REVISTA PERSPECTIVAS

VOLUMEN 3, N° 2 / JULIO - DICIEMBRE 2021 e-ISSN: 2661-6688

Estudio preliminar sobre conocimiento de Ciberseguridad en usuarios de PYMEs: Caso de estudio en Riobamba

Preliminary study on Cybersecurity Knowledge in users of SMEs: A Case study in Riobamba City

Gino Paúl Maggi Murillo*, Omar S. Gómez†

*Pontificia Universidad Católica del Ecuador Sede Ambato, Ambato, Ecuador

†GrIISoft Research Group, Escuela Superior Politécnica de Chimborazo, Riobamba, Ecuador

Email: *gino.p.maggi.m@pucesa.edu.ec, †ogomez@espoch.edu.ec

Resumen— Los ataques cibernéticos no sólo se presentan en empresas grandes, hoy en día todo el mundo se encuentra expuesto a este tipo de amenazas, éstas tienen como fin el interrumpir con la confidencialidad de la información del usuario. Este trabajo tiene como objetivo realizar un estudio preliminar sobre el conocimiento de ciberseguridad en usuarios de PYMEs (pequeña y mediana empresa) tomando como caso de estudio la ciudad de Riobamba - Ecuador. Como método, se realizó una investigación descriptiva. La información fue recolectada de forma transversal y se aplicó como método de investigación una encuesta. De una población de 100 empresas, se seleccionaron 30 mediante un muestreo probabilístico aleatorio simple. A esta muestra se aplicó un instrumento con el fin de obtener así un estado actual del nivel de conocimiento de los usuarios finales de las PYMEs. Finalmente se presenta un modelo estadístico representativo de la población que aporte al estado del arte para futuras investigaciones. Como resultados se observa que el 70 %de los usuarios tienen un nivel medio en conocimiento sobre ciberseguridad, el 13.33 % tiene un nivel alto y el 16,67 % un nivel bajo. Los resultados sugieren que los usuarios de PYMEs requieren seguir actualizando sus conocimientos en temas de ciberseguridad ya sea a través de la realización de campañas de concientización o una serie de capacitaciones de conceptos y técnicas en seguridad de la información.

***Palabras Clave*— Ciberseguridad, Ciberataques, PYMEs, Ingeniería Social, Contraseñas Seguras, Software Malicioso, Suplantación de Identidad.**

Abstract— Cyber-attacks not only occur in large companies, today everyone is exposed to this type of concern, which is intended to interrupt the confidentiality of user information. This work aims to carry out a preliminary study on the knowledge of cybersecurity in users of SMEs (small and medium-sized companies), taking the city of Riobamba - Ecuador as a case study. As a method, we carry out a descriptive investigation. The information was collected cross-sectionally and a survey was applied as a research method. From a population of 100 companies, 30 were selected by simple random probability sampling. An instrument was applied to this sample in order to obtain a current status of the level of knowledge of the end users of SMEs. Finally, a representative statistical model of the population is presented that contributes to the state of the art for future research. As results, it was observed that 70% of users have a medium level of knowledge about cybersecurity, 13.33% have a high level and 16.67% a low level. The results suggest that SME users need to continue updating their knowledge on cybersecurity issues either through awareness campaigns or a series of training on information security concepts and techniques.

***Keywords*— Cybersecurity, Cyber-attacks, SMEs, Social Engineering, Passwords Security, Malware, Phishing.**

I. Introducción

En la actualidad la ciberseguridad juega un papel muy importante en las actividades cotidianas de las PYMEs. El salvaguardar los activos de información es primordial, y es por este motivo que se emplea software antimalware, sistemas informáticos de control de acceso e intrusiones y mecanismos de respaldo de datos. Sin embargo, estas herramientas no se enfocan en el usuario final.

El internet evoluciona constantemente como lo hacen los ciberdelincuentes y sus técnicas de ataque, como usuarios de esta tecnología se debe tener en cuenta los peligros de navegar en la red y compartir información. Los riesgos a los que se enfrenta una PYME no siempre son los mismos, considerando que usar un editor de texto tiene menos implicaciones de seguridad que un sistema informático financiero [1].

Los ciberataques pueden ser orientados a distintos objetivos como: la infraestructura de red, bases de datos, versiones obsoletas de sistemas operativos y especialmente los usuarios. Las PYMEs al tener una infraestructura tecnológica limitada no están exentas de sufrir ataques informáticos. Al contrario, el hecho de tener un bajo nivel de protección contra amenazas, las convierten en objetivos más frecuentes para los atacantes.

Otro factor clave en las PYMEs es el no contar con un departamento de Tecnología, y si lo tienen, el personal no se dedica específicamente a la seguridad de los activos de información. La mayoría de las PYMEs no saben que son vulnerables hasta el momento en el que sufren un ataque.

Fecha de Recepción: 31/may/2021 Fecha de Aceptación: 28/jun/2021 DOI: 10.47187/perspectivas.vol3iss2.pp45-53.2021

Estas limitantes de infraestructura y personal pueden ser difíciles de solventar por falta de recursos. Ante este aspecto se evalúa la alternativa de invertir en capacitación, bajo la promesa que el personal con el conocimiento adecuado hará mejor uso de las herramientas de ciberseguridad existentes y serán menos propensos a sufrir un ataque.

Con el fin de evaluar el nivel de conocimiento en ciberseguridad de los usuarios en las PYMEs de la ciudad de Riobamba, el presente trabajo realiza un estudio preliminar acerca de los conceptos básicos que debe poseer una per-sona para proteger su información en la red. Esto será de vital importancia para las PYMEs puesto que se identificarán aquellas falencias conceptuales que podrán ser incluidas en un programa de capacitación integral en ciberseguridad, así como servir de insumo para futuros trabajos.

El resto del documento se encuentra organizado como se describe. En la sección II se describen los conceptos y términos generales para poder tener una mejor comprensión sobre el tema a tratar en este estudio. En la sección III se presenta una serie de trabajos similares en los que se realizan estudios semejantes y también tienen como objetivo evaluar el conocimiento en ciberseguridad. En la sección IV se describe el panorama de la ciberseguridad en el Ecuador. En la sección V se expone la metodología usada en el estudio, mientras que en la sección VI se presentan los resultados obtenidos, y finalmente, en la sección VII la discusión y conclusiones pertinentes.

II. Generalidades sobre Ciberseguridad

Con el objetivo de clarificar la terminología utilizada y el entorno de referencia se definen conceptos como: Ciberespacio, Ciberseguridad, Hacker y Ciberataque. En el libro titulado Cyberpower and National Security [2], se define el ciberespacio como: *"Un dominio global dentro del entorno de la información cuyo carácter único y distintivo está enmarcado por el uso de los espectros electrónicos y electromagnéticos para crear, almacenar, modificar, intercambiar y explotar información vía redes interdependientes e interconectadas usando Tecnologías de la Información y la Comunicación."*. La Norma ISO/IEC 27032 [3] define la ciberseguridad como la *"preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio"*. Hay que aclarar que el término "hacker" tiene una definición muy lejana a la que periódicamente se asocia, no hace referencia a un pirata informático, más bien se refiere a una persona que frente a las nuevas tecnologías y códigos de información, actuará con una profunda actitud crítica y sentido de la ética [4].

Finalmente se detallan los principales ataques y su frecuencia de ejecución. Al hablar de ciberataques se debe tener en cuenta que existen varios tipos y cada uno tiene su propia definición, los siguientes términos definen un ciberataque [5]:

- **Cibercrimen:** incluye delitos como por ejemplo: el fraude, robo, chantaje, falsificación. Haciendo uso de ordenadores y redes como medios para su ejecución.
- **Ciberterrorismo:** Este término es definido por el FBI de la siguiente manera: "El ciberterrorismo es el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos." [5].
- **Ciberguerra o guerra informática:** en este tipo de ataques se utiliza como campo de batalla el ciberespacio y como armas la gran variedad de herramientas informáticas y comandos que permiten atacar al enemigo con el objetivo de inhabilitar o robar información representativa.

Existen diversas técnicas para llevar a cabo un ataque, pueden ser ejecutadas de forma individual o en grupo, entre las principales técnicas se exponen las siguientes [6][7]:

- **Virus informáticos:** Programas maliciosos que infectan a otros archivos ya sea en el mismo equipo o en equipos que se encuentran en la misma red, su objetivo modificar archivos de importancia para el usuario.
- **SPAM:** Envío de correos de forma masiva, desde un remitente no conocido y casi siempre con publicidad en su contenido.
- **Keyloggers:** Programa o dispositivo que puede ser instalado en cualquier equipo con el objetivo de capturar todo lo que digital el usuario.
- **Troyanos:** Virus que utilizan la técnica de engaño para así ocultarse y pretender ser un programa o archivo habitual. Su objetivo es crear una puerta trasera para obtener el ingreso al equipo.
- **Fuerza Bruta:** Este ataque tiene como objetivo obtener el acceso a cuentas personales o empresariales ya sea de algún sitio web, servidor, correo electrónico, entre otros. Utiliza diferentes combinaciones de datos almacenados en diccionarios creados exclusivamente para este tipo de ataques, realizando varias combinaciones y tratando de acceder mediante un formulario de credenciales hasta obtener el acceso.
- **DDOS:** Ataque de denegación de servicios, esta técnica se remonta a 1999, es uno de los más eficientes, difícil de detectar para los mecanismos de seguridad. El objetivo de este ataque es dejar inhabilitado o sin servicio un sitio para un cliente, mediante el envío de un alto flujo de tráfico.
- **Clickjacking:** Creación de sitios con apariencia engañosa que secuestra clics del usuario, es decir, que incita al usuario a dar clic en diferentes partes del sitio y así permitir la descarga e instalación de código malicioso para el Sistema Operativo.
- **Phishing:** Consiste en obtener información de la víctima de forma fraudulenta, mediante el envío de correos o mensajes que buscan persuadir al usuario para que acceda a sitios maliciosos o falsos e ingresen su información y así obtener accesos.

A. Ingeniería Social

Es un conjunto de técnicas psicológicas y habilidades sociales que posee un individuo que son aplicadas consciente y premeditadamente, con el objetivo de obtener información de un tercero. En este caso, se presta mayor atención a las técnicas usadas para obtener acceso a sistemas informáticos,

correos electrónicos y credenciales de cuentas bancarias. Los ingenieros sociales en la gran mayoría no llegan a manipular los equipos o aplicaciones web afectadas.

En cuanto a los tipos de persona vulnerables, todas coinciden en las mismas debilidades referentes al software o de su espacio físico de trabajo. Kevin Mitnick, una de las personas más famosas del mundo por ataques informáticos aplicando la Ingeniería Social dijo: *"usted puede tener la mejor tecnología, firewalls, sistemas de detección de ataques, dispositivos biométricos... Lo único que se necesita es una llamada a un empleado desprevenido para acceder al sistema sin más. Tienen todo en sus manos..."* [6].

En una organización que aparentemente tiene implementados los mejores métodos y técnicas de seguridad aún existe la opción de ser atacados por un medio el cual no se puede controlar completamente, el factor humano. Este factor es tan vulnerable deebido a que, a diferencia de los elementos tecnológicos, es el único que puede decidir romper las reglas y ser engañado por el atacante [8].

La Ingeniería Social o también llamada el "arte de engañar", puede ser aplicada por cualquiera, desde un vendedor que puede persuadir a sus clientes a comprar sus productos, hasta un creador de malware para convencer a los usuarios más ingenuos a entregar sus credenciales de acceso. Cuando se habla de seguridad de la información según "Cristian Borghello" [9], el "arte de engañar" es utilizado para dos fines:

1) *"El usuario es tentado a realizar una acción necesaria para vulnerar o dañar un sistema, esto ocurre cuando el usuario recibe un mensaje que lo lleva a abrir un archivo adjunto, abrir la página web recomendada o visualizar un supuesto video"*.
2) *"El usuario es llevado a confiar información necesaria para que el atacante realice una acción fraudulenta con los datos obtenidos. Este es el caso del Scam y el Phishing, en los que el usuario entrega información al delincuente creyendo que lo hace a una entidad de confianza o con un pretexto de que obtendrá algo a cambio, generalmente un gran premio"*.

En el artículo de Parada y Lady Johana [10], se menciona que la Ingeniería Social tiene 3 formas de actuar:

1) Es una técnica pasiva basada principalmente en la observación y el análisis de un perfil psicológico de la víctima.
2) Esta técnica no es de forma presencial si no que se vale de otros medios de comunicación con la víctima como: celular o correos electrónicos. Con el fin de obtener información que le sirva para ejecutar el ataque.
3) Finalmente esta técnica, es de forma presencial y prácticamente haciendo un seguimiento más de cerca a la víctima y buscando información por ejemplo en la basura o en lugares que vaya visitando.

La principal herramienta de protección ante la suplantación de identidad es la capacitación de los usuarios. Estos conocimientos les permitirán tomar precauciones e identificar posibles ataques. Es por esta razón que se anexa en el presente estudio a la Ingeniería Social como parte de la conceptualización de la seguridad de la información.

III. Trabajos Relacionados

Existen investigaciones relacionadas al tema de estudio, no obstante, poseen un enfoque hacia la protección de la infraestructura de red y uso de software antimalware. En el presente artículo se considera la capacitación del usuario como herramienta fundamental y principal estrategia de defensa contra ataques, cambiando así el enfoque tradicional de ciberseguridad basado en el cumplimiento de políticas y adquisición de equipos.

En el trabajo "Survey and Lessons Learned on Raising SME Awareness about Cybersecurity" de Christophe Ponsard [11] se propone una serie de técnicas y lineamientos aprendidos después de haber realizado una campaña de concienciación en ciberseguridad en las PYMEs en Bélgica. Se recalca que las PYMEs hoy en día son el objetivo de la gran mayoría de ataques cibernéticos. Un claro ejemplo de esto es en el Reino Unido donde se informó que más del 60% de las PYMEs sufrieron al menos un ataque cibernético en el año 2017 y el tipo de ataque utilizado en casi todos los casos fue el ransomware. También se menciona que si bien el uso de herramientas tecnológicas para evitar este tipo de ataques es primordial, lo es también el conocimiento que tienen los usuarios que manipulan los sistemas en una empresa. Además, el estudio da a conocer varios instrumentos de evaluación, los cuales serán considerados en el presente estudio.

En el artículo "Calculated risk? A cybersecurity evaluation tool for SMEs" [12] realizado en Estados Unidos, se detalla una herramienta de evaluación de la ciberseguridad para las PYMEs. Esta evaluación es dirigida a los líderes de departamento de TI de cada empresa y pretende evaluar su nivel de madurez en cuanto a la seguridad de la información, se menciona que la preparación para la ciberseguridad es clave para el sustento y la supervivencia en el entorno digital actual sin importar el tamaño de la empresa. Esta herramienta fue aplicada de forma online, y una vez que se aplicó a las diferentes PYMEs, se evaluaron cada una de las brechas, si un puntaje caía más de un punto por debajo del promedio, esta brecha es señalada como seria y se realizan las debidas recomendaciones.

Existen estudios en los que se intenta evaluar la situación actual del delito informático y la pérdida monetaria que dejan como consecuencia estos ataques. En la Tabla I se muestran varios ejemplos de encuestas que han sido realizadas por grandes organizaciones para tratar de evaluar la solidez de las políticas y medidas de seguridad de TI en las PYMEs [13]-[18].

IV. Panorama General de la Ciberseguridad en el Ecuador

En el Ecuador existen un gran número de ciberataques todos los días, según la Fiscalía General del Estado, las 3 provincias del Ecuador con el mayor porcentaje de incidencias en delitos informáticos son: Pichincha con el 47.38%, Guayas con el 27.57% y El Oro con el 5.24% [19], obteniendo un total de 53463 denuncias realizadas entre los años 2014 y 2020. De estos, los 3 ataques con mayor número de denuncias son los siguientes: suplantación de identidad con 24052 denuncias,

Tabla I
EJEMPLO DE ENCUESTAS - EVALUACIÓN DEL CONOCIMIENTO DE CIBERSEGURIDAD

Organización	Año	Descripción
2019 Cyber Safety Insights Report Global Results	2019	El costo monetario por ciberdelitos.
FBI and NW3C	2020	Pérdida monetaria y cantidad de víctimas a causa de los delitos cibernéticos
MARSH and MICROSOFT	2019	Fuga de información de la empresa a causa del uso de dispositivos personales en el trabajo.
US Secret Service and CERT USA	2018	Se concluye que la administración de seguridad y TI utiliza más tecnología para defenderse pero aún se queda atrás la capacitación en seguridad hacia los usuarios.
AusCERT - BDO	2018	Destaca los métodos de defensa y ataques cibernéticos que enfrentan las organizaciones de Australia.
Accenturesecurity . Ponemon Institute	2019	El hallazgo incluye la victimización de diferentes amenazas de delitos cibernéticos y sus enfoques para abordarlas.

Figura 1. Resumen Reporte de Ciberseguridad 2020.

falsificación y uso de documentos falsos con 17913 denuncias y apropiación fraudulenta por medios electrónicos con 8022 denuncias [20]. Ecuador ocupa el puesto 98 en el ranking global de ciberseguridad con un score de 0.367 y en el ranking regional ocupa el puesto 14. Ecuador aún no cuenta con una estrategia de seguridad cibernética, sin embargo, se han logrado mejoras significativas en cuanto a sus capacidades cibernéticas para enfrentar esas amenazas, siendo apoyado en gran parte por el establecimiento EcuCERT, equipo de respuesta ante incidentes cibernéticos del país [21].

En la Figura 1 se muestra un contraste entre el año 2016 y 2020 en cuanto a la Formación, Capacitación y Habilidades de Seguridad Cibernética, así también de la Cultura Cibernética y Sociedad.

Como consecuencia de los ataques que sufren los usuarios finales a más de pérdidas monetarias y de información dejan como secuela la desconfianza de los usuarios en la economía digital, las encuestas indican que menos del 50% aún confían en que la tecnología ayude a mejorar sus vidas, estos resultados indican la falta de confianza que tiene la gente cuando se habla de ciberseguridad [22].

V. METODOLOGÍA

La investigación realizada es de tipo descriptiva ya que lo que se busca en este artículo es descubrir el conocimiento en ciberseguridad que tienen los usuarios de las PYMEs, no es experimental por que no se establece o se construye ninguna situación de forma intencional. Los datos son recolectados de forma transversal ya que se recolectan en un solo punto. Como método de investigación se aplicó una encuesta para recopilar la información necesaria y poder identificar el grado de conocimiento en ciberseguridad que poseen los usuarios de las empresas encuestadas.

Para poder cumplir con el objetivo de la investigación se ha definido un esquema para la elaboración de un instrumento que permite evaluar lo requerido, como se puede ver en la Tabla II, en la cual se identifican el número de preguntas que permite la evaluación de cada indicador con respecto al instrumento que se encuentra descrito en el Anexo 1.

Se define como variable de estudio general el "Nivel de conocimiento sobre ciberseguridad en los usuarios finales de las PYMEs". La triada de la seguridad de la información [23] constituye el principio fundamental que un profesional de la ciberseguridad persigue para proteger los activos de información. Estos principios están conformados por la Confidencialidad, Integridad y Disponibilidad (CID). A estos conceptos se agregó la Ingeniería Social, ya que es el principal método no-técnico al que se enfrentan hoy en día las organizaciones [24], conformando así cuatro dimensiones, para las cuales se han considerado 12 indicadores y se han obtenido 23 preguntas.

Para realizar la evaluación se define como instrumento de medición una encuesta, en la cual se utiliza la escala de Likert para la evaluación de los diferentes ítems. Esta escala se utiliza para cuantificar el grado de aceptación de alguna variable con un mínimo negativo a un máximo positivo y también es ideal para medir reacciones, actitudes y comportamientos de una persona, en este respecto al conocimiento de ciberseguridad que tiene cada usuario [25]. El instrumento consta de dos apartados: Información general, para recabar datos del usuario, que consta de 7 ítems y el apartado de conocimiento en ciberseguridad que consta de 23 ítems, el mismo que se encuentra en el Anexo 1 del presente estudio.

Para la definición de las preguntas de este instrumento se tomaron como referencia encuestas de entidades internacionales tales como: el "Instituto Nacional de ciberseguridad de España" [26], la encuesta "Cyber Crime and Security Survey" publicada por el AusCERT y el BDO de Australia [17] con la temática en delitos informáticos, y también preguntas del estudio titulado "Survey and Lessons Learned on Raising SME Awareness about Cybersecurity" [11], el cual evidencia una clara sensibilización en las PYMEs para que puedan concientizar a sus usuarios sobre la ciberseguridad. Esta encuesta fue desarrollada en el estado de Michigan, con el apoyo de la administración de pequeñas empresas de EE.UU.

Este instrumento será aplicado a un grupo finito de usuarios, que laboren y cumplan el perfil de usuario al que se debe aplicar el instrumento. El usuario debe laborar constantemente en algún dispositivo que se encuentre conectado a internet, el resto de usuarios de la PYMEs quedan descartados. Como

Tabla II
OPERACIONALIZACIÓN DE LA VARIABLE GENERAL

Pregunta Científica	Variable	Dimensiones de la ciberse-guridad	Indicadores
¿Cómo evaluar el nivel de conocimiento de ciberseguridad que tienen los usuarios finales en las PYMEs en la ciudad de Riobamba?	Nivel de conocimiento sobre ciberseguridad en el usuario final	CONFIDENCIALIDAD	Accesos no autorizados (Preguntas: 8,9,10)
			Políticas de confidenciales y privacidad de datos personales (Preguntas: 11,12)
			Complejidad de Contraseñas (Preguntas: 13,14)
		INTEGRIDAD	Uso de software antimalware (Preguntas: 15,16)
			Riesgo de instalar programas de fuentes desconocidas (Preguntas: 17,18)
			Cifrado de archivos (Preguntas: 19,20,21)
		DISPONIBILIDAD	Servicios institucionales no disponibles (Preguntas: 22)
			Respaldo de la información (Preguntas: 23,24,25)
		INGENIERÍA SOCIAL	Validación correo electrónico legítimo (Preguntas: 26,27,28)
			Conocimiento de navegación segura (Preguntas: 29,30)

consecuencia de la adaptación realizada para obtener este instrumento, se asume que dichos cuestionarios ya han pasado por un proceso de validación, sin embargo, en este estudio se aplica la estrategia de validación de revisión por 2 expertos.

El método de muestreo que se utilizó es el Probabilístico Aleatorio Simple, el cual indica que todos los elementos de la población definida tienen la misma probabilidad de ser seleccionados [27]. Antes de aplicar el método de muestreo se identifica el número de empresas PYMEs que existen en la ciudad de Riobamba, las cuales representaran la población. Finalmente, mediante el método de muestreo se obtiene la cantidad de empresas a las que se aplicará el instrumento.

En el GAD Municipal de la ciudad de Riobamba no cuenta con un registro exacto en el cual se cataloguen las empresas como PYMEs, y tampoco en el catastro del SRI. Es por esto que para la definición de la cantidad de empresas a ser encuestadas se ha recabado información obtenida del Directorio de Empresas y Establecimientos (DIEE), el cual genera información estadística sobre la estructura empresarial ecuatoriana a partir de sus registros administrativos y proporciona información de empresas que durante el año fiscal registraron movimientos económicos de ventas, personal ocupado–afiliado, medido a través de plazas de empleo registrados en la seguridad social y/o realizaron una declaración al RISE, desde una perspectiva sectorial y territorial [28].

En la base de datos del DIEE se encuentra un listado de todas las empresas que existen en el Ecuador, catalogadas por Provincia, Cantón, Estrato de ventas, Estrato de plazas de trabajo, entre otros. Con base en este listado y apli-cando filtros en los siguientes campos: Provincia Chimborazo, Cantón Riobamba, empresas obligadas a llevar contabilidad, empresas que tengan un estrato de ventas desde $100.001 hasta $2'000.000 USD, empresas que no tengan una fecha de cese de actividades legales y que la plaza de empleo sea entre 10 y 99 personas. Una vez aplicados todos estos filtros los cuales permiten definir una PYME en el Ecuador según el estudio reportado en [29]. Mediante este proceso se han obtenido un total de 100 empresas PYMEs que existen en la ciudad de Riobamba.

Una vez determinado el tamaño de la población (N) se puede calcular la muestra de empresas a las que posteriormente se aplicará el instrumento, según la ecuación 1 [30]:

```
z<-1.282 #intervalo de confianza del 80% (Z-score)
sd<-0.5
e<-0.1 #margen de error del 10%
N<-100
((z^2*sd*(1-sd))/e^2) /
(1 + (( (z^2*sd*(1-sd)) /e^2)-1) / N)
```

Figura 2. Cálculo de la muestra en R Commander.

$$m = \frac{\frac{Z^2 * sd * (1-sd)}{e^2}}{1 + \frac{\frac{Z^2 * sd * (1-sd)}{e^2} - 1}{N}} \quad (1)$$

donde:

- m: Tamaño de la muestra.
- N: tamaño poblacional, en este caso 100.
- Z: es el nivel de confianza, se determina un 80
- sd: indica el grado de variación esperado en las respuestas, dado que el instrumento aún no se aplica es común definir un valor de 0.5 (50
- e: es el margen de error, es la aproximación del valor estimado de la muestra con respecto al valor 'real' de la población. En este caso se utilizó el 10% de margen de error.

Para aplicar la fórmula se empleó el software R Commander, el cual es un programa estadístico de código abierto impulsado por comandos basado en Lenguaje S [31]. En la Figura 2 se puede visualizar la fórmula codificada en el software. Una vez aplicada la fórmula se obtiene un total de 30 empresas como muestra. Considerando que la población era de 100 PYMEs, la muestra representa 30 casos a analizar, lo cual es el mínimo recomendado para no caer en la categoría de muestra pequeña [32].

VI. RESULTADOS

Se realizó un análisis descriptivo y una triangulación de los datos obtenidos, desde los resultados de cada una de las dimensiones hasta la obtención de los resultados del "Nivel de conocimiento en ciberseguridad". En la Tabla III se detalla la desviación estándar y la media de cada una de las dimensiones.

Una vez que se ha calculado la desviación estándar de cada dimensión se procede a establecer los puntos de corte de una

Tabla III
ESTADÍSTICA DESCRIPTIVA DE LAS DIMENSIONES

Dimensión	Mínimo	Máximo	Media	Desviación Estándar
Confidencialidad	16	31	22,17	3,788
Integridad	14	30	20,87	3,371
Disponibilidad	7	19	14,57	2,431
Ingeniería Social	7	22	15,47	3,748

Tabla IV
PUNTOS DE CORTE PARA SEGMENTAR LOS RESULTADOS

Dimensión	Punto de corte Izquierda	Punto de corte Derecha
Confidencialidad	18	26
Integridad	18	24
Disponibilidad	12	17
Ingeniería Social	12	19

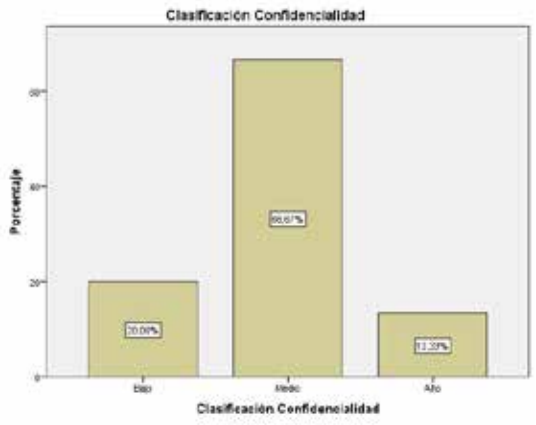

Figura 3. Resultados dimensión Confidencialidad.

distribución normal. Estos puntos se obtienen de sumar y restar el valor de la desviación estándar con respecto a la media como se muestra en la Tabla IV. Los valores que se encuentren dentro de los puntos de corte estarán en el nivel medio y los valores que se encuentren en los extremos serán considerados en el nivel bajo y alto, respectivamente.

Para verificar la consistencia interna del instrumento, se realizó un análisis del coeficiente "Alfa de Cronbach" usando el software SPSS. Como resultado se obtuvo un coeficiente de 0.802 con un numero de elementos igual a 23, lo que representa el 80.2% de fiabilidad del instrumento. Este coeficiente según George y Mallery [33] indica que el nivel de fiabilidad es BUENO.

Una vez obtenidos los puntos de corte, se calculan los porcentajes del nivel de conocimiento de cada una de las dimensiones.

Como se observa en la Figura 3, en la dimensión "Confidencialidad" se obtuvo que del total de usuarios encuestados, el 20% tiene un nivel de conocimiento bajo, el 66.67% tiene un nivel de conocimiento medio y el 13.13% tiene un nivel de conocimiento alto.

En la dimensión "Integridad" se obtuvo que el 20% tiene un nivel de conocimiento bajo, el 73.3% un nivel de conocimiento medio y el 6.7% un nivel de conocimiento alto, como se muestra en la Figura 4.

En la dimensión "Disponibilidad", como se muestra en

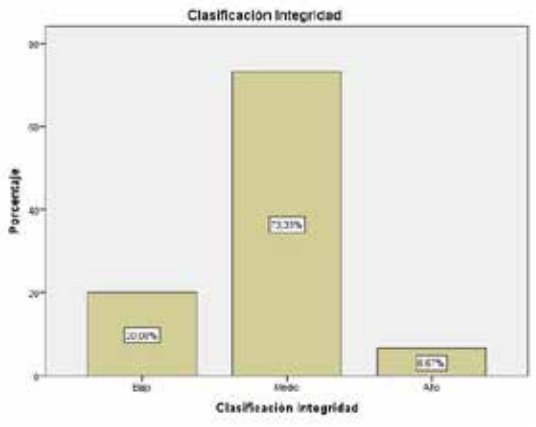

Figura 4. Resultados dimensión Integridad.

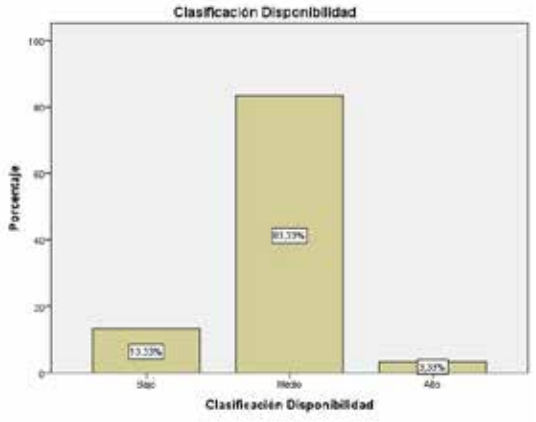

Figura 5. Resultados dimensión Disponibilidad.

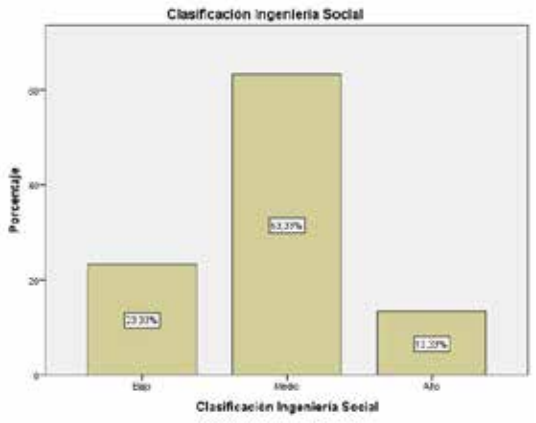

Figura 6. Resultados dimensión Ingeniería Social.

la Figura 5, se obtuvo que el 13.33% tiene un nivel de conocimiento bajo, el 83.33% tiene un nivel de conocimiento medio y el 3.33% tiene un nivel de conocimiento alto.

Finalmente, en la dimensión "Ingeniería Social", como se muestra en la Figura 6, se obtuvo que el 23.33% tiene un nivel de conocimiento bajo, el 63.33% un nivel de conocimiento medio y el 13.33% un nivel de conocimiento alto.

Una vez procesados los resultados por dimensión se aplicó

Tabla V
ESTADÍSTICA DESCRIPTIVA DE LA CIBERSEGURIDAD

Variable	Mínimo	Máximo	Media	Desviación Estándar
Ciberseguridad	16	31	22.17	3.788

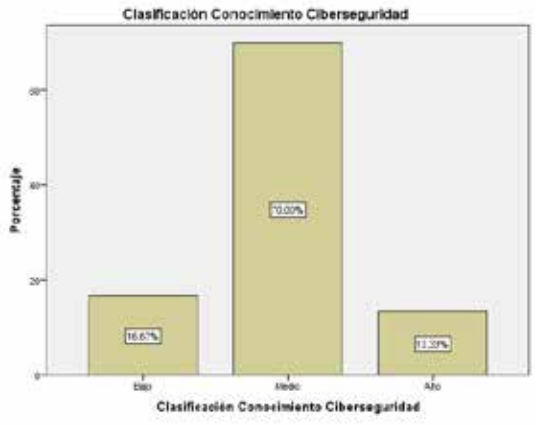

Figura 7. Resultados sobre conocimiento de Ciberseguridad.

estadística descriptiva, este análisis se puede apreciar en la Tabla V.

De estos datos, el de mayor relevancia es la desviación estándar, ya que nuevamente junto con el valor medio permite calcular los puntos de corte hacia la izquierda y la derecha de una distribución normal, los mismos que son 63 y 84, respectivamente.

Al final como se muestra en la Figura 7 el 70% de los usuarios tuvieron un nivel de conocimiento en ciberseguridad MEDIO, el 13.33% un nivel ALTO y el 16.67% un nivel BAJO, de un total de 30 personas encuestadas, correspondientes a una muestra de 30 PYMEs de la ciudad de Riobamba.

Los resultados obtenidos en este estudio, indican que la mayoría de los usuarios en las PYMEs de la ciudad de Riobamba, tienen un nivel de conocimiento en ciberseguridad Medio. Esta información será de gran utilidad para definir conceptos claves que podrían ser parte de las campañas de concientización, sobre métodos y técnicas que los usuarios deben apropiarse para prevenir ser víctimas de un ciberataque.

VII. DISCUSIÓN Y CONCLUSIONES

Debido a la situación actual a causa de la pandemia, la recolección de los datos se realizó de forma online, como consecuencia de esto las actividades de cada empresa se han visto interrumpidas causando una limitación importante durante la ejecución de la investigación. El hecho de informarles a los usuarios que la encuesta es online y que ingresen a un enlace para poder llenarla, ya generaba un poco de incertidumbre y desconfianza en ellos, ocasionando que los tiempos previstos en la recolección de los datos se extienda.

Para verificar la consistencia interna del instrumento y así obtener resultados confiables en el estudio, se calculó el Alfa de Cronbach, dio como resultado un coeficiente de 80.2% de confiabilidad, es decir que todos los ítems del instrumento se interrelacionan y permiten obtener un resultado cohesionado.

El instrumento por su construcción genérica puede ser aplicado en otras poblaciones puesto que no se basa en la cantidad de usuarios sino en el conocimiento que tienen estos usuarios, el nivel de conocimiento de ciberseguridad de una empresa es tan alto como lo es el nivel de conocimiento del usuario menos capacitado.

El instrumento que se utilizó en este estudio tiene un enfoque global sobre el conocimiento en ciberseguridad a diferencia del enfoque abordado en el trabajo [11], en el cual se perfila a los usuarios en 3 roles: Dueño de una cafetería, Administrador de redes y plomero. Se considera que la ciberdelincuencia no distingue roles ni estatus social, por lo que un conocimiento genérico de medidas de prevención es recomendable.

Un hecho rescatable y a ser considerado en futuros trabajos es que las empresas no denuncian haber sufrido un ciberataque por el miedo a ser manchada su reputación. En este aspecto sería recomendable incluir en el presente cuestionario preguntas, indicadores o una dimensión respecto al impacto en una organización y sus clientes como consecuencia de un ataque informático.

Según el reporte “2019 Cyber Safety Insights Report Global Results” [13] los incidentes más frecuentes se dan por infección de malware en los dispositivos. En el presente estudio se hace referencia a la dimensión integridad, en donde los usuarios tienen un conocimiento de nivel medio del 73,33%. Con respecto al uso de software antimalware antivirus e instalación de software de orígenes desconocidos, los usuarios están conscientes de estas vulnerabilidades y se protegen ante ellas, no obstante se recomendaría el uso de software legítimo como principal método de defensa, ya que los programas crackeados pueden incluir vulnerabilidades no detectables.

En vista de que este es un primer estudio en el que se realiza una evaluación del conocimiento en ciberseguridad en las PYMEs de la ciudad de Riobamba, es necesario replicarlo en otras provincias o ciudades para verificar si se pueden generalizar los resultados aquí expuestos.

En base a los resultados obtenidos en el estudio se concluye que los usuarios de las PYMEs en la ciudad de Riobamba tienen un nivel de conocimiento medio en ciberseguridad. Además, se sugiere que es necesario que las PYMEs en la ciudad de Riobamba realicen campañas de concientización sobre la protección ante ataques basados en Ingeniería Social y ransomware.

Finalmente, este estudio deja como resultado un instrumento de evaluación de conocimiento en ciberseguridad, que podría ser aplicado en varios perfiles de usuario dentro de una PYME, permitiendo así a las empresas realizar estudios internos y basados en los resultados tomar acciones de mejora e implementar campañas internas de concientización sobre ciberseguridad.

AGRADECIMIENTOS

Se agradece al Ing. Fausto Cevallos por su apoyo y guía para el desarrollo de este estudio.

REFERENCIAS

[1] S. M. Bellovin, «Cybersecurity for Small Businesses», p. 10.

[2] Franklin D., Kramer, Stuart H., y Larry K., Cyberpower and National Security, 1st ed. PotomacBooks, 2009.
[3] ISO / IEC 27032, «Information technology — Security techniques — Guidelines for cybersecurity». jul. 2012. [En línea]. Disponible en: https://www.iso.org/standard/44375.html
[4] I. Soria Guzman, Ética hacker,seguridad y vigilancia, 1.a ed. 2016. [En línea]. Disponible en: http://ru.iiec.unam.mx/3463/1/EticaHackerSeguridadVigilancia.pdf
[5] M. M. Pollitt, «Cyberterrorism — fact or fancy?», Computer Fraud & Security, vol. 1998, n.o 2, pp. 8-10, feb. 1998, doi: 10.1016/S1361-3723(00)87009-8.
[6] F. J. U. Centeno, «CIBERATAQUES, la mayor amenaza actual», n.o 09, p. 18.
[7] S. M. Toapanta Toapanta, H. A. Mera Caicedo, B. A. Naranjo Sanchez, y L. E. Mafla Gallegos, «Analysis of security mechanisms to mitigate hacker attacks to improve e-commerce management in Ecuador», 2020, pp. 242-250. doi: 10.1109/ICICT50521.2020.00044.
[8] J. Mieres, «Debilidades de seguridad comúnmente explotadas», p. 17.
[9] C. Borghello, «El arma infalible: la Ingeniería Social». abr. 13, 2019.
[10] C. Parada y Lady Johana, «Ataques informáticos, ethical hacking y conciencia de seguridad informática en niños», instname:Universidad Piloto de Colombia, jul. 2015, Accedido: dic. 08, 2020. [En línea]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/2870
[11] Christophe Ponsard, Jeremy Grandclaudon, y Sebastien Bal, «Survey and Lessons Learned on Raising SME Awareness about Cybersecurity», SCITEPRESS, vol. 1, pp. 558-563, 2019, doi: 10.5220/0007574305580563.
[12] M. Benz y D. Chatterjee, «Calculated risk? A cybersecurity evaluation tool for SMEs», Business Horizons, vol. 63, n.o 4, pp. 531-540, jul. 2020, doi: 10.1016/j.bushor.2020.03.010.
[13] The Harris Poll, «2019 CYBER SAFETY INSIGHTS REPORT GLOBAL RESULTS», 2019. [En línea]. Disponible en: https://now.symassets.com/content/dam/norton/campaign/NortonReport/2020/2019_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf
[14] FBI y NW3C, «Internet Crime Complaint Center», FBI AND NW3C, 2020. [En línea]. Disponible en: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
[15] MARSH y MICROSOFT, «2019 Global Cyber Risk Perception Survey», FBI AND NW3C, 2019. [En línea]. Disponible en: https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf
[16] CERT US State, «2018 U.S. State of Cybercrime», 2018. [En línea]. Disponible en: https://images.idgesg.net/assets/2018/11/201820us20state20of20cybercrime_sample20slides_gated20for20insider.pdf
[17] AusCERT y BDO, 2018/2019 Cyber Security Survey. 2019. [En línea]. Disponible en: https://www.bdo.com.au/getattachment/Microsites/Cyber-Security/2018-2019-Cyber-Security-Survey-Results/Download-Report/elements/Download-Report/1113_18_19-Cybersecurity-Report.pdf
[18] Ponemon Institute y AccentureSecurity, «THE COST OF CYBERCRIME», 2019. [En línea]. Disponible en: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf
[19] Fiscalía General del Estado, «Fiscalía General del Estado | Los delitos informáticos van desde el fraude hasta el espi-onaje». https://www.fiscalia.gob.ec/los-delitos-informaticos-van-desde-el-fraude-hasta-el-espionaje/ (accedido nov. 26, 2020).
[20] El Universo, «Los delitos informáticos crecen en Ecuador; cada clic en la web deja su rastro», El Universo, Ecuador, sep. 27, 2020. Accedido: nov. 26, 2020. [En línea]. Disponible en: https://www.eluniverso.com/noticias/2020/09/27/nota/7991905/delitos-informaticos-internet-casos-reales-redes-sociales-ecuador
[21] International Telecommunication Union, Global Cybersecurity Index, 2018.a ed. 2018. [En línea]. Disponible en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
[22] O. BID, «Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe | Publications», Banco Interamericano de Desarrollo y Organización de los Estados Americanos, 2, 2020. Accedido: nov. 26, 2020. [En línea]. Disponible en: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf
[23] Maraino Díaz Rodrigo, «La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad», 2020-11-03, p. 18p, nov. 03, 2020.
[24] J. Duran Pamplona, «Principales características, modos de perpetración y vulneración de la seguridad informática a través de la modalidad carding.», may 2020, Accedido: abr. 04, 2021. [En línea]. Disponible en: http://repository.unad.edu.co/handle/10596/34366
[25] Ankur Scale, Saket Kale, Satish Chandel, y D.K. Pal, «View of Likert Scale: Explored and Explained», 20-02-2015, pp. 396-403, 2015, doi: 10.9734/BJAST/2015/14975.
[26] INCIBE, «¿Cuánto sabes? | Oficina de Seguridad del Internauta», INCIBE. https://www.osi.es/es/cuanto-sabes (accedido dic. 13, 2020).
[27] A. Acharya, A. Prakash, P. Saxena, y A. Nigam, «Sampling: Why and How of it?», Indian Journal of Medical Specilaities, ene. 2013, doi: 10.7713/ijms.2013.0032.
[28] I. N. de E. y Censos, «Directorio de Empresas», Instituto Nacional de Estadística y Censos. https://www.ecuadorencifras.gob.ec/directoriodeempresas/dic. 05, 2020). (accedido
[29] D. Delgado y G. Chávez, «Las Pymes en el Ecuador», Observatorio de la Economía Latinoamericana, n.o abril, abr. 2018, Accedido: abr. 05, 2021. [En línea]. Disponible en: https://www.eumed.net/rev/oel/2018/04/pymes-ecuador-financiamiento.html
[30] Ronald E. Walpole y Raymond H. Myers, Probabilidad y Estadística para Ingeniería y ciencias, Novena. México: PEARSON EDUCACIÓN, 2012.
[31] John Fox, «Getting Started With the R Commander: A BasicStatistics Graphical User Interface to R», Journal of Statistical Software, pp. 1-42.
[32] Elia Beatriz Pineda, Eva Luz de Alvarado, y Francisca H. de Canales, Manual para el desarrollo de personal de salud, Segunda. Washington D.C., 1994. [En línea]. Disponible en: https://n9.cl/f1x1t
[33] Darren George y Paul Mallery, IBM SPSS Statistics 26 Step by Step A simple Guide and Reference, 16.a ed. New York: Routledge.
[34] N. Amrin, «The Impact of Cyber Security on SMEs», ago. 14, 2014. https://essay.utwente.nl/65851/ (accedido abr. 09, 2021).

Anexos

Anexo 1. Instrumento

El instrumento se encuentra dividido en 5 segmentos: Información General, donde se recaban datos que el investigador creía podrían ser útiles para el estudio y como se muestra en la Tabla VI tiene 7 ítems. La "Confidencialidad" que contiene 7 ítems con 3 indicadores, como se muestra en la Tabla VII. La "Integridad" que contiene 7 ítems con 3 indicadores, como se muestra en la Tabla VIII. La "Disponibilidad" que contiene 4 ítems con 2 indicadores, como se muestra en la Tabla IX. Y finalmente, la "Ingeniería Social" que está compuesta por 5 ítems y 2 indicadores como se muestra en la Tabla X.

Tabla VI
Preguntas relacionadas a Información General

N°	Pregunta
1	Edad
2	Sexo
3	Área laboral en la que se desempeña
4	Empresa donde labora
5	Cargo que desempeña en la empresa
6	¿Cuánto conoce usted sobre ciberseguridad?
7	¿Con qué frecuencia ha escuchado en su área laboral que otra persona ha sufrido un ataque informático?

Tabla VII
PREGUNTAS RELACIONADAS A DIMENSIÓN DE CONFIDENCIALIDAD

N°	Indicador	Pregunta	Escala de evaluación Likert
8	Accesos no autorizados	¿Con qué frecuencia recibe notificaciones de acceso no autorizado a su correo electrónico?	Muy frecuentemente (1) Frecuentemente (2) Ocasionalmente (3) Raramente (4) Nunca (5)
9		¿Con qué frecuencia revisa los intentos de inicio de sesión, en su cuenta de correo electrónico?	Muy frecuentemente (5) Frecuentemente (4) Ocasionalmente (3) Raramente (2) Nunca (1)
10		¿Con qué frecuencia cambia las credenciales de acceso a sus cuentas?	Muy frecuentemente (5) Frecuentemente (4) Ocasionalmente (3) Raramente (2) Nunca (1)
11	Políticas de confidencialidad y privacidad de datos personales	¿Con qué frecuencia lee las políticas de confidencialidad y privacidad de datos personales, cuando se registra en una aplicación empresarial, web o móvil?	Muy frecuentemente (5) Frecuentemente (4) Ocasionalmente (3) Raramente (2) Nunca (1)
12		¿Ha encontrado algún sitio web en el que no se le presente una política de privacidad de datos al momento de registrarse?	Siempre (5) Casi Siempre (4) A veces (3) Casi nunca (2) Nunca (1)
13	Complejidad de Contraseñas	¿Cuán importante es para usted tener una contraseña segura en sus aplicaciones?	Muy importante (5) Importante (4) Neutral (3) Poco Importante (2) No es importante (1)
14		Las contraseñas que usted utilizada contienen las siguientes características: longitud mayor de 10 caracteres, palabras no comunes o secuencias, tipo de caracteres variados (*,$,@,&, entre otros), letras mayúsculas.	Siempre (5) Casi Siempre (4) A veces (3) Casi nunca (2) Nunca (1)

Tabla VIII
PREGUNTAS RELACIONADAS A DIMENSIÓN DE INTEGRIDAD

N°	Indicador	Pregunta	Escala de evaluación Likert
15	Uso de software antimalware	¿Con qué frecuencia realiza un escaneo de virus en sus dispositivos?	Muy frecuentemente (5) Frecuentemente (4) Ocasionalmente (3) Raramente (2) Nunca (1)
16		¿Con qué frecuencia recibe notificaciones de su antivirus de páginas o archivos potencialmente peligrosos para sus dispositivos?	Muy frecuentemente (1) Frecuentemente (2) Ocasionalmente (3) Raramente (4) Nunca (5)
17	Riesgo de instalar programas de fuentes desconocidas	¿Está consciente del riesgo que implica instalar programas/aplicaciones crackeadas o de fuentes desconocidas?	Siempre (5) Casi Siempre (4) A veces (3) Casi nunca (2) Nunca (1)
18		¿Cuán importante considera usted que es tener instalado un antivirus con licencia, actualizaciones automáticas y escaneos de malware programados en sus dispositivos?	Muy importante (5) Importante (4) Neutral (3) Poco Importante (2) No es importante (1)
19	Cifrado de archivos	¿Con qué frecuencia ha notado archivos en su equipo con una extensión extraña o que no ha logrado identificar?	Muy frecuentemente (5) Frecuentemente (4) Ocasionalmente (3) Raramente (2) Nunca (1)
20		¿Ha sufrido alguna vez pérdida de información a causa de algún virus informático?	Siempre (5) Casi Siempre (4) A veces (3) Casi nunca (2) Nunca (1)
21		¿Ha sido víctima de un ataque informático en el cual le han pedido dinero para recuperar su información?	Siempre (5) Casi Siempre (4) A veces (3) Casi nunca (2) Nunca (1)

Tabla IX
PREGUNTAS RELACIONADAS A DIMENSIÓN DE DISPONIBILIDAD

N°	Indicador	Pregunta	Escala de evaluación Likert
22	Servicios institucionales no disponibles	¿Con qué frecuencia las diferentes aplicaciones de su empresa han fallado o no se han encontrado disponibles?	Muy frecuentemente (5) Frecuentemente (4) Ocasionalmente (3) Raramente (2) Nunca (1)
23	Respaldo de la información	¿Con qué frecuencia usted genera un respaldo de la información importante que contienen sus dispositivos?	Muy frecuentemente (5) Frecuentemente (4) Ocasionalmente (3) Raramente (2) Nunca (1)
24		¿Cuán importante considera usted que es almacenar los respaldos de su información en un lugar seguro?	Muy importante (5) Importante (4) Neutral (3) Poco Importante (2) No es importante (1)
25		¿Está usted de acuerdo en que los respaldos de la información se los debe almacenar en la nube o en algún lugar diferente de su propio equipo?	Muy de acuerdo (5) De acuerdo (4) Indiferente (3) En desacuerdo (2) Muy en desacuerdo (1)

Tabla X
PREGUNTAS RELACIONADAS A DIMENSIÓN "INGENIERÍA SOCIAL"

N°	Indicador	Pregunta	Escala de Likert
26	Validación correo electrónico legítimo	¿Con qué frecuencia usted verifica la dirección del remitente de un correo electrónico?	Muy frecuentemente (5) Frecuentemente (4) Ocasionalmente (3) Raramente (2) Nunca (1)
27		¿Con qué frecuencia revisa la veracidad de los enlaces en botones de correos electrónicos bancarios?	Muy frecuentemente (5) Frecuentemente (4) Ocasionalmente (3) Raramente (2) Nunca (1)
28		¿Ha recibido alguna vez un correo electrónico de su banco, solicitando datos personales y acceder a un link para confirmar los mismos?	Muy frecuentemente (5) Frecuentemente (4) Ocasionalmente (3) Raramente (2) Nunca (1)
29	Conocimiento de navegación segura	Cuando navega en internet, ¿Revisa usted que las páginas a las que accede sean seguras, es decir; que contengan https en su dirección url?	Siempre (5) Casi Siempre (4) A veces (3) Casi nunca (2) Nunca (1)
30		Cuando le envían un link para descargar un documento, ¿Verifica usted que el link sea confiable?	Siempre (5) Casi Siempre (4) A veces (3) Casi nunca (2) Nunca (1)