UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE ETHICAL HACKING PARA MEJORAR LA GESTIÓN DE RIESGOS INFORMATICOS DE LA CLINICA AMERICANA SERFARMED - PUCALLPA.”

Tesis para optar el título profesional de

INGENIERO DE SISTEMAS

GUILLERMO WILFREDO, TORRES RAMIREZ

Pucallpa - Perú

2022

UNIVERSIDAD NACIONAL DE UCAYALI
FACULTAD DE INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL
ESCUELA PROFESIONAL DE INGENIERÍA CIVIL
COMISIÓN DE GRADOS Y TÍTULOS

ACTA DE EVALUACIÓN DE SUSTENTACIÓN DE TESIS N° 006-2023

GRADUANDO : **Bach. TORRES RAMIREZ, GUILLERMO WILFREDO**

TEMA : **"IMPLEMENTACIÓN DE ETHICAL HACKING PARA MEJORAR LA GESTIÓN DE RIESGOS INFORMÁTICOS DE LA CLÍNICA AMERICANA SERFARMED - PUCALLPA".**

ASESOR : **M.Sc. RONALD HAROLD ULLOA GÁLVEZ**

CRITERIOS	PUNTAJE			
	3	2	1	0
I- PRESENTACION				
* MOTIVACION		X		
* TONO DE VOZ			X	
* CALIDAD DE MATERIAL AUDIOVISUAL		X		
II- DESARROLLO DE CONTENIDO				
* SECUENCIA		X		
* DOMINIO DE VOZ			X	
* USO ADECUADO DEL MATERIAL		X		
* VALIDEZ DE LOS HALLAZGOS		X		
III- ABSOLUCION DE PREGUNTAS				
* RESPONDE A LAS PREGUNTAS FORMULADAS POR EL JURADO		X		
IV- APORTE CIENTIFICO Y TECNOLOGICO				
* AL DESARROLLO DE LA COMUNIDAD		X		
* A LA PROFESION		X		

EVALUACION

- EXCELENCIA — 26 A 30 PUNTOS
- UNANIMIDAD — 21 A 25 PUNTOS
- MAYORIA — 16 A 20 PUNTOS
- DESAPROBADO — 15 A MENOS

CALIFICACION FINAL :
PUNTAJE : **18 / 30**

CONCLUSIONES:
APROBADO POR : MAYORIA
DESAPROBADO POR :

JURADO EVALUADOR

M.Sc. CLOTILDE RÍOS HIDALGO DE CERNA
PRESIDENTE

MG. FREDDY ELAR FERRARI FERNANDEZ
MIEMBRO

M.Sc. EUCLIDES PANDURO PADILLA
MIEMBRO

M.SC. CLOTILDE RÍOS HIDALGO DE CERNA
SECREARIA ACADÉMICA

PUCALLPA, 10 DE ABRIL DEL 2023

"IMPLEMENTACIÓN DE ETHICAL HACKING PARA MEJORAR LA GESTIÓN DE RIESGOS INFORMATICOS DE LA CLINICA AMERICANA SERFARMED - PUCALLPA."

Elaborado por:

Bach. Guillermo Wilfredo Torres Ramirez

Aprobado por:

Ing. Msc. Clotilde Rios Hidalgo De Cerna
Presidente

Ing. Msc. Euclides Panduro Padilla
Miembro

Ing. Mg Freddy Elar Ferrari Fernández
Miembro

Asesor :

Ing. Msc Ronald Harold Ulloa Gálvez
Miembro

UNIVERSIDAD NACIONAL DE UCAYALI

DIRECCION GENERAL DE PROPIEDAD INTELECTUAL

CONSTANCIA

ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN
SISTEMA ANTIPLAGIO URKUND

Nº V/0101-2023.

La Dirección de Producción Intelectual, hace constar por la presente, que el Informe final de tesis, titulado:
"IMPLEMENTACIÓN DE ETHICAL HACKING PARA MEJORAR LA GESTIÓN DE RIESGOS INFORMÁTICOS DE LA CLÍNICA AMERICANA SERFARMED - PUCALLPA"

Autor(es)	:	**TORRES RAMIREZ, GUILLERMO WILFREDO**
Facultad	:	**INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL**
Escuela	:	**ING. SISTEMAS**
Asesor(a)	:	**Mg. ULLOA GÁLVEZ, RONALD HAROLD**

Después de realizado el análisis correspondiente en el Sistema Antiplagio URKUND, dicho documento presenta un **porcentaje de similitud 10%.**

En tal sentido, de acuerdo a los criterios de porcentaje establecidos en el artículo 9 de la DIRECTIVA DE USO DEL SISTEMA ANTIPLAGIO URKUND, el cual indica que no se debe superar el 10%. Se declara, que el trabajo de investigación: SI Contiene un porcentaje aceptable de similitud, por lo que SI se aprueba su originalidad.

En señal de conformidad y verificación se firma y se sella la presente constancia

Fecha: 22/02/2023

Mg. JOSÉ MANUEL CÁRDENAS BERNAOLA
Director de Producción Intelectual

UNIVERSIDAD NACIONAL DE UCAYALI

UByP - REPOSITORIO INSTITUCIONAL

AUTORIZACIÓN DE PUBLICACIÓN DE TESIS

REPOSITORIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI

Yo, GUILLERMO WILFREDO TORRES RAMIREZ

Autor(a) de la TESIS de pregrado titulada:

« IMPLEMENTACIÓN DE ETHICAL HACKING PARA MEJORAR LA GESTIÓN DE RIESGOS INFORMÁTICOS DE LA CLINICA AMERICANA SERFARMED - PUCALLPA »

Sustentada el año: 2023

Con la asesoría de: Ing. MSc. RONALD HAROLD ULLOA GÁLVEZ

En la Facultad de: INGENIERIA DE SISTEMAS E INGENIERIA CIVIL

Escuela Profesional de: INGENIERIA DE SISTEMAS

Autorizo la publicación:

PARCIAL ☐ Significa que se publicará en el repositorio institucional solo La caratula, la dedicatoria y el resumen de la tesis. Esta opción solo es válida marcar **si su tesis o documento presenta material patentable**, para ello deberá presentar el trámite de CATI y/o INDECOPI cuando se lo solicite la DGPI UNU.

TOTAL ☒ Significa que todo el contenido de la tesis y/o documento será publicada en el repositorio institucional

De mi trabajo de investigación en el Repositorio Institucional de la Universidad Nacional de Ucayali (www.repositorio.unu.edu.pe), bajo los siguientes términos:

Primero: Otorgo a la Universidad Nacional de Ucayali **licencia no exclusiva** para reproducir, distribuir, comunicar, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público en general mi tesis (incluido el resumen) a través del Repositorio Institucional de la UNU, en formato digital sin modificar su contenido, en el Perú y en el extranjero; por el tiempoy las veces que considere necesario y libre de remuneraciones.

Segundo: Declaro que la **tesis es una creación de mi autoría** y exclusiva titularidad, por tanto me encuentro facultado a conceder la presente autorización, garantizando que la tesis no infringe derechos de autor de terceras personas, caso contrario, me hago único(a) responsable de investigaciones y observaciones futuras, de acuerdo a lo establecido en el estatuto de la Universidad Nacional de Ucayali, la Superintendencia Nacional de Educación Superior Universitaria y el Ministerio de Educación.

En señal de conformidad firmo la presente autorización.

Fecha: 10 / 04 / 2023

Email: torresguillermo028@gmail.com

Teléfono: 947344066

Firma: 

DNI: 41592215

DEDICATORIA

A mis maestros quienes nunca desistieron al enseñarme, aun sin importar que muchas veces no ponía atención en clase, a ellos que continuaron depositando su esperanza en mí.

AGRADECIMIENTO

A mi familia, por haberme dado la oportunidad de formarme en esta prestigiosa universidad y haber sido mi apoyo durante todo este tiempo

INDICE DE CONTENIDOS

Pag.

ACTA DE SUSTENTACIÓN 2
CONSTANCIA ANTIPLAGIO 4
AUTORIZACION DE PUBLICACION 5
DEDICATORIA 6
AGRADECIMIENTO 7
INDICE DE CONTENIDOS 8
LISTA DE TABLAS 11
LISTA DE FIGURAS 13
RESUMEN 15
ABSTRACT 16
INTRODUCCIÓN 17
CAPÍTULO I 18
PLANTEAMIENTO DEL PROBLEMA 18
1.1. DESCRIPCIÓN Y FUNDAMENTACIÓN DEL PROBLEMA 18
1.2. FORMULACIÓN DEL PROBLEMA 20
1.2.1. Problema General. 20
1.2.2. Problemas Específicos. 20
1.3. OBJETIVOS. 20
1.3.1. Objetivo General. 20
1.3.2. Objetivos Específicos. 20
1.4. JUSTIFICACIÓN, IMPORTANCIA Y LIMITACIONES. 21
1.4.1. JUSTIFICACIÓN. 21
1.4.2. IMPORTANCIA. 21
1.4.3. LIMITACIONES. 22
1.5. HIPÓTESIS 22

1.5.1. Hipótesis General 22
1.5.2. Hipótesis Específica 22
1.6. DELIMITACIONES DE LA INVESTIGACIÓN 22
1.6.1. Delimitación Espacial. 22
1.6.2. Delimitación Social. 23
1.6.3. Delimitación Temporal. 23
1.6.4. Delimitación Conceptual. 23
1.7. VARIABLES 23
1.7.1. Variable independiente: 23
1.7.2. Variable dependiente: 23
1.8. SISTEMA DE VARIABLES, DIMENSIONES E INDICADORES. 24
1.8.1. Operacionalización de las variables 24
CAPÍTULO II....25
MARCO TEÓRICO....25
2.1. ANTECEDENTES DE LA INVESTIGACIÓN 25
2.2. BASES TEÒRICAS 28
2.3. DEFINICIÓN DE TÉRMINOS BÁSICOS. 51
CAPÍTULO III....52
METODOLOGÍA DE LA INVESTIGACIÓN 52
3.1. METOGOLOGÍA Y TÉCNICAS UTILIZADAS 52
3.1.1. Tipo de investigación 52
3.1.2. Nivel de investigación 52
3.1.3. Diseño de la investigación 52
3.2. POBLACIÓN Y MUESTRA 53
3.3. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS. 53
3.4. PROCESAMIENTO DE DATOS 54
3.5. TRATAMIENTO DE LOS DATOS 56
CAPÍTULO IV 57

IMPLEMENTACION DE LA SOLUCIÓN 57
4.1. LA EMPRESA 57
4.2. Ethical Hacking 59
4.3. Fases del Ethical Hacking. (securitcrs, 2020) 61
4.4. Desarrollo de fases. 61
CAPÍTULO V 75
RESULTADOS Y DISCUSIÓN 75
INTERPRETACIÓN DE RESULTADOS PRE TEST 75
INTERPRETACIÓN DE RESULTADOS POST TEST 86
CONCLUSIONES 102
RECOMENDACIONES 103
REFERENCIAS BIBLIOGRÁFICAS 104
ANEXOS 106

LISTA DE TABLAS

Tabla 1. Dimensiones e indicadores de las variables 24
Tabla 2.Correlación entre Etapas del H.E. y Fases OSSTMM 31
Tabla 3.Escala de probabilidad de ocurrencia de una menaza. 47
Tabla 4.Escala del impacto de materialización de un riesgo 48
Tabla 5.Escala de relevancia de un riesgo 48
Tabla 6.Escala de evaluación del riesgo. 48
Tabla 7.Confidencialidad, integridad y Disponibilidad. 60
Tabla 8.Cantidad de Información por tipo 64
Tabla 9.Servicios identificados 64
Tabla 10.Vulnerabilidades encontradas 68
Tabla 11.Gestión de Riesgo 71
Tabla 12.Amenazas y Vulnerabilidades 71
Tabla 13.Escala de evaluación 72
Tabla 14.Riesgos Analizados 73
Tabla 15.Mecanismos de protección. 74
Tabla 16.Análisis de Frecuencia PREG1 75
Tabla 17.Análisis de Frecuencia PREG2 76
Tabla 18.Análisis de Frecuencia PREG3 77
Tabla 19.Análisis de Frecuencia PREG4 78
Tabla 20.Análisis de Frecuencia PREG05 79
Tabla 21.Análisis de Frecuencia PREG6 80
Tabla 22.Análisis de Frecuencia PREG07 81
Tabla 23.Análisis de Frecuencia PREG08 82
Tabla 24.Análisis de Frecuencia PREG09 83
Tabla 25.Análisis de Frecuencia PREG10 84

Tabla 26.Análisis de Frecuencia PREG11 85
Tabla 27.Análisis de Frecuencia PREG01 86
Tabla 28.Análisis de Frecuencia PREG02 87
Tabla 29.Análisis de Frecuencia PREG03 88
Tabla 30.Análisis de Frecuencia PREG04 89
Tabla 31.Análisis de Frecuencia PREG05 90
Tabla 32.Análisis de Frecuencia PREG06 91
Tabla 33.Análisis de Frecuencia PREG07 92
Tabla 34. Análisis de Frecuencia PREG09 94
Tabla 35. Análisis de Frecuencia PREG10 95
Tabla 36.Análisis de Frecuencia PREG11 96
Tabla 37.Calculo del valor crítico y la función de prueba 98
Tabla 38. Comparación del resultado de la aplicación del cuestionario, pre y post test 98
Tabla 39: Coeficiente de Correlación 115
Tabla 40: GUÍA DE OBSERVACIÓN.....116
Tabla 41.RESUMEN DE GUÍA DE OBSERVACIÓN.....116

LISTA DE FIGURAS

Figura 1: Fases OSSTMM 30

Figura 2: Proceso de Gestión de Riesgos 32

Figura 3: Flujograma PDAR 33

Figura 4: Elementos de Escaneo y Enumeración 35

Figura 5: Fases del proyecto 39

Figura 6:. ISO 31000 - Marco de trabajo para la gestión de riesgos 40

Figura 7:. Modelo de madurez 45

Figura 8: Diagrama de metodología Propuesta para prueba de penetración orientada a riesgos 50

Figura 9: Organigrama 58

Figura 10:Elementos de la Seguridad Informática 60

Figura 11: Fases del Ethical Hacking 61

Figura 12. Análisis de Frecuencia PREG01 75

Figura 13.Análisis de Frecuencia PREG02 76

Figura 14.Análisis de Frecuencia PREG03 77

Figura 15.Análisis de Frecuencia PREG04 78

Figura 16.Análisis de Frecuencia PREG05 79

Figura 17.Análisis de Frecuencia PREG06 80

Figura 18.Análisis de Frecuencia PREG07 81

Figura 19.Análisis de Frecuencia PREG08 82

Figura 20.Análisis de Frecuencia PREG09 83

Figura 21.Análisis de Frecuencia PREG10 84

Figura 22.Análisis de Frecuencia PREG11 85

Figura 23.Análisis de Frecuencia PREG01 86

Figura 24.Análisis de Frecuencia PREG02 87

Figura 25.Análisis de Frecuencia PREG03 88
Figura 26.Análisis de Frecuencia PREG04 89
Figura 27.Análisis de Frecuencia PREG05 90
Figura 28.Análisis de Frecuencia PREG06 91
Figura 29.Análisis de Frecuencia PREG07 92
Figura 30.Análisis de Frecuencia PREG08 93
Figura 31.Análisis de Frecuencia PREG09 94
Figura 32.Análisis de Frecuencia PREG10 95
Figura 33.Análisis de Frecuencia PREG11 96
Figura 34.Determinación del valor crítico de la hipótesis general, con apoyo de la tabla de distribución normal 97

RESUMEN

Toda empresa que tenga como meta mejorar o perdurar en el tiempo, debe implementar sistemas informáticos para sus procesos, establecer conexiones a través de redes locales e internet.

Los sistemas implementados garantizan fluidez y celeridad, pero también pueden ser puntos vulnerables que pueden utilizados por personas negativas, esta investigación trata la aplicación del Ethical Hacking con la finalidad de descubrir carencias, vacíos o puertas de acceso no autorizados, para luego implementar mecanismos de seguridad y control, garantizando el resguardo de la organización.

Palabras Claves: Ethical, Hacking, vulnerabilidad, riesgo, controles.

ABSTRACT

Any company that aims to improve or endure over time, must implement computer systems for their processes, establish connections through local networks and internet. The implemented systems guarantee fluidity and speed, but they can also be vulnerable points that can be used by negative people, this research deals with the application of Ethical Hacking in order to discover gaps, loopholes or unauthorized access doors, and then implement security and control mechanisms, ensuring the safety of the organization.

Keywords: Ethical, Hacking, vulnerability, risk, controls.

INTRODUCCIÓN

La implementación de TI en las organizaciones es imprescindible si esta pretender participa en el mercado competitivo y así mismo prosperar, las implementaciones van desde: computadoras personales, impresoras conectadas por red, equipos de comunicación, softwares, etc.

Asimismo, ningún sistema es infalible, toda implementación de TI posee un porcentaje de vulnerabilidad, que, al ser descubierta por agentes maliciosos, se encontrarían en expuestos, con un nivel de seguridad muy bajo; por lo cual, se vio conveniente realizar esta investigación aplicando el Ethical Hacking.

A continuación, se describe la estructura de capítulos:

En el Capítulo I – Planteamiento del problema, Descripción, formulación, objetivos, justificación, importancia, limitaciones, hipótesis, delimitaciones, variables. En el Capítulo II – Marco Teórico, antecedentes, bases teóricas, definición de términos. En el Capítulo III – Metodología, tipo y nivel de investigación, población, técnicas e instrumentos, procesamiento y tratamiento.

En el Capítulo IV – La solución del problema. Capítulo V – Resultados y Discusión, y finalmente las conclusiones, recomendaciones referencias bibliográficas y anexos.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. DESCRIPCIÓN Y FUNDAMENTACIÓN DEL PROBLEMA

La presente investigación tiene como objetivo Mejorar la gestión de riesgos en los sistemas informáticos de CLINICA AMERICANA SERFARMED mediante la implementación de ethical hacking seleccionando la herramienta que más se ajuste en cada etapa. A si mismo evaluar técnicas de ethical hacking ejecutando pruebas de penetración sobre la seguridad informática de la red de datos de la clínica Permitiendo realizar el diagnostico de vulnerabilidades.

CLINICA AMERICANA SERFARMED maneja Activos informáticos, así como aplicaciones generando información valiosa y vulnerable por lo que se propone implementar técnicas de Ethical Hacking Para Mejorar La Gestión De Riesgos Informáticos De La clínica para un mejor control de acceso a la red de datos que permita evaluar, diagnosticar vulnerabilidades en la seguridad informática y de esta manera obtener como resultado una red de datos más eficiente garantizando la seguridad de los datos ante los diferentes ataques de intrusos o terceros.

LA CLINICA AMERICANA SERFARMED no es ajena a la problemática planteada anteriormente, pues se evidenció que hubo vulnerabilidad de información de pacientes, y ataques de phishing.

Por otro lado, la implementación de software de Gestión de servicios médicos como es el caso de historias clínicas electrónicas en la misma clínica se realizó sin tener en cuenta una planificación adecuada para la reducción de las vulnerabilidades que

afecten a la información del paciente. Esto trae consigo como resultado que se detecte una mala gestión del departamento de TI en el manejo de la seguridad de la información.

Así mismo Esto ocasiona que el uso inadecuado de las redes de comunicaciones, bases de datos y publicación electrónica de la información, necesarios en el desarrollo de cualquier actividad provoca en los procesos de negocio una progresiva amenaza tecnológica. En la actualidad, es esencial garantizar no sólo la continuidad de tales procesos, sino la seguridad, validez y eficacia de las transacciones realizadas y la protección de la información gestionada.

En los últimos años, LA CLINICA AMERICANA SERFARMED ha abordado un camino hacia la modernización de sus procesos de trabajo, en parte como resultado de la aplicación de compromisos legales y obligaciones con terceros. constituye el elemento central sobre el que pivota la seguridad del personal, las instalaciones y la información en la clínica.

En mi calidad de tesista, se logró percibir síntomas tales como: a) Inadecuada gestión de riesgos de la infraestructura tecnológica, b) incumplimiento de los niveles de servicio a los usuarios por caídas constantes de los sistemas infectados, c) Malestar por parte del personal médico respecto a la lentitud, inoperatividad de los equipos de cómputo, d) Malestar por parte del personal médico al no poder utilizar con seguridad los diferentes activos informáticos de la clínica. e) Reclamos por la inoperatividad de equipos debido a la infección de virus y ransonware. Asimismo, se logró identificar que las causa son: Inadecuado control de operaciones de seguridad informática por parte del personal de Informática TI en la gestión de servicios de TI (Incidencias, activos, problemas, etc.).

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1. Problema General.

¿En qué medida la implementación de ethical hacking mejorara la gestión de riesgos informáticos DE LA CLINICA AMERICANA SERFARMED.?

1.2.2. Problemas Específicos.

- ¿En qué medida la implementación de ethical hacking mejorará el Número de Riesgos Identificados DE LA CLINICA AMERICANA SERFARMED - PUCALLPA.?
- ¿En qué medida La implementación de ethical hacking mejorara el Número de Riesgos Analizados DE LA CLINICA AMERICANA SERFARMED - PUCALLPA?
- ¿En qué medida La implementación de ethical hacking mejorara el Número de Riesgos tratados DE LA CLINICA AMERICANA SERFARMED - PUCALLPA?

1.3. OBJETIVOS.

1.3.1. Objetivo General.

Determinar de qué manera la implementación ethical hacking mejorará la gestión de riesgos informáticos DE LA CLINICA AMERICANA SERFARMED Pucallpa.

1.3.2. Objetivos Específicos.

- Determinar de qué manera la implementación de ethical hacking mejorará el Número de Riesgos Identificados DE LA CLINICA AMERICANA SERFARMED - PUCALLPA.

- Determinar de qué manera la implementación de ethical hacking mejorara el Número de Riesgos Analizados DE LA CLINICA AMERICANA SERFARMED - PUCALLPA.
- Determinar de qué manera la implementación de ethical hacking mejorara el Número de Riesgos tratados DE LA CLINICA AMERICANA SERFARMED - PUCALLPA.

1.4. JUSTIFICACIÓN, IMPORTANCIA Y LIMITACIONES.

1.4.1. JUSTIFICACIÓN.

Justificación teórica

El hacking ético contempla procedimientos orientados a la seguridad informática, Es éticamente justificable por consentimiento de los interesados, con el objetivo de identificar deficiencias de los sistemas e infraestructura digital.

Justificación práctica

El hacking ético será aplicado como herramienta para diagnosticar carencias de seguridad a nivel de la infraestructura de Ti en LA CLINICA AMERICANA SERFARMED – PUCALLPA, y de esta manera garantizar la seguridad de forma permanente.

Justificación metodológica

Para el desarrolla de la presente investigación se cumplirá con aplicación del método científico, así como el cumplimiento de los lineamientos establecidos por la facultad de sistemas de una Universidad Nacional de Ucayali.

1.4.2. IMPORTANCIA.

La solución que se implementará es de suma importancia y apoyo a las actividades de seguridad de TI, debido a que se pretende contar con un

instrumento que mejore la gestión de los riegos informáticos en la CLINICA AMERICANA SERFARMED, garantizando la seguridad de la misma.

1.4.3. LIMITACIONES.

Se trabajará directamente con un equipo autorizado con acceso directo a toda la red, con el fin de optimizar resultados que, al ser procesados, se determine las vulnerabilidades en la red actual de trabajo.

1.5. HIPÓTESIS

1.5.1. Hipótesis General

La implementación de ethical hacking mejora la gestión de riesgos informáticos DE LA CLINICA AMERICANA SERFARMED - Pucallpa.

1.5.2. Hipótesis Específica

- La implementación de ethical hacking mejora el Número de Riesgos Identificados DE LA CLINICA AMERICANA SERFARMED - PUCALLPA.
- La implementación de ethical hacking mejora el Número de Riesgos Analizados DE LA CLINICA AMERICANA SERFARMED – PUCALLPA.
- La implementación de ethical hacking mejora el Número de Riesgos tratados DE LA CLINICA AMERICANA SERFARMED - PUCALLPA.

1.6. DELIMITACIONES DE LA INVESTIGACIÓN

1.6.1. Delimitación Espacial.

La presente investigación tuvo lugar en la CLINICA AMERICANA SERFARMED – PUCALLPA, específicamente sobre su parque informático, se tuvo que evaluar los sistemas, hardware y software, que se utilizan en cada uno de los procesos internos.

1.6.2. Delimitación Social.

Esta investigación significará un punto de inicio o base para futuras investigación en el campo del Ethical Hacking, donde les permitan mejorar una realidad problemática, CLINICA AMERICANA SERFARMED – PUCALLPA, debido a los resultados de esta investigación cuenta con mecanismos de seguridad y controles que salvaguardan la información crítica.

1.6.3. Delimitación Temporal.

La presente investigación tuvo su origen en el año 2022, asimismo, se ha se cumplido con todos requisitos impuestos por la Oficina de Grados y Títulos de la FISeIC de la UNU.

1.6.4. Delimitación Conceptual.

En la presente investigación, se trata de fundamentos relacionados a software, servicios, análisis de riego, políticas y controles que fueron aplicados para tratar una situación problemática.

1.7. VARIABLES

1.7.1. Variable independiente:

Ethical Hacking

1.7.2. Variable dependiente:

Gestión de Riesgos Informáticos.

1.8. SISTEMA DE VARIABLES, DIMENSIONES E INDICADORES.

1.8.1. Operacionalización de las variables

Tabla 1. *Dimensiones e indicadores de las variables*

Variables	Definición conceptual	Definición Operacional	Indicadores
Ethical Hacking	Consiste en realizar, desde la perspectiva de un hacker malicioso, ataques controlados sobre los sistemas informáticos, detectando y aprovechando las vulnerabilidades. Todo esto con el fin de comunicar a la organización de los riesgos de seguridad (Astudillo, 2015).	Está comprendida por las dimensiones: planeación Vulnerabilidades Evaluación de riesgos Informe de resultados	- Activos de la empresa. - Nivel de identificación de software Critico. - Número de vulnerabilidades mitigadas - nivel de vulnerabilidades - Nivel de riesgos - Numero de informes.
Gestión de Riesgos Informáticos.	La gestión de riesgos TI busca garantizar la integridad, confidencialidad y accesibilidad a todos los datos informáticos de una organización, una tarea especialmente importante para las empresas en un escenario en que los sistemas de información se vuelven cada vez más indispensables. (hacknoid, 2015).	Está comprendida por las dimensiones: Riesgos Identificados. Riesgos analizados. Riesgos tratados.	- Nivel de plan de continuidad de negocio - Puertos USB. acticos en las Pcs. O servidores. - Frecuencia de limpieza de metadatos de archivos. - Nivel de Políticas de Seguridad - Frecuencia de monitoreos de los sistemas informáticos. - Sistema Operativo y de aplicaciones actualizado - Capacitación en temas de seguridad - Frecuencia de Realización de pruebas de Ethical Hacking - Transición de contraseñas de modo seguro - Nivel de regla de complejidad en contraseñas - Nivel de incidencias

Fuente: Elaboración propia

CAPÍTULO II

MARCO TEÓRICO

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

Internacionales

Oñate, O. & Martínez, C. (2017). La Investigación permitió realizar mejoras en la seguridad de la red inalámbrica de la Universidad Nacional de Chimborazo aplicando hacking ético En su investigación tuvo como objetivo se tiene como objetivos analizar las técnicas de hacking ético aplicado a las redes inalámbricas para determinar que herramientas son apropiadas para mitigar las vulnerabilidades y desarrollar un manual políticas de seguridad adecuadas los escenarios que se está realizando en la investigación. La metodología que se utiliza en la investigación es un estudio longitudinal, pues se obtiene datos de las vulnerabilidades de la red inalámbrica sin el uso de hacking ético y con el uso de hacking ético, teniendo como resultado un manual de políticas de seguridad, aplicable a las distintas vulnerabilidades encontradas. Para lo cual, se analiza e identifica parámetros de medición como el promedio de equipos conectados a la red inalámbrica, número de dispositivos que se pueden ser vulnerables a un análisis de paquetes o sniffer, nivel de vulnerabilidad detectada por descubrimiento de contraseñas y/o spoofing, nivel de calidad servicio y por último el nivel de políticas de administración aplicadas. Para realizar las mediciones pre y post sobre los escenarios de la red inalámbrica, se utilizan sistemas operativos como Kali Linux, Wifislax, Backtrack, equipos activos de red como wiresslan controller y servidor Radius. Se utiliza T-STUDENT para la comprobación de la hipótesis obteniendo los resultados siguientes: en la red de estudiantes el número

de clientes con posibilidad de ser analizados sus paquetes o sniffer bajan de 867.60 clientes a 468.20 clientes con una media de 399,400 y en la red de Docentes bajan de 522.40 clientes a 285.80 clientes con una media de 236,600. De acuerdo a la auditoría técnica realizada y el manual de políticas de seguridad desarrollado y entregado con Acta Entrega Recepción al Administrador de Red; en base a las vulnerabilidades detectadas en la red inalámbrica de la Universidad Nacional de Chimborazo, se concluye que se podrá mejorar la seguridad.

Franco Romero, G. A. (2019). En su investigación se realizó un análisis de las vulnerabilidades que afectan a los sistemas VoIP, para conocer estas vulnerabilidades se efectuaron pruebas de Pentesting basadas en hacking ético, sobre un ambiente de simulación previamente definido que permitió llevar a cabo las pruebas requeridas. Las pruebas que se ejecutaron son: Escaneo de Puertos y Dispositivos SIP, Ataques de Fuerza Bruta, Escuchas Ilegales. Gracias a los softwares de virtualización se puede simular y tener en operatividad un Sistema VoIP estándar, estos tipos de escenarios son los más usados por las empresas, lo que facilitó poder cumplir con los objetivos propuestos.

Asimismo, se menciona antecedentes internacionales (Francis, 2016) en su tesis presenta la explotación automatizada de la red informática a través de Penetration Testing (ANEX), un sistema automatizado de Pentesting diseñado para infiltrarse en una red informática y trazar rutas desde una red comprometida a una máquina de destino especifica. Los resultados mostraron ataques exitosos en múltiples niveles de red y confirmó la eficiencia y eficacia del diseño de la utilización de fuentes automatizadas y de código abierto**.**

Nacionales

Espinoza Araujo, Christian Omar. (2020) en su investigación tuvo como objetivo mejorar la gestión de riesgos en los sistemas informáticos de la Municipalidad Provincial de Moyobamba a través de la implementación de Ethical Hacking. La metodología que se empleó para el Ethical Hacking básicamente tenía las siguientes fases: Reconocimiento, Escaneo, Enumeración, Análisis de Vulnerabilidades, Hacking de Sistemas y Escalado de Privilegios. Asimismo, los indicadores de la variable dependiente: gestión de riesgos, fueron relacionados según criterios. Se utilizó la investigación cuantitativa con el diseño experimental del tipo preexperimental con un Pre-Test y Post-Test, teniendo como variable independiente el Ethical Hacking y variable dependiente la Gestión de Riesgos. La población estuvo conformada por los sistemas informáticos que incluía servidores, computadoras, sistemas operativos, software y Data Center, haciendo un total de 280, pero la muestra se tomó solo de 25 sistemas informáticos para realizar una mejor investigación. Para identificar amenazas se empleó el cuestionario en los trabajadores de la oficina de tecnologías de información y para el análisis de vulnerabilidades se utilizó escáneres, como Nessus, OpenVas y Acunetix. Al finalizar el trabajo de investigación se logró identificar 35 vulnerabilidades y 10 amenazas. Por otro lado, para calcular el nivel del riesgo se realizó la multiplicación de amenaza x vulnerabilidad en valores cuantitativos de: 0 – 10 y valores cualitativos de: muy alto, alto, moderado, bajo, muy bajo. Se encontró 13 riesgos en nivel alto, 17 riesgos en nivel moderado y 5 riesgos en nivel bajo. Una vez clasificados se procedió a brindar alternativas de solución para su posterior mitigación.

Durand More, A. D. (2019). En su investigación tuvo como objetivo evaluar técnicas de Ethical Hacking ejecutando pruebas de penetración sobre la seguridad informática de una red de datos que permitan el diagnóstico de vulnerabilidades en una empresa prestadora de servicios (Ciudad de Lambayeque – Chiclayo). La presente investigación, es de tipo cuantitativo y de diseño cuasi experimental, dado que se tomarán resúmenes de herramientas de hacking ético en determinados momentos sobre la red de la empresa prestadora de servicios. La muestra para la investigación fueron los dispositivos conectados en la red de la empresa prestadora, se trabajó directamente con un equipo autorizado con acceso directo a toda la red, con el fin de optimizar resultados que, al ser procesados, se concluyó que existen vulnerabilidades en la red actual de trabajo. Concluyendo que en la presente investigación existen políticas y normas de mitigación de vulnerabilidades, tanto físicas como lógicas que se deben implementar con el fin de disminuir fallas en la red y acceso a intrusos para el perjuicio de la documentación existente en la empresa.

2.2. BASES TEÒRICAS

ETHICAL HACKING, se refiere a la acción de “hackear” los sistemas informáticos de una organización, previa autorización firmada, en el cual se utilizan las mismas técnicas y herramientas de un “Black Hat Hacker”, el cual es una persona que rompe la seguridad de un sistema informático con fines ilícitos; sin embargo, el Ethical Hacking busca de una manera legal y legítima identificar vulnerabilidades de un sistema informático en la parte del software y hardware, informando a la organización sobre los resultados obtenidos, al mismo tiempo de brindar alternativas de solución para poder corregirlas y mitigarlas (Baloch, 2015, p. 02)

En el campo del hacking ético, existen metodologías o marcos de trabajo, que permiten la ejecución y documentación de esta actividad, de una manera ordenada, algunas de estas metodologías son Open Source Security Testing Methodology Manual – OSSTMM o Manual de la Metodología Abierta de Testeo de Seguridad, Open Web Application Security Project – OWASP, enfocado a determinar y combatir las causas de inseguridad en el software, principalmente en aplicaciones web, e Information Systems Security Assessment Framework – ISSAF, el cual es un marco de trabajo enfocado en las practicas relacionadas a un testeo de seguridad

OSSTMM.

El Manual de la Metodología Abierta de Testeo de Seguridad u Open Source Security Testing Methodology Manual, es una metodología desarrollada por el Instituto para la Seguridad y Metodologías Abiertas o ISECOM, por sus siglas en inglés (Institute for Security and Open Methodologies), y fue publicada a finales del año 2000, lo cual marcó un hito pues hasta el momento no existían documentos que de manera abierta y estandarizada, agruparan las actividades a tener en cuenta, por parte de un profesional en seguridad informática, a la hora de realizar una evaluación de seguridad. Después de su publicación, ISECOM ha venido actualizando la metodología OSSTMM, hasta encontrarse en este momento en su versión 3.

Esta metodología, se basa en 7 grandes fases, las cuales se ilustran en Figura 1:

Figura 1: Fases OSSTMM



Fuente:(geekslinuxchile, 2020)

Como se observa en la anterior imagen, las fases de OSSTMM, proporcionan una metodología que se encuentra totalmente alineada con las fases del hacking ético.

A continuación, Haremos una descripción más detallada de las fases de la metodología, las herramientas aplicables a cada fase y los resultados de la aplicación de estas.

A grandes rasgos, OSSTMM aborda las siguientes etapas:

- ✓ Obtener y analizar la información existente del sistema
- ✓ Testear los sistemas operativos, su configuración y servicios en comparación con la documentación del sistema
- ✓ Búsqueda de vulnerabilidades y análisis a través de test de penetración
- ✓ Realizar pruebas de integridad a todos los resultados

- ✓ Mapear los resultados de los sistemas y servicios evaluados
- ✓ Realizar Evaluación del Riesgo – RAV, para las debilidades encontradas
- ✓ Mapear los resultados y dar recomendaciones

Estas etapas tienen una correlación directa con las fases del hacking ético, así:

Tabla 2.Correlación entre Etapas del H.E. y Fases OSSTMM

Etapa H.E.	Fase OSSTMM
Planeación	- Obtener y analizar la información existente del sistema
Descubrimiento	- Testear los sistemas operativos, su configuración y servicios en comparación con la documentación delsistema
Ataque	- Búsqueda de vulnerabilidades y análisis a través de testde penetración - Realizar pruebas de integridad a todos los resultados
Reporte	- Mapear los resultados de los sistemas y serviciosevaluados - Realizar Evaluación del Riesgo – RAV, para lasdebilidades encontradas - Mapear los resultados y dar recomendaciones

Fuente: Elaboración propia

Como se observa, la metodología OSSTMM propone un modelo de análisis y evaluación de vulnerabilidades de manera amplia y ordenada, que documenta los resultados y las recomendaciones en materia de seguridad informática, basado en todo el proceso realizado. Esto es lo que se pretende lograr con el presente proyecto, tener un análisis que permita a la Entidad, en este caso la CLINICA AMERICANA SERFARMED – PUCALLPA, tomar medidas y decisiones que propendan por la seguridad de la información que actualmente administra.

CERTIFIED ETHICAL HACKER (CEH), es una certificación de hacking ético desarrollada por el Consejo Internacional de Consulta de Comercio Electrónico de los Estados Unidos, que tiene una metodología para desarrollar un correcto Ethical Hacking. (EC-Council, 2019)

EXPLOIT, es un tipo de código malicioso escrito en lenguajes de programación como Python, Ruby, C ++, etcétera, para el aprovechamiento de una vulnerabilidad en un sistema con el fin de tener control sobre este (VILLEGAS, 2018)

GESTIÓN DE RIESGOS, en el contexto de la seguridad informática, la gestión de riesgos toma en cuenta las vulnerabilidades, las fuentes de amenazas y los controles de seguridad que se planifican e implementan para determinar el nivel de riesgo, grado de probabilidad y alternativas de solución (New York State Information Technology Service, 2015).

Culminada la fase 2 y comenzando la fase 3 del hacking ethical se procederá a realizar la gestión de riesgos.

Figura 2: Proceso de Gestión de Riesgos



Fuente: (researchgate, 2022)

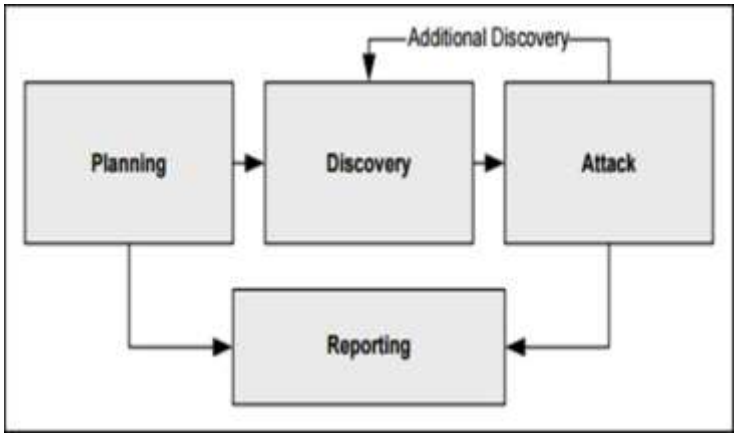
Metodología a desarrollar:

El presente proyecto, se desarrolla a través de cuatro fases, que son: Planeación, Descubrimiento, Ataque, Reportes. Es a través de estas 4 fases que se pretende dar alcance y cumplimiento a los objetivos planteados en el presente proyecto. Estas cuatro fases, también conocidas como Planning, Discovery, Attack, and Reporting – PDAR, se encuentran alineadas con las fases del hacking ético.

A continuación, se presenta una imagen que contiene un flujograma del PDAR (Planeación, Descubrimiento, Araque y Reportes), como se observa, su proceso inicial es la planeación y una vez culminada esta fase, es posible pasar a la fase de descubrimiento, para posteriormente continuar con el ataque, lo cual corresponde a la realización de las pruebas de penetración como tal; si durante esta fase se obtienen descubrimientos adicionales, estos deberán ser tratados como tal y realizar el ataque o explotación de los mismos, de ser pertinente. Todos los hallazgos obtenidos durante la fase de ataque deben ser documentados en los reportes destinados para tal fin.

A continuación, se presenta el flujograma de PDAR, según la NIST-SP 800-42

Figura 3: *Flujograma PDAR*



Fuente: (henryraul, 2021)

En los siguientes párrafos, se presenta una descripción detallada de cada una de las fases que componen la presente metodología.

Planeación

En esta fase de define el alcance que tendrá el hacking ético, también se aprueba la realización de esta actividad y se establecen los acuerdos de confidencialidad. Del lado del equipo de pruebas, se define la metodología a utilizar. Igualmente es necesario tener en cuenta las restricciones en cuanto a horarios y tiempos de

pruebas y ataques, además de las restricciones legales que pueda requerir la Entidad.

Descubrimiento

La fase de descubrimiento es una de las fases más amplias en el proceso de hacking ético y es aquí donde empieza el trabajo recabando información sobre el objetivo a atacar. Se divide en 3 momentos:

- Footprinting
- Escaneo y enumeración
- Análisis de vulnerabilidades

Footprinting

Es la primera actividad que se debe realizar, es una tarea no intrusiva en donde se busca obtener el máximo de información sobre la organización y sus sistemas informáticos, componentes hardware y demás, aquí se aplican varias técnicas tales como:

- Ingeniería Social
- Búsquedas avanzadas con Google
- Social Networking a través de sitios como LinkedIn, Twitter, Google plus, Facebook entre otros

Escaneo y enumeración

Durante esta etapa, se busca identificar sistemas activos, puertos abiertos y servicios activos y esto se realiza a través del escaneo de puertos, escaneo de redes y escaneo de vulnerabilidades.

En la siguiente imagen se observan los elementos a tener en cuenta durante el escaneo y la enumeración:

Figura 4: Elementos de Escaneo y Enumeración



Fuente: (CEH,2018)

Para la etapa de escaneo y enumeración existen se herramientas tales como Nmap, Angry IP Scanner, Hping, Xprof2, WinFingerprint, a través de las cuales es posible tener un primer acercamiento a lo que es la infraestructura y topología de red implementada por la Entidad, así como enumerar los puertos y servicios que se encuentran habilitados en los diferentes hosts que integran dicha red informática.

Análisis de vulnerabilidades

Una vez culminadas las etapas de escaneo y enumeración, es posible continuar con el análisis de vulnerabilidades, aquí se utilizan herramientas tales como Nessus, OpenVAS, Shadow Securtity Scanner, ISS Scanner. El funcionamiento de dichas herramientas se basa en inspeccionar los puertos y servicios habilitados en los distintos hosts de la red y realizar un análisis de vulnerabilidades, en comparación con las que se encuentran documentadas por el Common Vulnerabilities and Exposures – CVE y otras no documentadas pero

conocidas. Estas son básicamente debilidades en la configuración o implementación de servicios que se tienen implementados.

Ataque

Esta fase es el corazón de un hacking ético, es aquí donde toda la teoría se pone en práctica, donde la información recabada anteriormente se utiliza para explotar las vulnerabilidades encontradas y hackear los sistemas informáticos objetivo. Se divide principalmente en dos momentos:

- Explotación
- Elevación de privilegios

Explotación

En esta fase se explotan las vulnerabilidades encontradas anteriormente, para ello se hace uso de exploits que pueden ser buscados en una base de datos de estos o crear scripts que permitan realizar esta explotación. Es recomendable que el o los encargados de realizar esta fase, tengan conocimientos en lenguajes de scripting como lo son Phyton, Pearl o incluso Ruby.

Es necesario que esta fase se ejecute muy cuidadosamente, siendo pertinente determinar cuáles vulnerabilidades se van a comprobar a través de los diferentes exploits, pues algunos podrían afectar los sistemas que se encuentren en producción o que la Entidad pueda considerar críticos para su operación, e incluso llegar generar fallos que puedan poner en riesgo la disponibilidad de servicios ofrecidos por la Rama Judicial.

Existen bases de datos donde se pueden encontrar exploits los cuales se encuentran listos para ejecutar, aunque es altamente recomendad realizar pruebas de los exploits que se pretenden utilizar, en un ambiente controlado o de pruebas, antes de ejecutarlos la infraestructura en producción. Algunas de esas bases de datos de exploits son:

https://www.exploit-db.com/ http://www.hack0wn.com/ https://es.0day.today/

Igualmente existen marcos de trabajo o aplicaciones que permiten realizar estas tareas de explotación, tales como: Metasploit, Core Security, Immunity CANVAS, Exploit Pack, Armitage, Nexpose17. A traves de estos frameworks es posible facilitar la explotación de ciertas vulnerabilidades, toda vez que contienen o permiten implementar los scripts que vulneran las debilidades encontradas, pudiendo confirmar la existencia de las mismas.

En ocasiones, algunos de estos exploits deben ejecutarse con privilegios elevados y es allí donde interviene la siguiente fase:

Elevación de Privilegios

En esta fase, el hacker o tester, debe adquirir un nivel de acceso que le permita realizar las actividades pertinentes, en este proceso ser necesario la utilización de software o ciertas herramientas que le permitan escalar privilegios de manera que pueda realizar su labor sin restricciones.

La elevación de privilegios no siempre se da a nivel de usuarios, a veces se da a niel de máquinas, cuando se utiliza una maquina como pivote, para poder acceder a otras, esto se conoce como Daisy Chaining

Reporte

Esta es la última etapa del proceso de hacking ético, en ella se registran todas las actividades desarrolladas, las vulnerabilidades encontradas y se realizan recomendaciones para solucionar estas vulnerabilidades y que contramedidas se pueden tomar.

Es recomendable guardar registro de las acciones realizadas, durante las fases anteriores (planeación, descubrimiento y ataque) esto ayuda a la construcción del reporte final.

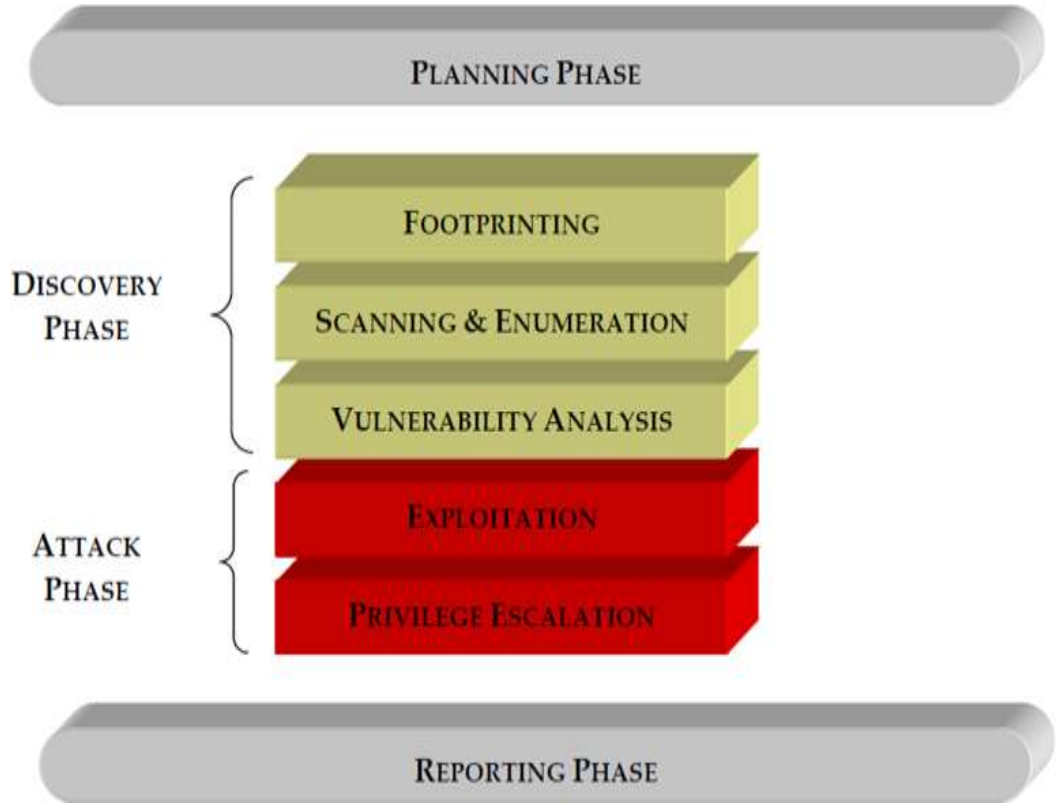
El reporte debe contener aspectos técnicos de las tareas realizadas, en un lenguaje general que pueda entender la gerencia de la organización, además debe contener como mínimo, los siguientes elementos:

- Resumen ejecutivo
- Resultados detallados de las actividades realizadas
- Valoración vulnerabilidades encontradas (Nivel de riesgo)
- Impacto sobre la organización
- Recomendaciones

Es necesario mencionar, que OSSTMM cuenta con unas herramientas que permiten realizar la valoración de los niveles de riesgo a través de aplicaciones matemáticas, que permiten no solo cualificar sino cuantificar tales niveles, para poder generar una evaluación en nivel de cumplimiento, en cuanto a seguridad informática se refiere.

De manera gráfica, las fases del presente proyecto pueden observarse a continuación, en la siguiente figura:

Figura 5: Fases del proyecto

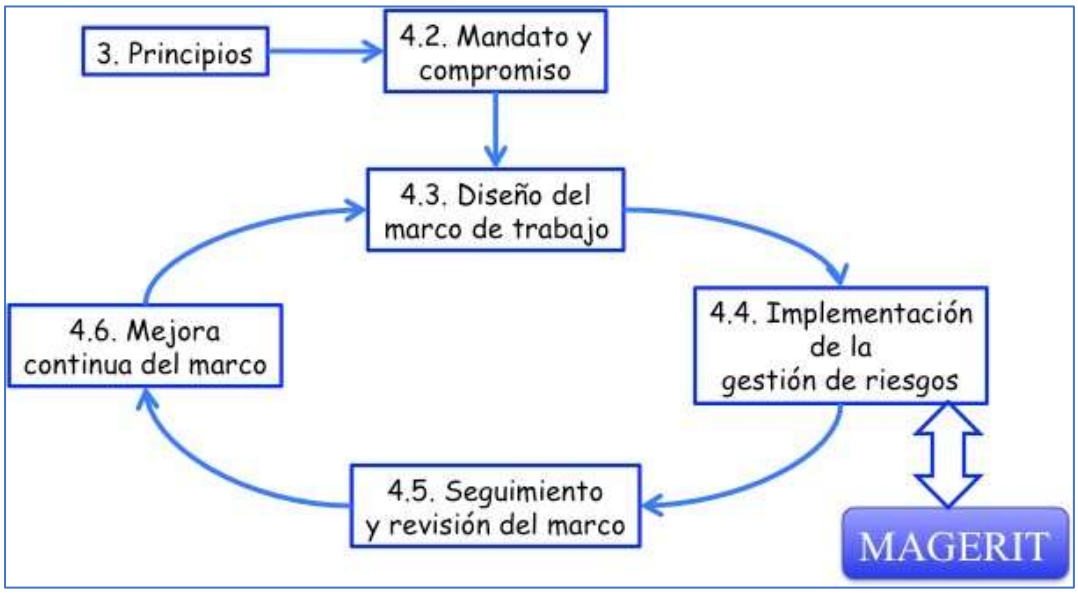


Fuente: (nvlpubs, 2020)

Metodología de Gestión de riesgos Magerit

Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina “Proceso de Gestión de los Riesgos”, sección 4.4 (“Implementación de la Gestión de los Riesgos”)dentro del “Marco de Gestión de Riesgos”. En otras palabras, MAGERIT implementa el Procesode Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

Figura 6:. *ISO 31000 - Marco de trabajo para la gestión de riesgos*



Fuente: (amelica,2020)

ISO 27001

Un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001 se fundamenta principalmente en la identificación y análisis de las principales amenazas para, a partir de este punto de partida, poder establecer una evaluación y planificación de dichos riesgos.

Una amenaza se puede definir como cualquier evento que puede afectar los activos de información y se relaciona, principalmente, con recursos humanos, eventos naturales o fallas técnicas. Algunos ejemplos pueden ser: ataques informáticos externos, infecciones con malware, una inundación, un incendio o cortes de fluido eléctrico.

Pero en ocasiones basta una omisión o despiste por parte del personal de la empresa, como el uso de una simple pulsera imantada, para que se pueda llegar a producir un daño grave, e incluso irreparable, de la información.

En definitiva, se trata de elaborar una adecuada gestión de riesgos que permita a las organizaciones conocer cuáles son las principales vulnerabilidades de sus activos de información.

Un correcto proceso de identificación de riesgos implica:

- Identificar todos aquellos activos de información que tienen algún valor para la organización.
- Asociar las amenazas relevantes con los activos identificados.
- Determinar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas.
- Identificar el impacto que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo.

Análisis y evaluación de los riesgos y sus consecuencias

Se debe analizar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información, evaluando de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades e impactos en los activos.

Además de riesgo en sí, es necesario analizar también sus consecuencias potenciales, que son muchas y de distinta gravedad: desde una simple dispersión de la información a la pérdida o robo de datos relevantes o confidenciales.

Una posible metodología de evaluación de riesgos estaría compuesta de las siguientes fases:

Recogida y preparación de la información.

Identificación, clasificación y valoración los grupos de activos.

Clasificación de las amenazas tras su previa identificación.

Identificación y estimación de las vulnerabilidades.

Identificar, tipificar y valorar los impactos.

Evaluación y análisis del riesgo.

Criticidad del riesgo

Por este motivo, se deben evaluar las consecuencias potenciales para poder evaluar su criticidad: riesgo aceptable y riesgo residual.

Riesgo aceptable

No se trata de eliminar totalmente el riesgo, ya que muchas veces no es posible ni tampoco resultaría rentable, sino de reducir su posibilidad de ocurrencia y minimizar las consecuencias a unos niveles que la organización pueda asumir, sin que suponga un perjuicio demasiado grave a todos los niveles: económico, logístico, de imagen, de credibilidad, etc.

Riesgo residual

Se trata del riesgo que permanece y subsiste después de haber implementado los debidos controles, es decir, una vez que la organización haya desarrollado completamente un SGSI. Es un reflejo de las posibilidades de que ocurra un incidente, pese a verse implantado con eficacia las medidas evaluadoras y correctoras para mitigar el riesgo inherente.

El compromiso del liderazgo

La norma ISO 27001 otorga un peso cualitativo muy importante a la Dirección, la cual debe ejercer el liderazgo del sistema de seguridad. A partir de aquí, se debe establecer un plan de trabajo en el que quede perfectamente definida la segregación de tareas. Dicho de otro modo: se tiene que establecer con exactitud quién tiene que hacer cada función y cómo ejecutarla.

Los dueños del riesgo según ISO 27001

La norma ISO 27001 establece la figura de Dueño del Riesgo, asociándose cada amenaza potencial o real a un responsable, que es la persona que se asegura que se lleven a cabo las distintas actividades. Dicho responsable no tiene por qué ser la persona que finalmente ejecuta los controles, sino alguien que se responsabiliza de que realmente los controles se están llevando a cabo acorde a lo establecido.

Por lo tanto, es necesario definir la estructura organizacional del SGSI, seleccionado el personal idóneo dependiendo del tamaño de la empresa y el alcance definido para la implantación del SGSI. De acuerdo a las dos anteriores variables, se puede determinar el número de profesionales con los perfiles necesarios que formarán parte del grupo de seguridad de la información de la institución.

Álvarez (2018) propone una nueva metodología que permite realizar todo el ciclo de Hacking ethical, incluyendo evaluación de riesgos la cual la divide en 4 fases

Fase 1.- Acuerdo, alcance y recopilación de información.

En esta fase se definirán acuerdos y alcance de la auditoría con el comité gerencial de la empresa, para lograrlo de manera exitosa, se utilizan formatos, plantillas que se exponen en el capítulo 2 del manual OSSTMM versión 3.0 y al capítulo 4 del marco de seguridad ISSAF versión 0.2.1. Luego, se levanta la información de todos los activos de la empresa basándose en un análisis de impacto o riesgo con respecto a los objetivos de la empresa; obteniendo los que intervendrán en las pruebas de penetración.

Con esta información se procede a realizar la programación de las siguientes fases de la metodología.

Fase 2. Ejecución.

Esta es la fase que se lleva a cabo el escaneo de vulnerabilidades, evaluación de seguridad y pruebas de penetración. Para ello se definen primeramente las líneas tecnológicas a aplicar las pruebas.

Líneas tecnológicas a aplicar las pruebas de penetración.

Las líneas de aplicación donde se aplicarán las pruebas de penetración, serán: Infraestructura de red (ethernet, inalámbrica, elemento de seguridad, accesos remotos), sistemas operativos (plataformas, versiones), servicios (firewall, IDS, IPS, honey pots) y aplicaciones (locales y ámbito web).

Escaneo o recopilación de información

Este paso es fundamental para el éxito de las pruebas de penetración. Por esto, se debe recopilar todos los datos posibles, categorizados en 2 aspectos: información pública del sistema (footprinting) e información concreta como sistemas, elementos de red, mecanismos de seguridad, versiones de los sistemas (fingerprinting).

Footprinting

La información pública o footprinting se puede obtener por medio de técnicas avanzadas en buscadores como google o bing, páginas web especializada como www.netcraft.com ó www.goolag.org, herramientas especializadas para búsqueda como maltego, netblug, herramientas para obtener datos de servidores web y herramientas para extracción de los metadatos de los documentos de los sitios web como Foca, anubis.

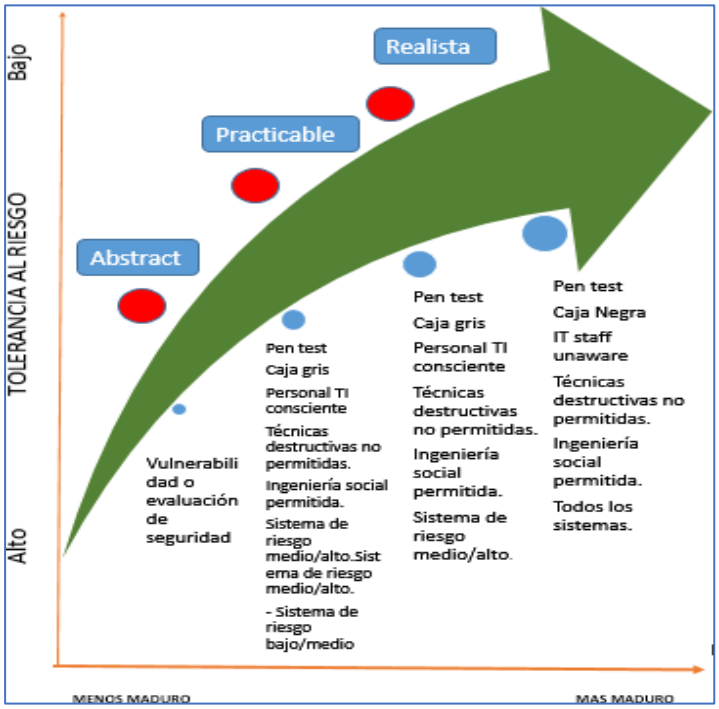
Fingerprinting

A fin de obtener información concreta, se realiza la fase de sondeo y fase de enumeración. El primero es una actividad que intenta una conexión a cada uno de los sistemas para provocar una respuesta y extraer información; aquí se utilizan herramientas de escaneo como nmap, netcat, traceroute. Por otro lado, la enumeración se utiliza para obtener información detallada y precisa de un objetivo.

Evaluación de seguridad

A continuación, se determina el nivel de seguridad que se aplicará a la organización dependiendo de la madurez en que se encuentre, con el fin de determinar el tipo pruebas de penetración a ejecutarse. Para ello, se utiliza el modelo de madurez expuesto en la figura 7.

Figura 7:. *Modelo de madurez*



Fuente: (Deusto, 2019)

Se considerará los lineamientos de la metodología antes mencionadas de OOSSTM en su versión básica PDAR.

Tipo de prueba de penetración

Luego, se establece tipo de pruebas de penetración en función del conocimiento del auditor y las áreas, así puede ser, caja negra, caja blanca, caja gris.

Una vez establecido el tipo de prueba de penetración, se procede a ejecutarlas mediante el análisis y explotación de vulnerabilidades

Análisis de Vulnerabilidades

Una vez obtenida la información se procede a realizar el análisis de vulnerabilidades. Para esto, se utilizará herramientas automáticas como OpenVas, Nessus, las cuales sondean posibles vulnerabilidades a partir de datos que se recopilan sobre sistemas operativos, servicios, aplicaciones con ámbito local como web, realizando un diseño de infraestructura de red donde se visualiza la ubicación, funcionalidad, de elementos de software y hardware instalados en la misma, donde se realiza el análisis de las vulnerabilidades o debilidades que puedan presentar los mismos.

Explotación de vulnerabilidades e intrusión

Luego del análisis de vulnerabilidades se procede a explotar las mismas, esto es, materializar la amenaza en las aplicaciones o elementos de red que se encontraron mencionadas vulnerabilidades. Para ello, se utiliza un conjunto de técnicas y herramientas de hacking ético que pueden ser ejecutadas de forma manual o automática. Una vez explotadas se tratan de escalar los privilegios a fin de aumentar los permisos para acceder a otros servicios, utilizando técnicas hacking como sniffer, keylogger,

rootkit. Como opcional se realizará la eliminación de huellas, borrando la información de los registros de cada una de las intrusiones.

Fase 3.- Evaluación de riesgo.

En esta fase se genera una matriz de riesgos con respecto a cada activo definido en la primera fase y en base al análisis de vulnerabilidades, pruebas de penetración realizadas en la fase 2. A continuación, se aplican métricas que categoricen los riesgos, para finalmente evaluarlos dependiendo del impacto a los objetivos de la empresa. En esta fase, también se puede definir los controles y procedimientos que se deberían utilizar para mitigar los riesgos encontrados.

Análisis de riesgos

Una vez identificadas las vulnerabilidades y las amenazas, se determinan los riesgos inherentes y se procede a realizar el análisis de cada riesgo; el mismo que consiste en determinar la probabilidad de ocurrencia de los mismos, así como su impacto. Para ello se considera tres variables: probabilidad, impacto e importancia.

Tabla 3.Escala de probabilidad de ocurrencia de una menaza.

Valor	Escala	Concepto
3	Muy probable	Puede suceder 1 vez al año y ha sucedido otras veces
2	Probable	Puede ocurrir alguna vez/ha ocurrido una sola vez
1	Improbable	No ha ocurrido antes, pero puede ocurrir en circunstancias excepcionales.

Fuente: Elaboración propia

Por otro lado, para determinar la segunda variable que es el impacto, se utilizará:

Tabla 4.Escala del impacto de materialización de un riesgo

Valor	Escala	Concepto
3	Alto	Las consecuencias amenazarán los objetivos y la supervivencia de la organización
2	Medio	Las consecuencias harán realizar cambios significativos en la organización o sus operaciones.
1	Bajo	Las consecuencias pueden solucionarse con cambios y aplicación de políticas.

Fuente: Elaboración propia

Finalmente, para determinar la tercera variable, que es la relevancia e importancia del riesgo, el cual se muestra.

Tabla 5.Escala de relevancia de un riesgo

Valor	Escala	Concepto
10	Alta	Factor de riesgo relevante o muy importante para la organización o entidad.
5	Media	Factor de riesgo de relevancia media para la organización o entidad.
1	Baja	Factor de riesgo no relevante para la organización

Fuente: Elaboración propia

Evaluación del riesgo

A fin de evaluar el riesgo, se lo clasifica de acuerdo a los resultados obtenidos en las variables definidas en la sección anterior, análisis de riesgo. Para ello se utiliza la escala de clasificación del riesgo:

Tabla 6.Escala de evaluación del riesgo.

Calificación Final	Riesgo	Color
De 1 a 10	**Bajo**	**Verde**
De 11 a 30	**Aceptable**	**Naranja**
De 31 a 90	**Alto**	**Rojo**

Fuente: Elaboración propia

Una vez definidas los parámetros o escalas para la revaluación del riesgo, se procederá a calificarlos en la matriz de riesgos; obteniendo de manera automática el resultado de acuerdo con el color establecido.

Para realizar la evaluación, se debe considerar las calificaciones obtenidas. Si el riesgo es bajo, permite a la organización asumirlo, esto es, que no es necesario establecer controles ya que su ocurrencia es mínima, su impacto es bajo y su grado de importancia baja.

Sin embargo, si el riesgo es aceptable o alto, significa que la posibilidad de ocurrencia puede ser muy probable, por lo que es necesario implementar medidas de control que permitan disminuir el grado de impacto.

Valoración de riesgos

En la valoración de los riesgos es donde se establecen las prioridades y revisión de controles; los cuales pueden ser preventivos o correctivos. El tipo de control preventivo es aquel que elimina la causa del riesgo y prevenir su ocurrencia o materialización; y correctivos, aquel que reestablecen la actividad luego que se materializa la amenaza. Además, se debe determinar si el control está documentado, si se está aplicando en la actualidad y si es efectivo para minimizar el riesgo.

Gestión o tratamiento de los riesgos

En esta gestión o tratamiento se identifican las opciones para mitigarlos, esto es, realización de acciones dentro de un plan de mejoras; Sin embargo, es pertinente analizar el costo beneficio de la gestión de riesgo para tomar la mejor decisión.

Fase 4. Generación de informes.

En esta fase se elaboran los informes técnicos y ejecutivos. En el informe técnico se mostrarán las vulnerabilidades encontradas en los activos físicos y lógicos, además de las herramientas utilizadas para ello. El informe ejecutivo consta primeramente de los riesgos en que puede incurrir la empresa y los controles o procedimientos adecuados que se deberían implementar en base a un análisis costo/beneficio. Haciendo referencia a las metodologías estudiadas, se pueden utilizar lo enunciado en el manual OSSTMM versión 3.0 – capítulo 13 – Reporting with the STAR. Así también en el marco ISSAF versión 0.2.1 – capítulo 5 – Phase III – Post Assessment. Por último, en la guía de pruebas de OWASP versión 3.0 – capítulo 5.2, "como escribir el informe de pruebas".

A continuación, en la figura 7, se muestra el diagrama de la nueva propuesta metodológica para pruebas de penetración.

Figura 8: *Diagrama de metodología Propuesta para prueba de penetración orientada a riesgos*



***Fuente**: Álvarez (2018).*

2.3. DEFINICIÓN DE TÉRMINOS BÁSICOS.

KALI LINUX, es una distribución basada en el sistema operativo Debian, que se enfoca en auditorias de seguridad, análisis forense digital e ingeniería inversa (Offensive Security, 2013)

METADATOS, son datos que contienen información relativa a un documento o fichero concreto. Así, por ejemplo, un archivo de texto podría contener entre sus metadatos multitud de información relacionada con su procedencia, como datos sobre su autor, su fecha de creación y modificación, qué otros usuarios han manipulado el documento o el software utilizado para su redacción (Alonso, 2018, p. 15).

AMENAZA, en seguridad informática, se define como cualquier circunstancia o evento con el potencial de causar daño a un sistema informático (Governance & Standards División, 2017)

SISTEMA INFORMÁTICO, es la combinación de hardware, software y personal informático que permite procesar y almacenar la información digital

RIESGO, en el contexto de la seguridad informática, riesgo es la probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes, generando perdidas y daños (ISO 31000).

VULNERABILIDAD, es una debilidad, el cual puede ser atacado y usado como punto de entrada al sistema. (Oriyano, 2016).

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1. METOGOLOGÍA Y TÉCNICAS UTILIZADAS

3.1.1. Tipo de investigación

Aplicada, Debido a que busca la resolución de un problema de una empresa privada - Pucallpa. referente a la minimización de riesgos en sus sistemas informáticos.

3.1.2. Nivel de investigación

El nivel de la investigación será descriptivo, se efectuará una descripción de la población, el fenómeno o la situación que se encuentra alrededor del cual se centra el estudio. Se procura proporcionar información acerca del qué, cuando, como y donde, relativo al problema de investigación.

3.1.3. Diseño de la investigación

Se aplicará el método “Pre test – Post test” en la medición de la variable dependiente ante la aplicación de la variable independiente.

Se puede representar mediante la siguiente simbología:

Ecuación 1: Método “Pre test – Post test”.

GE: O1 -> X -> O2

Donde:

GE: Grupo Pre Experimental

O1: Datos de la Pre- Prueba para los indicadores de la variable dependiente antes de implementar el modelo de seguridad evaluando herramientas de hacking ético.

X: La implementación de un modelo de seguridad, evaluando herramientas de hacking ético = Estimulo o condición experimental.

O2: Datos de la Post- Prueba para los indicadores de la variable dependiente una vez implementado el modelo seguridad evaluando herramientas de hacking ético.

3.2. POBLACIÓN Y MUESTRA

Población

Para esta investigación, la población lo constituye todos los sistemas informáticos, que incluyen los operadores y software y hardware de la CLINICA AMERICANA SERFARMED - PUCALLPA, los cuales hacen un total de 25 entre computadoras, servidores, sistemas operativos y aplicaciones.

Muestra

Se opta por el muestreo no probabilístico, por conveniencia, siendo el tamaño de la muestra un total 25 (operadores y sistemas informáticos entre computadoras, sistemas operativos y data center).

3.3. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS.

Para el trabajo de recolección de información se utilizaron las siguientes técnicas:

ANÁLISIS DOCUMENTAL El análisis documental es una operación intelectual que da lugar a un subproducto o documento secundario que actúa como intermediario o instrumento de búsqueda obligado entre el documento original y el usuario que solicita información (Castillo, 2005).

ENCUESTA Es el método mediante el cual se define una relación intensiva y concreta entre los actores sociales o el hecho social y el investigador, de los que

se consiguen datos que pasan a ser sintetizados para desarrollar la investigación. (Fabbri, 2020).

Para la presente investigación se utilizaron los siguientes instrumentos:

ARCHIVO DIGITAL Documento que se revisan mediante una computadora con programas como Word, Excel, Repositorios, base de datos y otros que a comparación de los archivos físico permiten un acceso fácil para el análisis de la información.

CUESTIONARIO Es el tipo de encuesta que se lleva a cabo de manera escrita mediante un formato o instrumento el cual contiene una serie de preguntas. El cuestionario es autoadministrado ya que debe ser llenado solo por el encuestado, sin participación del encuestador.

Todo instrumento debe ser validado, es decir, debe ser evaluado y revisado en su metodología, diseño y contenido. Para la presente investigación, la validación del instrumento estará a cargo del juicio de expertos, luego de identificar la problemática existente, los objetivos y las variables que se desean medir, procederán a revisar el cuestionario, verificando que con su aplicación se podrán cumplir los objetivos definidos y elaborar la propuesta.

3.4. PROCESAMIENTO DE DATOS

Todo instrumento debe ser validado, es decir, debe ser evaluado y revisado en su metodología, diseño y contenido. Para la presente investigación, la validación del instrumento estará a cargo del juicio de expertos, luego de identificar la problemática existente, los objetivos y las variables que se desean medir,

procederán a revisar el cuestionario, verificando que con su aplicación se podrán cumplir los objetivos definidos y elaborar la propuesta.

Encuesta

Instrumento: **Cuestionario**

- **Ubicación**: La encuesta será realizada en las instalaciones de LA CLINICA AMERICANA SERFARMED. – Av. Sáenz Peña 165, Pucallpa – Departamento de Ucayali.
- **Recursos:** Para la recolección de datos se hará uso del cuestionario virtual.
- **Tiempo:** El cuestionario de preguntas se aplicará en 1 día, durante 1 hora, dándose inicio a las 3:00 pm, y finalizando a las 4:00 pm, por ser un horario de disponibilidad del personal, para comenzar luego con el procesamiento de datos.

El software que utilizara para la presente investigación es el IBM SPSS Statistics Base, Software de análisis estadístico que presenta las funciones principales necesarias para realizar el proceso analítico de principio a fin. Es fácil de utilizar e incluye un amplio rango de procedimientos y técnicas para ayudar a aumentar los ingresos, superar a la competencia, dirigir investigaciones y tomar mejores decisiones (IBM, 2015). Los datos obtenidos y su posterior procesamiento serán interpretados en: Tablas, figuras elaboradas en diagrama de barras, prueba de hipótesis, correlación de datos, Alfa de Cronbach, medias, varianzas.

3.5. TRATAMIENTO DE LOS DATOS

Análisis cuantitativo.

Se utilizarán tablas y cuadros estadísticos y herramientas con funciones estadísticas.

CAPÍTULO IV

IMPLEMENTACION DE LA SOLUCIÓN

4.1. LA EMPRESA

Nombre: CLINICA AMERICANA SERFARMED

MISION:

Empresa Prestadora de Servicios de Salud de mediana y alta complejidad, en el área Preventiva de Salud Ocupacional y Asistencial ofrecemos a nuestros clientes externos e internos atención humanizada, elevando nuestro servicio. Haciendo de sus necesidades y expectativas con altos estándares en nuestros servicios.

Con actitud de mejora continua e innovación con oportunidad, calidad, integralidad en la prestación de servicios, y con un talento humano idóneo, con espacialidades e infraestructura y tecnología de punta; ayudando a la satisfacción de las necesidades de salud de nuestros clientes y, garantizando la prevención, seguridad en la Salud, la calidad en el servicio y la conservación del medio ambiente.

Desarrollando nuestra imagen a nivel nacional e internacional y liderar en los servicios de medicina ocupacional, ambiental y asistencial, con una permanente proyección a la alta optimización de nuestros servicios.

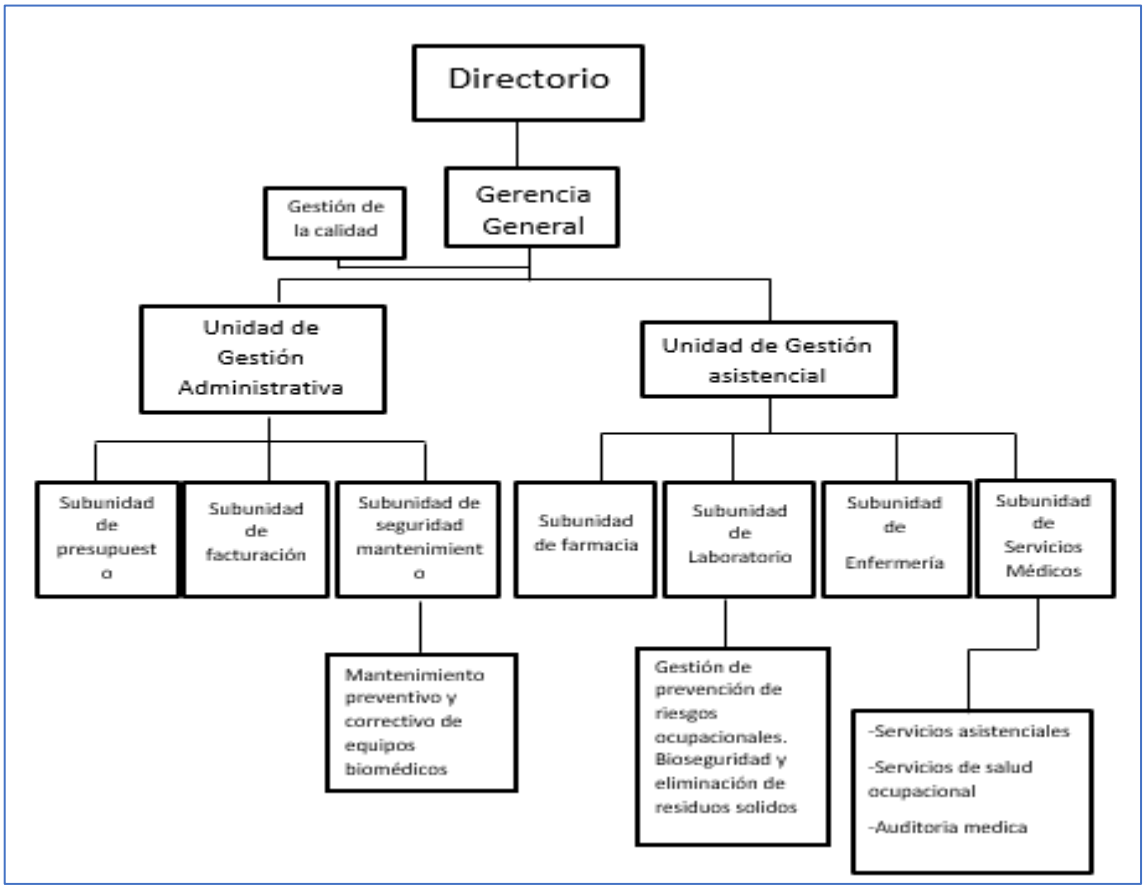
VISION:

Al 2024 La Clínica Americana. SERFARMED S.A. será un centro de referencia por su amplio portafolio de servicios de calidad, oportunidad y confianza en la atención a nuestros clientes en Prevención ,Salud Ocupacional Y asistencial y tener un posicionamiento a nivel nacional y

estará comprometida a desarrollar los servicios de salud preventiva ocupacional y asistencial, manteniendo altos estándares de calidad, seguridad, con el respeto y compromiso de protección del medio ambiente, y responsabilidad garantizando el manejo eficaz y eficiente de los servicios. Contando con un talento humano idóneo, infraestructura y tecnología de punta; desarrollando un impacto positivo contribuyente en el departamento. Estableciendo estos lineamientos como principio y valores para el sostenimiento de nuestra empresa.

ORGANIGRAMA

Figura 9: Organigrama



***Fuente**: (SERFARMED,2016)*

EQUIPOS DE COMPUTO – MARCAS, MODELOS

NUMERO DE COMPUTADORAS: 12 equipos

MARCA: COMPATIBLE.

MEMORIA RAM: 8GB

DISCO DURO: DISCO DE 240 GB

MODELO: SATA

Cuenta con el Software para Laboratorio Clínico – SIGLA

SOFTWARE Sistema SYSCOM

SOFTWARE(Plataforma) de SUSALUD

SISTEMA OPERATIVO: Windows 10

SERVIDOR – MARCA, MODELO

Modelo: HP PROLIANT ML350E GEN8 INTEL XEON E5-2407 1P

4.2. Ethical Hacking

La CLINICA AMERICANA SERFARMED, es una empresa que cuenta con equipamiento informático, sistemas de computado, equipo de comunicación; pero no cuenta con procedimientos , ni políticas de seguridad sobre estos sistemas, lo cual lo posiciona en una zona de riesgo donde la integridad, disponibilidad y confidencialidad se encuentra vulnerables; por lo cual, es de suma importancia que se implementes procedimientos y políticas de seguridad, con el fin de garantizar los procesos y activos de información.

Asimismo, el acceso a internet es la puerta mas frecuente para el ingreso de un sin número de amenazas, tales como: Malwares, virus, ataques DoS, etc. debido a ellos es imposible deshacerse de estas amenazas, pero si se puede mitigar su impacto a través de procedimientos y políticas de seguridad que los respalden.

A continuación, se muestran los elementos que forman parte de la seguridad informática:

Figura 10:Elementos de la Seguridad Informática



Fuente: (b-one-informatica,2016)

Confidencialidad. Sólo las personas autorizadas pueden acceder a los datos y a los activos de información. (Rish, 2020).

Integridad. Los datos deben estar intactos, ser precisos y completos, y los sistemas informáticos deben mantenerse operativos. (tutorialspoint, 2022).

Disponibilidad. Los usuarios deben poder acceder a la información o a los sistemas cuando lo necesiten. (exabeam, 2022).

Tabla 7.Confidencialidad, integridad y Disponibilidad.

	RIESGO	CONTROL
Confidencialidad	Perdida de privacidad Acceso no autorizado Hurto de identidad	Encriptación Autenticación Controlar accesos
Integridad	Información imprecisa, no confiable Fraude	Registros de auditoria
Disponibilidad	Paralización de procesos organizacionales	Copias de seguridad

Fuente: Elaboración propia

4.3. Fases del Ethical Hacking. (securitcrs, 2020)

Figura 11: Fases del Ethical Hacking



Fuente: (securitcrs,2015)

4.4. Desarrollo de fases.

Para la implementación del Ethical Hacking se aplicó la distribución de Linux denominada KALI LINUX.

Fase de Reconocimiento.

El objetivo de esta fase es recopilar la mayor cantidad de información posible a nivel técnico tales como: los sistemas, los dominios, metadatos y servicios.

Para el procedimiento de recopilación se hará uso del comando **Whois**.

```
root@admin: ~# whois serfarmed.com
Domain Name: serfarmed.com
WHOIS server: NIC .com
Sponsoring Registrar: NIC . com
Domain Status: ok
```

Para la recopilación de emails, hosts, a partir del dominio serfarmed.com se aplicará el comando **Harvester**.

```
root@admin: ~# theharvester – d serfarmed.com -l 300 -b all
```

Donde: -d: es el nombre del dominio, -l: Numero de resultados y -b: fuente de datos.

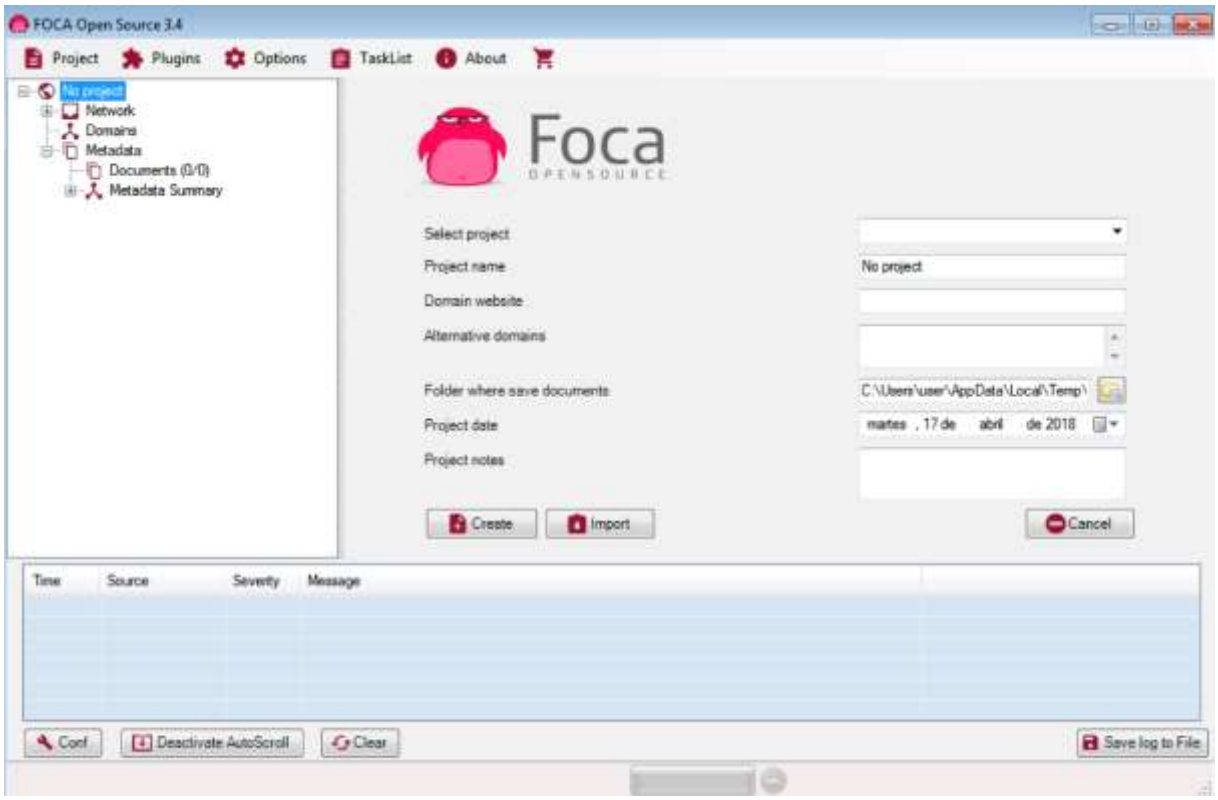
Se obtuvo como resultados 16 correos electrónicos, los cuales se muestran a continuación:

```
[+] Emails found:
aramirez@serfarmed.com
bpezo@serfarmed.com
erios@serfarmed.com
webmaster@serfarmed.com
mcachay@serfarmed.com
atapullima@serfarmed.com
…
```

Los dominios detectados fueron:

```
[-] Resolving hostsnames IPs…
Autoriscor.serfarmed.com: empty
Cpanel. .serfarmed.com:164.163.223.120
intranetlan.serfarmed.com: 204.96.120.68
serfarmed.com: 181.164.227.251
```

Para la identificación de metadatos se utilizó el software **FOCA**, a través del cual se idéntica: Documentos pdf, office, webs visitadas, buscadores utilizados llegando a determinar lo siguiente:


FOCA Open Source 3.4
Project
Plugins
Options
TaskList
About
No project
Network
Domains
Metadata
Documents (0/0)
Metadata Summary
Foca
OPENSOURCE
Select project
Project name
No project
Domain website
Alternative domains
Folder where save documents
C:\Users\user\AppData\Local\Temp\
Project date
martes , 17 de abril de 2018
Project notes
Create
Import
Cancel
Time
Source
Severity
Message
Conf
Deactivate AutoScroll
Clear
Save log to File

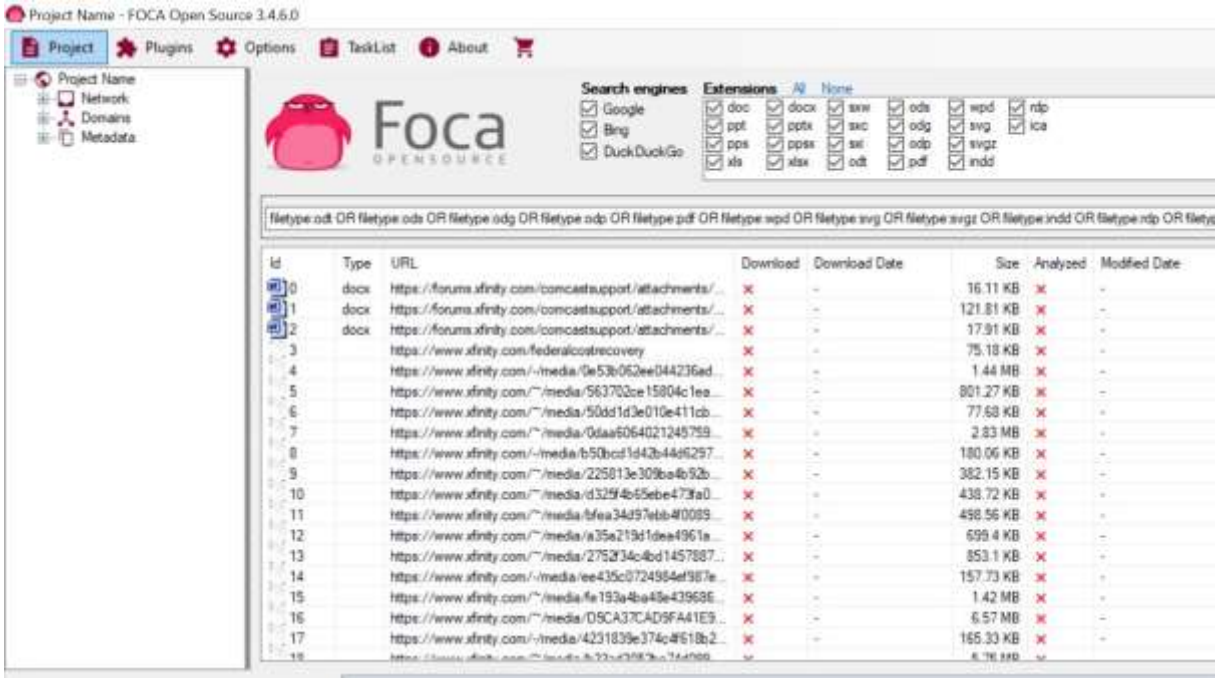

Project Name - FOCA Open Source 3.4.6.0
Project
Plugins
Options
TaskList
About
Project Name
Network
Domains
Metadata
Foca
OPENSOURCE
Search engines
Google
Bing
DuckDuckGo
Extensions
All
None
doc
docx
sxw
ods
wpd
rdp
ppt
pptx
sxc
odg
svg
ica
pps
ppsx
sxi
odp
svgz
xls
xlsx
odt
pdf
indd
filetype:odt OR filetype:ods OR filetype:odg OR filetype:odp OR filetype:pdf OR filetype:wpd OR filetype:svg OR filetype:svgz OR filetype:indd OR filetype:rdp OR filety
Id
Type
URL
Download
Download Date
Size
Analyzed
Modified Date
0 docx https://forums.xfinity.com/comcastsupport/attachments/... 16.11 KB
1 docx https://forums.xfinity.com/comcastsupport/attachments/... 121.81 KB
2 docx https://forums.xfinity.com/comcastsupport/attachments/... 17.91 KB
3 https://www.xfinity.com/federalcostrecovery 75.18 KB
4 https://www.xfinity.com/-/media/0e53b062ee044236ad... 1.44 MB
5 https://www.xfinity.com/~/media/563702ce15804c1ea... 801.27 KB
6 https://www.xfinity.com/~/media/50dd1d3e010e411cb... 77.68 KB
7 https://www.xfinity.com/~/media/0daa606402124575 9... 2.83 MB
8 https://www.xfinity.com/-/media/b50bcd1d42b44d6297... 180.06 KB
9 https://www.xfinity.com/~/media/225813e309ba4b92b... 382.15 KB
10 https://www.xfinity.com/~/media/d329f4b65ebe473fa0... 438.72 KB
11 https://www.xfinity.com/~/media/bfea34d97ebb4f0089... 498.56 KB
12 https://www.xfinity.com/~/media/a35a219d1dea4961a... 699.4 KB
13 https://www.xfinity.com/~/media/2752f34c4bd1457887... 853.1 KB
14 https://www.xfinity.com/-/media/ee435c0724984ef987e... 157.73 KB
15 https://www.xfinity.com/~/media/fe193a4ba43e439686... 1.42 MB
16 https://www.xfinity.com/~/media/D5CA37CAD9FA41E9... 6.57 MB
17 https://www.xfinity.com/-/media/4231839e374c4f618b2... 165.33 KB

Tabla 8.Cantidad de Información por tipo

Tipo	Cantidad
Documentos descargados	389
Nombres de usuarios	19
Software	25
Impresoras	03

Fuente: Elaboración propia

Para identificas los servicios que accedieron los equipos conectados a internet y los sitios web visitados, se utilizó la herramienta **ZoomEye,**



Obteniéndose los siguiente:

Tabla 9.Servicios identificados

Tipo	Nombre	Url
Web	phpMyAdmin	https://www.serfarmed.com/phpmyadmin
Contenedor	Apache	
Modulo	PHP	
Base de datos	MySQL	
S.O	Centos	

Fuente: Elaboración propia

Fase de escaneo.

Para el monitoreo del funcionamiento de la red se efectuó el escaneo del protocolo de mensajes de Internet – ICMP, donde se identificó hosts activos. La herramienta utilizada fue el Angry IP Scanner, a través del cual se obtuvo la siguiente información:



Fuente: (linuxsecrets,2019)

Hosts Escaneados	Hosts Activos
22	20

Fuente: Procedimiento del autor

Para obtener información de los hosts que se encuentran activos y disponibles, los servicios, el tipo de sistemas operativos, los puertos abiertos, etc. se hizo uso de **Nmap (Network Mapper) – Zenmap,** con la información recopilada, se efectuó la indagación del SO del servidor, obteniendo lo siguiente:

Nmap –O 192.168.0.10

Running: Microsoft Windows 2016 R2

El análisis de los paquetes enviados tiene como finalidad determinar que paquetes son enviados junto con URG, PSH y FIN. Los paquetes RST son correspondidos por

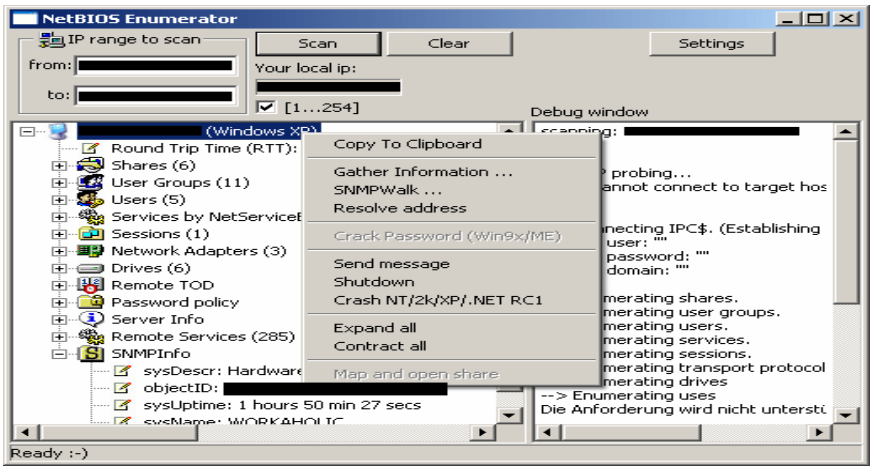
puertos cerrados. FLAGS es el valor en forma de señal para un proceso. Para lograra este análisis se efectuó el escaneo con **Xmax** a la Ip del servidor.

```
root@admin: ~# nmap -sX -T4 192.168.0.10
Starting Nmap 7.71 ( https://nmap.org ) at 2022-08-222 14:32 EDT
Nmap scan report for serv1. Serfarmed.red (192.168.0.10)
Host is up (0.00031s latency)
All 1000 scanned ports on serv1. Serfarmed.red (192.168.0.10) are closed
MAC Address: 3ª:25:6C:64:F1:67 (Hp Proliant)
```

Fase de Acceso.

En esta etapa se efectúa las conexiones activas sobre el sistema, para recabar información de las terminales, usuarios, grupos, recursos compartidos, etc.

Para obtener la lista de equipos (computadoras personales) que son parte del dominio y la información de los recursos que estos comparten, se utilizó la herramienta **NetBIOS Enumerator**.



A través del comando Nbtscan de Kali linux se muestra información de la tabla de netbios del servidor Serv1.

```
root@admin: nbtscan -v -r 192.168.0.10
Doing NBT name scan for addresses from 192.168.0.10

NetBIOS Name Table for Host 192.168.0.10

Incomplete packet, 164 bytes long.
Name            Service         Type
-----------------------------------------------
SERV1           <00>            UNIQUE
SERFARMED       <00>            GROUP
…
```

Fase manteniendo acceso.

Fase limpiando huellas.

El siguiente paso es obtener información sobre las tablas de nombres NetBios, cache de nombres, etc.

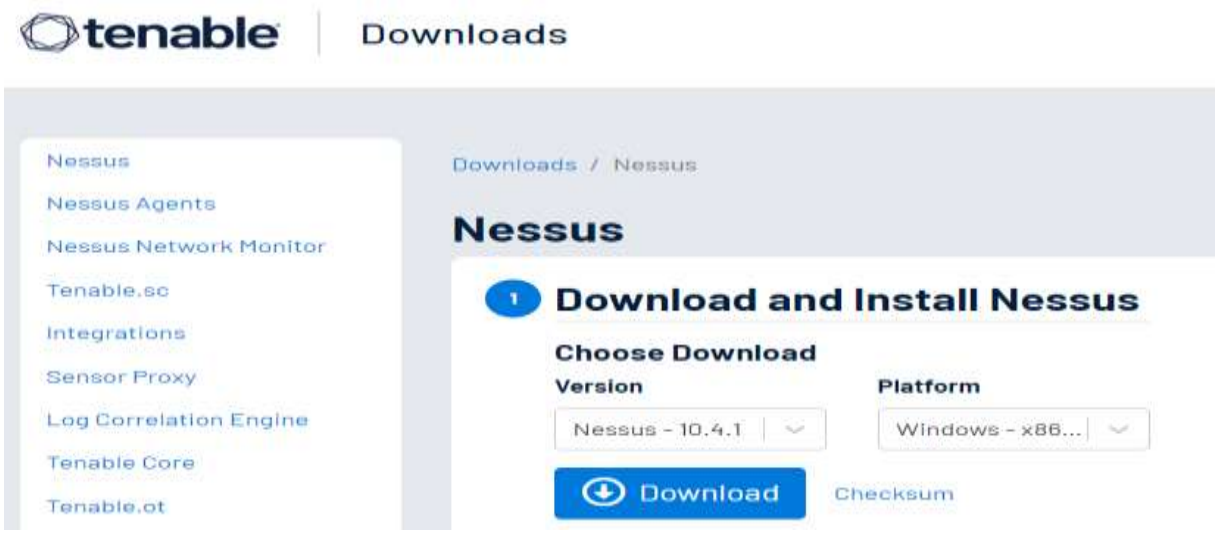
```
Nbstat -A 192.168.0.10
```

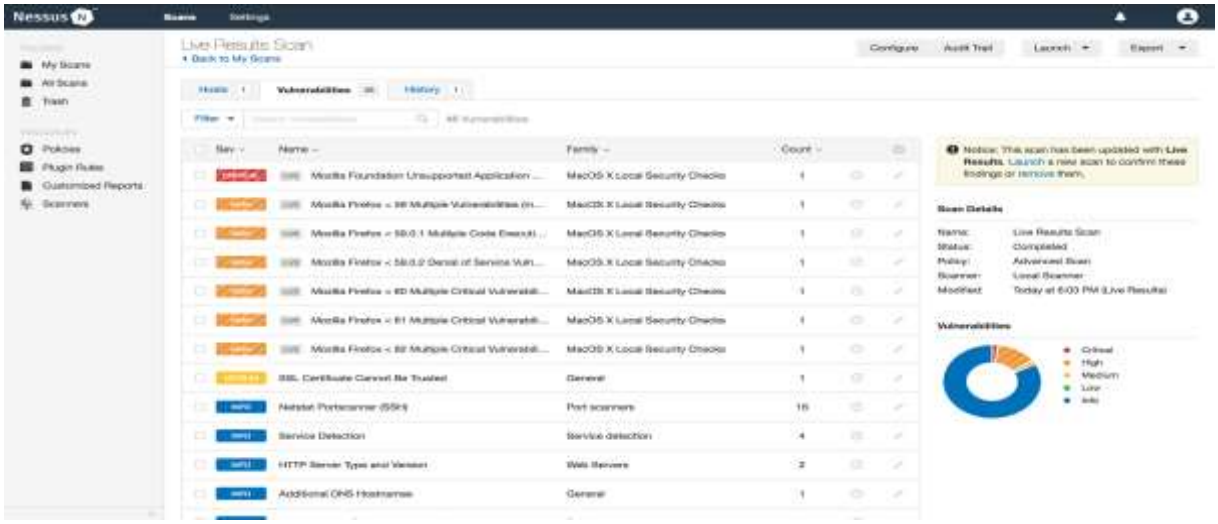
Para la enumeración de información sobre los dispositivos, impresoras, hardware que soporten protocolo SNMP se utiliza el comando nmap sobre el puerto UDP 161.

```
root@admin:  nmap 192.168.0.22 -Pn 161 -sV
```

Fase de Análisis de vulnerabilidades.

Se pretende identificad los puntos débiles de las aplicaciones y sistemas, con la finalidad de cuantificar el nivel de seguridad actual que pueda hacer frente a ataques de hackeo o fallas. Este análisis permite reducir el impacto sobre falencias del sistema. La herramienta Nessus, nos permitió determinar que vulnerabilidades existen en la red, detectando agujeros en los servidores y las computadoras personales (Tenable.com, s/f).





Después de ejecutar el programa obtuvieron datos, y a continuación se muestra una parte:

Tabla 10.Vulnerabilidades encontradas

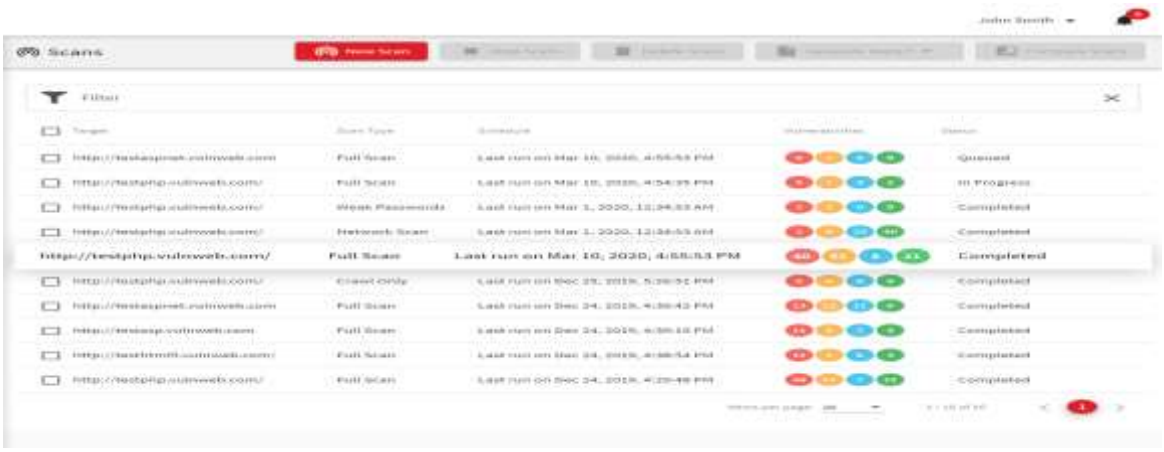
Host	IP	SO	Vulnerabilidad	Riego	Descripción
Pc020	192.1680.20	W10	DNS Serve Cache Snooping	Medio	DNS responde a consultas del exterior.
			SSL Certificate Cannot Be Trusted	Medio	Certificado gratuito, SSL
Pc021	192.1680.21	W10	DNS Serve Cache Snooping	Medio	DNS responde a consultas del exterior.
			SSL Certificate Cannot Be Trusted	Medio	Certificado gratuito, SSL
Pc022	192.1680.22	W10	Network Time Protocol (NTP) Mode 6 Scanner	Medio	El NTP remote atiende a las peticiones del modo 6. Los equipos que generan respuesta son utilizados en ataques de amplificación.
Pc023	192.1680.23	W10	PHP Unsupported Version Detection	Critico	Versión PHP desactualizado

			HTTP TRACE / TRACK Methods Allowed	Medio	El servidor es compatible con los métodos TRACE y/o TRACK. TRACE - HTTP para la depuración errores
			SSH Weak Algorithms Supported	Medio	El host tiene una vulnerabilidad de divulgación de información (man-in-the-middle), por el error del algoritmo de cifrado RC4.
			SNMP Agent Default Community Name (public)	Medio	El SNMP este servicio no debe estar expuesto si no se hace uso de SNMP.
Pc024	192.1680.24	W10	HTTP TRACE / TRACK Methods Allowed	Medio	El servidor compatible con los métodos TRACE y/o TRACK. TRACE y TRACK
			SNMP 'GETBULK' Reflection DDoS	Medio	El servicio SNMP responde con una gran cantidad de datos a unas solicitudes de 'GETBULK'

Para realizar la evaluación de vulnerabilidades que puede presentar problemas en la red, equipos, aplicación se utilizó el software OpenVAS



Para efectuar pruebas de seguridad de aplicaciones web se utilizó la herramienta Acunetix.



Fase de Hacking del Sistema.

Los exploits DoublePulsar y EternalBlue se aprovechan de las vulnerabilidades del protocolo SMB v1 el mismo que se ejecuta en los puertos TCP 139 y 445, A continuación, se muestran los pasos a seguir:

1. Escanear puertos con nmap y verificar si están abiertos.
2. Para buscar el scanner que detecta la vulverabilidad SMB se hace a través de Metasploit Framework.
3. Seleccionar el scanner y enviar a la dirección IP del equipo, y verificar si posee vulnerabilidad.
4. Si el host es vulnerable, se aplica DoublePulsar y EternalBlue
5. Se envía el exploit a la dirección IP de la víctima y luego enviar el payload.
6. Se ejecuto el exploit para crear la sesión en Meterpreter. Y si el exploit se ejecutó correctamente se puede ejecutar código remoto al sistema hackeado.
7. Elevar los privilegios de usuario: getsystem
8. Habilitar la opción “kiwi”, que permitirá extraer las contraseñas
9. Extraer contraseña con: creds all
10. Interactuar con el CMD
11. Enviar el ransomware WannaCry.

Gestión de Riesgo

Un riego en informática viene a ser la probabilidad que se presente una amenaza, valiéndose de una vulnerabilidad, esto al final producir un impacto sobre el sistema.

Para poder ejecutar la gestión de riesgo, se tuvieron que identificas y clasificar los activos informáticos más importantes, cuyo detalle se muestra a continuación:

Tabla 11.Gestión de Riesgo

Activo	Descripción	Tipología		Clasificación		
		Software	Hardware	Importancia		
				Bajo	Medio	Alto
Pcs	Computadoras Personales de escritorio		X			X
Equipos de redes	Equipos de comunicaciones y redes, switch, hubs, router		X			X
Servidor BD	Contiene el gestor de base de datos y la información de la misma.	X				X
Servidor DNS	Servidor de resolución de nombres	X				X
Servidor Proxy	Servidor gestión de accesos a la red	X			X	
Portal Web	Portal institucional	X			X	
SO	Sistemas Operativos	X				X

Amenazas y Vulnerabilidades

Tabla 12.Amenazas y Vulnerabilidades

Ide Riego	Amenaza	Vulnerabilidad	Descripción
R01	Movimientos Telúricos	Carencia de un plan de contingencia	Al producirse la amenaza existe la probabilidad que los equipos y sistemas de información sean perjudicados.
R02	Uso de medios De almacenamiento externos	No existen mecanismo de bloque	Los dispositivos de almacenamiento portátil, pueden estar infectados con software malicioso.
R03	Divulgación de Información confidencial	Carecían de mecanismos de seguridad contra el envío de	La información enviada puede ser información crítica de la organización.

		información a través de correos electrónicos. No existen mecanismos para la encriptación de información.	Al no estar cifrado la información enviada es vulnerable.
R04	Ausencia en Políticas de Seguridad	Carencia de SGSI	El SGSI asegura a través de políticas y procedimientos la información crítica.
		No se aplican procedimiento de Ethical Hacking	Se podría detectar falencias sobre los sistemas informáticos.
R05	Falta de monitoreo en os equipos informáticos	Carencia de baterías externas	Si se produce un corte de fluido electico los equipos son impactados de forma negativa.
		Lentitud en el funcionamiento de los equipos	La falta de mantenimiento provoca mal funcionamiento de los componentes.
R06	Software sin actualización	Carencia de parches de seguridad	La actualización de los softwares garantiza la seguridad de los mismo y de la información.
R07	Accesos no autorizados	Carencia de acceso biométrico	El acceso a los puntos críticos de informática es vulnerable por que únicamente se cuenta con una puerta simple, sin controles
		Carencia de cámaras de video.	No se posee registro en video de los ingresos a los puntos críticos.
R09	Mala Configuración del sistema	Firewall inoperativo	Se encuentra expuesto a potenciales amenazas.
		DNS Cache Snooping	El servidor no posee el bit de recursividad.
		SSL verdadero	Es auto firmado y por lo tanto es vulnerable
		Algoritmo débil SSH	El sistema actual RC4 es muy inseguro

Amenazas y Vulnerabilidades

Para el cálculo del nivel de riego se utiliza la siguiente forma:

Riego = Amenaza*Vulnerabilidad.

La escala de evaluación se detalla en la tabla siguiente:

Tabla 13.Escala de evaluación

Valores			Descripción
Cualitativos	**Cuantitativos**		
Muy Malo	96-100	10	Amenaza produce varios efectos negativos.
Alto	80 - 95	8	Se podría esperar un efecto negativo
Moderado	21 - 79	5	Se puede esperar la amenaza con efecto grave.
Bajo	5 - 20	2	Efecto adverso limitado
Muy Bajo	0 - 4	0	Riesgo insignificante

Riesgos analizados (amenazas - vulnerabilidades)

Tabla 14.Riesgos Analizados

Ide Riego	Amenaza	Vulnerabilidad	Probabilidad Amenaza	Probabilidad Vulnerabilidad	Nivel Riesgo
R01	Movimientos Telúricos	Carencia de un plan de contingencia	Bajo	Mul Alto	Bajo
R02	Uso de medios De almacenamiento externos	No existen mecanismo de bloque	Alto	Moderado	Moderado
R03	Divulgación de Información confidencial	Carecían de mecanismos de seguridad contra el envío de información a través de correos electrónicos. No existen mecanismos para la encriptación de información.	Alto	Muy Alto	Alto
R04	Ausencia en Políticas de Seguridad	Carencia de SGSI	Alto	Muy Alto	Alto
		No se aplican procedimiento de Ethical Hacking	Alto	Muy Alto	Alto
R05	Falta de monitoreo en os equipos informáticos	Carencia de baterías externas	Alto	Alto	Moderado
		Lentitud en el funcionamiento de los equipos	Alto	Moderado	Moderado
R06	Software sin actualización	Carencia de parches de seguridad	Alto	Muy Alto	Alto
R07	Accesos no autorizados	Carencia de acceso biométrico	Moderado	Moderado	Moderado
		Carencia de cámaras de video.	Moderado	Bajo	Bajo
R08	Mala Configuración del sistema	Firewall inoperativo	Alto	Muy Alto	Alto
		DNS Cache Snooping	Alto	Moderado	Moderado
		SSL verdadero	Alto	Moderado	Moderado
		Algoritmo débil SSH	Alto	Moderado	Moderado

Mecanismos de protección – mitigación de riesgos.

Para evaluar la mitigación nos basamos en 04 posibilidades: Asumir, Se acepta el riego; Evitar: Elimina la causa; Reducir; Instalación de controles; Transferir: Aplicar otra alternativa

Tabla 15.Mecanismos de protección.

Ide Riego	Amenaza	Vulnerabilidad	Protección	Estrategia
R01	Movimientos Telúricos	Carencia de un plan de contingencia	Implementar backups	ASUMIR
R02	Uso de medios De almacenamien to externos	No existen mecanismo de bloque	Implementar políticas GPO	REDUCIR
R03	Divulgación de Información confidencial	Carecían de mecanismos de seguridad contra el envío de información a través de correos electrónicos. No existen mecanismos para la encriptación de información.	Implementar filtro ya sea con software o físico	REDUCIR
R04	Ausencia en Políticas de Seguridad	Carencia de SGSI	Implementar SGSI	REDUCIR
		No se aplican procedimiento de Ethical Hacking	Aplicar mecanismo de Ciberseguridad	REDUCIR
R05	Falta de monitoreo en os equipos informáticos	Carencia de baterías externas	Implementar UPS,	REDUCIR
		Lentitud en el funcionamiento de los equipos	Mantenimiento continuo	REDUCIR
R06	Software sin actualización	Carencia de parches de seguridad	Wsus	REDUCIR
R07	Accesos no autorizados	Carencia de acceso biométrico	Implementar dispositivo	REDUCIR
		Carencia de cámaras de video.	Implementar video vigilancia	REDUCIR
R08	Mala Configuración del sistema	Firewall inoperativo	Activar y actualizar	REDUCIR
		DNS Cache Snooping	Deshabilitar	REDUCIR
		SSL verdadero	Adquirir SSL	REDUCIR
		Algoritmo débil SSH	Eliminas algoritmo RC4	REDUCIR

CAPÍTULO V

RESULTADOS Y DISCUSIÓN

INTERPRETACIÓN DE RESULTADOS PRE TEST

PREG1

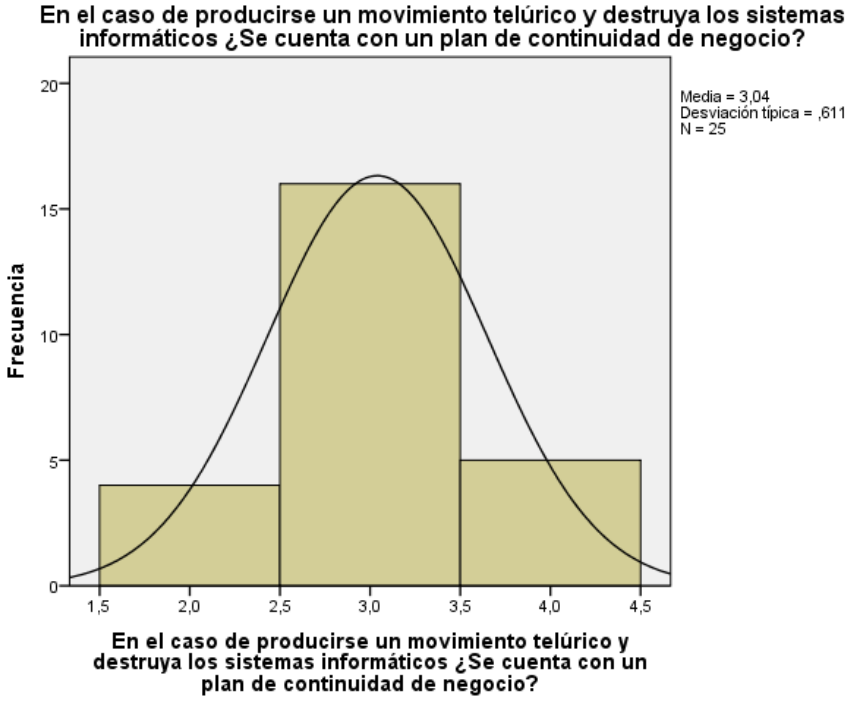
Tabla 16. ***Análisis de Frecuencia PREG1***

En el caso de producirse un movimiento telúrico y destruya los sistemas informáticos ¿Se cuenta con un plan de continuidad de negocio?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Casi Nunca	4	16,0	16,0	16,0
	A veces	16	64,0	64,0	80,0
	Casi Siempre	5	20,0	20,0	100,0
	Total	25	100,0	100,0	

Fuente: IBM SPSS

Figura 12. ***Análisis de Frecuencia PREG01***



Fuente: IBM SPSS

Interpretación de gráfico: De acuerdo a la percepción de los encuestados el 16.0% etiqueta casi nunca, el 64% etiqueta A veces y el 20% etiqueta Casi Siempre.

PREG2

*Tabla 17.**Análisis de Frecuencia PREG2***

¿Los puertos USB están activados en las computadoras?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Nunca	2	8,0	8,0	8,0
	Casi Nunca	10	40,0	40,0	48,0
	A veces	9	36,0	36,0	84,0
	Casi Siempre	4	16,0	16,0	100,0
	Total	25	100,0	100,0	

Fuente: IBM SPSS

*Figura 13.**Análisis de Frecuencia PREG02***



Fuente: IBM SPSS

Interpretación de gráfico: De acuerdo a la percepción de los encuestados el 8.0% etiqueta nunca, el 40% etiqueta Casi Nunca, el 36% etiqueta A veces, y el 16% etiqueta Casi Siempre.

PREG3

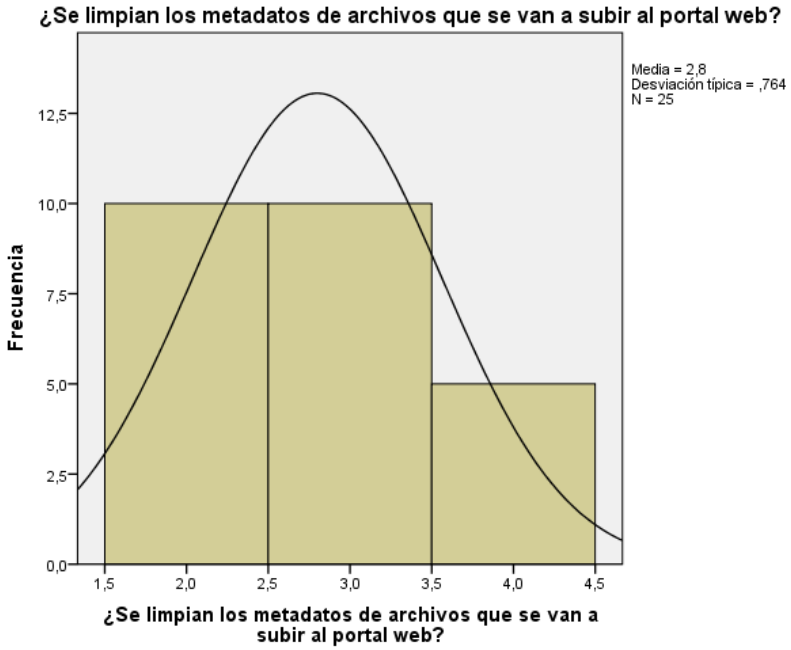
*Tabla 18.**Análisis de Frecuencia PREG3***

¿Se limpian los metadatos de archivos que se van a subir al portal web?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Casi Nunca	10	40,0	40,0	40,0
	A veces	10	40,0	40,0	80,0
	Casi Siempre	5	20,0	20,0	100,0
	Total	25	100,0	100,0	

Fuente: IBM SPSS

*Figura 14.**Análisis de Frecuencia PREG03***



Fuente: IBM SPSS

Interpretación de gráfico: De acuerdo a la percepción de los encuestados el 40.0% etiqueta Casi Nunca, el 40% etiqueta A veces, y el 20% etiqueta Casi Siempre.

PREG4

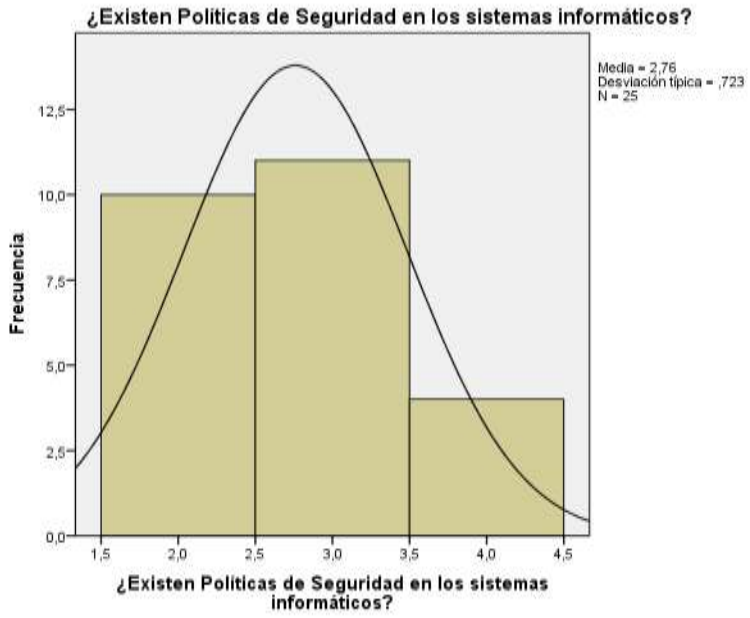
*Tabla 19.**Análisis de Frecuencia PREG4***

¿Existen Políticas de Seguridad en los sistemas informáticos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Casi Nunca	10	40,0	40,0	40,0
	A veces	11	44,0	44,0	84,0
	Casi Siempre	4	16,0	16,0	100,0
	Total	25	100,0	100,0	

Fuente: IBM SPSS

*Figura 15.**Análisis de Frecuencia PREG04***



Fuente: IBM SPSS

Interpretación de gráfico: De acuerdo a la percepción de los encuestados el 40.0% etiqueta Casi Nunca, el 44% etiqueta A veces, y el 16% etiqueta Casi Siempre.

PREG05

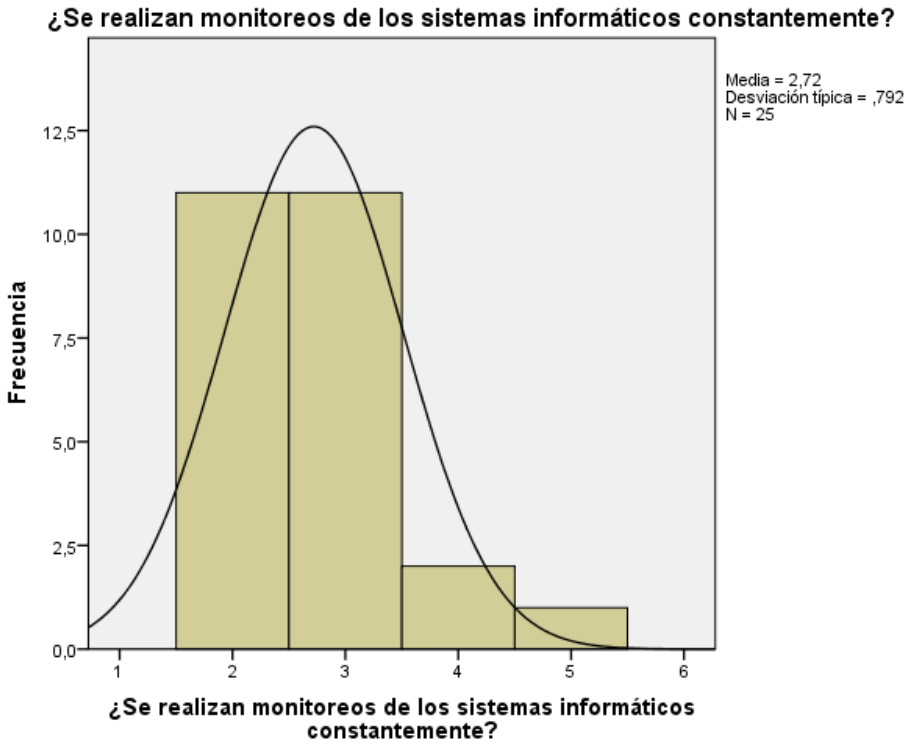
*Tabla 20.**Análisis de Frecuencia PREG05***

¿Se realizan monitoreos de los sistemas informáticos constantemente?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Casi Nunca	11	44,0	44,0	44,0
	A veces	11	44,0	44,0	88,0
	Casi Siempre	2	8,0	8,0	96,0
	Siempre	1	4,0	4,0	100,0
	Total	25	100,0	100,0	

Fuente: IBM SPSS

*Figura 16.**Análisis de Frecuencia PREG05***



Fuente: IBM SPSS

Interpretación de gráfico: De acuerdo a la percepción de los encuestados el 44.0% etiqueta Casi Nunca, el 44% etiqueta A veces, el 8% etiqueta Casi Siempre y el 4% etiqueta Siempre.

PREG6

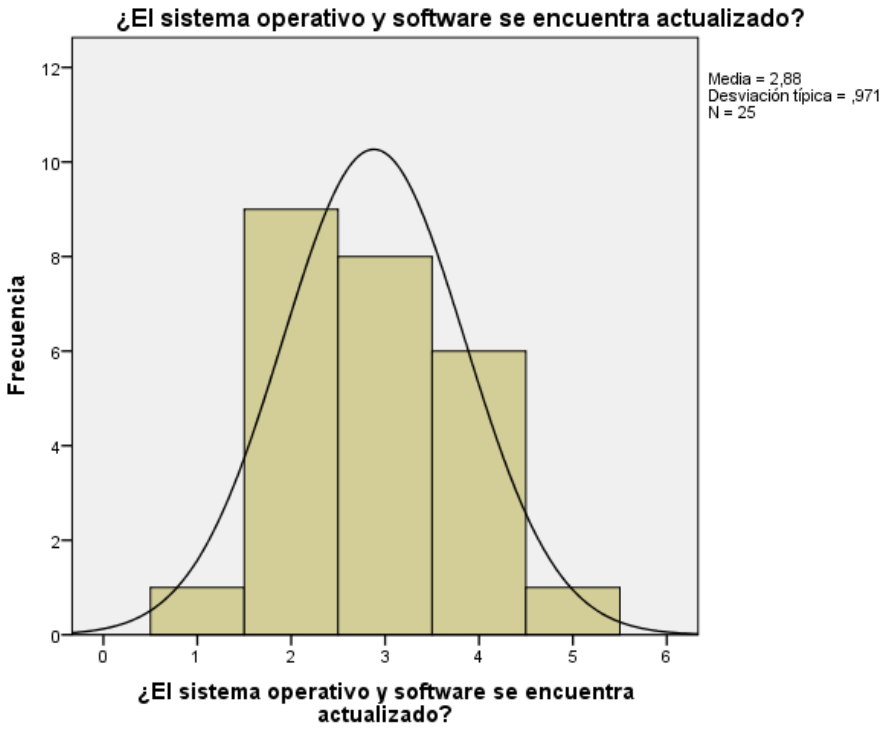
*Tabla 21.**Análisis de Frecuencia PREG6***

¿El sistema operativo y software se encuentra actualizado?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Nunca	1	4,0	4,0	4,0
	Casi Nunca	9	36,0	36,0	40,0
	A veces	8	32,0	32,0	72,0
	Casi Siempre	6	24,0	24,0	96,0
	Siempre	1	4,0	4,0	100,0
	Total	25	100,0	100,0	

Fuente: IBM SPSS

*Figura 17.**Análisis de Frecuencia PREG06***



Fuente: IBM SPSS

Interpretación de gráfico: De acuerdo a la percepción de los encuestados el 4.0% etiqueta Nunca, el 36% etiqueta Casi Nunca, el 32% etiqueta A veces y el 24% etiqueta Casi Siempre y el 4% etiqueta Siempre.

PREG07

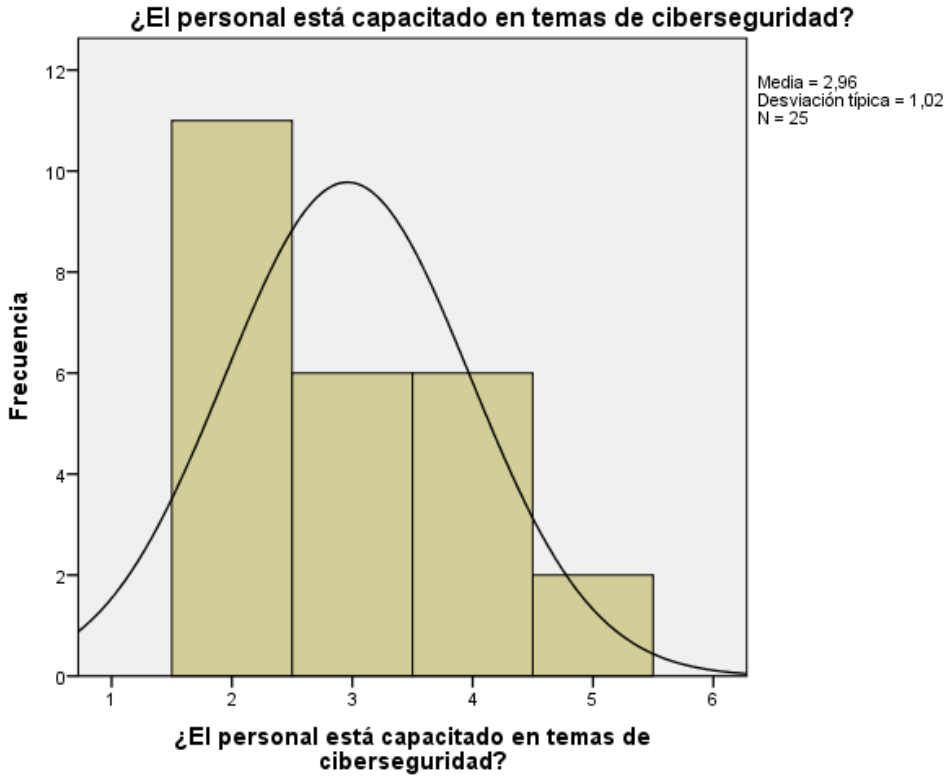
*Tabla 22.**Análisis de Frecuencia PREG07***

¿El personal está capacitado en temas de ciberseguridad?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Casi Nunca	11	44,0	44,0	44,0
	A veces	6	24,0	24,0	68,0
	Casi Siempre	6	24,0	24,0	92,0
	Siempre	2	8,0	8,0	100,0
	Total	25	100,0	100,0	

Fuente: IBM SPSS

*Figura 18.**Análisis de Frecuencia PREG07***



Fuente: IBM SPSS

Interpretación de gráfico: De acuerdo a la percepción de los encuestados el 44.0% etiqueta Casi Nunca, el 24% etiqueta A veces, el 24% etiqueta Casi Siempre y el 8% etiqueta Siempre.

PREG08

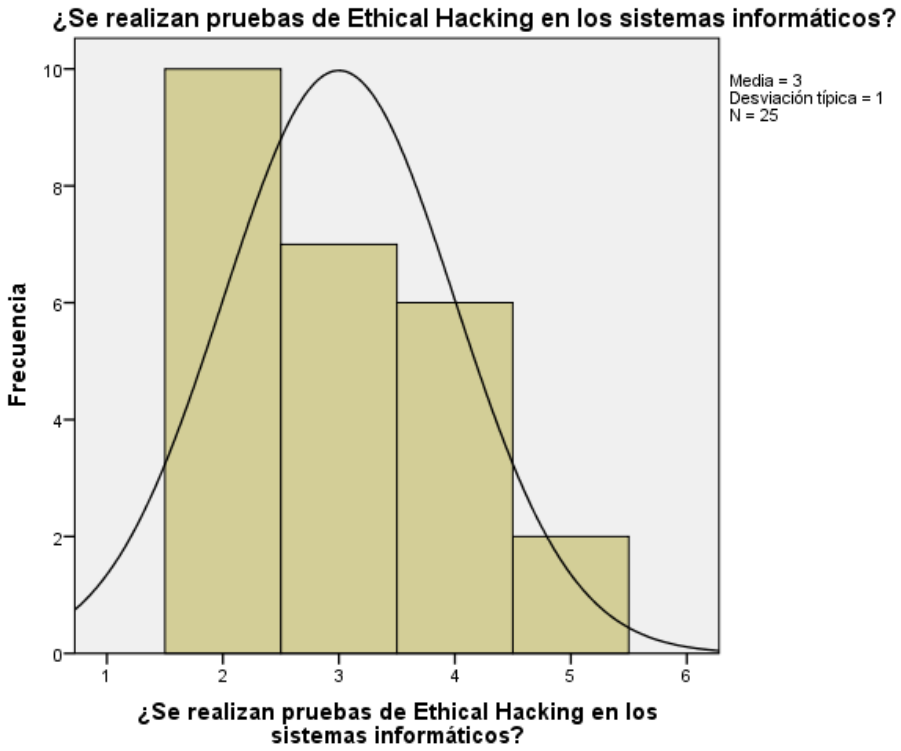
Tabla 23. ***Análisis de Frecuencia PREG08***

¿Se realizan pruebas de Ethical Hacking en los sistemas informáticos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Casi Nunca	10	40,0	40,0	40,0
	A veces	7	28,0	28,0	68,0
	Casi Siempre	6	24,0	24,0	92,0
	Siempre	2	8,0	8,0	100,0
	Total	25	100,0	100,0	

Fuente: IBM SPSS

Figura 19. ***Análisis de Frecuencia PREG08***



Fuente: IBM SPSS

Interpretación de gráfico: De acuerdo a la percepción de los encuestados el 40.0% etiqueta Casi Nunca, el 28% etiqueta A veces, el 24% etiqueta Casi Siempre y el 8% etiqueta Siempre.

PREG09

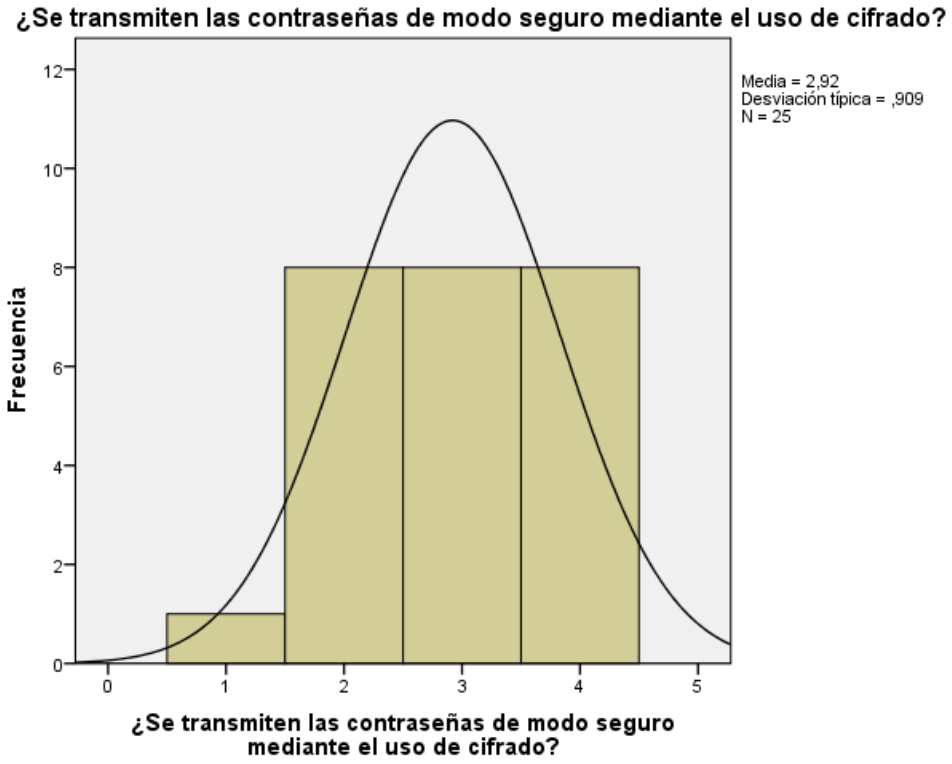
*Tabla 24.**Análisis de Frecuencia PREG09***

¿Se transmiten las contraseñas de modo seguro mediante el uso de cifrado?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Nunca	1	4,0	4,0	4,0
	Casi Nunca	8	32,0	32,0	36,0
	A veces	8	32,0	32,0	68,0
	Casi Siempre	8	32,0	32,0	100,0
	Total	25	100,0	100,0	

Fuente: IBM SPSS

*Figura 20.**Análisis de Frecuencia PREG09***



Fuente: IBM SPSS

Interpretación de gráfico: De acuerdo a la percepción de los encuestados el 4.0% etiqueta Nunca, el 32% etiqueta Casi Nunca, el 32% etiqueta A veces y el 32% etiqueta Casi Siempre.

PREG10

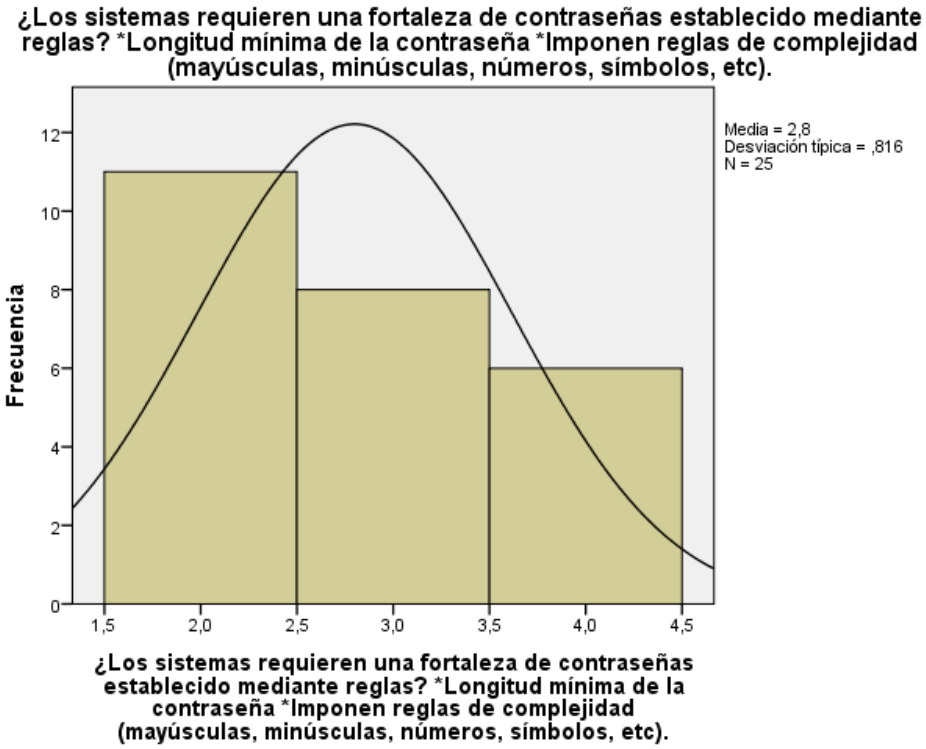
*Tabla 25.**Análisis de Frecuencia PREG10***

¿Los sistemas requieren una fortaleza de contraseñas establecido mediante reglas? *Longitud mínima de la contraseña *Imponen reglas de complejidad (mayúsculas, minúsculas, números, símbolos, etc).

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Casi Nunca	11	44,0	44,0	44,0
	A veces	8	32,0	32,0	76,0
	Casi Siempre	6	24,0	24,0	100,0
	Total	25	100,0	100,0	

Fuente: IBM SPSS

*Figura 21.**Análisis de Frecuencia PREG10***



Fuente: IBM SPSS

Interpretación de figura: De acuerdo a la percepción de los encuestados el 44.0% etiqueta Casi Nunca, el 32% etiqueta A veces, y el 24% etiqueta Casi Siempre.

PREG11

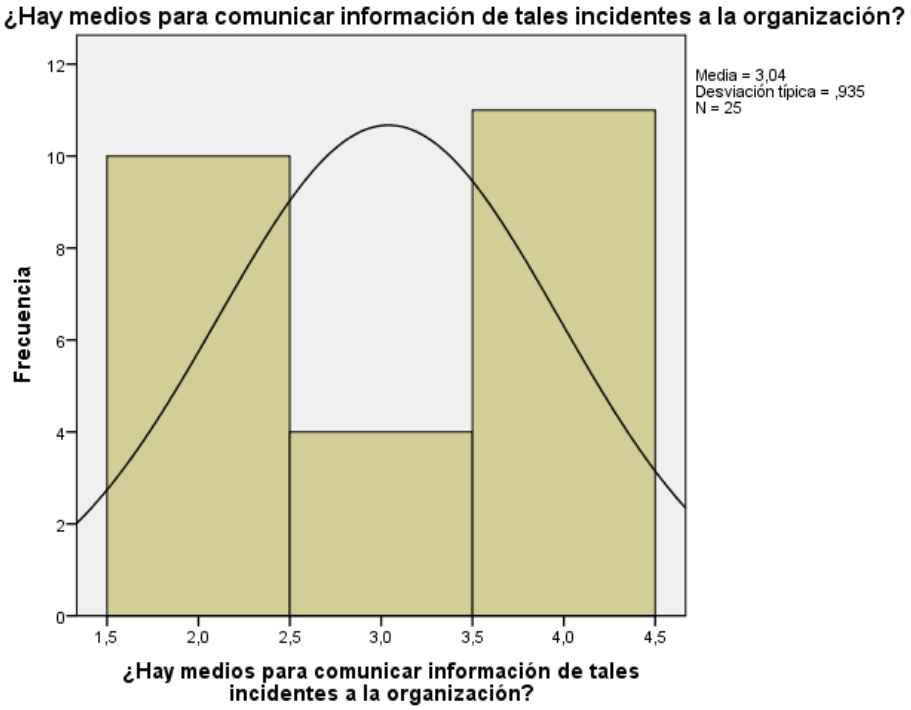
*Tabla 26.**Análisis de Frecuencia PREG11***

¿Hay medios para comunicar información de tales incidentes a la organización?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Casi Nunca	10	40,0	40,0	40,0
	A veces	4	16,0	16,0	56,0
	Casi Siempre	11	44,0	44,0	100,0
	Total	25	100,0	100,0	

Fuente: IBM SPSS

*Figura 22.**Análisis de Frecuencia PREG11***



Fuente: IBM SPSS

Interpretación de gráfico: De acuerdo a la percepción de los encuestados el 40.0% etiqueta Casi Nunca, el 16% etiqueta A veces, y el 44% etiqueta Casi Siempre.

INTERPRETACIÓN DE RESULTADOS POST TEST

PREG01

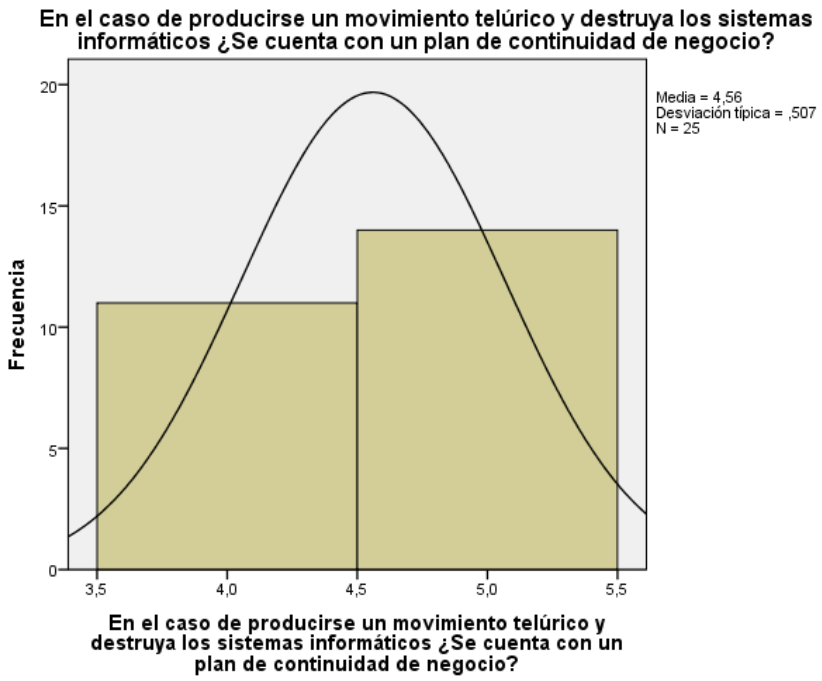
Tabla 27. ***Análisis de Frecuencia PREG01***

En el caso de producirse un movimiento telúrico y destruya los sistemas informáticos ¿Se cuenta con un plan de continuidad de negocio?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Casi Siempre	11	44,0	44,0	44,0
	Siempre	14	56,0	56,0	100,0
	Total	25	100,0	100,0	

Fuente: IBM SPSS

Figura 23. ***Análisis de Frecuencia PREG01***



Fuente: IBM SPSS

Interpretación de gráfico: De acuerdo a la percepción de los encuestados el 44.0% etiqueta Casi Siempre, y el 56% etiqueta Siempre.

PREG02

*Tabla 28.**Análisis de Frecuencia PREG02***

¿Los puertos USB están activados en las computadoras?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	A veces	1	4,0	4,0	4,0
	Casi Siempre	15	60,0	60,0	64,0
	Siempre	9	36,0	36,0	100,0
	Total	25	100,0	100,0	

Fuente: IBM SPSS

*Figura 24.**Análisis de Frecuencia PREG02***



Fuente: IBM SPSS

Interpretación de gráfico: De acuerdo a la percepción de los encuestados el 4.0% etiqueta A veces, el 60% etiqueta Casi Siempre y el 9% Siempre.

PREG03

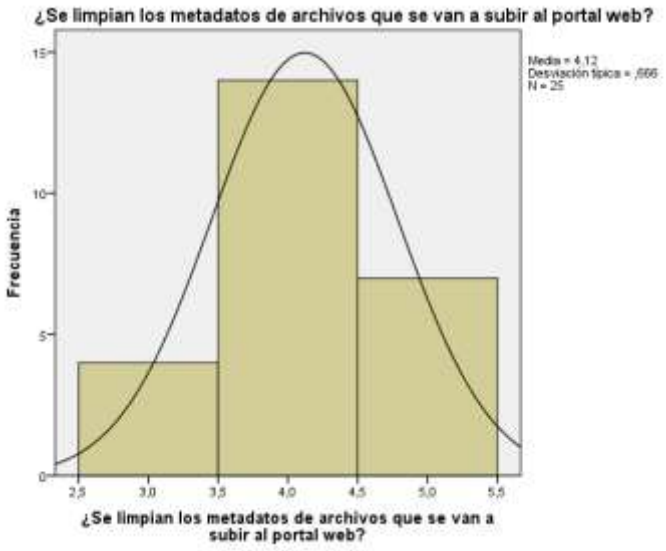
*Tabla 29.**Análisis de Frecuencia PREG03***

¿Se limpian los metadatos de archivos que se van a subir al portal web?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	A veces	4	16,0	16,0	16,0
	Casi Siempre	14	56,0	56,0	72,0
	Siempre	7	28,0	28,0	100,0
	Total	25	100,0	100,0	

Fuente: IBM SPSS

*Figura 25.**Análisis de Frecuencia PREG03***



Fuente: IBM SPSS

Interpretación de gráfico: De acuerdo a la percepción de los encuestados el 16.0% etiqueta A veces, el 56% etiqueta Casi Siempre y el 28% Siempre.

PREG04

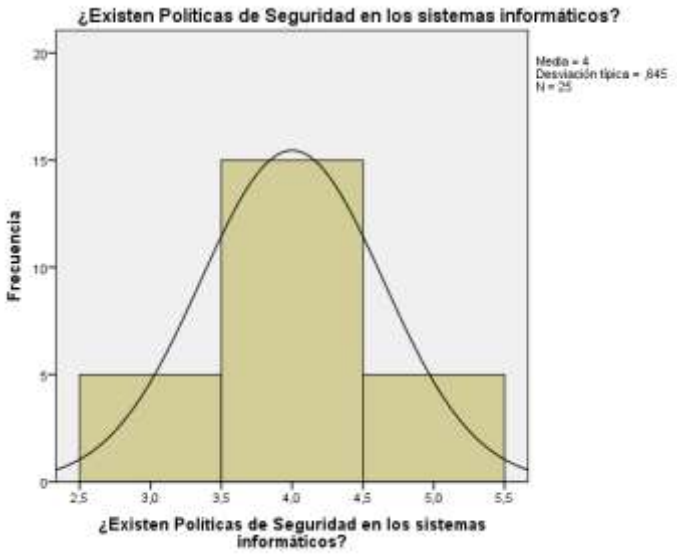
*Tabla 30.**Análisis de Frecuencia PREG04***

¿Existen Políticas de Seguridad en los sistemas informáticos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	A veces	5	20,0	20,0	20,0
	Casi Siempre	15	60,0	60,0	80,0
	Siempre	5	20,0	20,0	100,0
	Total	25	100,0	100,0	

Fuente: IBM SPSS

*Figura 26.**Análisis de Frecuencia PREG04***



Fuente: IBM SPSS

Interpretación de gráfico: De acuerdo a la percepción de los encuestados el 20.0% etiqueta A veces, el 60% etiqueta Casi Siempre y el 20% Siempre.

PREG05

*Tabla 31.**Análisis de Frecuencia** **PREG05***

¿Se realizan monitoreos de los sistemas informáticos constantemente?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	A veces	5	20,0	20,0	20,0
	Casi Siempre	14	56,0	56,0	76,0
	Siempre	6	24,0	24,0	100,0
	Total	25	100,0	100,0	

Fuente: IBM SPSS

*Figura 27.**Análisis de Frecuencia PREG05***



Fuente: IBM SPSS

Interpretación de gráfico: De acuerdo a la percepción de los encuestados el 20.0% etiqueta A veces, el 56% etiqueta Casi Siempre y el 24% Siempre.

PREG06

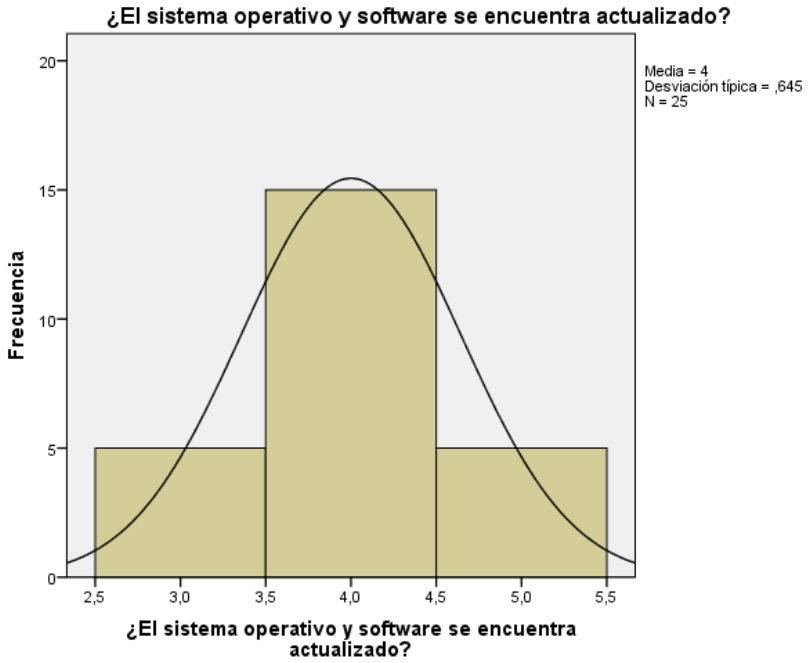
*Tabla 32.**Análisis de Frecuencia PREG06***

¿El sistema operativo y software se encuentra actualizado?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	A veces	5	20,0	20,0	20,0
	Casi Siempre	15	60,0	60,0	80,0
	Siempre	5	20,0	20,0	100,0
	Total	25	100,0	100,0	

Fuente: IBM SPSS

*Figura 28.**Análisis de Frecuencia PREG06***



Fuente: IBM SPSS

Interpretación de gráfico: De acuerdo a la percepción de los encuestados el 20.0% etiqueta A veces, el 60% etiqueta Casi Siempre y el 20% Siempre.

PREG07

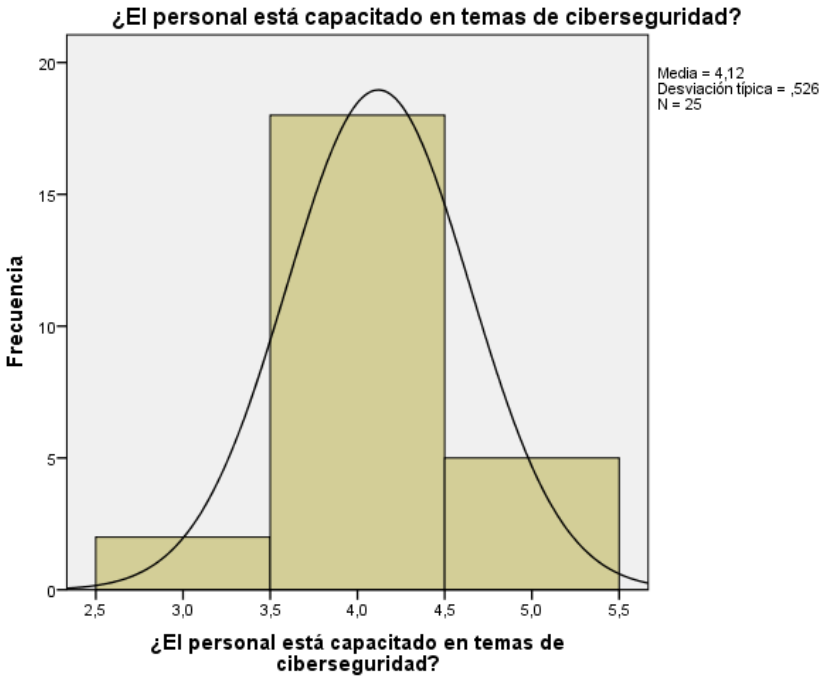
*Tabla 33.**Análisis de Frecuencia PREG07***

¿El personal está capacitado en temas de ciberseguridad?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	A veces	2	8,0	8,0	8,0
	Casi Siempre	18	72,0	72,0	80,0
	Siempre	5	20,0	20,0	100,0
	Total	25	100,0	100,0	

Fuente: IBM SPSS

*Figura 29.**Análisis de Frecuencia PREG07***



Fuente: IBM SPSS

Interpretación de gráfico: De acuerdo a la percepción de los encuestados el 8.0% etiqueta A veces, el 72% etiqueta Casi Siempre y el 20% Siempre.

PREG08

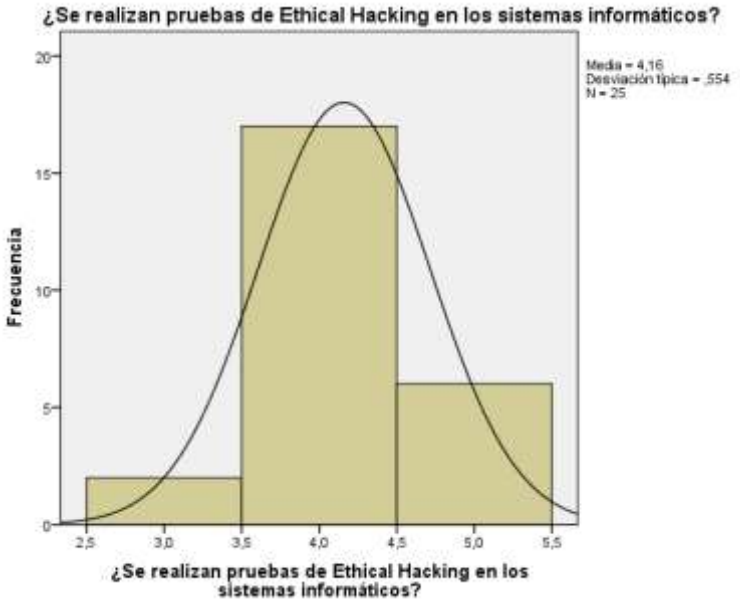
Cuadro 1: **Análisis de Frecuencia PREG08**

¿Se realizan pruebas de Ethical Hacking en los sistemas informáticos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	A veces	2	8,0	8,0	8,0
	Casi Siempre	17	68,0	68,0	76,0
	Siempre	6	24,0	24,0	100,0
	Total	25	100,0	100,0	

Fuente: IBM SPSS

*Figura 30.**Análisis de Frecuencia PREG08***



Fuente: IBM SPSS

Interpretación de gráfico: De acuerdo a la percepción de los encuestados el 8.0% etiqueta A veces, el 68% etiqueta Casi Siempre y el 24% Siempre.

PREG09

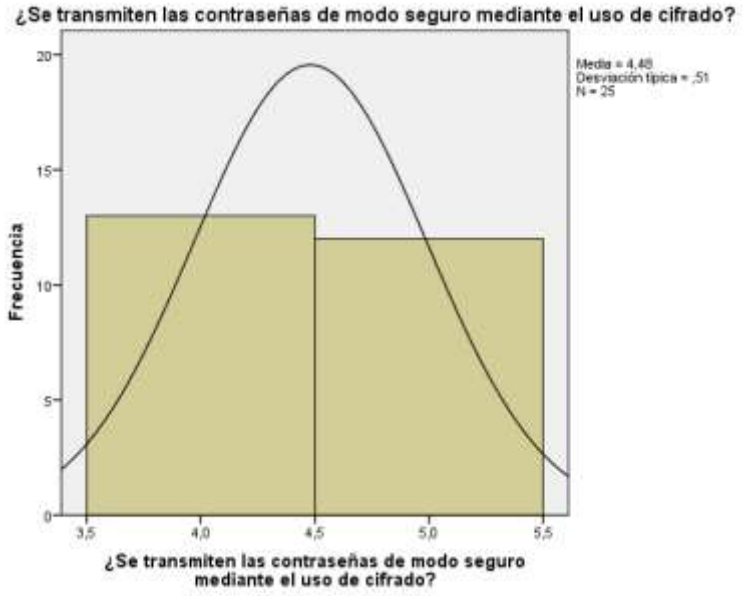
Tabla 34. ***Análisis de Frecuencia PREG09***

¿Se transmiten las contraseñas de modo seguro mediante el uso de cifrado?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Casi Siempre	13	52,0	52,0	52,0
	Siempre	12	48,0	48,0	100,0
	Total	25	100,0	100,0	

Fuente: IBM SPSS

*Figura 31.****Análisis de Frecuencia PREG09***



Fuente: IBM SPSS

Interpretación de gráfico: De acuerdo a la percepción de los encuestados el 52% etiqueta Casi Siempre y el 48% Siempre.

PREG10

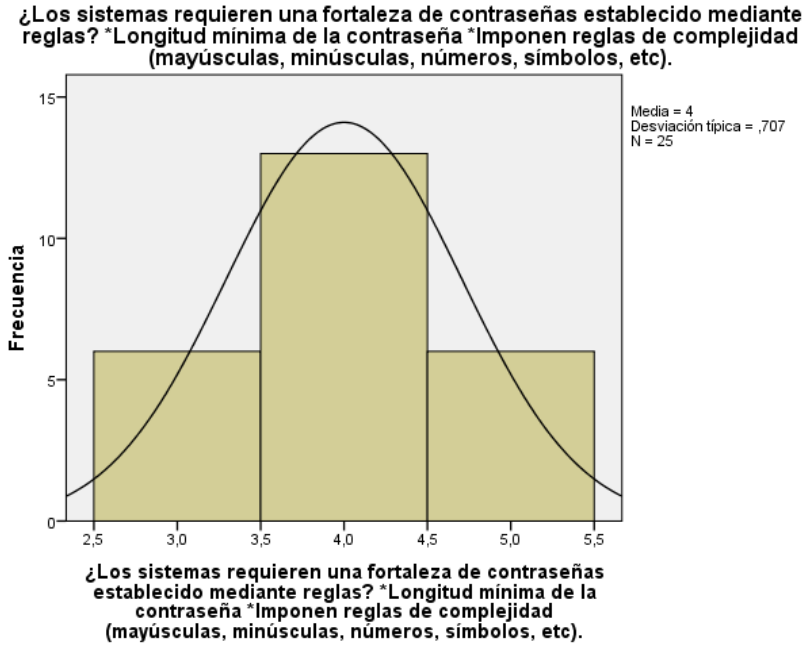
Tabla 35. ***Análisis de Frecuencia PREG10***

¿Los sistemas requieren una fortaleza de contraseñas establecido mediante reglas? *Longitud mínima de la contraseña *Imponen reglas de complejidad (mayúsculas, minúsculas, números, símbolos, etc).

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	A veces	6	24,0	24,0	24,0
	Casi Siempre	13	52,0	52,0	76,0
	Siempre	6	24,0	24,0	100,0
	Total	25	100,0	100,0	

Fuente: IBM SPSS

*Figura 32.****Análisis de Frecuencia PREG10***



Fuente: IBM SPSS

Interpretación de gráfico: De acuerdo a la percepción de los encuestados el 24.0% etiqueta A veces, el 52% etiqueta Casi Siempre y el 24% Siempre.

PREG11

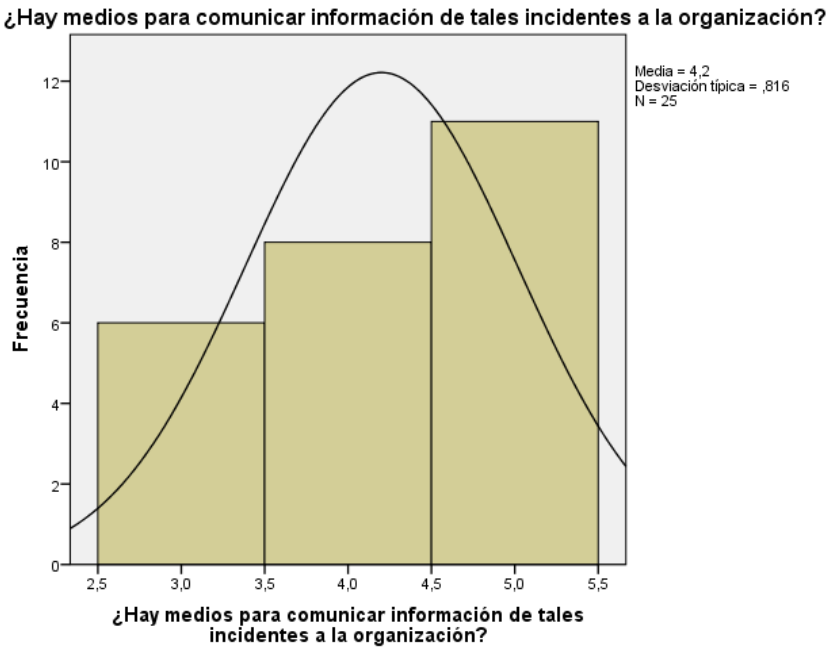
*Tabla 36.**Análisis de Frecuencia PREG11***

¿Hay medios para comunicar información de tales incidentes a la organización?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	A veces	6	24,0	24,0	24,0
	Casi Siempre	8	32,0	32,0	56,0
	Siempre	11	44,0	44,0	100,0
	Total	25	100,0	100,0	

Fuente: IBM SPSS

*Figura 33.**Análisis de Frecuencia PREG11***



Fuente: IBM SPSS

Interpretación de gráfico: De acuerdo a la percepción de los encuestados el 24.0% etiqueta A veces, el 32% etiqueta Casi Siempre y el 44% Siempre.

PRUEBA DE HIPÓTESIS

Paso 1: Planteamiento de la Hipótesis General

Hipótesis nula (***H0***) = La implementación de ethical hacking no mejora la gestión de riesgos informáticos de la CLINICA AMERICANA SERFARMED.

Hipótesis alterna (***H1***) = La implementación de ethical hacking si mejora la gestión de riesgos informáticos de la CLINICA AMERICANA SERFARMED.

Paso 2: Especificar el nivel de significancia y muestra

Nivel de significancia (α) = 5% (0.05)

Nivel de confiabilidad (1-α) = 95% (0.95)

Muestra (n) = 11

Paso 3: Determinación del valor crítico (***T***t)

Para el cálculo del valor crítico se ha empleado la tabla de distribución normal

$$Tt\ (1-\alpha)(n-1) \qquad Tt\ (1-0.05)(11-1) \qquad Tt\ (0.95)(10)=\mathbf{1}.8120$$

Figura 34. *Determinación del valor crítico de la hipótesis general, con apoyo de la tabla de distribución normal*

gl	.25	.20	.15	.10	.05	.025	.02	.01	.005	.0025	.001	.0005
1	1.000	1.376	1.963	3.078	6.314	12.71	15.89	31.82	63.66	127.3	318.3	636.6
2	0.816	1.061	1.386	1.886	2.920	4.303	4.849	6.965	9.925	14.09	22.33	31.60
3	0.765	0.978	1.250	1.638	2.353	3.182	3.482	4.541	5.841	7.453	10.21	12.92
4	0.741	0.941	1.190	1.533	2.132	2.776	2.999	3.747	4.604	5.598	7.173	8.610
5	0.727	0.920	1.156	1.476	2.015	2.571	2.757	3.365	4.032	4.773	5.893	6.869
6	0.718	0.906	1.134	1.440	1.943	2.447	2.612	3.143	3.707	4.317	5.208	5.959
7	0.711	0.896	1.119	1.415	1.895	2.365	2.517	2.998	3.499	4.029	4.785	5.408
8	0.706	0.889	1.108	1.397	1.860	2.306	2.449	2.896	3.355	3.833	4.501	5.041
9	0.703	0.883	1.100	1.383	1.833	2.262	2.398	2.821	3.250	3.690	4.297	4.781
10	0.700	0.879	1.093	1.372	1.812	2.228	2.359	2.764	3.169	3.581	4.144	4.587
11	0.697	0.876	1.088	1.363	1.796	2.201	2.328	2.718	3.106	3.497	4.025	4.437
12	0.695	0.873	1.083	1.356	1.782	2.179	2.303	2.681	3.055	3.428	3.930	4.318
13	0.694	0.870	1.079	1.350	1.771	2.160	2.282	2.650	3.012	3.372	3.852	4.221
14	0.692	0.868	1.076	1.345	1.761	2.145	2.264	2.624	2.977	3.326	3.787	4.140
15	0.691	0.866	1.074	1.341	1.753	2.131	2.249	2.602	2.947	3.286	3.733	4.073
16	0.690	0.865	1.071	1.337	1.746	2.120	2.235	2.583	2.921	3.252	3.686	4.015
17	0.689	0.863	1.069	1.333	1.740	2.110	2.224	2.567	2.898	3.222	3.646	3.965
18	0.688	0.862	1.067	1.330	1.734	2.101	2.214	2.552	2.878	3.197	3.611	3.922
19	0.688	0.861	1.066	1.328	1.729	2.093	2.205	2.539	2.861	3.174	3.579	3.883
20	0.687	0.860	1.064	1.325	1.725	2.086	2.197	2.528	2.845	3.153	3.552	3.850
21	0.686	0.859	1.063	1.323	1.721	2.080	2.189	2.518	2.831	3.135	3.527	3.819
22	0.686	0.858	1.061	1.321	1.717	2.074	2.183	2.508	2.819	3.119	3.505	3.792
23	0.685	0.858	1.060	1.319	1.714	2.069	2.177	2.500	2.807	3.104	3.485	3.768
24	0.685	0.857	1.059	1.318	1.711	2.064	2.172	2.492	2.797	3.091	3.467	3.745
25	0.684	0.856	1.058	1.316	1.708	2.060	2.167	2.485	2.787	3.078	3.450	3.725
26	0.684	0.856	1.058	1.315	1.706	2.056	2.162	2.479	2.779	3.067	3.435	3.707
27	0.684	0.855	1.057	1.314	1.703	2.052	2.158	2.473	2.771	3.057	3.421	3.690

Paso 04: Cálculo de la función prueba (Tc)

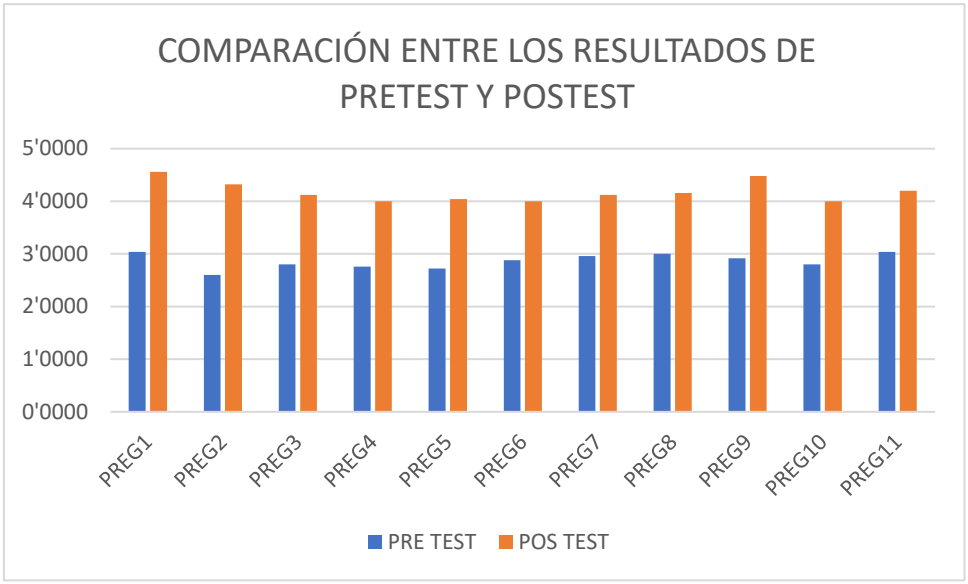
Para el cálculo de la función de prueba, se ha empleado el programa estadístico SPSS, insertando los valores promedios de los resultados del cuestionario aplicado:

*Tabla 37.**Calculo del valor crítico y la función de prueba***

N°	PREGUNTAS	MUESTRA	MEDIA	
			PRE TEST	POS TEST
1	PREG1	25	3.0400	4.5600
2	PREG2	25	2.6000	4.3200
3	PREG3	25	2.8000	4.1200
4	PREG4	25	2.7600	4.0000
5	PREG5	25	2.7200	4.0400
6	PREG6	25	2.8800	4.0000
7	PREG7	25	2.9600	4.1200
8	PREG8	25	3.0000	4.1600
9	PREG1-D	25	2.9200	4.4800
10	PREG2-D	25	2.8000	4.0000
11	PREG3-D	25	3.0400	4.2000

Tabla 38. Comparación del resultado de la aplicación del cuestionario, pre y post test

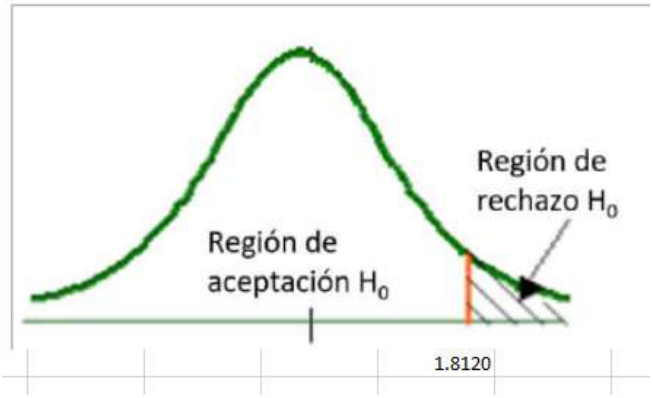
PREGUNTAS	PRE TEST	POS TEST	x̄	μ	x̄-μ
PREG1	3.0400	4.5600	1.520	1.3164	0.0415
PREG2	2.6000	4.3200	1.720	1.3164	0.1629
PREG3	2.8000	4.1200	1.320	1.3164	0.0000
PREG4	2.7600	4.0000	1.240	1.3164	0.0058
PREG5	2.7200	4.0400	1.320	1.3164	0.0000
PREG6	2.8800	4.0000	1.120	1.3164	0.0386
PREG7	2.9600	4.1200	1.160	1.3164	0.0244
PREG8	3.0000	4.1600	1.160	1.3164	0.0244
PREG9	2.9200	4.4800	1.560	1.3164	0.0594
PREG10	2.8000	4.0000	1.200	1.3164	0.0135
PREG11	3.0400	4.2000	1.160	1.3164	0.0244
PROMEDIO	**2.8655**	**4.1818**	**1.3164**	**1.3164**	
				SUMA	**0.3951**
				S	**0.1988**



Tc $= \dfrac{\bar{x} - \mu}{\dfrac{s}{\sqrt{n}}}$

μ	1.3164
S	0.1988
√n	3.3166
Tc	21.9656

Paso 05: Representación gráfica:



Paso 06: Toma de decisiones:

Como $\boldsymbol{Tc}$=21.9656 es mayor Tt=**1**.8120, se rechaza la H0 y se acepta la H1, por lo que luego de aplicar cálculos estadísticos, se determina que: La implementación de ethical hacking influye en la mejora la gestión de riesgos informáticos de la CLINICA AMERICANA SERFARMED.

DISCUSIÓN

Oñate, O. & Martínez, C. (2017). La Investigación permitió realizar mejoras en la seguridad de la red inalámbrica de la Universidad Nacional de Chimborazo aplicando hacking ético En su investigación tuvo como objetivo se tiene como objetivos analizar las técnicas de hacking ético aplicado a las redes inalámbricas para determinar que herramientas son apropiadas para mitigar las vulnerabilidades y desarrollar un manual políticas de seguridad adecuadas los escenarios que se está realizando en la investigación.

Espinoza Araujo, Christian Omar. (2020) en su investigación tuvo como objetivo mejorar la gestión de riesgos en los sistemas informáticos de la Municipalidad Provincial de Moyobamba a través de la implementación de Ethical Hacking. La metodología que se empleó para el Ethical Hacking básicamente tenía las siguientes fases: Reconocimiento, Escaneo, Enumeración, Análisis de Vulnerabilidades, Hacking de Sistemas y Escalado de Privilegios. Asimismo, los indicadores de la variable dependiente: gestión de riesgos, fueron relacionados según criterios. Se utilizó la investigación cuantitativa con el diseño experimental del tipo preexperimental con un Pre-Test y Post-Test, teniendo como variable independiente el Ethical Hacking y variable dependiente la Gestión de Riesgos. La población estuvo conformada por los sistemas informáticos que incluía servidores, computadoras, sistemas operativos, software y Data Center, haciendo un total de 280, pero la muestra se tomó solo de 25 sistemas informáticos para realizar una mejor investigación. Para identificar amenazas se empleó el cuestionario en los trabajadores de la oficina de tecnologías de información y para el análisis de vulnerabilidades se utilizó escáneres, como Nessus, OpenVas y Acunetix. Al finalizar el trabajo de investigación se logró identificar 35

vulnerabilidades y 10 amenazas. Por otro lado, para calcular el nivel del riesgo se realizó la multiplicación de amenaza x vulnerabilidad en valores cuantitativos de: 0 – 10 y valores cualitativos de: muy alto, alto, moderado, bajo, muy bajo. Se encontró 13 riesgos en nivel alto, 17 riesgos en nivel moderado y 5 riesgos en nivel bajo. Una vez clasificados se procedió a brindar alternativas de solución para su posterior mitigación.

Durand More, A. D. (2019). En su investigación tuvo como objetivo evaluar técnicas de Ethical Hacking ejecutando pruebas de penetración sobre la seguridad informática de una red de datos que permitan el diagnóstico de vulnerabilidades en una empresa prestadora de servicios (Ciudad de Lambayeque – Chiclayo).

A su vez la presente investigación sobre la implementación de ethical hacking mejora en un $\bar{x}$ = 1.3164 o 131.63% la gestión de riesgos informáticos de la CLINICA AMERICANA SERFARMED en sus indicadores: La implementación de ethical hacking mejora en un $\bar{x}$ = 142% el Número de Riesgos Identificados DE LA CLINICA AMERICANA SERFARMED; La implementación de ethical hacking mejora en un $\bar{x}$ = 124% el Número de Riesgos Analizados DE LA CLINICA AMERICANA SERFARMED;

La implementación de ethical hacking mejora en un $\bar{x}$ = 116% el Número de Riesgos tratados DE LA CLINICA AMERICANA SERFARMED.

CONCLUSIONES

- La implementación de ethical hacking mejora en un $\bar{x}$ = 1.3164 o 131.63% la gestión de riesgos informáticos de la CLINICA AMERICANA SERFARMED.
- La implementación de ethical hacking mejora en un $\bar{x}$ = 142% el Número de Riesgos Identificados valorados (5), referenciados en la Tabla N° 02: RESUMEN DE GUÍA DE OBSERVACIÓN DE LA CLINICA AMERICANA SERFARMED.
- La implementación de ethical hacking mejora en un $\bar{x}$ = 124% el Número de Riesgos Analizados valorados (5), referenciados en la Tabla N° 02: RESUMEN DE GUÍA DE OBSERVACIÓN DE LA CLINICA AMERICANA SERFARMED.DE LA CLINICA AMERICANA SERFARMED.
- La implementación de ethical hacking mejora en un $\bar{x}$ = 116% el Número de Riesgos tratados valorado (1), referenciados en la Tabla N° 02: RESUMEN DE GUÍA DE OBSERVACIÓN DE LA CLINICA AMERICANA SERFARMED.DE LA CLINICA AMERICANA SERFARMED.

RECOMENDACIONES

- Se recomienda utilizar la norma técnica peruana sobre sistemas de seguridad de la información o alguna norma de seguridad de la información internacional.
- Se recomienda realizar una clasificación de activos de acuerdo a la norma ISO 27001.
- Se recomienda que los sistemas informáticos deberían ser auditados mediante Ethical Hacking por lo menos una vez al año, ya que, todos los días aparecen nuevas amenazas y vulnerabilidades que pueden comprometer gravemente la confidencialidad, integridad y disponibilidad de la información, si estos no llegan a ser tratados de una manera adecuada.
- Se recomienda que las Política de seguridad de la información: Es un documento o puede ser un capítulo dentro de otro documento que define la forma en que la *dirección controla la gestión de la seguridad de la información.*

REFERENCIAS BIBLIOGRÁFICAS

Astudillo, Karina. Ethical Hacking 101: How to conduct professional pentestings in 21 days or less [en línea]. 1.a ed. Createspace Independent Pub, 2015. Disponible en: https://www.pdfdrive.com/ethical-hacking-101-how-to-conduct-professionalpentestings-in-21-days-or-less-e40802045.html ISBN: 978-1511610179

ALONSO, Chema. Pentesting con FOCA. 2.a ed. Madrid: 0xWord, 2018. 15 pp. ISBN: 978-84-616-6319-4.

BALOCH, Rafay. Ethical Hacking and Penetration Testing Guide [en línea]. 1.a ed. Florida: Taylor & Francis Group, 2014 [fecha de consulta: 15 de abril de 2019]. Disponible en: http://www.lepointdeau.fr/Ethical%20Hacking%20and%20Penetration%20Testing %20Guide%20-%20Baloch,%20Rafay.pdf ISBN: 978-1-4822-3162-5.

Durand more, a. D. (2019). Evaluación de técnicas de ethical hacking para el diagnóstico de vulnerabilidades de la seguridad informática en una empresa prestadora de servicios. Chiclayo - Perú. Universidad Señor de Sipán

Espinoza Araujo, Christian Omar (2020). Implementación de Ethical Hacking para mejorar la gestión de riesgos en los sistemas informáticos de la Municipalidad Provincial de Moyobamba. Perú. Universidad Cesar vallejo.

FRANCIS, Eric. (2016) Automated Network Exploitation Through Penetration Testing. Tesis (Master en Ciencias de la Computación). California: California Polytechnic State University. Disponible en: https://digitalcommons.calpoly.edu/theses/1592/

Franco Romero, G. A. (2019). Análisis de vulnerabilidades de seguridad en sistemas de VoIP, con el uso de herramientas de hacking ético. Ecuador.

Universidad de Guayaquil. Tesis. Recuperado a partir de http://repositorio.ug.edu.ec/handle/redug/39259

Governance & Standards Division, 2017, https://www.gov.uk/government/publications/corporate-governance-code-for-central-government-departments-2017

Hacknoid ,2021 obtenido en https://www.hacknoid.com/hacknoid/importancia-de-la-gestion-de-riesgos-informaticos/#:~:text=La%20gesti%C3%B3n%20de%20riesgos%20TI,vuelven%20cada%20vez%20m%C3%A1s%20indispensables.

ISO 31000, Obtenido en https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es.

Offensive Security, 2013, https://www.offensive-security.com/offsec/penetration-test-report-2013/

New York State Information Technology Service, 2015, https://www.osc.state.ny.us/state-agencies/audits/2016/08/24/effectiveness-information-technology-transformation.

Oñate, O. & Martínez, C. (2017). Mejoras en la seguridad de la red inalámbrica de la Universidad Nacional de Chimborazo aplicando hacking ético. Ecuador. Universidad Nacional de Chimborazo.

ORIYANO, Sean. Certified Ethical Hacker [en línea]. 9.a ed. Indiana: John Wiley & Sons, Inc., 2016 [fecha de consulta: 17 de abril de 2019]. Disponible en: https://www.pdfdrive.com/ceh-v9-certified-ethical-hacker-version-9- study-guide-e54415863.html ISBN: 978-1-119-25224-5.

VILLEGAS, Alejandro. Aplicación de los principios de la Ingeniería del Malware al contexto del Pentesting. Tesis (Master en Ingeniería Informática). Madrid: Universidad Autónoma de Madrid, 2018. Disponible en: http://hdl.handle.net/10486/685331.

ANEXOS

Anexos N° 1: Matriz de consistencia.

FORMULACIÓN DEL PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES	METODOLOGÍA DE LA INVESTIGACIÓN
¿En qué medida la implementación de ethical hacking mejorara la gestión de riesgos informáticos DE LA CLINICA AMERICANA SERFARMED? 1. ¿En qué medida la implementación de ethical hacking mejorará el Número de Riesgos Identificados DE LA CLINICA AMERICANA SERFARMED? 2. ¿En qué medida La implementación de ethical hacking mejorara el Número de Riesgos Analizados? 3. ¿En qué medida La implementación de ethical hacking mejorara el Número de Riesgos tratados?	Determinar de qué manera la implementación ethical hacking mejorará la gestión de riesgos informáticos DE LA CLINICA AMERICANA SERFARMED. 1. Determinar de qué manera la implementación de ethical hacking mejorará el Número de Riesgos Identificados DE LA CLINICA AMERICANA SERFARMED. 2. Determinar de qué manera la implementación de ethical hacking mejorara el Número de Riesgos Analizados DE LA CLINICA AMERICANA SERFARMED. 3. Determinar de qué manera la implementación de ethical hacking mejorara el Número de Riesgos tratados DE LA CLINICA AMERICANA SERFARMED.	la implementación de ethical hacking mejora la gestión de riesgos informáticos DE LA CLINICA AMERICANA SERFARMED. 1. La implementación de ethical hacking mejora el Número de Riesgos Identificados DE LA CLINICA AMERICANA SERFARMED. 2. La implementación de ethical hacking mejora el Número de Riesgos Analizados DE LA CLINICA AMERICANA SERFARMED. 3. La implementación de ethical hacking mejora el Número de Riesgos tratados DE LA CLINICA AMERICANA SERFARMED.	**Variable independiente:** Ethical Hacking **Dimensión** / **Indicadores** planeación: Activos de la empresa; Nivel de identificación de software Critico. Vulnerabilidades: Número de vulnerabilidades mitigadas; nivel de vulnerabilidades Evaluación de riesgos: Nivel de riesgos Informe de resultados: Numero de informes. **Variable dependiente:** Gestión de Riesgos Informáticos. **Dimensión** / **Indicadores** Riesgos Identificados: Nivel de plan de continuidad de negocio; Puertos USB. acticos en las Pcs. O servidores.; Frecuencia de limpieza de metadatos de archivos.; Nivel de Políticas de Seguridad; Frecuencia de monitoreos de los sistemas informáticos. Riesgos analizados: Sistema Operativo y de aplicaciones actualizado; Capacitación en temas de seguridad; Frecuencia de Realización de pruebas de Ethical Hacking; Transmisión de contraseñas de modo seguro; Nivel de regla de complejidad en contraseñas Riesgos tratados: Nivel de incidencias	**Tipo de investigación**: Aplicada **Nivel de investigación:** Descriptivo **Población:** Para esta investigación, la población lo constituye los operadores y todos los sistemas informáticos, que incluyen software y hardware de la CLINICA AMERICANA SERFARMED - PUCALLPA, los cuales hacen un total de 25 entre computadoras, servidores, sistemas operativos y aplicaciones. **Muestra:** Se opta por el muestreo no probabilístico, por conveniencia, siendo el tamaño de la muestra el tamaño de la población (un total 25 los operadores y sistemas informáticos entre computadoras, sistemas operativos y data center). **Diseño de la investigación: Pre Experimental** **Tratamiento de datos.** Para esta actividad nos agenciaremos de la herramienta IBM SPSS Stadistics versión 26. **Fuentes** / **Técnicas** / **Instrumentos** Primaria / Encuesta / -Cuestionarios

Anexos N° 2: Cuestionario de preguntas para la recolección de datos

Cuestionario

Estimado, con el presente cuestionario se pretende obtener datos respecto a la gestión de riesgos en los sistemas informáticos, para lo cual le solicito su colaboración, respondiendo a todas las preguntas con la mayor sinceridad posible. La información obtenida permitirá proponer sugerencias para mejorar la gestión de riesgos de seguridad de la información.

Marque con una (x) la alternativa que considera pertinente en cada pregunta.

ESCALA VALORATIVA

CÓDIGO	CATEGORIA	VALOR
S	Siempre	5
CS	Casi Siempre	4
AV	A veces	3
CN	Casi Nunca	2
N	Nunca	1

	VARIABLE: GESTIÓN DE RIESGOS					
	Indicador 01: Número de riesgos identificados	**S**	**CS**	**AV**	**CN**	**N**
1	En el caso de producirse un movimiento telúrico y destruya los sistemas informáticos ¿Se cuenta con un plan de continuidad de negocio?					
2	¿Los puertos USB están activados en las computadoras?					
3	¿Se limpian los metadatos de archivos que se van a subir al portal web?					
4	¿Existen Políticas de Seguridad en los sistemas informáticos?					
5	¿Se realizan monitoreos de los sistemas informáticos constantemente?					
	Indicador 02: Número de riesgos analizados.	**S**	**CS**	**AV**	**CN**	**N**
6	¿El sistema operativo y software se encuentra actualizado?					
7	¿El personal está capacitado en temas de ciberseguridad?					
8	¿Se realizan pruebas de Ethical Hacking en los sistemas informáticos?					
9	¿Se transmiten las contraseñas de modo seguro mediante el uso de cifrado?					
10	¿Los sistemas requieren una fortaleza de contraseñas establecido mediante reglas? *Longitud mínima de la contraseña *Imponen reglas de complejidad (mayúsculas, minúsculas, números, símbolos, etc).					
	Indicador 03: Número de riesgos tratados.	**S**	**CS**	**AV**	**CN**	**N**
11	¿Hay medios para comunicar información de tales incidentes a la organización?					

Anexos N° 3: Validación de los instrumentos por expertos

UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE INGENIERIA DE SISTEMAS E INGENIERIA CIVIL

I. DATOS GENERALES

1.1. APELLIDOS Y NOMBRES: **UNTIVEROS BARBOZA CINTHIA**

1.2. GRADO ACADÉMICO: **MAGISTER**

1.3. INSTITUCION QUE LABORA: **J&C TECHNET E.I.R.L**

1.4. TITULO DE LA INVESTIGACIÓN: **IMPLEMENTACIÓN DE ETHICAL HACKING PARA MEJORAR LA GESTIÓN DE RIESGOS INFORMÁTICOS DE LA CLINICA SERFARMED – PUCALLPA.**

1.5. AUTOR DEL INSTRUMENTO: **GUILLERMO WILFREDO TORRES RAMIREZ**

1.6. NOMBRE DEL INSTRUMENTO: **JUICIO DE EXPERTOS**

1.7. CRITERIOS DE APLICABILIDAD:

(a) De 01 a 09: (No válido, reformular) (b) De 10 a 12: (No válido, modificar) (c) De 13 a 15: (Válido, mejorar)
(d) De 16 a 18 (Válido, precisar) (e) De 19 a 20: (Válido, aplicar)

II. ASPECTOS A EVALUAR

INDICADORES DE EVALUACIÓN DEL INSTRUMENTO	CRITERIOS CUALITATIVOS – CUANTITATIVOS	Deficiente (01 - 09)	Regular (10 - 12)	Bueno (13 - 15)	Muy bueno (16 - 18)	Excelente (19 - 20)
1. CALIDAD	Esta formulado con lenguaje apropiado					19
2. OBJETIVIDAD	Esta expresado con conductas observables					19
3. ACTUALIDAD	Adecuado al avance de la ciencia y tecnología					19
4. ORGANIZACIÓN	Existe organización y lógica					19
5. SUFICIENCIA	Comprende los aspectos en cantidad y calidad					19
6. INTENCIONALIDAD	Adecuado para valorar los aspectos de estudio					19
7. CONSISTENCIA	Basado en aspecto teórico científico y del tema de estudio					19
8. COHERENCIA	Entre las variables, dimensiones e indicadores					19
9. METODOLOGÍA	La estrategia responde al propósito del estudio					19
10. CONVENIENCIA	Genera nuevas pautas para la investigación y construcción de teorías					19
SUB TOTAL						190
TOTAL						190

VALORACION CUANTITATIVA : 190
VALORACION CUALITATIVA : VALIDO
OPINION DE APLICABILIDAD : APLICAR

Lugar y Fecha: 13/04/22.

154157
Firma y post firma del experto
Código de colegiatura

DNI 40981627



UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE INGENIERIA DE SISTEMAS E INGENIERIA CIVIL

I. DATOS GENERALES

1.1. APELLIDOS Y NOMBRES: **AGURTO CHERRE CESAR AUGUSTO**.

1.2. GRADO ACADEMICO: **MAGISTER**

1.3. INSTITUCION QUE LABORA: **UNIVERSIDAD NACIONAL DE UCAYALI**

1.4. TITULO DE LA INVESTIGACION: **IMPLEMENTACIÓN DE ETHICAL HACKING PARA MEJORAR LA GESTIÓN DE RIESGOS INFORMATICOS DE LA CLINICA AMERICANA SERFARMED – PUCALLPA.**

1.5. AUTOR DEL INSTRUMENTO: **GUILLERMO WILFREDO TORRES RAMIREZ**

1.6. NOMBRE DEL INSTRUMENTO: **JUICIO DE EXPERTOS**

1.7. CRITERIOS DE APLICABILIDAD:

(a) De 01 a 09: (No válido, reformular) (b) De 10 a 12: (No válido, modificar) (c) De 13 a 15: (Válido, mejorar)
(d) De 16 a 18 (Válido, precisar) (e) De 19 a 20: (Válido, aplicar)

II. ASPECTOS A EVALUAR

INDICADORES DE EVALUACIÓN DEL INSTRUMENTO	CRITERIOS CUALITATIVOS – CUANTITATIVOS	Deficiente (01 - 09)	Regular (10 - 12)	Bueno (13 - 15)	Muy bueno (16 - 18)	Excelente (19 - 20)
1. CALIDAD	Esta formulado con lenguaje apropiado					19
2. OBJETIVIDAD	Esta expresado con conductas observables					19
3. ACTUALIDAD	Adecuado al avance de la ciencia y tecnología					19
4. ORGANIZACIÓN	Existe organización y lógica					19
5. SUFICIENCIA	Comprende los aspectos en cantidad y calidad					19
6. INTENCIONALIDAD	Adecuado para valorar los aspectos de estudio					19
7. CONSISTENCIA	Basado en aspecto teórico científico y del tema de estudio					19
8. COHERENCIA	Entre las variables, dimensiones e indicadores					19
9. METODOLOGÍA	La estrategia responde al propósito del estudio					19
10. CONVENIENCIA	Genera nuevas pautas para la investigación y construcción de teorías					19
SUB TOTAL						190
TOTAL						190

VALORACION CUANTITATIVA :190.
VALORACION CUALITATIVA :VALIDO.
OPINION DE APLICABILIDAD :APLICAR.

Lugar y Fecha: 29/03/2022

133453
Firma y post firma del experto
Código de colegiatura

DNI 18190341



UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE INGENIERIA DE SISTEMAS E INGENIERIA CIVIL

I. DATOS GENERALES

1.1. APELLIDOS Y NOMBRES: **YUPANQUI VILLANUEVA, ARTURO**

1.2. GRADO ACADEMICO: **MAGISTER**

1.3. INSTITUCION QUE LABORA: **UNIVERSIDAD NACIONAL DE UCAYALI**

1.4. TITULO DE LA INVESTIGACION: **IMPLEMENTACION DE ETHICAL HACKING PARA MEJORAR LA GESTION DE RIESGOS INFORMÁTICOS DE LA CLINICA SERFARMED – PUCALLPA.**

1.5. AUTOR DEL INSTRUMENTO: **GUILLERMO WILFREDO TORRES RAMIREZ**

1.6. NOMBRE DEL INSTRUMENTO: **JUICIO DE EXPERTOS**

1.7. CRITERIOS DE APLICABILIDAD:

(a) De 01 a 09: (No válido, reformular) (b) De 10 a 12: (No válido, modificar) (c) De 13 a 15: (Válido, mejorar)
(d) De 16 a 18 (Válido, precisar) (e) De 19 a 20: (Válido, aplicar)

II. ASPECTOS A EVALUAR

INDICADORES DE EVALUACIÓN DEL INSTRUMENTO	CRITERIOS CUALITATIVOS – CUANTITATIVOS	Deficiente (01 - 09)	Regular (10 - 12)	Bueno (13 - 15)	Muy bueno (16 - 18)	Excelente (19 - 20)
1. CALIDAD	Esta formulado con lenguaje apropiado					20
2. OBJETIVIDAD	Esta expresado con conductas observables					19
3. ACTUALIDAD	Adecuado al avance de la ciencia y tecnología					19
4. ORGANIZACIÓN	Existe organización y lógica					19
5. SUFICIENCIA	Comprende los aspectos en cantidad y calidad					19
6. INTENCIONALIDAD	Adecuado para valorar los aspectos de estudio					19
7. CONSISTENCIA	Basado en aspecto teórico científico y del tema de estudio					19
8. COHERENCIA	Entre las variables, dimensiones e indicadores					19
9. METODOLOGÍA	La estrategia responde al propósito del estudio					19
10. CONVENIENCIA	Genera nuevas pautas para la investigación y construcción de teorías					19
SUB TOTAL						191
TOTAL						191

VALORACIÓN CUANTITATIVA : 191
VALORACIÓN CUALITATIVA : VALIDO
OPINION DE APLICABILIDAD : APLICA.

Lugar y Fecha: 22/03/2022



Firma y post firma del experto
Código de colegiatura 98262
DNI: 40052478

***Anexos N° 4*: Evidencia de la aceptabilidad para realizar la investigación**

CARTA DE AUTORIZACIÒN

Pucallpa,23 de abril del 2022

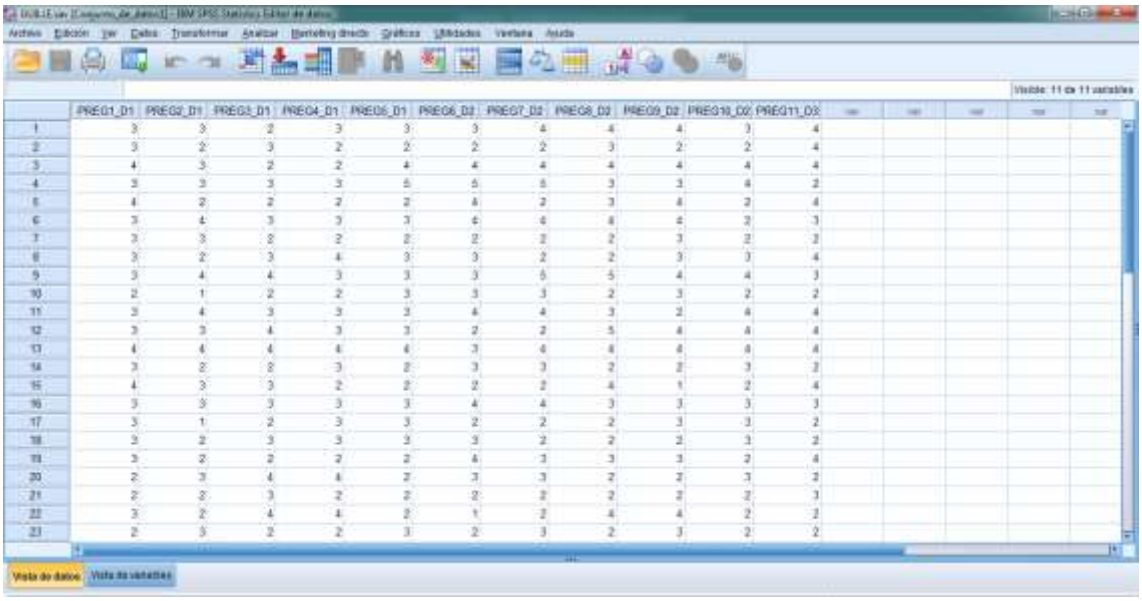
Por el presente documento, yo NICOLAS WALTER , identificado con DNI N°08914058, en calidad de representante legal de la clínica **SERVICIOS GENERALES SERFARMED SYS SA** , autorizo al bachiller en **Ingeniería De Sistemas, TORRES RAMIREZ, GUILLERMO WILFREDO** a utilizar las instalaciones de los servidores y computadoras que se encuentran en la clínica como parte del desarrollo de sus Tesis de Pregrado.

La empresa, precisa que toda información proporcionada será para uso exclusivamente académico.

CLINICA AMERICANA SERFARMED S.A.
Nicolas Walter Aguilar Carzas
GERENTE GENERAL

NICOLAS WALTER AGUILAR CARZAS
GERENTE GENERAL
DNI N° 08914058

Anexos N° 5: DATOS PRE TEST



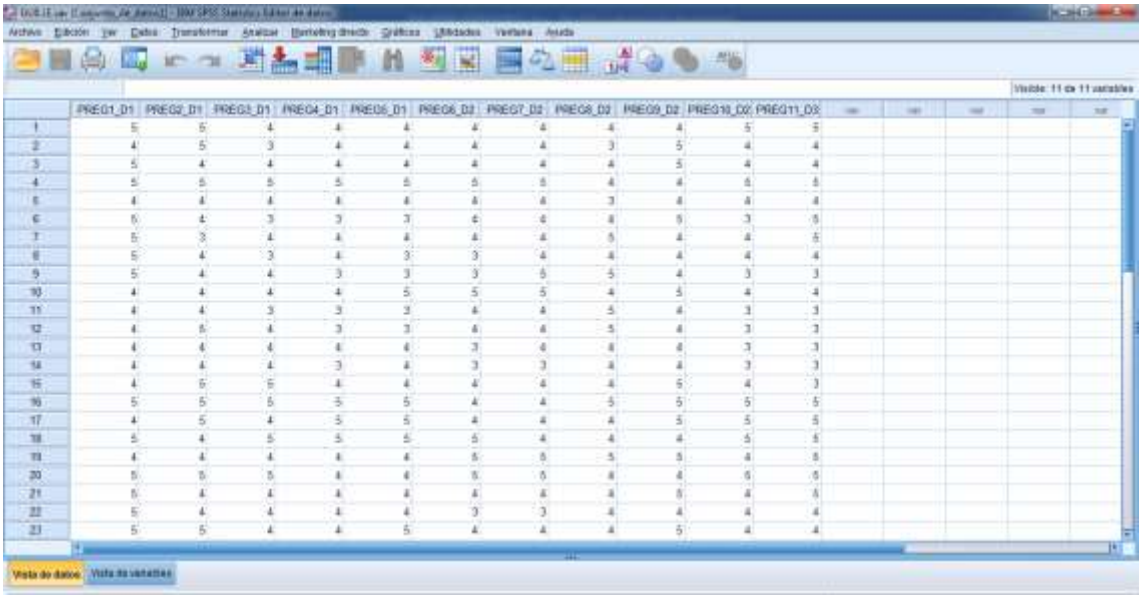
PREG1_D1	PREG2_D1	PREG3_D1	PREG4_D1	PREG5_D1	PREG6_D2	PREG7_D2	PREG8_D2	PREG9_D2	PREG10_D2	PREG11_D3
3	3	2	3	3	3	4	4	4	3	4
3	2	3	2	2	2	2	3	2	2	4
4	3	2	2	4	4	4	4	4	4	4
3	3	3	3	5	5	5	3	3	4	2
4	2	2	2	2	4	2	3	4	2	4
3	4	3	3	3	4	4	4	4	3	3
3	3	2	2	2	2	2	2	3	2	2
3	2	3	4	3	3	2	2	3	3	4
3	4	4	3	3	3	5	5	4	4	3
2	1	2	2	3	3	3	2	3	2	2
3	4	3	3	3	4	4	3	2	4	4
3	3	4	3	3	2	2	5	4	4	4
4	4	4	4	4	3	4	4	4	4	4
3	2	2	3	2	3	3	2	2	3	2
4	3	3	2	2	2	2	4	1	2	4
3	3	3	3	3	4	4	3	3	3	3
3	1	2	3	3	2	2	2	3	3	2
3	2	3	3	3	3	2	2	3	3	2
3	2	2	2	2	4	3	3	3	2	4
2	3	4	4	2	3	3	2	2	3	2
2	2	3	2	2	2	2	2	2	2	3
3	2	4	4	2	1	2	4	4	2	2
2	3	2	2	3	2	3	2	3	2	2

Anexos N° 6: FIABILIDAD ALPHA CRONBACH

Estadísticos de fiabilidad	
Alfa de Cronbach	N de elementos
,818	11

Tasa Porcentual: 81.8% de Fiabilidad, con etiqueta de valor < Muy Alta Correlación >

Anexos N° 7: DATOS POS TEST



PREG1_D1	PREG2_D1	PREG3_D1	PREG4_D1	PREG5_D1	PREG6_D2	PREG7_D2	PREG8_D2	PREG9_D2	PREG10_D2	PREG11_D3
5	5	4	4	4	4	4	4	4	5	5
4	5	3	4	4	4	4	3	5	4	4
5	4	4	4	4	4	4	4	5	4	4
5	5	5	5	5	5	5	4	4	5	5
4	4	4	4	4	4	4	3	4	4	4
5	4	3	3	3	4	4	4	5	3	5
5	3	4	4	4	4	4	5	4	4	5
5	4	3	4	3	3	4	4	4	4	4
5	4	4	3	3	3	5	5	4	3	3
4	4	4	4	5	5	5	4	5	4	4
4	4	3	3	3	4	4	5	4	3	3
4	5	4	3	3	4	4	5	4	3	3
4	4	4	4	4	3	4	4	4	3	3
4	4	4	3	4	3	3	4	4	3	3
4	5	5	4	4	4	4	4	5	4	3
5	5	5	5	5	4	4	5	5	5	5
4	5	4	5	5	4	4	4	5	5	5
5	4	5	5	5	5	4	4	4	5	5
4	4	4	4	4	5	5	5	5	4	5
5	5	5	4	4	4	4	4	4	4	5
5	4	4	4	4	4	4	4	5	4	5
5	4	4	4	4	3	3	4	4	4	4
5	5	4	4	5	4	4	4	5	4	4

Anexos N° 8: FIABILIDAD ALPHA CRONBACH

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,804	11

Tasa Porcentual: 80.4% de Fiabilidad, con etiqueta de valor < Muy Alta Correlación >

Tabla 39: Coeficiente de Correlación

Coeficiente de Correlación	Interpretación
0	Nula Correlación
De 0.01 a 0.19	Muy Baja Correlación
De 0.20 a 0.39	Baja Correlación
De 0.40 a 0.59	Moderada Correlación
De 0.60 a 0.79	Alta Correlación
De 0.80 a 0.99	Muy Alta Correlación
1	Perfecta Correlación

Fuente: Introducción conceptual al análisis multivariable. Un enfoque informático con los paquetes SPSS[1]

[1] BISQUERRA Alzina, R.; (1989). "Introducción conceptual al análisis multivariable. Un enfoque informático con los paquetes SPSS-X, BMDP", LISREL y SPAD. Barcelona: PPU.

Tabla 40: ***GUÍA DE OBSERVACIÓN***

I. Situación a Observar: Gestión de Riesgos Informáticos

II. Objetivo: Medir las Dimensiones: Riesgos Identificados – Riesgos analizados - Riesgos tratados relacionadas con sus indicadores respectivos.

III. Datos Generales:
   a. Fecha: __/__/2022
   b. Área a Observar: LA CLINICA AMERICANA SERFARMED
   c. Nombre del Observador: Guillermo Wilfredo TORRES RAMIREZ

IV. Gestión de Riesgos Informáticos.
   a. Dimensión Riesgos Identificados
      i. Número de Riesgos Identificados.

      _____
      _____

   b. Dimensión Riesgos Analizados
      i. Número de Riesgos Analizados.

      _____
      _____

   c. Dimensión Riesgos Tratados
      i. Número de Riesgos Tratados.

      _____
      _____

Tabla 41.RESUMEN DE GUÍA DE OBSERVACIÓN

	Cantidad	Detalle	Relación en GRI
Riesgos Identificados	5	1. Plan de continuidad de negocio 2. Puertos USB. acticos en las Pcs. O servidores 3. Frecuencia de limpieza de metadatos de archivos. 4. Políticas de Seguridad 5. Monitoreos de los sistemas informáticos.	Implementar técnicas de Ethical Hacking para los Riesgos Identificados como los Gestión de sistema operativo y software, Gestión de cuenta con una adecuada Configuración del sistema.
Riesgos Analizados	5	1. Sistema Operativo y de aplicaciones actualizado 2. Capacitación en temas de seguridad 3. Realización de pruebas de Ethical Hacking	Implementar técnicas de Ethical Hacking para los Riesgos Analizados como los puertos USB si están activados en los dispositivos, Mantenimiento de los metadatos de archivos que,

		4. Transmisión de contraseñas de modo seguro 5. regla de complejidad en contraseñas	en el portal web, Políticas de Seguridad en los sistemas
Riesgos Tratados	1	Gestión de Incidencias	informáticos, Se gestiona monitoreos de los sistemas informáticos constantemente , el sistema operativo y software se encuentra actualizado Implementar técnicas de Ethical Hacking para los Riesgos Identificados y Analizados, teniendo en cuenta la Evaluación del Riesgo.

Fuente: Elaboración Propia

Trabajo:
-Arreglo caratula
-Ajustar índice
-Agregar escaneados
- ordenado de bibliografía como APA
- conclsuions y recomendaciones en viñetas
- Solo a Indice de Figuras y Tablas, quitamos Graficos y Cuadros
- Ajustar textos
- buscar citas
- Ordenar bibliografía alfabéticamente