Análisis del reto de gestión de riesgos informáticos en PyMES Zona Zur de Tamaulipas

Manuel Eduardo Gutiérrez Ortiz[1], Mauricio Herrera Rodríguez[2] y Ana Elisa Moreno Herrera[3]

[1] *Universidad Autónoma de Tamaulipas, Facultad de Comercio y Administración de Tampico, Tampico, Tamaulipas, México, mgutierrez@docentes.uat.edu.mx, FCAT – UAT Campus Tampico S/N, (+52)8333007693*

[2] *Universidad Autónoma de Tamaulipas, Facultad de Comercio y Administración de Tampico, Tampico, Tamaulipas, México, mauherrera@gmail.com, FCAT – UAT Campus Tampico S/N, (+528331553166)*

[3] *Universidad Autónoma de Tamaulipas, Facultad de Comercio y Administración de Tampico, Tampico, Tamaulipas, México, aemoreno@docentes.uat.edu.mx, FCAT – UAT Campus Tampico S/N, (+52) 83332063627*

Información del artículo revisado por pares
Fecha de aceptación: junio-2021
Fecha de publicación en línea: diciembre-2021
DOI: https://doi.org/10.29105/vtga7.1-163

Resumen

Los retos y oportunidades de la implementación de nuevas tecnologías en las organizaciones enfrentan un desafío importante en la gestión de riesgos en el área de informática en las pequeñas y medianas empresas. En este trabajo se tiene como objetivo analizar cuantitativamente el impacto de dichos riesgos informáticos. Se realizo una investigación documental de artículos empíricos de donde se obtuvo un cuestionario que después de una prueba piloto de 40 sujetos, fue validado con una reducción de dimensiones y la aplicación de pruebas como la de Bartlett y KMO y después de definir los ítems se verificó su fiabilidad mediante el Alfa de Cronbach. Con el instrumento de investigación con validez total se aplicó a una muestra de 269 empresas PYMES de la zona sur del estado de Tamaulipas y después con un estudio correlacional explicativo, como resultado se obtuvo un modelo predictivo que comprobó que la gestión de riesgos en el área de informática disminuye la incidencia de delitos informáticos. El beneficio práctico de este trabajo permitirá a los pequeños y medianos empresarios tomar la decisión de invertir de manera más amplia en mecanismos de control de riesgos.

Abstract

The challenges and opportunities of the implementation of new technologies in organizations face an important challenge in risk management in the area of information technology in small and medium-sized companies. The objective of this work is to quantitatively analyze the impact of these computer risks. A documentary investigation of empirical articles was carried out from which a questionnaire was obtained that after a pilot test of 40 subjects, was validated with a reduction of dimensions and the application of tests such as Bartlett and KMO and after defining the items it was verified its reliability using Cronbach's Alpha. With the research instrument with full validity, it was applied to a sample of 269 SMEs in the southern area of the state of Tamaulipas and later with an explanatory correlational study, as a result a predictive model was obtained that verified that risk management in the area of computer science decreases the incidence of computer crime. The practical benefit of this work will allow small and medium entrepreneurs to make the decision to invest more broadly in risk control mechanisms.

Palabras clave: Área de informática, Delitos informáticos, Gestión de riesgos

Key words: Computing Area, Computer crime, Risk management.

Códigos JEL: M15, O33

JEL Codes: M15, O33

1. INTRODUCCIÓN

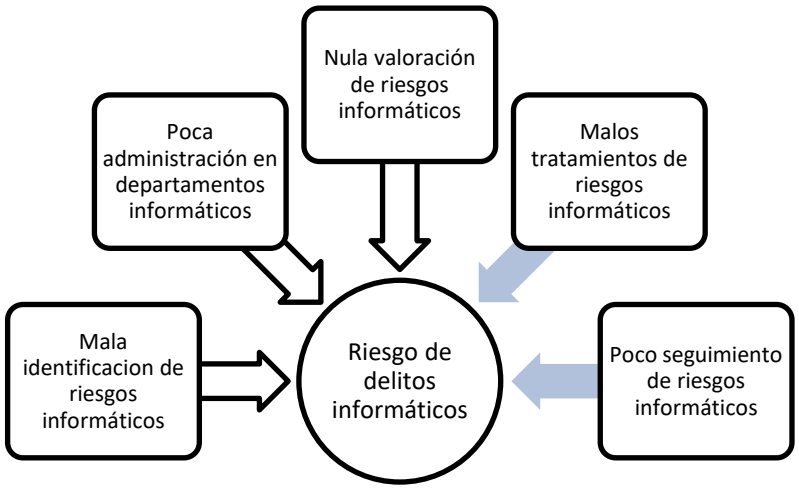
El área de informática en una organización es de vital importancia para el desempeño de sus actividades diarias y su propia supervivencia. Si la organización no cuenta con los mecanismos de gestión de riesgos adecuados para el área mencionada, es posible que el área mencionada sea deficiente en sus resultados o su costo de operación se eleve de manera desproporcionada y sin justificación. En la zona conurbada de Tampico- Madero - Altamira existen en noviembre de 2020 aproximadamente 890 empresas pequeñas y medianas que cuentan con una gestión informática según datos de las asociaciones CANACO, CANACINTRA, y CANIRAC en sus capítulos Tampico, Madero y Altamira; las cuales podrían optimizar su funcionamiento, a través del uso correcto de las tecnologías de la información, lo cual se puede lograr a través de mecanismos adecuados de control. En cuanto a la seguridad informática, según datos históricos (Pymenpresario, 2019), las pequeñas empresas, reciben el 36% de los ataques dirigidos al área de informática. En el ámbito de la legalidad de software, según datos de la Business Software Alliance en su reporte del año 2020 (BSA, 2020), en nuestro país el 49% del software se utiliza sin licencia, es decir, ilegalmente.

El objetivo de este artículo es difundir a la comunidad empresarial los elementos que pueden contribuir a la previsión de los delitos informáticos que pueden repercutir en daños en la información o económicos.

1.1. Planteamiento del problema

Cordero Morales, Ruiz y Torres (2013) afirman que … Un proyecto constituye una actividad progresiva, emprendida para crear un producto o servicio determinado. Por lo que su desarrollo necesita planificación y control debido a que requiere participación humana… por lo que la identificación de los riesgos es un elemento indispensable para la seguridad de las empresas. De la misma manera Novoa y Barrera (2015) mencionan que … la detección de fallas de seguridad, in- consistencias, redundancia y el descubrimiento de vulnerabilidades de seguridad, deben ser exploradas en etapas… por lo que respecto a los riesgos se requiere su administración, valoración, tratamiento, seguimiento y una comunicación eficaz que les permita a las empresas enfrentar de manera adecuada la incidencia de delitos informáticos. Por lo que se puede plantear al problema de investigación como el riesgo de delitos informáticos en las empresas y se representa en la figura 1.

Figura 1. Esquema del problema de investigación.



Fuente: Elaboración propia

1.2. Objetivo general

Determinar si las variables de administración de riesgos disminuyen la incidencia de los delitos informáticos en las PYMES de la zona sur del estado de Tamaulipas.

1.3. Hipótesis general

La identificación, administración, valoración y tratamiento de riesgos informáticos disminuye la incidencia de delitos informáticos en las PYMES del sur de Tamaulipas.

1.4. Preguntas de investigación.

La pregunta general de investigación es definir si ¿La identificación, administración, valoración y tratamiento de riesgos informáticos disminuye la incidencia de delitos informáticos en las PYMES del sur de Tamaulipas?

2. MARCO TEÓRICO

La teoría de los recursos analizada 10 años después de su planteamiento original, por Barney, Wright y Ketchen, (2001) muestra que los recursos deben ser administrados de manera eficaz y eficiente en particular cuando muestran las características de ser únicos, valiosos, inevitables y raros, tal y como fueron esbozados en 1991 dan pie a una metodología propuesta por Arévalo, Cedillo y Moscoso (2017) dado que los fabricantes suelen dedicar menos recursos a la seguridad de la información, son un objetivo popular para los ciberdelincuentes. Y solo se necesita un ataque cibernético para devastar todo el sistema operativo de un fabricante más pequeño. La maquinaria, los proveedores, los distribuidores o incluso los clientes conectados en red podrían ser pirateados a través de una computadora / dispositivo en una instalación de fabricación. Esto da pie al estudio de las siguientes variables.

2.1. Disminución de incidencia de delitos informáticos.

Las preocupaciones sobre los delitos cibernéticos han ido en aumento durante algún tiempo debido a una serie de ataques cibernéticos de alto perfil, nuevas regulaciones GDPR que harán que las empresas sean multadas por ser pirateadas y advertencias sin precedentes en EE. UU. Y el Reino Unido de que los piratas informáticos respaldados por Rusia están apuntando a la infraestructura de Internet occidental. (Alvarado-Zabala, Pacheco-Guzmán y Martillo-Alchundia, 2018)

El análisis de Beaming muestra que los ataques de ransomware como WannaCry y NotPetya fueron simplemente la punta del iceberg el año pasado. 2017 fue el peor año registrado por el gran volumen de ciberataques a empresas británicas, con todas y cada una de las empresas conectadas a Internet sometidas a un promedio de 231.028 ciberataques transmitidos por Internet, el equivalente a 633 ataques por día. El volumen de ataques continuó aumentando en los primeros tres meses de 2018, un período en el que la actividad adicional de delitos cibernéticos que se originó en los antiguos estados soviéticos significó que Europa superó a Asia para convertirse por primera vez en la fuente más común de ataques. Lo que incluso ha generado la búsqueda de protocolos para la mitigación de ciberataques (Olmedo y Gavilánez, 2018)

Por lo anterior se define en esta investigación a la disminución de incidencia de delitos informáticos que evite perdidas de información o económicas en la empresa.

2.2. Identificación de riesgos

Tejena-Macías (2018) comenta que la identificación de vulnerabilidades es una fase que desarrolla una lista de defecto o en ocasiones riesgos que pueden afectar la totalidad por lo que una metodología es interesante de implementar y es que uno de los mayores desafíos de la identificación de los riesgos es que la ciberseguridad es un campo en constante evolución, por lo que la identificación de riesgos es un objetivo en movimiento.

También Guerrero-Aguiar, Medina-León, y Nogueira-Rivera (2020) plantean pasos como los de establecer mecanismos para la identificación de los riesgos y coinciden en que con el tiempo ha evolucionado un enfoque básico que todas las metodologías de

identificación de riesgos tienden a seguir tales como el identificar los activos, las amenazas a esos activos y las vulnerabilidades a esas amenazas. Para determinar la exposición al riesgo cibernético, primero debe decidir cuáles son sus activos. Esto no es tan fácil como parece porque no se puede proteger todo, por lo que la empresa debe identificar los activos que deben protegerse y sus prioridades.

Por lo anterior se define en esta investigación a la identificación de riesgos como la identificación de los activos de información que tienen valor para la organización, asociar las amenazas con dichos activos, determinar las vulnerabilidades y el impacto que podría suponer una pérdida de confidencialidad,
integridad y disponibilidad para cada activo.

2.3. Valoración de riesgos

Gómez et al. (2019) en su plan de contingencia para los equipos y sistemas informáticos dan una propuesta metodológica para la evaluación de riesgos en proyectos de inversión en tecnologías de informática, esto es relevante porque la valoración de riesgos es fundamental para un programa sólido de seguridad de la información. Antes de que podamos implementar controles para prevenir un ataque, necesitamos saber el valor de lo que estamos protegiendo, la probabilidad de que ocurra una amenaza determinada, el costo de implementar el control preventivo y cómo tomamos la decisión de implementar el control. Entonces, la valoración de riesgos es la disciplina de identificar los riesgos que representan amenazas para la organización, identificando los controles potenciales que podrían mitigar esos riesgos y el proceso de toma de decisiones para determinar si implementar un control dado contra un riesgo dado.

También Figueroa et al. (2018) comentan que la seguridad informática es una disciplina que se encarga de evaluar los riesgos y que estos riesgos pueden ser vulnerabilidades que se expanden una gama de grises que puede ser muy amplia porque los riesgos se presentan de muchas formas y, a menudo, se clasifican de manera que separan los riesgos comerciales, los riesgos cibernéticos y los riesgos físicos entre sí. Sin embargo, en un programa de Gestión de Riesgos Empresariales (ERP) adecuado, no deben separarse. El liderazgo empresarial piensa en el riesgo en el contexto de nuevos competidores, caídas del mercado y nuevas condiciones regulatorias. Un director de instalaciones piensa en el riesgo en términos de tormentas eléctricas, fugas de gas o la pareja enojada de un empleado en el estacionamiento. El CIO piensa en el riesgo en términos de un ataque de denegación de servicio, ransomware en la base de datos clave o una computadora portátil perdida con información corporativa confidencial almacenada en el disco duro.

Por último Zabala, Castro y Rivera (2020) insisten que las tecnologías que facilitan la adquisición, almacenamiento, procesamiento, evaluación, transmisión, distribución y operación deberían de tener una metodología para la valoración de los riesgos y una valoración cuantitativa es más objetiva porque usa números para asignar un costo a los activos de una organización, la probabilidad de que ocurra una amenaza determinada, el valor esperado perdido en caso de que ocurra la amenaza y el costo de implementar la mitigación. Tener estos cálculos disponibles puede convertir la decisión de implementar un control en una sencilla decisión financiera.

Por lo anterior se define en este estudio a la valoración de riesgos como un adecuado estudio costo/beneficio entre el costo por pérdida de información y el costo de un sistema de seguridad, además de clasificar la instalación de dichos sistemas en términos de riesgo.

2.4. Tratamiento de riesgos

Jara (2018) comenta que la información que dé el resultado de la evaluación de riesgos informáticos debe ser atendida cuando la misma sea crítica y alta, de tal manera que la empresa debe destinar los recursos necesarios para cerrar estas acciones peligrosas con un plan de tratamiento y una metodología de Gestión de Riesgos de Seguridad de la Información. El tratamiento del riesgo es una parte cada vez más importante del trabajo de los gerentes y los ejecutivos de las tecnologías de la información. El tratamiento de riesgos incluye proteger los sistemas, las redes y los

datos corporativos, garantizar la disponibilidad de los sistemas y servicios, planificar la recuperación ante desastres y la continuidad del negocio, cumplir con las regulaciones gubernamentales y los acuerdos de licencia, y proteger a la organización contra una gama cada vez mayor de amenazas como virus, gusanos, software espía y otras formas de software malintencionado.

Menezo (2017) menciona que … además se logra incluir cierta variabilidad en los procedimientos que se implemente, el sistema será aún más robusto. La combinación más comúnmente utilizada en la actualidad es la autenticación mediante lo que se tiene y lo que se conoce como Two Factor Authentication… esta autenticación de dos factores es una de las mejores prácticas de seguridad de TI que proporciona una capa adicional de protección para el acceso al sistema. Es una medida de seguridad muy recomendable, pero nuestra encuesta anual sobre las mejores prácticas de gestión de TI muestra que no hay suficientes empresas que la utilicen de manera formal y coherente. Este informe comienza con una breve explicación de la autenticación de dos factores. A continuación, estudiamos los niveles de práctica y adopción de la autenticación de dos factores, examinándolos por tamaño de organización y sector.

Vera y Vera (2017) mencionan que el objetivo de la seguridad informática es proteger los recursos valiosos de la organización. El Tratamiento de Riesgos es el proceso de selección e implementación de medidas para modificar el riesgo. Las medidas de tratamiento de riesgos pueden incluir evitar, optimizar, transferir o retener el riesgo. Las medidas de seguridad se pueden seleccionar de un conjunto de medidas de seguridad que se utilizan dentro del Sistema de Gestión de Seguridad de la Información (SGSI) de la organización. En este nivel, las medidas de seguridad son descripciones verbales de varias funciones de seguridad que se implementan técnicamente como, por ejemplo, los componentes de software o hardware o las formas organizativas como las políticas y procedimientos establecidos.

Por lo anterior se define en esta investigación al tratamiento de riesgos como los elementos que conforman medidas para evitar perfeccionar, trasladar o paralizar el riesgo de la información y recursos informáticos y económicos de la empresa.

3. MÉTODO

Este trabajo tiene como objetivo determinar si los constructos independientes impactan en la variable dependiente por lo que en el tipo de estudio se realiza una investigación cuantitativa, descriptiva, correlacional, explicativa y transversal como se detalla en el punto 3.1. y siguientes.

El diseño de la investigación parte de una revisión a la literatura identificada en bases de datos de revistas indexadas en EBSCO y SCOPUS, a partir de ahí se definió un cuestionario de investigación con diversas preguntas que fue validado mediante una prueba piloto con 40 sujetos y después se aplicó una reducción de dimensiones con pruebas como los valores KMO y Bartlett (Salas-Arbeláez, Solarte y Vargas 2017; Hernández, 2015; Munévar et al. 2016), además de determinada su fiabilidad con el Alfa de Cronbach. (Soler y Soler, 2012; Merino-Soto, 2016)

Después el instrumento de investigación con validez total fue aplicado a la muestra seleccionada de la población y con análisis estadísticos se realizó una regresión lineal múltiple con el software SPSS V.25 con la que se después de analizar los descriptivos se determinó el modelo de investigación producto de este estudio y se establecieron las conclusiones y recomendaciones finales.

3.1. Población, muestra y sujetos de investigación.

La población de estudio son 890 PYMES, que cuentan con una gestión informática, en la zona sur del estado de Tamaulipas que corresponden a los municipios de Altamira, Madero y Tampico según datos de un censo realizado de manera personal y directo, en noviembre de 2020, con las gerencias de las asociaciones CANACO, CANACINTRA, y CANIRAC en sus capítulos Tampico, Madero y Altamira.

Los sujetos de estudio son los encargados de las áreas de informática y de

esta población se realiza la determinación del tamaño de la muestra para la aplicación del instrumento (SurveyMonkey, 2019) y se utiliza esta calculadora virtual porque el tamaño de la muestra debe determinar la cantidad de elementos que deben encuestarse para ser representativa de forma estadística. La mencionada calculadora virtual considera el tamaño de la población, el margen de error, el nivel de confianza del muestreo y la probabilidad de que ocurra dicho evento estadístico con fórmula mostrada en la figura 2.

Figura 2. Determinación de la muestra.

$$n = \frac{\frac{z^2\, p\,(1-p)}{e^2}}{1 + \frac{z^2\, p\,(1-p)}{e^2\, N}\ )}$$

n = Tamaño de la muestra
N = tamaño de la población
e = margen de error (porcentaje expresado con decimales)
z = puntuación z
p= probabilidad de éxito
N= 890
e = 5%
z= 1.96 (nivel de confianza del 95%)
p=50%

Tamaño de la muestra = 269

Fuente: Elaboración propia

La selección de los sujetos de estudio se realizó en base a un análisis aleatorio simple que se realizó con el padrón identificado de las empresas mencionadas en la población, el cual se registró en Excel y mediante una formula se seleccionaron los negocios que tenían la misma probabilidad de ser encuestados.

3.2. Modelo conceptual.

De la hipótesis general se desprenden las siguientes variables:

Variable dependiente: disminución de incidencia de delitos informáticos.

Variables independientes: Identificación de riesgos (IDRI); Análisis de Riesgos (ADRI); Valoración de riesgos (VDRI), Tratamiento de Riesgos (TRDR).

De donde se puede plantear el siguiente:

Modelo de la investigación.

$Y = \beta\ IDRI + \beta\ ADRI + \beta\ VDRI + \beta\ TRDR + \varepsilon$

Donde:

Y = Disminución de incidencia de delitos informáticos

IDRI= Identificación de riesgos

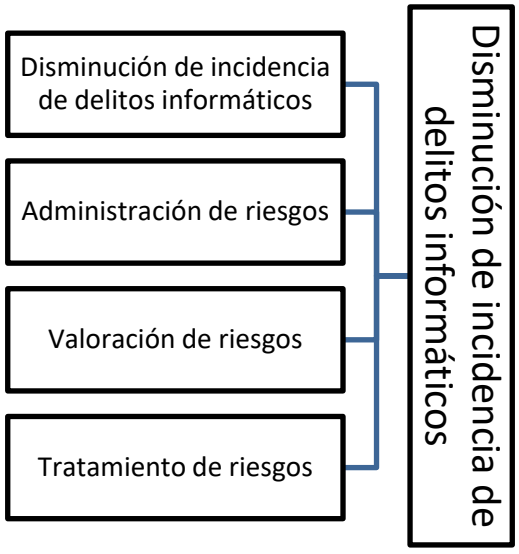
ADRI= Administración de riesgos

VDRI= Valoración de riesgos

TRDR= Tratamiento de riesgos

De lo anterior se puede representar el modelo conceptual en la figura 3

Figura 3. Modelo conceptual de la investigación.



Fuente: Elaboración propia

Las pruebas estadísticas para realizar son una reducción de dimensiones con rotación VARIMAX, así como la fiabilidad con el Alfa de Cronbach. Además, se realiza una regresión múltiple con los constructos independientes Identificación de riesgos, Administración de riesgos, Valoración de riesgos y Tratamiento de riesgos para ver como impactan a la Disminución de incidencia de delitos informáticos.

3.3. Instrumento de investigación.

Como ya se mencionó se realizaron cuestionarios que después de una prueba piloto, una reducción de dimensiones y un análisis de fiabilidad quedó definido un instrumento de investigación para los constructos seleccionados, con ítems con validez total que se muestra en la tabla 1.

Tabla 1. Instrumento de investigación

Variable	Ítem
Y	1. La incidencia de delitos informáticos procedentes del exterior de empresa tiene una tendencia a la baja.
	2. La incidencia de delitos informáticos procedentes del interior de empresa tiene una tendencia a la baja.
	3. Se han disminuido las perdidas cuantificables para la empresa causadas por delitos informáticos.
IDRI	1. Se han identificado los principales riesgos relacionados con uso de la informática en la organización.
	2. Antes de implementar un nuevo sistema, se realiza un análisis preliminar de riesgos.
	3. Se utiliza algún método o técnica para efectuar el análisis de riesgos.
	4. Existen bitácoras de las fallas de los equipos de cómputo y su atención
ADRI	1. Existen controles adecuados para las compras de hardware y software relacionadas con el área de informática
	2.Existen controles documentales y responsivas de la asignación de equipos y software de cómputo al personal
	3. Existen controles de versiones de software instaladas en los diferentes equipos de cómputo
	4. Se cuenta con la seguridad física adecuada para el área de informática (protección antiincendios, lugar libre de inundaciones, vigilancia)
	5. Se cuenta con la seguridad lógica adecuada para el área de informática (privilegios, claves de acceso, antivirus)
	6. El presupuesto que se asigna a la seguridad física, lógica y a la gestión de riesgos se

	considera el adecuado.
VDRI	1. Se realizan reuniones de trabajo para valorar la posibilidad de ocurrencia de un riesgo informático 2. En la valoración de los riesgos participa todo el personal involucrado en los procesos relacionados con la función informática. 3. Se ha cuantificado el impacto económico en la organización que tendría la ocurrencia de cada riesgo identificado 4. El proceso de valoración de riesgos se lleva a cabo de manera periódica
TRDR	1. Se han tomado medidas para disminuir el impacto en caso de ocurrir alguna de las situaciones identificadas como riesgos por el uso de TIC 2. Existen planes de contingencia para el caso de que ocurran algunas de las situaciones previstas como riesgos por el uso de la informática en la organización 3. Los planes de contingencia se revisan y actualizan para valorar su pertinencia. 4. El personal ha recibido entrenamiento adecuado para actuar en caso de una contingencia referente al área informática

Fuente. Elaboración propia

Los estudios de validación total del instrumento de investigación realizada con los estadísticos de la varianza total explicada ayudan a explicar los hallazgos que están relacionados con la hipótesis de este estudio, porque muestra el porcentaje acumulado que explica el constructo con las pruebas de Bartlett y KMO, que confirman la validez al presentar un Sig. menor de 0.05, en todos los casos y el Alfa de Cronbach, con valores mayores de 0.8 lo que confirma la fiabilidad de todos los constructos que se presentan en la tabla 2.

Tabla 2. Estadísticos y pruebas del instrumento de investigación

Ítem	Varianza	Bartlett	KMO	Alfa Cronbach
Y1	78.937	0.000	0.794	0.820
IDRI1	78.631	0.000	0.825	0.826
ADRI1	92.176	0.000	0.721	0.801
VDRI1	83.425	0.000	0.763	0.842
TRDR1	78.033	0.000	0.708	0.806

Fuente. Elaboración propia

4. RESULTADOS

Después de aplicar el instrumento de investigación a la muestra a 269 empresas que fueron seleccionadas, se tuvieron que rechazar 8 encuestas por identificarse inconsistencias y que fueron sustituidas por otras 8 nuevas empresas que se seleccionaron de la misma forma que las de la muestra original. Los resultados de los datos generales se presentan en tabla 3.

Tabla 3. Datos generales de la muestra

Tipo de negocio	Nivel educativo del encargado	Sexo
22 fábricas o constructoras 8.2%	0 Sin estudios 0%	118 Hombres 44%
136 Comercios 50.21%	5 Primaria 2%	151 Mujeres 56%
30 Negocios de alimentos 11.3%	8 Secundaria 3%	
81 Despachos o servicios 30.29%	13 Bachillerato 5%	
	243 Superior 90%	

Fuente. Elaboración propia

En la tabla 4 se muestran algunos descriptivos que verifican pruebas importantes para los constructos como menciona Etxeberria (2007) acerca de la ANOVA con valores menores de 0.05 para verificar que los datos de la varianza y que muestre su validez, también se revisa la no aditividad, que permite

hacer comparaciones múltiples lo que también explica la aceptación o rechazo de la hipótesis, de la misma forma con el valor de T cuadrado de Hotelling y Kolmogorov – Smirnov, todos con Sig. menores de 0.05, que muestran la bondad de ajuste, es decir cómo se corresponden los datos con la distribución teórica. (Uriel y Manzano, 2002; Ruiz, 2018)

Tabla 4. Descriptivos de constructos.

Ítem	ANOVA		T cuadrado de Hotelling		KMO	
	Sig.	No aditividad		Sig.	Estadístico de prueba	Sig. asintótica
Y	0.000	0.014	14.727	0.001	0.198	0.002
IDRI	0.000	0.003	21.437	0.000	0.189	0.000
ADRI	0.004	0.000	18.226	0.000	0.209	0.002
VDRI	0.000	0.007	17.897	0.000	0.194	0.000
TRDR	0.000	0.014	15.627	0.001	0.209	0.002

Fuente. Elaboración propia

Por último, se presentan los coeficientes de correlación y colinealidad que son los que permiten definir el modelo predictivo, al explicar la fortaleza de la relación lineal entre las variables, (Valverde y Valverde, 2006), además de la t de Student con Sig. menores de 0.05 lo que se muestra en la tabla 5.

Tabla 5. Coeficientes de correlación y colinealidad.

Model	**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**	**95.0% Confidence Interval for B**		**Correlations**			**Collinearity Statistics**	
	B	*Std. Error*	*Beta*			*Lower Bound*	*Upper Bound*	*Zero order*	*Partial*	*Part*	*Tolerance*	*VIF*
1 Constant	1.166	0.249		0.668	.005	.324	.657					
IDRI	0.065	0.050	0.065	0.309	.012	.033	.163	.244	.081	.052	.641	1.559
ADRI	0.035	0.056	0.030	0.629	.030	.075	.145	.299	.039	.025	.695	1.440
VDRI	0.015	0.054	0.013	0.286	.000	.090	.121	.234	.018	.011	.727	1.375
TRDR	0.007	0.052	0.007	0.133	.001	.095	.109	.334	.008	.005	.627	1.594

a. Variable Dependiente: Y *Colinealidad entre variables independientes VIF < 10*

Fuente. Elaboración propia con SPSS V.25

De acuerdo con todo el análisis realizado a la investigación con 269 encuestas, se puede concluir que las preguntas para cada constructo son válidas, no tienen correlación entre ellas, ninguna depende de las otras y el índice de factor de varianza VIF de todos los constructos indica que no existe multicolinealidad entre ellos, con lo que se puede dar por válido el modelo propuesto y permite establecer un modelo estadístico con parámetros de regresión significativos de (t) que justifican el modelo de esta investigación de la siguiente forma.

Y = 1. 166 + 0.065 IDRI + 0.030 ADRI + 0.013 VDRI + 0.007 TRDR + E

5. CONCLUSIONES

De acuerdo con esta investigación se puede afirmar que los elementos de la seguridad informática tienen un impacto con la disminución de la incidencia de delitos informáticos, de acuerdo con la hipótesis general que fue producto de la revisión de literatura científica encontrada, después de todo el proceso ya descrito y con los resultados de este trabajo se encontró que todas las variables fueron significativas.

Todos estos elementos de gestión de riesgos se predicen de acuerdo con el modelo producto de la investigación y respecto a la situación de 2021 en la que se realizó este estudio transversal en el Sur del estado de Tamaulipas. En particular habrá una disminución en la incidencia de delitos

informáticos y se recomienda a los empresarios que se recomienda identificar los principales riesgos relacionados con uso de la informática en la organización y de manera importante antes de implementar un nuevo sistema de gestión de riesgos se debe realizar un análisis preliminar de los mismos.

También es importante deben manejar controles adecuados para las compras de hardware y software relacionadas con el área de informática. De la misma forma manejar controles documentales y responsivas de la asignación de equipos y software de cómputo al personal. Así como manejar controles de versiones de software instaladas en los diferentes equipos de cómputo.

Otro aspecto importante es recomienda realizar reuniones de trabajo para valorar la posibilidad de ocurrencia de un riesgo informático y dentro de estas reuniones de valoración de los riesgos debe participar todo el personal involucrado en los procesos relacionados con la función informática además de cuantificar el impacto económico en la organización que tendría la ocurrencia de cada riesgo identificado.

Por último, se recomienda tomar medidas para disminuir el impacto en caso de ocurrir alguna de las situaciones identificadas como riesgos por el uso de las TI y definir planes de contingencia para el caso de que ocurran algunas de las situaciones previstas como riesgos por el uso de la informática en la organización además de que el personal debe recibir entrenamiento adecuado para actuar en caso de una contingencia referente al área informática.

REFERENCIAS

Alvarado-Zabala, J., Pacheco-Guzmán, J., & Martillo-Alchundia, I. (2018). *El análisis y gestión de riesgos en gobiernos de ti desde el enfoque de la metodología MAGERIT*. Contribuciones a las Ciencias Sociales, (noviembre).

Arévalo, F. M., Cedillo, I. P., & Moscoso, S. A. (2017). *Metodología Ágil para la Gestión de Riesgos Informáticos Agile Methodology for Computer Risk Management*. Revista Killkana Técnica. Vol, 1(2).

Valverde, G. R., & Valverde, B. R. (2006). Colinealidad y mínimos cuadrados ponderados. *Revista venezolana de análisis de coyuntura*, 12(1), 283-296.

Uriel, E., & Manzano, J. A. (2002). Análisis multivariante aplicado (Vol. 76, pp. 270-271). Paraninfo.

Etxeberria, J. (2007). Regresión múltiple. *Regresión múltiple*, 0-0.

Salas-Arbeláez, L., Solarte, M. G., & Vargas, G. M. (2017). Efecto de la cultura organizacional en el rendimiento de las PYMES de Cali. *Suma de negocios*, 8(18), 88-95.

Barney, J. B., Wright, M., & Ketchen, D. J. (2001). *The resource based view of the firm: Ten years after 1991*. Journal of Management, Vol 27, 625-43.

BSA (2020) Updated: BSA Framework for Secure Software, *BSA | The Software Alliance*. 2021 BSA | The Software Alliance.

Ruiz Bueno, A. (2018). Esquematización de modelos de Analisis de la Varianza (Anova y modelo lineal general).

Cordero Morales, D., Ruiz Constanten, Y., & Torres Rubio, Y. (2013). *Sistema de Razonamiento Basado en Casos para la identificación de riesgos de software*. Revista Cubana de Ciencias Informáticas, 7(2), 222-239.

Hernández, O. J. G. (2015). Validez y confiabilidad del instrumento "Percepción de comportamientos de cuidado humanizado de enfermería PCHE 3ª versión". *Aquichan*, 15(3), 381-392.

Munévar, F. R., Vargas, L. B., Borda, D. B., Alpi, S. V., & Quiceno, J. M. (2016). Validez de constructo y confiabilidad del Connor-Davidson Resilience Scale (CD-RISC 10) en población colombiana con enfermedades crónicas. *Salud & Sociedad*, 7(2), 130-137.

Figueroa-Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., & Saltos-Gómez, J. A. (2018). *La seguridad informática y la seguridad de la información*. Polo del conocimiento, 2(12), 145-155.

Gómez, E. F., Duchimaza, J., Holguín, J. R., & Lindao, M. A. (2019). Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT. Revista Científica y Tecnológica UPSE, 6(1), 34-41.

Guerrero-Aguiar, M., Medina-León, A., & Nogueira-Rivera, D. (2020). *Procedimiento de gestión de riesgos como apoyo a la toma de decisiones.* Ingeniería Industrial, 41(1).

Jara Pérez, D. F. (2018). *Valoración y Plan de Tratamiento de Riesgos de Seguridad de la Información para los Procesos Incluidos en el Alcance del SGSI del Cliente TGE de la Empresa ASSURANCE CONTROLTECH.*

Menezo, G. (2017). *Sistema de autenticación de dos factores basado en tarjeta inteligente y tecnologías NFC*. Atribución-NoComercial-SinDerivadas 3.0 España. UNIVERSIDAD DE CANTABRIA

Merino-Soto, C. (2016). Diferencias entre coeficientes alfa de Cronbach, con muestras y partes pequeñas: Un programa VB. *anales de psicología*, 32(2), 587-588.

Novoa, H. A., & Barrera, C. R. (2015). *Metodologías para el análisis de riesgos en los sgsi*. Publicaciones e Investigación, 9, 73-86.

Olmedo, J. I., & Gavilánez, F. L. (2018). *Análisis de los ciberataques realizados en América Latina*. INNOVA Research Journal, 3(9), 172-181.

Pymempresario (2019), Pymempresario.com Pymempresario – Plataforma colaborativa para emprendedores y PyMEs, *webrate*, Pymempresario.com is hosted by GOOGLE - Google LLC, US in United States.

SurveyMonkey (2019) Calculadora del tamaño de muestra, *SurveyMonkey Audience.*

Tejena-Macías, M. A. (2018). *Análisis de riesgos en seguridad de la información*. Polo del conocimiento, 3(4), 230-244.

Vera, V. D. G., & Vera, J. C. G. (2017). *Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas*. Scientia et technica, 22(2), 193-197.

Zabala, C. A. P., Castro, A. K. S., & Rivera, M. M. G. (2020). *Las Tics como herramienta para la gestión de riesgos*. RECIMUNDO, 4(1 (Esp)), 173-181.