Modelo de madurez para los protocolos de seguridad en la fuga de datos de empresas de telecomunicaciones aplicando el marco de framework de NIST

1st Solis Leon, Brian Joel
Departamento de ingeniería de sistemas
Universidad Peruana de Ciencias Aplicadas (UPC)
Lima, Perú
U201812234@upc.edu.pe

2nd Di Paola Jara, Renzo Giovanni
Departamento de ingeniería de sistemas
Universidad Peruana de Ciencias Aplicadas (UPC)
Lima, Perú
U20171C422@upc.edu.pe

3rd Copaja Cornejo, Richard Nivaldo
Departamento de ingeniería de sistemas
Universidad Peruana de Ciencias Aplicadas (UPC)
Lima, Perú
PCSIRCOP@upc.edu.pe

***Abstract*— Los ataques dirigidos a la seguridad de la información y las filtraciones de datos en las empresas de telecomunicaciones en Perú ocasionan considerables pérdidas tanto económicas como en términos de reputación social. Por esta razón, se han implementado protocolos de respuesta para hacer frente a estas situaciones. Sin embargo, la mera implementación y desarrollo de estos protocolos no es suficiente para prevenir o contrarrestar los ataques de manera efectiva. Por lo tanto, se propone una solución tecnológica que combina un modelo de evaluación de madurez para los protocolos y un sistema de informes que proporciona información sobre el nivel actual y las posibles mejoras que se pueden aplicar a los protocolos evaluados. Nuestro proyecto tiene como objetivo reducir los ataques a las empresas del sector de las telecomunicaciones y al mismo tiempo permitirles evaluar el estado de sus protocolos en términos de ciberseguridad, lo que les brinda un mayor conocimiento sobre las posibles situaciones que podrían resultar de un mal uso de los protocolos. Para validar nuestro proyecto, hemos contado con la participación de 4 expertos en ciberseguridad, quienes lo han utilizado durante un período determinado con el fin de obtener información suficiente para ofrecer su opinión. Al finalizar el período de uso, se les envió un formulario para evaluar el nivel de satisfacción con respecto a nuestro proyecto, utilizando los indicadores que hemos establecido. El nivel final de satisfacción obtenido fue del 73.88%, lo que indica que nuestro proyecto ha tenido éxito según la evaluación de los expertos en seguridad.**

Index Terms – Modelo de madurez, protocolos de respuesta, NIST, evaluación

I. INTRODUCCIÓN

Los datos son fundamentales para cualquier empresa, debido a que no son solo relevantes para análisis de datos, sino también para otros sectores como finanzas, marketing, ventas, y desarrollo, entre otros [1]. Por ello, si los datos se exponen a ciberdelincuentes de ingeniería social seria crucial para la empresa porque se expondría información confidencial [2]. Las empresas peruanas son muy vulnerables, es por ello por lo que Perú ocupo el puesto 40 en el país con mayor registro a ataques cibernéticos [3].

Los ataques cibernéticos ocurren en cualquier empresa no importa el tamaño como en Chile donde el phishing está afectando a grandes empresas[4] o en Ecuador donde las fugas de información están alertando a las Pymes [5]. Dentro del Perú, en los años 2020, se registró 72 mil intentos de Ransomwares dentro de los meses de enero a septiembre [6]. Dentro de las soluciones planteadas para estos problemas varias empresas emplean protocolos de seguridad en la seguridad de la información. No obstante, esto no es lo suficiente para solucionar el problema debido a que ciertos protocolos no se encuentran bien implementados. El 71% de los ataques de seguridad de la información se debe a fallos tecnológicos, entre ellos corresponde el 31% el mal uso humano de las normas ISO [7].

Dentro de las tecnologías que se presentan actualmente existe una solución que es un modelo de madurez de capacidades de ciberseguridad para identificar el impacto de los factores de eficiencia interna en la efectividad externa de la ciberseguridad, cuyo resultado fue en el apoyo de aumentar la eficacia de la ciberseguridad [8]. Además, dentro de los protocolos QKD de ciberseguridad mejorados, detallan que se crean algoritmos para la detección de ataques informáticos [9].

A pesar de los resultados de los proyectos anteriores, no existe una solución detallada para los protocolos de respuesta frente un escenario de ataque cibernético. Con el objetivo de evitar los riesgos asociados con la falta de protocolos de seguridad que se adapten a las situaciones actuales, se ha propuesto la creación de un modelo de madurez que pueda evaluar el nivel de seguridad de una empresa frente a casos reales.

Para nuestros clientes del sector de telecomunicaciones, se ha realizado un modelo de madurez a través de un sistema en el cual les permite identificar el nivel de madurez de los protocolos de respuesta. El modelo va enfocado a lo que es prevención de fuga de datos, es por ello, que la evaluación se ha

realizado con el marco de framework de NIST. Las respuestas que se indican en el sistema donde se está evaluando nos permite no solamente identificar el estado deseado, las brecas y mejoras que pueden emplear.

El presente estudio está organizado de la siguiente manera: en la sección 2 se exponen investigaciones previas relacionadas con el tema a tratar. La sección 3 se enfoca en el desarrollo del modelo de modelo de madurez y sus niveles, mientras que en la sección 4 se muestran los resultados obtenidos y se discuten. Finalmente, la sección 5 expone las conclusiones y las recomendaciones para futuros trabajos.

II. TRABAJOS RELACIONADOS

Dentro del ámbito de los modelos de madurez enfocados en la seguridad de datos y ciberseguridad se han encontrado 5 trabajos que presentan una propuesta similar a la que nosotros hemos estado planteando.

TABLE I.
Trabajos relacionados

Rubro	Tecnologías	Año	Métrica	Source
Protocolos de seguridad de la información	Modelo de protocolo PTP	2021	Detección de impactos en la empresa.	[8]
Modelo de madurez	Modelo de madurez ISM3	2021	Estudio de modelo de madurez.	[9]
Protocolos de seguridad de la información	Protocolos de fuga de datos	2022	Detección de 40% de amenazas internas.	[10]
Modelo de madurez	Modelo de madurez CMMI	2022	Gestión de los niveles de madurez e implementación de una optimización de los niveles	[11]
Modelo de madurez	Modelo de madurez MIL4	2020	Reducción de los impactos de ciberseguridad	[12]

La investigación realizada nos ha permitido examinar cómo se aplican los modelos de madurez en escenarios de ciberseguridad. Se han identificado diferentes niveles de madurez utilizados en algunos casos [12]. Estos niveles ayudan a salvaguardar la seguridad del sector en el que se aplican, brindando una descripción de la situación actual. Cada modelo tiene su propia forma de representar los niveles de madurez, pero todos cumplen el objetivo de proporcionar información sobre el estado actual de un contexto específico [9]. Por ejemplo, un estudio de modelo de madurez reveló la necesidad de automatizar los recursos para la atención al cliente y los controles de seguridad [11].

Los niveles de madurez no solo nos brindan una visión de la situación actual de lo que se está evaluando, sino que también permiten métricas de evaluación y análisis para una mejor comprensión y planificación de acciones futuras. En este trabajo, se identificó que los niveles de madurez menos relevantes eran la gestión cuantitativa y la optimización sostenible. Estos tres trabajos están relacionados con el uso de modelos de madurez y la aplicación de niveles de madurez. Cada uno de ellos nos proporciona una perspectiva de lo que se puede lograr al identificar y utilizar los niveles de madurez, así como los beneficios que ofrecen en las evaluaciones y análisis de resultados. Estos trabajos están estrechamente relacionados con los aspectos investigados en nuestro propio proyecto.

Los protocolos relacionados con la seguridad de la información y la ciberseguridad son de gran utilidad, ya que nos permiten tener una visión clara de la dirección que tomará nuestro proyecto [8]. El autor de un estudio se enfocó en mejorar los protocolos de seguridad con el objetivo de proteger de manera eficiente y ordenada la infraestructura informática y todo lo que esté conectado a ella. Como resultado, se realizó un análisis exhaustivo de los protocolos de seguridad y su capacidad de respuesta [10].

Por otro lado, la investigación realizada nos proporciona protocolos para protegernos de fugas de datos e identificar posibles amenazas internas. A partir de esta evaluación de protocolos, se logró detectar más del 40% de las amenazas internas. El objetivo de examinar múltiples investigaciones centradas en sus protocolos es observar cómo se evalúan los protocolos en diferentes casos y analizar los resultados obtenidos a partir de estas evaluaciones.

En resumen, los protocolos de seguridad de la información y la ciberseguridad desempeñan un papel crucial en la protección de la infraestructura informática. Las investigaciones realizadas se centran en mejorar y evaluar estos protocolos, lo que nos brinda información valiosa sobre su eficacia y los resultados obtenidos.

III. CONTRIBUCIÓN

A. Inicio

En el ámbito de las telecomunicaciones, el uso de la información es fundamental. Por lo tanto, si se produce una filtración de datos, las empresas podrían sufrir graves consecuencias. Con el fin de abordar este problema, hemos creado un sistema de evaluación y automatización de resultados que establece un modelo de madurez. Este modelo evalúa los protocolos de respuesta en casos de filtraciones de datos, con el objetivo de prevenir riesgos que las empresas de telecomunicaciones no habían identificado previamente.

B. Método

1. Propuesta

En este estudio se propone una solución tecnológica junto con un modelo de madurez para evaluar los protocolos de respuesta en el sector de las telecomunicaciones. Mediante esta evaluación, se buscarán las discrepancias y deficiencias que presentan los protocolos en relación con la situación actual del sector. El proyecto consta de dos partes: evaluación y generación de informes. Para llevar a cabo la evaluación, se ha utilizado el marco de NIST[13], ya que proporciona un enfoque integral, basado en estándares y mejores prácticas, flexibilidad, enfoque basado en riesgos, orientación práctica y amplia aceptación en cuanto a la seguridad de la información.

La figura 1, ilustra la interacción entre nuestro proyecto y el cliente, así como el seguimiento realizado para garantizar un funcionamiento claro. También se visualiza cómo interactúan las capas de negocio y las de datos en nuestro proyecto.

Después de cada evaluación de los protocolos, el usuario tendrá la capacidad de ver los resultados de su análisis. Los informes que hemos desarrollado proporcionan una comprensión más clara de las situaciones experimentadas por los usuarios evaluados, al mismo tiempo que nos ofrecen opciones de mejora que podemos implementar para fortalecer nuestros protocolos.

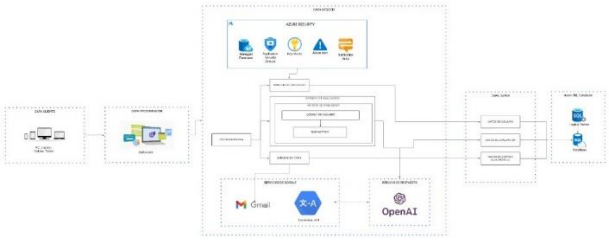

Fig 1. Arquitectura física del proyecto que se empleó para el desarrollo del software.

2. Modelo de madurez

Para poder desarrollar nuestro proyecto, hemos tenido primero que plantear cuales deben ser nuestros niveles de madurez. Finalmente, escogimos los niveles de madurez de CMMI[14] dándole un enfoque de lo que trata situaciones de la empresa de sector de telecomunicaciones con respecto a fuga de datos. Nuestros niveles de madurez son los siguientes.

a. *Inicial:* Los protocolos de respuesta no se encuentran en condiciones estables frente a posibles casos de ataques de ciberseguridad, o no se encuentran implementados.
b. *Gestionado:* Los protocolos de respuesta solamente realizan actividades que se han planificado, más no involucra otros actores. Presentan brechas de mejora .
c. *Definido:* Los protocolos de respuesta son entendidos y descritos por estándares, procedimientos, herramientas y métodos.
d. *Predecible:* Los protocolos de respuesta presentan el objetivo claro para afrontar los ataques de ciberseguridad. Describe las acciones de cada proceso
e. *Optimizado:* Los protocolos de respuesta presentan mejora continua frente a cada posible ataque de ciberseguridad que se presenta. Presentan objetivos claros y detalle de las acciones.

3. Modelo de desarrollo

En nuestro proyecto, llevamos a cabo una evaluación de los protocolos utilizando un conjunto de 31 preguntas que se basan en las subcategorías del marco de framework de NIST. Cada pregunta va acompañada de respuestas que simulan situaciones reales que podrían enfrentar los protocolos. Estas respuestas proporcionan información crucial para el análisis de los protocolos, enriqueciendo nuestros informes en Excel y PDF. En la segunda imagen, se muestran las subcategorías seleccionadas para nuestra evaluación, junto con sus funciones principales y la pregunta correspondiente a cada subcategoría. La elección de estas 31 subcategorías, en lugar de las 108 que ofrece el marco de framework de NIST, se basa en su capacidad para expresar y brindar un mejor entendimiento de las situaciones que enfrentan las empresas del sector de las telecomunicaciones, así como los principales motivos detrás de la fuga de datos.

TABLE II.
Preguntas de evaluación de protocolos de respuesta

Función	Subcategoría	Pregunta
Identificar	ID.GV.1	¿Cómo se establecen las políticas de seguridad cibernética y quienes son los implicados?
	ID.GV.2	¿Cómo se distribuye los roles y responsabilidades de la seguridad de la información?
	ID.RA.6	¿Cómo son las reacciones respecto a los riesgos que se podrían presentar?
	ID.SC.3	¿Cómo se emplea y que medidas ejerce la información en procesos involucrados?
Proteger	PR.AT.5	¿Cómo se divide los roles de seguridad física y cibernética? ¿Cuáles son sus responsabilidades?
	PR.DS.1	¿Cómo es la administración de los datos en reposo?
	PR.DS.2	¿Cómo es la administración de los datos en tránsito?
	PR.DS.5	¿Cómo se implementan las protecciones de filtraciones de datos?
	PR.IP.4	¿Cómo son las copias de seguridad de la información en la compañía?

	PR.IP.6	¿Cómo es la gestión de la eliminación los datos?
	PR.PT.1	¿Cómo son los registros de auditoría dentro de la compañía?
	PR.PT.2	¿Cómo protegen los medios de comunicación para la entrega de datos de seguridad de la información
	PR.PT.3	¿Cómo es la gestión del principio menor funcionalidad para la configuración de los sistemas?
	PR.PT.4	¿Cómo se encuentran las redes de comunicaciones y control de la compañía?
	PR.PT.5	¿En que influye la implementación de mecanismos que logran los requisitos de resiliencia?
Detectar	DE.AE.1	¿Cómo se establecen y gestiona los flujos de datos esperados de los usuarios y sistemas?
	DE.AE.3	¿Qué se realizan con los datos de los eventos?
	DE.CM.1	¿Cómo es el monitoreo de red para los posibles eventos de seguridad cibernética?
	DE.CM.2	¿Cómo es el monitoreo de físico para los posibles eventos de seguridad cibernética?
	DE.CM.3	¿Cómo es la actividad personal para detectar los posibles riesgos de seguridad cibernética?
	DE.CM.6	¿Cómo se realiza el monitoreo a la actividad de proveedores externos frente a posibles eventos de seguridad cibernética?
Responder	RS.AN.1	¿Cómo actúan con las notificaciones del sistema de detección?
	RS.AN.2	¿Cómo la compañía comprende el impacto de los incidentes?
	RS.AN.3	¿Cuál es la importancia de realizar análisis forenses?
	RS.AN.5	¿Cómo se establecen los procesos para analizar y responder vulnerabilidades de fuentes internas y externas?
	RS.MI.1	¿Cómo se contienen los incidentes de la seguridad de la información?
	RS.MI.2	¿Cómo se mitigan los incidentes de la seguridad de la información?
	RS.MI.3	¿Qué acciones realiza si se encuentran vulnerabilidades dentro de la seguridad de la información?
	RS.IM.1	¿Se realiza un proceso de lecciones aprendidas por los planes de respuesta?
Recuperar	RC.RP.1	¿Cómo son los pasos por seguir para la ejecución de un plan de recuperación?
	RC.IM.2	¿Cómo se efectúan las estrategias se recuperación?

A partir de los resultados obtenidos en la evaluación, nuestro sistema nos permite determinar el nivel de prioridad de manera precisa mediante una fórmula establecida: Prioridad = (Estado deseado - Estado obtenido) * Criticidad. Esta fórmula nos permite identificar los protocolos que requieren una atención prioritaria y aquellos que se encuentran en un estado estable. La prioridad asignada a cada evaluación de protocolos nos brinda un mejor entendimiento de nuestros reportes. La figura 2 representa el modelo que describe el funcionamiento de nuestro sistema y destaca los aspectos más importantes para la identificación de prioridades, así como los informes que proporcionan información sobre mejoras e indicadores claves relacionados con ellos.

Fig 2. Modelo de desarrollo del proyecto

4. *Módulos*
   a. *Módulo de evaluación:* Dentro del módulo de evaluación, se encuentra el sistema que detalla nuestro modelo de madurez y sus diferentes niveles representativos. Proporcionamos una breve descripción de nuestro proyecto y los pasos a seguir para llevar a cabo una evaluación precisa. Dentro de este módulo, se encuentra el formulario de evaluación que consta de 31 preguntas basadas en el marco de framework de NIST. Cada pregunta presenta 5 opciones de respuesta que representan casos frecuentes observados en el sector de las telecomunicaciones. Estas opciones de respuesta están asociadas a diferentes niveles de madurez dependiendo del contexto de los protocolos. Después de completar obligatoriamente las 31 preguntas en esta evaluación, todos los datos recopilados se dirigen a nuestro módulo de reportes. El módulo de evaluación adquiere una gran relevancia al permitirnos obtener información completa a través de la evaluación realizada por el usuario. Esto nos brinda una mayor conciencia sobre el estado de nuestros protocolos con relación a los casos observados durante la evaluación.

Fig 3. Módulo de evaluación de los protocolos de respuesta.

b. *Módulo de reportes:* En el módulo de reportes, es necesario que el usuario haya completado previamente su evaluación para obtener los resultados correspondientes. Este módulo está basado en una página web de identificación de usuario, donde cada usuario debe ingresar su contraseña, lo que nos permite visualizar únicamente las evaluaciones que ha realizado. Dentro de este sistema, se aplica una fórmula para determinar las prioridades de cada protocolo. Los resultados de esta fórmula se reflejan en dos informes presentados en la página. Uno de estos informes, en formato Excel, permite examinar en detalle los resultados, incluyendo los GAPS, las prioridades y una evaluación detallada basada en el marco de framework de NIST y nuestro modelo de madurez. El informe de Excel se genera automáticamente utilizando las funciones proporcionadas por la extensión EPPlus. Por otro lado, nuestros informes en formato PDF son documentos que proporcionan opciones de mejora para los protocolos que han sido calificados como de alta o media prioridad. Estas opciones de mejora son generadas por una inteligencia artificial de OpenIA, que hemos programado para que brinde un enfoque más adecuado a la seguridad de la información. De esta manera, las respuestas y sugerencias de mejora ofrecen un enfoque más efectivo para la mejora de los protocolos.

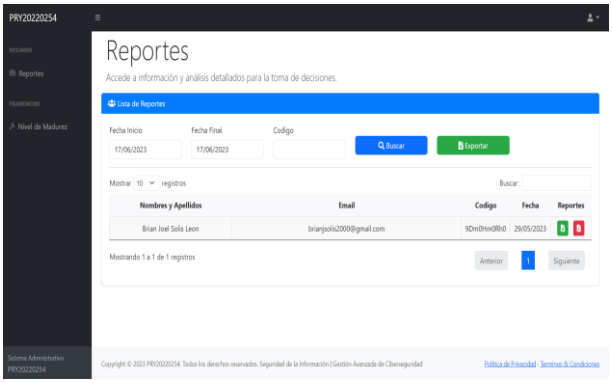

Fig 4. Módulo de reportes posterior a la evaluación de los protocolos de respuesta

IV. VALIDACIÓN Y RESULTADOS

A. Validación

Para respaldar la validación de nuestro proyecto, hemos solicitado la opinión de 4 expertos en el campo de seguridad de la información. Les hemos proporcionado una explicación exhaustiva sobre el funcionamiento de nuestro proyecto, mostrando los resultados obtenidos y las nuevas opciones de mejora que hemos desarrollado. Después de presentarles nuestro proyecto, procedimos a utilizar un formulario de evaluación. Esta evaluación se basa en la escala de Likert, que va del 1 al 5, donde 1 representa la calificación más baja y 5 la más alta. Los resultados de la evaluación están vinculados a 4 indicadores clave que hemos definido para la creación del formulario.

TABLE III.
Indicadores para validación de proyecto

Indicador	Descripción	Pregunta	Porcentaje
IND001	Satisfacción y usabilidad del modelo de madurez	1 y 3	30%
IND002	Evaluación de protocolos de respuesta	4	30%
IND003	Experiencia de usuario y diseño de software	8 y 9	15%
IND004	Usabilidad del proyecto en escenarios reales	10	25%

Para determinar el éxito de nuestro proyecto, se establece como criterio obtener un porcentaje de evaluación superior al 70% basado en las valoraciones de los resultados. Para calcular este porcentaje de evaluación, se promedian todas las calificaciones otorgadas por los expertos y se realiza una sumatoria, dividiéndola luego por el número total de evaluadores.

$$Prom_{IND001} = 30\% \times (Prom_{Ev.1}(P_1 + P_3) + Prom_{Ev.2}(P_1 + P_3) + Prom_{Ev.3}(P_1 + P_3) + Prom_{Ev.4}(P_1 + P_3)$$

$$Prom_{IND002} = 30\% \times (Prom_{Ev.1}(P_4) + Prom_{Ev.2}(P_4) + Prom_{Ev.3}(P_4) + Prom_{Ev.4}(P_4)$$

$$Prom_{IND003} = 30\% \times (Prom_{Ev.1}(P_8 + P_9) + Prom_{Ev.2}(P_8 + P_9) + Prom_{Ev.3}(P_8 + P_9) + Prom_{Ev.4}(P_8 + P_9)$$

$$Prom_{IND004} = 30\% \times (Prom_{Ev.1}(P_{10}) + Prom_{Ev.2}(P_{10}) + Prom_{Ev.3}(P_{10}) + Prom_{Ev.4}(P_{10})$$

$$\%Satisfacción = (\frac{Prom_{IND001} + Prom_{IND002} + Prom_{IND003} + Prom_{IND004}}{4})$$

Fig 5. Fórmulas para determinar el porcentaje de satisfacción del proyecto por parte de los expertos.

Al concluir la evaluación, hemos obtenido un nivel de satisfacción de 3.69 en la escala de Likert, y al aplicar los porcentajes de evaluación de nuestros indicadores, hemos alcanzado un nivel de satisfacción del 73.88%. Este resultado ha superado nuestras expectativas según la métrica establecida con los expertos. Dentro de las preguntas del formulario, se incluyeron preguntas que nos sirven para retroalimentar nuestro proyecto e identificar cuáles son las opciones de mejora que podemos presentar. Entre los comentarios que más han destacado fueron que no solo nos centremos en el marco de framework de NIST, sino que también consideremos otros framework como OWASP, entre otros.

B. Resultados

A continuación se presentarán los resultados de evaluación de un experto de seguridad de la información y una explicación de los resultados que se han obtenido. Primeramente, debe realizar la evaluación de los protocolos a través del módulo de evaluación. Finalizando la evaluación, tenemos como resultado los reportes que nos dan los siguientes datos.

TABLE IV.
Mapa de calor detallado de evaluación de un experto

Función/ Prioridad	Objetivo Alcanzado	Bajo	Medio	Alto	Crítico
Identificar	1	1	1	0	1
Proteger	0	6	4	0	1
Detectar	1	2	3	0	0
Responder	0	3	4	1	0
Recuperar	0	0	2	0	0

Según los resultados de la evaluación de nuestro usuario, se puede concluir que sus protocolos se sitúan en un nivel de riesgo medio a bajo en términos de posibles fugas de datos. Sin embargo, existen dos subcategorías de evaluación que se encuentran en un nivel crítico y uno en alto, y requieren una atención prioritaria para mitigar posibles riesgos. Mediante esta evaluación y análisis de datos, obtenemos una visión más clara de la situación de nuestra empresa y podemos identificar cómo corregir nuestros protocolos para alcanzar un nivel bajo o incluso eliminando cualquier riesgo de pérdida o filtración de información.

Dentro del informe en formato PDF, se proporciona un análisis detallado de las acciones que la empresa puede llevar a cabo para reducir el nivel de los protocolos identificados como de alta o crítica prioridad. Nuestra inteligencia artificial está capacitada para brindar información precisa y adaptada a las circunstancias específicas de la empresa.

En resumen, nuestro modelo de madurez ha demostrado ser efectivo, ya que ha permitido al experto identificar los protocolos que representan un mayor riesgo para la empresa. Esto nos proporciona la capacidad de prevenir posibles ataques de seguridad de la información y mitigar el riesgo de filtración de datos.

V. CONCLUSIONES

El proyecto tiene como objetivo desarrollar un modelo de madurez para evaluar los protocolos de respuesta utilizando el marco de framework de NIST a través de un sistema. La validación del proyecto ha sido realizada por 4 expertos en ciberseguridad, quienes han confirmado que el proyecto presenta una mejora del 73.88% en comparación con otros modelos preventivos existentes. Esta mejora se debe a que nuestro modelo de madurez se enfoca específicamente en el sector de las telecomunicaciones y los sistemas proporcionan un enfoque sólido en la evaluación y mejora de los protocolos de seguridad de los clientes. Esto refleja la creciente importancia de la seguridad de los datos en el entorno digital actual y ofrece un recurso valioso para las empresas que buscan mejorar sus prácticas en esta área.

El manejo de la evaluación de los protocolos a través de dos módulos ha brindado una gran contribución. El primer módulo se encarga de recopilar datos mediante evaluaciones de los protocolos de respuesta, mientras que el segundo realiza un análisis exhaustivo de estos datos para generar resultados claros y prácticos. Esta sinergia maximiza la utilidad de la información recopilada y ofrece a los clientes un servicio integral y seguro, desde la evaluación hasta la generación de informes.

Los informes generados son específicos para cada cliente, reflejando sus resultados individuales y brindando recomendaciones personalizadas. Este nivel de personalización aumenta el valor de los informes para los clientes, ya que pueden identificar directamente las áreas en las que necesitan mejorar y tomar acciones específicas en consecuencia.

REFERENCES

[1] Sogeti. (2020, noviembre 25). La importancia de la calidad de los datos en las empresas. Publicación de Blog. Recuperado de:

https://itblogsogeti.com/2020/11/25/la-importancia-de-la-calidad-de-los-datos-en-las-empresas/
[2] Willis Towers Watson. (s.f.). ¿Eres consciente de los problemas que puede generar un ingeniero social en tu empresa? . Publicación de blog. Recuperado de https://willistowerswatsonupdate.es/ciberseguridad/eres-consciente-de-los-problemas-que-puede-generar-un-ingeniero-social-en-tu-empresa/
[3] Corletti Estrada A. (2017, noviembre). “Ciberseguridad, estrategia informática”. Libro virtual gratuito de Learning Consulting. Recuperado de: pp. 95 – 113. ISBN 978-84-697-7205-8
[4] Oxman (2013, diciembre) Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming". Recuperado de: Revista de Derecho. Edición 41. ISSN 0718-6851
[5]Barriga Diaz R. (2016, diciembre) Factores que producen la fuga de información en las empresas del Ecuador. Articulo científico. Recuperado de: https://hdl.handle.net/20.500.12672/5377
[6] Veliz J. (2020, octubre 15) El peligro crece: Cada 18 segundos ocurre un ataque de ransomwares en Latinoamérica. RPP. Recuperado de: https://rpp.pe/tecnologia/mas-tecnologia/robo-de-datos-cada-18-segundos-ocurre-un-ataque-de-ransomware-en-latinoamerica-kaspersky-noticia-1298662?ref=rpp
[7] Seguridad de información (2015, septiembre 15) ¿Cómo evitar fallos tecnológicos con la norma ISO/IEC 27001:2013? Seguridad de información. Recuperado de: https://www.pmg-ssi.com/2015/09/fallos-tecnologicos-iso-iec-27001-2013/
[8] Alghamdi W. & Schukat M. (2021, abril 1) Precision time protocol attack strategies and their resistance to existing security extensions. Recuperado de: https://doi.org/10.1186/s42400-021-00080-y
[9] Osamah M.M. Al-Matar, Iman M.A. Helal, Sherif A. Mazen & Sherif Elhennawy B (2021, julio 2) Adopting security maturity model to the organizations’ capability model. Recuperado de: https://doi.org/10.1016/j.eij.2020.08.001
[10] Herrera I., García J., Ramos J., Molina S., De la Torre I. & Rodrigues J. (2022, julio 14) Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat. Recuperado de: https://doi.org/10.1007/s10586-022-03668-2
[11] Luo W. & Che Chen Y. (2022, enero 6) Constructing a teaching capability maturity model for content and language integrated learning teachers in Taiwan. Recuperado de: https://doi.org/10.1057/s41599-021-00928-1.
[12] Ravdeep K. ; Ramin K. & Adithya T. (2019, octubre 18) Cybersecurity for railways – A maturity model. Recuperado de: https://doi.org/10.1177/0954409719881849
[13] Revista Ciberseguridad para pequeños negocios (s.f) ¿Qué es y cómo funciona el marco de seguridad de NIST? Recuperado de: https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-NIST
[14] Pérez E., Pérez I., Rodríguez Y. (2014, marzo 26) Modelos de madurez y su idoneidad para aplicar en pequeñas y medianas empresas. Recuperado de: ISSN 1815-5936.