

UNIVERSIDAD PERUANA LOS ANDES
FACULTAD DE INGENIERIA
**ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS
Y COMPUTACIÓN**



**IMPLEMENTACIÓN DE LA PLATAFORMA DE INTERCAMBIO
DE INFORMACIÓN DE MALWARE PARA LA PREDICCIÓN DE
CIBERATAQUES DEL DEPARTAMENTO DE
CIBERSEGURIDAD, LIMA**

**PARA OPTAR EL TÍTULO PROFESIONAL DE:
INGENIERIA DE SISTEMAS Y COMPUTACIÓN**

AUTOR:

Bach. IBARRA ROJAS, DANNY STEPH

ASESOR:

Mg. QUISPE REYES, CARLOS FELIX

LÍNEA DE INVESTIGACIÓN:

NUEVAS TECNOLOGÍAS Y PROCESOS

HUANCAYO – PERÚ

2021

HOJA DE CONFORMIDAD DE JURADOS

**DR. RUBEN DARIO TAPIA SILGUERA
PRESIDENTE**

**DR. MAGNO TEÓFILO BALDEON TOVAR
JURADO**

**DR. EDWARD EDDIE BUSTINZA ZUASNABAR
JURADO**

**MG. MAGLIONI ARANA CAPARACHIN
JURADO**

**MG. LEONEL UNTIVEROS PEÑALOZA
SECRETARIO DOCENTE**

DEDICATORIA

Al forjador de mi camino, a Dios, por acompañarme y siempre levantarme de mis caídas y cuidar de mí, y que cada día con mi fe, he podido lograr el término de esta meta. También dedicar a mi madre Gemina Rojas quien es el motor y guía en mi camino. Asimismo, dedicar a mi hijo Thiago André quien se convierte en la luz de un nuevo camino en mi vida. Por otro lado, dedico este trabajo a mi abuelito Q.E.P.D., Santos Rojas Parrilla, quien en vida fue la figura paterna y me acompañó en lo largo de mi camino, que también fue el apoyo y fortaleza para cumplir esta meta que hoy se convierte en una realidad culminada.

AGRADECIMIENTO

Este informe es el resultado del esfuerzo y dedicación para mi trabajo de investigación de tesis realizado en el período de 2021, como parte de mi estudio en la carrera de Ingeniería de Sistemas y Computación en la Universidad Peruana de los Andes. Estoy muy satisfecho con el progreso y el resultado de este estudio, que no fue posible sin la cooperación y el apoyo de varias personas y sus organizaciones. Me complace tomar esto como una oportunidad para agradecerles su asistencia y contribución para este estudio.

Primeramente, mi más profunda gratitud a Dios, por ser la fuerza más grande que me motiva e impulsa a seguir avanzando y aprovechando cada nueva oportunidad que se presenta.

Un agradecimiento muy especial a mi madre e hijo, por brindarme la motivación y el entusiasmo durante todo el período de esta tesis

Seguidamente, agradecer a mi esposa quien me apoyó incondicionalmente durante mi formación profesional, es una persona que me inspira cada día en auto superarme y soy capaz de apostar todo por ella.

De igual manera mis agradecimientos a la Universidad Peruana los Andes (UPLA) a toda la facultad de Ingeniería, a mis profesores y asesores en especial a la Dra. Karin Rojas Romero, el Dr. Luis Torres Cabanillas y el Mg Carlos Félix Quispe Reyes, quienes me han apoyado de muchas maneras; sin su aliento, confianza en mi trabajo y retroalimentación oportuna y constructiva, este estudio apenas se habría completado. Gracias a ellos quienes me brindaron conocimientos muy importantes los cuales fueron una guía de mi camino profesional.

Es un honor para mí reconocer las diversas ayudas que he recibido de todos los miembros de mi familia, amigos y compañeros de trabajo, les agradezco sus sugerencias y comentarios a lo largo de la planificación y el desarrollo de este trabajo de tesis. Su buena disposición para dedicar su tiempo tan generosamente ha sido muy apreciada.

CONSTANCIA 176

DE SIMILITUD DE TRABAJOS DE INVESTIGACIÓN POR EL SOFTWARE DE PREVENCIÓN DE PLAGIO TURNITIN

La Dirección de Unidad de Investigación de la Facultad de Ingeniería, hace constar por la presente, que el informe final de tesis titulado IMPLEMENTACIÓN DE LA PLATAFORMA DE INTERCAMBIO DE INFORMACIÓN DE MALWARE PARA LA PREDICCIÓN DE CIBERATAQUES DEL DEPARTAMENTO DE CIBERSEGURIDAD, LIMA.

Cuyo autor (a) (es) : Danny Steph, Ibarra Rojas.
Facultad : Ingeniería.
Escuela Profesional : Ingeniería de Sistemas y Computación
Asesor (a) (es) : Mg. Carlos Félix, Quispe Reyes.

Que, fue presentado con fecha 24.05.2023 y después de realizado el análisis correspondiente en el software de prevención de plagio Turnitin con fecha 25.05.2023; con la siguiente configuración de software de prevención de plagio Turnitin:

- Excluye bibliografía.
- Excluye citas.
- Excluye cadenas menores de a 20 palabras.
- Otro criterio (especificar)

Dicho documento presenta un porcentaje de similitud de 19%. En tal sentido, de acuerdo a los criterios de porcentajes establecidos en el artículo N°11 del Reglamento de uso de software de prevención de plagio, el cual indica que no se debe superar el 30%. Se declara, que el trabajo de investigación: si contiene un porcentaje aceptable de similitud. Observaciones: ninguna.

En señal de conformidad y verificación se firma y sella la presenta constancia.

Huancayo 29 de mayo del 2023



Dr. Santiago Zevallos Salinas
Director de la Unidad de Investigación

CONTENIDO

CONTENIDO	6
CONTENIDO DE TABLAS	8
CONTENIDO DE FIGURAS.....	9
RESUMEN.....	10
ABSTRACT.....	11
INTRODUCCIÓN.....	12
CAPÍTULO I.....	13
PLANTEAMIENTO DEL PROBLEMA.....	13
1.1 Descripción de la realidad problemática.....	13
1.2 Delimitación del problema.....	17
1.2.1 Espacial	17
1.2.2 Temporal.....	18
1.3 Formulación del problema.....	18
1.3.1 Problema General.....	18
1.3.2 Problemas Específicos	18
1.4 Justificación.....	18
1.4.1 Práctica	18
1.4.2 Teórica	19
1.4.3 Metodológica.....	19
1.5 Objetivos	19
1.5.1 Objetivo General.....	19
1.5.2 Objetivos Específicos	20
CAPÍTULO II.....	21
MARCO TEÓRICO.....	21
2.1 Antecedentes	21
2.1.1 Antecedentes Internacionales	21
2.1.2 Antecedentes Nacionales.....	26
2.2 Marco Conceptual	29
2.2.1 Definición de las Variables y sus dimensiones	29
2.2.2 Definición de la metodología implementada en la investigación	36
2.3 Definición de términos.....	44
CAPÍTULO III.....	46
HIPÓTESIS.....	46
3.1 Hipótesis General.....	46
3.2 Hipótesis Específicas	46
3.3 Variables	46
3.3.1 Definición Conceptual de las variables	46
3.3.2 Definición Operacional de las variables	47

CAPITULO IV	48
METODOLOGÍA.....	48
4.1 Método de Investigación	48
4.2 Tipo de Investigación	48
4.3 Nivel de Investigación	48
4.4 Diseño de Investigación.....	49
4.5 Población y muestra.....	50
4.6 Técnicas e Instrumentos de recolección de datos	50
4.6.1 Nivel de Confiabilidad	51
4.7 Técnicas de procesamiento y análisis de datos	55
4.7.1 Procesamiento de información	55
4.7.2 Análisis de datos.....	55
4.8 Aspectos éticos de la Investigación	55
4.9 Desarrollo de la solución.....	56
IMPLEMENTACIÓN DE LA PLATAFORMA DE INTERCAMBIO DE INFORMACIÓN DE MALWARE (MISP)	57
APLICACIÓN DE LA METODOLOGÍA CYBERSECURITY FRAMEWORK NIST EN EL FUNCIONAMIENTO DE LA PLATAFORMA MISP.	74
CAPITULO V	86
RESULTADOS	86
5.1 Descripción de resultados.....	86
5.2 Contrastación de hipótesis.....	93
5.2.1 Prueba de contraste de hipótesis general.....	95
5.2.2 Prueba de contraste para hipótesis específica 1	96
5.2.3 Prueba de contraste para hipótesis específica 2	98
5.2.4 Prueba de contraste para hipótesis específica 3	99
ANÁLISIS Y DISCUSIÓN DE RESULTADOS	101
CONCLUSIONES.....	105
RECOMENDACIONES	107
REFERENCIAS BIBLIOGRÁFICAS.....	108
ANEXOS.....	111
Anexo 1: Matriz de consistencia	111
Anexo 2: Matriz de operacionalización de las variables.....	113
Anexo 3: Matriz de operacionalización del instrumento	114
Anexo 4: Instrumento de investigación.....	115
Anexo 5: Validez del instrumento	118
Anexo 6: Data de procesamiento de datos	120
Anexo 7: Consentimiento / Carta de aceptación	122

CONTENIDO DE TABLAS

TABLA I CORRELACIÓN DE PEARSON PARA TIEMPO EN REALIZAR LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS	52
TABLA II CORRELACIÓN DE PEARSON PARA NÚMERO DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS.....	53
TABLA III CORRELACIÓN DE PEARSON PARA TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD	54
TABLA IV IDENTIFICACIÓN DE ACTIVOS.....	75
TABLA V IDENTIFICACIÓN DE AMENAZAS CIBERNÉTICAS.....	76
TABLA VI ESTUDIO DE LA CONDICIÓN GESTIÓN DE ACTIVOS	77
TABLA VII ESTUDIO DE LA CONDICIÓN EVALUACIÓN DE RIESGOS.....	77
TABLA VIII ESTUDIO DE LA CONDICIÓN ESTRATEGIA DE GESTIÓN DE RIESGOS.....	77
TABLA IX MEDIDAS Y CONTROLES DE SEGURIDAD.....	78
TABLA X ESTUDIO DE LA CONDICIÓN GESTIÓN DE IDENTIDAD Y CONTROL DE ACCESO	79
TABLA XI ESTUDIO DE LA CONDICIÓN CONCIENCIA Y CAPACITACIÓN	79
TABLA XII ESTUDIO DE LA CONDICIÓN SEGURIDAD DE DATOS	79
TABLA XIII ESTUDIO DE LA CONDICIÓN PROCESOS Y PROCEDIMIENTOS DE PROTECCIÓN DE LA INFORMACIÓN	80
TABLA XIV ESTUDIO DE LA CONDICIÓN MANTENIMIENTO.....	80
TABLA XV VULNERABILIDADES CIBERNÉTICAS.....	81
TABLA XVI ESTUDIO DE LA CONDICIÓN ANOMALÍAS Y EVENTOS	81
TABLA XVII ESTUDIO DE LA CONDICIÓN VIGILANCIA CONTINUA DE SEGURIDAD	82
TABLA XVIII ESTUDIO DE LA CONDICIÓN PROCESOS DE DETECCIÓN	82
TABLA XIX ESTUDIO DE LA CONDICIÓN PLANIFICACIÓN DE RESPUESTA	83
TABLA XX ESTUDIO DE LA CONDICIÓN COMUNICACIONES	83
TABLA XXI ESTUDIO DE LA CONDICIÓN ANÁLISIS.....	83
TABLA XXII ESTUDIO DE LA CONDICIÓN MITIGACIÓN	84
TABLA XXIII ESTUDIO DE LA CONDICIÓN MEJORAS	84
TABLA XXIV ESTUDIO DE LA CONDICIÓN PLANIFICACIÓN DE RECUPERACIÓN.....	85
TABLA XXV ESTUDIO DE LA CONDICIÓN MEJORAS	85
TABLA XXVI ESTUDIO DE LA CONDICIÓN COMUNICACIONES.....	86
TABLA XXVII ESTADÍSTICOS DESCRIPTIVOS DE LAS DIMENSIONES POR TIPO DE PRUEBA	86
TABLA XXVIII RESUMEN DE LOS ESTADÍSTICOS DESCRIPTIVOS DE LAS DIMENSIONES.	89
TABLA XXIX PRUEBA DE NORMALIDAD DE KOLMOGÓROV-SMIRNOV	94
TABLA XXX RANGOS PARA PRUEBA DE U DE MANN-WHITNEY	95
TABLA XXXI ESTADÍSTICOS DE PRUEBA PARA PRUEBA DE U DE MANN-WHITNEY	96
TABLA XXXII RANGOS PARA PRUEBA DE U DE MANN-WHITNEY - TIEMPO EN REALIZAR LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS	97
TABLA XXXIII ESTADÍSTICOS DE PRUEBA PARA PRUEBA DE U DE MANN-WHITNEY - TIEMPO EN REALIZAR LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS.	97
TABLA XXXIV RANGOS PARA PRUEBA DE U DE MANN-WHITNEY - NÚMERO DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS	98
TABLA XXXV ESTADÍSTICOS DE PRUEBA PARA PRUEBA DE U DE MANN-WHITNEY - NÚMERO DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS....	99
TABLA XXXVI RANGOS PARA PRUEBA DE U DE MANN-WHITNEY - TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD	100
TABLA XXXVII ESTADÍSTICOS DE PRUEBA PARA PRUEBA DE U DE MANN-WHITNEY - TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD.....	100
TABLA XXXVIII MATRIZ DE CONSISTENCIA.....	111
TABLA XXXIX MATRIZ DE OPERACIONALIZACIÓN DE VARIABLE DEPENDIENTE: PREDICCIÓN DE CIBERATAQUES	113
TABLA XL MATRIZ DE OPERACIONALIZACIÓN DEL INSTRUMENTO.....	114
TABLA XLI DATA DE PROCESAMIENTO DE DATOS.....	120

CONTENIDO DE FIGURAS

FIG. 1. UBICACIÓN GEOGRÁFICA DEL DEPARTAMENTO DE CIBERSEGURIDAD DE LA DIVISIÓN DE INFORMÁTICA DIRTIC PNP.	17
FIG. 2. PORTAL DEL MALWARE INFORMATION SHARING PLATFORM (MISP).	30
FIG. 3. INTERACCIÓN DE INSTANCIAS MISP.	32
FIG. 4. DESCRIPCIÓN GENERAL DE LAS AMENAZAS EN MISP.	33
FIG. 5. COMPONENTES PRINCIPALES DEL MARCO DE CIBERSEGURIDAD.	36
FIG. 6. ESTRUCTURA DEL NÚCLEO DEL MARCO DE CIBERSEGURIDAD NIST.	37
FIG. 7. FUNCIONES DEL MARCO NIST.	39
FIG. 8. CATEGORÍAS, SUBCATEGORÍAS Y REFERENCIAS INFORMATIVAS.	40
FIG. 9. NIVELES DE IMPLEMENTACIÓN DEL MARCO NIST.	42
FIG. 10. PERFILES DEL MARCO DE CIBERSEGURIDAD NIST.	43
FIG. 11. MARCO DE TRABAJO DE CIBERSEGURIDAD NIST.	44
FIG. 12. DISEÑO DE INVESTIGACIÓN.	49
FIG. 13. TABLA DE CONFIABILIDAD, HERNÁNDEZ, FERNÁNDEZ Y BAPTISTA (2010).	55
FIG. 14. MEDIDOR DE HARDWARE PARA IMPLEMENTAR MISP.	58
FIG. 15. PROCEDIMIENTO PARA LA INSTALACIÓN DE LA PLATAFORMA MISP.	59
FIG. 16. AGREGAR USUARIO “MISP” CON PRIVILEGIOS DE ADMINISTRADOR.	59
FIG. 17. DESCARGA DE SCRIPT DE MISP.	60
FIG. 18. EJECUTAR SCRIPT DE MISP.	60
FIG. 19. INSTALACIÓN AUTOMÁTICA DE MISP.	61
FIG. 20. CREDENCIALES DE ACCESO AL MISP.	61
FIG. 21. ACCESO A INTERFAZ DE MISP.	62
FIG. 22. CAMBIO DE CONTRASEÑA.	62
FIG. 23. USUARIO ADMINISTRADOR DE MISP.	63
FIG. 24. INICIO DE SESIÓN EN MISP.	63
FIG. 25. DEMOSTRACIÓN DE LA INSTALACIÓN MISP.	64
FIG. 26. LISTADO DE TODOS LOS EVENTOS EN MISP.	65
FIG. 27. VISTA DETALLADA DE UN EVENTO EN MISP.	66
FIG. 28. LISTADO DE ATRIBUTOS ADJUNTOS EN UN EVENTO MISP.	67
FIG. 29. DESCARGAR EVENTO DE MISP.	67
FIG. 30. AGREGAR EVENTO EN MISP.	69
FIG. 31. INFORMACIÓN DEL EVENTO CREADO EN MISP.	69
FIG. 32. AGREGAR ATRIBUTOS EN EL EVENTO MISP.	70
FIG. 33. ATRIBUTOS AGREGADOS EN EL EVENTO MISP.	71
FIG. 34. AGREGAR ETIQUETAS EN EL EVENTO MISP.	71
FIG. 35. ETIQUETAS AGREGADAS EN EL EVENTO MISP.	72
FIG. 36. PUBLICAR EVENTO MISP.	72
FIG. 37. EVENTO PUBLICADO EN MISP.	73
FIG. 38. UTILIZACIÓN DE PLATAFORMA DE INTERCAMBIO DE INFORMACIÓN DE MALWARE (MISP).	73
FIG. 39. FUNCIONES MARCO CIBERSEGURIDAD NIST.	74
FIG. 40. DIAGRAMA DE CAJAS SOBRE CAPACIDADES DE MONITOREO – TIEMPO EN REALIZAR LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS (PRE TEST) Y (POST TEST).	91
FIG. 41. DIAGRAMA DE CAJAS SOBRE CAPACIDADES DEFENSIVAS – NÚMERO DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS (PRE TEST) Y (POST TEST).	92
FIG. 42. DIAGRAMA DE CAJAS SOBRE ACCIONES PREVENTIVAS – TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD (PRE TEST) Y (POST TEST).	93
FIG. 43. FICHA DE REGISTRO TIEMPO EN REALIZAR LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS.	115
FIG. 44. FICHA DE REGISTRO NÚMERO DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS.	116
FIG. 45. FICHA DE REGISTRO TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD.	117
FIG. 46. CERTIFICADO DE VALIDEZ ESPECIALIDAD.	118
FIG. 47. CERTIFICADO DE VALIDEZ METODOLÓGICO.	119
FIG. 48. CARTA DE ACEPTACIÓN.	122

RESUMEN

La presente investigación titulada “Implementación de la plataforma de intercambio de información de malware para la predicción de ciberataques en el Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP”, la problemática se ha basado en establecer si la implementación de la plataforma de intercambio de información de malware mejora la predicción de ciberataques, continuando con el objetivo fue determinar que la implementación de la plataforma de intercambio de información de malware mejora la predicción de ciberataques. Asimismo, se planteó la metodología de la investigación aplicada, con un enfoque cuantitativo y diseño de investigación experimental. En efecto, la conclusión de la investigación se da por necesidades y requerimientos funcionales que ostentó para la predicción de ciberataques y que, con la implementación de la plataforma de intercambio de información de malware (MISP) ayudó a fortalecer los niveles de seguridad en el Departamento de Ciberseguridad.

Palabras claves: ciberseguridad, ciberataque, malware, MISP.

ABSTRACT

The present investigation entitled "Implementation of the platform for the exchange of malware information for the prediction of cyberattacks in the Department of Cybersecurity of the Division of Informatics of the DIRTIC PNP", the problem has been based on establishing whether the implementation of the platform of Malware information exchange improves the prediction of cyberattacks, continuing with the objective was to determine that the implementation of the malware information exchange platform improves the prediction of cyberattacks. Likewise, the applied research methodology was raised, with a quantitative approach and experimental research design. Indeed, the conclusion of the investigation is given by needs and functional requirements that it held for the prediction of cyberattacks and that, with the implementation of the malware information exchange platform (MISP) helped to strengthen the security levels in the Department of Cybersecurity.

Keywords: cybersecurity, cyberattack, malware, MISP.

INTRODUCCIÓN

Hoy en día recopilar, procesar y compartir información es un aspecto crítico en la gestión de la ciberseguridad. El informe tuvo como objetivo determinar que la implementación de la plataforma de intercambio de información de malware mejora la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la Dirección de Tecnología de la Información y Comunicaciones de la Policía Nacional del Perú (DIRTIC PNP). La implementación y funcionamiento de la plataforma se realizó siguiendo las fases del Cybersecurity Framework v1.1 de NIST, por ser un marco de ciberseguridad que integra estándares y mejores prácticas que ayudan a las organizaciones a gestionar los riesgos y a navegar de una manera más segura. El presente informe de tesis se enmarca en cinco capítulos, detallando a continuación cada uno de ellos:

Capítulo primero: El problema de investigación, describe el planteamiento, la delimitación espacial y temporal, así como también la formulación del problema general y problemas específicos. Asimismo, se justifica el aporte práctico, teórico y metodológico; y, por último, se define el objetivo general y los objetivos específicos de la investigación.

Capítulo segundo: El marco teórico, se basó en teorías, artículos científicos ubicadas en los motores de búsqueda de investigaciones científicas y también se consideró tesis internacionales y nacionales para profundizar los antecedentes que aportan a la investigación.

Capítulo tercero: Damos a conocer la hipótesis general y específicas, las variables y su operacionalización.

Capítulo cuarto: Damos a conocer la metodología de estudio teniendo en cuenta el método, tipo, nivel y diseño de la investigación; población y muestra; técnicas e instrumentos de recolección de datos y procesamiento del mismo, asimismo el desarrollo de la solución.

Capítulo quinto: Se describe los resultados de la investigación con interpretación para cada variable, con la prueba de hipótesis correspondiente.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la realidad problemática

El 2020 ha sido un año de transformaciones tecnológicas en el que las instituciones, organizaciones, entidades públicas, privadas, y los usuarios se han visto obligados acomodarse a un nuevo modelo de vida, en cuanto al distanciamiento social, el empleo de tecnologías para conservar la comunicación y el teletrabajo con todas las medidas que este acarreaba.

Referente a lo expuesto anteriormente, los ciberdelincuentes supieron utilizar estos nuevos modelos de vida para encontrar nuevas aberturas de ciberseguridad tanto en la infraestructura de la institución como en los usuarios, por medio del uso de la ingeniería social y otras técnicas de ciberataques.

Empezando por el contexto mundial, según [1] en su reporte de incidentes y amenazas, informó sobre el aumento masivo de ataques de ransomware que afectaron a empresas e instituciones de todo el mundo, representando actualmente la amenaza informática más grave para las empresas e instituciones en términos de cantidad de ataques diarios y su impacto potencial en la continuidad del negocio, generando una pérdida financiera de \$18 millones anuales, el cual demostró la importancia de contar con un sistema que ayude a recopilar y compartir información de los ciberataques, que ayude a mejorar sus sistemas y procedimientos de seguridad informática.

El año 2020 simbolizó la máxima incidencia de ciberdelitos en el cual el virus del Sars-Cov2 presentaba consecuencias que vinculaban con aquellos ataques que prácticamente dejó al descubierto las vulnerabilidades que presentaron gran cantidad de empresas que no tenían la forma adecuada de trabajar remotamente. Por ello, la [2] en su informe tecnológico menciona distintos temas acerca de la repercusión que padeció la ciberseguridad debido a las consecuencias de la pandemia, para lo cual se detectó un aumento no solo en la cantidad de ciberataques, sino más bien en la intensidad de estos hechos. En cifras, en el 2019, se detectó 3.172 amenazas

cibernéticas de alto nivel de peligro, mientras que, en el año 2020, se registró 6.690 amenazas cibernéticas. Por otra parte, se ha registrado un total de 73.184 ciberataques en todo el 2020, lo cual indica que fue un aumento del 70% en relación al año anterior.

Asimismo, el [3] en su boletín de seguridad realizado en el año 2021, percibió un promedio de 380.000 archivos maliciosos diarios, lo que infiere un incremento del 6,2% en semejanza con el año 2019. Según el boletín, el 99% de las empresas internacionales admiten haber sufrido un ciberataque durante el 2020. Teniendo como déficit y limitación el recopilar y compartir información de las amenazas para poder predecir estos ciberataques.

Continuando en la actualidad, el [4] en su reporte realizado, constató un incremento del 27% de los ciberataques a sitios web del estado derivados de los EE.UU. y otros países registrado en el 2019 y un 58% registrados en 2020, asimismo, se detalló que los delitos cibernéticos contra las empresas se incrementó a un 38%, 20 puntos porcentuales sobre los casos registrados en el año anterior.

Como seguimiento de esta actividad, la empresa de seguridad [5] en un estudio realizado en Latinoamérica, anunció que se registraron más de 45 billones de ciberataques en el periodo del 2020. En efecto, considerando solo los tres últimos meses del año 2020, hubo 21 billones de ciberataques en el territorio. Los ciberataques se basan dependiendo del fin que se desee lograr o el perjuicio que se quiere provocar, y estos pueden mostrarse de distintos métodos. Asimismo, se informó que los ciberdelincuentes para lograr sus objetivos utilizan una secuencia de métodos, las cuales se aplican de forma individual o combinada. Entre los métodos más habituales tenemos los virus, el envío abundante de correos no deseados o phishing, la suplantación de identidad, la instalación de keyloggers, la utilización de ransomware o troyanos para el control total de los sistemas o el robo de la información, la utilización de rootkits y la utilización de archivos bots.

Con el objetivo de prevenir y mejorar la respuesta ante los ciberataques descritos anteriormente, aparecen en escena las actividades de intercambio de información de malware por organismos internacionales, nacionales y locales de ciberseguridad.

En el contexto nacional, en cuanto a [6] en su informe del laboratorio de inteligencia de amenazas en América Latina, que reúne y examina eventos de ciberseguridad a nivel mundial, anunció que el Perú fue el tercer país de la región con más intentos de ciberataques en el Latinoamérica. El Perú fue objetivo de 615 millones de intentos de ciberataques entre el período del 2021. Mientras que en Latinoamérica los ciberataques ascendieron a los 16 mil millones de intentos. A su vez, informó que muchas son las instituciones y organizaciones que no cuentan con un sistema de intercambio de información de amenazas cibernéticas el cual permita anticiparse a estos.

Asimismo, en el ámbito nacional, el [7] perteneciente a la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, es la entidad encargada de “dirigir los esfuerzos para determinar, adelantar y enfrentar los desafíos del ciberespacio y establecer la defensa ante los ciberataques, con el fin de abastecer al país una posición segura en el ámbito de la ciberseguridad”; actualmente el Centro Nacional de Seguridad Digital tiene implementado la Plataforma MISP (Malware Information Sharing Platform), siendo esta, una plataforma de conocimiento sobre ciberataques con el objetivo de recopilar, almacenar y distribuir información referente a ciberataques dirigidos, inteligencia, información de fraude financiero informático, noticias de vulnerabilidades, inclusive información antiterrorista, con la finalidad de usar la información para la predicción de ciberataques a favor de las infraestructuras, instituciones y usuarios.

Por otro lado, el [7] en sus boletines de alerta integrada de seguridad digital, anunció que las incidencias de correos electrónicos con información mentirosa para engañar a las personas o instituciones se incrementó en un 25% mediante campañas de phishing o de ingeniería social sobre temas de coronavirus, bonificaciones, propagandas bancarias y de entretenimiento, siendo estos informados en su plataforma MISP para que otras instituciones puedan mejorar sus niveles de seguridad.

En cuanto al contexto local, el Departamento de Ciberseguridad fue creado con Resolución Directoral N.º 027-2018-DIRGEN/SUB.DG-PNP de fecha 29 enero del 2018, y actualmente depende de la División de Informática de la Dirección de Tecnología de la Información y Comunicaciones de la

Policía Nacional del Perú (DIRTIC PNP), tiene como misión “Coordinar la respuesta ante amenazas y/o ataques informáticos y prevenir el acceso no autorizado de la información, asegurando los pilares de la seguridad de la información”, en los sistemas de información perteneciente a la PNP. El Departamento de Ciberseguridad se enfrenta a más de 100 incidentes de todo tipo y naturaleza aproximadamente, sin embargo, cada día aparecen nuevas amenazas cibernéticas a proporción del 5% de las frecuentes, siendo los más vulnerables a nivel local los sistemas que almacenan información referente a investigaciones policiales, denuncias o requisitorias y antecedentes como son los Sistemas de Denuncias Policiales, Sistema de Requisitorias y Antecedentes Policiales y el Sistema de Investigación Criminal. Por lo tanto, luchar contra estos ciberataques individualmente es casi imposible.

Enfocando a la problemática, el Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP, no contaba con una plataforma de intercambio de información de malware que permita recopilar, almacenar y distribuir información sobre los ciberataques suscitados a nivel nacional y/o mundial, y que ayude a mejorar las capacidades de monitoreo, las capacidades defensivas y las acciones preventivas del Departamento. Para la investigación se tuvo que implementar la plataforma de intercambio de información de malware el cual pudo mejorar los procesos antes mencionados.

En consecuencia, ante el incremento y la complejidad de los ciberataques a nivel nacional y mundial, se requirió para nuestra investigación un alto nivel de intercambio de información entre las organizaciones vinculadas con la ciberseguridad en especial con la gestión y control de ciberataques. La identificación, evaluación y la gestión de ciberataques que se realizó en el Departamento de Ciberseguridad, logró el intercambio información de forma eficiente y eficaz mediante la plataforma, aumentando las capacidades defensivas y acciones preventivas para prevenir ciberataques; asimismo, se pudo mejorar las capacidades de monitoreo para evitar que se repitan de forma general y contribuir así a mejorar con eficiencia y eficacia, al ahorro de tiempo y esfuerzo para predecir los ciberataques.



Fig. 1. Ubicación geográfica del Departamento de Ciberseguridad de la División de Informática DIRTIC PNP.

En la Fig. 1 se evidencia la ubicación geográfica del Departamento de Ciberseguridad de la División de Informática DIRTIC PNP donde se realizó la investigación.

1.2 Delimitación del problema

1.2.1 Espacial

Este proyecto propuesto se encuentra dentro del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP, donde se trabajó con registros y personal que labora en el departamento, siendo los especialistas en ciberseguridad, enfocados a detectar y a defender de los ciberataques ocurridos diariamente, para lograr la gestión e intercambio de información sobre las amenazas.

1.2.2 Temporal

La actual investigación se efectuó desde marzo a diciembre del 2021 en el Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP.

1.3 Formulación del problema

1.3.1 Problema General

¿De qué manera la Implementación de la plataforma de intercambio de información de malware mejora la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP?

1.3.2 Problemas Específicos

- ¿Cómo la implementación de la plataforma de intercambio de información de malware mejora las capacidades de monitoreo para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP?
- ¿En qué medida la implementación de la plataforma de intercambio de información de malware mejora las capacidades defensivas para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP?
- ¿En qué medida la implementación de la plataforma de intercambio de información de malware mejora las acciones preventivas para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP?

1.4 Justificación

1.4.1 Práctica

En la investigación se planteó la implementación de la plataforma de intercambio de información de malware en el Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP, para mejorar la predicción de ciberataques, estos que ocurren diariamente a escala internacional, nacional y local; asimismo, esta investigación

benefició a todo el personal policial que labora en el Departamento mencionado.

1.4.2 Teórica

En la investigación se aplicó las teorías establecidas por el [8] y el [9], obteniéndose nuevos conocimientos, de los cuales, en las pruebas de hipótesis se pudo demostrar que las funciones que realiza esta plataforma son muy eficientes para la predicción de ciberataques, los cuales pueden generalizarse a otros casos similares.

1.4.3 Metodológica

Para tal efecto, se justificó de manera metodológica, porque la manera como se abordó esta investigación ayudó como referencia para los profesionales de la ciberseguridad que buscan generar nuevas ideas y conocimientos sobre los ciberataques suscitados diariamente, teniendo como propósito agregar nuevos instrumentos de aprendizaje para otras futuras investigaciones, logrando aportar ideas en base a los indicadores planteados para alcanzar a su vez, la satisfacción de los usuarios y la veracidad de la información. Asimismo, para la elaboración de la investigación se basó en el Cybersecurity Framework v1.1 del Instituto Nacional de Estándares y Tecnología (NIST). Por su parte [10] en su [11] define que es una metodología con un sentido para disminuir el riesgo asociado a las amenazas cibernéticas que puedan complicar la ciberseguridad.

1.5 Objetivos

1.5.1 Objetivo General

Determinar de qué manera la implementación de la plataforma de intercambio de información de malware mejora la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP.

1.5.2 Objetivos Específicos

- Definir en qué medida la implementación de la plataforma de intercambio de información de malware mejora las capacidades de monitoreo para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP.
- Describir en qué medida la implementación de la plataforma de intercambio de información de malware mejora las capacidades defensivas para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP.
- Describir en qué medida la implementación de la plataforma de intercambio de información de malware mejora las acciones preventivas para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes

Para la presente investigación, se revisó algunos artículos y tesis internacionales y nacionales relacionadas a los indicadores de estudio, que nos permitió realizar semejanzas para solucionar el problema que se estuvo investigando.

2.1.1 Antecedentes Internacionales

En contexto internacional tomando como referencia a [12] en su artículo de investigación, analizaron la pandemia de COVID-19 desde el enfoque del ciberdelito y destacaron la variedad de ciberataques experimentados a nivel mundial durante la pandemia. Los ciberataques se analizaron dentro del contexto de eventos globales clave para revelar el modus-operandi de las campañas de ciberataques. El análisis muestra cómo después de lo que parecían ser grandes brechas entre el brote inicial de la pandemia en China y el primer ciberataque relacionado con COVID-19, los ciberataques se volvieron mucho más frecuentes. El análisis procede a utilizar el Reino Unido como un estudio de caso para demostrar cómo los ciberdelincuentes aprovecharon los eventos destacados y los anuncios gubernamentales para diseñar y ejecutar cuidadosamente campañas de ciberdelincuencia.

En cuanto al informe de [13] se planteó como objetivo principal ganar medidas de prevención en ciberseguridad sin que exista un ámbito normativo, y favorecer una variedad de sociedades por medio de un modelo de contribución entendida y triunfante, que posibilite conformar una civilización organizacional de ciberseguridad en nuestro ámbito nacional. Para su informe utilizó el método cuantitativo porque señala que la índole específica del MISP es su esquema horizontal, conociéndose como plataforma de igual a igual, en el que cada parte usuario del MISP puede dar y recibir información, teniendo como resultado difundir entre las organizaciones la implementación y configuración de la plataforma de intercambio de información de malware

(MISP). Asimismo, se llegó a la conclusión que la importancia de aprobar el MISP en una institución permite mejorar las capacidades de ciberseguridad y análisis de datos, en especial mediante términos de recopilación, respaldo, procesamiento y visibilidad de la información.

Por otra parte, en la publicación de [14] se presentó un marco de evaluación para analizar y comparar las plataformas de intercambio de inteligencia sobre amenazas (Threats Intelligence Sharing Platforms - TISP) actuales, que es de interés latente para la investigación como para la práctica. Para esto, propuso como objetivo de esta investigación presentar un marco para analizar y comparar las TISP y demostrar su aplicabilidad. Para la investigación se utilizó el método cuantitativo porque se desarrolló un protocolo de revisión sistemática de literatura. El presente aporte que tiene el artículo es que, en el futuro se centrará en una evaluación integral de todos los TISP disponibles, junto con el establecimiento de una ponderación de criterios y funciones dentro del marco.

Del mismo modo, en el artículo de investigación de [15] se utilizó el método cuantitativo porque para obtener las consecuencias de predicción deduce constituir una secuencia de fases que admitan la configuración de los distintos instrumentos técnicos, así como la indagación de los resultados. Asimismo, tiene como objetivo predecir posibles acontecimientos de ciberseguridad que les permita a las instituciones tramitar de forma más dinámica los peligros que existe en su sistema. Como conclusión del estudio, se puede observar que a partir de los ingresos es probable conocer la verosimilitud de que un ciberataque sea victorioso con base en los acontecimientos trascendentales y las fórmulas empleadas del filtro. El aporte que tiene este trabajo de investigación se basa en que se puedan deducir acciones y se puedan formar diferentes estrategias para ayudar a disminuir el riesgo cibernético.

Avanzando en el tema, en la investigación de [16], se tuvo como objetivo analizar cómo las TICs han participado en un rol principal en la administración del consciencia intelectual que, a partir de las atribuciones

logradas, posibilita a las instituciones, por medio de la auditoría forense defenderse debidamente para responder ante ciberataques de cualquier nivel que involucre directamente o indirectamente a los factores internos de las organizaciones y por ende que altere los procesos o competitividad de un mundo globalizado. El marco metodológico utilizado es de tipo exploratorio, descriptivo y documental sobre los tópicos recopilados en ciberseguridad organizacional. El resultado y conclusión de esta investigación muestra que la ciberseguridad incorporado a la auditoría forense como medida para la prevención y detección de crímenes informáticos apoyan mediante evidencias para los procesos judiciales y los recursos de tecnología e información para poseer y tomar mejores decisiones en relación a los niveles estratégicos, sistemáticos y operativos de las instituciones.

Aparte de ello, en la tesis de [17] indicó que el aporte del presente trabajo es mantener un registro del estado del entorno a lo largo del tiempo y detectar amenazas lo antes posible. Además, la tesis tiene como objetivo conseguir un entorno estable, que una vez desplegado y bien configurado sea capaz de automatizar el ciclo de tratamiento de las muestras, incluyendo desde su extracción del tráfico de red hasta su paso por los diferentes tipos de analizadores. Los métodos utilizados en el trabajo se componen de cinco fases como investigación, diseño, implementación, experimentación y documentación. Como conclusión del presente trabajo se tiene que este proyecto podría utilizarse en auditorías de seguridad, también serviría para determinar de forma puntual si existe algún tipo de malware circulando por el entorno auditado.

En cuanto al artículo de [18] se revisó enfoques sobre el intercambio de información sobre ciberseguridad e identificó que las técnicas que intentan equilibrar de manera óptima entre la inversión cibernética, el riesgo cibernético, la privacidad y el intercambio de inteligencia de amenazas cibernéticas están ganando más atención. En contraste con el enfoque anterior, la investigación se basa en gran medida en la inspección directa de inteligencia de amenazas cibernéticas real obtenido de varias fuentes, con el uso de herramientas de código abierto cuando sea necesario.

Según [19] en su artículo de investigación, objetan que las chicas y medianas empresas (PYME) son los motores de las economías nacionales. Las estructuras flexibles de las pymes, su rápida adaptación al cambio; facilita a las economías de los países superar rápidamente las crisis. Factores como la competencia, el cambio y la globalización obligan a las PYME a utilizar las tecnologías de la información y la comunicación. Gracias a estas tecnologías, el concepto de tiempo y espacio ha desaparecido y se ha hecho posible llegar a servicios y productos financieros electrónicos desde cualquier parte del mundo gracias a una herramienta y red móvil. Paralelamente a todos estos desarrollos, especialmente en los últimos años, los incidentes de fraude con contribuciones de ingeniería social y los abusos de los trabajadores han puesto la seguridad de la información en un primer plano. Las PYMES, que no emplean mano de obra calificada en tecnologías de la información y tienen el prejuicio de que el riesgo de seguridad de la información solo afecta a las grandes empresas, se convierten en blancos fáciles para los ciberdelincuentes. Los riesgos derivados de la carencia de seguridad de la información, también conlleva otros riesgos como el riesgo reputacional y el riesgo legal. El objetivo de este estudio; Se trata de revelar una metodología simple y sencilla que las PYME con medios limitados pueden utilizar contra los peligros de seguridad de la información.

De acuerdo al artículo de investigación de [20] mencionaron que el sistema de información se ha popularizado y se utiliza para ayudar a la eficacia y eficiencia del funcionamiento de una empresa. El sistema “traiga su propio dispositivo” (BYOD) es una tendencia creciente en el entorno corporativo, donde los empleados pueden acceder al sistema desde cualquier lugar. El sistema BYOD es el desarrollo de información del sistema mediante el uso de alguna tecnología como una red privada virtual (VPN) o el uso de alguna aplicación para que el cliente en la oficina de la red externa pueda acceder a las redes internas con un sistema remoto. El sistema remoto tiene la fuerza para ayudar a los empleados que trabajan en cualquier lugar y en cualquier momento, lo que podría generar algún problema para la seguridad. El problema de seguridad que puede ocurrir es el acceso no autorizado y la

pérdida de información importante de la empresa. Las organizaciones que empezaron a utilizar el sistema BYOD, quieren mejorar la seguridad del sistema utilizando el análisis de riesgo, con el objetivo de proteger los datos internos. El uso del análisis de riesgos del Cybersecurity Framework NIST ayudará a las organizaciones a comprender el riesgo del sistema BYOD. Los resultados de los análisis obtenidos por el uso del análisis de riesgos en el sistema BYOD se encuentran en la necesidad de desarrollar alguna mejora en términos del sistema de seguridad recomendado.

Asimismo, en el artículo de investigación de [21], se tuvo como objetivo general crear un método que faculte la recopilación, almacenamiento y distribución de información precisa con la finalidad de proceder de forma acelerada y eficiente contra los ciberataques. El aporte de la investigación es revertir un mejor enfoque del malware, sus técnicas de ataque y brindar las tareas de previsión y contestación ante incidentes vinculados con la actividad. El método a utilizar es el cuantitativo porque se basa en la inteligencia generada por empresas que sufrieron ciberataques. La conclusión de la investigación radica en crear una relación de confianza, vencer el temor a brindar visibilidad a la información conseguida y lograr una aprobación para dar forma a la información.

Posteriormente, en la tesis de [22] se tiene como objetivo el análisis de la ciberseguridad y su influencia en las políticas de seguridad de la información de la Armada del Ecuador. La investigación siguió la metodología de la revisión documental y se dividió en tres etapas (búsqueda, selección y estudio de la información). El resultado favorece las aproximaciones a los antecedentes de la ciberseguridad para la conformación de políticas efectivas de seguridad de la información.

Finalmente, en la investigación científica de [23] presenta la plataforma de intercambio de información de malware (MISP) y el proyecto de intercambio de amenazas, una plataforma confiable, que permite recopilar y compartir importantes indicadores de compromiso (IoC) de ataques dirigidos, pero también información sobre amenazas como vulnerabilidades

o indicadores financieros utilizados en casos de fraude. El objetivo de MISP es ayudar a establecer acciones preventivas y contramedidas utilizadas contra ataques dirigidos. Habilite la detección a través de colaborativo-intercambio de conocimientos sobre el malware existente y otras amenazas. La metodología se basa en la inteligencia de amenazas cibernéticas real obtenido de un gran número de fuentes que normalmente están siendo utilizadas por los sistemas y productos de seguridad actuales. La conclusión de esta investigación está en la interfaz web del MISP y el uso de la plataforma para presentar información estadística sobre las amenazas recopiladas.

2.1.2 Antecedentes Nacionales

En el contexto nacional, dentro de ese marco, en la tesis de [24] tiene como finalidad principal usar un patrón dinámico para optimizar el área de gerencia a la infraestructura de las TIC. Utilizando un método cuantitativo porque consiste en poder tomar decisiones con prospectiva para resguardar recursos o activos de información, obteniendo valor adicional optando por las estrategias de prevención. El aporte de la tesis es de permitir tomar decisiones para la defensa y resguardar la infraestructura de TIC en las instituciones, para esto se necesitan factores que puedan ser modificados y ajustados en relación a numerosos entornos. Como conclusión se llegó a demostrar que el uso del patrón apoya en la toma de decisiones con respecto a los usuarios encargados de seguridad, obteniendo una reducción en la cantidad de alertas que se registran en las áreas.

Según [25] en su artículo de investigación señala que tiene como objetivo plantear el uso de la metodología basada en el Marco NIST para la gestión adecuada de la ciberseguridad en las organizaciones gubernamentales en el marco de la entrega de servicios digitales. Muchas organizaciones gubernamentales han estado gestionando la ciberseguridad sin un proceso definido; esto genera que la gestión sea deficiente y sin indicadores. En cuanto a que, si están implementando la metodología basada en el marco de ciberseguridad de NIST, manifiesta que el 36,8% de los encuestados tienen un nivel de desacuerdo, 31,6% un nivel de indecisión,

15,8% un nivel de acuerdo, 10,5% un nivel totalmente en desacuerdo y 5.3% un nivel totalmente de acuerdo. En tanto, la variable gestión de la ciberseguridad señala que el 36,8% de los Ministerios encuestados presentan un nivel de desacuerdo; 36,8% un nivel indeciso, 15,8% un nivel de acuerdo y 10,5% un nivel totalmente en desacuerdo, en conclusión, se ha demostrado que el uso de la metodología basada en el marco de ciberseguridad de NIST influye en la gestión de la ciberseguridad en las organizaciones gubernamentales y está claro que actualmente no la están utilizando lo que provoca un nivel de liderazgo relativamente bajo en la implementación de medidas de seguridad relativas a la gestión de la ciberseguridad.

No obstante, en el artículo de investigación de [26] tuvo como objetivo el sugerir estrategias incorporadas de ciberseguridad obligatorias para reforzar la seguridad nacional digital del Perú. La investigación tuvo como metodología de tipo descriptiva y el diseño no experimental. Tuvo como conclusión que la ciberseguridad establece un deber social que demanda estructuración entre el sector público y el sector privado, lo que en el Perú aún no se definió.

De la misma forma, en su artículo de [27] tiene como finalidad el análisis de un sistema relacionado a la Seguridad de la Información Nacional en respuesta a los numerosos ataques cibernéticos que amenaza la información del gobierno. En consideración a la metodología empleada, se puede mencionar que es de tipo descriptiva, presenta un diseño no experimental. Y teniendo como resultado de la misma se puede apreciar que es vital desarrollar un refuerzo en la educación, la capacitación y el camino de los profesionales especialistas en ciberseguridad, como también implantar un efecto de conciencia sobre la ciberseguridad para todas las fases de formación institucional y profesional del individuo.

Siguiendo este razonamiento, la tesis de [28] tiene la metodología cuantitativa porque se basa en un ambiente de trabajo identificado y que se actualiza continuamente con la ayuda de la sociedad. Asimismo, el objetivo general es fomentar una guía de análisis de logs que posibilite determinar los

ciberataques utilizando instrumentos de Data Analytics. El resultado de la tesis facilita a las organizaciones un instrumento a su alcance para trabajar frente a los ciberataques, los cuales van de aumento conforme las tecnologías de información evolucionan. La conclusión de la tesis se enfoca en las soluciones obtenidas, que al emplear el patrón son muy accesibles y simple para ser aplicado por el equipo especialista en seguridad informática de las instituciones.

Tal es el caso de la tesis de [29], la metodología utilizada es cuantitativo porque se ejecutó la equiparación de instrumentos de ciberseguridad que fueron capaces de hacer frente a los ciberataques, con la intención de capturar información de los forasteros y mejorar las acciones preventivas en los servidores y base de datos. La finalidad principal es realizar un análisis de los instrumentos de ciberseguridad que afronten los ciberataques encontrados en servidores web y base de datos. El resultado de la tesis es identificar los incidentes de ciberseguridad, localizando entre ellos a los ciberataques con mayor impacto en servidores y base de datos. Finalmente, como conclusión de la tesis se logró examinar y estudiar la impresión que provocaron los ciberataques.

Por otro lado, al revisar la tesis de [30] la inicialización de esta tesis, accedió cooperar a que las empresas tomen consideración sobre la importancia que se debe otorgar a la protección de su información, ya que, si la información es robada o utilizado por personas extrañas a la empresa conllevaría a consecuencias desfavorables para la empresa misma, a tal punto de quebrantar. Asimismo, tiene como objetivo establecer la administración de la seguridad informática para prevenir la fuga de información en las PYMES. La metodología utilizada es la Cuantitativa porque con esta tesis ayudaran a promover una sociedad de prevención y detección de ciberataques en las PYMES. Por otra parte, el resultado de la tesis es informar relación con el riesgo que simboliza no estar listos para los numerosos ciberataques presentes en la actualidad y se ofrecerá información de qué manera elaborar los planes y estrategias operativas relacionadas en reducir los ciberataques.

Como complemento, en la tesis de [31] tiene como aporte contribuir a tomar decisiones frente a los ciberataques suscitados, mediante la aplicación de mapas auto organizados a la información brindada por los logs conseguidos. Como objetivo de la tesis es desarrollar un software basado en mapas auto organizados que esté presente de manera visual la identificación de ciberataques. La conclusión que brinda es obtener una retribución de valores más eficiente a los valores de los parámetros. El método utilizado es cuantitativo porque se aplica sobre la base de un proyecto implementado en una institución y que corresponde al inicio de una solución de protección contra ciberataques.

2.2 Marco Conceptual

2.2.1 Definición de las Variables y sus dimensiones

Para la investigación se requirió tener un conocimiento eficaz de las variables de estudio; asimismo, la **variable independiente** viene a ser la **Implementación de la plataforma de intercambio de información de malware**, según [8], sostiene que la plataforma de intercambio de información de malware (MISP) es una plataforma de conocimiento contra ciberataques especialmente empleada para brindar, resguardar e interactuar con indicadores de compromiso en ciberataques, con la finalidad de tener una sociedad colaborativa sobre los ciberataques existentes, cuyo objetivo es ayudar a mejorar las medidas preventivas y de detección en las instituciones u organizaciones públicas o privadas.

De la misma manera, el [8] define que la plataforma MISP, permite a las instituciones u organizaciones intercambiar información sobre cualquier tipo de ciberataques. En consecuencia, los usuarios de MISP se favorecen del conocimiento cooperativo sobre los ciberataques suscitados a nivel mundial.

Por último, el [8] menciona que la plataforma MISP, está desarrollada como software libre (código abierto) por un grupo de desarrolladores de CIRCL y muchos otros colaboradores.

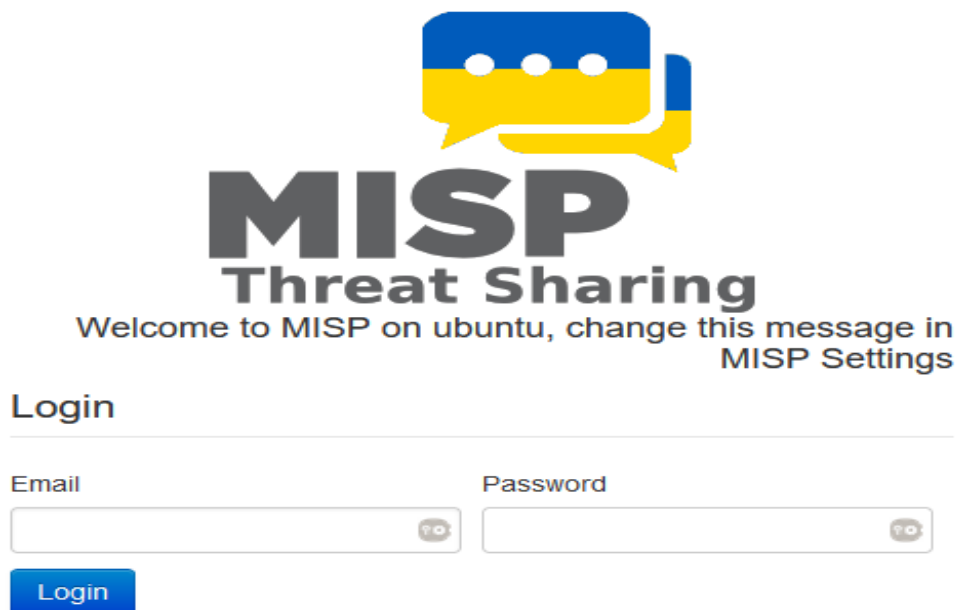


Fig. 2. Portal del Malware Information Sharing Platform (MISP).

En la Fig. 2 se muestra el portal de inicio de la Plataforma de Intercambio de Información de Malware desarrollada por el CIRCL de Luxemburgo.

Dentro de ese marco, la plataforma MISP tiene como objetivos:

- Ayudar a mejorar las contramedidas utilizadas contra ciberataques dirigidos y establecer acciones preventivas y de detección en las instituciones y organizaciones.
- Facilitar el almacenamiento de información técnica y no técnica sobre ciberataques.
- Compartir información sobre ciberataques con otras organizaciones y grupos de confianza. Generar una plataforma de confianza con información confiable de socios confiables.
- Almacenar toda la información en un formato estructurado de otras instancias sobre ciberataques.

Así como también tiene las siguientes características:

- MISP es una herramienta con características de eficiencia, precisión y escalabilidad.
- La información que se distribuye en MISP se conoce como evento, en el cual tiene una variedad de atributos, y estos se reconocen por tipo, valor, categoría y otras variables de texto por ejemplo fecha, grado de

amenaza, especificaciones de la institución e información sobre los participantes de las amenazas .

- Permite la conexión con otras aplicaciones de intrusión de detección de sistemas como SIEM o IDS que contienen API REST adaptativos para poder incorporar soluciones internas con dicho sistema.

Dentro de la plataforma existen perfiles de los usuarios que interactúan y que comparten información, algunos ejemplos pueden ser:

- Analistas de malware dispuestos a compartir indicadores.
- Analistas de seguridad buscando, validando y utilizando indicadores en operaciones.
- Analistas de inteligencia reuniendo información sobre adversarios específicos.
- Equipos de estudios de riesgos dispuestos a conocer las nuevas amenazas, probabilidad y ocurrencias.
- Analistas de fraude dispuestos a compartir indicadores financieros para detectar fraudes financieros.

¿Qué organizaciones interactúan en la plataforma MISP?

Las comunidades son grupos de usuarios que comparten dentro de un conjunto de objetivos y/o valores, y se tiene entre lo más comunes:

- CIRCL opera múltiples instancias MISP con más de 950 organizaciones y 2400 usuarios.
- Grupos de confianza que ejecutan comunidades MISP en modo aislado.
- Sector financiero utilizan MISP como un mecanismo de intercambio.
- Organizaciones militares e internacionales (OTAN, militares, CSIRTs, CERTs, etc.)
- Los proveedores de seguridad que ejecutan sus propias comunidades.
- Entidades del estado como Ministerios, Gobiernos regionales, Municipalidades.

Asimismo, al implementar el MISP, se tiene como beneficios:

- Conocer antes de ser golpeado por algo que otro sector ha enfrentado antes.

- Amenazas híbridas: cómo pueden ser cosas aparentemente no relacionadas.
- Información interesante para correlacionar.
- Preparar otras comunidades para la capacidad y cultura de compartir.

Modelos de conexión:

- Conectándose a una instancia MISP alojada por un CSIRT.
- Alojando su propia instancia y conectándose al MISP de CSIRT.
- Convertirse en miembro de una comunidad sectorial MISP que está conectada a la comunidad de CSIRT.

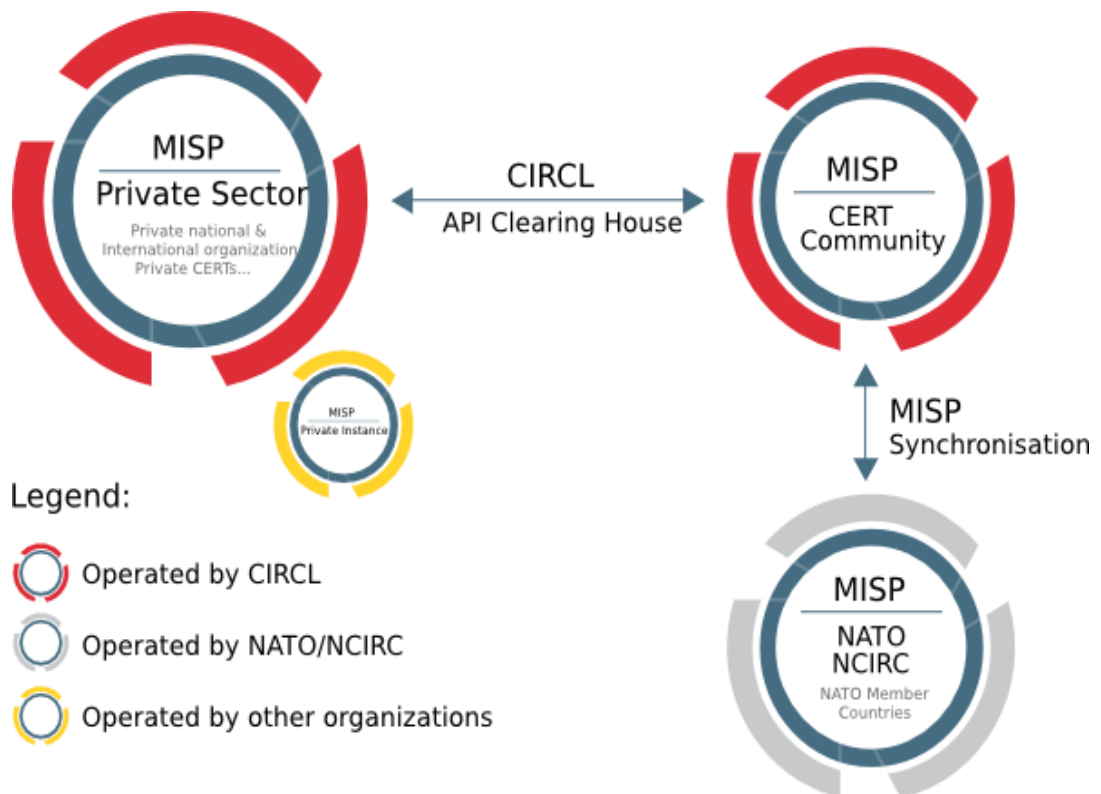


Fig. 3. Interacción de instancias MISP.

En la Fig. 3 se muestra la interacción de las instancias MISP administrados por el CIRCL de Luxemburgo.

Published	Creator org	ID	Clusters	Etiquetas	#Attr.	#Corr.	Date	Info	Distribution	Acciones
✓	PCM	107		C SIRT-Inst=="Explotación de vulnerabilidades conocidas" C SIRT-Inst=="Explotación de vulnerabilidades día cero"	1		2021-12-13	Vulnerabilidad crítica de biblioteca de Java Log4J	Community ↵	👁
✓	PCM	106		C SIRT-Inst=="Phishing"	3		2021-12-22	Nueva campaña de phishing que suplanta la identidad del Banco BBVA Continental	Community ↵	👁
✓	PCM	105		C SIRT-Inst=="Interrupción de servicios tecnológicos" Resuelto	3		2021-12-15	Incidente de Indisponibilidad de la nube AWS	Community ↵	👁
☐	✗	PNP-PERU	104	C SIRT-Inst=="Phishing" C SIRT-Inst=="Portal fraudulento" Resuelto	2		2021-11-22	Phishing a los correos institucionales de la PNP desde cuenta suplantada de Microsoft	Community ↵	📄 🗑 👁
☐	✓	PNP-PERU	102	C SIRT-Inst=="Divulgación no autorizada de información personal" C SIRT-Inst=="Fuga de Información" Resuelto	1		2021-09-25	Posible venta de credenciales de acceso a los sistemas policiales	Community ↵	📄 🗑 👁
✗	PCM	103		C SIRT-Inst=="Crypto Robbing Ransomware" En Proceso	1		2021-11-08	Infección de Ransomware ROGER v4.434, [MUNICALLAO]	Community ↵	No publicado 👁
✓	PCM	101		C SIRT-Inst=="Difamación Imagen Institucional a través de Internet" C SIRT-Inst=="Phishing" En Proceso	2		2021-09-15	Reporte de URL fraudulento respecto al subsidio YANAPAY	All ↵	👁
✓	PCM	100		C SIRT-Inst=="Explotación de vulnerabilidades conocidas" C SIRT-Inst=="Malware" En Proceso TLP:=="Verde"	4		2021-09-03	Atacantes utilizan la vulnerabilidad de ShowDoc para difundir malware	All ↵	👁
✓	PCM	99		C SIRT-Inst=="Backdoors" C SIRT-Inst=="Malware" C SIRT-Inst=="RootKit"	3		2021-08-31	Detección de Malware en el archivo APK de "SnapTime Cam 11" para Android.	All ↵	👁
✓	PCM	98		C SIRT-Inst=="Modificación de información" C SIRT-Inst=="Modificación del sitio web" C SIRT-Inst=="Phishing" TLP:=="Ambar"	2		2021-09-04	Detección de sitio web fraudulento del Banco Interbank	All ↵	👁
✓	PCM	97		C SIRT-Inst=="Phishing" Resuelto TLP:=="Ambar"	2		2021-09-04	Phishing, suplantando la identidad en Paypal	Community ↵	👁
✓	PCM	95		C SIRT-Inst=="Phishing" Resuelto	2		2021-08-22	Detección de una nueva campaña de Phishing a Microsoft Office 365	Community ↵	👁
✓	PCM	96		C SIRT-Inst=="Derechos de Autor" C SIRT-Inst=="Phishing"	3		2021-08-21	Phishing, suplantando la identidad del banco Interbank	Community ↵	👁
✓	PCM	94		C SIRT-Inst=="Phishing" C SIRT-Inst=="Portal fraudulento" Resuelto	1		2021-07-26	Intento de Fraude via SMS [Phishing BBVA]	Community ↵	👁
✓	PCM	93		C SIRT-Inst=="Phishing"	1		2021-07-14	Phishing clon de pagina del Banco [BBVA Peru]	Community ↵	👁

Fig. 4. Descripción general de las amenazas en MISP.

En la Fig. 4 se muestra la descripción general de todas las amenazas reportadas en la Plataforma MISP.

Por otro lado, se describió las dimensiones de la variable implementación de la plataforma de intercambio de información de malware, siendo la primera (a) **Control de ciberataques**, en el cual [32] lo representa como protocolos que permiten preparar a una institución para reducir las posibilidades de un ataque cibernético, reconociendo herramientas o aplicaciones y brindando sesiones de ayuda para la defensa en contra de estos. Al mismo tiempo se ha desfragmentado esta dimensión en el siguiente indicador: (a.1) **Ciberataques identificados**, del mismo modo [32] indica que este punto es realizado con la finalidad de lograr la identificación de vulnerabilidades y amenazas que atente contra la seguridad de un activo de información.

En ese sentido nuestro trabajo de investigación conceptualiza a la segunda dimensión (b) **Respuesta ante ciberataques**, en el cual [33] lo describe como proyecto efectivo en respuesta a los planes previos a un ciberataque, debido que las consecuencias del daño a la infraestructura informática pueden ocasionar grandes pérdidas económicas. Para ello se dividió en el siguiente indicador (b.1) **Alertas**, donde [21], menciona que estos tienen un volumen muy alto de información relacionada con eventos de seguridad asociados a la actividad que desarrolla y que puede complementar en colaboración con otros actores públicos o privados relacionados con la ciberseguridad.

Asimismo, damos paso con la tercera dimensión (c) **Intercambio de información**, en el cual [21], define como la recopilación, almacenamiento y distribución de la información imprescindible para proceder de forma rápida y eficaz contra los ciberataques. Lo anteriormente expuesto, se dividió en el siguiente indicador: (c.1) **Recopilación de información**, según [21], indica que el objetivo principal es proporcionar a las empresas una comprensión profunda sobre los ciberataques que presentan los mayores riesgos para su infraestructura y cómo proteger su información a largo y corto plazo.

Siguiendo con la descripción de variables, se alega la variable dependiente, **Predicción de ciberataques** a [15], quienes afirman que

predecir un ciberataque es obtener datos actuales y aplicar las distintas medidas de protección, con la finalidad de obtener un aproximado de lo que puede suceder.

Por otro parte, se describieron las dimensiones que se encuentran dentro de la variable mencionada anteriormente, (a) **Capacidades de monitoreo**, en la cual [34], denota como capacidades de monitoreo de seguridad que puedan detectar un ataque a través de la supervisión en varios niveles dentro de su institución. Igualmente, esta dimensión se ha fragmentado en el siguiente indicador (a.1) **Tiempo en realizar la recolección de información de amenazas**, según [34], lo define como un punto de vista sistematizado de agrupar y controlar información de distintas fuentes a fin de obtener una vista completa y precisa de un objetivo.

En tal sentido, continuaremos describiendo la siguiente dimensión (b) **Capacidades defensivas**, en la cual [34], expresa que son capacidades que nos permiten detectar un ciberataque a nuestros sistemas informáticos antes de que ocurra, o en el peor de los casos en el momento en el que ocurre. Asimismo, se ha dividido en el siguiente indicador: (b.1) **Número de intrusos detectados en el sistema de detección de intrusos**, según [15], infiere que dicho indicador permite el reconocimiento de posibles ataques informáticos, analizando el historial de uso de las redes, servicios y aplicaciones informáticas de acceso restringido o historial fraudulento.

Por consiguiente, se describió la siguiente dimensión (c) **Acciones preventivas**, en la cual [34] indica que tiene como objetivo prevenir y reducir el impacto de estos ciberataques implementando controles tecnológicos preventivos que refuercen la seguridad de la información en las instituciones. A esta dimensión, se ha catalogado el siguiente indicador: (c.1) **Tiempo en realizar la copia de seguridad**, en el cual [32] define que el factor clave para prevenir los ciberataques es fundamental que se realice copia a toda la información que se almacenan dentro de los sistemas.

2.2.2 Definición de la metodología implementada en la investigación

En lo que concierne a la aplicación de la metodología, el [11] consiste en un manual relacionado a normas, estándares o políticas para que las instituciones administren y disminuyan eficientemente el nivel de peligro en ciberseguridad. Promueve la interrelación en la administración del peligro en ciberseguridad en medio de las entidades interesados de la institución tanto interno y externo.

Consta de tres factores fundamentales:

- i. Núcleo.
- ii. Niveles de implementación.
- iii. Perfiles.

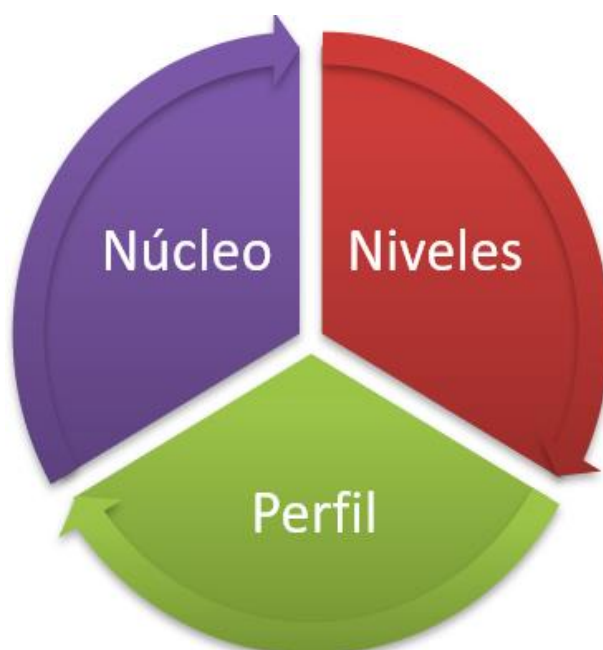


Fig. 5. Componentes principales del Marco de Ciberseguridad.

En la Fig. 5 se muestra los componentes principales del Marco de Ciberseguridad NIST en su versión 1.1.

- i. El núcleo del marco es la agrupación de procedimientos capaces de lograr objetivos específicos relacionados a la ciberseguridad y toma relación ejemplificando guías de cómo lograr dichos objetivos. Dicho Núcleo no es conjunto de enunciados pertenecientes a una lista de verificación de acciones por hacer. Esto representa a los objetivos importantes de la ciberseguridad reconocidas por aquellas partes

catalogadas como beneficioso para administrar los peligros en ciberseguridad. Este núcleo presenta cuatro elementos, los cuales son; funciones, categorías, subcategorías y referencias informativas.






	Funciones	Categorías	Subcategorías	Referencias informativas
	Identificar			
	Proteger			
	Detectar			
	Responder			
	Recuperar			

Fig. 6. Estructura del núcleo del Marco de Ciberseguridad NIST.

La Fig. 6 muestra la estructura del núcleo del marco, de los cuales consta de funciones, categorías, subcategorías y referencias informativas.

Los elementos del núcleo del marco trabajan de la siguiente manera:

- a. Las **Funciones**; Son aquellas que estructuran los procedimientos comunes de ciberseguridad en su rango máximo, estas funciones responden a la secuencia de: identificación, protección, detección, respuesta y recuperación, encargadas de expresar la gestión de riesgos

de una institución en relación a la información, adoptar decisiones y optimización de riesgos.

Las funciones se complementan con las metodologías ciertas para la administración de incidencias y apoyan a revelar la trascendencia de la financiación en seguridad de la información. Las funciones básicas del marco son:

- **Identificar (ID):** Desenvuelve un conocimiento estructurado de la organización que sirve para gestionar los peligros de la información, como también, activos personales o recursos inmateriales. Esto permite que una institución tenga concentración en sus estrategias preventivas de peligros o riesgos.
- **Proteger (PR):** Detalla las pautas de seguridad oportuna para asegurar la cesión de servicios de las infraestructuras críticas. Esto considera la intención de prohibir o reprimir la trascendencia de una potencial actividad en seguridad cibernética.
- **Detectar (DE):** Especifica los procedimientos necesarios para descubrir flujo de sucesos de un proceso de seguridad cibernética, otorgando el acierto inesperado de estos.
- **Responder (RS):** Comprende procedimientos necesarios para tomar respuesta ante sucesos de ciberataques, implementando la cualidad de reprimir la trascendencia de un potente activo.
- **Recuperar (RC):** Reconocimiento de procedimientos necesarios para resguardar la planificación de resiliencia y para laborar servicios que hayan sido deteriorados por un procedimiento de seguridad cibernética.

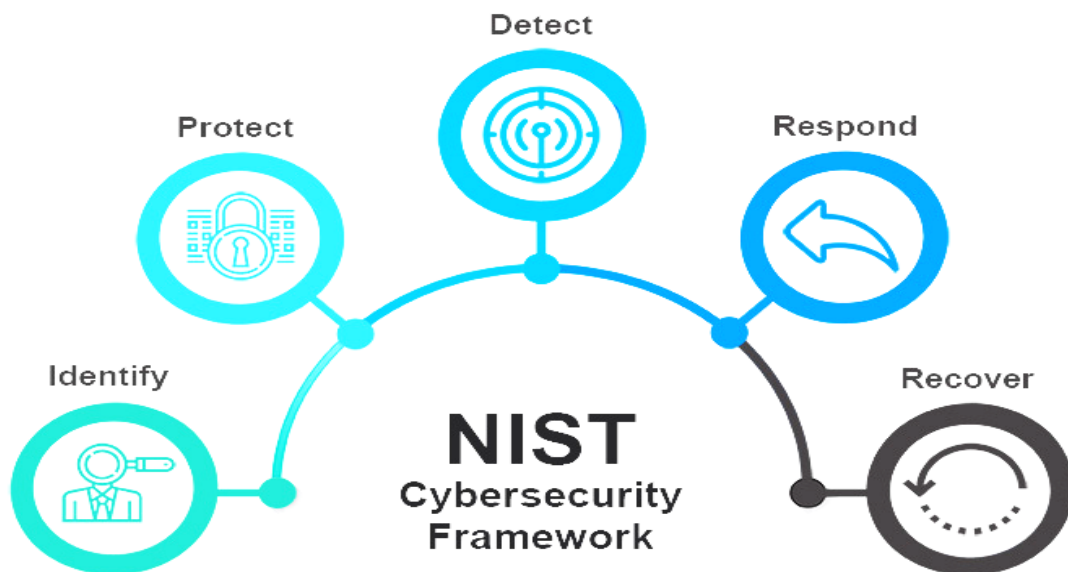


Fig. 7. Funciones del Marco NIST.

La Fig. 7 muestra las cinco funciones que cuenta el Marco de Ciberseguridad NIST los cuales son identificar, proteger, detectar, responder y recuperar.

- b. Las **Categorías** son la segmentación de una función, en agrupaciones de resultados de ciberseguridad vinculados a las necesidades programáticas y actividades propias.
- c. Las **Subcategorías** permiten la división de la categoría en los efectos característicos de procedimientos técnicos o de administración. Asimismo, brindan una agrupación de efectos que, si bien son complicados, cooperan en resguardar los objetivos de cada categoría. Algunos de estos ejemplos corresponden o involucran a los datos protegidos en descanso y las comunicaciones en relación a la detección de sistemas que se investigan.
- d. Las **Referencias Informativas** son características de reglas, pautas y métodos generales comprendidos en los entornos de infraestructura cruciales, los cuales ejemplifican un proceso para cumplir los efectos afiliados al núcleo del marco, siendo explicativo y no complicadas. Se enfocan en la guía entre entornos a lo que hace alusión con más regularidad durante las actividades del desarrollo de marco.

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO02.06, APO03.01 ISO/IEC 27001:2013 Clause 4.1 NIST SP 800-53 Rev. 4 PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	COBIT 5 APO10.01, BAI04.02, BAI09.02 ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	COBIT 5 DSS04.02 ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14

Fig. 8. Categorías, Subcategorías y Referencias informativas.

En la Fig. 8 se muestra el resumen referencial que contiene el Marco de Ciberseguridad NIST.

- ii. Los **Niveles de implementación del marco**: Especifica el nivel en que las prácticas de administración de riesgos de ciberseguridad de una institución muestran las características definidas. Los grados van desde Parcial (Nivel 1) a Adaptativo (Nivel 4) y detalla un nivel cada vez mayor de severidad, y qué tan bien constituidos están las decisiones de riesgo de ciberseguridad en decisiones de riesgo más amplias, y el grado en que la institución reparte y percibe información de ciberseguridad de fuentes externas.

Las definiciones de Nivel son las siguientes:

- a. **Nivel 1: Parcial**

- *Proceso de gestión de riesgos:* Las prácticas de gestión de riesgos no están concretas, en ocasiones se hace de manera reactiva.
- *Programa integrado de gestión de riesgos:* Hay poco conocimiento en la institución del riesgo de ciberseguridad, incluso, la gestión de este puede hacerse de manera irregular.
- *Participación Externa:* En general, la institución desconoce los riesgos de ciberseguridad de su cadena de suministro y no recibe ni comparte información con otras entidades para gestionar la ciberseguridad.

b. Nivel 2: Riesgo informado

- *Proceso de gestión de riesgos:* Aunque hay prácticas de gestión aceptadas por la dirección es posible que no se establezcan como políticas para toda la institución.
- *Programa integrado de gestión de riesgos:* Se tiene consciencia sobre el riesgo de ciberseguridad, sin embargo, no hay un enfoque definido para gestionarlo, es más, la información sobre esto se comparte informalmente.
- *Participación Externa:* La empresa es responsable de los riesgos de ciberseguridad, pero no actúa formalmente sobre estos.

c. Nivel 3: Repetible

- *Proceso de gestión de riesgos:* Las prácticas de gestión de riesgos de ciberseguridad están aceptadas y son políticas, además, se actualizan periódicamente.
- *Programa integrado de gestión de riesgos:* Toda la institución está enfocada en gestionar el riesgo de ciberseguridad, se tienen métodos para responder de forma oportuna y segura a los cambios que pueda tener y los encargados comunican regularmente sobre este.

- *Participación Externa*: La institución contribuye al entendimiento de los riesgos de ciberseguridad por parte de la comunidad, contribuye y recibe información de otras entidades. También comparte y actúa formalmente sobre los riesgos de ciberseguridad.

d. **Nivel 4: Adaptable**

- *Proceso de gestión de riesgos*: Adapta sus prácticas de ciberseguridad de acuerdo a sus actividades previas y lecciones aprendidas, además, es capaz de responder eficazmente a los recientes riesgos y amenazas.
- *Programa integrado de gestión de riesgos*: La institución está preparada para gestionar el riesgo de ciberseguridad y abordar posibles eventos de este tipo. Este riesgo es considerado igual de importante que otros riesgos a los que está expuesta.
- *Participación Externa*: Comparte información con otras entidades, además, actúa en tiempo real o casi real para entender y tomar acciones oportunas sobre los riesgos de ciberseguridad.



Fig. 9. Niveles de Implementación del Marco NIST.

La Fig. 9 muestra los niveles que se debe seguir en la implementación del Marco de Ciberseguridad NIST.

- iii. **Los Perfiles del marco:** Son la formación única de las condiciones y objetivos organizacionales de una institución, la comprensión al riesgo y los recursos con respecto a los resultados anhelados del núcleo. Los perfiles se pueden emplear para detallar oportunidades y renovar la postura de ciberseguridad relacionando un perfil “actual” con un perfil “objetivo”.
- El perfil actual faculta a las organizaciones realizar una comprobación objetiva de su programa de ciberseguridad en concordancia con el Marco de Ciberseguridad y conocer ciertamente cuál es su situación actual.
 - El perfil objetivo, comunicará la estrategia de liderazgo y la preferencia para el compromiso, capacitación, variación de políticas, cambios de procedimientos y adquisición de tecnología.
 - Para ello, se requiere la determinación de un programa de acción que incluya una priorización de labores dependiendo de las necesidades de negocio y procesos de administración de riesgos de la organización.

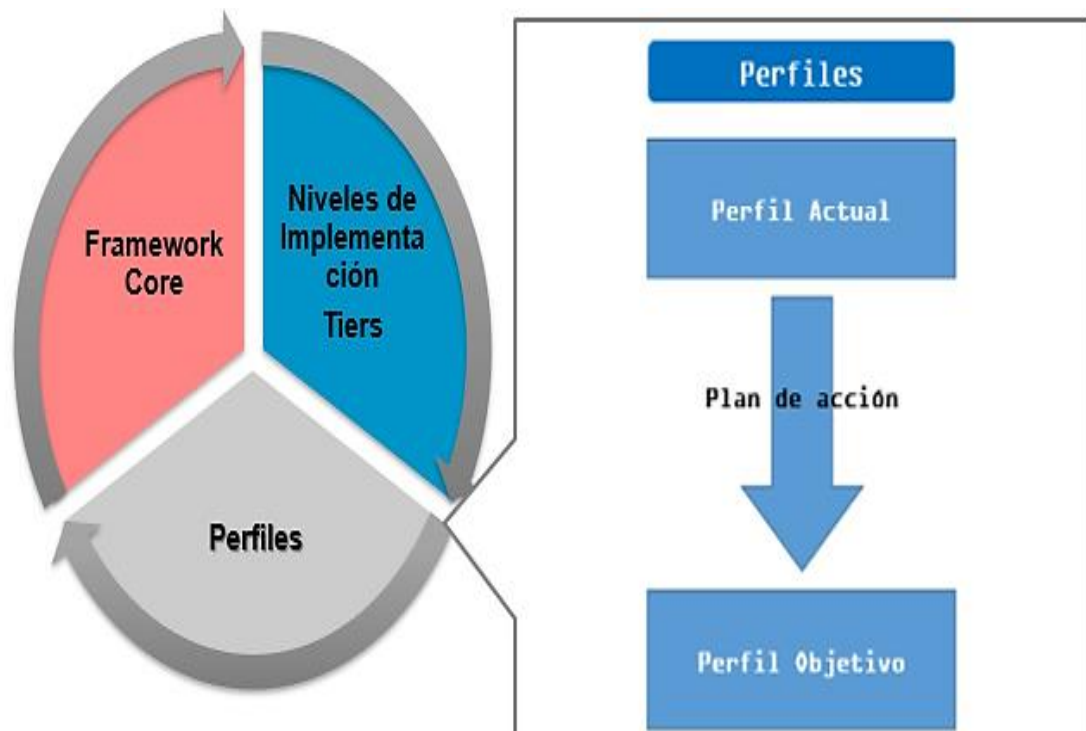


Fig. 10. Perfiles del Marco de Ciberseguridad NIST.

La Fig. 10 muestra los perfiles que se tiene considerado dentro del Marco de Ciberseguridad NIST.

De acuerdo a las especificaciones anteriormente mencionada, en la Fig. 11 se puede apreciar una arquitectura detallada del marco de trabajo de ciberseguridad de NIST.

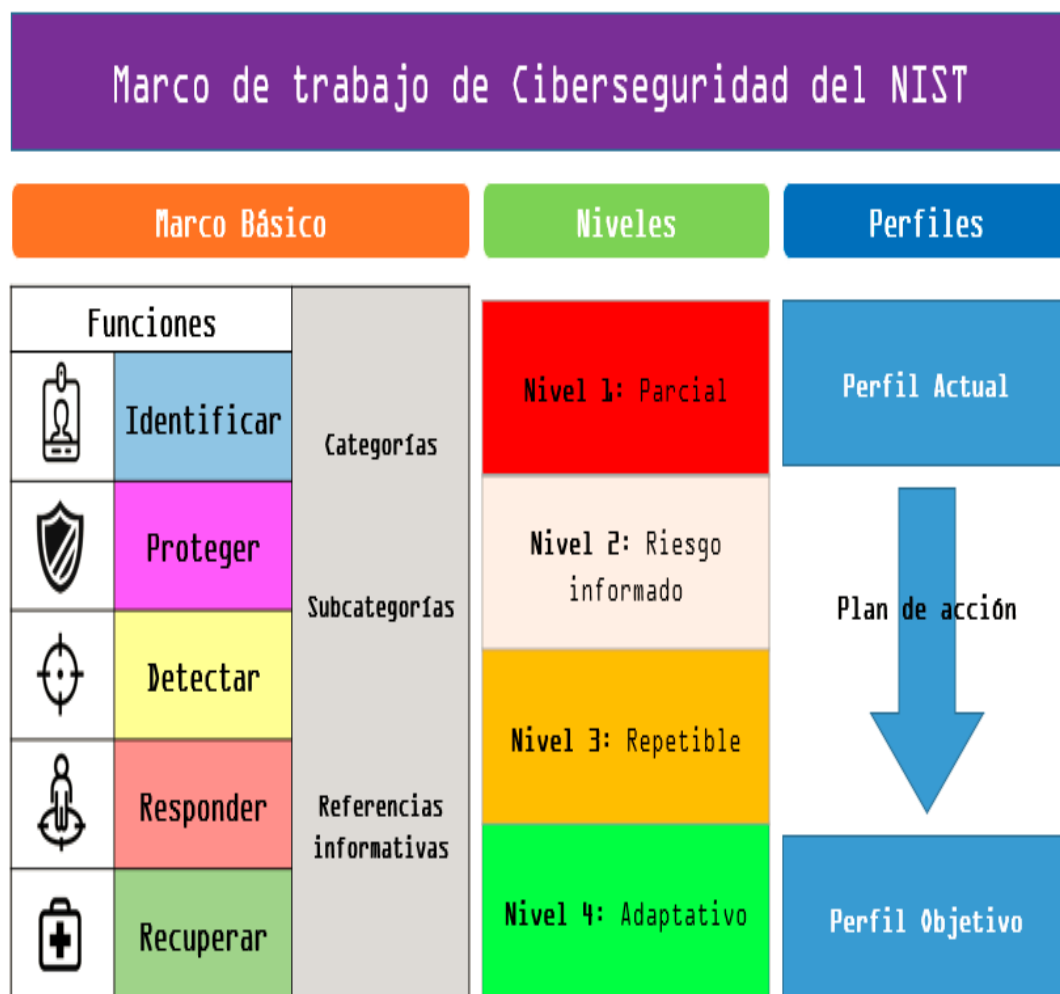


Fig. 11. Marco de trabajo de Ciberseguridad NIST.

2.3 Definición de términos

Activos informáticos: Son aquellos que tienen valor y están relacionados con el sistema informático.

Ciberseguridad: Son técnicas, procedimientos, métodos que se encargan de resguardar la información en los sistemas de información.

Ciberataque: Acción malintencionada que se realiza para afectar los principios de la información.

Ciberspacio: Ámbito artificial creado por la interacción de usuarios y medios informáticos de manera directa e indirecta.

Ciberamenaza: Circunstancias, individuos u organizaciones que pueden poner en riesgo la ciberseguridad.

Confidencialidad: La información no se divulga a usuarios que no tengan la debida autorización.

DDoS: (Denegación de servicio distribuida), es un ataque masivo tipo DoS, donde este ocurre en varias direcciones, es decir puede ser atacado por una institución de ciberdelincuentes.

Disponibilidad: Garantiza el acceso de los usuarios a los sistemas autorizados, cuando así se requiera.

DNS: (Domain Name Service), es una agrupación de estándares y servicios, donde los usuarios pueden reemplazar el uso de las direcciones IP para usar nombres de dominio.

Integridad: Garantiza que la información no se ha modificado o alterado de manera no autorizada.

MISP: Plataforma de intercambio de información de malware.

Malware: Todo programa o código malicioso que es dañino para los sistemas informáticos.

NIST: (National Institute of Standards and Technology), Instituto Nacional de Estándares y Tecnología.

Ransomware: Es un tipo de software malicioso que permite secuestrar el dispositivo de la víctima y poder apoderarse de su información o en algunos casos extorsionar a la víctima.

Trojanos: Son aquellos softwares que han sido modificados y que cumplen la función de cualquier otro programa normal, con la diferencia que este alberga en su interior un virus que vulnera tu seguridad mediante la instalación de actualizaciones y funciones innecesarias o spam.

Virus: Son categorizados por programas infectados que tienen la función de dañar archivos, ficheros y funcionalidades del equipo infectado.

Vulnerabilidad: Son aquellos fallos del sistema que actúa como puente entre los ciberdelincuentes y la información del sistema, esto puede ser aprovechado por técnicos propios de la institución o individuos externos denominados ciberdelincuentes.

CAPÍTULO III

HIPÓTESIS

3.1 Hipótesis General

La implementación de la plataforma de intercambio de información de malware mejora significativamente la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática DIRTIC PNP.

3.2 Hipótesis Específicas

- La implementación de la plataforma de intercambio de información de malware mejora significativamente las capacidades de monitoreo de la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP.
- La implementación de la plataforma de intercambio de información de malware mejora significativamente las capacidades defensivas de la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP.
- La implementación de la plataforma de intercambio de información de malware mejora significativamente las acciones preventivas de la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP.

3.3 Variables

3.3.1 Definición Conceptual de las variables

- **Variable Independiente (VI): Implementación de la plataforma de intercambio de información de malware.**

De acuerdo con [13] señala que es un sistema de libre acceso de conocimiento con la funcionalidad de brindar asistencia compartida, resguardar información e interrelacionar ataques cibernéticos, conocimiento de amenazas, fraudes financieros informáticos, vulnerabilidades e información antiterrorista. Tiene como finalidad, brindar ayuda en la implementación de

procedimientos para prevenir y defender respecto a ciberataques mediante el intercambio de información.

- **Variable Dependiente (VD): Predicción de ciberataques.**

Vinculado al concepto, [15] afirma que predecir un ciberataque es obtener datos actuales y aplicar las distintas medidas de protección, con la finalidad de obtener un aproximado de lo que puede suceder. Es muy potente entregar conocimientos, a la hora de tomar decisiones y es un aporte inmenso, ya que permite descubrir patrones que no están a la vista del ojo humano.

3.3.2 Definición Operacional de las variables

- **Variable Independiente (VI): Implementación de la plataforma de intercambio de información de malware.**

Plataforma para compartir información de malware es una herramienta que busca mejorar la predicción de ciberataques, manifestado a través del control de ciberataques, plan de respuesta ante ciberataques y el intercambio de información de ciberataques.

- **Variable Dependiente (VD): Predicción de ciberataques.**

La predicción de ciberataques busca mejorar el tiempo en realizar la recolección de información de amenazas de las capacidades de monitoreo, luego busca mejorar los números de intrusos detectados en el sistema de detección de intrusos de las capacidades defensivas y finalmente, busca mejorar el tiempo en realizar la copia de seguridad en las acciones preventivas.

CAPITULO IV

METODOLOGÍA

4.1 Método de Investigación

Según [35], el método hipotético deductivo, es el cúmulo de teorías e ideas básicas, elaborando en aspecto deductivo las consecuencias concretas de las hipótesis, y tratada de simular para unir la información pertinente. Por lo tanto, investiga la solución a los problemas planteados.

En el presente estudio se empleó el método de investigación hipotético deductivo, porque se consideró lo universal a lo particular, donde se utilizó una secuencia de herramientas e instrumentos que posibilita obtener los objetivos propuesto.

4.2 Tipo de Investigación

Según [36] la investigación aplicada toma el nombre de “investigación práctica”, que se califica porque busca la aplicación o utilización de los conocimientos obtenidos, a la vez que se consiguen otros, luego de implementar la práctica en investigación.

Por otro lado, [37] mencionan que el fuerte fundamental de la investigación cuantitativa está presente en la recopilación de datos numéricos. Asimismo, se centra en la función de medir la escala, frecuencia y el rango de un fenómeno, lo cual involucra estudiar los factores tangibles de la investigación.

Por lo tanto, se catalogó al tipo de investigación como aplicada con enfoque cuantitativo, ya que su finalidad es dar solución a un problema a través de la implementación de una herramienta tecnológica.

4.3 Nivel de Investigación

La investigación es de nivel explicativo, porque consiste en descubrir hechos mediante una correlación causa–efecto, con ello se decreta si favorece a las variables indirectamente y así alcanzar resultados que determinen la mejoría. Con este nivel de investigación se logró explicar y definir el nivel de correlación que existe entre la plataforma de intercambio de información de

malware y la predicción de ciberataques en el Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP.

4.4 Diseño de Investigación

Continuando, [38] sostiene que generalmente se llama diseño de investigación experimental a la manipulación intencional de la variable independiente de un modelo para estudiar y calcular las consecuencias en la variable dependiente, buscando determinar el impacto.

El presente estudio utilizó un diseño de investigación experimental con dos pruebas Pre-test (antes) y Post-test (después) de haber implementado la plataforma de intercambio de información de malware.

Dónde:

G : Es el grupo de usuarios que recibió la plataforma de intercambio de información de malware.

X : Experimento de la plataforma de intercambio de información de malware.

O₁ : Es el fruto de efectuar las pruebas sin la plataforma de intercambio de información de malware.

O₂ : Es el fruto de efectuar las pruebas con la plataforma de intercambio de información de malware.

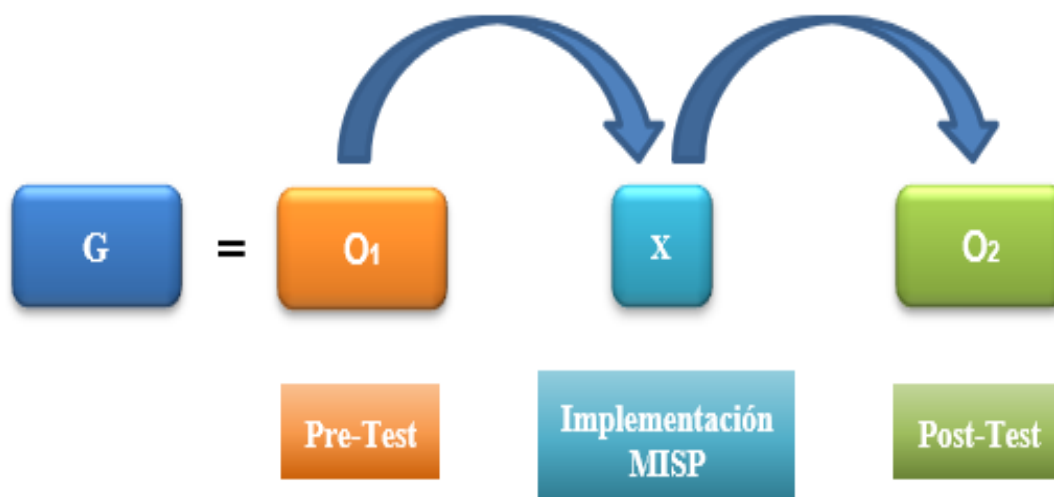


Fig. 12. Diseño de investigación.

En la Fig. 12 se muestra el Diseño de investigación experimental con dos mediciones Pre-test y Post-test de la implementación de la plataforma MISP.

4.5 Población y muestra

Población

En el contexto de metodología de la investigación científica, para [39] la población es el conjunto del objeto a estudiar, en donde las unidades de la población poseen una particularidad común, la cual se investiga y da origen a la información de la investigación.

Para fines de la investigación, la población está contemplada en 1 registro por día abarcando 2 periodos; el primer periodo para el pre-test fue de 3 meses desde mayo hasta julio del 2021 y del mismo modo, el segundo periodo para el post-test fue de 3 meses desde agosto hasta octubre del 2021, haciendo un total de 65 registros para cada periodo de evaluación. Así como se muestra en el Anexo 3.

- **Criterios de inclusión:** Para los registros se consideró a las actividades realizadas de lunes a viernes.
- **Criterios de exclusión:** Para los registros, no abarca las actividades realizadas los sábados y domingos.

Muestra

En el presente estudio no se estimó el uso de la técnica de muestreo; consecuentemente se utilizó el 100% de la población.

4.6 Técnicas e Instrumentos de recolección de datos

Para [40] refiere que la observación se caracteriza por ser interpretativa, es decir, identificar y aclarar aquello que se observa y que al final ofrece algún tipo de explicación acerca del evento.

En la investigación, la técnica e instrumento se emplearon en una oportunidad en particular, con el objetivo de recopilar información que fue de utilidad para la investigación.

- Técnicas de Recolección de Datos: Se empleó la Observación.
- Instrumentos de Recolección de Datos: Se utilizó las Fichas de Registros mostrados en el Anexo 3.

4.6.1 Nivel de Confiabilidad

Según [41] la prueba de investigación de test y retest, consiste en emplear un mismo test en dos situaciones distintas.

Asimismo, [42] definió sobre la estrategia test-retest que consiste en la utilización de un mismo instrumento a una misma muestra de sujetos en dos situaciones distintas. No existe una regla única respecto de cuál debe ser el lapso adecuado entre la primera y segunda utilización.

Para la confiabilidad del instrumento utilizado (caso numérico), se tomó, a través de la prueba de test y retest, asimismo, mediante la correlación de Pearson y su significativa para cada uno de los indicadores de cada dimensión:

- Dimensión 1: Capacidades de monitoreo.
 - ✓ Indicador: Tiempo en realizar la recolección de información de amenazas.

- Dimensión 2: Capacidades defensivas.
 - ✓ Indicador: Número de intrusos detectados en el sistema de detección de intrusos.

- Dimensión 3: Acciones preventivas.
 - ✓ Indicador: Tiempo en realizar la copia de seguridad.

Correlación de Pearson para TIEMPO EN REALIZAR LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS.

TABLA I
CORRELACIÓN DE PEARSON PARA TIEMPO EN REALIZAR LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS

Correlaciones			
		TIEMPO EN REALIZAR LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS (test)	TIEMPO EN REALIZAR LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS (retest)
TIEMPO EN REALIZAR LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS (test)	Correlación de Pearson	1	,885**
	Sig. (bilateral)		,003
	N	8	8
TIEMPO EN REALIZAR LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS (retest)	Correlación de Pearson	,885**	1
	Sig. (bilateral)	,003	
	N	8	8

** . La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Elaboración propia por el IBM SPSS Statistics.

Nota: En la tabla I, se observa el valor estadístico de la correlación de Pearson es de 0,885 siendo esta correlación muy significativa. Por lo que se puede garantizar un 99% de confianza, que en el entorno de estudio hay una correlación positiva muy elevada, porque el valor del Sig (bilateral) es de 0,003 que se encuentra por debajo del 0,01 requerido.

Correlación de Pearson para NÚMERO DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS.

TABLA II
CORRELACIÓN DE PEARSON PARA NÚMERO DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS

Correlaciones			
		NÚMERO DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS (test)	NÚMERO DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS (retest)
NÚMERO DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS (test)	Correlación de Pearson	1	,865**
	Sig. (bilateral)		,006
	N	8	8
NÚMERO DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS (retest)	Correlación de Pearson	,865**	1
	Sig. (bilateral)	,006	
	N	8	8

** . La correlación es significativa en el nivel 0,01 (bilateral).

Fuente: Elaboración propia por el IBM SPSS Statistics.

Nota: En la tabla II, se observa el valor estadístico de la correlación de Pearson es de 0,865 siendo esta correlación muy significativa. Por lo que se puede garantizar un 99% de confianza, que en el entorno de estudio hay una correlación positiva muy elevada, porque el valor del Sig (bilateral) es de 0,006 que se encuentra por debajo del 0,01 requerido.

Correlación de Pearson para TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD.

**TABLA III
CORRELACIÓN DE PEARSON PARA TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD**

Correlaciones

		TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD (test)	TIEMPO EN REALIZAR LA COPIA DE SEGURIDA (retest)
TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD test)	Correlación de Pearson	1	,833**
	Sig. (bilateral)		,010
	N	8	8
TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD (retest)	Correlación de Pearson	,833**	1
	Sig. (bilateral)	,010	
	N	8	8

** . La correlación es significativa en el nivel 0,05 (bilateral).

Fuente: Elaboración propia por el IBM SPSS Statistics.

Nota: En la tabla III, se observa el valor estadístico de la correlación de Pearson es de 0,833 siendo esta correlación muy significativa. Por lo que se puede garantizar un 99% de confianza, que en el entorno de estudio hay una correlación positiva muy elevada, porque el valor del Sig (bilateral) es de 0,010 que se encuentra por debajo del 0,05 requerido.

<i>Tabla de confiabilidad</i>				
Muy Baja	Baja	Moderada	Alta	Muy alta
0.00-0.20	0.20-0.40	0.40-0.60	0.60-0.80	0.80-1.00
0% de confiabilidad en la mediación (está contaminada de error)			100% de confiabilidad (no hay error)	
<i>Nota. Hernández, Fernández & Baptista (2010)</i>				

Fig. 13. Tabla de confiabilidad, Hernández, Fernández y Baptista (2010).

4.7 Técnicas de procesamiento y análisis de datos

4.7.1 Procesamiento de información

Para efectuar el proceso de manejo de la información, se empleó aplicaciones informáticas de tipo estadístico y lectura de datos como el mencionado IBM SPSS Statistics.

4.7.2 Análisis de datos

En la investigación se buscó equiparar los resultados del pre-test, que son los resultados obtenidos antes de implementar la plataforma, frente a los resultados del post-test, los cuales son aquellos resultados conseguidos después de realizar la implementación de la plataforma, donde se empleó la estadística descriptiva e inferencial, como la de Kolmogórov-Smirnov y la prueba de U de Mann-Whitney.

4.8 Aspectos éticos de la Investigación

Según [43]; “Puesto que la investigación científica es un comercio social, es lógico que una sociedad moralmente enferma pueda contaminar a los investigadores y científicos. No se trata únicamente de un asunto de preocupación por la honorabilidad de los sujetos de estudio o de las instituciones de investigación; es también un asunto de preocupación por la política estatal de investigación y, sobre todo, por los propios investigadores, que deben suscribirse a un código de ética”.

Según [43]; en la pregunta ¿Para quién investigar?; Responde: “Esto es un asunto que ya hemos iniciado en parte de nuestro análisis de la estrategia de investigación científica y técnica. Hoy, como en el pasado, el investigador prudente y ético se planteará constantemente esta pregunta; el resultado dependerá de su desarrollo filosófico, político, ético y otras circunstancias. Por otro lado, las universidades nacionales y privadas, que tienen un mayor nivel de discreción a la hora de elegir un tema de estudio, no guiarán todos sus esfuerzos, salvo notables excepciones, a investigar cómo perdurar el orden social. Independientemente de su origen campesino, no todos encaminarán su dedicación a los temas sociales a atender las demandas de las clases populares. Y este hecho, sin duda se ve reflejado como una falta de coherencia ética y es el resultado de una falta de educación ética, siendo lo más importante, una falta de conciencia de cambio social”.

4.9 Desarrollo de la solución

El desarrollo de la solución “Implementación de la plataforma de intercambio de información de malware (MISP)”, esta descrito en 3 fases siendo el primero, determinar los requisitos de recursos para la implementación de la plataforma; segundo, el procedimiento para la instalación de la plataforma; y tercero, el proceso de funcionamiento de la plataforma, conforme se muestra y detalla a continuación:

IMPLEMENTACIÓN DE LA PLATAFORMA DE INTERCAMBIO DE INFORMACIÓN DE MALWARE (MISP)

1. DETERMINAR LOS REQUISITOS DE RECURSOS PARA LA IMPLEMENTACIÓN DE LA PLATAFORMA MISP.

Cantidad y capacidad de recursos.

En la Fig. 14 se muestra y describe la cantidad y capacidad de recursos que un equipo de cómputo requiere para la implementación de la Plataforma MISP en el Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP.

¿Qué cantidad y capacidad de recursos se necesita para implementar el MISP?

En el Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP se promedia 50 incidentes o eventos de seguridad informática aproximadamente por cada mes; se requiere estimar la cantidad y capacidad de recursos en cuanto a Memoria RAM, DISCO DURO y CPU para los próximos 3 años.

¿Determinar cantidad de atributos?

- De cada incidente o evento en promedio, ¿Cuántos atributos se obtiene?
- Respuesta: 5 atributos (Indicadores de Compromiso – IoC).
 - ✓ $50 * 5$ atributos = 250 atributos por cada mes.
 - ✓ $250 * 36$ meses = 9 000 atributos.

¿Cuántos usuarios requiere?

- Respuesta: 10 usuarios

Cantidad de recursos que se necesita:

- MEMORIA RAM: 14GB
- DISCO DURO: 14GB
- CPU: 3 NÚCLEO



MISP Hardware Sizer (calculator)

Number of users:

10

Number of attributes (=field values):

9000

Percentage of attributes that correlate / overlap:

0% : OSINT free text attributes with no chance of two attributes in the database having the same value.
50% : a given attribute field will have the same value in 50% of events (already a huge value, rare and costly case)
If unknown, leave at 25% which is currently a good average.

25

Resulting RAM: GB

Resulting DISK: GB

Resulting CPU: * vCPU core(s) (Intel Xeon Level)

[README.txt](#) - [GitHub page](#) - [GitHub MISP](#) - [Project home](#)

Fig. 14. Medidor de hardware para implementar MISP.

REFERENCIA:

<https://www.misp-project.org/MISP-sizer/> <https://misp.github.io/MISP-sizer/>

2. PROCEDIMIENTO PARA LA INSTALACIÓN DE LA PLATAFORMA MISP.

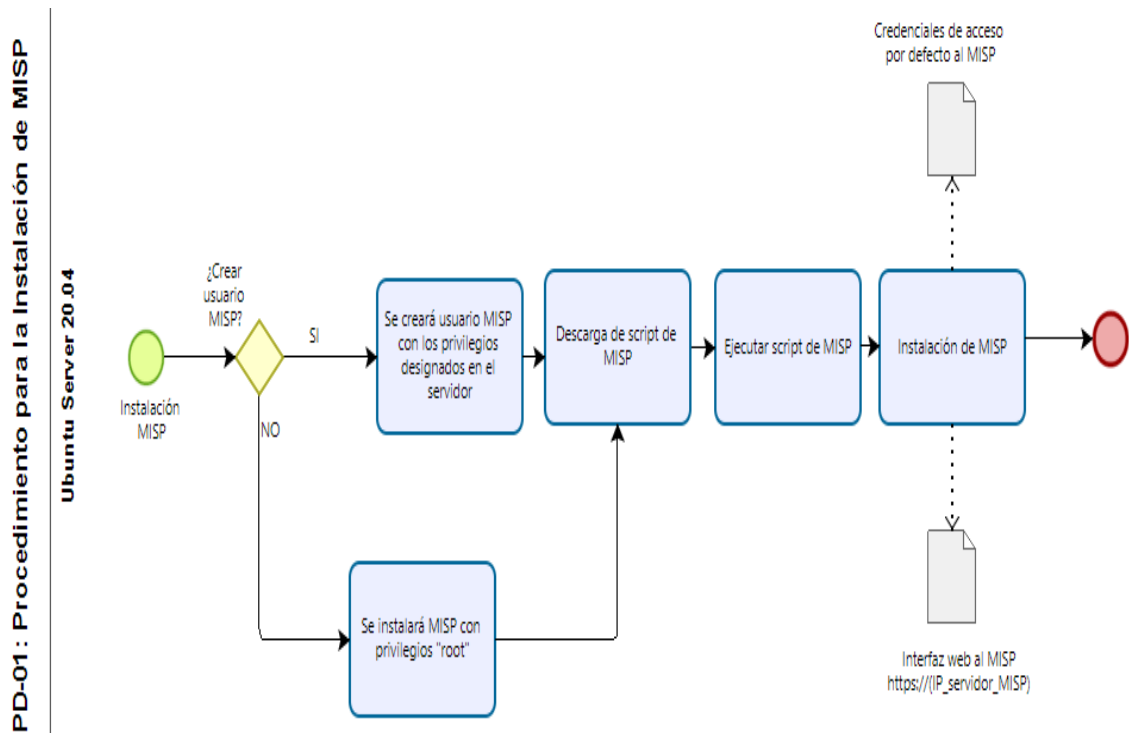


Fig. 15. Procedimiento para la instalación de la Plataforma MISP.

En la Fig. 15 se describe el paso a paso de la instalación de la Plataforma de Intercambio de Información de Malware (MISP) sobre el sistema operativo Ubuntu Server 20.04 en el Departamento de Ciberseguridad.

Paso 01: Agregar usuario “misp” con privilegios de administrador en el sistema operativo Ubuntu Server 20.04.

```
root@dirticpnp:/home/dirtic# adduser misp
Adding user `misp' ...
Adding new group `misp' (1001) ...
Adding new user `misp' (1001) with group `misp' ...
Creating home directory `/home/misp' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for misp
Enter the new value, or press ENTER for the default
  Full Name []: usuario misp
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] y
root@dirticpnp:/home/dirtic# usermod -aG sudo misp
root@dirticpnp:/home/dirtic# _
```

Fig. 16. Agregar usuario “misp” con privilegios de administrador.

Paso 04: Instalación de MISP.

```
Proceeding with the installation of MISP core
-----
Checking for sudo and installing etckeeper
[sudo] password for misp:
Hit:1 http://pe.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://pe.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:3 http://pe.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Get:4 http://pe.archive.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:5 http://pe.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [1,642 kB]
Get:6 http://pe.archive.ubuntu.com/ubuntu focal-updates/main amd64 c-n-f Metadata [14.8 kB]
Get:7 http://pe.archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packages [910 kB]
Get:8 http://pe.archive.ubuntu.com/ubuntu focal-updates/universe amd64 c-n-f Metadata [20.3 kB]
Get:9 http://pe.archive.ubuntu.com/ubuntu focal-security/main amd64 Packages [1,317 kB]
Get:10 http://pe.archive.ubuntu.com/ubuntu focal-security/main amd64 c-n-f Metadata [9,804 B]
Get:11 http://pe.archive.ubuntu.com/ubuntu focal-security/universe amd64 Packages [692 kB]
Get:12 http://pe.archive.ubuntu.com/ubuntu focal-security/universe amd64 c-n-f Metadata [14.0 kB]
Fetched 4,956 kB in 5s (993 kB/s)
```

Fig. 19. Instalación automática de MISP.

En este paso, en la Fig. 19 se procede con la instalación automática de MISP, en el cual solicitará ingresar la clave del usuario “misp” y continuar con el proceso de instalación.

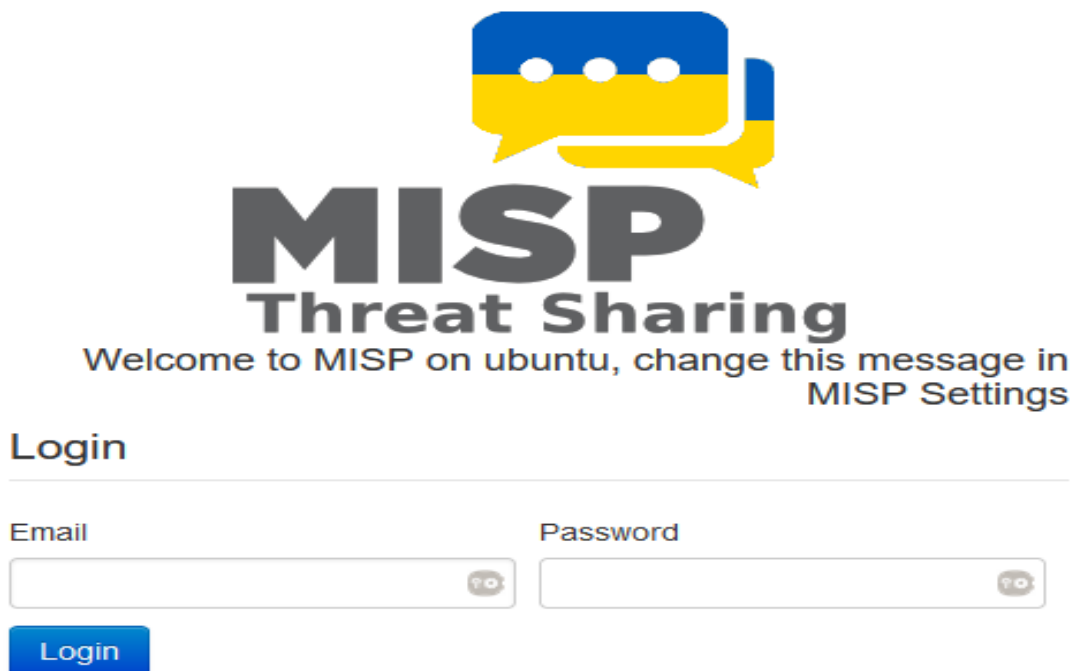
Paso 05: Credenciales de acceso al MISP.

```
##### (88%)
-----
Admin (root) DB Password:
User (misp) DB Password:
Authkey:
-----
MISP Installed, access here:
User:
Password:
-----
The following files were created and need either protection or removal (shred on the CLI)
/home/misp/mysql.txt
Contents:
Admin (root) DB Password:
User (misp) DB Password:
/home/misp/MISP-authkey.txt
Contents:
Authkey:
-----
The LOCAL system credentials:
User: misp
Password: # Or the password you used of your custom user
-----
GnuPG Passphrase is:
-----
To enable outgoing mails via postfix set a permissive SMTP server for the domains you want to contact:
sudo postconf -e 'relayhost = example.com'
sudo postfix reload
-----
Enjoy using MISP. For any issues see here: https://github.com/MISP/MISP/issues
-----
misp@dirtycnp:~$
```

Fig. 20. Credenciales de acceso al MISP.

Al finalizar la instalación, en la Fig. 20 se mostrará las credenciales de acceso por defecto a la plataforma, las credenciales de base de datos y las credenciales del sistema local de MISP.

Paso 06: Acceso a interfaz de MISP.



MISP
Threat Sharing

Welcome to MISP on ubuntu, change this message in
MISP Settings

Login

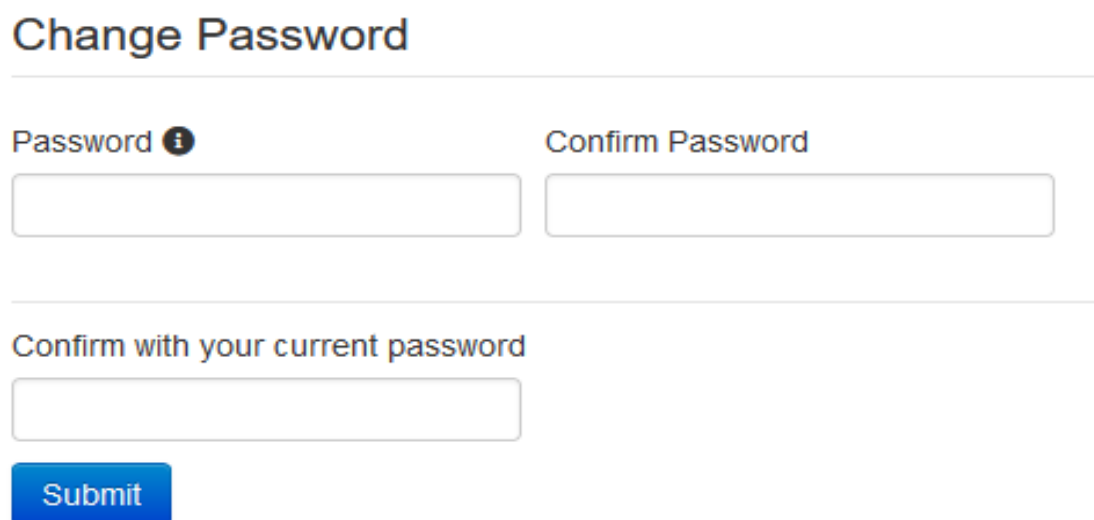
Email Password

Login

Fig. 21. Acceso a interfaz de MISP.

Una vez finalizado la instalación de MISP, en la Fig. 21 podemos acceder a la interfaz web desde [https://\(IP_servidor_MISP\)](https://(IP_servidor_MISP)). Posteriormente, para el inicio de sesión se utilizará las credenciales brindadas por defecto.

Paso 07: Cambio de contraseña.



Change Password

Password i Confirm Password

Confirm with your current password

Submit

Fig. 22. Cambio de contraseña.

En la Fig. 22 en el primer inicio de sesión se pedirá el cambio de contraseña de manera obligatoria. Posteriormente, se podrá acceder a las demás opciones y configuraciones de MISP.

Paso 08: Usuario creado en MISP.

User dibarrar@policia.gob.pe

ID	1
Email	dibarrar@policia.gob.pe
Organisation	DIRTIC PNP
Role	admin
Event alert enabled	Yes
Contact alert enabled	Yes
Invited By	N/A
NIDS Start SID	4000000
PGP key	N/A
Created	N/A

Fig. 23. Usuario administrador de MISP.

A continuación, en la Fig. 23 se muestra detalles del usuario administrador creado en la plataforma MISP.

Paso 09: Inicio de sesión en MISP.

POLICIA NACIONAL DEL PERÚ



DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN
Y COMUNICACIONES PNP

Login

Email

dibarrar@policia.gob.pe

Password

••••••••••

Login

Fig. 24. Inicio de sesión en MISP.

En la Fig. 24 finalizado las configuraciones y/o modificaciones por defecto, se debe iniciar sesión en la plataforma con las credenciales que se asignaron.



Fig. 25. Demostración de la Instalación MISP.

3. PROCESO DE FUNCIONAMIENTO DE LA PLATAFORMA MISP.

A. En la presente sección se describen todas las acciones que se realiza para recopilar información en la Plataforma de Intercambio de Información de Malware (MISP).

Paso 01: Listar todos los eventos; en la Fig. 26 la interfaz MISP permite al usuario tener una visión general o buscar eventos y atributos de eventos que ya están almacenados en el sistema de varias maneras.

Los eventos publicados contienen la siguiente información:

- La organización que lo creó; el número de identificación asignado por el sistema cuando se ingresó por primera vez; las etiquetas que se asignan al evento; el número de atributos que tiene el evento; la fecha del evento suscitado; una breve descripción del evento, y la distribución indicando cuáles son los privilegios para compartir el evento.

✘	PCM	103	🔒 CSIRT-Inst:=="Crypto Robbing Ransomware" 🟡 En Proceso	1	2021-11-08	Infección de Ransomware ROGER v4.434, [MUNICALLAO]	Community	No publicado
✓	PCM	101	👤 CSIRT-Inst:=="Difamación Imagen Institucional a través de Internet" 👤 CSIRT-Inst:=="Phishing" 🟡 En Proceso	2	2021-09-15	Reporte de URL fraudulento respecto al subsidio YANAPAY	All	
✓	PCM	100	🔒 CSIRT-Inst:=="Explotación de vulnerabilidades conocidas" 🔒 CSIRT-Inst:=="Malware" 🟡 En Proceso 🟢 TLP:=="Verde"	4	2021-09-03	Atacantes utilizan la vulnerabilidad de ShowDoc para difundir malware	All	
✓	PCM	99	🔒 CSIRT-Inst:=="Backdoors" 🔒 CSIRT-Inst:=="Malware" 🔒 CSIRT-Inst:=="RootKit"	3	2021-08-31	Detección de Malware en el archivo APK de "SnapTime Cam 11" para Android.	All	
✓	PCM	98	🔒 CSIRT-Inst:=="Modificación de información" 🔒 CSIRT-Inst:=="Modificación del sitio web" 🔒 CSIRT-Inst:=="Phishing" 🟡 TLP:=="Ambar"	2	2021-09-04	Detección de sitio web fraudulento del Banco Interbank	All	
✓	PCM	97	🔒 CSIRT-Inst:=="Phishing" 🟢 Resuelto 🟡 TLP:=="Ambar"	2	2021-09-04	Phishing, suplantando la identidad en Paypal	Community	
✓	PCM	95	🔒 CSIRT-Inst:=="Phishing" 🟢 Resuelto	2	2021-08-22	Detección de una nueva campaña de Phishing a Microsoft Office 365	Community	
✓	PCM	96	🔒 CSIRT-Inst:=="Derechos de Autor" 🔒 CSIRT-Inst:=="Phishing"	3	2021-08-21	Phishing, suplantando la identidad del banco Interbank	Community	
✓	PCM	94	🔒 CSIRT-Inst:=="Phishing" 🔒 CSIRT-Inst:=="Portal fraudulento" 🟢 Resuelto	1	2021-07-26	Intento de Fraude via SMS [Phishing BBVA]	Community	
✓	PCM	93	👤 CSIRT-Inst:=="Phishing"	1	2021-07-14	Phishing clon de pagina del Banco [BBVA Peru]	Community	
✓	PCM	92	🔒 CSIRT-Inst:=="Phishing" 🟢 Resuelto	3	2021-06-16	Phishing alojado en servidor web de la entidad [drtcp]	Community	

Fig. 26. Listado de todos los eventos en MISP.

Paso 02: Detalles de evento en MISP.

Un evento contiene la siguiente información:

- El identificador del evento; el UUID que sirve para reconocer de forma única a cada uno de los eventos: la organización que ha creado originalmente el evento; la lista de etiquetas asociadas con el evento; la fecha de detección, establecida por el usuario que crea el evento; el nivel de la amenaza que se asigna al evento; el estado del análisis; las reglas de distribución aplicadas al evento; una breve descripción del evento y si el evento ha sido publicado o no.

Atacantes utilizan la vulnerabilidad de ShowDoc para difundir malware











Event ID	100
UUID	7da93f64-6194-491c-8185-59c83fe1b860 
Creator org	PCM
Etiquetas	 CSIRT-Inst:="Explotación de vulnerabilidades conocidas"  CSIRT-Inst:="Malware"  En Proceso  TLP:="Verde"
Date	2021-09-03
Threat Level	 High
Analysis	Initial
Distribution	All communities  
Info	Atacantes utilizan la vulnerabilidad de ShowDoc para difundir malware
Published	Si (2021-09-05 12:55:15)
#Attributes	4 (0 Objects)
First recorded change	2021-09-05 12:53:59
Last change	2021-09-05 12:55:08
Modification map	
Sightings	0 (0) - restricted to own organisation only. 

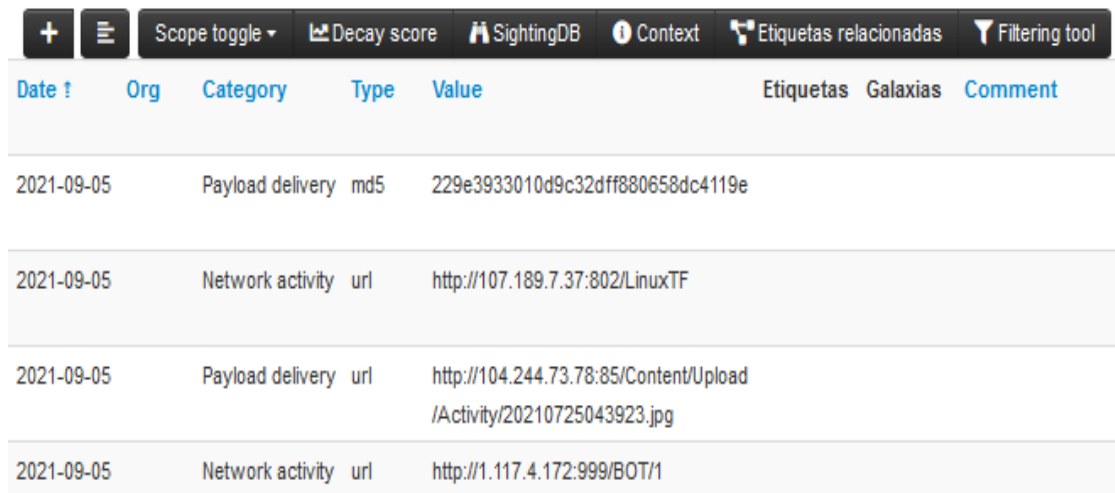
Fig. 27. Vista detallada de un evento en MISP.

En la Fig. 27 se muestra una los detalles de un evento en la Plataforma MISP.

Paso 03: Listado de atributos en los eventos MISP.

Un evento contiene atributos adjuntos con la siguiente información:

- La fecha de última modificación del atributo; la categoría del atributo, que muestra lo que describe el atributo; el tipo del valor contenido en el atributo; el valor real del atributo, que se describe un aspecto, definido por la categoría y tipo.

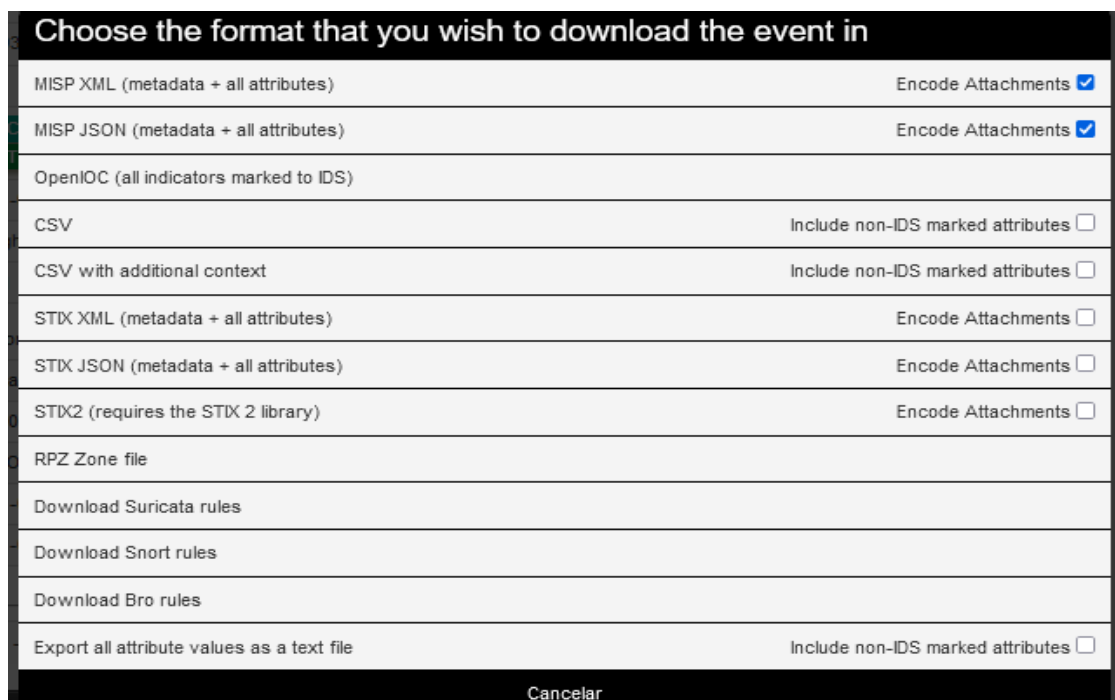


Date	Org	Category	Type	Value	Etiquetas	Galaxias	Comment
2021-09-05		Payload delivery	md5	229e3933010d9c32dff880658dc4119e			
2021-09-05		Network activity	url	http://107.189.7.37:802/LinuxTF			
2021-09-05		Payload delivery	url	http://104.244.73.78:85/Content/Upload/Activity/20210725043923.jpg			
2021-09-05		Network activity	url	http://1.117.4.172:999/BOT/1			

Fig. 28. Listado de atributos adjuntos en un evento MISP.

En la Fig. 28 se muestra el listado de los atributos adjuntos al evento.

Paso 04: Descargar eventos MISP.



Choose the format that you wish to download the event in	
MISP XML (metadata + all attributes)	Encode Attachments <input checked="" type="checkbox"/>
MISP JSON (metadata + all attributes)	Encode Attachments <input checked="" type="checkbox"/>
OpenIOC (all indicators marked to IDS)	
CSV	Include non-IDS marked attributes <input type="checkbox"/>
CSV with additional context	Include non-IDS marked attributes <input type="checkbox"/>
STIX XML (metadata + all attributes)	Encode Attachments <input type="checkbox"/>
STIX JSON (metadata + all attributes)	Encode Attachments <input type="checkbox"/>
STIX2 (requires the STIX 2 library)	Encode Attachments <input type="checkbox"/>
RPZ Zone file	
Download Suricata rules	
Download Snort rules	
Download Bro rules	
Export all attribute values as a text file	Include non-IDS marked attributes <input type="checkbox"/>
Cancelar	

Fig. 29. Descargar evento de MISP.

En la Fig. 29 se muestra las formas de descargar los eventos.

B. En la presente sección se describen todas las acciones que se realiza para compartir información en la Plataforma de Intercambio de Información de Malware (MISP).

Paso 01: Crear un evento.

Un evento es el registro de un muestrario con sus IOC (indicadores de compromiso) que se ha evidenciado de diferentes medios o se ha remitido desde un SIEM, IDS o IPS.

i. Para establecer un evento, podemos realizarlo desde el menú Events Actions/Add Event, o desde el menú principal Home, y en el menú lateral oprimir sobre Add Event.

ii. Para añadir un evento se debe agregar la siguiente información:

- Fecha de la creación del evento.
- Distribución. Este campo definirá si el evento será manifiesto por tu institución, por tu comunidad (entidades que son parte de la comunidad MISP a la que se pertenece), por comunidades conectadas a nuestra comunidad, o a todas las comunidades.
- Nivel de amenaza (alto, medio, bajo, indefinido).
- Estado en el que se encuentra el análisis (inicial, en curso, completado).
- Información relevante sobre el evento.
- Información adicional del evento, como puede ser un ID relacionado a otro programa (TheHive), o un identificador único universal (UUID).

Para la siguiente muestra, en la Fig. 30 se realizó un reporte sobre una URL de Telegram que posiblemente se encuentra vendiendo cuentas de accesos (usuario y contraseña) de los sistemas policiales de denuncias y requisitorias, habiéndose recopilado la información de un origen externo. Marcamos como nivel de amenaza alta debido a que en un análisis inicial observamos que es una cuenta de Telegram (URL), y como información del evento indicamos que se trata de una posible venta de credenciales de acceso a los sistemas policiales.

- List Events
- Add Event
- Importar desde...
- REST client

- List Attributes
- Search Attributes

- View Proposals
- Events with proposals
- View delegation requests

- Export
- Automation

Add Event

Date

Distribution i

Threat Level i

Analysis i

Event Info

Extends Event

Fig. 30. Agregar evento en MISP.

Paso 02: Tras pulsar el botón “enviar”, en la Fig. 31 se presentará el evento creado. Una vez acabado esto, se evidenciará la información general del evento, y se podrá integrar más información, como por ejemplo los IOC de la muestra, a los que MISP se refiere como Atributos.

Posible venta de credenciales de acceso a los sistemas poli...

Event ID	102
UUID	8c800362-6964-4f44-ae84-113fa8469a2f +
Creator org	PNP-PERU
Creator user	dibarrar@policia.gob.pe
Etiquetas	🌐+ 👤+
Date	2021-09-25
Threat Level	▲ High
Analysis	Initial
Distribution	This community only i ↔
Info	Posible venta de credenciales de acceso a los sistemas policiales
Published	No
#Attributes	0 (0 Objects)
First recorded change	
Last change	2021-09-25 21:18:25
Modification map	
Sightings	0 (0) - restricted to own organisation only. 🔗

Fig. 31. Información del evento creado en MISP.

Paso 03: Agregar atributos al evento; en este tercer paso para crear un evento es completarlo con atributos y archivos adjuntos. Este se puede hacer de manera manual o importarle los atributos desde un formato externo.

Fig. 32 para agregar un atributo nuevo, presionamos sobre el botón «+» (más) sobre el menú de la izquierda en Add Attribute, comenzando así un nuevo formulario. En este caso, vamos a señalar el tipo URL de la muestra, por lo que lo completamos de la siguiente manera.

Add Attribute

Category ⓘ Network activity

Type ⓘ url

Distribution ⓘ This community only

Value

https://t.me/PREMIUM27VIP

Contextual Comment

Posible venta de credenciales de acceso a los sistemas policiales

For Intrusion Detection System

Batch Import

Disable Correlation

First seen date 📅

Last seen date 📅

First seen time 🕒

HH:MM:SS.ssssss+TT:TT

Enviar Cancelar

Fig. 32. Agregar atributos en el evento MISP.

Fig. 33 se puede observar, que existen una gran variedad de categorías distintas a la hora de añadir un atributo, por lo que se deberá elegir la correspondiente dependiendo de la información que se tenga. Además, se podrá indicar que este atributo sirve para un IDS.

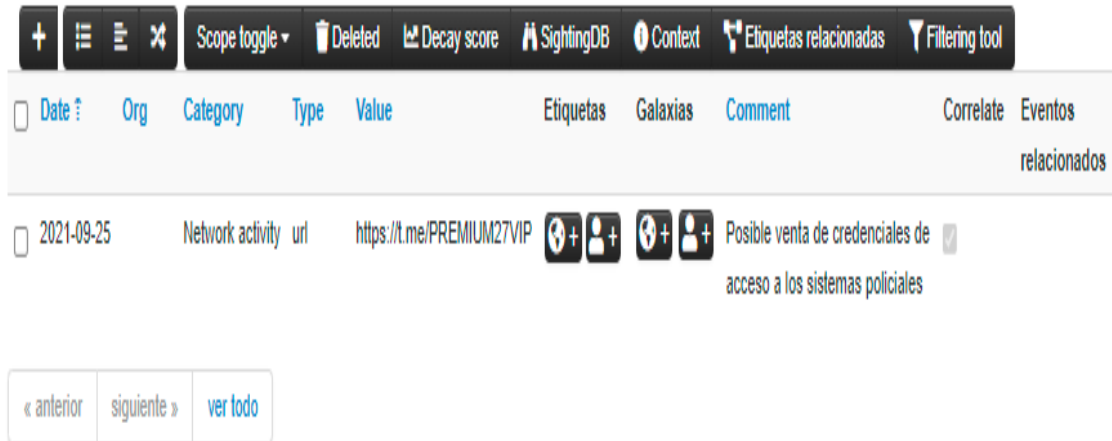


Fig. 33. Atributos agregados en el evento MISP.

Paso 04: Fig. 34 agregar etiquetas al evento; las etiquetas se suman a los atributos para permitir combinaciones avanzadas y la concatenación de atributos.

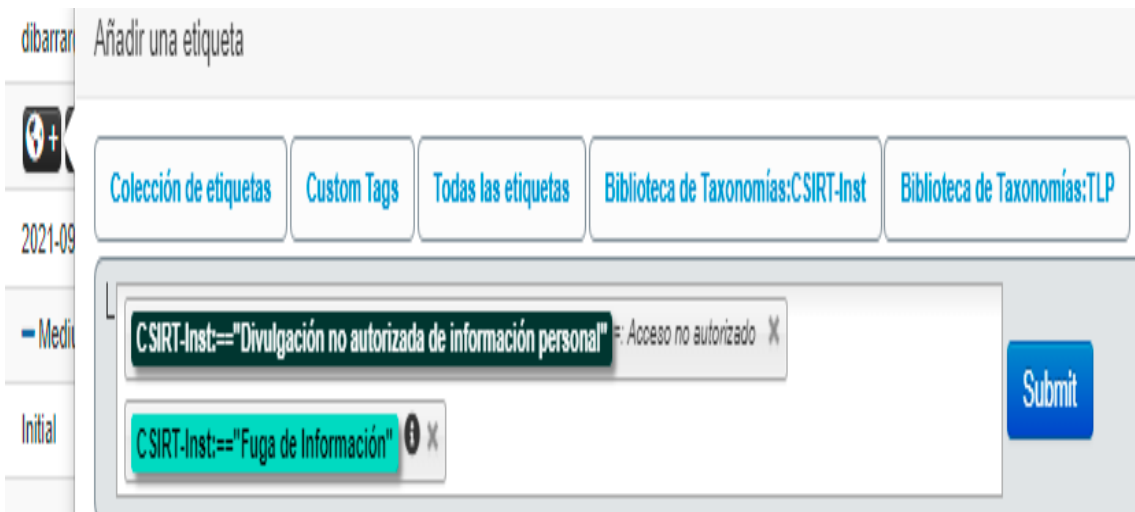


Fig. 34. Agregar etiquetas en el evento MISP.

Fig. 35 se puede apreciar que se agregaron las etiquetas de “Divulgación no autorizada de información personal” y “Fuga de información” por tener relación con la posible venta de credenciales de acceso a los sistemas policiales.

Posible venta de credenciales de acceso a los sistemas policiales

Event ID	102
UUID	8c800362-6964-4f44-ae84-113fa8469a2f
Creator org	PNP-PERU
Creator user	dibarrar@policia.gob.pe
Etiquetas	CSIRT-Inst:="Divulgación no autorizada de información personal" CSIRT-Inst:="Fuga de Información"
Date	2021-09-25
Threat Level	— Medium
Analysis	Initial
Distribution	This community only
Info	Posible venta de credenciales de acceso a los sistemas policiales
Published	No

Fig. 35. Etiquetas agregadas en el evento MISP.

Paso 05: Fig. 36 publicar el evento; una vez que todos los atributos y archivos adjuntos están cargados y configurados, es el momento de finalizar su creación publicando el evento y esto alertará a los usuarios elegibles del mismo y enviará el evento a las instancias a las que se conecta la instancia y lo propagará aún más en función de las reglas de distribución.



Fig. 36. Publicar evento MISP.

Posible venta de credenciales de acceso a los sistemas poli...

Event ID	102
UUID	8c800362-6964-4f44-ae84-113fa8469a2f
Creator org	PNP-PERU
Creator user	dibarrar@policia.gob.pe
Etiquetas	CSIRT-Inst:=="Divulgación no autorizada de información personal" x CSIRT-Inst:=="Fuga de Información" x
Date	2021-09-25
Threat Level	Medium
Analysis	Initial
Distribution	This community only
Info	Posible venta de credenciales de acceso a los sistemas policiales
Published	Si (2021-09-25 22:23:53)
#Attributes	1 (0 Objects)
First recorded change	2021-09-25 21:31:08
Last change	2021-09-25 22:12:04
Modification map	
Sightings	0 (0) - restricted to own organisation only.

Fig. 37. Evento publicado en MISP.

Paso 06: Demostración del uso de la plataforma MISP.

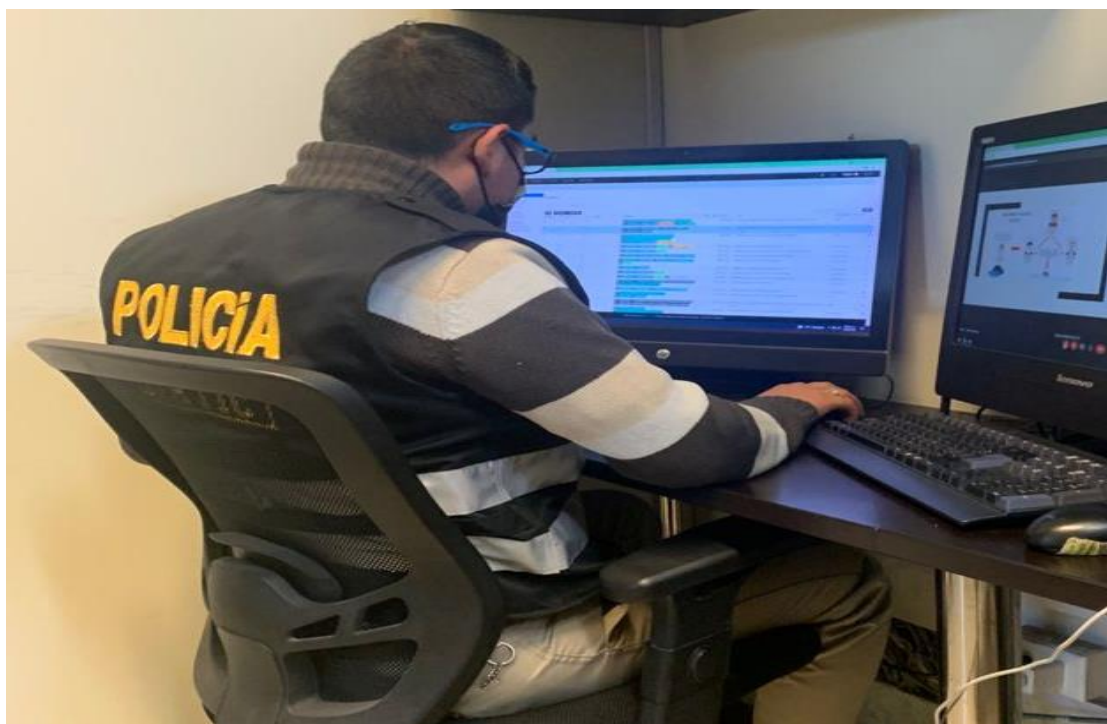


Fig. 38. Utilización de Plataforma de Intercambio de Información de Malware (MISP).

APLICACIÓN DE LA METODOLOGÍA CYBERSECURITY FRAMEWORK NIST EN EL FUNCIONAMIENTO DE LA PLATAFORMA MISP.

La presente sección se detalló la aplicabilidad de la metodología en la implementación de la plataforma MISP en el Departamento de Ciberseguridad. Teniendo en cuenta que, el Marco de Ciberseguridad NIST es un compuesto de buenas prácticas que posibilita la complementación o creación de un nuevo programa de ciberseguridad, para comprender los riesgos existentes con el fin administrarlos y poder reducir el impacto en la institución. Por otro lado, el marco se asienta en el ciclo de vida de la gestión de la ciberseguridad desde el punto de vista técnico organizacional. El ciclo de vida de la ciberseguridad se compone de funciones que permiten abstraer los principales conceptos de la ciberseguridad. A continuación, se describen las funciones:

- Identificar: Entender el contexto y conocer los activos y riesgos.
- Proteger: Aplicación de controles (técnicos, políticas, procesos) para mitigar riesgos.
- Detectar: Control y monitoreo.
- Responder: Reducir el impacto de un potencial incidente.
- Recuperar: Resiliencia y recuperación ante incidentes.



Fig. 39. Funciones Marco Ciberseguridad NIST.

Situación Actual

El Departamento de Ciberseguridad en base a sus funciones establecidas realiza patrullaje virtual en el internet y redes sociales con la finalidad de lograr información vulnerable respecto a los sistemas de información que cuenta la Policía Nacional del Perú.

Proceso: Respuesta a Incidentes de Seguridad

Objetivo: Reportar sobre posibles ventas de credenciales de acceso a los sistemas de información policial.

Función: IDENTIFICAR (ID)

Un avance clave para determinar el nivel de madurez es la identificación de los activos de información que cuenta el Departamento de Ciberseguridad y que se encuentren involucrados con el proceso y objetivo, con la finalidad de realizar un escaneo organizacional para gestionar los riesgos de ciberseguridad.

**TABLA IV
IDENTIFICACIÓN DE ACTIVOS**

Activos	Descripción
Sistema de Denuncias Policiales (SIDPOL)	Es un sistema policial donde se registran todas las denuncias realizadas por los ciudadanos a nivel comisarías y es administrada por la Dirección de Tecnología de la Información y Comunicaciones DIRTIC PNP.
Sistema de Información Policial (E-SINPOL)	Es un sistema policial donde se registran todos los antecedentes y requisitorias de los ciudadanos a nivel nacional y es administrada por la Dirección de Tecnología de la Información y Comunicaciones DIRTIC PNP.
Sistema Nacional de Registros de Denuncias de Investigación Criminal (SIRDIC)	Es un sistema policial donde se registran todas las denuncias realizadas por los ciudadanos a nivel de Direcciones Criminales y es administrada por la Dirección de Tecnología de la Información y Comunicaciones DIRTIC PNP.

Fuente: Elaboración propia.

Identificación de Amenazas cibernéticas: Reconocer las amenazas de cibernéticas que están expuestas los sistemas de información de la institución por medio de una lista de amenazas.

**TABLA V
IDENTIFICACIÓN DE AMENAZAS CIBERNÉTICAS**

Amenaza	Descripción
Phishing	Uso de tácticas de ingeniería social, donde las víctimas son engañadas por un correo electrónico o un enlace malintencionado, o manipuladas psicológicamente donde se aprovecha su declive natural a confiar.
Malware	Programas maliciosos que aprovechan vulnerabilidades y tratan de recopilar nombres de usuario y contraseñas y enviarlos a una base de datos exterior.
Agarre de formularios (Form-grabbing)	Técnica que tiene como objetivo recolectar los datos de formularios enviados por el usuario mediante un navegador web y enviarlos al panel de control malicioso.
Ataques de tipo Man in the Browser (navegador)	El modus operandi de esta amenaza es accionar como un proxy entre la víctima y el servicio al que el usuario desea acceder, ya sea modificando la comunicación entre las partes o monitoreando pasivamente las comunicaciones.
SQL injection	Los atacantes apuntan a sitios web vulnerables y generalmente tratan de explotar las vulnerabilidades SQL y las fallas de seguridad que les permita ejecutar código, leer el código fuente y modificar o eliminar archivos desde la base de datos.
Ataques de fuerza bruta y diccionario	Es el intento de adivinar o descubrir contraseñas al probar sistemáticamente cada combinación posible de caracteres hasta que la combinación correcta logre el acceso

Fuente: Elaboración propia.

Categorías aplicables de la función IDENTIFICAR (ID)

La categoría gestión de activos detalla que métodos utilizar para verificar la cantidad y tipos de activos con los que cuenta el Departamento de Ciberseguridad.

**TABLA VI
ESTUDIO DE LA CONDICIÓN GESTIÓN DE ACTIVOS**

Función	Identificador	Categoría	Descripción	Ejemplo
Identificar	ID.AM	Gestión de activos	Definir los niveles de atención de los recursos por clasificación, criticidad y valor.	Inventario de activos.

Fuente: Elaboración propia.

La categoría evaluación de riesgos detalla los métodos con los que posee para confrontar un ciberataque.

**TABLA VII
ESTUDIO DE LA CONDICIÓN EVALUACIÓN DE RIESGOS**

Función	Identificador	Categoría	Descripción	Ejemplo
Identificar	ID.RA	Evaluación de riesgos	En base al riesgo se evalúa y clasifica para su posterior tratamiento.	Política de gestión de riesgos

Fuente: Elaboración propia.

La categoría estrategia de gestión de riesgos detalla el proceso de las acciones a realizar para la identificación de algún evento que comprometa la funcionalidad de los sistemas.

**TABLA VIII
ESTUDIO DE LA CONDICIÓN ESTRATEGIA DE GESTIÓN DE RIESGOS**

Función	Identificador	Categoría	Descripción	Ejemplo
Identificar	ID.RM	Estrategia de gestión de riesgos	Al reconocer un evento que vulnere la integridad de la información se procede a salvaguardar la información actual y a tratar de eliminar el riesgo.	Procedimientos de gestión de riesgos

Fuente: Elaboración propia.

Función: PROTEGER (PR)

Una vez identificado el proceso, el objetivo y los activos de información del Departamento de Ciberseguridad, se procede con las medidas de seguridad oportunas y efectivas para garantizar la funcionalidad de los servicios críticos.

**TABLA IX
MEDIDAS Y CONTROLES DE SEGURIDAD**

Medidas de seguridad	Descripción
Política de acceso	Se fija la documentación de política y procedimientos de acceso a la información, en la cual concreta acciones, restricciones, penalización y responsables del acceso a los activos de información.
Credenciales de acceso	Se fija la lista de control de acceso de usuarios, dispositivos, protocolos de red, información, paquetes de datos que ayuden asegurar la seguridad de la información.
Perfiles de usuario	Se implementa el servicio de Directorio Activo para la gestión y control de usuario, en la cual se fija los permisos y medios tecnológicos que se puede consultar.
Autenticación doble factor	Se implementa el doble factor de autenticación, en el cual se estipula una segunda identidad a reconocer para todos los accesos de información tanto internos como remotos de los usuarios.
Formación inicial de usuarios	Todo el personal entrante de la institución, recibirá una capacitación inicial de sus cargos y la importancia de la seguridad de la información.
Copias de seguridad	Se fija la política de copias de la información, llevándose a cabo con procedimientos periódicos.
Controles de configuración	Por intermedio de registros documentales, se debe llevar la evidencia de cualquier cambio de configuración de un activo.
Eliminación de datos	Ningún dato se debe eliminar por completo, se debe establecer políticas y crear bases de datos adicionales en las cuales se guarden los registros.
Mantenimiento de software	Se realiza un plan de acción de mantenimiento futuras para el software o sistema en la institución.

Fuente: Elaboración propia.

Categorías aplicables de la función PROTEGER (PR)

La categoría gestión de identidad y control de acceso indica los métodos que poseen para la supervisión del acceso de sus usuarios al sistema.

**TABLA X
ESTUDIO DE LA CONDICIÓN GESTIÓN DE IDENTIDAD Y CONTROL DE ACCESO**

Función	Identificador	Categoría	Descripción	Ejemplo
Proteger	PR.AC	Gestión de identidad y control de acceso	Se determinan protocolos de identidad y acceso para el área y las plataformas por intermedio del registro y mantenimiento de cuentas de usuario.	Política de acceso. Credenciales de acceso. Autenticación doble factor.

Fuente: Elaboración propia.

La categoría conciencia y capacitación detalla los métodos y estrategias que posee la institución con el fin de concientizar a sus trabajadores sobre el valor de la ciberseguridad.

**TABLA XI
ESTUDIO DE LA CONDICIÓN CONCIENCIA Y CAPACITACIÓN**

Función	Identificador	Categoría	Descripción	Ejemplo
Proteger	PR.AT	Conciencia y capacitación	Crear plan de eventos de ciberseguridad donde los altos ejecutivos sean los principales sponsors en la comunicación de ciberseguridad.	.Formación de los usuarios. .Comunicación interna de ataques.

Fuente: Elaboración propia.

La categoría seguridad de datos detalla e indica los métodos para salvaguardar la integridad de la información conservada en su sistema.

**TABLA XII
ESTUDIO DE LA CONDICIÓN SEGURIDAD DE DATOS**

Función	Identificador	Categoría	Descripción	Ejemplo
Proteger	PR.DS	Seguridad de datos	Generar instructivo que contemple las funciones de la herramienta de cumplimiento para comprobar el software,	Copias de seguridad

el firmware y la integridad de la información.

Fuente: Elaboración propia.

La categoría procesos y procedimientos de protección de la información permite detallar protocolos para conservar la integridad de su información.

**TABLA XIII
ESTUDIO DE LA CONDICIÓN PROCESOS Y PROCEDIMIENTOS DE PROTECCIÓN DE LA INFORMACIÓN**

Función	Identificador	Categoría	Descripción	Ejemplo
Proteger	PR.IP	Procesos y procedimientos de protección de la información	Desarrollar procedimiento de administración de activos en caso de remoción, transferencia y/o disposición.	.Medidas de respuestas. .Gestión de vulnerabilidades.

Fuente: Elaboración propia.

La categoría mantenimiento ayudar identificar los tipos de mantenimiento que se realiza y la frecuencia.

**TABLA XIV
ESTUDIO DE LA CONDICIÓN MANTENIMIENTO**

Función	Identificador	Categoría	Descripción	Ejemplo
Proteger	PR.MA	Mantenimiento	Desarrollar procedimiento para mantenimiento incluyendo las actividades relacionadas.	Mantenimiento de software

Fuente: Elaboración propia.

Función: DETECTAR (DE)

Una vez establecidos los controles y medidas de seguridad respecto al proceso y objetivo, se procede con las labores de identificación de vulnerabilidades cibernéticas detectando de manera oportuna mediante alertas de ocurrencia.

**TABLA XV
VULNERABILIDADES CIBERNÉTICAS**

Vulnerabilidades	Descripción
Utilización de contraseñas por defecto	Los usuarios utilizan contraseñas generadas por defecto y no realizaron el cambio oportuno
Las contraseñas no cumplen con la política de seguridad	Las contraseñas utilizadas no cumplen con los 14 caracteres mínimos, no cumplen con la combinación de palabras mayúsculas y minúsculas, número y caracteres especiales y parafraseada.
No se realiza el cambio periódico de las contraseñas	Los usuarios no realizaron el cambio periódico de sus contraseñas.
Compartir credenciales de acceso	Los usuarios comparten con su entorno laboral y social sus credenciales de acceso.
No se realiza el monitoreo constante del uso de los sistemas de información	Los usuarios no realizan monitoreo de sus movimientos e ingresos en la plataforma.

Fuente: Elaboración propia.

Categorías aplicables de la función DETECTAR (DE)

La categoría anomalías y eventos ayuda identificar como la institución mitiga los incidentes previstos.

**TABLA XVI
ESTUDIO DE LA CONDICIÓN ANOMALÍAS Y EVENTOS**

Función	Identificador	Categoría	Descripción	Ejemplo
----------------	----------------------	------------------	--------------------	----------------

Detectar	DE.AE	Anomalías y eventos	Preparar procedimiento que cuente con métodos para la identificación de anomalías y eventos de seguridad, que comprenda las actividades de análisis de los ciberataques.	Análisis y recopilación de ataques. Alertas.
----------	-------	---------------------	--	--

Fuente: Elaboración propia.

La categoría vigilancia continua de seguridad reconoce los métodos que tiene la empresa para el monitoreo de sus ambientes.

**TABLA XVII
ESTUDIO DE LA CONDICIÓN VIGILANCIA CONTINUA DE SEGURIDAD**

Función	Identificador	Categoría	Descripción	Ejemplo
Detectar	DE.CM	Vigilancia continua de seguridad	Desarrollar procedimiento de monitoreo que incluya eventos de ciberseguridad relacionados a los activos, actividades y responsabilidades.	Monitorización general de no autorizados. Escaneo de vulnerabilidades.

Fuente: Elaboración propia.

La categoría procesos de detección detalla e indica los tipos de monitoreo de tránsito de red con los que cuenta la institución.

**TABLA XVIII
ESTUDIO DE LA CONDICIÓN PROCESOS DE DETECCIÓN**

Función	Identificador	Categoría	Descripción	Ejemplo
Detectar	DE.DP	Procesos de detección	Se localiza páginas con dominio malicioso mediante el LOG y se evitan con la utilización del ACL.	Cumplimiento de política de seguridad. Comunicación de eventos.

Fuente: Elaboración propia.

Función: RESPONDER (RS)

En esta función se precisan las acciones de respuesta ante posibles vulnerabilidades cibernéticas identificadas, dando como prioridad conservar el

impacto de un ataque cibernético en un círculo cerrado sin establecer una propagación del daño y mitigar dicha brecha de seguridad.

Categorías aplicables de la función RESPONDER (RS)

La categoría Planificación de la respuesta permite que los procesos y procedimientos de respuesta se realicen y se conservan garantizando una respuesta oportuna para descubrir eventos de ciberseguridad.

**TABLA XIX
ESTUDIO DE LA CONDICIÓN PLANIFICACIÓN DE RESPUESTA**

Función	Identificador	Categoría	Descripción	Ejemplo
Responder	RS.RP	Planificación de respuesta	Se establecen y mantienen todos los procesos de respuesta.	Plan de respuesta.

Fuente: Elaboración propia.

La categoría Comunicaciones determina que las acciones de respuesta se coordinan con las partes interesadas internas y externas, según corresponda.

**TABLA XX
ESTUDIO DE LA CONDICIÓN COMUNICACIONES**

Función	Identificador	Categoría	Descripción	Ejemplo
Responder	RS.CO	Comunicaciones	Diseñar un flujo de comunicación y desarrollar procedimientos para comunicar los planes de respuesta.	Información y compartición de incidentes

Fuente: Elaboración propia.

La categoría Análisis se practica para asegurar una respuesta adecuada y brindar soporte a las acciones de recuperación.

**TABLA XXI
ESTUDIO DE LA CONDICIÓN ANÁLISIS**

Función	Identificador	Categoría	Descripción	Ejemplo
---------	---------------	-----------	-------------	---------

Responder	RS.AN	Análisis	Establecer directrices para la recolección de evidencia, analizar y crear impacto de los incidentes detectados para el registro de lecciones aprendidas.	Análisis forense
-----------	-------	----------	--	------------------

Fuente: Elaboración propia.

La categoría Mitigación especifica que se realizan acciones para prevenir el esparcimiento de un evento, mitigar sus efectos y eliminar el incidente.

**TABLA XXII
ESTUDIO DE LA CONDICIÓN MITIGACIÓN**

Función	Identificador	Categoría	Descripción	Ejemplo
Responder	RS.MI	Mitigación	Se realizan actividades para mitigar los efectos y resolver el evento.	Mitigación y documentación de los eventos

Fuente: Elaboración propia.

La categoría Mejoras describe que las acciones de respuesta de la institución prosperan por la incorporación de lecciones aprendidas de las acciones de detección y respuesta actuales y anteriores.

**TABLA XXIII
ESTUDIO DE LA CONDICIÓN MEJORAS**

Función	Identificador	Categoría	Descripción	Ejemplo
Responder	RS.IM	Mejoras	Comprobar el impacto de los incidentes detectados para registrar las lecciones aprendidas y relacionarlo al plan de respuesta a los incidentes.	Estrategia y lecciones de mejora.

Fuente: Elaboración propia.

Función: RECUPERAR (RC)

En esta función se implantan controles para mantener y restablecer el servicio que haya sido perjudicado por alguna inseguridad cibernética, teniendo como objetivo restaurar la funcionalidad del servicio mitigando el impacto de la brecha

de seguridad en la fase anterior y poniéndolo a trabajar nuevamente en esta fase.

Categorías aplicables de la función RECUPERAR (RC)

La categoría Planificación de recuperación se implantan y mantienen los procesos de recuperación de la seguridad de información en la institución, asegurando la restauración de los activos perjudicados por los eventos de ciberseguridad.

**TABLA XXIV
ESTUDIO DE LA CONDICIÓN PLANIFICACIÓN DE RECUPERACIÓN**

Función	Identificador	Categoría	Descripción	Ejemplo
Recuperar	RC.RP	Planificación de recuperación	Desarrollar procedimientos para ejecutar actividades de recuperación durante los eventos de seguridad.	Políticas de seguridad de la información.

Fuente: Elaboración propia.

La categoría Mejoras determina que aplicando el filtro de las fases de protección y respuesta se formaliza implementar mejoras de seguridad en base a los eventos suscitados.

**TABLA XXV
ESTUDIO DE LA CONDICIÓN MEJORAS**

Función	Identificador	Categoría	Descripción	Ejemplo
Recuperar	RC.IM	Mejoras	Revisar el impacto de los incidentes detectados para detectar mejoras en el servicio.	Mejoras de incidentes.

Fuente: Elaboración propia.

La categoría Comunicaciones determina que las actividades de recuperación deber ser avisadas y coordinadas con todo el sector o personal involucrado y afectado con el evento de ciberseguridad, el cual se requiere superar y presentar nuevamente el servicio.

**TABLA XXVI
ESTUDIO DE LA CONDICIÓN COMUNICACIONES**

Función	Identificador	Categoría	Descripción	Ejemplo
Recuperar	RC.CO	Comunicaciones	Crear un flujo de aviso y desarrollar el proceso de comunicación luego de ser mitigado un evento de ciberseguridad.	Comunicación de recuperación.

Fuente: Elaboración propia.

CAPITULO V

RESULTADOS

Según el estudio realizado se implementó una plataforma para evaluar el nivel de las capacidades de monitoreo, las capacidades defensivas y las acciones preventivas con la finalidad de mejorar la predicción de ciberataques; para ello se decidió realizar un pre-test de la situación en que se encontraba el Departamento de Ciberseguridad de la División de Informática DIRTIC PNP; llegando así a conocer las condiciones reales que se encontró y luego se implementó la plataforma de intercambio de información de malware llegando a evaluar las nuevas condiciones mediante el post-test con la plataforma para verificar las hipótesis planteadas.

5.1 Descripción de resultados

Se ingresaron los datos en la aplicación IBM SPSS Statistics, obteniendo los resultados estadísticos descriptivos, mostrados en la tabla XXVII.

**TABLA XXVII
ESTADÍSTICOS DESCRIPTIVOS DE LAS DIMENSIONES POR TIPO DE PRUEBA**

Descriptivos				
Tipo de prueba			Estadístico	Desv. Error
TIEMPO EN REALIZAR LA RECOLECCIÓN	Pre Test	Media	6,1231	,09433
		Límite inferior	5,9346	

DE INFORMACIÓN DE AMENAZAS		95% de intervalo de confianza para la media	Límite superior	6,3115	
		Media recortada al 5%		6,1368	
		Mediana		6,0000	
		Varianza		,578	
		Desv. Desviación		,76050	
		Mínimo		5,00	
		Máximo		7,00	
		Rango		2,00	
		Rango intercuartil		1,00	
		Asimetría		-,212	,297
		Curtosis		-1,224	,586
		Media		4,1231	,09433
		TIEMPO EN REALIZAR LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS	Post Test	95% de intervalo de confianza para la media	Límite inferior
	Límite superior			4,3115	
Media recortada al 5%				4,1368	
Mediana				4,0000	
Varianza				,578	
Desv. Desviación				,76050	
Mínimo				3,00	
Máximo				5,00	
Rango				2,00	
Rango intercuartil				1,00	
Asimetría				-,212	,297
Curtosis				-1,224	,586
Media				91,2154	,77939
NÚMERO DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS	Pre Test	95% de intervalo de confianza para la media	Límite inferior	89,6584	
			Límite superior	92,7724	
		Media recortada al 5%		91,3120	
		Mediana		90,0000	
		Varianza		39,484	
		Desv. Desviación		6,28364	
		Mínimo		80,00	

		Máximo	100,00	
		Rango	20,00	
		Rango intercuartil	11,50	
		Asimetría	,016	,297
		Curtosis	-1,345	,586
NÚMERO DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS	Post Test	Media	111,2154	,77939
		95% de intervalo de confianza para la media	Límite inferior	109,6584
			Límite superior	112,7724
		Media recortada al 5%	111,3120	
		Mediana	110,0000	
		Varianza	39,484	
		Desv. Desviación	6,28364	
		Mínimo	100,00	
		Máximo	120,00	
		Rango	20,00	
		Rango intercuartil	11,50	
		Asimetría	,016	,297
		Curtosis	-1,345	,586
		TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD	Pre Test	Media
95% de intervalo de confianza para la media	Límite inferior			5,6301
	Límite superior			6,0007
Media recortada al 5%	5,7949			
Mediana	6,0000			
Varianza	,559			
Desv. Desviación	,74775			
Mínimo	5,00			
Máximo	7,00			
Rango	2,00			
Rango intercuartil	1,00			
Asimetría	,317			,297
Curtosis	-1,132			,586
TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD	Post Test			Media
		95% de intervalo de confianza para la media	Límite inferior	3,0877
			Límite superior	3,2815

Media recortada al 5%	3,1496	
Mediana	3,0000	
Varianza	,153	
Desv. Desviación	,39100	
Mínimo	3,00	
Máximo	4,00	
Rango	1,00	
Rango intercuartil	,00	
Asimetría	1,664	,297
Curtosis	,794	,586

Fuente: Elaboración propia por el IBM SPSS Statistics.

**TABLA XXVIII
RESUMEN DE LOS ESTADÍSTICOS DESCRIPTIVOS DE LAS DIMENSIONES**

Dimensiones	Tipo de prueba	Media	Desviación	Coefficiente de variación
Capacidades de monitoreo	Pre test	6,1231	,76050	12,4%
	Post test	4,1231	,76050	18,4%
Capacidades defensivas	Pre test	91,2154	6,28364	6,8%
	Post test	111,2154	6,28364	5,6%
Acciones preventivas	Pre test	5,8154	,74775	12,8%
	Post test	3,1846	,39100	12,2%

Fuente: Elaboración propia.

Interpretación:

De acuerdo a la tabla XXVIII, se tuvo el resumen de los estadísticos descriptivos en el cual la desviación estándar entre la media da como resultado el coeficiente de variación, donde se observó diferencias para cada dimensión por tipo de prueba (pre test y post test).

Para las capacidades de monitoreo se observó en la tabla XXVIII, que hay diferencias entre la media y la desviación estándar; asimismo, el coeficiente de variación es mayor para el post test (12,4%) sobre el pre test (18,4%).

Para las capacidades defensivas se observó en la tabla XXVIII, que hay diferencias entre la media y la desviación estándar; asimismo, el coeficiente de variación es mayor para el pre test (6,8%) sobre el post test (5,6%).

Para las acciones preventivas se observó en la tabla XXVIII, que hay diferencias entre la media y la desviación estándar; asimismo, el coeficiente de variación es mayor para el post test (12,8%) sobre el pre test (12,2%).

Diagrama de cajas sobre capacidades de monitoreo – TIEMPO EN REALIZAR LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS (pre test) y (post test).

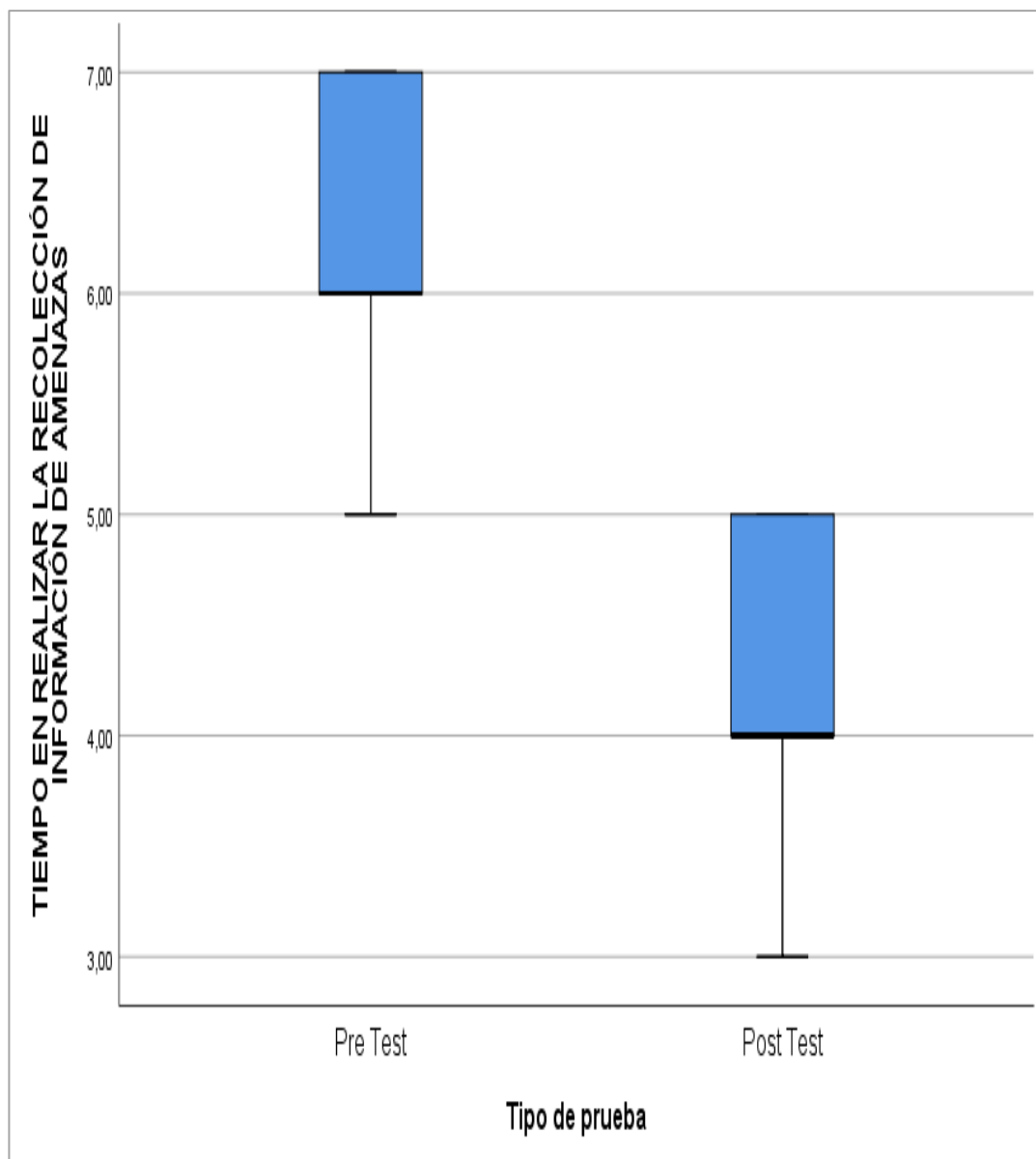


Fig. 40. Diagrama de cajas sobre capacidades de monitoreo – TIEMPO EN REALIZAR LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS (pre test) y (post test).

Interpretación:

En la Fig. 40, en el diagrama de cajas se observó las diferencias entre las medianas para el tiempo en realizar la recolección de información de amenazas, porque se tiene diferencias entre ambas pruebas del pre test y post test.

Diagrama de cajas sobre capacidades defensivas – NÚMERO DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS (pre test) y (post test).

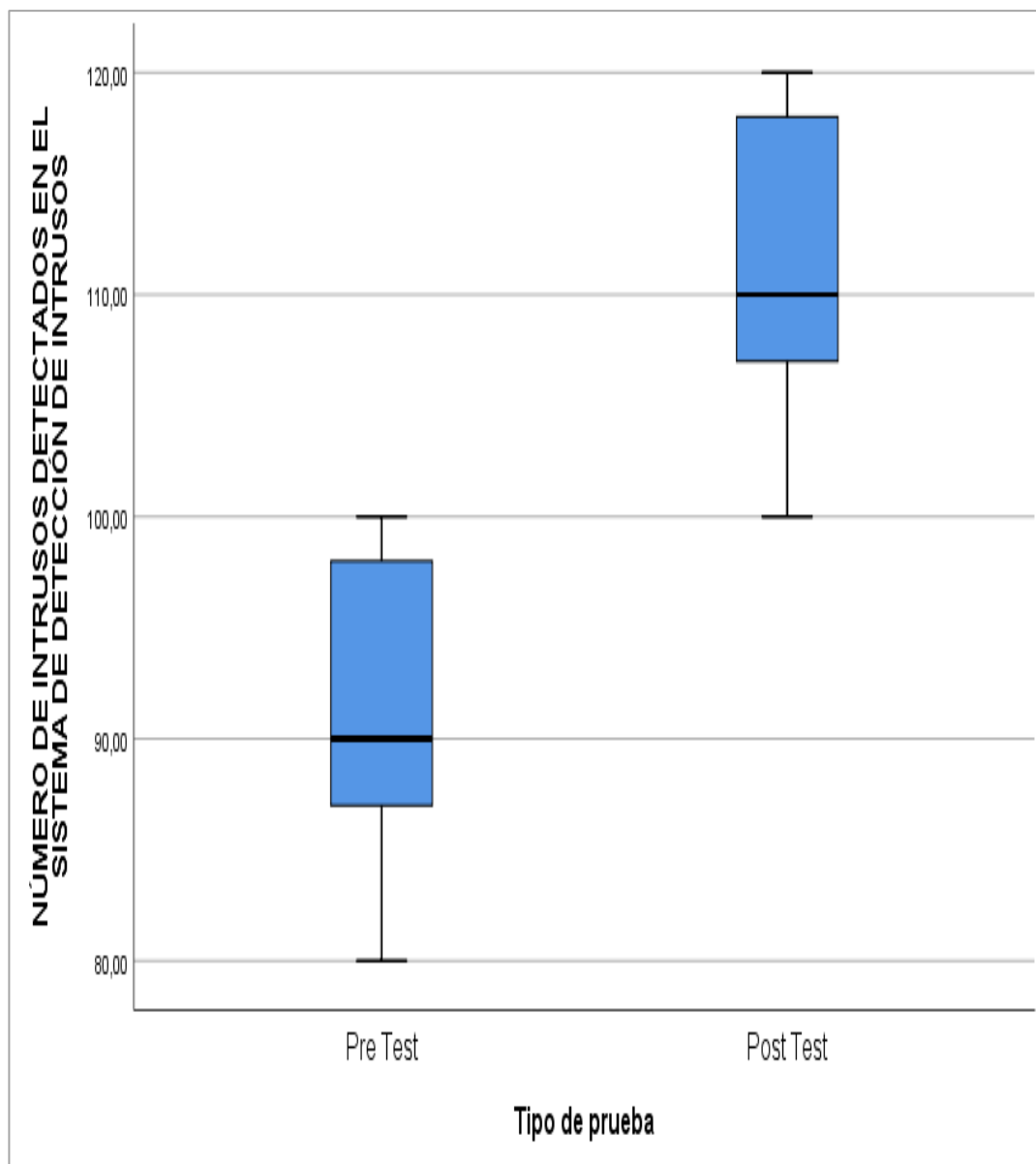


Fig. 41. Diagrama de cajas sobre capacidades defensivas – NÚMERO DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS (pre test) y (post test).

Interpretación:

En la Fig. 41, en el diagrama de cajas se observó las diferencias entre las medianas para el número de intrusos detectados en el sistema de detección de intrusos, porque se tiene diferencias entre ambas pruebas del pre test y post test.

Diagrama de cajas sobre acciones preventivas – TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD (pre test) y (post test).

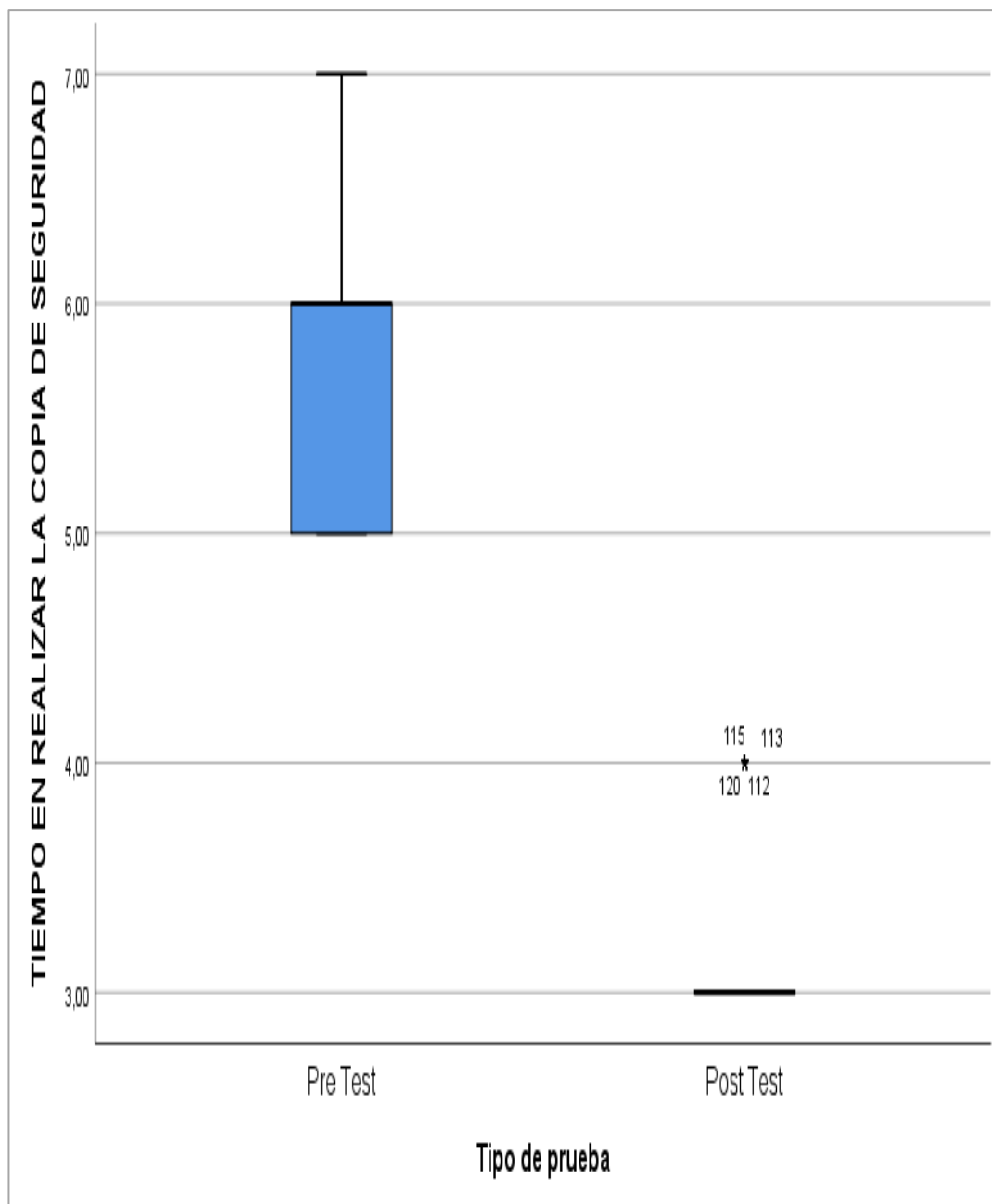


Fig. 42. Diagrama de cajas sobre acciones preventivas – TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD (pre test) y (post test).

Interpretación:

En la Fig. 42, en el diagrama de cajas se observó las diferencias entre las medianas para el tiempo en realizar la copia de seguridad, porque se tiene diferencias entre ambas pruebas del pre test y post test.

5.2 Contratación de hipótesis

Prueba de Normalidad

- H0: Los datos provienen de una distribución normal.
- H1: Los datos no provienen de una distribución normal.
- Nivel de significancia: 0.05
- Criterio de prueba:
 - ✓ Sig < 0,05 donde se rechaza la H0.
 - ✓ Sig > 0,05 se acepta la H0.

**TABLA XXIX
PRUEBA DE NORMALIDAD DE KOLMOGÓROV-SMIRNOV**

	Tipo de prueba	Kolmogórov-Smirnov ^a			Criterio Sig<0.05
		Estadístico	gl	Sig.	
TIEMPO EN REALIZAR LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS	Pre Test	,229	65	,000	No normal
	Post Test	,229	65	,000	No normal
NÚMERO DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS	Pre Test	,152	65	,001	No normal
	Post Test	,152	65	,001	No normal
TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD	Pre Test	,247	65	,000	No normal
	Post Test	,497	65	,000	No normal

a. Corrección de significación de Lilliefors.

Fuente: Elaboración propia por el IBM SPSS Statistics.

En la tabla XXIX, se aplicó la prueba de normalidad de Kolmogórov-Smirnov, donde se consideró que el Sig.=0,000<0,05 en el cual se rechaza la H0; es decir, se concluye que los datos no provienen de una distribución normal, en las dimensiones e indicadores. Por lo tanto, se consideró que son distribuciones no normales y se utilizaron procedimientos de la estadística no paramétrica. Para poder comparar ambos grupos no relacionados, correspondió a la prueba de U de Mann Whitney.

5.2.1 Prueba de contraste de hipótesis general

- H0: No Existen diferencias en la implementación de la plataforma de intercambio de información de malware para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática DIRTIC PNP, Lima.
- H1: Existen diferencias en la implementación de la plataforma de intercambio de información de malware para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática DIRTIC PNP, Lima.
- Nivel de significancia: 0,05
- Criterio: Si $p_{valor} = Sig < 0,05$ se rechaza la H0, caso contrario se acepta.

Prueba de U de Mann-Whitney

TABLA XXX
RANGOS PARA PRUEBA DE U DE MANN-WHITNEY

Rangos				
	Tipo de prueba	N	Rango promedio	Suma de rangos
TIEMPO EN LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS EN DÍAS	Pre Test	65	95,35	6197,50
	Post Test	65	35,65	2317,50
	Total	130		
NÚMERO DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS	Pre Test	65	33,05	2148,50
	Post Test	65	97,95	6366,50
	Total	130		
TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD EN DÍAS	Pre Test	65	98,00	6370,00
	Post Test	65	33,00	2145,00
	Total	130		

Fuente: Elaboración propia por el IBM SPSS Statistics.

En la tabla XXX, se exhibe una explicación de los tipos de prueba comparados, la suma de rangos y un valor que representa cual tipo tiene una mediana mayor, este dato es el rango promedio, que se consigue de dividir la suma de rangos de cada tipo de prueba entre la cantidad de datos, para los indicadores de cada dimensión.

TABLA XXXI
ESTADÍSTICOS DE PRUEBA PARA PRUEBA DE U DE MANN-WHITNEY
Estadísticos de prueba^a

	TIEMPO EN REALIZAR LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS	NÚMERO DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS	TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD
U de Mann-Whitney	172,500	3,500	,000
W de Wilcoxon	2317,500	2148,500	2145,000
Z	-9,267	-9,827	-10,286
Sig. asintótica(bilateral)	,000	,000	,000

a. Variable de agrupación: tipo de prueba

Fuente: Elaboración propia por el IBM SPSS Statistics.

Interpretación:

En consideración a la tabla XXXI, y en relación a la prueba de U de Mann-Whitney, se puede inferir que la predicción de ciberataques (basado en los indicadores de las tres dimensiones que la conforman) presentó en cada caso una significancia= $0,000 < 0,05$ por ende, la prueba es significativo, por ello se deduce que presentan desigualdades en la implementación de la plataforma de intercambio de información de malware para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática DIRTIC PNP, Lima.

5.2.2 Prueba de contraste para hipótesis específica 1

- H0: No Existen diferencias en la implementación de la plataforma de intercambio de información de malware para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática DIRTIC PNP, Lima.
- H1: Existen diferencias en la implementación de la plataforma de intercambio de información de malware para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática DIRTIC PNP, Lima.
- Nivel de significación: 0,05

- Criterio: Si $p_{valor} = \text{Sig} < 0,05$ se rechaza la H_0 , caso contrario se acepta.

Prueba de U de Mann-Whitney

TABLA XXXII
RANGOS PARA PRUEBA DE U DE MANN-WHITNEY - TIEMPO EN REALIZAR LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS

Rangos				
	Tipo de prueba	N	Rango promedio	Suma de rangos
TIEMPO EN REALIZAR LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS	Pre Test	65	95,35	6197,50
	Post Test	65	35,65	2317,50
	Total	130		

Fuente: Elaboración propia por el IBM SPSS Statistics.

Interpretación:

Tomando en consideración los resultados de la tabla XXXII, se puede decir que el indicador tiempo en realizar la recolección de información de amenazas de la dimensión capacidades de monitoreo en el pre test presenta una estimación de 95,35 y por otro lado en el post test presenta una estimación de 35,65.

TABLA XXXIII
ESTADÍSTICOS DE PRUEBA PARA PRUEBA DE U DE MANN-WHITNEY - TIEMPO EN REALIZAR LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS.

Estadísticos de prueba^a	
TIEMPO EN REALIZAR LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS	
U de Mann-Whitney	172,500
W de Wilcoxon	2317,500
Z	-9,267
Sig. asintótica(bilateral)	,000

a. Variable de agrupación: tipo de prueba

Fuente: Elaboración propia por el IBM SPSS Statistics.

Interpretación:

En consideración a la tabla XXXIII, y en relación a la prueba de U de Mann-Whitney, se puede inferir que el indicador tiempo en realizar la recolección de información de amenazas de la dimensión capacidades de monitoreo

presentaron una $\text{Sig.}=0,000<0,05$ por ende, la prueba es significativo y se rechaza H_0 , por ello se deduce que presentan desigualdades en la implementación de la plataforma de intercambio de información de malware para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática DIRTIC PNP, Lima.

5.2.3 Prueba de contraste para hipótesis específica 2

- H_0 : No Existen diferencias en la implementación de la plataforma de intercambio de información de malware para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática DIRTIC PNP, Lima.
- H_1 : Existen diferencias en la implementación de la plataforma de intercambio de información de malware para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática DIRTIC PNP, Lima.
- Nivel de significación: 0,05
- Criterio: Si $p\text{valor} = \text{Sig} < 0,05$ se rechaza la H_0 , caso contrario se acepta.

Prueba de U de Mann-Whitney

TABLA XXXIV
RANGOS PARA PRUEBA DE U DE MANN-WHITNEY - NÚMERO DE INTRUSOS
DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS

Rangos				
	Tipo de prueba	N	Rango promedio	Suma de rangos
NÚMERO DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS	Pre Test	65	33,05	2148,50
	Post Test	65	97,95	6366,50
	Total	130		

Fuente: Elaboración propia por el IBM SPSS Statistics.

Interpretación:

Tomando en consideración los resultados de la tabla XXXIV, se puede decir que el indicador número de intrusos detectados en el sistema de detección de intrusos de la dimensión capacidades defensivas en el pre test presenta una estimación de 33,05 y por otro lado en el post test presenta una estimación de 97,95.

TABLA XXXV
ESTADÍSTICOS DE PRUEBA PARA PRUEBA DE U DE MANN-WHITNEY - NÚMERO
DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS

Estadísticos de prueba^a

	NÚMERO DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS
U de Mann-Whitney	3,500
W de Wilcoxon	2148,500
Z	-9,827
Sig. asintótica(bilateral)	,000

a. Variable de agrupación: tipo de prueba

Fuente: Elaboración propia por el IBM SPSS Statistics.

Interpretación:

En consideración a la tabla XXXV, y en relación a la prueba de U de Mann-Whitney, se puede inferir que el indicador número de intrusos detectados en el sistema de detección de intrusos de la dimensión capacidades defensivas presentaron una Sig.=0,000<0,05 por ende, la prueba es significativo y se rechaza H0, por ello se deduce que presentan desigualdades en la implementación de la plataforma de intercambio de información de malware para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática DIRTIC PNP, Lima.

5.2.4 Prueba de contraste para hipótesis específica 3

- H0: No Existen diferencias en la implementación de la plataforma de intercambio de información de malware para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática DIRTIC PNP, Lima.
- H1: Existen diferencias en la implementación de la plataforma de intercambio de información de malware para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática DIRTIC PNP, Lima.
- Nivel de significación: 0,05
- Criterio: Si pvalor= Sig <0,05 se rechaza la H0, caso contrario se acepta.

Prueba de U de Mann-Whitney

TABLA XXXVI
RANGOS PARA PRUEBA DE U DE MANN-WHITNEY - TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD

Rangos				
	Tipo de prueba	N	Rango promedio	Suma de rangos
TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD	Pre Test	65	98,00	6370,00
	Post Test	65	33,00	2145,00
	Total	130		

Fuente: Elaboración propia por el IBM SPSS Statistics.

Interpretación:

Tomando en consideración los resultados de la tabla XXXVI, se puede decir que el indicador tiempo en realizar la copia de seguridad de la dimensión acciones preventivas en el pre test presentan una estimación de 98,00 y por otro lado en el post test presenta una estimación de 33,00.

TABLA XXXVII
ESTADÍSTICOS DE PRUEBA PARA PRUEBA DE U DE MANN-WHITNEY - TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD

Estadísticos de prueba^a

TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD	
U de Mann-Whitney	,000
W de Wilcoxon	2145,000
Z	-10,286
Sig. asintótica(bilateral)	,000

a. Variable de agrupación: tipo de prueba

Fuente: Elaboración propia por el IBM SPSS Statistics.

Interpretación:

En consideración a la tabla XXXVII, y en relación a la prueba de U de Mann-Whitney, se puede inferir que el indicador tiempo en realizar la copia de seguridad de la dimensión acciones preventivas presentaron una Sig.=0,000<0,05 por ende, la prueba es significativo y se rechaza H0, por ello se deduce que presentan desigualdades en la implementación de la plataforma de intercambio de información de malware para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática DIRTIC PNP, Lima.

ANÁLISIS Y DISCUSIÓN DE RESULTADOS

En base a todos los resultados en la presente investigación realizada, se analizó y se realizó una comparativa respecto a los indicadores planteados como son el tiempo en realizar la recolección de información de amenazas de la dimensión capacidades de monitoreo, el número de intrusos detectados en el sistema de detección de intrusos de la dimensión capacidades defensivas y el tiempo en realizar la copia de seguridad de la dimensión acciones preventivas, para determinar que la implementación de la plataforma de intercambio de información de malware mejora la predicción de ciberataques en el Departamento de Ciberseguridad de la División de Informática DIRTIC PNP.

Primero: Con respecto al primer indicador, tiempo en realizar la recolección de información de amenazas de la dimensión capacidades de monitoreo; antes que se implemente la plataforma de intercambio de información de malware se revela en el pre-test el tiempo promedio en realizar la recolección de información de amenazas en 6,1231 con un coeficiente de variación de 12,4% y después de implementar la plataforma de intercambio de información de malware se revela en el post-test el tiempo promedio en realizar la recolección de información de amenazas en 4,1231 con un coeficiente de variación de 18,4%, dando como resultado una mejora para el tiempo en realizar la recolección de información de amenazas. Al emplear la prueba de normalidad de Kolmogórov-Smirnov, se puede notar que el valor Significancia=0,000 cuyo valor es menor de 0,05 tanto en pre-test y post-test, por ende, el test es significativo, por lo tanto, se concluye que existen desigualdades en la implementación de la plataforma de intercambio de información de malware para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática DIRTIC PNP, Lima.

Asimismo, en relación a los resultados obtenidos en la tesis realizada por [15], resaltó la gran importancia que se tiene al implementar un sistema para la predicción de ciberataques, obteniendo como resultado que el sistema SCADA tuvo la mejor probabilidad de predicción de ataques (98%) para la recolección de información y monitoreo de

amenazas, teniendo mucho potencial que puede verse en igualdad de condiciones con respecto al uso de la plataforma de intercambio de información de malware (MISP); este antecedente corrobora los resultados de la presente investigación.

Segundo: Con respecto al segundo indicador, número de intrusos detectados en el sistema de detección de intrusos de la dimensión capacidades defensivas; antes que se implemente la plataforma de intercambio de información de malware se revela en el pre-test el número promedio en 91,2154 con un coeficiente de variación de 6,8% y después de implementar la plataforma de intercambio de información de malware se revela en el post-test el número promedio en 111,2154 con un coeficiente de variación de 5,6%, dando como resultado una mejora para el número de intrusos detectados en el sistema de detección de intrusos. Al emplear la prueba de normalidad de Kolmogórov-Smirnov, se puede notar que el valor Significancia=0,001 cuyo valor es menor de 0,05 tanto en pre-test y post-test, por ende, el test es significativo, por lo tanto, se concluye que existen desigualdades en la implementación de la plataforma de intercambio de información de malware para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática DIRTIC PNP, Lima.

Por otro lado, en relación a los resultados obtenidos en la tesis de [30], indicó la importancia en que se debe dar al resguardo del activo de información de la institución mediante técnicas defensivas, obteniéndose como resultado que la implementación de herramientas de seguridad perimetral tuvo la mejor probabilidad de predicción de ataques (70%) en las técnicas defensivas ante los ciberataques, teniendo mucho potencial y pudiéndose ver en igualdad de condiciones con respecto al uso de la plataforma de intercambio de información de malware (MISP); este antecedente corrobora los resultados de la presente investigación.

Tercero: Con respecto al tercer indicador, tiempo en realizar la copia de seguridad de la dimensión acciones preventivas; antes que se implemente la

plataforma de intercambio de información de malware se revela en el pre-test el tiempo promedio en realizar la copia de seguridad en 5,8154 con un coeficiente de variación de 12,8% y después de implementar la plataforma de intercambio de información de malware se revela en el post-test el tiempo promedio en realizar la copia de seguridad en 3,1846 con un coeficiente de variación de 12,2%, dando como resultado una mejora para el tiempo en realizar la copia de seguridad. Al emplear la prueba de normalidad de Kolmogórov-Smirnov, se puede notar que el valor Significancia=0,000 cuyo valor es menor de 0,05 tanto en pre-test y post-test, por ende, el test es significativo, por lo tanto, se concluye que existen desigualdades en la implementación de la plataforma de intercambio de información de malware para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática DIRTIC PNP, Lima.

Continuando con lo anterior, y en referencia a los resultados obtenidos en el artículo de [27], indicó la importancia en desarrollar una sólida estrategia de residencia cibernética, significando el desarrollo de la capacidad para detectar y corregir los ciberataques y se obtuvo como resultado que la implementación de un mecanismo de resguardo de información y cooperación tuvo la mejor probabilidad de predicción de ataques (75%) en las acciones correctivas ante los ciberataques y tiene mucho potencial y puede verse en igualdad de condiciones con respecto al uso de la plataforma de intercambio de información de malware (MISP); este antecedente corrobora los resultados de la presente investigación.

Cuarto: En razón a los componentes de la investigación como el marco teórico, antecedentes mencionados, estadísticas empleada y resultados obtenidos sirvió en gran escala para demostrar las diferentes evidencias existentes en la implementación de la plataforma de intercambio de información de malware (MISP), logrando obtener resultados que demuestra el nivel de capacidades de monitoreo mejoró en un 18,4%, el nivel de capacidades defensivas mejoró en un 5,6% y el nivel de

acciones preventivas mejoró en un 12,2%, mejorando la predicción de ciberataques en el Departamento de Ciberseguridad de la División de Informática DIRTIC PNP, Lima.

CONCLUSIONES

En base a los resultados obtenidos en la presente investigación se concluye lo siguiente:

Primero: Se concluye que el indicador tiempo en realizar la recolección de información de amenazas de la dimensión capacidades de monitoreo para mejorar la predicción de ciberataques en el Departamento de Ciberseguridad de la División de Informática DIRTIC PNP, en el pre-test presenta una estimación de 95,35 y por otro lado en el post-test presenta una estimación de 35,65. Asimismo, en relación a la prueba de U de Mann-Whitney, presenta un nivel de significancia igual a 0,000 siendo menor a 0,05 demostrando que el resultado es significativo y que presentan desigualdades en la implementación de la plataforma de intercambio de información de malware (MISP).

Segundo: Se concluye que el indicador número de intrusos detectados en el sistema de detección de intrusos de la dimensión capacidades defensivas para mejorar la predicción de ciberataques en el Departamento de Ciberseguridad de la División de Informática DIRTIC PNP, en el pre-test presenta una estimación de 33,05 y por otro lado en el post-test presenta una estimación de 97,95. Asimismo, en relación a la prueba de U de Mann-Whitney presenta un nivel de significancia igual a 0,000 siendo menor a 0,05 demostrando que el resultado es significativo y que presentan desigualdades en la implementación de la plataforma de intercambio de información de malware (MISP).

Tercero: Se concluye que el indicador tiempo en realizar la copia de seguridad de la dimensión acciones preventivas para mejorar la predicción de ciberataques en el Departamento de Ciberseguridad de la División de Informática DIRTIC PNP, en el pre-test presenta una estimación de 98,00 y por otro lado en el post-test presenta una estimación de 33,00. Asimismo, en relación a la prueba de U de Mann-Whitney presenta un nivel de significancia igual a 0,000 siendo menor a 0,05 demostrando que el resultado es significativo y que presentan desigualdades en la

implementación de la plataforma de intercambio de información de malware (MISP).

Cuarto: Por último, se concluyó que en relación a la prueba de U de Mann-Whitney, se puede inferir que la predicción de ciberataques basado en los indicadores de las tres dimensiones que la conforman, presentó en cada caso un nivel de significancia igual a 0,000 siendo menor a 0,05 demostrando que es significativo y que presentan desigualdades en la implementación de la plataforma de intercambio de información de malware (MISP). Logrando mejorar los niveles de las capacidades de monitoreo, capacidades defensivas y acciones preventivas del Departamento de Ciberseguridad de la División de Informática DIRTIC PNP.

RECOMENDACIONES

A continuación, se detalla las recomendaciones para futuras investigaciones:

- Primero: Se recomienda a las futuras investigaciones reconocer correctamente la realidad problemática de la institución para lograr implementar cualquier herramienta tecnológica que ayude a mejorar la ciberseguridad.
- Segundo: Dirigido a siguientes estudios que posean semejanza con esta investigación se debe tomar en cuenta los indicadores de las capacidades de monitoreo ya que tiene la finalidad de establecer optimización en la predicción de ciberataques, identificando información fundamental acerca de los tipos, técnicas de ataques cibernéticos, análisis de vulnerabilidades y entidades que fueron vulnerados o posibles atacantes.
- Tercero: Se sugiere para otras investigaciones similares, es recomendable también tomar en cuenta los indicadores de las capacidades defensivas, con la finalidad de mejorar la prevención, protección y resiliencia de los activos de información, que permitirá la solución a los ciberataques que se suscitan en la institución.
- Cuarto: Se sugiere para otras investigaciones similares, es recomendable también tomar en cuenta los indicadores de las acciones preventivas dentro de la institución con la finalidad de llegar a responder de manera eficaz a los ciberataques y así evitar que el ciberataque logre su objetivo en la institución.

REFERENCIAS BIBLIOGRÁFICAS

- [1] Computer Emergency Response Team France (CERT-FR), «Rapports menaces et incidents,» Agence Nationale de la Sécurité des Systèmes d'Information, 2020. [En línea]. Available: <https://cert.ssi.gouv.fr/cti/>. [Último acceso: Marzo 2021].
- [2] INTERPOL, «Aumento alarmante de los ciberataques durante la epidemia de COVID-19,» 2020. [En línea]. Available: <https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19>. [Último acceso: Marzo 2021].
- [3] Kaspersky Security Network (KSN), «Boletín de seguridad Kaspersky 2020. Estadísticas,» 2020. [En línea]. Available: <https://securelist.lat/kaspersky-security-bulletin-2020-statistics/92035/>. [Último acceso: 10 Marzo 2021].
- [4] Centro Nacional para Incidentes Cibernéticos de Rusia (NCIRCC), «Reporte Ciberseguridad,» europapress, 2021. [En línea]. Available: <https://www.europapress.es/internacional/noticia-rusia-denuncia-incremento-ciberataques-sitios-gubernamentales-eeuu-20210427154656.html>. [Último acceso: Marzo 2021].
- [5] FORTINET, «América Latina sufrió más de 41 billones de intentos de ciberataques en 2020,» FortiGuard Labs, 2021. [En línea]. Available: <https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2021/latin-america-suffered-more-than-41-billion-cyberattack-attempts-in-2020>. [Último acceso: Marzo 2021].
- [6] FortiGuard Labs de FORTINET, «Perú sufrió alrededor de 1.3 mil millones de intentos de ciberataques cada hora el 2021,» FortiGuard Labs, 2021. [En línea]. Available: <https://www.fortiguard.com>. [Último acceso: Marzo 2021].
- [7] Centro Nacional de Seguridad Digital (CNSD), «Alerta integrada de seguridad digital del CNSD,» Presidencia del Consejo de Ministros, 2021. [En línea]. Available: <https://www.gob.pe/institucion/pcm/colecciones/791-alerta-integrada-de-seguridad-digital-del-cnsd>. [Último acceso: Marzo 2021].
- [8] Computer Incident Response Center Luxembourg (CIRCL), «MISP - Open Source Threat Intelligence Platform,» Copyright 2008 - 2020 CIRCL Computer Incident Response Center Luxembourg, 2008-2020. [En línea]. Available: <https://www.circl.lu/services/misp-malware-information-sharing-platform/>. [Último acceso: Abril 2021].
- [9] «MISP Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing,» MISP project. Software released under approved open source licenses and content of this website released as CC BY-SA 3.0, [En línea]. Available: <https://www.misp-project.org>. [Último acceso: 2021].
- [10] National Institute of Standards and Technology , «NIST,» U.S. Department of Commerce, 2009. [En línea]. Available: <https://www.nist.gov/cyberframework>. [Último acceso: 2021].
- [11] National Institute of Standards and Technology (NIST), «Cybersecurity Framework version 1.1,» 2018. [En línea]. Available: <https://doi.org/10.6028/NIST.CSWP.04162018>. [Último acceso: Abril 2021].
- [12] H. S. Lallie, L. A. Shepherd, J. R.C. Nurse, A. Erola, G. Epiphaniou, C. Maple, X. Bellekens, «Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic,» *Computers & Security*, vol. 105, nº 102248, 2021.

- [13] M. Kurte, «Implementación y configuración de MISP para compartir información de malware,» CSIRT, Chile, 2020.
- [14] S. Bauer, D. Fischer, C. Sauerwein, S. Latzel, D. Stelzer, R. Breu, «Towards an Evaluation Framework for Threat Intelligence Sharing Platforms,» de *Proceedings of the 53rd Hawaii International Conference on System Sciences*, Hawaii, 2020.
- [15] S. Quiroz, J. Zapata, H. Vargas, «Predicción de ciberataques en sistemas industriales SCADA a través de la implementación del filtro Kalman,» *TecnoL*, vol. 23, nº 48, pp. 249-267, 2020.
- [16] E. Caamaño, R. Gil, «Prevención de riesgos por ciberseguridad desde la auditoría forense: conjugando el talento humano organizacional,» *NOVUM, revista de Ciencias Sociales Aplicadas*, vol. I, nº 10, pp. 61-80, 2020.
- [17] M. Gutierrez, «Diseño de un Entorno Open Source para Análisis Automatizados de Malware,» Trabajo Fin de Grado Inédito, Universidad de Sevilla, Sevilla, 2019.
- [18] A. Pala, J. Zhuang, «Information Sharing in Cybersecurity: A Review,» *Decision Analysis*, vol. 16, nº 3, pp. 172-196, 2019.
- [19] B. Murat, T. Cihan, «Küçük ve Orta Büyüklükteki İşletmelerde Bilgi Güvenliği (Information Security in Small And Medium Size Companies),» *Third Sector Social Economic Review; Ankara*, vol. 54, nº 1, pp. 478-501, 2019.
- [20] A. Retnowardhani, R. Diputra, Y. Sudarya, «Security risk analysis of bring your own device (BYOD) system in manufacturing company at Tangerang,» *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 17, nº 2, pp. 753-762, 2019.
- [21] M. Rego, P. Perez, «El intercambio de información de ciberamenazas,» *Cuadernos de estrategia*, nº 185, pp. 139-170, 2017.
- [22] A. Vaca, «Incidencia de la inteligencia de negocios en la ciberseguridad, con aplicación en las políticas nacionales, caso Ecuador,» Universidad de las Fuerzas Armadas ESPE. Maestría en Gestión de Sistemas de Información e Inteligencia de Negocios., Ecuador, 2017.
- [23] C. Wagner, A. Dulaunoy, G. Wagener, A. Iklody, «MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform,» *In Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security (WISCS '16)*, pp. 49-56, 2016.
- [24] C. Cáceda, «Modelo dinámico para la gestión de seguridad de la infraestructura de las tecnologías de información y comunicación,» Tesis para optar el título de Ingeniero de Sistemas. Escuela Profesional de Ingeniería de Sistemas, Facultad de Ingeniería de Sistemas, Universidad Nacional Mayor de San Marcos, Lima, Perú, 2021.
- [25] M. Frayssinet, D. Esenarro, F. Juárez, M. Díaz, «Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations,» *3C TIC. Cuadernos de desarrollo aplicados a las TIC*, vol. 10, nº 2, pp. 123-141, 2021.
- [26] F. Arrieta, «Capacidades del Ejército del Perú para afrontar las nuevas amenazas contra la seguridad nacional,» *Revista De Ciencia E Investigación En Defensa - CAEN*, vol. 1, nº 4, pp. 7-22, 2020.
- [27] D. Taipe, «Sistema de Seguridad Cibernética Nacional frente a los ciberataques como amenaza a la seguridad nacional,» *Revista De Ciencia E Investigación En Defensa - CAEN*, vol. 1, nº 2, pp. 43-48, 2020.

- [28] R. Villayzan, J. Gutierrez, «Modelo de identificación de ciberamenazas para PYMES de servicios tecnológicos usando herramientas de Data Analytics,» Universidad Peruana de Ciencias Aplicadas (UPC), Lima, Perú, 2020.
- [29] J. Izquierdo, T. Tafur, «Mecanismos de seguridad para contrarrestar ataques informáticos en servidores web y base de datos,» Universidad Señor de Sipán (Escuela de Ingeniería de Sistemas), Pimentel, Perú, 2017.
- [30] A. Inoguchi, E. Macha, «Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las PYMES del Perú, 2016,» Universidad San Ignacio de Loyola, Lima, Perú, 2017.
- [31] A. Bernal, U. Varea, «Diseño de un aplicativo de software orientado a la identificación de incidencias de malware basado en mapas auto-organizados,» Universidad Peruana de Ciencias Aplicadas (UPC), Lima, Perú, 2015.
- [32] C. Angarita, C. Guzmán, «Protocolos para la mitigación de ciberataques en el hogar. Caso de estudio: estratos 3 y 4 de la ciudad de Bogotá,» Universidad Católica de Colombia - RIUCaC , Bogotá, Colombia, 2017.
- [33] L. Aguilar, «Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0),» *Cuadernos de estrategia*, nº 185, pp. 19-64, 2017.
- [34] A. Villalba, J. Corchado, «Análisis de las ciberamenazas,» *Cuadernos de estrategia*, nº 185, pp. 97-138, 2017.
- [35] M. Guanipa, Reflexiones Básicas sobre Investigación, vol. 26, Maracaibo, Venezuela: Universidad Privada Dr. Rafael Beloso Chacín, 2010, pp. 183-195.
- [36] W. Murillo, «La investigación científica,» 2008. [En línea]. Available: <https://www.monografias.com/trabajos15/invest-cientifica/invest-cientifica>. [Último acceso: 2021].
- [37] D. Chawla, N. Sondhi, Research Methodology, Vikas Publishing, 2011.
- [38] F. Kerlinger, Enfoque conceptual de la investigación del comportamiento, México: Nueva Editorial Interamericana. Actualmente se publica por McGraw—Hill Interamericana, 1979.
- [39] M. Tamayo y Tamayo, El proceso de la investigación científica, México: Limusa, 2000.
- [40] J. L. Arias, Técnicas e instrumentos de investigación científica, Arequipa, Perú: Enfoques Consulting EIRL, 2020.
- [41] G. Fulcher, F. Davidson, Language Testing and Assessment, London and New York: Routledge, 2007.
- [42] J. Muñiz, «LAS TEORÍAS DE LOS TESTS: TEORÍA CLÁSICA Y TEORÍA DE RESPUESTA A LOS ÍTEMS,» *Papeles del Psicólogo*, vol. 31, nº 1, pp. 57-66, 2010.
- [43] H. Ñaupas Paitán, Metodología de la investigación cuantitativa-cualitativa y redacción de la tesis - 4ta. Edición, Bogotá: Ediciones de la U, 2014.
- [44] F. Freire, «Plan de contingencia ante ciberataques,» Tesis de Postgrado de la la Facultad de Ingeniería Eléctrica y Computación, Guayaquil, Ecuador, 2017.

ANEXOS

Anexo 1: Matriz de consistencia

**TABLA XXXVIII
MATRIZ DE CONSISTENCIA**

Implementación de la plataforma de intercambio de información de malware para la predicción de ciberataques del Departamento de Ciberseguridad, Lima						
Problema General	Objetivo General	Hipótesis General	Variable	Dimensiones	Indicadores	Metodología
¿De qué manera la implementación de la plataforma de intercambio de información de malware mejora la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP?	Determinar de qué manera la implementación de la plataforma de intercambio de información de malware mejora la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP.	La implementación de la plataforma de intercambio de información de malware mejora significativamente la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP.	Implementación de la plataforma de intercambio de información de malware	Control de ciberataques	Ciberataques identificados	Enfoque: Cuantitativo
				Respuesta ante ciberataques	Alertas	Método Hipotético: Deductivo Tipo de Investigación: Aplicada
				Intercambio de información	Recopilación de información	Diseño de la Investigación: Experimental Corte Longitudinal: Pre-test y Post-test Población: 1 registro por día desde mayo a julio para el pre test y desde agosto a octubre para el post test, haciendo 65 registros para cada periodo de evaluación.

Problema Específico	Objetivo Específico	Hipótesis Específico	Variable	Dimensiones	Indicadores	
¿Como la implementación de la plataforma de intercambio de información de malware mejora las capacidades de monitoreo para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP?	Definir en qué medida la implementación de la plataforma de intercambio de información de malware mejora las capacidades de monitoreo para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP.	La implementación de la plataforma de intercambio de información de malware mejora significativamente las capacidades de monitoreo para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP.		Capacidades de monitoreo	Tiempo en realizar la recolección de información de amenazas	Instrumento: Ficha de observación
¿En qué medida la implementación de la plataforma de intercambio de información de malware mejora las capacidades defensivas para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP?	Describir en qué medida la implementación de la plataforma de intercambio de información de malware mejora las capacidades defensivas para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP.	La implementación de la plataforma de intercambio de información de malware mejora significativamente las capacidades defensivas para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP.	Predicción de ciberataques	Capacidades defensivas	Número de intrusos detectados en el sistema de detección de intrusos	Estadística Descriptiva: Tablas y figuras
¿En qué medida la implementación de la plataforma de intercambio de información de malware mejora las acciones preventivas para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP?	Describir en qué medida la implementación de la plataforma de intercambio de información de malware mejora las acciones preventivas para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP.	La implementación de la plataforma de intercambio de información de malware mejora significativamente las acciones preventivas para la predicción de ciberataques del Departamento de Ciberseguridad de la División de Informática de la DIRTIC PNP.		Acciones preventivas	Tiempo en realizar la copia de seguridad	Estadística Diferencial: Prueba de Kolmogórov-Smirnov y U de Mann-Whitney

Fuente: Elaboración propia.

Anexo 2: Matriz de operacionalización de las variables

TABLA XXXIX
MATRIZ DE OPERACIONALIZACIÓN DE VARIABLE DEPENDIENTE: PREDICCIÓN DE CIBERATAQUES

Variable de estudio	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Descripción	Instrumento
Predicción de ciberataques	Vinculado al concepto, [15] afirma que predecir un ciberataque es obtener datos actuales y aplicar las distintas medidas de protección, con la finalidad de obtener un aproximado de lo que puede suceder. Es muy potente entregar conocimientos, a la hora de tomar decisiones y es un aporte inmenso, ya que permite descubrir patrones que no están a la vista del ojo humano.	La predicción de ciberataques inicia con las capacidades de monitoreo, luego con las capacidades defensivas y cierra con las acciones preventivas.	Capacidades de monitoreo	Tiempo en realizar la recolección de información de amenazas	Punto de vista sistemático de agrupar y medir información de distintas fuentes a fin de obtener una vista completa y precisa de un objetivo.	Ficha de Registro
			Capacidades defensivas	Número de intrusos detectados en el sistema de detección de intrusos	Permite la identificación de posibles ataques informáticos, analizando el historial de uso de las redes, servicios y aplicaciones informáticas de acceso restringido o historial fraudulento	Ficha de Registro
			Acciones preventivas	Tiempo en realizar la copia de seguridad	Es un factor clave para prevenir los ciberataques, es fundamental que se realice copia a toda la información o los datos que se almacenan dentro de los sistemas	Ficha de Registro

Fuente: Elaboración propia.

Anexo 3: Matriz de operacionalización del instrumento

**TABLA XL
MATRIZ DE OPERACIONALIZACIÓN DEL INSTRUMENTO**

Variable de estudio	Dimensiones	Indicadores	Ítem o Reactivo	Escala Valorativa	Instrumento
	Capacidades de monitoreo	Tiempo en realizar la recolección de información de amenazas	Tiempo en días	Tiempo	- Observación - Ficha de registro
Predicción de ciberataques	Capacidades defensivas	Número de intrusos detectados en el sistema de detección de intrusos	Número de intrusos	Cantidad	- Observación - Ficha de registro
	Acciones preventivas	Tiempo en realizar la copia de seguridad	Tiempo en días	Tiempo	- Observación - Ficha de registro

Fuente: Elaboración propia.

Anexo 4: Instrumento de investigación

FICHA DE REGISTRO				
Investigador	Danny Steph Ibarra Rojas			
Lugar de Investigación	Departamento de Ciberseguridad, Lima.			
Indicador	TAV: Tiempo en realizar la recolección de información de amenazas (antes y después de la plataforma)			
Tiempo en realizar la recolección de información de amenazas (antes y después de la plataforma) (TRIA)				
Tiempo en realizar la recolección de información de amenazas - Pre-test (TRIAA)			$TRIA = \frac{TRIAA}{TRIID}$	
Tiempo en realizar la recolección de información de amenazas - Post-test (TRIID)				
N°	TIPO DE PRUEBA			
	FECHA	PRE-TEST TIEMPO EN REALIZAR LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS	FECHA	POST-TEST TIEMPO EN REALIZAR LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS
1	LUNES 03 - MAYO	6 Horas	LUNES 02 - AGOSTO	4 Horas
2	MARTES 04 - MAYO	5 Horas	MARTES 03 - AGOSTO	3 Horas
3	MIERCOLES 05 - MAYO	7 Horas	MIERCOLES 04 - AGOSTO	5 Horas
4	JUEVES 06 - MAYO	5 Horas	JUEVES 05 - AGOSTO	3 Horas
5	VIERNES 07 - MAYO	6 Horas	VIERNES 06 - AGOSTO	4 Horas
6	LUNES 10 - MAYO	5 Horas	LUNES 09 - AGOSTO	3 Horas
7	MARTES 11 - MAYO	7 Horas	MARTES 10 - AGOSTO	5 Horas
8	MIERCOLES 12 - MAYO	5 Horas	MIERCOLES 11 - AGOSTO	3 Horas
9	JUEVES 13 - MAYO	7 Horas	JUEVES 12 - AGOSTO	5 Horas
10	VIERNES 14 - MAYO	7 Horas	VIERNES 13 - AGOSTO	5 Horas
11	LUNES 17 - MAYO	7 Horas	LUNES 16 - AGOSTO	5 Horas
12	MARTES 18 - MAYO	6 Horas	MARTES 17 - AGOSTO	4 Horas
13	MIERCOLES 19 - MAYO	5 Horas	MIERCOLES 18 - AGOSTO	3 Horas
14	JUEVES 20 - MAYO	6 Horas	JUEVES 19 - AGOSTO	4 Horas
15	VIERNES 21 - MAYO	6 Horas	VIERNES 20 - AGOSTO	4 Horas
16	LUNES 24 - MAYO	5 Horas	LUNES 23 - AGOSTO	3 Horas
17	MARTES 25 - MAYO	6 Horas	MARTES 24 - AGOSTO	4 Horas
18	MIERCOLES 26 - MAYO	7 Horas	MIERCOLES 25 - AGOSTO	5 Horas
19	JUEVES 27 - MAYO	6 Horas	JUEVES 26 - AGOSTO	4 Horas
20	VIERNES 28 - MAYO	7 Horas	VIERNES 27 - AGOSTO	5 Horas
21	LUNES 31 - MAYO	5 Horas	LUNES 30 - AGOSTO	3 Horas
22	MARTES 01 - JUNIO	6 Horas	MARTES 31 - AGOSTO	4 Horas
23	MIERCOLES 02 - JUNIO	7 Horas	MIERCOLES 01 - SETIEMBRE	5 Horas
24	JUEVES 03 - JUNIO	7 Horas	JUEVES 02 - SETIEMBRE	5 Horas
25	VIERNES 04 - JUNIO	6 Horas	VIERNES 03 - SETIEMBRE	4 Horas
26	LUNES 07 - JUNIO	7 Horas	LUNES 06 - SETIEMBRE	5 Horas
27	MARTES 08 - JUNIO	6 Horas	MARTES 07 - SETIEMBRE	4 Horas
28	MIERCOLES 09 - JUNIO	7 Horas	MIERCOLES 08 - SETIEMBRE	5 Horas
29	JUEVES 10 - JUNIO	6 Horas	JUEVES 09 - SETIEMBRE	4 Horas
30	VIERNES 11 - JUNIO	6 Horas	VIERNES 10 - SETIEMBRE	4 Horas
31	LUNES 14 - JUNIO	6 Horas	LUNES 13 - SETIEMBRE	4 Horas
32	MARTES 15 - JUNIO	6 Horas	MARTES 14 - SETIEMBRE	4 Horas
33	MIERCOLES 16 - JUNIO	7 Horas	MIERCOLES 15 - SETIEMBRE	5 Horas
34	JUEVES 17 - JUNIO	7 Horas	JUEVES 16 - SETIEMBRE	5 Horas
35	VIERNES 18 - JUNIO	7 Horas	VIERNES 17 - SETIEMBRE	5 Horas
36	LUNES 21 - JUNIO	6 Horas	LUNES 20 - SETIEMBRE	4 Horas
37	MARTES 22 - JUNIO	7 Horas	MARTES 21 - SETIEMBRE	5 Horas
38	MIERCOLES 23 - JUNIO	6 Horas	MIERCOLES 22 - SETIEMBRE	4 Horas
39	JUEVES 24 - JUNIO	7 Horas	JUEVES 23 - SETIEMBRE	5 Horas
40	VIERNES 25 - JUNIO	5 Horas	VIERNES 24 - SETIEMBRE	3 Horas
41	LUNES 28 - JUNIO	5 Horas	LUNES 27 - SETIEMBRE	3 Horas
42	MARTES 29 - JUNIO	5 Horas	MARTES 28 - SETIEMBRE	3 Horas
43	MIERCOLES 30 - JUNIO	6 Horas	MIERCOLES 29 - SETIEMBRE	4 Horas
44	JUEVES 01 - JULIO	7 Horas	JUEVES 30 - SETIEMBRE	5 Horas
45	VIERNES 02 - JULIO	5 Horas	VIERNES 01 - OCTUBRE	3 Horas
46	LUNES 05 - JULIO	6 Horas	LUNES 04 - OCTUBRE	4 Horas
47	MARTES 06 - JULIO	5 Horas	MARTES 05 - OCTUBRE	3 Horas
48	MIERCOLES 07 - JULIO	5 Horas	MIERCOLES 06 - OCTUBRE	3 Horas
49	JUEVES 08 - JULIO	7 Horas	JUEVES 07 - OCTUBRE	5 Horas
50	VIERNES 09 - JULIO	5 Horas	VIERNES 08 - OCTUBRE	3 Horas
51	LUNES 12 - JULIO	6 Horas	LUNES 11 - OCTUBRE	4 Horas
52	MARTES 13 - JULIO	6 Horas	MARTES 12 - OCTUBRE	4 Horas
53	MIERCOLES 14 - JULIO	6 Horas	MIERCOLES 13 - OCTUBRE	4 Horas
54	JUEVES 15 - JULIO	6 Horas	JUEVES 14 - OCTUBRE	4 Horas
55	VIERNES 16 - JULIO	5 Horas	VIERNES 15 - OCTUBRE	3 Horas
56	LUNES 19 - JULIO	7 Horas	LUNES 18 - OCTUBRE	5 Horas
57	MARTES 20 - JULIO	7 Horas	MARTES 19 - OCTUBRE	5 Horas
58	MIERCOLES 21 - JULIO	7 Horas	MIERCOLES 20 - OCTUBRE	5 Horas
59	JUEVES 22 - JULIO	6 Horas	JUEVES 21 - OCTUBRE	4 Horas
60	VIERNES 23 - JULIO	6 Horas	VIERNES 22 - OCTUBRE	4 Horas
61	LUNES 26 - JULIO	6 Horas	LUNES 25 - OCTUBRE	4 Horas
62	MARTES 27 - JULIO	7 Horas	MARTES 26 - OCTUBRE	5 Horas
63	MIERCOLES 28 - JULIO	7 Horas	MIERCOLES 27 - OCTUBRE	5 Horas
64	JUEVES 29 - JULIO	6 Horas	JUEVES 28 - OCTUBRE	4 Horas
65	VIERNES 30 - JULIO	6 Horas	VIERNES 29 - OCTUBRE	4 Horas

Observaciones:




Elaborado por: Danny Steph Ibarra Rojas Bach. Ingeniería de Sistemas	Revisado por: Dra. Karín Corina Rojas Romero R. CIP: 110497	Aprobado por: José Antonio Ventura Rueda Jefe del Departamento de Ciberseguridad
		
	Dra. Karín C. Rojas Romero ING. COM. Y SISTEMAS R. CIP. 110497	José Antonio VENTURA RUEDA CAPITÁN S PNP JEFE DEL DPTO DE CIBERSEGURIDAD DIRTIC PNP

Fig. 43. Ficha de registro Tiempo en realizar la recolección de información de amenazas.




FICHA DE REGISTRO				
Investigador	Danny Steph Ibarra Rojas			
Lugar de Investigación	Departamento de Ciberseguridad, Lima.			
Indicador	NID: Número de intrusos detectados en el sistema de detección de intrusos (antes y después de la plataforma)			
Número de intrusos detectados en el sistema de detección de intrusos (antes y después de la plataforma) (NID)				
Número de intrusos detectados en el sistema de detección de intrusos - Pre-test (NIDA)			$NID = \frac{NIDA}{NIDD}$	
Número de intrusos detectados en el sistema de detección de intrusos - Post-test (NIDD)				
N°	TIPO DE PRUEBA			
	FECHA	PRE-TEST NÚMERO DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS	FECHA	POST-TEST NÚMERO DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS
1	LUNES 03 - MAYO	80	LUNES 02 - AGOSTO	100
2	MARTES 04 - MAYO	86	MARTES 03 - AGOSTO	106
3	MIÉRCOLES 05 - MAYO	87	MIÉRCOLES 04 - AGOSTO	107
4	JUEVES 06 - MAYO	88	JUEVES 05 - AGOSTO	108
5	VIERNES 07 - MAYO	98	VIERNES 06 - AGOSTO	118
6	LUNES 10 - MAYO	99	LUNES 09 - AGOSTO	119
7	MARTES 11 - MAYO	90	MARTES 10 - AGOSTO	110
8	MIÉRCOLES 12 - MAYO	87	MIÉRCOLES 11 - AGOSTO	107
9	JUEVES 13 - MAYO	83	JUEVES 12 - AGOSTO	103
10	VIERNES 14 - MAYO	84	VIERNES 13 - AGOSTO	104
11	LUNES 17 - MAYO	81	LUNES 16 - AGOSTO	101
12	MARTES 18 - MAYO	89	MARTES 17 - AGOSTO	109
13	MIÉRCOLES 19 - MAYO	95	MIÉRCOLES 18 - AGOSTO	115
14	JUEVES 20 - MAYO	96	JUEVES 19 - AGOSTO	116
15	VIERNES 21 - MAYO	93	VIERNES 20 - AGOSTO	113
16	LUNES 24 - MAYO	87	LUNES 23 - AGOSTO	107
17	MARTES 25 - MAYO	84	MARTES 24 - AGOSTO	104
18	MIÉRCOLES 26 - MAYO	93	MIÉRCOLES 25 - AGOSTO	113
19	JUEVES 27 - MAYO	98	JUEVES 26 - AGOSTO	118
20	VIERNES 28 - MAYO	100	VIERNES 27 - AGOSTO	120
21	LUNES 31 - MAYO	99	LUNES 30 - AGOSTO	119
22	MARTES 01 - JUNIO	100	MARTES 31 - AGOSTO	120
23	MIÉRCOLES 02 - JUNIO	98	MIÉRCOLES 01 - SETIEMBRE	118
24	JUEVES 03 - JUNIO	99	JUEVES 02 - SETIEMBRE	119
25	VIERNES 04 - JUNIO	98	VIERNES 03 - SETIEMBRE	118
26	LUNES 07 - JUNIO	96	LUNES 06 - SETIEMBRE	109
27	MARTES 08 - JUNIO	87	MARTES 07 - SETIEMBRE	107
28	MIÉRCOLES 09 - JUNIO	87	MIÉRCOLES 08 - SETIEMBRE	107
29	JUEVES 10 - JUNIO	84	JUEVES 09 - SETIEMBRE	104
30	VIERNES 11 - JUNIO	89	VIERNES 10 - SETIEMBRE	109
31	LUNES 14 - JUNIO	90	LUNES 13 - SETIEMBRE	110
32	MARTES 15 - JUNIO	100	MARTES 14 - SETIEMBRE	120
33	MIÉRCOLES 16 - JUNIO	90	MIÉRCOLES 15 - SETIEMBRE	110
34	JUEVES 17 - JUNIO	81	JUEVES 16 - SETIEMBRE	101
35	VIERNES 18 - JUNIO	82	VIERNES 17 - SETIEMBRE	102
36	LUNES 21 - JUNIO	85	LUNES 20 - SETIEMBRE	105
37	MARTES 22 - JUNIO	89	MARTES 21 - SETIEMBRE	109
38	MIÉRCOLES 23 - JUNIO	87	MIÉRCOLES 22 - SETIEMBRE	107
39	JUEVES 24 - JUNIO	87	JUEVES 23 - SETIEMBRE	107
40	VIERNES 25 - JUNIO	88	VIERNES 24 - SETIEMBRE	108
41	LUNES 28 - JUNIO	88	LUNES 27 - SETIEMBRE	108
42	MARTES 29 - JUNIO	86	MARTES 28 - SETIEMBRE	106
43	MIÉRCOLES 30 - JUNIO	94	MIÉRCOLES 29 - SETIEMBRE	114
44	JUEVES 01 - JULIO	95	JUEVES 30 - SETIEMBRE	115
45	VIERNES 02 - JULIO	97	VIERNES 01 - OCTUBRE	117
46	LUNES 05 - JULIO	98	LUNES 04 - OCTUBRE	118
47	MARTES 06 - JULIO	91	MARTES 05 - OCTUBRE	111
48	MIÉRCOLES 07 - JULIO	90	MIÉRCOLES 06 - OCTUBRE	110
49	JUEVES 08 - JULIO	99	JUEVES 07 - OCTUBRE	119
50	VIERNES 09 - JULIO	100	VIERNES 08 - OCTUBRE	120
51	LUNES 12 - JULIO	100	LUNES 11 - OCTUBRE	120
52	MARTES 13 - JULIO	100	MARTES 12 - OCTUBRE	120
53	MIÉRCOLES 14 - JULIO	84	MIÉRCOLES 13 - OCTUBRE	104
54	JUEVES 15 - JULIO	84	JUEVES 14 - OCTUBRE	104
55	VIERNES 16 - JULIO	83	VIERNES 15 - OCTUBRE	103
56	LUNES 19 - JULIO	89	LUNES 18 - OCTUBRE	109
57	MARTES 20 - JULIO	00	MARTES 19 - OCTUBRE	100
58	MIÉRCOLES 21 - JULIO	81	MIÉRCOLES 20 - OCTUBRE	101
59	JUEVES 22 - JULIO	92	JUEVES 21 - OCTUBRE	112
60	VIERNES 23 - JULIO	94	VIERNES 22 - OCTUBRE	114
61	LUNES 26 - JULIO	95	LUNES 25 - OCTUBRE	115
62	MARTES 27 - JULIO	99	MARTES 26 - OCTUBRE	119
63	MIÉRCOLES 28 - JULIO	99	MIÉRCOLES 27 - OCTUBRE	119
64	JUEVES 29 - JULIO	100	JUEVES 28 - OCTUBRE	120
65	VIERNES 30 - JULIO	98	VIERNES 29 - OCTUBRE	118
Observaciones:				
Elaborado por: Danny Steph Ibarra Rojas Bach. Ingeniería de Sistemas				
Revisado por: Dra. Karin Corina Rojas Romero R. CIP: 110497				
Aprobado por: José Antonio Ventura Rueda Jefe del Departamento de Ciberseguridad				
  				
José Antonio VENTURA RUEDA CAPITÁN S PNP JEFE DEL DPTO DE CIBERSEGURIDAD DIRTIC FNP				

Fig. 44. Ficha de registro Número de intrusos detectados en el sistema de detección de intrusos.





FICHA DE REGISTRO				
Investigador	Danny Steph Ibarra Rojas			
Lugar de Investigación	Departamento de Ciberseguridad, Lima.			
Indicador	TCS: Tiempo en realizar la copia de seguridad (antes y después de la plataforma)			
Tiempo en realizar la copia de seguridad (antes y después de la plataforma) (TCS)				
Tiempo en realizar la copia de seguridad - Pre-test (TCSA)			$TCS = \frac{TCSA}{TCSD}$	
Tiempo en realizar la copia de seguridad - Post-test (TCSD)				
N°	SEMANA	TIPO DE PRUEBA		
		PRE-TEST	SEMANA	POST-TEST
		TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD		TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD
1	LUNES 03 - MAYO	6 Horas	LUNES 02 - AGOSTO	3 Horas
2	MARTES 04 - MAYO	7 Horas	MARTES 03 - AGOSTO	4 Horas
3	MIÉRCOLES 05 - MAYO	5 Horas	MIÉRCOLES 04 - AGOSTO	3 Horas
4	JUEVES 06 - MAYO	7 Horas	JUEVES 05 - AGOSTO	4 Horas
5	VIERNES 07 - MAYO	6 Horas	VIERNES 06 - AGOSTO	3 Horas
6	LUNES 10 - MAYO	7 Horas	LUNES 09 - AGOSTO	4 Horas
7	MARTES 11 - MAYO	5 Horas	MARTES 10 - AGOSTO	3 Horas
8	MIÉRCOLES 12 - MAYO	5 Horas	MIÉRCOLES 11 - AGOSTO	3 Horas
9	JUEVES 13 - MAYO	5 Horas	JUEVES 12 - AGOSTO	3 Horas
10	VIERNES 14 - MAYO	5 Horas	VIERNES 13 - AGOSTO	3 Horas
11	LUNES 17 - MAYO	5 Horas	LUNES 16 - AGOSTO	3 Horas
12	MARTES 18 - MAYO	6 Horas	MARTES 17 - AGOSTO	3 Horas
13	MIÉRCOLES 19 - MAYO	7 Horas	MIÉRCOLES 18 - AGOSTO	4 Horas
14	JUEVES 20 - MAYO	6 Horas	JUEVES 19 - AGOSTO	3 Horas
15	VIERNES 21 - MAYO	6 Horas	VIERNES 20 - AGOSTO	3 Horas
16	LUNES 24 - MAYO	7 Horas	LUNES 23 - AGOSTO	3 Horas
17	MARTES 25 - MAYO	6 Horas	MARTES 24 - AGOSTO	3 Horas
18	MIÉRCOLES 26 - MAYO	5 Horas	MIÉRCOLES 25 - AGOSTO	3 Horas
19	JUEVES 27 - MAYO	6 Horas	JUEVES 26 - AGOSTO	3 Horas
20	VIERNES 28 - MAYO	5 Horas	VIERNES 27 - AGOSTO	3 Horas
21	LUNES 31 - MAYO	5 Horas	LUNES 30 - AGOSTO	3 Horas
22	MARTES 01 - JUNIO	6 Horas	MARTES 31 - AGOSTO	3 Horas
23	MIÉRCOLES 02 - JUNIO	5 Horas	MIÉRCOLES 01 - SETIEMBRE	3 Horas
24	JUEVES 03 - JUNIO	5 Horas	JUEVES 02 - SETIEMBRE	3 Horas
25	VIERNES 04 - JUNIO	6 Horas	VIERNES 03 - SETIEMBRE	3 Horas
26	LUNES 07 - JUNIO	5 Horas	LUNES 06 - SETIEMBRE	3 Horas
27	MARTES 08 - JUNIO	6 Horas	MARTES 07 - SETIEMBRE	3 Horas
28	MIÉRCOLES 09 - JUNIO	5 Horas	MIÉRCOLES 08 - SETIEMBRE	3 Horas
29	JUEVES 10 - JUNIO	6 Horas	JUEVES 09 - SETIEMBRE	3 Horas
30	VIERNES 11 - JUNIO	6 Horas	VIERNES 10 - SETIEMBRE	3 Horas
31	LUNES 14 - JUNIO	6 Horas	LUNES 13 - SETIEMBRE	3 Horas
32	MARTES 15 - JUNIO	6 Horas	MARTES 14 - SETIEMBRE	3 Horas
33	MIÉRCOLES 16 - JUNIO	5 Horas	MIÉRCOLES 15 - SETIEMBRE	3 Horas
34	JUEVES 17 - JUNIO	5 Horas	JUEVES 16 - SETIEMBRE	3 Horas
35	VIERNES 18 - JUNIO	5 Horas	VIERNES 17 - SETIEMBRE	3 Horas
36	LUNES 21 - JUNIO	6 Horas	LUNES 20 - SETIEMBRE	3 Horas
37	MARTES 22 - JUNIO	5 Horas	MARTES 21 - SETIEMBRE	3 Horas
38	MIÉRCOLES 23 - JUNIO	6 Horas	MIÉRCOLES 22 - SETIEMBRE	3 Horas
39	JUEVES 24 - JUNIO	5 Horas	JUEVES 23 - SETIEMBRE	3 Horas
40	VIERNES 25 - JUNIO	7 Horas	VIERNES 24 - SETIEMBRE	4 Horas
41	LUNES 28 - JUNIO	7 Horas	LUNES 27 - SETIEMBRE	4 Horas
42	MARTES 29 - JUNIO	7 Horas	MARTES 28 - SETIEMBRE	4 Horas
43	MIÉRCOLES 30 - JUNIO	6 Horas	MIÉRCOLES 29 - SETIEMBRE	3 Horas
44	JUEVES 01 - JULIO	5 Horas	JUEVES 30 - SETIEMBRE	3 Horas
45	VIERNES 02 - JULIO	7 Horas	VIERNES 01 - OCTUBRE	4 Horas
46	LUNES 05 - JULIO	6 Horas	LUNES 04 - OCTUBRE	3 Horas
47	MARTES 06 - JULIO	7 Horas	MARTES 05 - OCTUBRE	4 Horas
48	MIÉRCOLES 07 - JULIO	7 Horas	MIÉRCOLES 06 - OCTUBRE	4 Horas
49	JUEVES 08 - JULIO	5 Horas	JUEVES 07 - OCTUBRE	3 Horas
50	VIERNES 09 - JULIO	7 Horas	VIERNES 08 - OCTUBRE	4 Horas
51	LUNES 12 - JULIO	6 Horas	LUNES 11 - OCTUBRE	3 Horas
52	MARTES 13 - JULIO	6 Horas	MARTES 12 - OCTUBRE	3 Horas
53	MIÉRCOLES 14 - JULIO	6 Horas	MIÉRCOLES 13 - OCTUBRE	3 Horas
54	JUEVES 15 - JULIO	6 Horas	JUEVES 14 - OCTUBRE	3 Horas
55	VIERNES 16 - JULIO	7 Horas	VIERNES 15 - OCTUBRE	4 Horas
56	LUNES 19 - JULIO	5 Horas	LUNES 18 - OCTUBRE	3 Horas
57	MARTES 20 - JULIO	5 Horas	MARTES 19 - OCTUBRE	3 Horas
58	MIÉRCOLES 21 - JULIO	5 Horas	MIÉRCOLES 20 - OCTUBRE	3 Horas
59	JUEVES 22 - JULIO	6 Horas	JUEVES 21 - OCTUBRE	3 Horas
60	VIERNES 23 - JULIO	6 Horas	VIERNES 22 - OCTUBRE	3 Horas
61	LUNES 26 - JULIO	6 Horas	LUNES 25 - OCTUBRE	3 Horas
62	MARTES 27 - JULIO	5 Horas	MARTES 26 - OCTUBRE	3 Horas
63	MIÉRCOLES 28 - JULIO	5 Horas	MIÉRCOLES 27 - OCTUBRE	3 Horas
64	JUEVES 29 - JULIO	6 Horas	JUEVES 28 - OCTUBRE	3 Horas
65	VIERNES 30 - JULIO	6 Horas	VIERNES 29 - OCTUBRE	3 Horas
Observaciones:				
Elaborado por :		Revisado por :		Aprobado por :
Danny Steph Ibarra Rojas Bach. Ingeniería de Sistemas		Dra. Karin Corina Rojas Romero R. CIP: 110497		José Antonio Ventura Rueda Jefe del Departamento de Ciberseguridad
				
		Dra. Karin C. Rojas Romero ING. COMP Y SISTEMAS R. CIP. 110497		CS-386042 José Antonio VENTURA RUEDA CAPITAN S PNP JEFE DEL DPTO DE CIBERSEGURIDAD DIRTIC PNP

Fig. 45. Ficha de registro Tiempo en realizar la copia de seguridad.

Anexo 5: Validez del instrumento



Certificado de Validez del Instrumento que mide la Variable Predicción de Ciberataques

N°	DIMENSIONES / ítems		Pertinencia ¹			Relevancia ²			Claridad ³			Sugerencias	
			M	D	A	M	D	A	M	D	A		M
DIMENSIONES / ítems													
Dimensión 1: Capacidades de monitoreo													
TAV: Tiempo en realizar la recolección de información de amenazas (antes y después de la plataforma)													
2	Tiempo en realizar la recolección de información de amenazas – Pre-test (TRIAA)	Pre-test											
		Tiempo en realizar la recolección de información de amenazas		X			X					X	
3		Post-test											
4	Tiempo en realizar la recolección de información de amenazas – Post-test (TRIAD)	Tiempo en realizar la recolección de información de amenazas			X			X				X	
		Post-test											
Dimensión 2: Capacidades defensivas													
NID: Número de intrusos detectados en el sistema de detección de intrusos (antes y después de la plataforma)													
1	Número de intrusos detectados en el sistema de detección de intrusos – Pre-test (NIDA)	Pre-test											
2		Número de intrusos detectados en el sistema de detección de intrusos			X			X				X	
3		Post-test											
4	Número de intrusos detectados en el sistema de detección de intrusos – Post-test (NIDD)	Número de intrusos detectados en el sistema de detección de intrusos			X			X				X	
		Post-test											
Dimensión 3: Acciones preventivas													
TCS: Tiempo en realizar la copia de seguridad (antes y después de la plataforma)													
1	Tiempo en realizar la copia de seguridad – Pre-test (TCSA)	Pre-test											
2		Tiempo en realizar la copia de seguridad			X			X				X	
3		Post-test											
4		Tiempo en realizar la copia de seguridad – Post-test (TCSB)			X			X				X	

Observaciones: Es suficiente para la aplicación.

Opinión de aplicabilidad: Aplicable [X] No aplicable []

Apellidos y nombres del juez validador Dr. / Mg. Mg. Torres Cabanillas, Luis Dr. (C)

Especialidad del validador: Ingeniero Estadístico R. CIP: 49863 COD. ORCID: 0000-0003-2808-7753 DNI: 08404690


Pertinencia¹: El ítem corresponde al concepto teórico formulado.

Relevancia²: El ítem es apropiado para representar al componente o dimensión específica del constructo

Claridad³: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo.

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión.

MD	D	A	MA
Muy Débil	Débil	Aplicable	Muy Aplicable



Firma del Experto Informante
Especialidad

Fig. 46. Certificado de validez Especialidad.



Certificado de Validez del Instrumento que mide la Variable Predicción de Ciberataques

N°	DIMENSIONES / ítems		Pertinencia ¹		Relevancia ²			Claridad ³			Sugerencias		
	M	D	A	M	A	M	D	A	M	D		A	M
Dimensión 1: Capacidades de monitoreo													
TAV: Tiempo en realizar la recolección de información de amenazas (antes y después de la plataforma)													
2		Pre-test											
		Tiempo en realizar la recolección de información de amenazas – Pre-test (TRIAA)			X							X	
3		Post-test											
		Tiempo en realizar la recolección de información de amenazas – Post-test (TRIID)			X							X	
Dimensión 2: Capacidades defensivas													
NID: Número de intrusos detectados en el sistema de detección de intrusos (antes y después de la plataforma)													
1		Pre-test											
		Número de intrusos detectados en el sistema de detección de intrusos – Pre-test (NIDA)			X							X	
3		Post-test											
		Número de intrusos detectados en el sistema de detección de intrusos – Post-test (NIDD)			X							X	
Dimensión 3: Acciones preventivas													
TCS: Tiempo en realizar la copia de seguridad (antes y después de la plataforma)													
1		Pre-test											
		Tiempo en realizar la copia de seguridad – Pre-test (TCSA)			X							X	
3		Post-test											
		Tiempo en realizar la copia de seguridad – Post-test (TCSD)			X							X	

Observaciones: **Es suficiente para la aplicación.**

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [] No aplicable []

Apellidos y nombres del juez validador Dr. / Mg: Rojas Romero Karín
Especialidad del validador: Doctora de Sistemas R. CIP: 110497 COD. ORCID: 0000-0002-6867-0778 DNI: 32645104


 Dra. Karín C. Rojas Romero
 ING. COMP. Y SISTEMAS
 R. CIP. 110497

Pertinencia¹: El ítem corresponde al concepto teórico formulado.
 Relevancia²: El ítem es apropiado para representar al componente o dimensión específica del constructo
 Claridad³: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo.

Firma del Experto Informante
Metodológico

Fig. 47. Certificado de validez Metodológico.

Anexo 6: Data de procesamiento de datos

**TABLA XLI
DATA DE PROCESAMIENTO DE DATOS**

TIEMPO EN REALIZAR LA RECOLECCIÓN DE INFORMACIÓN DE AMENAZAS		NÚMERO DE INTRUSOS DETECTADOS EN EL SISTEMA DE DETECCIÓN DE INTRUSOS		TIEMPO EN REALIZAR LA COPIA DE SEGURIDAD	
Pre test	Post test	Pre test	Post test	Pre test	Post test
6.00	4.00	80.00	100.00	6.00	3.00
5.00	3.00	86.00	106.00	7.00	4.00
7.00	5.00	87.00	107.00	5.00	3.00
5.00	3.00	88.00	108.00	7.00	4.00
6.00	4.00	98.00	118.00	6.00	3.00
5.00	3.00	99.00	119.00	7.00	4.00
7.00	5.00	90.00	110.00	5.00	3.00
5.00	3.00	87.00	107.00	5.00	3.00
7.00	5.00	83.00	103.00	5.00	3.00
7.00	5.00	84.00	104.00	5.00	3.00
7.00	5.00	81.00	101.00	5.00	3.00
6.00	4.00	89.00	109.00	6.00	3.00
5.00	3.00	95.00	115.00	7.00	4.00
6.00	4.00	96.00	116.00	6.00	3.00
6.00	4.00	93.00	113.00	6.00	3.00
5.00	3.00	87.00	107.00	7.00	3.00
6.00	4.00	84.00	104.00	6.00	3.00
7.00	5.00	93.00	113.00	5.00	3.00
6.00	4.00	98.00	118.00	6.00	3.00
7.00	5.00	100.00	120.00	5.00	3.00
5.00	3.00	99.00	119.00	5.00	3.00
6.00	4.00	100.00	120.00	6.00	3.00
7.00	5.00	98.00	118.00	5.00	3.00
7.00	5.00	99.00	119.00	5.00	3.00
6.00	4.00	98.00	118.00	6.00	3.00
7.00	5.00	89.00	109.00	5.00	3.00
6.00	4.00	87.00	107.00	6.00	3.00
7.00	5.00	87.00	107.00	5.00	3.00
6.00	4.00	84.00	104.00	6.00	3.00
6.00	4.00	89.00	109.00	6.00	3.00
6.00	4.00	90.00	110.00	6.00	3.00
6.00	4.00	100.00	120.00	6.00	3.00
7.00	5.00	90.00	110.00	5.00	3.00
7.00	5.00	81.00	101.00	5.00	3.00
7.00	5.00	82.00	102.00	5.00	3.00
6.00	4.00	85.00	105.00	6.00	3.00
7.00	5.00	89.00	109.00	5.00	3.00
6.00	4.00	87.00	107.00	6.00	3.00
7.00	5.00	87.00	107.00	5.00	3.00
5.00	3.00	88.00	108.00	7.00	4.00
5.00	3.00	88.00	108.00	7.00	4.00
5.00	3.00	86.00	106.00	7.00	4.00
6.00	4.00	94.00	114.00	6.00	3.00
7.00	5.00	95.00	115.00	5.00	3.00
5.00	3.00	97.00	117.00	7.00	4.00
6.00	4.00	98.00	118.00	6.00	3.00

5.00	3.00	91.00	111.00	7.00	4.00
5.00	3.00	90.00	110.00	7.00	4.00
7.00	5.00	99.00	119.00	5.00	3.00
5.00	3.00	100.00	120.00	7.00	4.00
6.00	4.00	100.00	120.00	6.00	3.00
6.00	4.00	100.00	120.00	6.00	3.00
6.00	4.00	84.00	104.00	6.00	3.00
6.00	4.00	84.00	104.00	6.00	3.00
5.00	3.00	83.00	103.00	7.00	4.00
7.00	5.00	89.00	109.00	5.00	3.00
7.00	5.00	86.00	106.00	5.00	3.00
7.00	5.00	81.00	101.00	5.00	3.00
6.00	4.00	92.00	112.00	6.00	3.00
6.00	4.00	94.00	114.00	6.00	3.00
6.00	4.00	95.00	115.00	6.00	3.00
7.00	5.00	99.00	119.00	5.00	3.00
7.00	5.00	99.00	119.00	5.00	3.00
6.00	4.00	100.00	120.00	6.00	3.00
6.00	4.00	98.00	118.00	6.00	3.00

Anexo 7: Consentimiento / Carta de aceptación



"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Bicentenario del Perú: 200 años de Independencia"

San Isidro, 01 de febrero de 2021

CARTA DE ACEPTACIÓN

Por medio de la presente tenemos el agrado de dar a conocer que el Sr. Danny Steph Ibarra Rojas, identificado con documento de identidad 70320048, ha sido admitido para realizar el desarrollo del proyecto de investigación "Implementación de la Plataforma de Intercambio de Información de Malware para la predicción de ciberataques" en el Departamento de Ciberseguridad de la División de Informática de la Dirección de Tecnología de la Información y Comunicaciones de la Policía Nacional del Perú, teniendo como fecha de inicio el 01 de febrero del 2021 y como fecha de culminación el 30 de Setiembre del 2021.

Atentamente.

OS-368042
José Antonio VENTURA RUEDA
CAPITAN S PNP
JEFE DEL DPTO DE CIBERSEGURIDAD
DIRTIC PNP

Fig. 48. Carta de aceptación.