UNIVERSIDAD PERUANA UNIÓN

ESCUELA DE POSGRADO

Unidad de Posgrado de Ingeniería y Arquitectura

Marco de referencia “HOGO” para ciberseguridad en PyMES basado en ISO 27002 y 27032

Tesis para obtener el Grado Académico de Maestro(a) en Ingeniería de Sistemas con Mención en Dirección y Gestión en Tecnología de Información

Autor:

Carlos Francisco Cruzado Puente de la Vega
Liset Sulay Rodriguez Baca

Asesor:

Mg. Lizeth Huanca López
Dra. Erika Acuña Salinas

Lima, enero del 2022

DECLARACIÓN JURADA DE AUTORÍA DE TESIS

Lizet Huanca López de la Escuela de Posgrado, Unidad de Posgrado de Ingeniería y Arquitectura , de la Universidad Peruana Unión.

DECLARO:

Que la presente investigación titulada: **"MARCO DE REFERENCIA "HOGO" PARA CIBERSEGURIDAD EN PYMES BASADO EN ISO 27002 Y 27032"** constituye la memoria que presenta el (la) bachiller Carlos Francisco Cruzado Puente de la Vega y bachiller Liset Sulay Rodriguez Baca para aspirar al Grado Académico de Maestro(a) en Ingeniería de Sistemas con Mención en Dirección y Gestión en Tecnología de Información cuya tesis ha sido realizada en la Universidad Peruana Unión bajo mi dirección.

Las opiniones y declaraciones en este informe son de entera responsabilidad del autor, sin comprometer a la institución.

Y estando de acuerdo, firmo la presente declaración en la ciudad de Lima a los 20 días del mes de enero del año 2022.

Lizeth Huanca López

ACTA DE SUSTENTACIÓN DE TESIS DE MAESTRO(A) 0

En Lima, Ñaña, Villa Unión, a 20 días del mes de enero del año 2022, siendo las 03:00 p. m, se reunieron en la modalidad online sincrónica, bajo la dirección del Señor Presidente del Jurado: Mg. Immer Elías Cuellar Rodriguez, el secretario: Dr. Josué Edison Turpo Chaparro, los demás miembros: Mg. Fernando Manuel Asin Gomez y el Mg. Nemias Saboya Rios y el asesor: Mg. Lizeth Geaninne Huanca Lopez, con el propósito de administrar el acto académico de sustentación de Tesis de Maestro(a) titulada: "Marco de referencia "HOGO" para ciberseguridad en PyMES basado en ISO 27002 y 27032" del Bachiller/Licenciado(a) Carlos Francisco Cruzado Puente de la Vega y Liset Sulay Rodriguez Baca Conducente a la obtención del Grado Académico de Maestro(a) en: Ingeniería de Sistemas

(Nomenclatura del Grado Académico)

con Mención en Dirección y Gestión de Tecnologías de Información El Presidente inició el acto académico de sustentación invitando al candidato hacer uso del tiempo determinado para su exposición. Concluida la exposición, el Presidente invitó a los demás miembros del Jurado a efectuar las preguntas, cuestionamientos y aclaraciones pertinentes, los cuales fueron absueltos por el candidato. Luego se produjo un receso para las deliberaciones y la emisión del dictamen del Jurado.

Posteriormente, el Jurado procedió a dejar constancia escrita sobre la evaluación en la presente acta, con el dictamen siguiente:

Bachiller/Licenciado (a): Carlos Francisco Cruzado Puente de la Vega y Liset Sulay Rodriguez Baca

CALIFICACIÓN	ESCALAS			Mérito
	Vigesimal	Literal	Cualitativa	
Aprobado	18	A-	Con nominación muy bueno	Sobresaliente

(*) Ver parte posterior

Finalmente, el Presidente del Jurado invitó al candidato a ponerse de pie, para recibir la evaluación final. Además, el Presidente del Jurado concluyó el acto académico de sustentación, procediéndose a registrar las firmas respectivas.

Presidente

Secretario

Asesor

Miembro

Miembro

Bachiller/Licenciado(a)

[a.]Marco de referencia “HOGO” para ciberseguridad en PyMES basado en ISO 27002 y 27032

Carlos F. Cruzado
UPG Ingeniería y Arquitectura,Escuela de Posgrado
Universidad Peruana Unión
Lima, Perú
0000-0001-7471-3140

Liset S. Rodriguez-Baca
UPG Ingeniería y Arquitectura,Escuela de Posgrado
Universidad Peruana Unión
Lima, Perú

0000-0003-1850-615X

Lizeth G.Huanca-López

UPG Ingeniería y Arquitectura,Escuela de Posgrado
Universidad Peruana Unión
Lima, Perú
0000-0003-0855-4406

Erika I. Acuña-Salinas
UPG Ingeniería y Arquitectura,Escuela de Posgrado
Universidad Peruana Unión
Lima, Perú
0000-0002-0907-719X

***Abstract*—A medida que las tecnologías de información y comunicación se van empoderando en las organizaciones, también son víctimas de ataques en el ciberespacio, generando ~~una~~ la necesidad de protección del activo más importante, la información. Por esta razón, es importante el desarrollo del marco referencial “HOGO” basado en las buenas prácticas del ISO 27002 y los controles de seguridad del ISO 27032 para la ciberseguridad en las PyMES. Los resultados de la investigación muestran los beneficios de la implementación del marco referencial “HOGO” en las PyMES, aplicando buenas prácticas relacionadas a la seguridad en internet, de las infraestructuras criticas para la información, seguridad de las redes y seguridad de la información.**

Keywords—Ciberseguridad, PyME, ISO 27032, marco referencial “HOGO”

I. Introduction

Desde inicios del 2020 hasta la actualidad la sociedad se encuentra viviendo una emergencia sanitaria, por ello, los consumidores a nivel mundial han adoptado el comercio electrónico para realizar compras de productos y servicios, a comparación de los tiempos pre pandemia[1]. Las consecuencias de esta coyuntura está afectando en gran medida a la economía mundial generando una profunda recesión y las empresas medianas y pequeñas(PyMES), las cuales desempeñan un rol importante en economías emergentes, se encuentran muy afectadas económicamente [2] [3].

Por ello, las PyMES están buscando adaptarse y permanecer activos en el mercado [3][4]. El cese de operaciones ha ocasionado que muchas empresas se encuentren enfrentando problemas financieros[5][6]. Aquellas PyMEs que aún se esfuerzan por mantenerse en el mercado han adecuado su modelo de negocio empleando tecnologías de la información [7][8]. En el Perú, el 55% de empresas han implementado las modificaciones en su organigrama con la finalidad de adecuarse al modelo de negocio digital, esto se caracteriza por el *home office* y las interacciones a través de la tecnología de información con clientes y proveedores [9]. Ante el incremento de estos cambios ha llamado la atención a personas inescrupulosas con el propósito de extraer información relevante de las PyMES. Además, solicitan una compensación económica por la recuperación de su información, afectando la continuidad de sus operaciones y bloqueando los accesos. Según el reporte del 2020 de Fortinet [10], en Latinoamérica, el número de intenciones de ciberataques durante el mismo periodo, asciende a 7.000 millones. Del mismo modo, el incremento de incidentes relacionados a *ransomware* se incrementó desde el último año, asimismo el *phishing* es el ataque más común [11]. Las PyMES que recientemente han migrado a plataforma digitales presentan un alto grado de vulnerabilidad de su información dado que cuentan con una infraestructura tecnológica débil [12]. Para las PyMES, esos ataques cibernéticos producto de las vulnerabilidades representan un fuerte impacto en términos económicos, de credibilidad y de fácil acceso a personas inescrupulosas con conocimientos en aspectos de ciberseguridad [13].

Algunas situaciones que enfrentan las PyMES son: (1) la filtración de datos que hace que la empresa pierda la confianza de sus clientes y proveedores (vulnerabilidades a nivel de aplicaciones, y a nivel de servidor), (2) también puede generar inestabilidad económica, porque la mayoría de los ciberdelitos se envían a través de ransomware para paralizar las operaciones comerciales y posteriormente solicitar una compensación económica para la recuperación de su información (vulnerabilidad a nivel de usuario)[14].

Según el estudio de Sophos del 2020, aproximadamente el 75% de los ciberataques de ransomware culminan en el cifrado de los datos [15]. Los cibercriminales lograron cifrar los datos en el 73 % de estos ataques. La mayoría de los ataques de ransomware exitosos incluyen información alojada en nube pública. La mayoría de PyMES emplean servicios como Google Drive, Dropbox y entre otros. [16].

Existen estudios que evidencian que el uso de marcos de referencia o modelos de seguridad de la información que mitigan las vulnerabilidades considerando el accionar de las personas y su responsabilidad en el cumplimiento de políticas para proteger la información de las organizaciones [17][18]. Sin embargo, estos antecedentes no consideran la ciberseguridad que, en la coyuntura actual, impacta fuertemente a la continuidad del negocio de las PyMES.

Por lo tanto, se propone el desarrollo de un marco referencial denominado “HOGO”. Esto está basado en dos normativas ISO 27002 y 27032, cuyo objetivo es reducir los posibles riesgos de ciberseguridad relacionado a las operaciones online, información financiera, imagen de las

PyMES, relación con clientes y proveedores y proteger el activo más importante: la información.

La estructura de este articulo comprende la introduccion, revisión de literatura, metodologia, resultados y conclusiones.

II. LITERATURE REVIEW

La ciberseguridad se sostiene en la seguridad de la información, seguridad de las aplicaciones, seguridad de la red y seguridad de internet como pilares principales. Además, corresponde a la protección necesaria a los servicios de infraestructura crítica[14]. La seguridad se encarga de la protección de los activos contra las amenazas. En tal sentido, se comprende por amenazas al potencial abuso de los activos protegidos.

Ciberespacio es el ambiente complejo producto de la interrelación entre los recursos humanos, *software* y servicios de internet a través de componentes tecnológicos virtuales en internet[14]. La seguridad en el ciberespacio se refiere a la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio[14].

La norma ISO 27001 proporciona los requerimientos para establecer, implementar, mantener continuamente un sistema de gestión de seguridad de la información que permita garantizar la confidencialidad, integridad y disponibilidad (CID) [19]. El propósito es proporcionar una metodología para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) en una empresa. En esta norma existen 4 etapas: planificar (P), hacer (D), verificar (C), actuar(A) [19].

NIST (National Institute of Standards and Technology) recomienda a los negocios de todo tamaño administrar y mitigar los riegos relacionados a ciberseguridad [20].

ISO 27002 brinda controles para la seguridad de la información en las organizaciones y prácticas de gestión para la seguridad de la información, considerando seleccionar, implementar y gestionar los controles tomando en cuenta los riesgos del contexto para la seguridad de la información de la empresa [21].

ISO 27032 proporciona recomendaciones para la seguridad de la información en las organizaciones y prácticas de gestión para la seguridad de la información, considerando seleccionar, implementar y gestionar los controles tomando en cuenta los riesgos del contexto para la seguridad de la información de la empresa [14].

Para conocer las características relevantes de los principales marcos de referencia y normas relacionados a la seguridad de la información, se elaboró un cuadro comparativo (ver tabla I).

TABLE I. CHART COMPARATIVE

Criterios	Marcos de trabajo, Normas			
	NIST	*ISO 27002*	*ISO 27032*	*ISO 27001*
Políticas y procedimientos de seguridad	X	X		X
Resguardo de CID	X	X	X	X
Manejo de incidencias	X	X	X	X
Manejo de recursos				X
Manejo de riesgos	X			X
Ataques			X	
Seguridad en Internet	X	X	X	X
Mejora continua	X	X	X	X
Código malicioso			X	X
Transferencia de información	X	X	X	X
Dispositivos móviles				X
Manejo de infraestructura	X			

Cada marco de referencia y norma de la seguridad de la información y/o ciberseguridad cuentan con un conjunto de criterios que permiten gestionar los diversos sistemas de información de una empresa. En base al análisis desarrollado, se determinó emplear ISO 27002 e ISO 27032 como normas base para la construcción del marco referencial “HOGO”.

En muchos países, se define a las pequeñas y medianas empresas (PyMES) a las organizaciones que tienen entre 10 y 250 colaboradores. Sin embargo, no existe una definición estandarizada de una PyME. Estas organizaciones, por naturaleza, pueden ser desde pequeños proveedores de servicios hasta proveedores de productos digitales, artesanías de calidad o instrumentos sofisticados con expectativas de negocio global[22]

La revision de la literatura realizada proporciona la base para afirmar que la ciberseguridad en las Pymes es relevante para enfrentar vulnerabilidades que se pueden generar en el ciberespacio y afectar la continuidad del negocio.

III. METHODOLOGY

A. Diseño e Implementación del modelo

La construcción del marco referencial “HOGO” integró las buenas prácticas del ISO 27002 y los controles de seguridad del ISO 27032. Esta integración ayuda a contextualizar la normativa para mejorar la ciberseguridad en las PyMES. En consecuencia, se ha planteado cinco fases y un conjunto de actividades para su desarrollo.

En la fase I denominada Determinación de requerimientos, se desarrolló la exploración de información. Además, se realizó la revisión de normativas, artículos científicos, tesis orientadas a la seguridad de la información y a la ciberseguridad en las organizaciones. Luego, se realizó el análisis de contexto considerando información clasificada referente a ciberseguridad en las organizaciones, se analizó cómo esas normativas responden a las necesidades actuales.

Fig. 1. Phase1: Determination of requirements

En la fase II denominada Diseño del marco referencial "HOGO"se ejecutó un análisis comparativo de los controles de las ISO 27002 y 27032, además, se evaluó la existencia de una convergencia, divergencia o complemento entre ellas; generando una lista de controles priorizados luego de haber discriminado algunos elementos en duplicidad o que no estaban orientados a la ciberseguridad. Una vez que se tuvo la lista de controles priorizados como insumo, se procedió a estructurarlos según las dimensiones: seguridad en internet, protección de las infraestructuras críticas para la información, seguridad de las redes, seguridad de la información. Las dimensiones tienen soporte teórico en la 27032.

Para la elaboración del instrumento de recolección de datos (lista de cotejo) se realizó de esta manera. En primer lugar, se diseñó una guía de ponderación considerando a cada dimensión como factor primario y a cada objetivo de control como factor específico. Cada factor primario equivale a 100%. Cada factor especifico se pondera el 100% entre la cantidad de controles de seguridad de cada objetivo de control (cantidad redondeada). En segundo lugar, se redactó cada control que fue evaluado y se estructuró según las dimensiones y objetivos de control. En tercer lugar, se aplicó la técnica de juicio de expertos para la validación del instrumento de recolección de datos. Dichos expertos tuvieron un perfil profesional destacado, con Título Profesional de Ingeniero de Sistemas con experiencia en el rubro de seguridad de la información, además, en ciberseguridad en organizaciones grandes, medianas y pequeñas. Los criterios de validación del marco referencial "HOGO" fueron la coherencia, pertinencia y relevancia referente a su aplicabilidad e impacto en PyMES considerando las dimensiones: seguridad en internet, protección de las infraestructuras críticas para la información, seguridad de las redes, seguridad de la información. El perfil de las PyMES fueron aquellas empresas que tienen entre 10 y 250 colaboradores y que sus procesos de negocios se desarrollen en el ciberespacio. Finalmente, como resultado se obtuvo el instrumento validado, asimismo, el documento del marco referencial estuvo preparado para ser implementado. El marco referencial se validó por su aplicación en contexto real de una PyME.

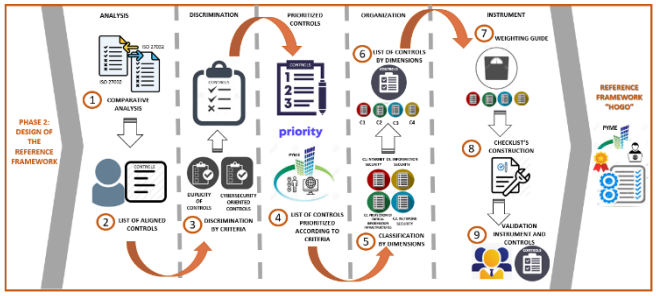

Fig. 2. Phase2: Design of the reference framework

En la fase III denominada Implementación del marco referencial "HOGO", se llevó a cabo en una PyME del rubro logístico. Para esto se realizó un análisis GAP, del mismo modo, se efectuó un diagnóstico situacional de la organización, que permitió conocer características relevantes de las operaciones, de los clientes y de los proveedores a través de la aplicación del instrumento de lista de cotejo, cuyo contenido fueron: las dimensiones, los objetivos de controles y los controles del marco referencial "HOGO". Los valores que se obtuvieron en el cumplimento de cada control de ciberseguridad se consideró como el pretest.

De acuerdo con los resultados del pretest, se han identificado los valores que no llegaron a la línea base establecida (55% de cumplimiento del objetivo de control) y se priorizó las oportunidades de mejora a implementar. Del mismo modo, se han aplicado criterios de priorización como: impacto, probabilidad de ocurrencia, presupuesto, disponibilidad de recursos y tiempo. Luego, se procedió con la ejecución de oportunidades de mejora priorizadas, realizando la implementación de controles de ciberseguridad para reducir las brechas existentes. Posterior a la implementación de controles de ciberseguridad se aplicó la lista de cotejo para verificar el cumplimiento de cada control. Con ello se han obtenido los datos del postest.

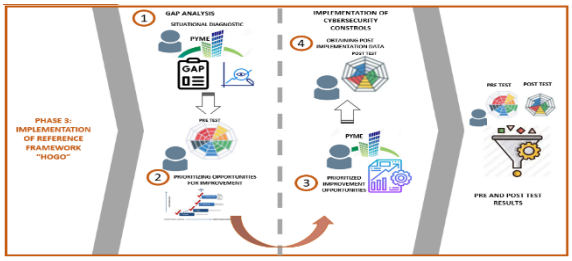

Fig. 3. Phase3: Implementation of refernece framework "HOGO"

En la fase IV denominada Visualización de resultados, se elaboró una matriz con los resultados obtenidos del pre y postest que permitió comparar dichos valores; luego se realizó la interpretación de resultados desarrollando un análisis de indicadores, verificando el porcentaje de cumplimiento de controles de ciberseguridad; permitiendo conocer si la brecha disminuyó o no.

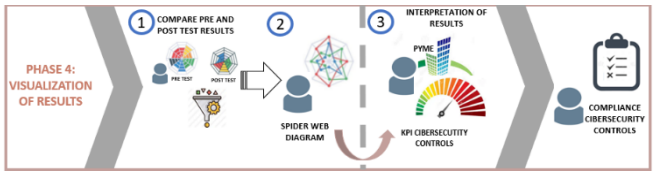

Fig. 4. Phase 4: Visualization of results

En la fase V, denominada Mejora continua se consideran controles que no alcanzaron el nivel esperado y se procede a registrar en el plan de mejora.

Fig. 5. Phase5:Continuous improvement

IV. RESULTS

En la fase uno denominada "Determinación de requerimientos" se logró revisar el estado de arte para conocer más acerca de la normativa de ciberseguridad y seguridad de la información, empleo de estrategias para el manejo o mitigación de vulnerabilidades en el ciberespacio. Además, se detectó que es imprescindible cubrir la brecha de conocimiento de ciberseguridad enfocada en las PyMEs, con la finalidad de reducir posibles riesgos que enfrentan estos negocios al realizar operaciones online, transferir información

financiera entre clientes y proveedores, compartir información sensible a través de la red y entre otros.

En la fase dos, "Diseño de marco referencial HOGO"; se desarrolló el marco referencial que está compuesto por 58 controles de ciberseguridad, organizados en cuatro dimensiones.

En la fase tres, se implementó el marco referencial "HOGO" en una PyME del rubro logístico. Esta PyME se encuentra doce años en el mercado, cuenta con un promedio treinta colaboradores que interactúan en el ciberespacio con los clientes y los proveedores. Asimismo, emplea sistemas de información como aplicativo móvil con geolocalización, GPS para el monitoreo de sus unidades móviles, manejo de cuentas en la nube pública y privada, comparten recursos empleando Google drive, OneDrive, herramientas digitales como zoom, meet para reuniones de negocio y trabajo.

Se recopiló información del pretest aplicando el instrumento de recolección de datos a los procesos de negocio de la PyME, y se obtuvo los siguientes resultados: En la figura 6, se observa que para la dimensión 1: Seguridad en Internet; se obtuvo un porcentaje de cumplimiento de 10% en aplicar controles de ciberseguridad referente a códigos maliciosos, 10% relacionado a revisión de requisitos legales y un 20% en empleo de herramientas para seguridad en internet.

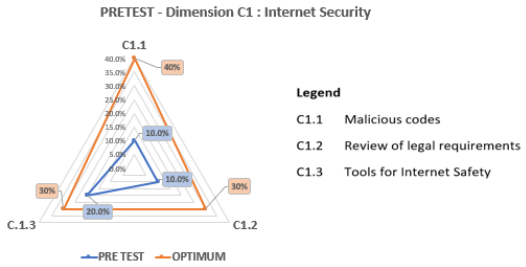

Fig. 6. Resultados del pretest – Dimensión 1: Seguridad en Internet

En la figura 7, se aprecia que para la dimensión 2: Protección de la infraestructura crítica para la información; se obtuvo un porcentaje de cumplimiento de 20% en aplicar controles de ciberseguridad referente análisis de vulnerabilidad del servidor, 10% en ejecución de software anti malintencionado, 20% en monitoreo y programación de intercambio de información proveedores.

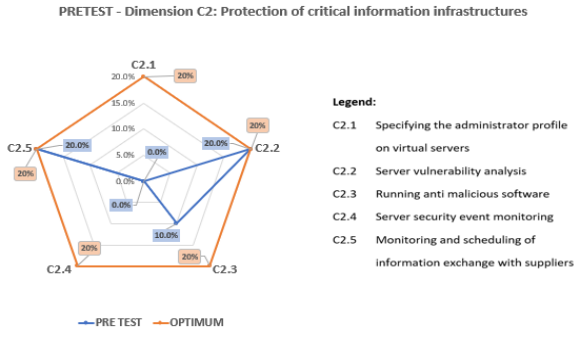

Fig. 7. Resultados del pretest – Dimensión 2: Protección de la infraestructura crítica para la información

En la figura 8, se observa que para la dimensión 3: Seguridad de las redes; se obtuvo un porcentaje de cumplimiento de 10% en aplicar controles de ciberseguridad referente a la seguridad de la red de usuarios finales, 5% en contar con políticas referente al empleo de *firewall* y sistemas de detección de intrusos(HIDS).

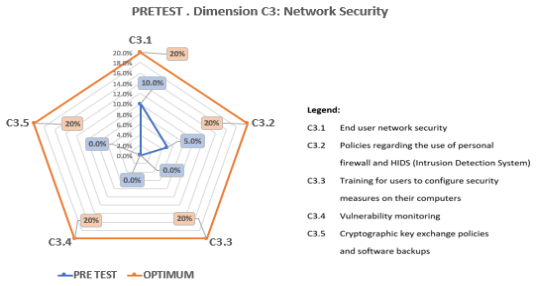

Fig. 8. Resultados del pretest- Dimensión3: Seguridad de las redes

En la figura 9, se observa que para la dimensión 4: Seguridad de la información; se obtuvo un porcentaje de cumplimiento de 10% referente a la aplicación de controles de ciberseguridad que empleen acuerdos de confidencialidad de información de usuarios,7.5% de cumplimiento en aspectos relacionados a la seguridad de la información en los acuerdos con clientes y proveedores, 5% referente a políticas de clasificación y categorización de información, procedimientos para clasificación de la información según su criticidad e importancia, 2.5% en acciones que involucren actualización periódica a los usuarios en temas de contrarrestar ataques de ingeniería social, instalación de software y publicación de controles para garantizar el mínimo nivel de seguridad.

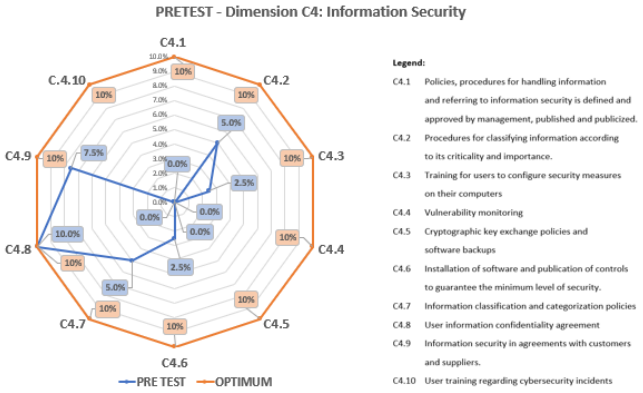

Fig. 9. Resultados del prestest- Dimensión4: Seguridad de la Información

Luego del análisis de la información obtenida en el pretest, se priorizó las oportunidades de mejora considerando la matriz impacto por urgencia, como se puede apreciar en la tabla II y tabla III.

TABLE II. MATRIZ DE PROBABILIDAD

Probabilidad de Ocurrencia	***Significado***	***Valor***
Recurrente	Casi certero que ocurra.	5
Probable	Probable que se produzca.	4
Posible	Probable que se produzca a veces.	3
Insual	Puede ocurrir en algún momento.	2
Remoto	Nunca puede ocurrir.	1

TABLE III. MATRIZ DE IMPACTO

Impacto	***Significado***	***Valor***
Catastrófico	Incluye directamente en el cumplimiento de las actividades principales, se pierde continuidad del negocio por un período prolongado.	5
Peligroso	Causa una pérdida significativamente.Además se refiere una cantidad importante de tiempo a la alta dirección en investigar y corregir errores.	4
Moderado	Causa pérdidas importantes pero manejable en tiempo y costo.	3
Menor	Causa un daño que se puede corregir en el corto tiempo, no afecta el cumplimiento de lo sobjetivos estratégicos.	2
Insignificante	Puede tener un pequeño o nulo efecto en la organización.	1

En la figura 10, se observa el baremo de acuerdo con el producto obtenido, considerando niveles desde muy bajo a muy alto.

BAREMO				
[1 -5]	[6-10]	[11-15]	[16-20]	[21-25]
MUY BAJA	BAJA	MEDIA	ALTA	MUY ALTA

Fig. 10. Matriz de impacto por urgencia

En la tabla IV, se puede apreciar la matriz de impacto por urgencia.

TABLE IV. MATRIZ DE IMPACTO

Probabilidad		**Impacto**				
		Catastrófico	***Peligroso***	***Moderado***	***Menor***	***Insignificante***
		5	4	3	2	1
Frecuente	5	25	20	15	10	5
Probable	4	20	16	12	8	4
Ocasional	3	15	12	9	6	3
Psible	2	10	8	6	4	2
Improbable	1	5	4	3	2	1

Considerando las oportunidades de mejora priorizadas, se procedió a su implementación , obteniendo los resultados del postest.

En la fase cuatro, visualización de los resultados; se realizó la comparación entre el porcentaje de cumplimiento antes y después de implementar el marco referencial “HOGO”.

En la figura 11, se observa la comparación entre el porcentaje de cumplimiento del pre y post test de la dimensión 1: Seguridad en Internet. Se observa que en el postest se obtuvo un porcentaje de cumplimiento de 40% en aplicar controles de ciberseguridad referente a códigos maliciosos, 20% relacionado a revisión de requisitos legales y un 30% en empleo de herramientas para seguridad en internet.

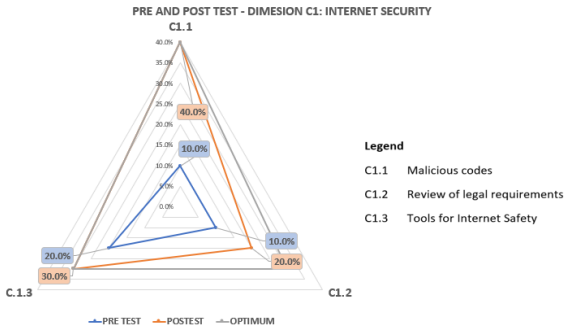

Fig. 11. Pre and postest results - Dimension 1: Internet Security

En la figura 12, se observa que para la dimensión 2: Protección de la infraestructura crítica para la información; en el postest se obtuvo un porcentaje de cumplimiento de 20% en aplicar controles de ciberseguridad referente a la especificación de perfil del administrador en los servidores virtuales, 20% en análisis de vulnerabilidad del servidor, 20% en ejecución de software anti malintencionado, 20% en supervisión de eventos de seguridad del servidor, 20% en monitoreo y programación de intercambio de información proveedores.

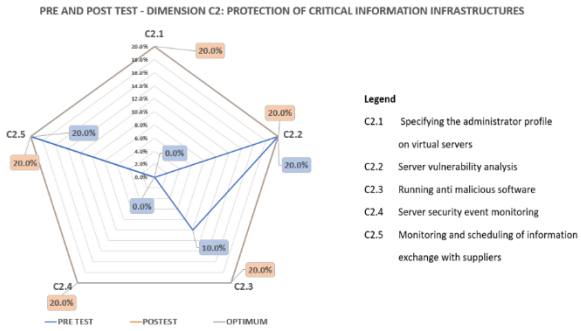

Fig. 12. Pre and postest results – Dimension 2: Protection of critical information infrastructures

En la figura 13 se observa que para la dimensión 3: Seguridad de las redes; en el postest se obtuvo un porcentaje de cumplimiento de 15% en aplicar controles de ciberseguridad referente a la seguridad de la red de usuarios finales, 10% en contar con políticas referente al empleo de firewall y sistemas de detección de intrusos(HIDS), 20% en capacitación a usuarios de configuración de medidas de seguridad en sus computadoras, 20% en monitoreo de vulnerabilidades y 20% en políticas de intercambio de claves criptográficas y copias de seguridad de software.

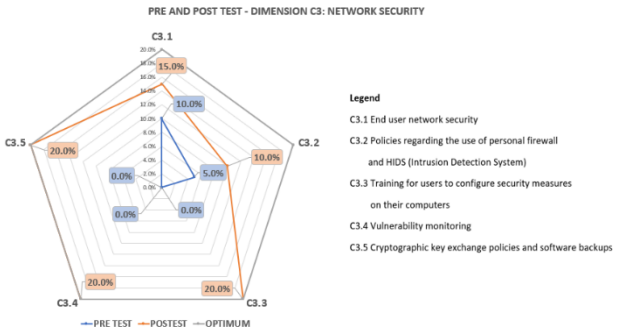

Fig. 13. Pre and postest results – Dimension 3: Network Security

En la figura 14 se observa que para la dimensión 4: Seguridad de la información; se obtuvo en el postest un

porcentaje de cumplimiento de 10% en aplicar controles que involucren a las políticas, procedimientos de manejo de la información y referentes a la seguridad de la información que se encuentran definidas y aprobadas por la gerencia, publicada y socializada; 5% de cumplimiento relacionado a procedimientos para clasificación de la información según su criticidad e importancia, 10% de cumplimiento de controles relacionados a la actualización periódica a los usuarios referente a los conocimientos para contrarrestar ataques de ingeniería social, 10% referente a instalación de software y publicación de controles para garantizar el nivel mínimo de seguridad, 10% referente a políticas de clasificación y categorización de información, 10% referente a la aplicación de controles de ciberseguridad que empleen acuerdos de confidencialidad de información de usuarios,10% de cumplimiento en aspectos relacionados a la seguridad de la información en los acuerdos con clientes y proveedores, 10% de cumplimiento en capacitación al usuario referente a los incidentes de ciberseguridad.

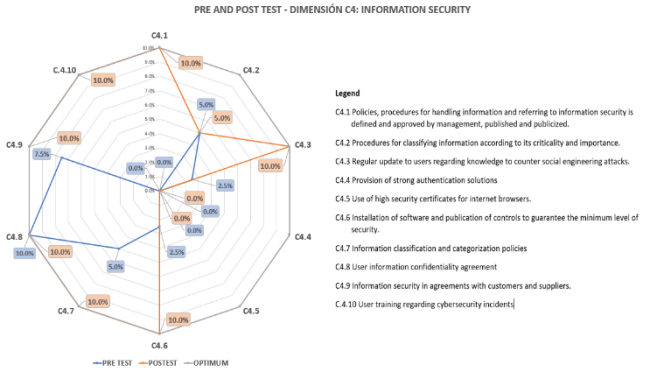

Fig. 14. Pre and postest results – Dimension 4: Information Security

A pesar de la implementación de las oportunidades de mejora, aún existe una brecha del 10% en el control de ciberseguridad de revisión de requisitos legales de la dimensión 1. En la dimensión 3, aún mantiene un porcentaje de 15% de incumplimiento de los controles relacionados a la seguridad de la red en usuarios finales y políticas referente al empleo de firewall personal y HIDS (Sistema de detección de intrusos). Asimismo, se tiene un 25% de incumplimiento de controles en la dimensión 4 relacionados con la provisión de soluciones de autenticación sólida y el uso de certificados de alta seguridad para navegadores de internet. Estas oportunidades de mejora que no alcanzaron el nivel esperado serán consideradas en el plan de mejora que corresponde a la fase V denominada mejora continua.

V. CONCLUSION

La implementación del modelo referencial "HOGO" permite que una organización brinde confianza a sus clientes, proveedores, socios estratégicos al realizar transacciones online. Las PyMES que implementan los controles de seguridad recomendados en el marco referencial en mención, aplican buenas prácticas relacionados a la seguridad en internet, de las infraestructuras criticas para la información, seguridad de las redes y seguridad de la información. Toda PyME que logre aplicar los controles de ciberseguridad del marco referencial mencionado garantiza los pilares de la seguridad de la información tales como la integridad, disponibilidad y confidencialidad.

Al aplicar los controles de ciberseguridad del marco referencial "HOGO", se logró reducir la brecha inicial de la organización referente a la ciberseguridad. Se afirma que se cumple el proceso de mejora continua, ya que los controles de ciberseguridad que no alcanzaron el nivel esperado fueron considerados como insumo para el plan de mejora que se implementará en un tiempo cercano planificando una inversión para su ejecución.

Existen controles de ciberseguridad que requieren un mayor tiempo para evaluar su impacto como por ejemplo las políticas referentes al empleo de firewall personas y sistema de detección de intrusos (HIDS).

Por lo tanto, el marco referencial "HOGO" es pertinente para que las PyMES que empleen tecnologías de información y comunicación (TIC´S), internet en el desarrollo de sus operaciones; implementen controles de ciberseguridad, ya que no requiere mucha inversión, pero si dedicación en la implementación de acciones de mejora, así como también crear una cultura de ciberseguridad en los recursos humanos para que actúen como protección en ataques de ingeniería social.

REFERENCES

[1] UNCTAD, "COVID-19 and E-commerce," 2020.

[2] OMC, "Comité de Obstáculos Técnicos al Comercio," 2021.

[3] Organizacion internacional del Trabajo, "Prevención y mitigación de COVID-19 en el trabajo para Pequeñas y Medianas Empresas," 2020.

[4] Naciones Unidas, "Informe Especial COVID-19 No 4: las empresas frente a la COVID-19: emergencia y reactivación," pp. 1–24, 2020.

[5] IPE, "Informe ipe," *Décimo quinto Inf. análisis del impacto económico del Covid-19 en el Perú- JUNIO 2020*, vol. 15, pp. 1–45, 2020, [Online]. Available: https://www.ipe.org.pe/portal/informe-ipe-xv-impacto-del-covid-19-en-la-economia-peruana/.

[6] A. Zurita Heredia and M. Dini, "Análisis de las políticas de apoyo a las pymes para enfrentar la pandemia de COVID-19 en América Latina," *Cepal*, p. 118, 2021, [Online]. Available: https://repositorio.cepal.org//handle/11362/46743.

[7] M. C. Fernández Díez and P. Puig Gabarró, "Los desafíos del comercio electrónico para las PyME: Principales claves en el proceso de digitalización," *Los desafíos del Comer. electrónico para las PyME Princ. claves en el proceso Digit.*, 2020, doi: 10.18235/0002311.

[8] F. León, "E-commerce Latinoamérica.En tiempos del COVID-19 2020," 2020. https://latam.payu.com/reporte-covid.

[9] Confiep, "Liderando la transformación hacia un nuevo entorno laboral," 2020. https://www.confiep.org.pe/noticias/el-55-de-empresas-peruanas-ya-ha-implementado-cambios-en-su-estructura-organizacional-para-adaptarse-a-un-nuevo-modelo-digital-caracterizado-por-el-trabajo-remoto-segun-un-estudio-de-ey/.

[10] Fortinet, "Resumen Ejecutivo Global." https://www.fortiguardthreatinsider.com/es/bulletin/Q4-2020.

[11] Verizon, "DBIR 2021 Data Breach Investigations Report," *Postmedieval*, vol. 11, no. 1. 2021, [Online]. Available: https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf?_ga=2.158153790.541921009.1629683026-1925016902.1629683026.

[12] G. Update and W. Efforts, "State of Cybersecurity 2020," pp. 1–23, 2020.

[13] ESET, "Security Report Latinoamérica 2021." [Online]. Available: https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf.

[14] ISO/IEC 27032:2012, "INTERNATIONAL STANDARD ISO / IEC techniques — Guidelines for information," vol. 2008. 2012.

[15] Sophos, “Informe De Amenazas,” 2020.

[16] M. Esther and G. D. E. Pedro, “El Estado del Bienestar,” *Filosofia*, pp. 261–263, 2001.

[17] Z. N. Rasulovich, “Information Security Issues For Travel Companies - IEEE Conference Publication,” [Online]. Available: https://ieeexplore.ieee.org/document/9011896.

[18] K. E. H. A. Alhosani, S. K. A. Khalid, N. A. Samsudin, S. Jamel, and K. M. Bin Mohamad, “A policy driven, human oriented information security model: A case study in UAE banking sector,” *2019 IEEE Conf. Appl. Inf. Netw. Secur. AINS 2019*, pp. 12–17, 2019, doi: 10.1109/AINS47559.2019.8968705.

[19] ISO/IEC27001, “Information Technology.Security techniques . Information Security management systems. Requirements.” .

[20] NIST Cybersecurity Framework Team, “Framework for improving critical infrastructure cybersecurity,” *Proc. Annu. ISA Anal. Div. Symp.*, vol. 535, pp. 9–25, 2018.

[21] ISO/IEC 27002:2013, “Information technology- Security Techniques- Code of practice for information security controls.” 2013.

[22] OMC, “Igualdad de condiciones para el comercio de las pymes,” p. 210, 2016, [Online]. Available: http://onlinebookshop.wto.org.