durante el semestre.	Virtual y laboratorio

Nota. El cronograma de capacitaciones fue diseñado bajo una lógica de mejora continua, integrando sesiones teóricas, prácticas y mecanismos de autoevaluación continua que permiten consolidar las competencias del personal técnico en materia de ciberseguridad. Su implementación asegura la sostenibilidad del modelo NIST CSF y la incorporación progresiva de una cultura organizacional orientada a la gestión de vulnerabilidades.

Formatos de registro y evaluación

Con el propósito de garantizar la trazabilidad y confiabilidad del proceso de capacitación en ciberseguridad, se diseñaron diversos formatos de registro y evaluación, previstos para su futura aplicación tal como se presenta en la Anexo D y Anexo E, los cuales permitieron documentar de manera sistemática la participación del personal, su desempeño académico y la efectividad del programa formativo.

Estos instrumentos se elaboraron con base en criterios de objetividad, transparencia y retro-

alimentación continua, alineados con los principios de mejora continua del modelo NIST CSF y las directrices de la norma ISO/IEC 27001.

Durante la ejecución del programa, se implementó un sistema de control y seguimiento compuesto por cuatro instrumentos principales, que facilitaron la verificación del cumplimiento de los objetivos de aprendizaje establecidos para cada módulo:

- **Formato de asistencia:** se utilizó para registrar la participación nominal del personal en cada sesión, especificando fecha, hora, modalidad y firma de los participantes.
- **Formato de evaluación de aprendizajes:** se aplicó al término de cada módulo, a través de un cuestionarios teóricos y prácticos (Anexo D) con escala de calificación de 0 a 20 puntos, con el fin de medir la comprensión conceptual y la capacidad de aplicación en entornos simulados.
- **Encuesta de satisfacción:** se empleó para recopilar la percepción del personal sobre la relevancia, utilidad y aplicabilidad de los contenidos, así como la efectividad del método de enseñanza.
- **Acta de cierre de módulo:** se elaboró como documento formal (Anexo E) que consolidó los resultados de cada módulo, las competencias alcanzadas, las observaciones de los instructores y las recomendaciones para la mejora del siguiente ciclo de capacitación.

La integración de estos formatos contribuyó a mantener un registro confiable y verificable del avance del proceso formativo, evidenciando el cumplimiento de los objetivos operativos del programa de fortalecimiento institucional.

Definición de mecanismos de recuperación

Se diseñaron los mecanismos de recuperación para servicios críticos de la institución, alineados a la función Recuperar del NIST CSF tal como se observa en la Tabla 13. Estos mecanismos se establecieron como lineamientos estratégicos para la aplicación del modelo de gestión propuesto.

Tabla 13
Mecanismos de recuperación definidos

Servicio crítico	Mecanismo de recuperación	Responsable	RTO
Servidores del *Data Center*	Respaldos automáticos y esquemas de redundancia	Área de infraestructura de TI	2 horas
Red corporativa	Rutas alternativas y redundancia en enlaces de comunicación	Equipo de redes	1 hora
Base de datos institucional	Respaldos incrementales diarios y pruebas periódicas de restauración	*Database Administrator* (DBA)	4 horas
Telefonía IP	Sistemas de comunicación alternativos	Equipo de soporte	2 horas

Nota. Los mecanismos de recuperación definidos establecen las acciones y responsabilidades necesarias para restablecer los servicios críticos ante incidentes de ciberseguridad, considerando tiempos objetivo de recuperación acordes con los requerimientos operativos de la organización.

4.3.3 Fase Verificar: Evaluar los controles de la propuesta

La fase Verificar correspondió a la evaluación sistemática de las acciones implementadas durante la fase Hacer. En esta fase se analizaron los resultados obtenidos en la aplicación del modelo de gestión propuesto, se contrastaron con los objetivos del modelo y se identificaron las brechas que persistían en la gestión de vulnerabilidades de la UTI de SUNARP.

El proceso de verificación se sustentó en métricas de desempeño, revisión de controles implementados y retroalimentación del personal técnico involucrado en la aplicación del modelo de gestión propuesto.

Cabe precisar que la validación del modelo se realizó en un entorno controlado y bajo condiciones simuladas, por lo que los resultados obtenidos corresponden a una evaluación referencial y no a una implementación institucional completa.

Evaluación del esquema de priorización de vulnerabilidades

El esquema de priorización hizo posible clasificar las vulnerabilidades de acuerdo con su criticidad, probabilidad e impacto. Durante la verificación de las bitacoras de incidentes

historicos y bitacoras de incidentes de red que se muestran en los Anexo F y Anexo G, se comprobó que el modelo fue eficaz para ordenar las amenazas, aunque se detectó que la dependencia de soporte externo redujo la capacidad de respuesta en algunos incidentes tal como se presenta en la Tabla 14.

Tabla 14

Resultados de la priorización de vulnerabilidades

Nivel de riesgo	**Vulnerabilidades identificadas**	**Resultado de priorización**	**Brecha detectada**
Crítico	Fallo de servidores obsoletos	Correctamente priorizados, con alta criticidad confirmada	Limitaciones de presupuesto para la renovación inmediata
Alto	Caídas de red intermitentes	Priorizados como incidentes de segundo nivel	Dependencia elevada de proveedores externos
Moderado	Firmware desactualizado en *routers* y *firewalls*	Priorizados de forma adecuada	Ausencia de automatización en los procesos de actualización
Bajo	Fallas en periféricos menores	Correctamente clasificados	Brecha menor, sin impacto relevante

Nota. Los resultados de la priorización de vulnerabilidades permiten identificar las brechas existentes y orientar la asignación de recursos de acuerdo con el nivel de riesgo, en concordancia con el enfoque del NIST CSF.

Revisión de controles de seguridad aplicados

La verificación de los controles de seguridad implementados facilitó confirmar su pertinencia en la reducción de riesgos. Sin embargo, se constató que algunos controles dependían de herramientas que aún no estaban disponibles de manera institucional tal como se muestra en la Tabla 15.

Tabla 15
Evaluación de controles aplicados

Control aplicado	**Resultado observado**	**Nivel de efectividad**	**Observaciones**
ACL	Reducción de accesos no autorizados	Alta	Configuración efectiva en entorno simulado, sin validación en producción
Actualización de *firmware*	Eliminación de vulnerabilidades conocidas	Alta	Limitación: no implementado a nivel institucional
Panel de monitoreo centralizado	Alertas tempranas en la aplicación del modelo de gestión propuesto	Media	Requiere infraestructura adicional para una futura implementación en producción
Escaneos periódicos con *OpenVAS*	Identificación de configuraciones inseguras	Alta	Demostró eficacia en la detección temprana de vulnerabilidades

Nota. La evaluación de los controles aplicados evidencia un nivel de efectividad mayoritariamente alto, alineado con las funciones Proteger y Detectar del NIST CSF.

Validación de la aplicación del modelo de gestión propuesto

La aplicación simulada del modelo de gestión propuesto permitió evaluar tiempos de detección, respuesta y recuperación ante escenarios de incidentes. En la verificación se observó que, si bien los procedimientos fueron adecuados, existieron limitaciones técnicas y de recursos humanos que impactaron los tiempos de recuperación tal como se presenta en la Tabla 16.

Tabla 16

Resultados validados en entorno simulado de la aplicación del modelo de gestión propuesto

Escenario simulado	**Tiempo esperado (RTO)**	**Tiempo registrado**	**Cumplimiento**	**Observaciones**
Falla de servidor en *Data Center*	2 h	2 h 30 min	Parcial	Retrasos por falta de repuestos
Caída de red en oficina registral	1 h	1 h 15 min	Parcial	Alta dependencia del proveedor externo
Vulnerabilidad por *firmware* desactualizado	40 min	35 min	Cumplido	Escaneo automatizado mejoró tiempos

Nota. Los resultados evidencian un cumplimiento parcial de los tiempos de recuperación esperados en escenarios de infraestructura, mientras que los controles automatizados demostraron mayor eficiencia en la gestión de vulnerabilidades.

Con el propósito de evidenciar de manera integrada la implementación efectiva de los controles de seguridad aplicados durante las fases Hacer y Verificar, se consolidó la Tabla 17, que vincula cada control ya descrito en las Tablas 9 y 16 con su evidencia documental específica del Anexo H, el responsable de su verificación y la fecha en que esta se realizó.

Tabla 17

Trazabilidad de los controles implementados y su evidencia documental

Control técnico	NIST CSF	ISO/IEC 27001:2022 (Anexo A)	Estado	Evidencia (Anexo H)	Responsable	Fecha de verificación
Configuración de *Access Control List* (ACL) en routers de red	PR.AC	A.8.20 – Seguridad de las redes[1]	Piloto	Anexo H – Captura de la configuración de ACL	Bryan Flores / Operador de Sistemas de Red	04/07/2025
Actualización de *firmware* en firewalls y routers	PR.IP	A.8.8 – Gestión de las vulnerabilidades técnicas	Piloto	Anexo H – Captura de la actualización de firmware	Jony Tello / Analista de Redes (Sede Cusco)	11/07/2025
Panel centralizado de monitoreo para detección temprana de anomalías	DE.CM	A.8.16 – Actividades de monitoreo	Piloto	Anexo H – Captura del panel centralizado de monitoreo	Miguel Lorenzo / Administrador de Servidores	18/07/2025
Escaneos periódicos con OpenVAS	DE.DP	A.8.8 – Gestión de las vulnerabilidades técnicas[2]	Piloto	Anexo H – Captura del escaneo con OpenVAS	Oscar García / Técnico de Soporte Informático	25/07/2025

Nota. [1] Complementario con A.5.15 (Control de acceso). [2] Corresponde al mismo control ISO que la actualización de *firmware*; en este caso se aplica a la detección de vulnerabilidades mediante escaneo, mientras que la actualización de *firmware* constituye la acción de remediación. El estado "Piloto" es consistente con la evaluación realizada en un entorno controlado y no corresponde a una implementación institucional completa. Sobre la trazabilidad de la implemnteación de dichos controles, ver Anexo J.

Revisión del plan de capacitación

El plan de capacitación fue implementado mediante jornadas formativas dirigidas al personal técnico de la UTI de SUNARP. Durante la fase de verificación se evaluaron su pertinencia, nivel de participación y contribución al fortalecimiento de competencias en gestión de vulnerabilidades. La ejecución del programa contó con registros de asistencia, material fotográfico y evidencias documentales, los cuales respaldan la participación del personal y la realización efectiva de las actividades programadas.

Durante la verificación se confirmó que el contenido respondió a las necesidades del personal; sin embargo, el alcance parcial del programa y la falta de indicadores longitudinales

limitaron la validación integral de su impacto en el comportamiento y desempeño del personal técnico, como se observa en la Tabla 18.

Tabla 18
Verificación del plan de capacitación

Tema de capacitación	Resultado esperado	Resultado alcanzado	Brecha identificada
Marco NIST CSF	Comprensión general del marco	Aplicación inicial con comprensión satisfactoria	Falta de medición en desempeño real
Herramientas de detección	Uso uniforme de *OpenVAS* y antivirus	Uso parcial en sesiones prácticas	No se midió efectividad práctica
Procedimientos de respuesta a incidentes	Reducción en tiempos de reacción	Implementación parcial en ejercicios simulados	Impacto no evaluado

Nota. La verificación del plan de capacitación evidencia brechas entre los resultados esperados y los alcanzados, principalmente por el alcance parcial de la ejecución y la limitada medición del desempeño posterior, lo que restringe la evaluación integral de su efectividad.

Evaluación del programa de capacitación

En esta etapa se revisó el plan de capacitación en identificación de vulnerabilidades diseñado en la fase Hacer. Asimismo, la revisión comprendió el análisis de la pertinencia de los contenidos, la aplicabilidad de los formatos, la factibilidad del cronograma y la utilidad de los instrumentos de registro y evaluación. Para fines de validación, se evaluó el modelo de gestión propuesto mediante encuestas y observaciones realizadas al personal técnico como se muestra el en Anexo D, lo que posibilitó obtener evidencias concretas sobre la participación, el nivel de aprendizaje y la percepción institucional respecto a la capacitación planteada. La ejecución del componente de capacitación constituyó una validación práctica del modelo propuesto, al permitir medir la aceptación del personal, la transferencia de conocimientos y la factibilidad operativa de su aplicación institucional.

a. **Pertinencia de los contenidos**

   La revisión confirmó que los módulos diseñados (Introducción al NIST CSF, gestión de vulnerabilidades, herramientas de detección, respuesta a incidentes y planes de recuperación) respondían a las necesidades identificadas en el diagnóstico. La estructura secuencial

del plan permitió asegurar una progresión de conocimientos: desde lo conceptual hasta la práctica en entornos simulados.

b. **Aplicación del modelo de gestión en los formatos de capacitación**

Durante la aplicación del modelo de gestión propuesto se evaluó el funcionamiento de los distintos formatos de capacitación:

- **Talleres presenciales:** se registró una asistencia cercana al 80 % del personal convocado, destacando la participación en ejercicios prácticos.
- **Sesiones virtuales:** la totalidad del personal tuvo acceso a las sesiones, aunque se observaron diferencias en el nivel de interacción y participación.
- **Laboratorios prácticos:** se registró una asistencia del 60 %, debido a limitaciones de infraestructura; sin embargo, quienes participaron lograron un mayor nivel de aprendizaje y apropiación de contenidos.

Autoformación: se mostró que el 70 % completó el material digital, evidenciando así la necesidad de establecer métricas de seguimiento más estrictas.

c. **Cronograma temático y ejecución del programa**

El cronograma semestral (de mayo a octubre de 2025) fue revisado y se determinó que su cumplimiento resultaba factible dentro del sistema de gestión propuesto, además la evaluación del desarrollo de los módulos mes a mes evidenció que los tiempos planteados eran realistas. No obstante, se identificó la necesidad de integrar pausas de retroalimentación y sesiones de repaso con el fin de reforzar la curva de aprendizaje del personal participante tal como se muestra en la Tabla 19.

Tabla 19

Resultados de participación por módulo

Módulo	Contenido	Formato principal	Asistencia registrada	Nivel de aprendizaje alcanzado
1. Introducción al NIST CSF	Fundamentos del marco	Virtual	100 %	Alto (conceptual)
2. Gestión de vulnerabilidades	Identificación y clasificación	Taller presencial	83.33 %	Medio–Alto
3. Herramientas de detección	Uso de *OpenVAS* y SIEM	Laboratorio práctico	58.33 %	Alto (operativo)
4. Respuesta a incidentes	Escenarios de reacción	Taller práctico	75 %	Alto (operativo)
5. Recuperación de servicios críticos	RTO, RPO y planes de continuidad	Taller presencial	83.33 %	Medio–Alto
6. Evaluación de aprendizajes	Integración final y examen	Mixto	91.67 %	Validación integral

Nota. La planificación de los módulos evidencia una progresión desde contenidos conceptuales hacia actividades prácticas, con altos niveles de aprendizaje alcanzados en los módulos operativos y de evaluación final.

Tabla 20

Calificaciones obtenidas por participante en los módulos de capacitación

Participante	M1	M2	M3	M4	M5	M6	Promedio
P01	16	17	18	17	18	18	17.3
P02	15	16	17	16	17	17	16.3
P03	18	17	19	18	18	19	18.2
P04	14	15	16	15	16	16	15.3
P05	17	17	18	17	18	18	17.5
P06	16	16	17	17	17	17	16.7
P07	15	16	16	16	17	17	16.2
P08	17	18	–	17	19	19	18.0
P09	14	15	–	15	16	16	15.2
P10	16	15	–	–	17	18	16.5
P11	13	–	–	–	–	13	13.0
P12	13	–	–	–	–	–	13.0

Nota. El símbolo "–" indica que el participante no asistió al módulo correspondiente. Los promedios fueron calculados considerando únicamente los módulos efectivamente cursados por cada participante. De

los 12 participantes registrados, 10 obtuvieron calificaciones promedio iguales o superiores a 14 puntos, alcanzándose una tasa de aprobación del 83.33 %.

d. **Formatos de registro y evaluación**

La revisión de los instrumentos diseñados en los Anexos E y F evidenció que los formatos de asistencia, cuestionarios de evaluación, encuestas de satisfacción y actas de cierre permitieron proyectar un control exhaustivo del proceso. A partir de la aplicación del modelo de gestión propuesto se evidenció que:

- El 83.33 % del personal (10 de 12 participantes) alcanzó un promedio final igual o superior a 14 puntos en la escala vigesimal.
- El 16.67 % del personal (2 de 12 participantes) requirió reforzamiento en el uso de herramientas de detección y gestión de vulnerabilidades.
- El nivel de satisfacción promedio fue de 4.2/5, destacando positivamente las actividades prácticas desarrolladas en los módulos de detección, respuesta a incidentes y recuperación de servicios.
- La asistencia promedio registrada durante el programa fue superior al 80 %, evidenciando un alto compromiso del personal con las actividades de capacitación.
- Los resultados obtenidos permitieron validar la pertinencia de los contenidos desarrollados y su alineación con las necesidades identificadas en la UTI de SUNARP.

Limitaciones y áreas de mejora

La revisión hizo posible identificar ciertas limitaciones y aspectos que requieren atención en la aplicación del modelo de gestión propuesto:

- Restricción de equipos y laboratorios para atender a la totalidad del personal de manera simultánea.
- Riesgo de baja participación en los módulos de autoformación en ausencia de mecanismos de supervisión efectivos.
- Necesidad de fortalecer la parte práctica mediante ejercicios y actividades adicionales en escenarios reales de la SUNARP.

4.3.4 Fase Actuar: Mejora continua del modelo

La fase Actuar consistió en el análisis de los resultados de la verificación y en la definición de acciones correctivas y de mejora continua para optimizar el modelo de ciberseguridad basado en NIST CSF para la gestión de vulnerabilidades en la UTI de SUNARP.

Se establecieron lineamientos estratégicos que permitieron reforzar la aplicabilidad del modelo y sentar las bases para futuras implementaciones a mayor escala en la institución.

Acciones correctivas derivadas de la verificación

Con base en los resultados obtenidos en la fase Verificar, se identificaron las principales brechas y se definieron las acciones correctivas necesarias para mitigarlas tal como se presenta en la Tabla 21.

Tabla 21
Acciones correctivas propuestas

Brecha identificada	Acción correctiva	Responsable propuesto	Prioridad
Dependencia de proveedores externos en la recuperación de red	Establecer convenios de soporte con tiempos de atención garantizados con SLA	Área de Infraestructura TI	Alta
Falta de infraestructura para monitoreo centralizado	Implementar gradualmente un SIEM institucional	Equipo de Seguridad Informática	Alta
Retrasos en recuperación de servidores críticos	Plan de renovación tecnológica y adquisición de repuestos	UTI	Alta
Cobertura parcial y limitada medición del plan de capacitación	Fortalecer el programa de formación con indicadores de desempeño y mayor cobertura operativa	Oficina de RRHH y UTI	Media

Nota. Las acciones correctivas propuestas priorizan la reducción de dependencias externas, el fortalecimiento del monitoreo de seguridad y la mejora de las capacidades organizacionales mediante capacitación y renovación tecnológica.

4.4 Ajustes al modelo de ciberseguridad

Se realizaron ajustes al sistema de gestión propuesto con el fin de alinearlo mejor con las necesidades reales de la institución:

- **Función Identificar (ID):** se recomendó mantener actualizada la matriz de activos y riesgos con una periodicidad semestral.
- **Función Proteger (PR):** se incorporó la implementación de políticas claras de gestión de parches y actualizaciones automáticas.
- **Función Detectar (DE):** se planteó la integración del sistema de gestión propuesto con una plataforma SIEM en fases posteriores.
- **Función Responder (RS):** se definió un protocolo de coordinación con proveedores externos para reducir los tiempos de respuesta.
- **Función Recuperar (RC):** se sugirió fortalecer los planes de continuidad mediante ejercicios periódicos de recuperación institucional.

4.5 Propuesta de mejora continua

El sistema de gestión propuesto se concibió como un mecanismo dinámico de mejora continua, orientado a garantizar su sostenibilidad en el tiempo y su capacidad de adaptación frente a nuevas amenazas. Para ello, se definieron indicadores que permiten monitorear la eficacia de las acciones implementadas y sirven como insumo para la toma de decisiones estratégicas en la UTI de SUNARP como se observa en la Tabla 22.

La incorporación de estos indicadores no solo facilitará la evaluación periódica de los procesos de ciberseguridad, sino que también fomentará una cultura institucional de control, seguimiento y retroalimentación permanente. De esta forma, el modelo no queda limitado a una propuesta estática, sino que se transforma en un ciclo continuo de aprendizaje organizacional, capaz de detectar desviaciones y promover acciones correctivas oportunas.

Tabla 22
Indicadores de mejora continua

Indicador	Fórmula	Meta	Frecuencia de medición
Tiempo medio de detección (MTTD)	$\sum$ tiempos de detección / nº de incidentes	< 10 minutos	Mensual
Tiempo medio de respuesta (MTTR)	$\sum$ tiempos de respuesta / nº de incidentes	< 30 minutos	Mensual
Tiempo medio de recuperación (MTTRc)	$\sum$ tiempos de recuperación / nº de incidentes	≤ 2 horas	Trimestral
Porcentaje de personal capacitado	(Nº personal capacitado / total personal) × 100	100 %	Semestral
Cumplimiento de actualización de *firmware*	(Dispositivos actualizados / total dispositivos) × 100	≥ 95 %	Trimestral

Nota. Los indicadores definidos permiten evaluar de manera continua la efectividad de los controles de detección, respuesta y recuperación, así como el nivel de capacitación y mantenimiento tecnológico de la organización.

4.6 Proyección de implementación a mayor escala

La aplicación del modelo de gestión propuesto en la sede Cusco representó un punto de partida para validar su pertinencia y funcionalidad. A partir de los resultados alcanzados, se planteó una ruta de adopción progresiva que permita escalar el modelo a nivel institucional, asegurando que su implementación responda a las necesidades específicas de cada oficina registral y, al mismo tiempo, mantenga una alineación con los estándares internacionales de ciberseguridad.

La proyección considera un proceso gradual de maduración, que contempla la estandarización de buenas prácticas, la consolidación de capacidades técnicas del personal y la integración de herramientas tecnológicas avanzadas, con el fin de garantizar uniformidad y consistencia en toda la organización.

Ruta de adopción propuesta:

1. Consolidar el modelo en la sede Cusco como experiencia inicial, incorporando las mejoras identificadas en la fase de aplicación.

2. Extender progresivamente la implementación a otras sedes de la Zona Registral N.° X, ajustando el modelo a las particularidades de cada dependencia.

3. Diseñar una estrategia de despliegue nacional que integre el modelo en todas las oficinas registrales de SUNARP, considerando fases de capacitación, auditoría y retroalimentación institucional.

De esta manera, se busca que la SUNARP no solo refuerce su postura de ciberseguridad a nivel regional, sino que también se convierta en un referente nacional en la gestión de vulnerabilidades en el sector público.

CAPÍTULO V

RESULTADOS

El presente capítulo expone los resultados obtenidos durante la implementación piloto del modelo de ciberseguridad basado en los marcos NIST CSF e ISO/IEC 27001 en la UTI de la Zona Registral N.° X de SUNARP. Los resultados son presentados desde una perspectiva cuantitativa y estadística, con el propósito de evaluar el impacto del modelo sobre la continuidad operativa de la infraestructura tecnológica, el fortalecimiento de las capacidades técnicas del personal y la efectividad global de la propuesta.

Para ello, se analizaron indicadores técnicos de disponibilidad y recuperación de servicios, los resultados de las evaluaciones de capacitación realizadas al personal de TI y los contrastes estadísticos aplicados a las mediciones obtenidas antes y después de la implementación del modelo.

5.1 Evaluación técnica del impacto del modelo en la infraestructura

Con el propósito de complementar los resultados obtenidos mediante instrumentos de percepción y reducir posibles sesgos subjetivos, la efectividad del modelo de ciberseguridad fue evaluada a partir de indicadores operativos extraídos de las bitácoras de incidentes y registros de soporte técnico de la infraestructura tecnológica institucional.

La evaluación se centró en la capacidad de recuperación de los servicios críticos ante eventos de indisponibilidad, considerando métricas ampliamente utilizadas en la gestión de continuidad operativa. Entre ellas, se analizó el MTTR, el cual permite determinar el tiempo promedio requerido para restablecer un servicio afectado luego de la ocurrencia de un incidente.

El cálculo del MTTR se realizó mediante la siguiente expresión:

$$\text{MTTR} = \frac{\sum_{i=1}^{n} (T_{\text{solución},i} - T_{\text{incidente},i})}{n} \tag{5.1}$$

donde $T_{\text{incidente}}$ representa la marca temporal correspondiente al reporte inicial de la falla, $T_{\text{solución}}$ corresponde al momento en que se confirmó la recuperación del servicio y n representa el número total de incidentes registrados durante el periodo de análisis.

De manera complementaria, se evaluó el porcentaje de cumplimiento de los RTO, considerando los umbrales definidos por el modelo para cada tipo de servicio crítico. Este indicador permitió determinar el grado de alineamiento entre los tiempos reales de recuperación y las metas establecidas para garantizar la continuidad operativa.

$$\% \text{ Cumplimiento RTO} = \left(\frac{\text{Incidentes recuperados dentro del umbral}}{\text{Total de incidentes registrados}} \right) \times 100 \tag{5.2}$$

Los resultados obtenidos se presentan en la Tabla 23, donde se observa el comportamiento de los principales componentes tecnológicos evaluados durante la ejecución del piloto.

Tabla 23

Métricas técnicas de continuidad y disponibilidad en la infraestructura de red

Componente / Servicio Crítico	**RTO Objetivo**	**% Cumplimiento Real**	**MTTR Promedio Observado**
Enlaces de Red Corporativa	1 hora	60.0 %	1 h 45 min
Servidores de Datos (*Data Center*)	2 horas	65.0 %	2 h 15 min
Telefonía IP / Comunicaciones	2 horas	70.0 %	1 h 20 min
Sistemas Críticos (SIR RPV / SPRL)	4 horas	85.0 %	3 h 10 min

Nota. El porcentaje de cumplimiento real representa el grado en que los tiempos de recuperación observados alcanzaron los objetivos establecidos para cada servicio crítico. El MTTR corresponde al tiempo promedio requerido para restaurar la operación normal después de una interrupción.

Los resultados evidencian que los sistemas críticos institucionales alcanzaron los mayores niveles de cumplimiento respecto a los objetivos de recuperación establecidos, registrando un cumplimiento del 85 %. Asimismo, los servicios de telefonía IP presentaron tiempos de recuperación inferiores al umbral definido. En contraste, los enlaces de red corporativa y los servidores de datos mostraron oportunidades de mejora debido a que sus tiempos promedio de recuperación aún superan ligeramente los objetivos planteados.

En términos generales, los indicadores obtenidos reflejan una mejora en la capacidad de respuesta y recuperación de la infraestructura tecnológica, contribuyendo al fortalecimiento de la continuidad operativa institucional.

5.2 Análisis estadístico del desarrollo de capacidades técnicas

Uno de los componentes fundamentales del modelo propuesto fue el fortalecimiento de las competencias del personal técnico responsable de la gestión y operación de los servicios tecnológicos. Por esta razón, además del control de asistencia a las actividades formativas, se efectuó una evaluación de conocimientos al finalizar el programa de capacitación.

La valoración fue realizada durante el desarrollo del **Módulo 6: Evaluación de Aprendizajes**, permitiendo medir objetivamente el nivel de comprensión y apropiación de los conceptos relacionados con gestión de riesgos, controles de seguridad y continuidad operativa.

Los resultados consolidados se presentan en la Tabla 24.

Tabla 24

Estadísticos descriptivos de las calificaciones finales del personal técnico

Indicador estadístico	Valor obtenido (escala vigésimal)
Media aritmética (μ)	16.10
Mediana	16.25
Moda	17.00
Nota máxima	19.00
Nota mínima	13.00
Tasa de aprobación (%)	83.33 %

Nota. Los estadísticos descriptivos corresponden a las calificaciones finales obtenidas por el personal técnico participante en el programa de capacitación. La tasa de aprobación se calculó considerando como nota mínima aprobatoria 14 puntos en la escala vigésimal.

Los estadísticos descriptivos muestran un desempeño favorable del personal participante. La proximidad entre la media, la mediana y la moda evidencia una distribución relativamente homogénea de las calificaciones, mientras que la tasa de aprobación del 83.33 % confirma el logro de los objetivos de aprendizaje planteados para el programa de capacitación.

Estos resultados sugieren que la estrategia formativa implementada contribuyó efectivamente al fortalecimiento de las capacidades técnicas necesarias para la adopción y sostenibilidad del modelo de ciberseguridad propuesto.

5.3 Validación estadística de la efectividad del modelo

Con la finalidad de determinar si las mejoras observadas durante la fase piloto fueron consecuencia de la implementación del modelo y no producto de variaciones aleatorias, se realizaron pruebas de inferencia estadística sobre los datos obtenidos antes y después de la intervención.

El análisis contempló tanto variables relacionadas con las competencias técnicas del personal como indicadores asociados a la recuperación de servicios críticos, permitiendo evaluar integralmente los efectos del modelo en el contexto institucional.

5.3.1 Evaluación del fortalecimiento de capacidades mediante la prueba de Wilcoxon

Análisis Estadístico de la Variable: Competencias del Personal Técnico

Para corroborar la efectividad del programa de capacitación estructurado bajo el enfoque del NIST CSF y el ciclo PDCA, se procedió a contrastar el estado de las competencias técnicas del personal antes y después de la aplicación del programa. La capacitación fue desarrollada con la participación de 12 colaboradores de la Unidad de Tecnologías de la Información (UTI); sin embargo, para el análisis estadístico inferencial se seleccionó una muestra técnica de 6 participantes, conformada por el personal directamente responsable de las actividades de administración de vulnerabilidades, monitoreo de infraestructura tecnológica, soporte especializado y respuesta ante incidentes.

El conocimiento *Pre-test* se determinó a partir del formulario de diagnóstico inicial aplicado al personal técnico seleccionado, donde se evidenciaron brechas en aspectos relacionados con la identificación de vulnerabilidades, gestión de riesgos, detección de incidentes y recuperación de servicios. Por otro lado, el conocimiento *Post-test* se obtuvo a partir de las evaluaciones teóricas y prácticas consolidadas en las Actas de Cierre de los Módulos 1 al 6, donde se registró el desempeño alcanzado por los participantes en la aplicación de los conocimientos adquiridos y el uso de herramientas especializadas para la gestión de vulnerabilidades.

La Tabla 25 presenta la matriz de datos ordinales (escala de 1 a 5) correspondiente a los 6 participantes técnicos evaluados, la cual sirvió como base para el procesamiento estadístico mediante el software SPSS.

Tabla 25

Matriz de datos Pre y Post-test del nivel de competencias técnicas (N = 6)

Sujeto	Cargo / Perfil Técnico	Nivel Pre-Test	Nivel Post-Test	Dirección del Cambio
1	Analista de Redes (Sede Cusco)	1 (Inicial)	4 (Gestionado)	Positivo (+)
2	Operador UTI (Sede Cusco)	1 (Inicial)	4 (Gestionado)	Positivo (+)
3	Analista de Redes (Sede Quillabamba)	1 (Inicial)	5 (Optimizado)	Positivo (+)
4	Técnico de Soporte Informático	1 (Inicial)	4 (Gestionado)	Positivo (+)
5	Administrador de Servidores	1 (Inicial)	5 (Optimizado)	Positivo (+)
6	Operador de Sistemas de Red	1 (Inicial)	4 (Gestionado)	Positivo (+)

Nota: Escala de medición basada en niveles de madurez y competencias del modelo propuesto (1: Inicial, 5: Optimizado). Fuente: Formulario de diagnóstico de la UTI y actas de cierre de capacitación.

Al procesar la información de la Tabla 25 mediante la prueba de Rangos con Signo de Wilcoxon, se constató que no existieron rangos negativos ni empates, reflejando una mejora uniforme en las competencias técnicas de los participantes seleccionados.

Para analizar la evolución de las competencias técnicas de la muestra técnica seleccionada ($n = 6$), se empleó la prueba no paramétrica de rangos con signo de Wilcoxon, considerando un nivel de significancia de $\alpha = 0{,}05$.

El hecho de que los 6 participantes de la muestra técnica hayan mostrado una mejora positiva, sin rangos negativos ni empates (0 rangos negativos y 6 positivos, según se reporta en la Tabla 26), se explica por tres factores identificables en el propio diseño del piloto. En primer lugar, la Tabla 25 muestra que los 6 participantes partieron del mismo nivel basal más bajo de la escala (Nivel 1: Inicial), lo que genera un efecto de piso (*floor effect*): al no existir un nivel inferior posible, la probabilidad de observar un cambio negativo era nula, y cualquier progreso en el desempeño se traduce necesariamente en una dirección de cambio positiva. En segundo lugar, la capacitación no fue una intervención general, sino un programa estructurado de 6 módulos dirigido específicamente a las competencias medidas en el Pre-test y el Post-test

(identificación de vulnerabilidades, gestión de riesgos, detección de incidentes y recuperación de servicios), lo que incrementa la probabilidad de un efecto positivo consistente. En tercer lugar, se reconoce como limitación metodológica que la evaluación Post-test fue realizada mediante las actas de cierre del propio programa de capacitación, sin un grupo de control ni un evaluador externo independiente, por lo que el resultado, si bien estadísticamente significativo (p = 0,026), debe interpretarse con cautela respecto de un posible sesgo del evaluador, y se recomienda que investigaciones futuras repliquen esta evaluación incorporando un grupo de control y un evaluador externo.

Tabla 26

Estadísticos de contraste de la prueba de Wilcoxon para Competencias Técnicas

Estadístico de Contraste	Post-test - Pre-test
Z	-2.232[a]
Asymp. Sig. (bilateral)	0.026

[a] Basado en rangos negativos.
Fuente: Elaboración propia a partir de los datos obtenidos en el formulario de diagnóstico y las actas de cierre de capacitación.

Como se observa en la Tabla 26, el valor de significancia obtenido fue de $p = 0{,}026$, inferior al nivel crítico de $\alpha = 0{,}05$. En consecuencia, se concluye que existe evidencia estadísticamente significativa de mejora en las competencias técnicas del personal después de la aplicación del programa de capacitación.

Este resultado indica que los participantes fortalecieron sus conocimientos en aspectos relacionados con la identificación de vulnerabilidades, gestión de riesgos, detección de incidentes y mecanismos de recuperación de servicios, contribuyendo al cumplimiento de los objetivos planteados por el modelo de ciberseguridad basado en NIST CSF e ISO/IEC 27001.

Justificación Metodológica de la Muestra y Poder de la Prueba de Wilcoxon

Aunque el programa de capacitación fue desarrollado con la participación de 12 colaboradores de la UTI, la evaluación inferencial se realizó sobre una muestra técnica de 6 participantes seleccionados mediante muestreo no probabilístico por criterio. Esta selección estuvo conformada por especialistas cuyas funciones se encuentran directamente relacionadas con la gestión de vulnerabilidades, monitoreo de infraestructura tecnológica, administración de redes, soporte especializado y respuesta ante incidentes de seguridad.

La elección de esta muestra permitió evaluar el impacto del modelo propuesto sobre el grupo de trabajo responsable de ejecutar los procedimientos operativos asociados a la identificación, detección, respuesta y recuperación frente a incidentes de ciberseguridad. Asimismo, permitió concentrar el análisis en los perfiles con mayor incidencia en la operación y sostenibilidad del modelo implementado.

Considerando el tamaño reducido de la muestra y la naturaleza ordinal de los datos obtenidos, se utilizó la prueba no paramétrica de Rangos con Signo de Wilcoxon, recomendada para estudios con muestras pequeñas y distribuciones cuya normalidad no puede garantizarse.

Al procesar las puntuaciones obtenidas mediante el software estadístico SPSS, se identificaron 0 rangos negativos y 6 rangos positivos, obteniéndose un estadístico de contraste $Z = -2{,}232$ y un valor de significancia bilateral de $p = 0{,}026$. Dado que este valor es inferior al nivel de significancia establecido ($\alpha = 0{,}05$), se concluye que el programa de capacitación generó una mejora estadísticamente significativa en las competencias técnicas del personal evaluado.

Los resultados obtenidos respaldan la efectividad del componente de capacitación del modelo propuesto y evidencian su contribución al fortalecimiento de las capacidades institucionales para la gestión de vulnerabilidades, en concordancia con los lineamientos establecidos por el marco NIST CSF y la norma ISO/IEC 27001.

La objetividad de los resultados obtenidos con la muestra técnica de 6 participantes se sustenta en dos elementos. Primero, la evaluación Pre-test y Post-test se aplicó bajo los mismos instrumentos y la misma rúbrica de calificación tanto a los 6 participantes de la muestra técnica como a los 12 participantes del programa completo (Anexo E), sin diferenciar criterios de evaluación entre ambos grupos, lo que evita un sesgo de selección en la forma de medir el desempeño. Segundo, la selección de los 6 participantes respondió a un criterio funcional predefinido antes de la evaluación (personal directamente responsable de la gestión de vulnerabilidades, monitoreo, soporte y respuesta ante incidentes), y no a una selección posterior basada en los resultados obtenidos, lo que descarta que la muestra haya sido escogida por mostrar mejores resultados. No obstante, se reconoce como limitación metodológica que el tamaño reducido de la muestra (n = 6) restringe la validez externa de los resultados, por lo que estos deben interpretarse como evidencia preliminar del efecto del modelo en el grupo evaluado, y

no como una generalización automática a la totalidad del personal técnico de la UTI.

5.3.2 Evaluación de los tiempos de recuperación operativa mediante la prueba t de Student

Respecto a la variable cuantitativa correspondiente a los tiempos de recuperación de servicios críticos, previamente se verificó el supuesto de normalidad mediante la prueba de Shapiro-Wilk, obteniéndose un valor de $p = 0{,}214$, superior al nivel de significancia establecido.

Al cumplirse dicho supuesto, se aplicó la prueba t de Student para muestras relacionadas sobre una muestra emparejada de diez categorías de incidentes registradas en las bitácoras institucionales.

Tabla 27
Resultados de la prueba t-Student para muestras relacionadas (RTO en minutos)

Comparación de Medias	Media	Desv. Est.	t	gl	Sig. (bilateral)
Tiempo RTO PRE – Tiempo RTO POST	136.80	114.53	3.778	9	0.004

Fuente: Elaboración propia a partir del procesamiento de datos de incidentes históricos de red.

Los resultados expuestos en la Tabla 27 muestran un estadístico de contraste de $t(9) = 3{,}778$ con un nivel de significancia de $p = 0{,}004$. Dado que este valor es inferior a 0.01, se concluye que existen diferencias estadísticamente significativas entre los tiempos de recuperación observados antes y después de la implementación del modelo.

5.4 Análisis de brechas operativas y discusión de factores críticos

Si bien el contraste estadístico confirma una reducción significativa en los tiempos globales de indisponibilidad ($p = 0{,}004$), la evaluación técnica desagregada expuesta en la Tabla 23 revela que ciertos componentes estructurales aún muestran brechas respecto a las metas ideales del modelo. Específicamente, los enlaces de Red Corporativa y los *Data Center* registraron un cumplimiento real del RTO del 60.0 % y 65.0 % respectivamente, con los MTTR que superaron ligeramente los umbrales de 1 y 2 horas planificados.

Un análisis cualitativo y documental detallado de las bitácoras de incidentes de red permite

identificar que estas desviaciones no responden a deficiencias en el diseño procedimental del modelo, sino a factores exógenos e infraestructurales preexistentes en la UTI:

- **Dependencia de proveedores externos y contingencias de última milla:** Los registros de caídas de los enlaces de red evidencian que una alta proporción de los eventos de indisponibilidad prolongada estuvo asociada a averías masivas de la Red Nacional de Fibra Óptica (contingencias operadas por *PRONATEL* o caídas de infraestructura de enlaces del proveedor *Plasmatronics*). Incidentes críticos como rupturas de fibra óptica o degradaciones severas de enlaces intermitentes limitaron la capacidad de respuesta inmediata del equipo técnico interno, supeditando el restablecimiento definitivo del servicio a los SLA de terceros.

- **Obsolescencia tecnológica en el equipamiento crítico:** La revisión del inventario de activos institucionales y las encuestas aplicadas al personal de TI determinaron que un porcentaje considerable del hardware crítico en producción presenta obsolescencia tecnológica (con tiempos de compra que remontan al año 2015 en servidores *rack* clave o switches de borde con desgaste operativo continuado). Esta condición de obsolescencia se traduce directamente en fallas recurrentes de hardware, bloqueos de memoria y dificultades para el aprovisionamiento inmediato de repuestos, incrementando de forma inevitable el MTTR promedio observado en el *Data Center* (2h 15m).

- **Curva de adopción operativa de las capacidades técnicas:** Aunque el programa de capacitación cerró con una tasa de aprobación teórica del 83.33 % y una media sobresaliente de 16.10 puntos, la bitácora del piloto consignó que, ante incidentes de alta complejidad, algunos participantes requirieron asistencia guiada o recurrieron a flujos tradicionales reactivos antes de la plena interiorización de las herramientas automatizadas (como el escáner de vulnerabilidades *OpenVAS* o el monitoreo SIEM). Esto corrobora que la transferencia de capacidades técnicas requiere un proceso de maduración progresiva y simulaciones periódicas en entornos reales para consolidar la agilidad operativa que demandan los RTO más estrictos.

A pesar de estas limitaciones físicas y logísticas, la implementación teórica y el despliegue

del piloto demostraron una optimización proyectada cercana al 30 % en los tiempos de mitigación si se compara con el histórico institucional sin directrices normativas. En consecuencia, se determina que el modelo adaptado del NIST CSF e ISO/IEC 27001 es técnicamente viable y altamente efectivo para coordinar la primera respuesta y el aislamiento de amenazas, requiriendo de manera complementaria una renovación gradual de la infraestructura de hardware y la formalización de contratos de contingencia de red para alcanzar los niveles óptimos de resiliencia operativa institucional.

Por tanto, la evidencia empírica respalda la efectividad de la propuesta, demostrando que la adopción de controles alineados con ISO/IEC 27001 y las funciones de recuperación del NIST CSF contribuyó significativamente a reducir los tiempos de indisponibilidad de los servicios críticos y fortalecer la continuidad operativa de la infraestructura tecnológica institucional.

La atribución de las brechas remanentes a factores exógenos, y no al diseño del modelo, se sustenta en un criterio analítico explícito: se compararon los componentes evaluados (Tabla 22) según el grado de control operativo que el personal de la UTI ejerce sobre cada uno. Los sistemas críticos institucionales (SIR RPV y SPRL), cuya operación y mantenimiento dependen directamente del personal técnico de la UTI, alcanzaron el mayor cumplimiento de RTO (85,0 %); en cambio, los enlaces de red corporativa y los servidores de datos, cuyo funcionamiento depende parcialmente de proveedores externos de conectividad y de hardware con fecha de adquisición previa al inicio de esta investigación (2015, según el Anexo C), presentaron los cumplimientos más bajos (60,0 % y 65,0 %). Esta correspondencia entre el grado de control operativo disponible y el nivel de cumplimiento alcanzado —contrastada con la evidencia documental de las bitácoras de incidentes de red (Anexo G), que registran de manera explícita las fechas y causas de las interrupciones atribuidas a proveedores externos— constituye el criterio metodológico utilizado para diferenciar las limitaciones atribuibles a factores exógenos preexistentes de las que serían atribuibles al diseño o a la aplicación del modelo propuesto.

DISCUSIONES

El análisis de los resultados obtenidos tras el diagnóstico y la aplicación del piloto controlado del Modelo de Ciberseguridad para la Gestión de Vulnerabilidades (MCGV) permite contrastar los hallazgos empíricos con la literatura científica y los antecedentes normativos considerados en el marco teórico.

El diagnóstico inicial de la UTI de SUNARP – Sede Cusco reveló que un 50 % del personal técnico carecía de formación formal en gestión de vulnerabilidades, lo que se traducía en una administración predominantemente reactiva y dependiente del soporte de proveedores externos para la atención de incidentes críticos. Esta realidad concuerda con lo expuesto por Tøndel *et al.* (2021), quien argumenta que las organizaciones gubernamentales suelen priorizar la operatividad inmediata sobre la gestión proactiva de riesgos, perpetuando brechas en las capacidades internas del personal. Asimismo, la alta recurrencia de caídas de red y fallas de hardware identificadas en los reportes históricos y en la bitácora de red (Anexos F y G) se observó de manera empírica junto con la falta de inventarios dinámicos y actualizados por criticidad, sin que se haya calculado un coeficiente estadístico de correlación entre ambas variables; esta asociación empírica es consistente con lo señalado por **?**, quien indica que más del 60 % de las vulnerabilidades detectadas en sistemas de información gubernamentales se deben a la ausencia de visibilidad y control sobre los activos tecnológicos, un escenario que se replicaba de forma similar en la UTI antes de la formulación de esta propuesta.

La integración de las funciones del NIST CSF (Identificar, Proteger, Detectar, Responder y Recuperar) con el ciclo PDCA demostró ser una alternativa viable para estructurar la ciberseguridad en la institución. La validación en el entorno controlado, sustentada en la prueba de Wilcoxon ($Z = -2{,}232$; $p = 0{,}026$, Tabla 26), evidenció una mejora estadísticamente significativa en las competencias técnicas del personal evaluado. Estos resultados respaldan la postura de Behl (2021), quien afirma que los marcos de ciberseguridad no deben ser vistos como estándares rígidos, sino como herramientas adaptables que impulsan la madurez organizacional de manera progresiva. Además, la complementariedad de los controles específicos de la norma

ISO/IEC 27001:2022 robusteció la fase de Planificar y Hacer, cerrando brechas operativas que los instructivos internos previos de la institución (SUNARP, 2021) no alcanzaban a mitigar por su enfoque estrictamente general.

Uno de los hallazgos más significativos del piloto controlado fue la evaluación de los mecanismos de recuperación para servicios críticos. Aunque se establecieron tiempos objetivo estrictos (RTO de 2 horas para servidores y 1 hora para red corporativa), la medición real mostró un cumplimiento del 60,0 % en los enlaces de red corporativa y del 65,0 % en los servidores de datos, frente al 85,0 % alcanzado en los sistemas críticos SIR RPV y SPRL (Tabla 23). Un análisis documental de las bitácoras de incidentes de red permite atribuir estas brechas remanentes a factores exógenos e infraestructurales —y no a deficiencias del modelo—, en particular a la dependencia de proveedores externos de conectividad (contingencias de la Red Nacional de Fibra Óptica y del proveedor Plasmatronics) y a la obsolescencia de hardware crítico con fecha de adquisición registrada en el inventario institucional (Anexo C) desde 2015. Esta atribución se sustenta en que las brechas se concentran precisamente en los componentes donde las bitácoras documentan eventos de causa externa, mientras que los componentes bajo control directo del personal de la UTI alcanzaron los niveles de cumplimiento más altos (85,0 %), lo que evidencia que el desempeño del modelo varía en función del grado de control operativo disponible y no de su diseño. La prueba t de Student aplicada sobre las diez categorías de incidentes registradas ($t(9) = 3{,}778$; $p = 0{,}004$, Tabla 27) confirma una reducción estadísticamente significativa en los tiempos de recuperación globales, resultado consistente con los hallazgos de **?**, quien resalta que la formalización de procedimientos y el entrenamiento continuo disminuyen el impacto de los incidentes de seguridad incluso en entornos con limitaciones presupuestarias o de equipamiento.

Finalmente, la proyección de una ruta de adopción progresiva —iniciando en la sede Cusco, escalando a la Zona Registral N.° X y proyectándose a nivel nacional— responde a la necesidad de construir una cultura de ciberseguridad sostenible en el aparato estatal. Esta estrategia se alinea con las recomendaciones expresadas por Almagro (2019), donde se enfatiza que el fortalecimiento de las capacidades de defensa digital en las instituciones públicas debe ser un proceso incremental, descentralizado y adaptado a las realidades operativas de cada región geográfica.

CONCLUSIONES

1. La adaptación e implementación piloto del MCGV, basado en el NIST CSF v1.1 y la norma ISO/IEC 27001:2022, fortaleció de manera estadísticamente significativa tanto las competencias técnicas del personal como los tiempos de recuperación operativa de la UTI de SUNARP – Sede Cusco. La prueba t de Student para muestras relacionadas arrojó un valor de p = 0,004, evidenciando una reducción significativa en los tiempos de RTO, mientras que la prueba de Wilcoxon confirmó una mejora en las competencias técnicas del personal (p = 0,026), lo que evidencia una transición viable de un esquema operativo reactivo hacia uno gestionado, dentro del alcance piloto delimitado en el numeral 1.5.

2. El diagnóstico integral evidenció que la gestión de vulnerabilidades en la UTI es predominantemente reactiva y presenta brechas estructurales: inventarios de activos desactualizados, obsolescencia tecnológica en el hardware crítico (con equipos adquiridos desde 2015, según el Anexo C), ausencia de herramientas de monitoreo centralizado y dependencia de soporte externo. El 50 % del personal técnico carecía de formación formal en gestión de vulnerabilidades, lo que ampliaba la superficie de exposición institucional.

3. Las funciones del NIST CSF más relevantes para el contexto institucional resultaron ser Identificar, Detectar y Responder, dado que las brechas operativas detectadas se concentraron en estas áreas. El diagnóstico situó a la organización en un nivel intermedio de madurez; la integración de los controles de ISO/IEC 27001:2022 complementó el enfoque del NIST CSF y aportó estructura formal a las fases de Planificar y Hacer del ciclo PDCA.

4. El esquema de priorización de vulnerabilidades diseñado, basado en la criticidad del activo, la probabilidad de ocurrencia y el impacto de la amenaza, resultó eficaz para estructurar la toma de decisiones técnicas. Los sistemas críticos institucionales (SIR RPV y SPRL) alcanzaron el mayor nivel de cumplimiento de RTO (85 %), mientras que los enlaces de red corporativa y los servidores de datos presentaron cumplimientos de 60 %

y 65 % respectivamente, limitados por factores exógenos —dependencia de proveedores externos y obsolescencia del equipamiento— y no por deficiencias en el diseño del modelo, según se sustenta en el numeral 5.4.

5. El programa de capacitación estructurado bajo el ciclo PDCA y las funciones del NIST CSF generó una mejora estadísticamente significativa en las competencias técnicas del personal evaluado ($Z = -2{,}232$; $p = 0{,}026$). Los seis participantes de la muestra técnica seleccionada transitaron de un nivel inicial (nivel 1) a niveles gestionado u optimizado (niveles 4 y 5); de los 12 participantes del programa completo, el 83,33 % alcanzó una calificación promedio igual o superior a 14 puntos (media = 16,10), con una satisfacción promedio de 4,2/5. Estos resultados deben interpretarse considerando el tamaño reducido de la muestra estadística ($n = 6$) y el diseño preexperimental sin grupo de control, características que se detallan como limitación metodológica en el numeral 5.3.1.

6. Los mecanismos de recuperación estructurados bajo métricas de RTO, junto con la integración operativa de herramientas de monitoreo como OpenVAS y la proyección de un SIEM institucional, se asociaron a una reducción estadísticamente significativa en los tiempos de recuperación de servicios críticos ($t(9) = 3{,}778$; $p = 0{,}004$), con una diferencia de medias de 136,80 minutos entre el pre y el post intervención. Esta mejora está condicionada a una renovación gradual de la infraestructura de hardware y a la formalización de contratos de contingencia de red con proveedores externos, factores exógenos al modelo que constituyen su principal restricción operativa.

RECOMENDACIONES

- Se recomienda desarrollar futuras investigaciones que amplíen el modelo propuesto hacia el diseño, implementación y evaluación integral de un SGSI, considerando la totalidad de los requisitos establecidos en la ISO/IEC 27001:2022, incluyendo el contexto organizacional, liderazgo, planificación, gestión de riesgos, declaración de aplicabilidad, operación, evaluación del desempeño y mejora continua. Esta línea permitiría estudiar la articulación integral entre el NIST CSF, el ciclo PDCA y los requisitos de la norma, considerando que la presente investigación se concentró principalmente en aquellos controles y procesos relacionados con la gestión de ciberseguridad dentro del ámbito delimitado del estudio.

- Se recomienda realizar investigaciones que analicen la evolución del modelo desarrollado en la presente tesis hacia el NIST CSF 2.0, incorporando la función *Govern* (Gobernar) y evaluando su relación con las funciones *Identify*, *Protect*, *Detect*, *Respond* y *Recover*. Asimismo, futuras investigaciones podrían determinar cómo esta nueva estructura se articula con los requisitos y controles de la ISO/IEC 27001:2022 y con las etapas del ciclo PDCA, con el propósito de establecer un modelo integrado de mayor alcance para la gestión de la ciberseguridad en entidades públicas.

- Se recomienda desarrollar investigaciones de tipo longitudinal que evalúen la evolución de los resultados obtenidos durante periodos prolongados, permitiendo determinar si las mejoras observadas en la gestión de vulnerabilidades, detección, respuesta, recuperación y desempeño de los controles se mantienen en el tiempo. Este tipo de estudios permitiría complementar la evaluación realizada en la presente investigación y analizar la evolución de la madurez de ciberseguridad mediante mediciones periódicas de indicadores técnicos y de gestión.

- Se recomienda realizar investigaciones comparativas que repliquen el modelo propuesto en diferentes sedes, oficinas o entidades públicas con características distintas de infraestructura tecnológica, tamaño, conectividad, criticidad de servicios y nivel de madurez en

ciberseguridad. Esto permitiría determinar la capacidad de generalización del modelo, identificar los factores que condicionan su aplicabilidad y establecer qué componentes requieren adaptación según el contexto organizacional.

- Se recomienda desarrollar investigaciones que complementen la evaluación cualitativa de riesgos utilizada en la presente investigación mediante métodos cuantitativos o semi-cuantitativos. Como líneas futuras podrían analizarse modelos como *Factor Analysis of Information Risk* (FAIR) u otras metodologías de cuantificación del riesgo, incorporando variables relacionadas con probabilidad de ocurrencia, impacto económico, criticidad de activos, exposición, frecuencia de incidentes y tiempo de recuperación. Esto permitiría comparar los resultados obtenidos mediante diferentes enfoques de valoración y determinar cuál proporciona mayor capacidad para apoyar la toma de decisiones en materia de ciberseguridad.

- Se recomienda desarrollar investigaciones orientadas al diseño y evaluación de soluciones automatizadas que integren el inventario de activos, identificación de vulnerabilidades, priorización de riesgos, seguimiento de remediación y monitoreo de eventos de seguridad. Asimismo, podrían estudiarse arquitecturas que incorporen tecnologías SIEM y *Security Orchestration, Automation and Response* (SOAR) para analizar la capacidad de automatizar la correlación de eventos, generación de alertas y respuesta ante incidentes. Esta línea permitiría profundizar los procesos tecnológicos abordados en la presente investigación y evaluar experimentalmente el impacto de la automatización sobre indicadores como tiempo de detección, tiempo de respuesta y tiempo de recuperación.

BIBLIOGRAFÍA

Almagro, L. (2019). *Un abordaje integral de la Ciberseguridad*.

Alshaikh, M. (2020a). *Cybersecurity Risk Management Framework for Government Information Systems Based on the NIST Cybersecurity Framework. International Journal of Computer Science and Information Security*, 18(3):1–10.

Alshaikh, M. (2020b). *Developing cybersecurity culture to influence employee behavior: A practice perspective*. *Computers & Security*, 98:102003.

Argüezo Ramirez, E. D. (2019). *Propuesta de un Sistema de Gestión de Seguridad de Información para la protección de activos de información basado en la norma ISO 27001 en el área de informática de la Municipalidad Provincial de Huánuco*.

Behl, A. (2021). *Integrating the NIST Cybersecurity Framework and ISO/IEC 27001 for Vulnerability Management in Public Sector Organizations*. *Journal of Information Security and Applications*, 58:102718.

Betancourt, D. (2018). *Ciclo de Deming (PDCA): Qué es y cómo logra la mejora continua*.

Calderon Aquiño, C. J. (2022). *Modelo de Sistema de Ciberseguridad para la Gestión de Riesgo de una Empresa de Matizados de Pintura de Lima*.

Cordova Facundo, Y. y Rodriguez Polo, J. A. (2023). *Modelo de ciberseguridad para mejorar la seguridad de la información*.

Demirkan, S., Demirkan, I., y Mckee, A. (2020). *Blockchain technology in the future of business cyber security and accounting*. *Journal of Management Analytics*, pp. 189–208.

European Union Agency for Cybersecurity (2023). *ENISA Threat Landscape 2023*.

Falcon Fernández, J. A. (2021). *Propuesta de implementación de un sistema de Gestión de Seguridad de la información basado en la norma ISO 27001 para una empresa de Telecomunicaciones*.

Flores Callejas, J., Afifi, A., y Lozinskiy, N. (2021). *La ciberseguridad en las organizaciones del sistema de las Naciones Unidas*.

Hanacek, N. (2018). *NIST releases version 1.1 of its popular Cybersecurity Framework.* NIST.

Hernández Sampieri, R. y Mendoza Torres, C. P. (2018). *Metodología de la Investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill Interamericana.

ISO/IEC (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*.

Jara Fuentealba, N. y Jorquera Cruz, A. (2021). *La responsabilidad de la Administración del Estado por incidentes de ciberseguridad. Revista Chilena de Derecho y Tecnología*, pp. 201–230.

Lindemulder, G. (2024). *¿Qué es la Ciberseguridad?*

López Fernández, J. L. (2017). *Análisis y Gestión de vulnerabilidades de sistemas informáticos con software libre (AGVISL)*.

Méndez Gálvez, C. (2020). *Desarrollo de un plan de seguridad de la información basado en estándares para empresa de seguros*.

National Institute of Standards and Technology (2018). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)*.

NIST CSWP (2024). *The NIST Cybersecurity Framework (CSF) 2.0*.

NQA (2024). *Guía de implementación de Sistemas de Gestión de Seguridad de la Información*.

Peñafiel, K. A. (2021). *Factors that determine computer vulneration and the development. Revista Científica*, 21.

Presidencia del Consejo de Ministros (2021). *Política Nacional de Gobierno Digital al 2030*.

Ramirez Vargas, J. A. y Pereda Otero, L. R. (2023). *Propuesta de implementación de un modelo de ciberseguridad basado en el marco NIST v1.1*.

Saeckel, A. (2023). *Gestión de la vulnerabilidad en el contexto de la norma ISO 27001*.

Santiago, H. (2018). *Herramientas para la gestión de calidad*.

Scarfone, K. y Mell, P. (2012). *Guide to Vulnerability Assessment*.

Siegel, S. y Castellan, N. J. (1995). *Estadística no paramétrica aplicada a las ciencias de la conducta*. Trillas.

SUNARP (2021). *Instructivo de evaluación y tratamiento de riesgos del sistema de gestión de seguridad de la información*.

Tomaylla Castillo, A. J. y Balbin Balbin, W. (2024). *Propuesta de Implementación del Framework NIST CSF 1.1 para una entidad gubernamental*.

Tøndel, I. A., Line, M. B., y Jaatun, M. G. (2021). *Information security incident management: Current practice as reported in the literature*. *Computers & Security*, 102:102164.

Triola, M. F. (2018). *Estadística*. Pearson, 12 edición.

Walpole, R. E., Myers, R. H., Myers, S. L., y Ye, K. (2012). *Probabilidad y estadística para ingeniería y ciencias*. Pearson, 9 edición.

Yánez Intriago, J. A. (2022). *Aplicación del NIST Cybersecurity Framework en el Instituto Superior Tecnológico Sucre*.

ANEXOS

A. Matriz de consistencia

Problema	Objetivos	Hipótesis	Variables / Indicadores	Metodología
Problema General: ¿De qué manera la implementación de un modelo basado en el NIST CSF mejora la gestión de vulnerabilidades en la UTI de SUNARP - Sede Cusco?	**Objetivo General:** Proponer un modelo basado en el NIST CSF para mejorar la gestión de vulnerabilidades en la UTI de SUNARP.	La implementación del modelo basado en el NIST CSF mejora significativamente la gestión de vulnerabilidades en la UTI de SUNARP.	**Variable Independiente:** Modelo NIST CSF **Variable Dependiente:** Gestión de vulnerabilidades **Indicadores:** - Identificación de activos - Detección de vulnerabilidades - Tiempo de respuesta - Nivel de riesgo	Tipo: Aplicada Nivel: Descriptivo - Propositivo Método: Analítico Técnicas: - Encuesta - Análisis documental Instrumentos: - Cuestionario - Ficha de registro
Problema Específico 1: ¿Cuál es el estado actual de la gestión de vulnerabilidades en la UTI de SUNARP?	**Objetivo Específico 1:** Diagnosticar el estado actual de la gestión de vulnerabilidades.	La identificación del estado actual permite evidenciar las principales brechas en la gestión de vulnerabilidades.	Indicadores: - Inventario de activos - Incidentes registrados - Nivel de conocimiento del personal	Técnicas: - Encuesta - Revisión documental
Problema Específico 2: ¿Qué criterios del NIST CSF son aplicables a la gestión de vulnerabilidades?	**Objetivo Específico 2:** Identificar los criterios del NIST CSF aplicables.	La aplicación de los criterios del NIST CSF permite estructurar la gestión de vulnerabilidades.	Indicadores: - Cumplimiento de funciones (ID, PR, DE, RS, RC) - Nivel de alineación con ISO 27001	Técnica: - Análisis comparativo

Continúa en la siguiente página

Problema	Objetivos	Hipótesis	Variables / Indicadores	Metodología
Problema Específico 3: ¿Cómo priorizar las vulnerabilidades según su nivel de riesgo?	**Objetivo Específico 3:** Diseñar un esquema de priorización de vulnerabilidades.	La priorización basada en impacto y probabilidad mejora la asignación de recursos.	Indicadores: - Nivel de riesgo - Clasificación (Crítico, Alto, Medio, Bajo)	Técnica: - Análisis de riesgos
Problema Específico 4: ¿Cómo fortalecer las capacidades del personal en la identificación de vulnerabilidades?	**Objetivo Específico 4:** Proponer estrategias de capacitación.	La capacitación mejora la detección temprana de vulnerabilidades.	Indicadores: - Nivel de conocimiento - Participación en capacitaciones	Técnica: - Encuesta
Problema Específico 5: ¿Cómo mejorar la recuperación de los servicios críticos?	**Objetivo Específico 5:** Definir mecanismos de recuperación.	La implementación de planes de recuperación reduce el tiempo de inactividad.	Indicadores: - RTO - Continuidad del servicio	Técnica: - Análisis técnico

B. Cuestionario aplicado al personal de la UTI

1. ¿Qué tipo de activos tecnológicos (*hardware/red*) son considerados críticos para la operación diaria?
2. ¿Existe un inventario actualizado de estos activos?¿Cada cuánto se actualiza?
3. ¿Con qué se realiza mantenimiento o evaluación de riesgos a los equipos de red y hardware?
4. ¿Tienen un procedimiento establecido para identificar vulnerabilidades en dispositivos (por ejemplo, *firmware* desactualizado, puertos abiertos)?
5. ¿Qué tipos de herramientas utilizan para detectar o prevenir vulnerabilidades?
6. ¿Tienen conocimiento del marco NIST CSF o alguna norma relacionada con seguridad de la información?
7. ¿Se ha presentado algún incidente reciente relacionado con fallas de hardware o de red?¿Cómo fue gestionado?
8. ¿Hay políticas o manuales internos que orienten sobre cómo actuar frente a vulnerabilidades o amenazas tecnológicas?
9. ¿Han recibido capacitación en gestión de vulnerabilidades?¿Con qué frecuencia?
10. ¿Qué mejoras consideraría necesarias en cuanto a la gestión actual de vulnerabilidades?

Se adjunta el link de las respuestas del cuestionario realizado al personal de la UTI - SUNARP.

`https://docs.google.com/spreadsheets/d/1A5RTtJ1BPf5kD0rbamNZRZK2dPIhZ8c6XZCVM8-2H`
`edit?usp=sharing`

C. Inventario de activos tecnológicos

Cod. Patr.	Bien	Marca	Modelo	Serie	Estado	Ubicación
0038	SERVIDOR TIPO RACK	LENOVO	SYSTEM X3650M5	EZZB224	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - DATA CENTER
10035	IMPRESORA DE ETIQUETA - IMPRESORA DE TICKET	EPSON	TH-H6000V-054	X83P002731	ACTIVO	CENTRO MAC CUSCO - MODULO DE ATENCION SUNARP
10065	SWITCH PARA RED - DE BORDE DE 24 PUERTOS	HP	2930F-24G+POE+4SFP+	TW08HKW0VJ	ACTIVO	OFICINA REGISTRAL CUSCO 1ER PISO - ARCHIVO
10066	SWITCH PARA RED - DE BORDE DE 24 PUERTOS	HP	2930F-24G+POE+4SFP+	TW0BHKW2KF	ACTIVO	OFICINA REGISTRAL CUSCO 1ER PISO - ARCHIVO
10067	SWITCH PARA RED - DE BORDE DE 24 PUERTOS	HP	2930F-24G+POE+4SFP+	TW11HKW1GJ	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - RACK
10068	SWITCH PARA RED - DE BORDE DE 24 PUERTOS	HP	2930F-24G+POE+4SFP+	TW11HKW1S4	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - RACK
10069	SWITCH PARA RED - DE BORDE DE 24 PUERTOS	HP	2930F-24G+POE+4SFP+	TW0AHKW2KG	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - PUBLICIDAD
10070	SWITCH PARA RED - DE BORDE DE 24 PUERTOS	HP	2930F-24G+POE+4SFP+	TW0AHKW2MG	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - RACK
10071	SWITCH PARA RED - DE BORDE DE 48 PUERTOS	HP	2930F-24G+POE+4SFP+	TW0AHKX1V0	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - RACK
10072	SWITCH PARA RED - DE BORDE DE 48 PUERTOS	HP	2930F-48G+POE+4SFP+	TW0AHKX1Y6	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CATASTRO REGISTRAL
10073	SWITCH PARA RED - PRINCIPAL (CORE) DE 24 SLOTS	HP	3810M-24SFP+250W	SG07K450MQ	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - DATA CENTER
10074	SWITCH PARA RED - PRINCIPAL (CORE) DE 24 SLOTS	HP	3810M-24SFP+250W	SG09K450M4	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - DATA CENTER

Continúa en la siguiente página

Cod. Patr.	Bien	Marca	Modelo	Serie	Estado	Ubicación
10091	IMPRESORA LASER	LEXMARK	MS823DN	4064845013M1F	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS 03
10099	IMPRESORA LASER	LEXMARK	MS823DN	4064845013M7D	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - PUBLICIDAD
10104	IMPRESORA LASER	LEXMARK	MS823DN	4064845013M20	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - PUBLICIDAD
10105	SISTEMA DE PROTECCION Y SEGURIDAD PARA RED - FIREWALL	FORTINET	FORTIGATE 601E	FG6H1ETB20907118	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - DATA CENTER
10106	SISTEMA DE PROTECCION Y SEGURIDAD PARA RED - FIREWALL	FORTINET	FORTIGATE 601E	FG6H1ETB20907226	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - DATA CENTER
10110	EQUIPO MULTIFUNCIONAL COPIADORA IMPRESORA SCANNER	LEXMARK	MX722ADHE	74641101246GR	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - TRAMITE FEDATARIO
10115	EQUIPO MULTIFUNCIONAL COPIADORA IMPRESORA SCANNER	LEXMARK	MX722ADHE	7464045023RCZ	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS 01
10116	EQUIPO MULTIFUNCIONAL COPIADORA IMPRESORA SCANNER	LEXMARK	MX722ADHE	7464045023R9D	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CATASTRO REGISTRAL
10121	EQUIPO MULTIFUNCIONAL COPIADORA IMPRESORA SCANNER	LEXMARK	MX722ADHE	7464045023RCN	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - PUBLICIDAD
10123	EQUIPO MULTIFUNCIONAL COPIADORA IMPRESORA SCANNER	LEXMARK	MX722ADHE	7464045023RCX	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS
10124	EQUIPO MULTIFUNCIONAL COPIADORA IMPRESORA SCANNER	LEXMARK	MX722ADHE	74641101246DG	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - DEFENSOR DEL USUARIO
10155	EQUIPO DE CONTROL DE ACCESO	BIT4ID	TOKENME TKV3	1326336180168710	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS
10156	EQUIPO DE CONTROL DE ACCESO	BIT4ID	TOKENME TKV3	IT19070017605	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - ASISTENTE REGISTRAL

Continúa en la siguiente página

Cod. Patr.	Bien	Marca	Modelo	Serie	Estado	Ubicación
10165	EQUIPO DE CONTROL DE ACCESO	BIT4ID	TOKENME TKV3	IT19070017615	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CORDINADOR CATASTRO
10166	EQUIPO DE CONTROL DE ACCESO	BIT4ID	TOKENME TKV3	IT19070017621	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - OPERADOR EN SISTEMAS
10168	EQUIPO DE CONTROL DE ACCESO	BIT4ID	TOKENME TKV3	IT19070017623	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - ANALISTA EN SISTEMAS
10176	EQUIPO DE CONTROL DE ACCESO	BIT4ID	TOKENME TKV3	IT19070017641	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - PUBLICIDAD
10189	EQUIPO DE CONTROL DE ACCESO	BIT4ID	TOKENME TKV3	IT19070017682	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - JEFATURA UREG
10194	EQUIPO DE CONTROL DE ACCESO	BIT4ID	TOKENME TKV3	IT19070017672	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - BASE DE DATOS
10196	EQUIPO DE CONTROL DE ACCESO	BIT4ID	TOKENME TKV3	IT19070017661	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - SGTD AREA DE DIGITALIZACION
10199	EQUIPO DE CONTROL DE ACCESO	BIT4ID	TOKENME TKV3	IT19070017664	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - ENTREGA DE PUBLICIDAD
10205	EQUIPO DE CONTROL DE ACCESO	BIT4ID	TOKENME TKV3	IT19070017655	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - JEFATURA UREG
10209	MICROFONO DINAMICO PARA AURICULAR	LOGITECH	G432	2139ME03JF48	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - REGISTRO DE PERSONAS JURIDICAS
10215	MICROFONO DINAMICO PARA AURICULAR	LOGITECH	G432	2139ME03K798	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS 03
10221	MICROFONO DINAMICO PARA AURICULAR	LOGITECH	G432	2144ME034448	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS
10222	MICROFONO DINAMICO PARA AURICULAR	LOGITECH	G432	2139ME03JF58	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - REGISTRO DE PERSONAS JURIDICAS

Continúa en la siguiente página

Cod. Patr.	Bien	Marca	Modelo	Serie	Estado	Ubicación
10224	MICROFONO DINAMICO PARA AURICULAR	LOGITECH	G432	2139ME03K678	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS 02
10233	MICROFONO DINAMICO PARA AURICULAR	LOGITECH	G432	2139ME03J828	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - TECNICO EN SISTEMAS
10234	MICROFONO DINAMICO PARA AURICULAR	LOGITECH	G432	2144ME034428	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - BASE DE DATOS
10239	VIDEO CAMARA PARA COMPUTADORA	CREATIVE	LIVE! CAM SYNC 1080P V2	W6VF0880211022512	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - JEFATURA UREG
10242	VIDEO CAMARA PARA COMPUTADORA	CREATIVE	LIVE! CAM SYNC 1080P V2	W6VF0880211022516	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS 03
10243	VIDEO CAMARA PARA COMPUTADORA	CREATIVE	LIVE! CAM SYNC 1080P V2	W6VF0880211022518	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - REGISTRO DE PERSONAS JURIDICAS
10244	VIDEO CAMARA PARA COMPUTADORA	CREATIVE	LIVE! CAM SYNC 1080P V2	W6VF0880211022519	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS
10251	VIDEO CAMARA PARA COMPUTADORA	CREATIVE	LIVE! CAM SYNC 1080P V2	W6VF0880211022766	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - REGISTRO DE PERSONAS JURIDICAS
10254	VIDEO CAMARA PARA COMPUTADORA	CREATIVE	LIVE! CAM SYNC 1080P V2	W6VF0880211022769	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS 02
10263	VIDEO CAMARA PARA COMPUTADORA	CREATIVE	LIVE! CAM SYNC 1080P V2	W6VF0880211022778	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - TECNICO EN SISTEMAS
10264	VIDEO CAMARA PARA COMPUTADORA	CREATIVE	LIVE! CAM SYNC 1080P V2	W6VF0880211022779	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - BASE DE DATOS
10269	COMPUTADORA PERSONAL PORTATIL	LENOVO	THINKPAD T14 GEN 2.0	PF3M0HXG	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - JEFATURA UTI
10270	COMPUTADORA PERSONAL PORTATIL	LENOVO	THINKPAD T14 GEN 2.0	PF3MNHFV	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - JEFATURA ZONAL

Continúa en la siguiente página

Cod. Patr.	Bien	Marca	Modelo	Serie	Estado	Ubicación
10286	EXTINTOR DE POLVO QUIMICO SECO TIPO ABC DE 6 kg	NACIONAL ANRE	S/M	S/S	ACTIVO	OFICINA REGISTRAL CUSCO 1ER PISO - ARCHIVO
10291	EXTINTOR DE POLVO QUIMICO SECO TIPO ABC DE 6 kg	NACIONAL ANRE	S/M	S/S	ACTIVO	OFICINA REGISTRAL CUSCO 1ER PISO - ARCHIVO
10292	EXTINTOR DE POLVO QUIMICO SECO TIPO ABC DE 6 kg	NACIONAL ANRE	S/M	S/S	ACTIVO	OFICINA REGISTRAL CUSCO 1ER PISO - ARCHIVO
10293	EXTINTOR DE POLVO QUIMICO SECO TIPO ABC DE 6 kg	NACIONAL ANRE	S/M	S/S	ACTIVO	OFICINA REGISTRAL CUSCO 1ER PISO - ARCHIVO
10294	EXTINTOR DE POLVO QUIMICO SECO TIPO ABC DE 6 kg	NACIONAL ANRE	S/M	S/S	ACTIVO	OFICINA REGISTRAL CUSCO 1ER PISO - ARCHIVO
10295	EXTINTOR DE POLVO QUIMICO SECO TIPO ABC DE 6 kg	NACIONAL ANRE	S/M	S/S	ACTIVO	OFICINA REGISTRAL CUSCO 1ER PISO - ARCHIVO
10296	EXTINTOR DE POLVO QUIMICO SECO TIPO ABC DE 6 kg	NACIONAL ANRE	S/M	S/S	ACTIVO	OFICINA REGISTRAL CUSCO 1ER PISO - ARCHIVO
10297	EXTINTOR DE POLVO QUIMICO SECO TIPO ABC DE 6 kg	NACIONAL ANRE	S/M	S/S	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - PASADIZO
10305	EXTINTOR DE POLVO QUIMICO SECO TIPO ABC DE 6 kg	NACIONAL ANRE	S/M	S/S	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - JEFATURA UREG
10307	EXTINTOR DE POLVO QUIMICO SECO TIPO ABC DE 6 kg	NACIONAL ANRE	S/M	S/S	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - AREA REGISTRAL
10309	EXTINTOR DE POLVO QUIMICO SECO TIPO ABC DE 6 kg	NACIONAL ANRE	S/M	S/S	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS 03
10326	HORNO MICROONDAS 23 L	SAMSUNG	AGE83X	JGKR7WET600141	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - COMEDOR
10334	CALEFACTOR	IMACO	OFR11AO	S/S	ACTIVO	OFICINA REGISTRAL CUSCO 1ER PISO - CAJA PREFERENCIAL

Continúa en la siguiente página

Cod. Patr.	Bien	Marca	Modelo	Serie	Estado	Ubicación
10341	CALEFACTOR	IMACO	OFR11AO	S/S	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - JEFATURA UREG
10342	CALEFACTOR	IMACO	OFR11AO	S/S	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - AREA REGISTRAL
10344	CALEFACTOR	IMACO	OFR11AO	S/S	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PERSONAS JURIDICAS
10348	CALEFACTOR	IMACO	OFR11AO	S/S	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CAJA 8
10365	AUDIFONOS PROFESIONALES	LOGITECH	G432	2214ME015228	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - JEFATURA UREG
10367	AUDIFONOS PROFESIONALES	LOGITECH	G432	2214ME015268	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - JEFATURA UTI
10368	AUDIFONOS PROFESIONALES	LOGITECH	G432	FALTA	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - ANALISTA EN SISTEMAS
10369	AUDIFONOS PROFESIONALES	LOGITECH	G432	2214ME0152Y8	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS
10370	AUDIFONOS PROFESIONALES	LOGITECH	G432	2214ME0151L8	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PERSONAS JURIDICAS
10371	AUDIFONOS PROFESIONALES	LOGITECH	G432	2214ME0151M8	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS 01
10372	AUDIFONOS PROFESIONALES	LOGITECH	G432	2214ME015238	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CORDINADOR CATASTRO
10373	AUDIFONOS PROFESIONALES	LOGITECH	G432	2214ME0151N8	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CORDINADOR CATASTRO
10378	AUDIFONOS PROFESIONALES	LOGITECH	G432	2214ME0150L8	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - AREA REGISTRAL

Continúa en la siguiente página

Cod. Patr.	Bien	Marca	Modelo	Serie	Estado	Ubicación
10383	VIDEO CAMARA PARA COMPUTADORA	CREATIVE	LIVE CAM SYNC V2	W6VF 0880 2110 2299 5X	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CORDINADOR CATASTRO
10384	VIDEO CAMARA PARA COMPUTADORA	CREATIVE	LIVE CAM SYNC V2	W6VF0880211022895U	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CORDINADOR CATASTRO
10387	VIDEO CAMARA PARA COMPUTADORA	CREATIVE	LIVE CAM SYNC V2	W6VF 0880 2110 2298 4U	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PERSONAS JURIDICAS
10388	VIDEO CAMARA PARA COMPUTADORA	CREATIVE	LIVE CAM SYNC V2	W6VF 0880 2110 2299 1W	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - ANALISTA EN SISTEMAS
10389	VIDEO CAMARA PARA COMPUTADORA	CREATIVE	LIVE CAM SYNC V2	W6VF 0880 2110 2298 9H	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS 01
10390	VIDEO CAMARA PARA COMPUTADORA	CREATIVE	LIVE CAM SYNC V2	W6VF 0880 2110 2299 2Y	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS
10392	VIDEO CAMARA PARA COMPUTADORA	CREATIVE	LIVE CAM SYNC V2	W6VF 0880 2110 2299 7B	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - AREA REGISTRAL
10396	VIDEO CAMARA PARA COMPUTADORA	CREATIVE	LIVE CAM SYNC V2	W6VF 0880 2110 2298 3K	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - JEFATURA UTI
10403	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0076822W09	ACTIVO	OFICINA REGISTRAL CUSCO 1ER PISO - ARCHIVO
10405	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0077322W09	ACTIVO	OFICINA REGISTRAL CUSCO 1ER PISO - ARCHIVO
10408	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0180022W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - PUBLICIDAD
10411	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0181422W09	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS
10412	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0178922W09	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS

Continúa en la siguiente página

Cod. Patr.	Bien	Marca	Modelo	Serie	Estado	Ubicación
10417	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0178722W09	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS
10418	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0179822W09	ACTIVO	OFICINA REGISTRAL CUSCO 1ER PISO - CAJA PREFERENCIAL
10419	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0030322W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CATASTRO REGISTRAL
10421	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0032522W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CATASTRO REGISTRAL
10424	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0077422W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CATASTRO REGISTRAL
10425	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0076722W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CATASTRO REGISTRAL
10438	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0177722W09	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REG PROPIEDAD 06
10440	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0077222W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CATASTRO REGISTRAL
10442	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0178322W09	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - REGISTRO DE PERSONAS JURIDICAS
10444	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0176722W09	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS
10451	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0175822W09	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - REGISTRO DE PERSONAS JURIDICAS
10460	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0175722W09	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REG PROPIEDAD 06
10461	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0180622W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - TRAMITE FEDATARIO

Continúa en la siguiente página

Cod. Patr.	Bien	Marca	Modelo	Serie	Estado	Ubicación
10462	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0180822W09	BAJA	OFICINA REGISTRAL CUSCO 3ER PISO - UTI II
10463	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0176922W09	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS 01
10468	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0079122W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CATASTRO REGISTRAL
10470	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0082122W09	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PERSONAS JURIDICAS
10473	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0179322W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CATASTRO REGISTRAL
10474	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0179222W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CATASTRO REGISTRAL
10475	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0082222W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CAJA 3
10477	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0032022W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CORDINADOR CATASTRO
10478	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0031122W09	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - JEFATURA UREG
10481	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0030222W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CATASTRO REGISTRAL
10484	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0078922W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - DEFENSOR DEL USUARIO
10485	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0082522W09	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - SGTD AREA DE DIGITALIZACION
10486	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0082322W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CATASTRO REGISTRAL

Continúa en la siguiente página

Cod. Patr.	Bien	Marca	Modelo	Serie	Estado	Ubicación
10488	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0032622W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CATASTRO REGISTRAL
10489	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0030922W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - PUBLICIDAD
10490	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0032422W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CATASTRO REGISTRAL
10491	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0078322W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - MESA DE PARTES
10493	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0078822W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CATASTRO REGISTRAL
10498	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0079922W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CAJA 4
10504	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0031722W09	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS 04
10509	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0031922W09	ACTIVO	OFICINA REGISTRAL CUSCO 4TO PISO - SECRETARIA DE UREG
10514	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0079822W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CAJA 2
10517	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0179522W09	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS
10520	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0030722W09	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS 03
10527	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0180322W09	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - BASE DE DATOS
10528	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0081122W09	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - ANALISTA EN SISTEMAS

Continúa en la siguiente página

Cod. Patr.	Bien	Marca	Modelo	Serie	Estado	Ubicación
10529	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0080622W09	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - UTI II
10530	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0031822W09	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - REGISTRO DE PREDIOS 02
10532	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0031622W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CATASTRO REGISTRAL
10540	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0178022W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CAJA 7
10541	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0177822W09	ACTIVO	OFICINA REGISTRAL CUSCO 3ER PISO - JEFATURA UTI
10543	ACUMULADOR DE ENERGIA - EQUIPO DE UPS	LEGRAND KEOR SPX	KEOR SPX	WO9TH0081622W09	ACTIVO	OFICINA REGISTRAL CUSCO 2DO PISO - CAJA 5

D. Cuestionarios teóricos y prácticos

D.1 Cuestionario - Módulo 1: Introducción al NIST CSF

Parte teórica

1. ¿Qué es el NIST CSF?
2. Mencione las cinco funciones del NIST CSF.
3. Explique la función “Identificar”.
4. ¿Cuál es el objetivo de la función “Proteger”?
5. Diferencie entre “Detectar” y “Responder”.

Parte práctica

1. Identifique 3 activos críticos de una organización.
2. Clasifique los activos según su importancia.
3. Proponga 2 medidas de protección para cada activo.

D.2 Cuestionario - Módulo 2: Gestión de vulnerabilidades

Parte teórica

1. ¿Qué es una vulnerabilidad?

2. Diferencie entre amenaza y riesgo.

3. ¿Qué es un escaneo de vulnerabilidades?

4. ¿Qué es el *Common Vulnerability Scoring System* (CVSS)?

5. ¿Cómo se priorizan las vulnerabilidades?

Parte práctica

1. Analice un sistema con múltiples vulnerabilidades.

2. Clasifique las vulnerabilidades según su riesgo.

3. Proponga un plan de mitigación.

D.3 Cuestionario - Módulo 3: Herramientas de detección

Parte teórica

1. ¿Qué es *OpenVAS*?
2. ¿Qué es un SIEM?
3. ¿Qué es un evento de seguridad?
4. Diferencie entre evento y alerta.
5. ¿Qué es la correlación de eventos?

Parte práctica

1. Analice un reporte de *OpenVAS*.
2. Identifique vulnerabilidades críticas.
3. Interprete logs y detecte eventos sospechosos.

D.4 Cuestionario - Módulo 4: Respuesta a incidentes

Parte teórica

1. ¿Qué es un incidente de seguridad?
2. Mencione las fases de respuesta a incidentes.
3. ¿Qué es contención?
4. ¿Qué es erradicación?
5. ¿Por qué es importante documentar incidentes?

Parte práctica

1. Analice un caso de ataque informático.
2. Proponga acciones de contención.
3. Diseñe un plan de respuesta.

D.5 Cuestionario - Módulo 5: Recuperación de servicios

Parte teórica

1. ¿Qué es continuidad del negocio?

2. Defina RTO.

3. Defina RPO.

4. Diferencie entre backup y recuperación.

5. ¿Qué es un plan de contingencia?

Parte práctica

1. Diseñe un plan básico de recuperación.

2. Defina RTO y RPO para un sistema crítico.

3. Proponga estrategias de respaldo.

D.6 Evaluación Final (Módulos 1 al 5)

El siguiente cuestionario tiene como objetivo evaluar de manera integral los conocimientos teóricos y prácticos adquiridos en los módulos de capacitación, abarcando desde fundamentos del NIST CSF hasta la recuperación de servicios críticos.

Parte I: Evaluación teórica

1. ¿Qué es el NIST CSF y cuál es su finalidad?
2. Mencione y explique brevemente las cinco funciones del NIST CSF.
3. Defina los siguientes conceptos:
    - Activo
    - Vulnerabilidad
    - Amenaza
    - Riesgo
4. ¿Qué es un escaneo de vulnerabilidades y cuál es su importancia?
5. Explique el concepto de priorización de vulnerabilidades y mencione un criterio utilizado.
6. ¿Qué es un SIEM y cuál es su función en la seguridad informática?
7. Diferencie entre evento de seguridad y alerta.
8. ¿Qué es un incidente de seguridad informática?
9. Mencione las fases de respuesta a incidentes.
10. Defina los siguientes términos:
    - RTO
    - RPO

Parte II: Evaluación práctica

Caso:

Una entidad pública presenta los siguientes problemas:

- Sistemas desactualizados.
- Ausencia de monitoreo de eventos.
- No cuenta con respaldos recientes.
- Se detecta un posible acceso no autorizado.

Responda lo siguiente:

1. Identifique al menos 3 activos críticos en el escenario planteado.
2. Detecte y describa 3 vulnerabilidades presentes.
3. Clasifique las vulnerabilidades según su nivel de riesgo (alto, medio, bajo).
4. Proponga al menos 3 medidas de protección basadas en el NIST CSF.
5. Describa cómo utilizaría una herramienta de detección (como *OpenVAS* o SIEM) en este caso.
6. Identifique el incidente de seguridad presente y describa sus características.
7. Proponga acciones de respuesta inmediata (contención).
8. Diseñe un plan básico de recuperación del servicio.
9. Defina valores estimados de RTO y RPO para el sistema afectado.
10. Proponga mejoras para evitar futuros incidentes.

E. Plantilla de acta de cierre

ACTA DE CIERRE DE MÓDULO DE CAPACITACIÓN

Entidad:	Oficina Registral Cusco
Módulo:	_____
Fecha de ejecución:	_____
Modalidad:	_____
Instructor(es):	_____
Número de participantes:	_____

1. Descripción del módulo:

En la presente fecha se dio por concluido el módulo de capacitación, el cual tuvo como objetivo fortalecer las competencias del personal en materia de ciberseguridad, abordando contenidos teóricos y prácticos alineados al marco NIST CSF.

2. Resultados de evaluación:

Indicador	**Resultado**
Promedio general	_____
Nota máxima	_____
Nota mínima	_____
Participantes aprobados	_____
Participantes desaprobados	_____

3. Competencias alcanzadas:

4. Observaciones:

5. Recomendaciones:

_____ _____ _____

Instructor Instructor Participante

F. Bitácora de incidentes históricos

N°	I/R	Asunto	Usuario	Oficina Física	Servicio	Categoría	Fecha Reporte	Fecha de Registro	Estado
1	INCIDENTE	Juridica a natural	Wendy Rosario Sanchez Suclli	Cusco	SPR	SOPORTE	7/11/2019	7/11/2019 14:57:29	CERRADO
2	INCIDENTE	Visualización	Angela Rocio Durand Chaiña	Cusco	VISUALIZAR	1. INMUEBLES	7/11/2019	7/11/2019 15:41:12	CERRADO
3	INCIDENTE	Recuperar partida	Wendy Rosario Sanchez Suclli	Cusco	SPR	SOPORTE	8/11/2019	8/11/2019 12:12:05	CERRADO
4	INCIDENTE	Predios Cusco	Monica Yessenia Gamarra de la Flor	Cusco	VISUALIZAR	1. INMUEBLES	8/11/2019	8/11/2019 13:35:37	CERRADO
5	INCIDENTE	Error al encender monitor	Angela Rocio Durand Chaiña	Cusco	HARDWARE	2. MONITOR	11/11/2019	11/11/2019 08:42:01	CERRADO
6	INCIDENTE	Escaneo de documento	Angela Rocio Durand Chaiña	Cusco	SISTEMA OPERATIVO	7. SOPORTE	11/11/2019	11/11/2019 09:26:48	CERRADO
7	INCIDENTE	Faltan imágenes en la partida	Jose Andree Pacheco Calcine	Cusco	VISUALIZAR	1. INMUEBLES	11/11/2019	11/11/2019 09:29:50	CERRADO
8	INCIDENTE	Cambio de IP del SPRL	Noeli del Pilar Castillo Lovaton	Cusco	SPRL - EXTRANET	1. Req. Cambio de IP	5/3/2019	5/03/2019 08:45:21	CERRADO
9	INCIDENTE	Pred Espinar	Elizabeth Juana Caballero Nakamine	Cusco	VISUALIZAR	1. INMUEBLES	11/11/2019	11/11/2019 12:44:08	CERRADO
10	INCIDENTE	Error de encendido	Maria Celia Concha Camacho	Cusco	HARDWARE	REFRENDADORA	11/11/2019	11/11/2019 13:23:10	CERRADO
11	INCIDENTE	Error figura imágenes de predios	zrxexterno Soporte Externo	Cusco	VISUALIZAR	2. JURIDICAS	11/11/2019	11/11/2019 16:56:31	CERRADO
12	INCIDENTE	Soporte	Percy David Quispe Huayhua	Cusco	HARDWARE	1. CPU	12/11/2019	12/11/2019 10:30:16	CERRADO
13	INCIDENTE	Soporte	Derling Talavera Miranda	Cusco	HARDWARE	1. CPU	12/11/2019	12/11/2019 10:31:38	CERRADO
14	INCIDENTE	Soporte	Elisa Soledad Arregui Negron	Cusco	HARDWARE	3. TECLADO	12/11/2019	12/11/2019 10:34:32	CERRADO
15	INCIDENTE	Problema en visualización	Karol Xiomara Ramirez Molina	Cusco	VISUALIZAR	1. INMUEBLES	12/11/2019	12/11/2019 13:40:16	CERRADO

N°	I/R	Asunto	Usuario	Oficina Física	Servicio	Categoría	Fecha Reporte	Fecha de Registro	Estado
16	INCIDENTE	Habilitación de dos equipos	Derling Talavera Miranda	Cusco	HARDWARE	1. CPU	5/3/2019	5/03/2019 09:17:07	CERRADO
17	INCIDENTE	Error en máquina virtual	Miguel Angel Guzman Flores	Cusco	SISTEMA OPERATIVO	6. ERROR MAQUINA VIRTUAL	13/11/2019	13/11/2019 12:00:40	CERRADO
18	INCIDENTE	Soporte impresora	Adriana Gabriela Tello Justiniani	Cusco	HARDWARE	5. IMPRESORA	13/11/2019	13/11/2019 17:33:17	CERRADO
19	INCIDENTE	Soporte impresora	Hetbelin Imelda Perez Suarez	Cusco	HARDWARE	5. IMPRESORA	13/11/2019	13/11/2019 17:34:30	CERRADO
20	INCIDENTE	Reseteo de clave consulta	Patricia Salas Sanchez	Cusco	CONSULTA REGISTRAL	SOPORTE	5/3/2019	5/03/2019 10:18:00	CERRADO
21	INCIDENTE	Soporte	Verenice Bellota Ortega	Cusco	HARDWARE	5. IMPRESORA	14/11/2019	14/11/2019 15:50:25	CERRADO
22	INCIDENTE	Visualización	Ronald Yony Candia Ticona	Cusco	VISUALIZAR	1. INMUEBLES	14/11/2019	14/11/2019 15:54:09	CERRADO
23	INCIDENTE	Visualización	Ronald Yony Candia Ticona	Cusco	VISUALIZAR	1. INMUEBLES	14/11/2019	14/11/2019 15:55:27	CERRADO
24	INCIDENTE	SPRL - EXTRANET - SOPORTE	Maria Celia Concha Camacho	Cusco	SPRL - EXTRANET	2. Req. Transferencia Carga	5/3/2019	5/03/2019 10:18:06	ANULADO
25	INCIDENTE	Bloqueo título	Naysha Farfan Bellota	Cusco	LIBRO DIARIO	SOPORTE	14/11/2019	14/11/2019 15:58:24	CERRADO
26	INCIDENTE	Solicita visualización	Nancy Champi Monterroso	Cusco	VISUALIZAR	1. INMUEBLES	15/11/2019	15/11/2019 13:21:22	CERRADO
27	INCIDENTE	Soporte scanner	Carlos Alberto Rodrigo Ccapatinta	Cusco	HARDWARE	5. IMPRESORA	15/11/2019	15/11/2019 13:28:14	CERRADO
28	INCIDENTE	Error partida	Zulema Montesinos Quispichu	Cusco	VISUALIZAR	1. INMUEBLES	15/11/2019	15/11/2019 14:54:48	CERRADO
29	INCIDENTE	Trabajos sábado 16 de noviembre POI	Nilton Paredes Lopez	Cusco	VISUALIZAR	1. INMUEBLES	15/11/2019	15/11/2019 15:30:23	CERRADO
30	INCIDENTE	Visualización	Karol Xiomara Ramirez Molina	Cusco	VISUALIZAR	1. INMUEBLES	18/11/2019	18/11/2019 09:56:16	CERRADO
31	INCIDENTE	Error partida	Zulema Montesinos Quispichu	Cusco	VISUALIZAR	1. INMUEBLES	19/11/2019	19/11/2019 11:17:05	CERRADO

N°	I/R	Asunto	Usuario	Oficina Física	Servicio	Categoría	Fecha Reporte	Fecha de Registro	Estado
32	INCIDENTE	SPRL - EXTRANET ERROR EN CARGA LABORAL	Maria Celia Concha Camacho	Cusco	SPRL - EXTRANET	7. Incidente - Otros	5/3/2019	5/03/2019 11:20:59	ANULADO
33	INCIDENTE	Error de inicio	Percy David Quispe Huayhua	Cusco	SISTEMA OPERATIVO	7. SOPORTE	19/11/2019	19/11/2019 15:03:13	CERRADO
34	INCIDENTE	Pred Cusco	Miguel Angel Guzman Flores	Cusco	VISUALIZAR	1. INMUEBLES	19/11/2019	19/11/2019 15:14:11	CERRADO
35	INCIDENTE	Cambio de estado de título	Naysha Farfan Bellota	Cusco	LIBRO DIARIO	SOPORTE	19/11/2019	19/11/2019 15:16:30	CERRADO
36	INCIDENTE	Predios Espinar	Elizabeth Juana Caballero Nakamine	Cusco	VISUALIZAR	1. INMUEBLES	20/11/2019	20/11/2019 08:45:47	CERRADO
37	INCIDENTE	Cambio de driver	Luis Miguel Del Castillo Suarez	Cusco	HARDWARE	5. IMPRESORA	20/11/2019	20/11/2019 08:50:48	CERRADO
38	INCIDENTE	Extensión de uso	Elizabeth Juana Caballero Nakamine	Cusco	SGIT	SOPORTE	20/11/2019	20/11/2019 08:52:09	CERRADO
39	INCIDENTE	Error de impresión	Wilber Alvarez Monterola	Cusco	HARDWARE	5. IMPRESORA	20/11/2019	20/11/2019 09:08:03	CERRADO
40	INCIDENTE	Predios Cusco	Marisela Lisbeth Carrillo Yupanqui	Cusco	CONSULTA REGISTRAL	SOPORTE	20/11/2019	20/11/2019 09:09:57	CERRADO
41	INCIDENTE	Visualización	Ronald Yony Candia Ticona	Cusco	VISUALIZAR	1. INMUEBLES	20/11/2019	20/11/2019 10:34:28	CERRADO
42	INCIDENTE	SIR a SARP	Natzu Kyoko Yakazu Rodriguez	Cusco	SARP	SOPORTE	20/11/2019	20/11/2019 10:35:25	CERRADO
43	INCIDENTE	Soporte	Shanery Hurtado Valderrama	Cusco	SARP	SOPORTE	20/11/2019	20/11/2019 10:40:20	CERRADO
44	INCIDENTE	Soporte	Elvis Vargas Saire	Cusco	HARDWARE	1. CPU	20/11/2019	20/11/2019 10:41:36	CERRADO
45	INCIDENTE	Soporte	Zulema Montesinos Quispichu	Cusco	HARDWARE	2. MONITOR	20/11/2019	20/11/2019 10:42:16	CERRADO
46	INCIDENTE	RENIEC	Nay Ruth Figueroa Candia	Cusco	RENIEC Biométrico	SOPORTE	20/11/2019	20/11/2019 10:43:10	CERRADO

N°	I/R	Asunto	Usuario	Oficina Física	Servicio	Categoría	Fecha Reporte	Fecha de Registro	Estado
47	INCIDENTE	RENIEC	Fabiola Mendoza Cardenas	Cusco	RENIEC Biométrico	SOPORTE	20/11/2019	20/11/2019 10:45:22	CERRADO
48	INCIDENTE	Soporte Gabriela Escobar	Monica Yessenia Gamarra de la Flor	Cusco	SPR	SOPORTE	20/11/2019	20/11/2019 10:48:34	CERRADO
49	INCIDENTE	Visualización	Karol Xiomara Ramirez Molina	Cusco	VISUALIZAR	1. INMUEBLES	20/11/2019	20/11/2019 11:52:37	CERRADO
50	INCIDENTE	Soporte SPR	Noeli del Pilar Castillo Lovaton	Cusco	SPR	SOPORTE	20/11/2019	20/11/2019 11:55:23	CERRADO
51	INCIDENTE	Títulos masivos	Nay Ruth Figueroa Candia	Cusco	SCUNAC	SOPORTE	20/11/2019	20/11/2019 12:01:19	CERRADO
52	INCIDENTE	Restablecer contraseña	Josmel David Arias Espinoza	Cusco	CONSULTA REGISTRAL	SOPORTE	20/11/2019	20/11/2019 12:02:49	CERRADO
53	INCIDENTE	Soporte SARP	Nay Ruth Figueroa Candia	Cusco	SARP	SOPORTE	20/11/2019	20/11/2019 12:06:10	CERRADO
54	INCIDENTE	PJ a PN	Wendy Rosario Sanchez Suclli	Cusco	SPR	SOPORTE	20/11/2019	20/11/2019 12:08:51	CERRADO
55	INCIDENTE	LIBRO DIARIO SOPORTE	Violeta Tupfia Gamarra	Cusco	LIBRO DIARIO	SOPORTE	20/11/2019	20/11/2019 15:56:17	CERRADO
56	INCIDENTE	Error Firma PDF	Mery Huillca Cursi	Cusco	SIR	SOPORTE	5/3/2019	5/03/2019 12:58:35	CERRADO
57	INCIDENTE	Error partida 02075409	Zulema Montesinos Quispichu	Cusco	VISUALIZAR	1. INMUEBLES	21/11/2019	21/11/2019 09:13:25	CERRADO
58	INCIDENTE	Error título SID	Yelvin Dueñas Castañeda	Cusco	SIR	SOPORTE	5/3/2019	5/03/2019 13:26:25	CERRADO
59	INCIDENTE	SARP	Nay Ruth Figueroa Candia	Cusco	SCUNAC	SOPORTE	22/11/2019	22/11/2019 15:16:13	CERRADO
60	INCIDENTE	Visualización	Verenice Bellota Ortega	Cusco	VISUALIZAR	1. INMUEBLES	22/11/2019	22/11/2019 15:18:09	CERRADO
61	INCIDENTE	Distribución	Violeta Tupfia Gamarra	Cusco	LIBRO DIARIO	SOPORTE	22/11/2019	22/11/2019 15:19:13	CERRADO
62	INCIDENTE	Visualización	Elisa Soledad Arregui Negron	Cusco	VISUALIZAR	1. INMUEBLES	22/11/2019	22/11/2019 15:20:10	CERRADO
63	INCIDENTE	Declaración Jurada	Nay Ruth Figueroa Candia	Cusco	OFIMÁTICA	SOPORTE	22/11/2019	22/11/2019 15:29:46	CERRADO
64	INCIDENTE	Error en la partida 02062088 predios	Zulema Montesinos Quispichu	Cusco	VISUALIZAR	1. INMUEBLES	22/11/2019	22/11/2019 16:02:21	SOPORTE EXTERNO

N°	I/R	Asunto	Usuario	Oficina Física	Servicio	Categoría	Fecha Reporte	Fecha de Registro	Estado
65	INCIDENTE	Acceso a partida SIR	Marco Antonio Castro Suarez	Cusco	VISUALIZAR	1. INMUEBLES	22/11/2019	22/11/2019 16:42:25	CERRADO
66	INCIDENTE	Configuración de impresora	Maura Cancha Gutierrez	Cusco	SISTEMA OPERATIVO	7. SOPORTE	25/11/2019	25/11/2019 11:50:35	CERRADO
67	INCIDENTE	Configuración de impresora	Percy David Quispe Huayhua	Cusco	SISTEMA OPERATIVO	7. SOPORTE	25/11/2019	25/11/2019 11:50:49	CERRADO
68	INCIDENTE	Configuración de impresora	Maura Huayllapuma Calcina	Cusco	SISTEMA OPERATIVO	7. SOPORTE	25/11/2019	25/11/2019 11:50:58	CERRADO
69	INCIDENTE	Configuración de impresora	Miguel Angel Guzman Flores	Cusco	SISTEMA OPERATIVO	7. SOPORTE	25/11/2019	25/11/2019 11:51:09	CERRADO
70	INCIDENTE	Configuración de impresora	Adriana Gabriela Tello Justiniani	Cusco	SISTEMA OPERATIVO	7. SOPORTE	25/11/2019	25/11/2019 11:51:19	CERRADO
71	INCIDENTE	Pred Cusco	Adriana Gabriela Tello Justiniani	Cusco	VISUALIZAR	1. INMUEBLES	25/11/2019	25/11/2019 12:43:44	CERRADO
72	INCIDENTE	Pred Cusco	Adriana Gabriela Tello Justiniani	Cusco	VISUALIZAR	1. INMUEBLES	25/11/2019	25/11/2019 12:43:58	CERRADO
73	INCIDENTE	Pred Cusco	Adriana Gabriela Tello Justiniani	Cusco	VISUALIZAR	1. INMUEBLES	25/11/2019	25/11/2019 12:44:22	CERRADO
74	INCIDENTE	Pred Cusco	Adriana Gabriela Tello Justiniani	Cusco	VISUALIZAR	1. INMUEBLES	25/11/2019	25/11/2019 12:44:35	CERRADO
75	INCIDENTE	Pred Cusco	Adriana Gabriela Tello Justiniani	Cusco	VISUALIZAR	1. INMUEBLES	25/11/2019	25/11/2019 12:44:40	CERRADO
76	INCIDENTE	Configuración de impresora VMware	Elizabeth Juana Caballero Nakamine	Cusco	SISTEMA OPERATIVO	7. SOPORTE	26/11/2019	26/11/2019 10:46:23	CERRADO
77	INCIDENTE	Configuración de impresora	Elizabeth Juana Caballero Nakamine	Cusco	SISTEMA OPERATIVO	7. SOPORTE	26/11/2019	26/11/2019 10:46:45	CERRADO

N°	I/R	Asunto	Usuario	Oficina Física	Servicio	Categoría	Fecha Reporte	Fecha de Registro	Estado
78	INCIDENTE	Predios Cusco	Ingrid Cornejo Lazo	Cusco	VISUALIZAR	1. INMUEBLES	26/11/2019	26/11/2019 10:50:37	CERRADO
79	INCIDENTE	Soporte	Eliana Carla Fernandez Gamarra	Cusco	HARDWARE	1. CPU	26/11/2019	26/11/2019 13:00:03	CERRADO
80	INCIDENTE	Soporte	Nay Ruth Figueroa Candia	Cusco	SCUNAC	SOPORTE	26/11/2019	26/11/2019 13:11:08	CERRADO
81	INCIDENTE	Parte digital incorrecto	Noeli del Pilar Castillo Lovaton	Cusco	SPR	SOPORTE	5/3/2019	5/03/2019 17:11:54	CERRADO
82	INCIDENTE	Error en la partida	Zulema Montesinos Quispichu	Cusco	VISUALIZAR	1. INMUEBLES	27/11/2019	27/11/2019 09:38:54	CERRADO
83	INCIDENTE	Visualización de PE	Eduardo Fabian Luque Paredes	Cusco	VISUALIZAR	1. INMUEBLES	27/11/2019	27/11/2019 09:52:24	CERRADO
84	INCIDENTE	Error partida	Zulema Montesinos Quispichu	Cusco	VISUALIZAR	1. INMUEBLES	27/11/2019	27/11/2019 16:15:40	CERRADO
85	INCIDENTE	Actualizar SIR	Ana Maria Bustamante Muñiz	Cusco	SIR	SOPORTE	2/12/2019	2/12/2019 10:32:26	CERRADO
86	INCIDENTE	Título SARP	Luz Angelica Vargas Medina	Cusco	SARP	SOPORTE	6/3/2019	6/03/2019 09:46:26	CERRADO
87	INCIDENTE	Visualización	Elisa Soledad Arregui Negron	Cusco	VISUALIZAR	1. INMUEBLES	2/12/2019	2/12/2019 10:34:14	CERRADO
88	INCIDENTE	Soporte	Reyna Carolina Melgar Olazabal	Cusco	SIR	SOPORTE	2/12/2019	2/12/2019 12:32:06	CERRADO
89	INCIDENTE	Soporte	Aldair Claudio Quirita Achahuanco	Cusco	SISTEMA OPERATIVO	6. ERROR MAQUINA VIRTUAL	2/12/2019	2/12/2019 12:39:46	CERRADO
90	INCIDENTE	Soporte SARP	Luz Angelica Vargas Medina	Cusco	SARP	SOPORTE	2/12/2019	2/12/2019 12:42:34	CERRADO
91	INCIDENTE	Soporte	Karol Xiomara Ramirez Molina	Cusco	SARP	SOPORTE	2/12/2019	2/12/2019 12:43:31	CERRADO
92	INCIDENTE	Soporte	Marisela Lisbeth Carrillo Yupanqui	Cusco	CONSULTA REGISTRAL	SOPORTE	2/12/2019	2/12/2019 12:47:44	CERRADO
93	INCIDENTE	Soporte SPR	Monica Yessenia Gamarra de la Flor	Cusco	SPR	SOPORTE	2/12/2019	2/12/2019 12:48:31	CERRADO
94	INCIDENTE	Visualización	Eliana Carla Fernandez Gamarra	Cusco	VISUALIZAR	1. INMUEBLES	2/12/2019	2/12/2019 16:05:35	CERRADO

N°	I/R	Asunto	Usuario	Oficina Física	Servicio	Categoría	Fecha Reporte	Fecha de Registro	Estado
95	INCIDENTE	Soporte SARP	Karol Xiomara Ramirez Molina	Cusco	SARP	SOPORTE	2/12/2019	2/12/2019 16:48:35	CERRADO
96	INCIDENTE	Error Perfil temporal de Windows	Maria Celia Concha Camacho	Cusco	SISTEMA OPERATIVO	7. SOPORTE	3/12/2019	3/12/2019 14:50:32	CERRADO
97	INCIDENTE	RENIEC	Mery Huillca Cursi	Cusco	RENIEC	SOPORTE RENIEC	4/12/2019	4/12/2019 12:50:42	CERRADO
98	INCIDENTE	SOPORTE	Eliana Carla Fernandez Gamarra	Cusco	CONSULTA REGISTRAL	SOPORTE	4/12/2019	4/12/2019 12:52:37	CERRADO
99	INCIDENTE	Visualización	Rudy Christopher Huaman Gutierrez	Cusco	VISUALIZAR	1. INMUEBLES	4/12/2019	4/12/2019 12:53:28	CERRADO
100	INCIDENTE	Soporte	Shanery Hurtado Valderrama	Cusco	SPR	SOPORTE	4/12/2019	4/12/2019 12:56:33	CERRADO

Comentario: Se registraron los primeros 100 incidentes y requerimientos analizados, por que en total se registraron 8208 incidentes y requerimientos.

G. Bitácora de incidentes de red

N°	Fecha	Hora	Remitente	Destinatario	Asunto	Cuerpo Correo Inicial	Oficina(s) Afectada(s)	Estado	Tiempo
1	03/02/2025	17:15	Miguel Lorenzo	SOPORTE INKA	Caída de red en Andahuaylas	Buenas tardes Sres. de Plasmatronics, no tenemos red en Andahuaylas. Su apoyo urgente con la solución, ya que es una oficina registral.	Andahuaylas	Caído	-
2	05/02/2025	14:04	Miguel Lorenzo	SOPORTE INKA	Problemas de comunicación entre anexos	Se han detectado problemas en la comunicación entre algunos anexos. El anexo 8425 no puede comunicarse con 8442 y 8451; el 8468 no puede comunicarse con 8478 y 8447; y los anexos 8418 y 8416 no pueden realizar llamadas a otros anexos.	Cusco; Infancia	Incidente en teléfonos IP	-
3	06/02/2025	14:40	Miguel Lorenzo	SOPORTE INKA	Caída de red (equipo MikroTik COT4)	Se reportó una caída de conexión con Sede Central, Bodega y otras oficinas. Se verificó que existía red local en Zona X, pero no había conexión con COT4, por lo que se reportó la incidencia al grupo de WhatsApp.	Cusco; Infancia; Andahuaylas; Santiago; San Jerónimo; San Sebastián; Quillabamba; Abancay	Caído	-
4	07/02/2025	15:42	Luis Ramos	SOPORTE INKA	Dificultades con el tiempo de respuesta de Bodega	Se reportan problemas en el tiempo de respuesta entre la OR de Andahuaylas y Bodega, lo que genera dificultades al momento de realizar las calificaciones de los títulos.	Andahuaylas	Intermitencia / altos tiempos de respuesta	-

N°	Fecha	Hora	Remitente	Destinatario	Asunto	Cuerpo Correo Inicial	Oficina(s) Afectada(s)	Estado	Tiempo
5	07/02/2025	15:25	Miguel Lorenzo	SOPORTE INKA	Lentitud al acceder a servicios de Bodega	Buenas tardes Sres. de Plasmatronics, su apoyo con la revisión de nuestro servicio de transmisión de datos, puesto que desde las 12 pm aproximadamente nos reportan lentitud con servicios de Bodega y demás zonas. Por ejemplo, desde Cusco se observa una latencia con el servicio de Plasmatronics de hasta 250 ms.	Cusco; Infancia; Andahuaylas; Santiago; San Jerónimo; San Sebastián; Quillabamba; Abancay	Intermitencia / altos tiempos de respuesta	–
6	12/02/2025	07:51	Vladimir Vargas	SOPORTE INKA	Posible caída en comunicaciones	Previo un cordial saludo, por la presente se informa caída en las comunicaciones, lo que generó que se caiga el Standby. Se comunica a fin de que se considere como falta de servicio por parte del proveedor o lo que vean por conveniente.	Cusco; Infancia	Corte de servicio	–
7	12/02/2025	08:11	Miguel Lorenzo	SOPORTE INKA	No tenemos red en Andahuaylas	Buen día, su apoyo por favor con la revisión urgente de la red de Andahuaylas. IP: 10.10.7.9, se llega a esta IP, pero no a la red interna 172.20.109.1.	Andahuaylas	Caído	–
8	12/02/2025	09:35	Miguel Lorenzo	SOPORTE INKA	Caída de red en Andahuaylas	Buen día Sres. de Plasmatronics, su apoyo urgente con la revisión de la red en Andahuaylas. Hubo un corte de luz en la ciudad; no obstante, en la oficina se viene trabajando con el grupo electrógeno, pero no se tiene activo el servicio de transmisión de datos. Se solicita su atención a la brevedad para restablecer el servicio.	Andahuaylas	Caído	–

N°	Fecha	Hora	Remitente	Destinatario	Asunto	Cuerpo Correo Inicial	Oficina(s) Afectada(s)	Estado	Tiempo
9	14/02/2025	13:05	SOPORTE INKA	M. Lorenzo – Cusco	Corte de 5 minutos por mantenimiento de equipo de cabecera en Abancay	Inge. Miguel, buenas tardes. A la 1:05 pm de hoy se realizará un corte en la agencia de Abancay por mantenimiento del equipo de cabecera. El corte será de 5 a 10 minutos aproximadamente.	Abancay	Corte de servicio	5–10 min
10	25/02/2025	16:58	Miguel Lorenzo	SOPORTE INKA	Sobre enlaces de Abancay y Andahuaylas	Buenas tardes estimado Soporte. Haciendo seguimiento a los enlaces de Plasmatronics, vemos que Abancay (172.20.101.x) y, a veces, Andahuaylas (172.20.109.x) tienen constante pérdida de paquetes e incremento en los tiempos de respuesta, lo que conlleva a quejas por parte de los usuarios. Asimismo, aún no se cuenta con monitoreo que permita identificar saturación o conocer el uso del ancho de banda en dichas oficinas.	Abancay y Andahuaylas	Intermitencia / pérdida de paquetes / altos tiempos de respuesta	–
11	27/02/2025	09:50	Miguel Lorenzo	SOPORTE INKA	No se tiene red en Abancay	Buen día Sres. de Plasmatronics, su apoyo urgente con la revisión del enlace de Abancay, ya que no tenemos conexión, ni a la red ni al MikroTik de dicha oficina. Agradezco su revisión a la brevedad.	Abancay	Corte de servicio	–
12	01/03/2025	17:15	Miguel Lorenzo	SOPORTE INKA	Oficina de Abancay sin servicio	Buen día Sres. de soporte, su apoyo urgente con la revisión de la red de Abancay el día de hoy 01/03/2025. Nos informan por favor.	Abancay	Caído	1 h 1 min

N°	Fecha	Hora	Remitente	Destinatario	Asunto	Cuerpo Correo Inicial	Oficina(s) Afectada(s)	Estado	Tiempo
13	02/03/2025	11:47	Miguel Lorenzo	SOPORTE INKA	Enlaces caídos (Urubamba, Sicuani, Andahuaylas, Puerto)	Buen día Sres. de Plasmatronic, me reportan que no hay red en Andahuaylas. Asimismo, según revisé, no se tiene red en Urubamba, Tambopata, Sicuani y Puerto. Debo entender que están realizando algunas configuraciones. De ser el caso, favor de informar, ya que tenemos personal en Andahuaylas laborando en oficina. En la mañana sí se tuvo servicio. Agradezco su atención y confirmar el restablecimiento del servicio en las oficinas indicadas.	Puerto Maldonado; Tambopata; Sicuani; Andahuaylas	Caído	1 día 1 h 45 min
14	05/03/2025	08:44	Miguel Lorenzo	SOPORTE INKA	Imposibilidad de acceder al SGD, SÍGUELO SUNARP y SRPL	Buen día estimado Soporte, su apoyo por favor, primero para descartar si se trata de un tema por parte de ustedes.	Chalhuahuacho	Servicios Web de SUNARP caídos	1 h 16 min
15	07/03/2025	10:15	Miguel Lorenzo	SOPORTE INKA	No se tiene red en Tambopata	Buen día estimado Soporte, vemos que desde hace un momento no se tiene red con la Oficina de Tambopata. Su revisión por favor. Gracias.	Tambopata	Intermitencias	1 h 45 min
16	07/03/2025	12:41	Miguel Lorenzo	SOPORTE INKA	Fwd: Solicito realizar pruebas de configuración de balanceo	Buenas tardes estimado Soporte, la única ventana que tenemos para poder realizar las pruebas de COT5 es el sábado a partir de las 9 pm. Por ello, se informa para contar con vuestra disponibilidad y proceder con las actividades de balanceo y pruebas. Favor de confirmarnos.	COT5	Falta configurar	1 día 7 h 49 min

N°	Fecha	Hora	Remitente	Destinatario	Asunto	Cuerpo Correo Inicial	Oficina(s) Afectada(s)	Estado	Tiempo
17	10/03/2025	09:03	Miguel Lorenzo	SOPORTE INKA	Incidente conexión servicio Internet OR Urubamba	Buenas tardes estimado Soporte, la única ventana que tenemos para poder realizar las pruebas de COT5 es el sábado a partir de las 9 pm. Por ello, se informa para contar con vuestra disponibilidad y proceder con las actividades de balanceo y pruebas. Favor de confirmarnos.	Urubamba	Servicios Web de SUNARP y Bodega caídos	18 h 41 min
18	11/03/2025	08:19	Miguel Lorenzo	SOPORTE INKA	Pérdida de paquetes con Bodega	Buen día estimados, su apoyo con la revisión urgente de la conexión a Bodega, ya que están reportando constantes pérdidas de paquetes a nivel zonal y Sede Central nos confirma que solo pasa con Zona X. Su atención por favor. Gracias.	Servicios de Bodega	Intermitencias	4 h 24 min
19	11/03/2025	19:04	Miguel Lorenzo	SOPORTE INKA	Sin acceso desde el VPN y alertas de indisponibilidad	Buenas tardes estimado Soporte, su apoyo con la revisión de la red de Cusco, ya que están llegando alertas de indisponibilidad, lo cual ocurre cuando hay desconexión de la red. Asimismo, tampoco podemos acceder por el VPN.	COT5	Caído	7 h 25 min
20	14/03/2025	08:00	Miguel Lorenzo	SOPORTE INKA	Sin red en Chalhuahuacho	Buen día Elmer / Richar, no tenemos servicio en Chalhuahuacho, su revisión por favor. Gracias.	Chalhuahuacho	Caído	4 h 08 min
21	19/03/2025	06:47	Miguel Lorenzo	SOPORTE INKA	No se tiene conexión con COT5	Buen día estimados, su apoyo con la revisión de COT5, nos informan por favor. Gracias.	COT5	Caído	7 h 28 min

N°	Fecha	Hora	Remitente	Destinatario	Asunto	Cuerpo Correo Inicial	Oficina(s) Afectada(s)	Estado	Tiempo
22	20/03/2025	07:58	Miguel Lorenzo	SOPORTE INKA	Sin red en Sicuani	Buen día Sres. de Soporte, su apoyo con la revisión de la Oficina de Sicuani. Urgente por favor. Gracias.	Sicuani	Caído	30 min
23	20/03/2025	11:30	Miguel Lorenzo	SOPORTE INKA	MDD y Tambopata inestable	Buenas tardes Elmer, el apoyo en MDD y Tambopata por favor.	MDD / Tambopata	Intermit.	7 h 20 min
24	21/03/2025	08:10	Miguel Lorenzo	SOPORTE INKA	Oficina Registral Sicuani	Buen día Elmer, tu apoyo por favor con la revisión del enlace de Sicuani. Nos confirman el ticket correspondiente de ser el caso. Asimismo, a fin de no demorar en la indisponibilidad, se sugiere utilizar el enlace de backup mientras se restablezca el servicio del enlace principal de esta oficina.	Sicuani	Caído	27 min
25	24/03/2025	12:02	Miguel Lorenzo	SOPORTE INKA	Oficina Registral Sicuani	Buen día Elmer, tu apoyo por favor con la revisión del enlace de Sicuani. Nos confirman el ticket correspondiente de ser el caso. Asimismo, se sugiere utilizar el enlace de backup mientras se restablezca el servicio del enlace principal.	Sicuani	Caído	41 min
26	25/03/2025	07:40	Miguel Lorenzo	SOPORTE INKA	Error al acceder a geovisores externos	Buenas tardes Elmer, tu apoyo con la revisión. Ya hicieron el descarte y con un Internet alternativo o con la red de Cusco normalmente se puede acceder, pero en Urubamba no permite. Desde Cusco también se puede acceder normalmente a las webs indicadas, pero en Urubamba no.	Urubamba	Sin Web	18 min

N°	Fecha	Hora	Remitente	Destinatario	Asunto	Cuerpo Correo Inicial	Oficina(s) Afectada(s)	Estado	Tiempo
27	27/03/2025	20:52	Miguel Lorenzo	SOPORTE INKA	Pérdida de conexión y alta latencia con Bodega	Buenas noches Elmer, según lo coordinado se reporta una desconexión que no permitía acceder por VPN a la red de Cusco. Luego del restablecimiento se observa un tiempo de respuesta a Bodega de 39 y 40 ms con pérdida de paquetes.	Cusco	Intermit.	2 h 33 min
28	31/03/2025	16:30	Miguel Lorenzo	SOPORTE INKA	Sin servicio de red durante apagón general en Cusco	Buenas tardes Sres. de Plasmatronics, se presentó un apagón en la Oficina de Cusco, generando desconexión a nivel de Cusco y las demás oficinas. Aunque se restableció el fluido eléctrico mediante grupo electrógeno, continuó sin servicio de transmisión de datos.	Cusco	Caído	25 min
29	16/04/2025	11:00	Miguel Lorenzo	SOPORTE INKA	Caída de red en Pto. Maldonado y Tambopata	Buen día Sres., su apoyo con la revisión de la red en Tambopata y MDD. Se ha reportado caída de ambos enlaces. Su revisión por favor; de ser el caso, se podría contar con el enlace de backup temporal.	MDD / Tambopata	Caído	1 día 1 h 45 min
30	16/04/2025	10:00	Plasmatronics	OPERADORES WIN	Sigo sin conexión, ticket 202523145	Buen día señores de WIN, necesito su apoyo de urgencia. Mi servicio se encuentra caído desde las 10:00 am del 16 de abril. Se solicita seguimiento a las VLAN 2660 y VLAN 2717 desde los Portales de Huachipa a Torre 5 (COT5).	COT5	Caído	5 días 10 h 26 min

N°	Fecha	Hora	Remitente	Destinatario	Asunto	Cuerpo Correo Inicial	Oficina(s) Afectada(s)	Estado	Tiempo
31	21/04/2025	05:38	Miguel Lorenzo	SOPORTE INKA	Sin red en Abancay	Buen día estimados, su apoyo por favor con la revisión de la red de Abancay. Se tiene normal fluido eléctrico, pero sin servicio de transmisión de datos. Su atención urgente. Gracias.	Abancay	Caído	17 h 17 min
32	25/04/2025	15:06	Miguel Lorenzo	SOPORTE INKA	No se tiene red en Qbba	Buenas tardes Sres. de soporte, su apoyo con la revisión de la red de Qbba, ya que desde hace un rato no se tiene servicio en esa oficina, pero sí se tiene energía eléctrica.	Quillabamba	Caído	11 h 16 min
33	26/04/2025	13:45	–	–	–	–	Espinar	Caído	8 h
34	01/05/2025	10:03	–	–	–	–	Urcos	Caído	4 h 07 min
35	04/05/2025	18:15	Miguel Lorenzo	SOPORTE INKA	Oficinas sin transmisión de datos	Buenas tardes estimados, vemos que tenemos varias oficinas sin servicio de red: Sicuani, Tambopata, Urcos, Urubamba, Abancay, Andahuaylas, Puerto Maldonado, Espinar, Quillabamba, Chalhuahuacho y COT5. Favor su revisión urgente y habilitación del servicio según plazo de bases.	Sicuani; Tambopata; Urcos; Urubamba; Abancay; Andahuaylas; Pto. Maldonado; Espinar; Quillabamba; Chalhuahuacho; COT5	Caído	18 h 24 min
36	07/05/2025	12:30	Miguel Lorenzo	SOPORTE INKA	Sin red en Tambopata y MDD	Buenas tardes, su apoyo con la revisión de la red en MDD y Tambopata. No tenemos servicio y se requiere a la brevedad el restablecimiento según bases. Su atención urgente.	MDD / Tambopata	Caído	4 h 24 min

N°	Fecha	Hora	Remitente	Destinatario	Asunto	Cuerpo Correo Inicial	Oficina(s) Afectada(s)	Estado	Tiempo
37	07/05/2025	18:30	Miguel Lorenzo	SOPORTE INKA	No se tiene red en las oficinas registrales	Buenas tardes Elmer, de nuevo no tengo red en todas las sedes, solo en Cusco. Urgente tu apoyo y restablecimiento según bases.	Sicuani; Tambopata; Urcos; Urubamba; Abancay; Andahuaylas; Pto. Maldonado; Espinar; Quillabamba; Chalhuahuacho; COT5	Caído	7 h 30 min
38	08/05/2025	08:39	Miguel Lorenzo	SOPORTE INKA	Sin servicio de transmisión de datos en Puerto M. y Tambopata	Buen día, luego del restablecimiento de la red, aproximadamente desde las 08:39 am se reporta MDD y Tambopata sin red. Es urgente el restablecimiento del servicio.	MDD / Tambopata	Caído	1 h 07 min
39	08/05/2025	09:37	Miguel Lorenzo	SOPORTE INKA	No tenemos servicio en Andahuaylas	Buen día estimados, 09:37 am se acaba de caer el servicio de transmisión de datos en Andahuaylas. Se requiere urgente su revisión y restablecimiento.	Andahuaylas	Caído	11 min
40	09/05/2025	14:45	Miguel Lorenzo	SOPORTE INKA	–	–	Andahuaylas	Caído	7 min
41	12/05/2025	04:00	Miguel Lorenzo	SOPORTE INKA	Sin red en Abancay	Buen día, no se tiene red en Abancay, aparentemente desde las 4 am. Su revisión urgente ya que a las 8 am inician labores.	Abancay	Caído	4 h 01 min
42	15/05/2025	12:05	–	–	–	–	Andahuaylas	Caído	30 min
43	17/05/2025	10:00	–	–	–	–	San Jerónimo	Caído	6 h

N°	Fecha	Hora	Remitente	Destinatario	Asunto	Cuerpo Correo Inicial	Oficina(s) Afectada(s)	Estado	Tiempo
44	21/05/2025	16:06	–	–	Caída de red en oficinas de sedes registrales	Buenas tardes, estimados. En horas de la tarde del día de hoy se ha presentado avería en la red, afectando a todas las oficinas de sedes, Chalhuahuacho y Urcos. Favor de generar su ticket e indicarnos el tiempo de solución.	Sicuani; Tambopata; Urcos; Urubamba; Abancay; Andahuaylas; Espinar; Puerto Maldonado; Quillabamba; Chalhuahuacho	Caído	1 h 27 min
45	22/05/2025	08:00	–	–	Nueva caída de red en oficinas de sedes registrales	–	Sicuani; Tambopata; Urcos; Urubamba; Abancay; Andahuaylas; Espinar; Puerto Maldonado; Quillabamba; Chalhuahuacho	Caído	1 h 20 min
46	25/05/2025	00:59	–	–	–	–	Tambopata	Caído	1 día 8 h 41 min
47	06/06/2025	12:52	PRONATEL NOC	GERENCIA INKASAT	Traslape de incidencias: INC000000082070 + INC000000080805	Se comunica que el día de hoy se ha generado una incidencia en nuestra red que afecta sus servicios: 311074, 1890311081 y 1890311088, correspondientes a los servicios Cusco–Puerto Maldonado.	Puerto Maldonado; Tambopata	Caído	8 h 35 min
48	08/06/2025	17:01	–	–	SUNARP-Urcos Ping Fallo	Buenas noches estimados Sres. de Plasmatronics, su apoyo con la revisión del enlace de Urcos. Desde las 5 pm no se tiene servicio. Indicaron por WhatsApp que se debe a un incidente de Pronatel. Favor de comunicar el restablecimiento.	Urcos	Caído	8 h 10 min

N°	Fecha	Hora	Remitente	Destinatario	Asunto	Cuerpo Correo Inicial	Oficina(s) Afectada(s)	Estado	Tiempo
49	11/06/2025	09:20	–	–	Pérdida de enlace: Azángaro–Macusani	Estimado NOC, se comunica que el día de hoy se ha generado una incidencia en nuestra red que afecta sus servicios. Nos encontramos trabajando para resolver la incidencia a la brevedad posible.	Puerto Maldonado; Tambopata	Caído	9 h 29 min
50	12/06/2025	00:34	–	–	–	–	Tambopata	Caído	8 h 30 min
51	17/06/2025	04:05	–	–	Fwd: SUNARP-Santiago Ping Fallo	Buen día Sres. de Soporte, su apoyo con la revisión de la oficina de Santiago, urgente por favor.	Santiago	Caído	9 h 07 min
52	20/06/2025	10:28	–	–	Pérdida de enlace: Azángaro–Macusani	Estimado NOC, se comunica que el día de hoy se ha generado una incidencia en nuestra red que afecta sus servicios. Nos encontramos trabajando para resolver la incidencia a la brevedad posible.	Puerto Maldonado; Tambopata	Caído	12 h 37 min
53	21/06/2025	13:55	–	–	Intermitencia de enlace: Cusco–Quillabamba	Estimado NOC, se comunica que el día de hoy se ha generado una incidencia en nuestra red que afectó sus servicios: 311024 y 1890311082, correspondientes a los enlaces Ayacucho–Quillabamba y Cusco–Quillabamba.	Quillabamba	Caído	19 min
54	23/06/2025	11:19	–	–	Intermitencia de enlace: Cusco–Quillabamba	Se comunica que el día de hoy se ha generado una incidencia en nuestra red que afectó sus servicios: 311024 y 1890311082, correspondientes a los enlaces Ayacucho–Quillabamba y Cusco–Quillabamba.	Quillabamba	Caído	11 min

N°	Fecha	Hora	Remitente	Destinatario	Asunto	Cuerpo Correo Inicial	Oficina(s) Afectada(s)	Estado	Tiempo
55	23/06/2025	12:44	–	–	Pérdida de enlace: Cusco–Quillabamba	En seguimiento al ticket INC000000082357 de Pronatel, correspondiente a la pérdida de enlace Cusco–Quillabamba, se reportaron cuatro interrupciones: de 12:44 a 13:04, de 15:55 a 16:05, de 16:55 a 19:08 y de 06:54 a 07:13 del día siguiente.	Quillabamba	Caído	3 h 03 min
56	30/06/2025	09:25	–	–	Abancay Ping Fallo (PRTG Network Monitor)	PRTG Network Monitor reportó fallo de Ping en Abancay debido a “TTL expired in transit”.	Abancay	Caído	4 h 04 min
57	30/06/2025	07:00	–	–	Intermitencia y altos tiempos de respuesta en Chalhuahuacho	Buen día estimados Sres. de Plasmatronics, su apoyo con la revisión del enlace de Chalhuahuacho. La red está muy intermitente y con altos tiempos de respuesta. Su apoyo urgente por favor.	Chalhuahuacho	Caído	7 h 02 min
58	03/07/2025	07:55	PRONATEL NOC	GERENCIA INKASAT	SUNARP-Puerto Maldonado Ping Fallo	Buen día señores, favor de revisar el enlace de Puerto Maldonado y Tambopata. De ser posible, si toma tiempo, considerar la contingencia correspondiente.	Puerto Maldonado; Tambopata	Caído	25 min
59	03/07/2025	12:48	PRONATEL NOC	GERENCIA INKASAT	Caída de red en Abancay y Andahuaylas	Buenas tardes señores, su atención con el restablecimiento del servicio en Abancay y Andahuaylas. Desde las 12:48 no se tiene red.	Abancay; Andahuaylas	Caído	6 h 58 min
60	04/07/2025	12:48	PRONATEL NOC	GERENCIA INKASAT	Sin red en San Jerónimo	Buen día estimados, su apoyo con el restablecimiento de la oficina de San Jerónimo por favor. Gracias.	San Jerónimo	Caído	1 día 17 h 30 min

N°	Fecha	Hora	Remitente	Destinatario	Asunto	Cuerpo Correo Inicial	Oficina(s) Afectada(s)	Estado	Tiempo
61	08/07/2025	15:58	PRONATEL NOC	GERENCIA INKASAT	Sin red en Puerto Maldonado y Tambopata	Buenas tardes señores de Plasmatronics, no se tiene red en Puerto Maldonado y Tambopata desde las 4 pm aproximadamente. Favor de revisar con urgencia y, de tratarse de una avería que tome mucho tiempo, activar la contingencia en ambas oficinas.	Puerto Maldonado; Tambopata	Caído	11 min
62	–	–	PRONATEL NOC	GERENCIA INKASAT	–	–	Tambopata	Caído	44 min
63	11/07/2025	08:08	PRONATEL NOC	GERENCIA INKASAT	Caída de red en Zona X	Buen día Sres. de Plasmatronics, desde las 08:08 am aproximadamente se cayó la red en todas las oficinas de Cusco. Se solicita la solución a la brevedad, ya que ninguna sede tiene conexión con Zona X.	Todas las oficinas de Zona X	Caído	1 h 43 min
64	17/07/2025	11:54	–	–	Sin red en MDD y Tambopata	Buenas tardes Sres. de Plasmatronic, su apoyo urgente con la revisión de la red en Puerto Maldonado y Tambopata. De ser el caso, si demora, activar la contingencia para evitar mucho tiempo de indisponibilidad.	Puerto Maldonado; Tambopata	Caído	23 h 45 min
65	18/07/2025	16:15	PRONATEL NOC	GERENCIA INKASAT	Sin llegada a Bodega ni servicios de Sede Central	Buenas tardes, estimados, no tenemos llegada a Bodega. Su atención urgente porque ninguna oficina puede trabajar sin acceso a los servicios de Sede Central.	Todas las oficinas de Zona X	Caído	4 h 31 min

N°	Fecha	Hora	Remitente	Destinatario	Asunto	Cuerpo Correo Inicial	Oficina(s) Afectada(s)	Estado	Tiempo
66	19/07/2025	03:11	PRONATEL NOC	GERENCIA INKASAT	Sin llegada a Bodega ni servicios de Sede Central	Buenas tardes, estimados, no tenemos llegada a Bodega. Su atención urgente porque ninguna oficina puede trabajar sin acceso a los servicios de Sede Central.	Todas las oficinas de Zona X	Caído	2 h 53 min
67	31/07/2025	16:45	PRONATEL NOC	GERENCIA INKASAT	SUNARP-Tambopata Ping Fallo	Buenas tardes estimados, no tenemos red en Tambopata desde las 4:45 pm. Se solicita apoyo para el restablecimiento del servicio.	Sicuani; Espinar; Puerto Maldonado; Tambopata	Caído	20 min

H. Evidencias

Nota. Captura obtenida durante la verificación de bitácoras de incidentes históricos y de red. Elaboración propia.

Nota. Captura obtenida durante la verificación de los activos informáticos registrados en SIGA en la UTI de SUNARP. Elaboración propia.

Nota. Captura obtenida durante la actualización de los activos informáticos. Elaboración propia.

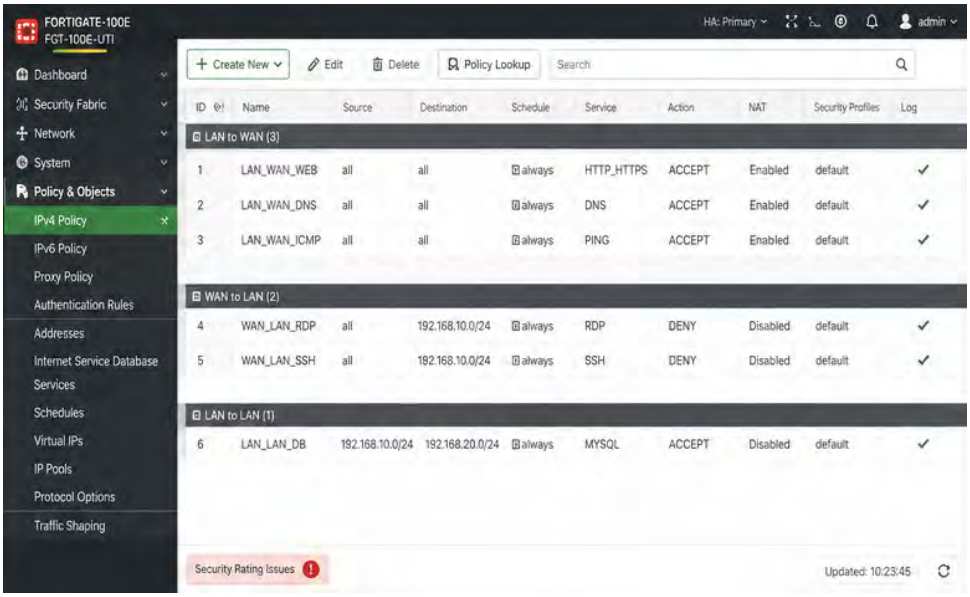
Nota. Captura obtenida durante la verificación del *Network Video Recorder* (NVR) en la UTI de SUNARP. Elaboración propia.

Nota. Captura obtenida durante la verificación del funcionamiento de los servidores en la UTI de SUNARP. Elaboración propia.

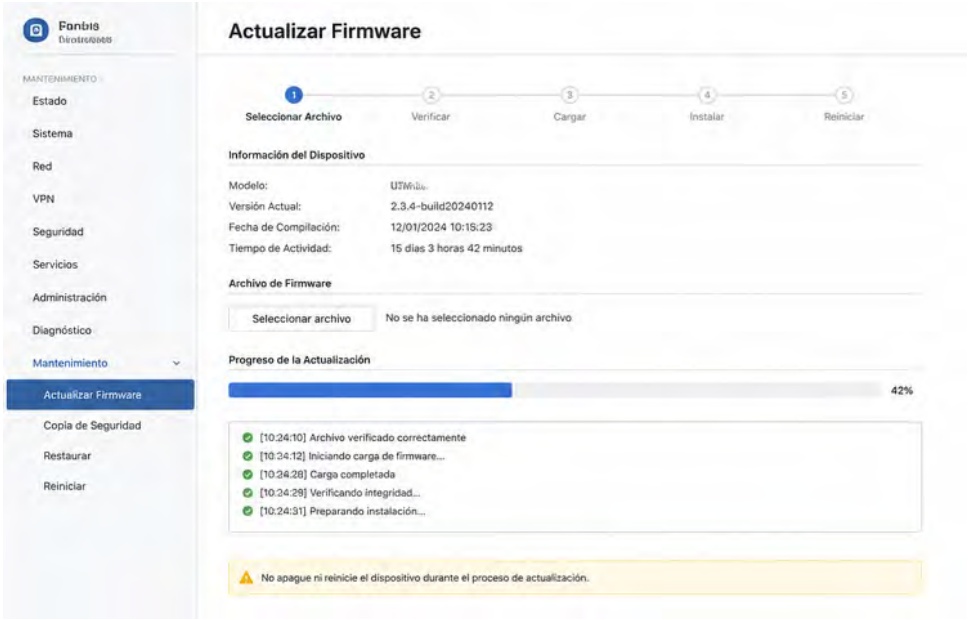
Nota. Captura obtenida durante la verificación del funcionamiento de los activos en los usuarios finales. Elaboración propia.

Nota. La imagen muestra al equipo responsable durante la exposición y validación del modelo propuesto de ciberseguridad, en el marco del programa de capacitación institucional dirigido al personal técnico de la UTI. Elaboración propia.

Nota. Presentación del cronograma secuencial de diez etapas del proceso de investigación utilizadas para diseñar, validar y aplicar el marco NIST CSF propuesto en SUNARP. Elaboración propia.



Nota. Captura de la configuración del control de acceso mediante ACL en los *routers* de red de la UTI, correspondiente al control PR.AC del NIST CSF y al control A.8.20 (Seguridad de las redes) de la norma ISO/IEC 27001:2022. Elaboración propia.



Nota. Captura de la actualización de *firmware* realizada en los *firewalls* y *routers* de la UTI, correspondiente al control PR.IP del NIST CSF y al control A.8.8 (Gestión de las vulnerabilidades técnicas) de la norma ISO/IEC 27001:2022. Elaboración propia.

Nota. Captura del panel centralizado de monitoreo implementado para la detección temprana de anomalías, correspondiente al control DE.CM del NIST CSF y al control A.8.16 (Actividades de monitoreo) de la norma ISO/IEC 27001:2022. Elaboración propia.

Nota. Captura del escaneo periódico de vulnerabilidades realizado con la herramienta OpenVAS, correspondiente al control DE.DP del NIST CSF y al control A.8.8 (Gestión de las vulnerabilidades técnicas) de la norma ISO/IEC 27001:2022. Elaboración propia.

ACTA DE CIERRE DE MODULO DE CAPACITACIÓN

Entidad:	Oficina Registral Cusco
Módulo:	Módulo 1: Introducción al NIST CSF
Fecha de ejecución:	30/05/2025
Modalidad:	Virtual
Instructor(es):	Kenny Carmona Choquemamani y Jeremy Lazo Mendoza
Número de participantes:	12

1. Descripción del módulo:

Se desarrolló el módulo con contenidos teóricos y prácticos orientados a fortalecer las capacidades del personal en ciberseguridad.

2. Resultados de evaluación:

Indicador	Resultado
Promedio general	15.33
Nota máxima	18.00
Nota mínima	13.00
Aprobados	10
Desaprobados	2

3. Competencias alcanzadas:

1 Comprensión de conceptos de ciberseguridad.
2 Aplicación de herramientas y técnicas.
3 Respuesta ante incidentes.

Instructor

Instructor

Participante
Victor Pancorima

Participante
Oscar Garcia

Participante
Jorge Vargas Acosta

Participante
Sony Vello Garcia

Participante
Bryan R. Flores

Participante
Elizabeth Palma Ortega

Participante
J. Miguel Aburuzo A.

Participante
Vladimir Vargas

Participante
Charlyhe Ccoa

Participante
Frady Sanchez

Participante
Luis Ramos.

Participante
Elvis Huaman

ACTA DE CIERRE DE MODULO DE CAPACITACIÓN

Entidad:	Oficina Registral Cusco
Módulo:	Módulo 2: Gestión de vulnerabilidades
Fecha de ejecución:	27/06/2025
Modalidad:	Taller Presencial
Instructor(es):	Kenny Carmona Choquemamani y Jeremy Lazo Mendoza
Número de participantes:	10

1. Descripción del módulo:

Se desarrolló el módulo con contenidos teóricos y prácticos orientados a fortalecer las capacidades del personal en ciberseguridad.

2. Resultados de evaluación:

Indicador	Resultado
Promedio general	16.2
Nota máxima	18
Nota mínima	15
Aprobados	10
Desaprobados	0

3. Competencias alcanzadas:

1 Comprensión de conceptos de ciberseguridad.
2 Aplicación de herramientas y técnicas.
3 Respuesta ante incidentes.

Instructor

Instructor

Participante
Victor Paucorima

Participante
Oscar Garcia

Participante
Jorge Vargas Acosta

Participante
Sony Pello Garcia

Participante
Bryan R. Flores

Participante
Elizabeth Palma Ortega

Participante
L. Miguel Porenzo A.

Participante
Vladimir Vargas

Participante
Charlyne Ccoa

Participante
Fredy Sanchez

Participante

Participante

ACTA DE CIERRE DE MODULO DE CAPACITACIÓN

Entidad:	Oficina Registral Cusco
Módulo:	Módulo 3: Herramientas de detección (OpenVAS y SIEM)
Fecha de ejecución:	25/07/2025
Modalidad:	Laboratorio Practico
Instructor(es):	Kenny Carmona Choquemamani y Jeremy Lazo Mendoza
Número de participantes:	7

1. Descripción del módulo:

Se desarrolló el módulo con contenidos teóricos y prácticos orientados a fortalecer las capacidades del personal en ciberseguridad.

2. Resultados de evaluación:

Indicador	Resultado
Promedio general	17.29
Nota máxima	19
Nota mínima	16
Aprobados	7
Desaprobados	0

3. Competencias alcanzadas:

1 Comprensión de conceptos de ciberseguridad.
2 Aplicación de herramientas y técnicas.
3 Respuesta ante incidentes.

Instructor

Instructor

Participante

Participante
Oscar Garcia

Participante
Jorge Vargas Acosta

Participante

Participante
Bryan R. Flores

Participante
Elizabeth Palma Orbeja

Participante
L. Miguel Lozano A

Participante
Madison Vargas

Participante

Participante

Participante

Participante

ACTA DE CIERRE DE MODULO DE CAPACITACIÓN

Entidad:	Oficina Registral Cusco
Módulo:	Módulo 4: Respuesta a incidentes
Fecha de ejecución:	29/08/2025
Modalidad:	
Instructor(es):	Kenny Carmona Choquemamani y Jeremy Lazo Mendoza
Número de participantes:	9

1. Descripción del módulo:

Se desarrolló el módulo con contenidos teóricos y prácticos orientados a fortalecer las capacidades del personal en ciberseguridad.

2. Resultados de evaluación:

Indicador	Resultado
Promedio general	16.49
Nota máxima	18
Nota mínima	15
Aprobados	9
Desaprobados	0

3. Competencias alcanzadas:

1 Comprensión de conceptos de ciberseguridad.
2 Aplicación de herramientas y técnicas.
3 Respuesta ante incidentes.

Instructor

Instructor

Participante
Victor Paucarima

Participante
OSCAR GARCIA

Participante
Jorge Vargas Acosta

Participante
Sony Tello Garcia

Participante
Bryan R. Flores

Participante
Elizabeth Palma Ortega

Participante
J. Miguel Barriga A

Participante
Vladimir Vargas

Participante
Charlyhe Ccoa

Participante

Participante

Participante

ACTA DE CIERRE DE MODULO DE CAPACITACIÓN

Entidad:	Oficina Registral Cusco
Módulo:	Módulo 5: Recuperación de servicios (RTO y RPO)
Fecha de ejecución:	26/09/2025
Modalidad:	Taller Presencial
Instructor(es):	Kenny Carmona Choquemamani y Jeremy Lazo Mendoza
Número de participantes:	10

1. Descripción del módulo:

Se desarrolló el módulo con contenidos teóricos y prácticos orientados a fortalecer las capacidades del personal en ciberseguridad.

2. Resultados de evaluación:

Indicador	Resultado
Promedio general	17.3
Nota máxima	19
Nota mínima	16
Aprobados	10
Desaprobados	0

3. Competencias alcanzadas:

1 Comprensión de conceptos de ciberseguridad.
2 Aplicación de herramientas y técnicas.
3 Respuesta ante incidentes.

Instructor

Instructor

Participante
Victor Pancorvina

Participante
Osmar Gonzalo

Participante
Jorge Vargas Acosta

Participante
Jony Tello Garcia

Participante
Bryan R. Flores

Participante
Elizabeth Palma Ochoa

Participante
J. Miguel Lorenzo A

Participante
Vladimir Vargas

Participante
Charlyhe Ccoa

Participante
Frady Sanchez

Participante

Participante

ACTA DE CIERRE DE MODULO DE CAPACITACIÓN

Entidad:	Oficina Registral Cusco
Módulo:	Módulo 6: Evaluación de Aprendizajes
Fecha de ejecución:	31/10/2025
Modalidad:	Mixto
Instructor(es):	Kenny Carmona Choquemamani y Jeremy Lazo Mendoza
Número de participantes:	11

1. Descripción del módulo:

Se desarrolló el módulo con contenidos teóricos y prácticos orientados a fortalecer las capacidades del personal en ciberseguridad.

2. Resultados de evaluación:

Indicador	Resultado
Promedio general	17.09
Nota máxima	19
Nota mínima	13
Aprobados	10
Desaprobados	1

3. Competencias alcanzadas:
Evaluación final teórica y práctica de los contenidos abordados durante el semestre.

Instructor

Instructor

Participante
Victor Panoramo

Participante
Oscar Gaggero

Participante
Jorge Vargas Acosta

Participante
Jony Pello Garcia

Participante
Bryan R. Flores

Participante
Elizabeth Palma Ortega

Participante
L. Miguel Lourizo A

Participante
Vladimir Vargas

Participante
Charlyne Cuba

Participante
Fraly Sanchez

Participante
Luis Ramos

Participante

I. Documentos de validación

Cusco, 23 de abril de 2025

ZONA REGISTRAL N° X - SEDE CUSCO
UNIDAD DE TECNOLOGÍAS DE INFORMACIÓN
Help Desk 1
23 ABR. 2025
Exp. N°:
Firma: Hora: 16:05

Señor(a):
Ing. Víctor Andres Paucarima Marroquin
Jefe de la Unidad de Tecnologías de la Información
Zona Registral N.° X – Sede Cusco
Superintendencia Nacional de los Registros Públicos – SUNARP

Asunto: Solicitud de autorización para el uso de la información necesario para la aplicación de trabajo de investigación.

De nuestra consideración:

Por medio de la presente, nosotros, **Kenny Harold Carmona Choquemamani** y **Jeremy Axl Lazo Mendoza**, bachilleres de la Escuela Profesional de Ingeniería Informática y de Sistemas de la Universidad Nacional de San Antonio Abad del Cusco, nos dirigimos a usted con el debido respeto para solicitar la autorización correspondiente para desarrollar y aplicar las actividades contempladas en nuestro trabajo de investigación titulado:

"PROPUESTA DE UN MODELO DE CIBERSEGURIDAD BASADO EN EL MARCO NIST CSF PARA LA GESTIÓN DE VULNERABILIDADES EN LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN DE SUNARP"

El propósito de la investigación es analizar el estado actual de la gestión de vulnerabilidades en la Unidad de Tecnologías de la Información, identificar oportunidades de mejora y proponer mecanismos alineados con las buenas prácticas establecidas por el marco NIST Cybersecurity Framework (NIST CSF) y la norma ISO/IEC 27001.

Las actividades a desarrollar comprenden la aplicación de cuestionarios, entrevistas técnicas, revisión documental de procesos relacionados con la gestión de vulnerabilidades, análisis de infraestructura tecnológica y actividades de capacitación dirigidas al personal participante, garantizando en todo momento la confidencialidad, integridad y uso exclusivo de la información con fines académicos.

Asimismo, nos comprometemos a respetar las políticas institucionales vigentes y a no divulgar información sensible que pudiera comprometer la seguridad de la entidad.

Agradecemos la atención brindada a la presente solicitud y quedamos atentos a cualquier información adicional que considere pertinente.

Atentamente,

Br. Kenny Harold Carmona Choquemamani
Escuela Profesional de Ingeniería Informática y de Sistemas
Firma: _____

Br. Jeremy Axl Lazo Mendoza
Escuela Profesional de Ingeniería Informática y de Sistemas
Firma: _____

CARTA DE AUTORIZACIÓN PARA EL USO DE INFORMACIÓN INSTITUCIONAL Y APLICACIÓN DE LA INVESTIGACIÓN

Cusco, 25 de abril de 2025

Por medio de la presente, la Unidad de Tecnologías de la Información de la Oficina Registral Cusco de la Superintendencia Nacional de los Registros Públicos (SUNARP), representada por **Ing. Victor Andres Paucarima Marroquin**, en calidad de **Jefe de la Unidad de Tecnologías de la Información**, autoriza a los bachilleres:

- Kenny Harold Carmona Choquemamani
- Jeremy Axl Lazo Mendoza

de la Escuela Profesional de Ingeniería Informática y de Sistemas de la Universidad Nacional de San Antonio Abad del Cusco, a utilizar información institucional necesaria para el desarrollo de la investigación titulada:

"PROPUESTA DE UN MODELO DE CIBERSEGURIDAD BASADO EN EL MARCO NIST CSF PARA LA GESTIÓN DE VULNERABILIDADES EN LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN DE SUNARP".

La autorización comprende el acceso y uso académico de información relacionada con:

- Inventario de activos tecnológicos.
- Registros históricos de incidencias tecnológicas.
- Bitácoras y reportes de infraestructura de red.
- Procedimientos internos relacionados con la gestión de vulnerabilidades.
- Información obtenida mediante entrevistas, cuestionarios y encuestas aplicadas al personal de la Unidad de Tecnologías de la Información.
- Documentación técnica necesaria para el diagnóstico y evaluación de la situación actual de la gestión de vulnerabilidades.

Los investigadores se comprometen a utilizar dicha información exclusivamente con fines académicos y de investigación, garantizando en todo momento la confidencialidad de los datos institucionales, la protección de la información sensible y el cumplimiento de los principios éticos aplicables a la investigación científica.

Asimismo, se deja constancia de que los resultados obtenidos serán empleados únicamente para fines académicos y no comprometerán la seguridad, continuidad operativa ni los intereses institucionales de SUNARP.

En señal de conformidad, se suscribe la presente autorización.

Nombre: Ing, Victor Andres Paucarima Marroquin
Cargo: Jefe de la Unidad de Tecnologías de la Información
DNI: 29672047
Unidad de Tecnologías de la Información
Oficina Registral Cusco – SUNARP

VICTOR ANDRES PAUCARIMA MARROQUIN
Jefe de la Unidad de Tecnologías de la Información
Zona Registral N° X - Sede Cusco

ZONA REGISTRAL N° X - SEDE CUSCO
UNIDAD DE TECNOLOGÍAS DE INFORMACIÓN
Help Desk 1
24 JUL. 2026
Exp. N°:
Firma: Hora: 15:56

Cusco, 24 de julio de 2026

Señor(a):
Ing. Víctor Andres Paucarima Marroquin
Jefe de la Unidad de Tecnologías de la Información
Zona Registral N.° X – Sede Cusco
Superintendencia Nacional de los Registros Públicos – SUNARP

Asunto: Solicitud de validación de la ejecución y resultados del trabajo de investigación.

De nuestra consideración:

Por medio de la presente, nosotros, **Kenny Harold Carmona Choquemamani** y **Jeremy Axl Lazo Mendoza**, bachilleres de la Escuela Profesional de Ingeniería Informática y de Sistemas de la Universidad Nacional de San Antonio Abad del Cusco, nos dirigimos a usted con el debido respeto para solicitar la emisión de un documento de conformidad que acredite la correcta ejecución de nuestro trabajo de investigación titulado:

"PROPUESTA DE UN MODELO DE CIBERSEGURIDAD BASADO EN EL MARCO NIST CSF PARA LA GESTIÓN DE VULNERABILIDADES EN LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN DE SUNARP".

Como es de su conocimiento, la investigación fue desarrollada en la Unidad de Tecnologías de la Información de la Oficina Registral Cusco, conforme a la autorización previamente otorgada por su despacho. Durante su ejecución se realizaron las actividades contempladas en el plan de investigación, incluyendo el levantamiento de información, la aplicación de instrumentos de recolección de datos, el análisis de la infraestructura tecnológica, la evaluación del proceso de gestión de vulnerabilidades, la implementación del piloto del modelo propuesto y la validación de los resultados obtenidos.

En ese sentido, solicitamos tenga a bien emitir una constancia donde se deje constancia de que las actividades de investigación fueron efectivamente ejecutadas dentro de la institución y que los resultados obtenidos, así como las conclusiones derivadas del estudio, fueron revisados y validados por la Unidad de Tecnologías de la Información, evidenciando que corresponden a las actividades desarrolladas durante el proceso de investigación.

La presente solicitud tiene como finalidad incorporar dicho documento como evidencia institucional dentro del expediente de sustentación de nuestra tesis.

Agradecemos de antemano la atención brindada y el permanente apoyo otorgado durante el desarrollo de la investigación.

Atentamente,

Br. Kenny Harold Carmona Choquemamani
Escuela Profesional de Ingeniería Informática y de Sistemas
Firma: _____

Br. Jeremy Axl Lazo Mendoza
Escuela Profesional de Ingeniería Informática y de Sistemas
Firma: _____

CARTA DE CONFORMIDAD SOBRE LA EJECUCIÓN Y VALIDACIÓN DE LOS RESULTADOS DEL TRABAJO DE INVESTIGACIÓN

Cusco, 31 de julio de 2026

Por medio de la presente, la Unidad de Tecnologías de la Información de la Oficina Registral Cusco de la Superintendencia Nacional de los Registros Públicos (SUNARP), representada por **Ing. Victor Andres Paucarima Marroquin**, en calidad de **Jefe de la Unidad de Tecnologías de la Información**, deja constancia de que los bachilleres:

- Kenny Harold Carmona Choquemamani
- Jeremy Axl Lazo Mendoza

de la Escuela Profesional de Ingeniería Informática y de Sistemas de la Universidad Nacional de San Antonio Abad del Cusco, desarrollaron y ejecutaron satisfactoriamente el trabajo de investigación titulado:

"PROPUESTA DE UN MODELO DE CIBERSEGURIDAD BASADO EN EL MARCO NIST CSF PARA LA GESTIÓN DE VULNERABILIDADES EN LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN DE SUNARP".

Se deja constancia de que las actividades de investigación fueron realizadas conforme al plan de trabajo autorizado, comprendiendo el diagnóstico de la situación actual de la gestión de vulnerabilidades, la recopilación y análisis de información institucional, la aplicación de instrumentos de investigación, la evaluación técnica de la infraestructura tecnológica, el diseño e implementación del modelo de ciberseguridad propuesto y la ejecución del piloto para validar su funcionamiento.

Asimismo, la Unidad de Tecnologías de la Información verificó el desarrollo de las actividades efectuadas durante la investigación y revisó los resultados obtenidos, constatando que estos reflejan la información recopilada, el análisis realizado y la evidencia generada durante la ejecución del estudio.

En consecuencia, se deja constancia de que las conclusiones y resultados presentados en el trabajo de investigación guardan correspondencia con las actividades desarrolladas en la Unidad de Tecnologías de la Información y constituyen un aporte técnico orientado al fortalecimiento de la gestión de vulnerabilidades, conforme al alcance de la investigación.

Adicionalmente, la Unidad de Tecnologías de la Información expresa su reconocimiento y agradecimiento a los bachilleres **Kenny Harold Carmona Choquemamani** y **Jeremy Axl Lazo Mendoza** por las jornadas de capacitación y sensibilización desarrolladas durante la ejecución de la investigación, las cuales contribuyeron al fortalecimiento de los conocimientos del personal en materia de gestión de vulnerabilidades, ciberseguridad y buenas prácticas basadas en el marco NIST CSF. Estas actividades constituyeron un aporte académico y técnico que favorece la mejora continua de las capacidades institucionales en el ámbito de la seguridad de la información.

La presente conformidad se expide a solicitud de los interesados para los fines académicos que estimen convenientes.

Nombre: Ing. Victor Andres Paucarima Marroquin
Cargo: Jefe de la Unidad de Tecnologías de la Información
DNI: 29672047
Unidad de Tecnologías de la Información
Oficina Registral Cusco – SUNARP

VICTOR ANDRES PAUCARIMA MARROQUIN
Jefe de la Unidad de Tecnologías de la Información
Zona Registral N° X - Sede Cusco

J. Implementación de los controles de ISO/IEC 27001:2022

El presente anexo documenta de manera detallada la aplicación de cada uno de los controles del Anexo A de la norma ISO/IEC 27001:2022 empleados como complemento de las funciones del NIST CSF dentro del modelo de ciberseguridad propuesto para la UTI de SUNARP – Sede Cusco como se muestran en las Tablas 32, 33, 34, 35, 36 y 37. Su propósito es sustentar, para cada control, la forma en que fue implementado, el responsable de su ejecución, la manera en que se adaptó a las condiciones específicas de la institución y del modelo propuesto, y la secuencia de pasos seguida durante el ciclo de mejora continua PDCA. La estructura de cada ficha se elaboró a partir de la información consolidada en las Tablas 7, 8, 9, 16 y 17 del capítulo de Desarrollo de la Investigación, así como de la evidencia fotográfica recogida en el Anexo H. Cabe precisar que, de manera consistente con lo señalado en el capítulo de Resultados y en las Discusiones, la totalidad de los controles descritos a continuación fueron validados en un entorno controlado y bajo la modalidad de piloto en la sede Cusco de la Zona Registral N.° X, por lo que las evidencias presentadas corresponden a una validación referencial y no a una certificación o implementación institucional completa del SGSI.

J.1 Control A.5.9 – Inventario de información y otros activos asociados

Tabla 32
Control A.5.9 – Inventario de información y otros activos asociados

Campo	Descripción
Función NIST CSF relacionada	ID.AM (Identificar – Gestión de activos)
Objetivo del control (ISO/IEC 27001:2022)	Garantizar que la información y los demás activos asociados a la información y a las instalaciones de procesamiento de información se encuentren identificados, y que se mantenga y aplique un inventario adecuado de dichos activos, incluyendo la designación de propietarios responsables.
Responsable de la implementación	UTI
Ámbito / activo de aplicación	Activos tecnológicos de la sede Cusco: servidores, *routers*, *firewalls*, NVR y equipos de usuario final registrados en el sistema institucional SIGA.
Estado de implementación	Implementado en la fase Planificar; verificado en campo durante la fase Verificar.
Evidencia documental	Anexo H – Capturas de la verificación y actualización de los activos informáticos registrados en SIGA.
Fecha de verificación	Verificación de campo realizada durante la fase Hacer del ciclo PDCA (previa a la aplicación de los controles técnicos).

Descripción de la implementación

Se construyó un inventario de activos clasificado y automatizado a partir de la información existente en el sistema institucional SIGA, contrastada con una verificación física en campo de los principales activos de la sede Cusco (servidores, *routers*, NVR y equipos de usuarios finales, según se documenta en el Anexo H). Los registros desactualizados o incompletos fueron corregidos y cada activo fue vinculado a un responsable dentro de la UTI.

Adaptación al contexto institucional y al modelo propuesto

Dado que el diagnóstico inicial evidenció inventarios dispersos y desactualizados —factor que, según lo discutido en el capítulo de Discusiones, se asocia empíricamente a la recurrencia de fallas de red y hardware—, el control se adaptó incorporando el criterio de criticidad definido en el esquema de priorización de vulnerabilidades (Tabla 8), de modo que el inventario no solo identificara los activos sino que los clasificara según su nivel de riesgo (crítico, alto, moderado, bajo) para orientar la asignación de recursos de la UTI.

Pasos seguidos para su aplicación

1. Extracción del listado de activos tecnológicos registrados en el sistema SIGA.
2. Verificación física en campo de los activos críticos (servidores, *routers*, NVR, equipos de usuario final), contrastando el registro formal con el estado real observado.
3. Actualización de los registros desactualizados o incompletos identificados durante la verificación.
4. Clasificación de cada activo según su nivel de criticidad, empleando el esquema de priorización de vulnerabilidades (Tabla 8).
5. Asignación de un responsable de la UTI para cada activo o grupo de activos inventariados.
6. Contraste final del inventario resultante con la categoría ID.AM del NIST CSF, verificando su cobertura funcional.

Resultado obtenido

Se obtuvo un inventario dinámico y confiable (Tabla 7) que sirvió de insumo directo para el esquema de priorización de vulnerabilidades y para la posterior aplicación de los controles de protección y detección.

J.2 Control A.6.3 – Concienciación, educación y formación en seguridad de la información

Tabla 33
Control A.6.3 – Concienciación, educación y formación en seguridad de la información

Campo	Descripción
Función NIST CSF relacionada	PR (Proteger), en articulación con la fase de fortalecimiento de capacidades del modelo propuesto
Objetivo del control (ISO/IEC 27001:2022)	Asegurar que el personal de la organización y las partes interesadas pertinentes reciban una formación adecuada en concienciación y educación sobre seguridad de la información, así como actualizaciones periódicas de las políticas y procedimientos institucionales relevantes para su función.
Responsable de la implementación	UTI, en coordinación con el área de RRHH
Ámbito / activo de aplicación	Personal técnico de la UTI de SUNARP – Sede Cusco (analistas de redes y sistemas, personal de soporte técnico).
Estado de implementación	Diseñado e implementado como plan de capacitación piloto; evaluado en la fase Verificar.
Evidencia documental	Anexo D (cuestionarios teóricos y prácticos), Anexo E (plantilla de acta de cierre) y Anexo H (registro fotográfico de las sesiones).
Fecha de verificación	Ejecutado conforme al cronograma semestral planificado (Tabla 12).

Descripción de la implementación

Se diseñó un programa de capacitación semestral estructurado en seis módulos progresivos (Tabla 12), desarrollado bajo cuatro formatos complementarios: talleres presenciales, sesiones virtuales, laboratorios de práctica guiada y material de autoformación (Tabla 11). El seguimiento del programa se sustentó en cuatro instrumentos: formato de asistencia, formato de evaluación de aprendizajes (escala 0–20), encuesta de satisfacción y acta de cierre de módulo.

Adaptación al contexto institucional y al modelo propuesto

El diseño se adaptó a la diversidad de perfiles, horarios laborales y disponibilidad de recursos del personal de la UTI, combinando modalidades presenciales, virtuales y autónomas. Los contenidos se alinearon directamente con las cinco funciones del NIST CSF (Identificar, Proteger, Detectar, Responder y Recuperar) y con los estándares complementarios ISO/IEC 27001 y 27005, respondiendo al diagnóstico inicial que evidenció que una parte relevante del personal técnico carecía de formación formal en gestión de vulnerabilidades.

Pasos seguidos para su aplicación

1. Diagnóstico de brechas de conocimiento mediante encuestas iniciales al personal técnico.
2. Diseño curricular de los seis módulos progresivos (introducción al NIST CSF, gestión de vulnerabilidades, herramientas de detección, respuesta a incidentes, recuperación de servicios críticos y evaluación final).
3. Selección de las modalidades de capacitación (taller presencial, sesión virtual, laboratorio guiado, autoformación) en función del contenido y del perfil de los participantes.
4. Elaboración de los instrumentos de registro y evaluación (Anexo D y Anexo E).
5. Ejecución piloto de las sesiones formativas, con registro fotográfico de evidencia (Anexo H).
6. Evaluación de resultados y brechas alcanzadas al término de cada módulo (Tabla 18).

Resultados obtenidos

Se logró un personal con competencias inicialmente fortalecidas en la identificación y gestión de vulnerabilidades; sin embargo, la verificación evidenció que el alcance parcial del programa y la ausencia de indicadores longitudinales limitaron la medición integral de su impacto en el desempeño real del personal.

J.3 Control A.8.20 – Seguridad de las redes (complementario con A.5.15 – Control de acceso)

Tabla 34
Control A.8.20 – Seguridad de las redes (complementario con A.5.15 – Control de acceso)

Campo	Descripción
Función NIST CSF relacionada	PR.AC (Proteger – Control de acceso)
Objetivo del control (ISO/IEC 27001:2022)	Gestionar, controlar y proteger las redes y los dispositivos de red para salvaguardar la información en los sistemas y aplicaciones, restringiendo el acceso a los usuarios y servicios estrictamente autorizados.
Responsable de la implementación	Bryan Flores – Operador de Sistemas de Red
Ámbito / activo de aplicación	*Routers* de red de la sede piloto Cusco (activo simulado).
Estado de implementación	Piloto, validado en entorno controlado.
Evidencia documental	Anexo H – Captura de la configuración de la ACL.
Fecha de verificación	04/07/2025

Descripción de la implementación

Se configuraron las ACL en los *routers* de red identificados como críticos, restringiendo el tráfico y los accesos exclusivamente a usuarios y direcciones autorizadas. De manera complementaria, se aplicó segmentación de red para reducir la superficie de ataque de los dispositivos críticos.

Adaptación al contexto institucional y al modelo propuesto

El control se aplicó de forma simulada sobre los *routers* de la sede Cusco identificados como de alta criticidad en el esquema de priorización de vulnerabilidades (Tabla 8), priorizando aquellos activos cuya afectación tendría mayor impacto sobre la continuidad de los servicios re-

gistrales. La segmentación complementaria se incorporó como respuesta directa a la recurrencia de caídas de red identificada en la bitácora de incidentes de red (Anexo G).

Pasos seguidos para su aplicación

1. Identificación de los *routers* de mayor criticidad a partir del inventario de activos y del esquema de priorización de vulnerabilidades.
2. Definición de las reglas de control de acceso según los perfiles de usuario autorizados de la UTI.
3. Configuración de las ACL en los dispositivos de red seleccionados.
4. Aplicación de segmentación de red para limitar la propagación de un eventual incidente.
5. Prueba de acceso restringido para verificar que solo los usuarios autorizados pudieran conectarse.
6. Registro fotográfico de la configuración como evidencia y validación por el responsable técnico el 04/07/2025.

Resultado obtenido

Se logró restringir los accesos exclusivamente a los usuarios autorizados (Tabla 9), fortaleciendo el control perimetral de los dispositivos de red evaluados en el piloto.

J.4 Control A.8.8 – Gestión de las vulnerabilidades técnicas (acción de remediación)

Tabla 35
Control A.8.8 – Gestión de las vulnerabilidades técnicas (acción de remediación)

Campo	Descripción
Función NIST CSF relacionada	PR.IP (Proteger – Procesos y procedimientos de protección de la información)
Objetivo del control (ISO/IEC 27001:2022)	Obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información en uso, evaluar la exposición de la organización ante ellas y tomar las medidas apropiadas para su remediación.
Responsable de la implementación	Jony Tello – Analista de Redes (Sede Cusco)
Ámbito / activo de aplicación	*Firewalls* y *routers* de la sede piloto Cusco (activo simulado).
Estado de implementación	Piloto, validado en entorno controlado.
Evidencia documental	Anexo H – Captura de la actualización de *firmware*.
Fecha de verificación	11/07/2025

Descripción de la implementación

A partir de las vulnerabilidades detectadas mediante los escaneos periódicos con OpenVAS (control DE.DP, descrito en la siguiente ficha), se ejecutó la actualización de *firmware* y software en los *firewalls* y *routers* identificados como vulnerables.

Adaptación al contexto institucional y al modelo propuesto

El control se articuló como la etapa de remediación de un ciclo de detección–corrección: los hallazgos del escaneo de vulnerabilidades alimentaron directamente la priorización de los dispositivos a actualizar, concentrando el esfuerzo en el *firmware* desactualizado identificado como riesgo de nivel moderado en el esquema de priorización (Tabla 8).

Pasos seguidos para su aplicación

1. Identificación de dispositivos con *firmware* desactualizado a partir de los resultados del escaneo con OpenVAS.
2. Verificación de las versiones de *firmware* disponibles publicadas por el fabricante de cada dispositivo.
3. Planificación de una ventana de mantenimiento para minimizar la afectación al servicio.
4. Ejecución de la actualización de *firmware* y software en los *firewalls* y *routers* seleccionados.
5. Verificación posterior del funcionamiento correcto de los dispositivos actualizados.
6. Registro fotográfico de la actualización como evidencia y validación por el responsable técnico el 11/07/2025.

Resultado obtenido

Se logró una reducción de las vulnerabilidades técnicas conocidas en los dispositivos actualizados (Tabla 9), cerrando parcialmente las brechas detectadas en la fase de escaneo.

J.5 Control A.8.16 – Actividades de monitoreo

Tabla 36
Control A.8.16 – Actividades de monitoreo

Campo	Descripción
Función NIST CSF relacionada	DE.CM (Detectar – Monitoreo continuo de seguridad)
Objetivo del control (ISO/IEC 27001:2022)	Monitorear las redes, los sistemas y las aplicaciones en busca de comportamientos anómalos, y evaluar los posibles incidentes de seguridad de la información mediante mecanismos de alerta temprana.
Responsable de la implementación	Miguel Lorenzo – Administrador de Servidores
Ámbito / activo de aplicación	Servidores de la sede piloto Cusco (activo simulado).
Estado de implementación	Piloto, validado en entorno controlado.
Evidencia documental	Anexo H – Captura del panel centralizado de monitoreo.
Fecha de verificación	18/07/2025

Descripción de la implementación

Se implementó un panel centralizado de monitoreo orientado a la detección temprana de anomalías en los servidores de la sede Cusco, generando alertas ante posibles intentos de intrusión.

Adaptación al contexto institucional y al modelo propuesto

El control se orientó a atender la dependencia de una gestión predominantemente reactiva identificada en el diagnóstico inicial, dotando a la UTI de un mecanismo de visibilidad continua sobre los servidores críticos del *Data Center*, cuya falla se identificó como uno de los escenarios de mayor impacto en la Tabla 10.

Pasos seguidos para su aplicación

1. Selección de la herramienta de monitoreo centralizado a emplear en el entorno piloto.
2. Definición de los indicadores y umbrales de alerta relevantes para los servidores críticos.
3. Instalación y configuración del panel de monitoreo sobre los servidores seleccionados.
4. Prueba de generación de alertas ante eventos simulados de anomalía o intrusión.
5. Registro fotográfico del panel en funcionamiento como evidencia y validación por el responsable técnico el 18/07/2025.

Resultado obtenido

Se logró la generación de alertas tempranas ante intentos de intrusión (Tabla 9), lo que —de acuerdo con los resultados de la Tabla 10— contribuyó a reducir el tiempo de detección en los escenarios simulados evaluados.

J.6 Control A.8.8 – Gestión de las vulnerabilidades técnicas (acción de detección)

Tabla 37
Control A.8.8 – Gestión de las vulnerabilidades técnicas (acción de detección)

Campo	Descripción
Función NIST CSF relacionada	DE.DP (Detectar – Procesos de detección)
Objetivo del control (ISO/IEC 27001:2022)	Obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información en uso mediante procesos sistemáticos de identificación y evaluación de su exposición.
Responsable de la implementación	Oscar García – Técnico de Soporte Informático
Ámbito / activo de aplicación	Equipos de red de la sede piloto Cusco (activo simulado).
Estado de implementación	Piloto, validado en entorno controlado.
Evidencia documental	Anexo H – Captura del escaneo con OpenVAS.
Fecha de verificación	25/07/2025

Descripción de la implementación

Se ejecutaron escaneos periódicos de vulnerabilidades sobre los equipos de red mediante la herramienta OpenVAS, con el fin de identificar configuraciones inseguras y *firmware* desactualizado.

Adaptación al contexto institucional y al modelo propuesto

Este control corresponde al mismo requisito normativo A.8.8 aplicado a la etapa de detección —a diferencia de la actualización de *firmware*, que constituye la acción de remediación—, por lo que ambos controles se diseñaron de manera articulada dentro del ciclo de gestión de vulnerabilidades técnicas del modelo propuesto, reforzando además las competencias del

personal en el uso de herramientas de escaneo trabajadas durante el programa de capacitación (control A.6.3).

Pasos seguidos para su aplicación

1. Instalación y configuración de la herramienta OpenVAS en el entorno de prueba.
2. Definición del alcance (equipos de red) y de la periodicidad de los escaneos.
3. Ejecución de los escaneos periódicos sobre los equipos seleccionados.
4. Análisis de los resultados para identificar configuraciones inseguras y vulnerabilidades técnicas.
5. Retroalimentación de los hallazgos hacia el control de remediación (actualización de *firmware*).
6. Registro fotográfico del escaneo como evidencia y validación por el responsable técnico el 25/07/2025.

Resultado obtenido

Se logró identificar configuraciones inseguras en los equipos de red evaluados (Tabla 9), insumo que permitió priorizar las acciones de remediación descritas en el control A.8.8 (remediación).