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

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

Julio Valverde Chávez
Augusto Cortez Vásquez*

Presentación: setiembre de 2017 Aceptación: noviembre de 2017

RESUMEN
El presente trabajo de investigación tiene como objetivo identificar los riesgos de seguridad en los Websites para conocer 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 a cuyos representantes se les entregaron encuestas formuladas con la finalidad de levantar la información respectiva. El resultado del estudio ha permitido establecer una metodología con propósitos muy específicos en el desarrollo de Websites, así como la aplicación de 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, bondades y focos de testeo de estas herramientas para hacer realmente efectiva la detección de vulnerabilidades en las Websites.

Palabras clave: riesgos de seguridad, gestión de información, Open source, crackers, seguridad en los Websites

ABSTRACT
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.

Keywords: risks of security, security of information, open source, crackers

* Universidad Ricardo Palma, Facultad de Ingeniería, <jvalverdech@urp.edu.pe>, <acortezv@urp.edu.pe>

1. Introducción

Situación problemática

Dado que los Websites tienen vulnerabilidades, es conveniente identificarlas y repararlas antes de que esos incidentes ocurran. Se debe entender que un equipo de desarrollo con experiencia puede producir códigos vulnerables. Este error lo cometen muchas compañías al pensar justamente lo contrario. 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 en que se corrigen estas vulnerabilidades. Para las vulnerabilidades de un Websites, 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.

Objetivos

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

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 de 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.

2. Marco teórico

2.1. Seguridad

En el entorno en que nos movemos, es necesario asegurar una comunicación fiable 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 invulnerabilidad 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.

2.2. Riesgo

Un riesgo se puede entender como una probabilidad de que una circunstancia adversa ocurra. Es decir, constituye una amenaza para el proyecto: para la actividad que se está desarrollando y para la organización en general. 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) [1].

2.3. Riesgos de seguridad

Los riesgos de seguridad son la combinación de uno o más eventos que pueden o no ocurrir en un determinado momento y que provocan un impacto indeseado. Puede ser una amenaza a alguna vulnerabilidad existente de la empresa, ya sea en bienes o activos. El encargado realiza una evaluación cuantitativa o cualitativa que permite conocer, minimizar y tomar decisiones con respecto a dicha amenaza [2].

El riesgo es una característica inherente a cualquier actividad, por lo que no debe considerarse un factor negativo, sino un elemento clave que la empresa debe conocer y gestionar. En ese sentido, el riesgo puede ser un factor diferenciador. Los riesgos han sido definidos como todos los posibles eventos que pueden afectar al cumplimiento de los objetivos de una organización. Dichos 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 [3].

2.4. Razones para realizar el análisis de riesgos

Existen muchas causas que pueden afectar la seguridad de la información de cualquier tipo de organización [4]. Entre ellas, mencionamos algunas:

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

2.5. Gestión de información

Es el proceso mediante el cual se desarrolla, interrelaciona y controla el manejo de la información utilizando la tecnología. El objetivo de gestionar información es facilitar su ubicación y ahorrar tiempo en la búsqueda de la misma. 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 supone 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, para contar con la información adecuada, en el tiempo y lugar adecuados. Algunos autores definen la gestión de información como el

manejo de la inteligencia organizacional que tiene como finalidad incrementar la eficacia, eficiencia y efectividad para el cumplimiento de su misión [4] y [5]. La inteligencia corporativa agrupa la información y el conocimiento con el que se cuenta, todo ello con miras a incrementar la productividad de la toma de decisiones. La eficacia es la relación positiva entre los objetivos y logros obtenidos. Por su parte, la eficiencia es la relación entre los logros obtenidos y los recursos invertidos, mientras que la efectividad es la relación entre los logros obtenidos, la inversión y el impacto de las acciones realizadas.

3. Metodología

De acuerdo con los objetivos planteados para la investigación, interesa 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, principalmente docentes y profesionales en área de Ingeniería de Sistemas. Para esto, se formaron grupos o estratos en tres niveles. El estrato I estuvo conformado por medianas empresas comercializadoras de maquinarias, equipos y materiales de Lima Metropolitana. El estrato II incluyó a los profesionales en Ingeniería Industrial y en Ingeniería de Sistemas y especialistas en Informática, y matemáticos computacionales de los colegios profesionales de Lima. Finalmente, el estrato III, estuvo formado por docentes en Informática en los niveles de pregrado y maestría de la Facultad de Ingeniería de la Universidad Ricardo Palma y la Universidad Nacional del Callao.

Marco muestral

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

Se ha podido comprobar, además, que el 70% de las medianas empresas de Lima Metropolitana no cuentan con un área de cómputo especializados para desarrollar aplicaciones Websites ni 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 sujetos observadores, a especialistas informáticos y docentes con amplia experiencia en el desarrollo de aplicaciones Websites.

Población

TABLA 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 pregrado	505
Total		**11,767**

Fuente: Colegio de Ingenieros. Capitulo Industriales y Sistemas.

La población está constituida por las empresas, especialistas en informática, y docentes del área Informática, como se muestra en el cuadro siguiente.

Tamaño de muestra

Para hallar el tamaño de muestra se utilizará el muestreo aleatorio simple. En toda investigación, el tamaño de muestra es muy importante, puesto que de este dependen la calidad y validez de los resultados. Una muestra demasiado grande implica un desperdicio de recursos y una muestra demasiado pequeña disminuye la utilidad de los resultados. En nuestra investigación, utilizaremos el muestreo aleatorio simple [6]. El tamaño de muestra en el muestreo aleatorio simple se calcula con la fórmula siguiente :

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

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

Donde:

n	:	tamaño de muestra
n_0	:	tamaño de muestra aproximado
N	:	tamaño de la población bajo estudio
Zα	:	valores correspondientes 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 fórmula, entonces, 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%; $\alpha/2$ = 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 fórmula (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.

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 el cuadro N° 02, después dele estrato de las *Empresas*, las proporciones más importantes se observan en las especialidades *Especialista en Informática* y *Docentes en Informática*.

TABLA 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 pregrado	23	35%
Total		66	100%

Fuente: Elaboración propia.

4. Resultados y discusión

Análisis, interpretación y discusión de resultados

FRECUENCIAS PORCENTUALES DE RESPUESTA POR CADA PREGUNTA:

TABLA 4. ¿CONSIDERA QUE LOS NIVELES DE SEGURIDAD DE LOS WEBSITES SON APROPIADOS EN LA EMPRESA?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Sí	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 maneja unos niveles de seguridad que permiten conocer que existe previsión en el promedio indicado para velar por la seguridad, aunque existe más del 62.1% que no guarda esta previsión.

TABLA 5. ¿Cree que el software de seguridad del websites en la empresa es óptimo?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Sí	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 están seguras de que los software para la implementación de las Websites son óptimos, mientras el 71.2% es de la opinión contraria.

TABLA 6. ¿Existen problemas de seguridad en los websites de la empresa?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Sí	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, según la fuente de opinión, que el 53.15% de empresas indican que sí existen problemas en los Websites. Solamente el 46.9% indica que no existen tales inconvenientes.

TABLA 7. Uno de los métodos de intrusión son los crackers. ¿Cree que pueden ser controlados?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Sí	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 dan como respuesta que la intrusión de crackers puede ser controlada. Un 41.5%, asevera lo contrario.

TABLA 8. ¿SE ALCANZAN LOS OBJETIVOS Y METAS ESTABLECIDOS EN LA EMPRESA PARA LA SEGURIDAD INFORMÁTICA?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Sí	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, el 34.8%, indica que sí están cumpliendo los objetivos y metas.

TABLA 9. ¿SE CUMPLEN EXHAUSTIVAMENTE LAS PRUEBAS DE TESTEO PARA COMPROBAR LA SEGURIDAD DE ATAQUES DE CRACKERS?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Sí	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 para hacer pruebas de testeo que busquen evitar y contrarrestar los ataques de intrusión, principalmente los llamados crackers. Solo el 24.6% asegura que realiza las pruebas de testeo respectivo.

TABLA 10. ¿EXISTEN RIESGOS DE SEGURIDAD DE LOS WEBSITES EN LA EMPRESA?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Sí	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 de seguridad en el manejo de Websites, el 80.0% responde que estos sí existen, mientras que un 20% considera como algo seguro la navegación en los sitios Web.

TABLA 11. ¿El software de websites es desarrollado por la empresa

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Sí	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, que el 34.95% está dedicado a desarrollar sus Websites, y la gran parte, es decir, el 65.1% trabaja con softwares desarrollados por empresas especializadas.

TABLA 12. En su opinión, ¿los websites son de fácil acceso y navegación para el cliente?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Sí	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. Solo el 30.3% no cuentan con la facilidad de navegación y acceso.

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

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Sí	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. Por su parte, el 49.2% señala que no existen tales problemas.

TABLA 14. EN SU OPINIÓN, ¿EL MANEJO DE LA INFORMACIÓN Y LA SEGURIDAD PODRÍAN MEJORAR EN LA EMPRESA

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Sí	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 de que la gestión de la información y la seguridad pueden mejorar 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

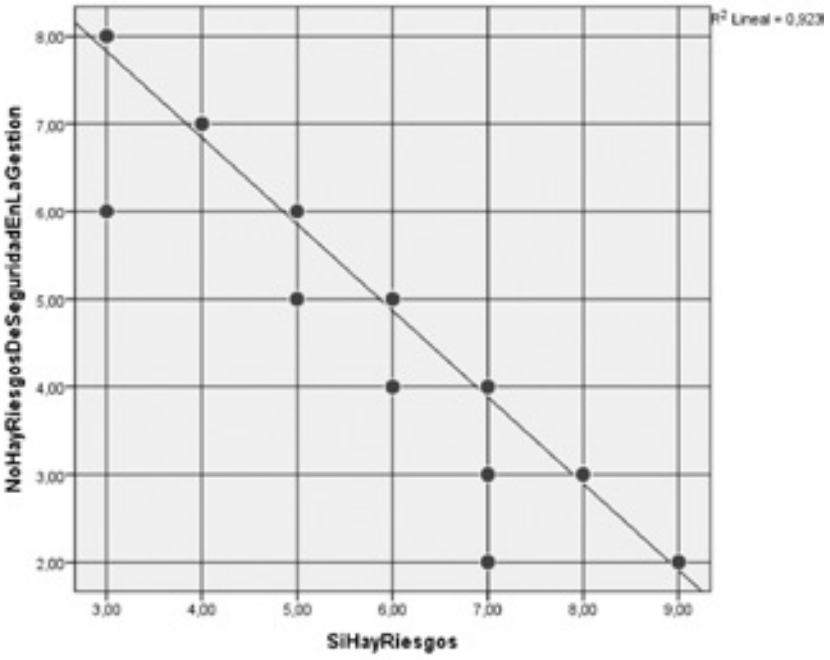
TABLA 15. CORRELACIONES

		Sí hay riesgos de seguridad en la gestión	No hay riesgos de seguridad en la gestión
Sí 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 la Correlación de Pearson es -0.961. Se trata de una correlación negativa muy fuerte. Esto quiere decir que, a mayor uso de los Websites, mayor es el riesgo que representa la seguridad en la gestión de información. El gráfico de la dispersión de los puntos del total de los datos está dado por:

GRÁFICO 1. Gráfico de la dispersión de puntos donde no hay riesgos de seguridad en la gestión con respecto a la variable de opinión en donde sí hay riesgos de seguridad



Fuente: Elaboración propia.

Como se puede apreciar, sí existe una correlación negativa muy fuerte entre "sí existe riesgo de seguridad en los Websites en las medianas empresas de Lima Metropolitana" y "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 conocer 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, que nos permitirá saber qué influencia tendrán las variables con respecto al riesgo de seguridad en la gestión de información con relación a otra variable en donde el riesgo de seguridad es muy bajo.

TABLA 16. Resumen del modelo

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

Fuente: Elaboración propia.

AUTOCORRELACIÓN

Por su parte, el estadístico de *Durbin-Watson* mide el grado de autocorrelación 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 tanto, podemos aseverar 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. 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: Sí 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 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 gestión						
b. Variables predictoras: (constante), sí 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 "Sí 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 18. Coeficientes

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

a. Variable dependiente: No hay riesgos de seguridad en la gestión.

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.

$$Y = a + b\,x \text{ (Ecuación de regresión lineal)}$$
$$Y = 10{,}785 - 0{,}986\,x$$

Observación: El Beta de la variable No Existe Riesgo es - 0,999. Esto significa que, a mayor uso de los Websites, mayor es el riesgo que representa la seguridad en la gestión de información.

El coeficiente de determinación múltiple (r^2)
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.

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

Se concluye que el 92.29% del Riesgo de Seguridad de la Websites está basado en la gestión de información cuando se usa las Websites.

5. Conclusiones

a) 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.
b) Para un mejor análisis de datos de investigación, una herramienta estadística SPSS es importante. Por esta razón, se la ha utilizado.
c) 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.

d) Del análisis e interpretación de los datos se puede apreciar, según la fuente de opinión, que el 53.15% de empresas indican que sí existen problemas de las Websites. Solamente el 46.9 % indican que no existen dichos inconvenientes.
e) 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.
f) Las pruebas de testeo nos permitirán conocer el nivel de seguridad. Estas pruebas evitarán los problemas con las Websites de las medianas empresas de Lima Metropolitana. Siempre la lealtad y honestidad del personal de la organización garantiza un mayor y mejor rendimiento.

6. Referencias bibliográficas

[1] P. Aguilera. *Seguridad informática*. Madrid: Editex, S.A., 2010.
[2] G. Pallas, *Metodología de un SGSI en un grupo empresarial jerárquico*, tesis de Maestría, Facultad de Ingeniería, Universidad de la República, Montevideo, 186 pp., 2009.
[3] J. Matalobos, "Análisis de riesgos de seguridad de la información", tesis profesional, Facultad de informática, Universidad politécnica de Madrid, Madrid. 274 pp., 2009.
[4] J. Areitio, *Seguridad de la información*. Madrid: Paraninfo, S.A., 2009.
[5] C. Chaín, *Introducción a la gestión y análisis de recursos de información en ciencia y tecnología*. Murcia: COMPOBELL, S.L., 1995.
[6] D. Raj, *Teoría del Muestreo*. Fondo de Cultura Económica, México 1980.
[7] S. Díaz, *Metodología de la investigación científica*. Lima: Editorial San Marcos, 2005.
[9] M. Fernández, "Técnicas comunes de ataque a equipos con sistema operativo Unix o derivados", tesis profesional, Universidad Nacional de Luján, Buenos Aires. 208 pp., 2008.
[10] J. González & Collazos, "Modelo de referencia para la introducción de iniciativas de gestión del conocimiento", *Ingeniare,* 17(2), 223-235, 2009.
[11] Harris y otros, *Hacking ético*. Madrid: Anaya Multimedia, S.A., 2005.
[12] S. Hernández, C. Fernández, y L. Baptista. *Metodología de la investigación*. México: McGraw Hill, 2003.
[13] G. Huilca. "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., 2012.
[14] La Nación, "Los principales riesgos de seguridad informática para las empresas locales". [En línea]. Disponible en http://www.lanacion.com.ar/907401-los-principales-riesgos-de-la- seguridad-informatica-para-las-empresas-locales [Accedido: 14-may-2016]
[15] N. Luhmann, *Sociología del riesgo*. México, D.F., Universidad Iberoamericana, A.C., 2006.
[16] G. Mojsiejczuk, "Seguridad en los sistemas operativos", tesis profesional, Facultad de Ciencias Exactas, Naturales y Agrimensura, Universidad Nacional del Nordeste, Argentina, 56 pp., 2007.
[17] F. Pacheco, y H. Jara, *Hackers al descubierto*. Madrid: Usershop¸2012.
[18] P. Patrón, y J. Espinoza, "El acceso a la información en la perspectiva de la protección de datos personales en el Perú. [En línea]. Disponible en http://www.derecho.usmp.edu.pe/cedetec/articulos/Ponencia_Patron_Espinoza_Ecuador.pdf. [Accedido: 14-may-2016]
[18] A. Pazmiño, "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., 2011.
[19] E. Prats, R. Buxarrais, & A. Tey, Ética de la información. Barcelona, Editorial UOC, 2004.
[20] L. Rodríguez, Ética. Bilbao: Biblioteca Autores Cristianos, 2001.

[21] RPP, "Páginas web del Gobierno peruano sufren ataques tras amenaza de Anonymous". [En línea]. Disponible en http://www.rpp.com.pe/anonymous -peru-noticia_378846.html. [Accedido: 12-may-2011]

[22] H. Sanchez, *Medodología y diseño de la investigación científica*, 4ta. edición. Lima-Perú: Editorial Visión Universitaria, 2009.

[23] C. Tori, *Hacking ético*. Buenos Aires: Mastroianni Impresiones, 2008.

[24] I. SumerVille, *Ingeniería de Software*, Madrid: Edit. Pearson, 2005.

[25] A. Verdesoto, "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., 2007.

[26] 24 Horas, "Hackers atacan página web de TV Perú en protesta a la masacre en Bagua". [En línea]. Disponible en http://www.24horas.com.pe/locales/125145-hackers-atacan-pagina-web-tv-peru-protesta-masacre-bagua. [Accedido: 12-jun-2013].