Recibido: 9 de septiembre del 2022 / Aceptado: 2 de noviembre del 2022
doi: https://doi.org/10.26439/interfases2022.n016.6021

# PROTOCOLO BÁSICO DE CIBERSEGURIDAD PARA PYMES

Olda Bustillos Ortega
obustillos@uia.ac.cr
https://orcid.org/0000-0003-2822-3428
Universidad Internacional de las Américas,
Escuela de Ingeniería, Costa Rica

Javier Rojas Segura
jrojass@uia.ac.cr
https://orcid.org/0000-0002-0488-4056
Universidad Internacional de las Américas,
Escuela de Ingeniería, Costa RIca

RESUMEN. Las restricciones de circulación impuestas por los gobiernos durante la pandemia del COVID-19 modificaron los patrones de consumo y la forma de hacer negocios, obligando a las pequeñas y medianas empresas a migrar a medios electrónicos para no perecer. Del mismo modo, la delincuencia incrementó su participación en el ciberespacio, explotando la vulnerabilidad de estas empresas por su dependencia de las tecnologías digitales y la falta de recursos para un manejo efectivo de la integridad, confidencialidad y disponibilidad de los datos. Por tanto, es necesario sensibilizar a las pequeñas y medianas empresas sobre la importancia de la ciberseguridad y prepararlas no solo para defenderse contra un ciberataque, sino también para una rápida y oportuna recuperación ante un posible incidente. El objetivo de esta investigación es proponer un protocolo básico de ciberseguridad, como principal estrategia de defensa contra ciberataques, que permita la continuidad del negocio en caso de un ataque cibernético. El protocolo se construye a partir de publicaciones académicas, tesis, normas técnicas y guías prácticas, examinadas en el contexto actual de las amenazas globales. La ciberseguridad es percibida por las pequeñas y medianas empresas como demasiado compleja y onerosa, por lo que se requieren soluciones económicas, efectivas y accesibles.

PALABRAS CLAVE: ciberseguridad, pymes, TIC, protocolo

## BASIC CYBERSECURITY PROTOCOL FOR SMES

ABSTRACT. Movement restrictions imposed by governments during the COVID-19 pandemic have changed consumption patterns and the way of doing business, forcing small and medium-sized companies to migrate their businesses to electronic media. Similarly, crime increased its participation in cyberspace, exploiting the vulnerability of these companies due to their dependence on digital technologies and the lack of resources for effective management of data integrity, confidentiality, and availability. Therefore, it is necessary to sensitize small and medium-sized companies about the importance of cybersecurity and prepare them not only to defend themselves against cyberattacks but also for a quick and timely recovery from possible incidents. The objective of this study is to propose a basic cybersecurity protocol as the primary defense strategy against cyberattacks, which allows business continuity in the event of a cyberattack. Academic publications, theses, technical standards, and practical guides examined in the current global threats context were the protocol's basis. Small and medium-sized companies perceive cybersecurity as too complex and onerous; thus, they require economical, effective, and accessible solutions.

KEYWORDS: cybersecurity, SME, ICT, protocol

## 1. INTRODUCCIÓN

En un ambiente empresarial globalizado y competitivo, como el que existe en la actualidad, las pequeñas y medianas empresas (pymes), la sociedad y las compañías, en general, dependen cada vez más de la tecnología, específicamente de sistemas de información, por lo que deben crear políticas de seguridad como un medio de protección, pues se ha demostrado que tienen una enorme influencia para aumentar los niveles de competitividad (Zuña Macancela et al., 2019). La preparación para la seguridad cibernética es clave para el sustento y la supervivencia en el entorno digital actual (Benz & Chatterjee, 2020), por lo que en el mundo muchas empresas aumentan sus presupuestos en ciberseguridad para prevenir los ciberataques (Zuña Macancela et al., 2019). Sobre este tema, el Gobierno de Japón (2021) reconoce que para las pymes es difícil destinar un presupuesto importante a la seguridad tecnológica, por lo que es necesario impulsar medidas de esta naturaleza dirigidas a este sector que sean económicas, efectivas y accesibles.

Las pymes presentan datos alarmantes con respecto a ciberseguridad (Peralta Zuñiga & Aguilar Valarezo, 2021), dado que la gran mayoría de los ataques se dirigen a ellas (Ponsard et al., 2019). Más aún, muchas de estas empresas no denuncian haber sufrido un ciberataque por miedo a afectar su reputación (Maggi Murillo & Gómez Gómez, 2021). Por eso, es importante no solo defenderse contra los ataques cibernéticos, sino también prepararse para una respuesta y recuperación rápida y oportuna ante estos incidentes (World Economic Forum [WEF], 2022).

El 57 % de las pymes indica que, ante un ciberataque, lo más probable es que quiebre o deje de funcionar (ENISA, 2021). A pesar de esto, las pymes no parecen darse cuenta de que la ciberseguridad no es algo que afecte solo a las organizaciones más grandes. De acuerdo con Ponsard et al. (2019), la explicación es que las medidas de seguridad se perciben como demasiado complejas, lentas y que requieren un alto nivel de conocimientos técnicos, así como elevados recursos. Tal como recomienda Ramírez Montealegre (2016), es necesario crear un protocolo orientado a las pymes que sea de fácil aplicación, de bajo costo y altamente efectivo.

El objetivo de esta investigación es proponer un protocolo básico de ciberseguridad para pymes, como herramienta fundamental y principal estrategia de defensa contra ciberataques, que permita asegurar la continuidad del negocio en caso de una contingencia. Lo anterior nos lleva a preguntarnos: ¿cómo pueden prevenir las pymes un incidente de seguridad cibernética?

La metodología utilizada abarca las etapas de investigación, adaptación de la información recopilada, revisión por expertos y, finalmente, la propuesta de un protocolo básico de ciberseguridad.

Como resultado de esta investigación se presenta un protocolo de ciberseguridad con el cual los usuarios y gerentes de las pymes pueden alcanzar una base para proteger sus datos, obteniendo una primera contextualización que les permita reconocer los conceptos de ciberseguridad más relevantes para la comprensión de un primer nivel. Este conocimiento irá madurando con el tiempo (Martínez & Blanco, 2020) hasta crear una cultura de ciberseguridad.

## 2. REVISIÓN DE LITERATURA

Las pequeñas y medianas empresas (pymes) tienen un papel destacado en el desarrollo económico de los países (Semrau et al., 2016), por lo que son consideradas la columna vertebral de las economías en el mundo (Eggers, 2020). En América Latina conforman el 99 % del parque empresarial y generan cerca de dos tercios del empleo de la región (Fernández & Puig, 2022). En Costa Rica las pymes representan el 97,5 % del parque empresarial, aportan el 35,7 % del PIB y contribuyen con el 33,0 % del empleo formal (Faith et al., 2022). A pesar de ello, estas organizaciones empresariales en Latinoamérica no están exentas de limitaciones y, por ende, de enfrentar diversos desafíos (Bartesaghi & Weck, 2022). La dependencia de las pymes de la tecnología e internet abre la puerta a vulnerabilidades frente al cibercrimen, las cuales ocasionan que la seguridad de la información sea un aspecto crítico para todas las pymes (Bruycker & Darville, 2017).

### 2.1 Situación actual de las pymes

Existe un reconocimiento generalizado entre los líderes de la mayoría de las industrias de que el papel de la tecnología digital está cambiando rápidamente: de ser un impulsor de la eficiencia marginal a ser un fundamental facilitador de la innovación y de la disrupción (Weinelt, 2016). La necesidad de competitividad e innovación de las pymes las convierte en grandes adoptadores de tecnologías digitales, lo que aumenta su exposición a los ciberataques (Ponsard et al., 2019). Estas empresas se encuentran entre las menos maduras y vulnerables en términos de riesgo de ciberseguridad y resiliencia (Benz & Chatterjee, 2020). Enfrentan muchos de los problemas de ciberseguridad que también tienen las grandes empresas, pero no cuentan con los recursos para abordar los riesgos de manera efectiva (Horn, 2017). No obstante, con la ciberpandemia cobrando impulso, no hay industria u organización que esté a salvo (Benz & Chatterjee, 2020).

Las pymes no pueden permitirse el lujo de retrasar su inversión en ciberseguridad (Benz & Chatterjee, 2020), ya que en la actualidad son el objetivo de la gran mayoría de ataques cibernéticos (Ponsard et al., 2019). Deben hacer un plan de contingencia, invertir en herramientas informáticas, capacitar al personal en ciberseguridad para

que todos hablen y manejen el mismo lenguaje (Zuña Macancela et al., 2019), y tomar conciencia de la importancia de implementar métodos más rígidos de seguridad informática, no únicamente para contrarrestar los perjuicios que puede generar un fraude informático, sino también para prevenirlos (Peralta Zuñiga & Aguilar Valarezo, 2021).

### 2.2 Seguridad cibernética

La seguridad de la información se ha convertido en una tendencia a nivel mundial, debido al lugar significativo y relevante que ocupa la información para toda compañía y al creciente aumento de amenazas en los últimos años. Actualmente, la seguridad no solo se refiere a la protección de los equipos con antivirus; con el paso del tiempo y el avance de la tecnología, han surgido nuevas técnicas de ataques para vulnerar sistemas informáticos (Morales et al., 2020).

La preparación para la seguridad cibernética está emergiendo como una competencia crítica para la supervivencia y el crecimiento de las organizaciones (Benz & Chatterjee, 2020), especialmente de las pymes. Ponsard et al. (2019) indican que, según la Alianza Nacional de Seguridad Cibernética (NCSA, por sus siglas en inglés), más de la mitad de las pymes hackeadas no pueden recuperarse y van a la quiebra dentro de los seis meses posteriores al ataque.

Los incidentes más frecuentes ocurren por infección de *malware* en los dispositivos (Maggi Murillo & Gómez Gómez, 2021). El término *malware*, acuñado por Yisrael Radai en 1990, se utiliza para describir la amplia gama de códigos maliciosos (Messmer, 2008). Existen diversas variantes de *malware*, por ejemplo, los virus, las bombas lógicas, los troyanos y los *worms* o gusanos. La diferencia entre ellas consiste en la forma como actúan (Gutiérrez-Cárdenas & Orihuela, 2016).

### 2.3 Amenazas

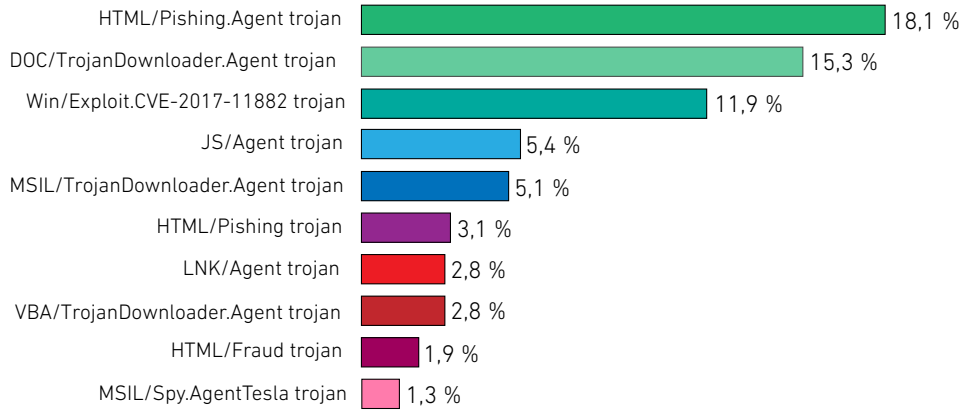
La amenaza de los ciberataques es global. Actualmente, existe *malware* capaz de causar un daño significativo a la infraestructura crítica de un país (Cherepanov & Lipovsky, 2017); por ejemplo, en el 2016, Ucrania sufrió el primer ataque de *malware* diseñado específicamente para atacar las redes eléctricas (Kovac, 2022). Los ataques cibernéticos no solo se dirigen a empresas grandes; hoy en día, la mayoría de las organizaciones se encuentran expuestas a este tipo de amenazas (Maggi Murillo & Gómez Gómez, 2021). Incluso el ciberespacio refleja tensiones geopolíticas, competencias entre los Estados y cuestiones de seguridad nacional (Gobierno de Japón, 2021); ejemplo de ello es que casi el 60 % de los ataques de RDP (*remote desktop protocol*) vistos durante el primer trimestre del 2022 provinieron de Rusia (Kovac, 2022). En Costa Rica, en la primera mitad del 2022, sistemas informáticos

públicos y privados fueron blanco de más de 513 millones de intentos de ciberataques, lo que constituye un repunte de 104 % en comparación con el mismo periodo del 2021 (Lara, 2022). Por otro lado, se encuentra la visión del individuo sobre las redes sociales, que son el medio de entretenimiento y comunicación de las personas. El usuario promedio tiene poco o nulo conocimiento sobre ciberamenazas, por lo que es víctima fácil de las páginas maliciosas que aparentan ser páginas regulares (Moncada Vargas, 2020).

El reporte global de amenazas de ESET (2022) indica que, después de permanecer estable durante algún tiempo, la cantidad de detecciones de amenazas aumentó un 20,1 % en el primer trimestre del 2022. La Figura 1 muestra los diez *malware* más detectados en este periodo.

**Figura 1**

*Los diez malware más detectados en el primer trimestre del 2022*




*Nota.* Reproducido de *Threat Report T1 2022*, por ESET, 2022 (https://www.welivesecurity.com/wp-content/uploads/2022/06/eset_threat_report_t12022.pdf).

Los primeros cuatro *malware* representan el 50,7 % de las amenazas detectadas por ESET (2022), tal como se observa en la Figura 1. El primero se suele usar en un archivo adjunto de correo electrónico de *phishing*. Los atacantes tienden a enviarlo en lugar de otros tipos de archivos, ya que los archivos adjuntos ejecutables generalmente se bloquean automáticamente o es más probable que levanten sospechas. Cuando se abre un archivo adjunto de este tipo, se abre un sitio de *phishing* en el navegador web, que se hace pasar, por ejemplo, por un banco, un servicio de pago o un sitio web de redes sociales. El sitio web solicita credenciales u otra información confidencial, que luego se envía al atacante.

El segundo *malware* es un documento malicioso de Microsoft Word, disfrazado de factura, formulario, documento legal u otra información aparentemente importante que descarga más *malware* de internet.

El tercero en importancia es un documento especialmente diseñado que explota la vulnerabilidad de Microsoft Equation Editor, un componente de Microsoft Office. Cuando el usuario abre el documento malicioso, se activa descargando *malware* adicional en la computadora.

El cuarto es un archivo JavaScript malicioso que se coloca en sitios web comprometidos pero legítimos, con el objetivo de lograr un compromiso de los visitantes.

Debido al alto número de ataques reportados en Latinoamérica en los últimos años y la cantidad creciente de robos y estafas realizadas como consecuencia de estos ataques cada año, el *phishing* es la ciberamenaza más grande en la actualidad (Moncada Vargas, 2020), y 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 ingrese su información y así obtener acceso (Maggi Murillo & Gómez Gómez, 2021). Existen otros métodos como, por ejemplo, el *pharming*, que es el redireccionamiento de un usuario que se encuentra en una página legítima a una página *phishing* a través de enlaces directos implantados en la página legítima (Abu-Nimeh et al., 2007). Las métricas más importantes para detectar páginas *phishing* derivan de experiencias humanas (Mao et al., 2018); sin embargo, como señala Moncada Vargas (2020), para identificar estas páginas maliciosas de manera dinámica y automática, se utiliza la inteligencia artificial y el *machine learning*.

### 2.4 Soluciones

Actualmente, se vive la era de la transformación digital, donde los negocios y sobre todo la información han migrado a medios digitales, lo cual implica un mayor reto para las organizaciones en la protección de sus datos (Morales et al., 2020). Las pymes y la sociedad en general empiezan a tomar conciencia de la enorme importancia de poseer adecuados sistemas de seguridad de la información, así como de la correcta gestión de datos (Zuña Macancela et al., 2019). El salvaguardar la información es primordial; por ese motivo, se emplea *software anti-malware*, sistemas informáticos de control de acceso e instrucciones y mecanismos de respaldo de datos (Maggi Murillo & Gómez Gómez, 2021). Al proteger estos activos, se asegura su confidencialidad, integridad y disponibilidad (Marchand-Niño & Ventocilla, 2020).

Las organizaciones mantienen un flujo constante de información con su entorno y a través de él puede entrar en riesgo el propio negocio por diversas amenazas,

tanto internas (fuga de información) como externas (suplantación, estafas, *malware*). Estas amenazas siempre están evolucionando, por lo que el *firewall* es el principal mecanismo de defensa y protección en el flujo de la información (Cortés Aldana, 2016). La estrategia de cuidar los datos mediante el uso de un *firewall* perimetral asegura la integridad, confidencialidad y disponibilidad, que son los tres pilares de la seguridad de la información (Morales et al., 2020). Los *firewalls* son dispositivos que buscan proteger la información, por lo que son una de las herramientas principales de seguridad informática (Cortés Aldana, 2016).

Sumado a esto, la ingeniería social continúa siendo el método de propagación de ataques informáticos más utilizado por los creadores de *malware*, quienes aprovechan las ventajas de cualquier medio de comunicación para engañar a los usuarios y lograr que estos terminen cayendo en una trampa que suele apuntar a un fin económico (Borghello, 2009). En estas circunstancias, es necesario un respaldo mantenido en un servidor independiente (Iao, 2021). La recuperación de la información obliga a buscar prácticas como los respaldos de los datos.

Es bien sabido que las herramientas tecnológicas no pueden garantizar por sí solas la seguridad de los sistemas; por el contrario, se requiere apoyo de los colaboradores dentro de la organización (Ponsard et al., 2019). Los usuarios de las pymes deben seguir actualizando sus conocimientos en temas de ciberseguridad a través de capacitaciones en temáticas relacionadas con seguridad de la información (Maggi Murillo & Gómez Gómez, 2021).

## 3. METODOLOGÍA

La gestión de riesgos puede resultar compleja para las pymes (Ramírez & González, 2020), por lo que en esta investigación cualitativa se propone un protocolo básico de ciberseguridad fundamentado en las etapas metodológicas de investigación, adaptación, revisión por expertos y propuesta.

### 3.1 Investigación

En esta etapa se procedió a la recopilación de información relacionada con la ciberseguridad de las pymes, consultando bases de datos tales como Google Scholar, ProQuest Digital Disertation and Theses e IEEE Xplore. Como resultado de esta etapa, se examinaron diversos trabajos de investigación (Benz & Chatterjee, 2020), tesis (Orellana, 2020), normas técnicas (ISO/IEC 27000, 2018), guías (Bruycker & Darville, 2017), así como buenas prácticas y tendencias en ciberseguridad (WEF, 2022).

Por otro lado, se analizó el contexto actual de las amenazas y vulnerabilidades que sufren las empresas a nivel global (ESET, 2022), y se tomó la información más reciente relacionada con amenazas en seguridad relevantes para este artículo.

### 3.2 Adaptación de la información recopilada

Una vez identificada la información de interés para la creación del protocolo, se procedió a la traducción en los casos en los que fue requerido; se seleccionó el contenido de artículos y documentos, así como la adaptación de la redacción, con vistas al objetivo de la investigación.

### 3.3 Revisión por expertos

La información recopilada y adaptada fue sometida al conocimiento de expertos locales en la materia. Así, se obtuvieron sugerencias, cambios y consejos para la construcción del protocolo. En esta etapa metodológica, se determinó que el protocolo estuviese integrado por los siguientes procesos: definición del perfil del usuario, políticas de privacidad, antivirus, *firewall*, políticas de acceso, infraestructura, respaldo o *backup* y sistemas de administración gerencial.

### 3.4 Propuesta de un protocolo

Producto de las anteriores etapas metodológicas, se construyó el protocolo, adaptando el conocimiento existente al contexto y requerimientos de las pymes, para ser implementado de una manera simple, práctica y efectiva. De este modo, las pymes pueden tener un nivel de protección razonable para resguardar la información y minimizar el riesgo.

## 4. PROPUESTA DE UN PROTOCOLO BÁSICO DE CIBERSEGURIDAD

La norma ISO/IEC 27001 ayuda a las pymes a estructurar la capacitación en seguridad cibernética de acuerdo con las mejores prácticas internacionales, así como a definir responsabilidades en caso de incumplimiento (BSI, 2022). Tal como lo expresan Marchand-Niño y Ventocilla (2020), una de las dificultades de estos estándares y regulaciones es el número y diversidad de controles que contienen; por ejemplo, la familia ISO/IEC establece 114 controles, mientras que el Instituto Nacional de Normas y Tecnología (NIST, por sus siglas en inglés) del Departamento de Comercio de los Estados Unidos define 444 controles de seguridad. De acuerdo con Ramírez Montealegre (2016), la implementación de este tipo de normas implica un gran esfuerzo y costo para las pymes, por lo que es necesario establecer un protocolo básico de fácil implementación y evaluación. En la Tabla 1 se propone el protocolo básico de ciberseguridad para pymes.

**Tabla 1**

*Protocolo básico de ciberseguridad para pymes*

| Nombre | Descripción | Fuentes |
|---|---|---|
| Definición del perfil de usuario | Definir los lineamientos para gestionar los privilegios de usuario para cada una de las unidades administrativas, departamentos o dependencias, de acuerdo con la estructura organizacional y el manual de funciones, teniendo claras cuáles son las actividades y la interacción de cada usuario con los sistemas informáticos en la organización para limitar su acceso. En caso de que la pyme no tenga dicha información, esta se debe construir según las funciones de los usuarios de cada sistema. | (Bruycker & Darville, 2017), (Australian Cyber Security Centre [ACSC], 2021), (Cybersecurity and Infrastructure Security Agency [CISA], 2021), (NCSA, 2018), (Marchand-Niño & Ventocilla, 2020), (Martínez & Blanco, 2020), (Cabezas Juárez, 2020) |
| Políticas de privacidad | En caso de que la pyme utilice el comercio electrónico, para que este sea fiable para el cliente potencial, se deben cumplir los requisitos legales y reglamentarios de privacidad, manejo de datos y seguridad, a los que obliga la legislación de cada país. Si se realizan compras en línea, se deben configurar los ajustes de privacidad para reforzar la seguridad y limitar la cantidad de datos compartidos con sus proveedores. En este punto también se deben definir políticas de uso de sitios, evitando que los colaboradores accedan a sitios riesgosos. | (Bruycker & Darville, 2017), (NCSA, 2018), (Navarro Uriol, 2020) |
| Antivirus | Toda pyme, sin importar su tamaño, debe definir los estándares y lineamientos básicos para el uso de antivirus en los equipos de cómputo. Este *software* debe estar actualizado y tener las respectivas licencias de uso. | (Bruycker & Darville, 2017), (ACSC, 2021), (CISA, 2021), (ENISA, 2021), (Gutiérrez-Cárdenas & Orihuela, 2016), (Marchand-Niño & Ventocilla, 2020), (De la Rosa, 2019), (Martínez & Blanco, 2020) |

(*continúa*)

(*continuación*)

| Nombre | Descripción | Fuentes |
|---|---|---|
| *Firewall* | Un *firewall* perimetral ayuda a monitorear, detectar y bloquear la mayor parte de las amenazas que se producen diariamente. Se ubica habitualmente en el punto de conexión de la red interna de la pyme con la red exterior (internet). Su función es realizar un filtrado, permitir y negar el paso a "intrusos" que no cumplan con las políticas que se configuran en el equipo, a fin de proteger la red interna de intentos de acceso no autorizados. La implementación de un *firewall* es técnicamente sencilla; desafortunadamente, no puede ofrecer protección una vez que el agresor lo traspasa o permanece en el entorno. | (Morales et al., 2020), (ENISA, 2021), (NCSA, 2018), (Bruycker & Darville, 2017), (Marchand-Niño & Ventocilla, 2020), (De la Rosa, 2019), (Martínez & Blanco, 2020), (Cuenca, 2016), (CISA, 2021) |
| Políticas de acceso | Es importante determinar los permisos de acceso apropiados para cada usuario y grupos de usuarios. Es necesario definir una lista de los usuarios a quienes se les permite el acceso a ciertos sitios y también a los que se les niega. | (Bruycker & Darville, 2017), (ACSC, 2021), (CISA, 2021), (NCSA, 2018), (Marchand-Niño & Ventocilla, 2020), (De la Rosa, 2019), (Ramírez & González, 2020) |
| Infraestructura | Se refiere a la selección de la arquitectura de operación, es decir, si se utilizará un servidor físico o en la nube, o bien una combinación, esto es, un servidor local con réplica en entorno *cloud*. Se deben establecer criterios de almacenamiento, control de accesos y perfiles de usuario, entre otros. En caso de que un tercero brinde el servicio, es recomendable tener el alcance claramente definido en un contrato. | (Martínez & Blanco, 2020), (Bruycker & Darville, 2017), (Palafox-Pascual, 2019), (NCSA, 2018), (Navarro Uriol, 2020), (Gobierno de Japón, 2021) |
| Respaldo de la información sensible | Se sugieren respaldos de los datos sensibles de la organización; para ello, es importante definir qué tipo de datos se deben resguardar, la frecuencia del respaldo, el tipo de dispositivos utilizados y el lugar para resguardar los respaldos, entre otros. | (Cabezas Juárez, 2020), (Martínez & Blanco, 2020), (Bruycker & Darville, 2017), (Iao, 2021), (Palafox-Pascual, 2019), (ACSC, 2021), (CISA, 2021), (ENISA, 2021), (Marchand-Niño & Ventocilla, 2020), (De la Rosa, 2019) |

(*continúa*)

(*continuación*)

| Nombre | Descripción | Fuentes |
|---|---|---|
| Definición de la metodología para el desarrollo y administración de los sistemas | Los sistemas de información gerencial pueden ser comprados a un tercero o desarrollados internamente. En el primer caso, es importante detallar las expectativas y el alcance en un acuerdo o contrato. En cambio, las pymes que tienen sistemas de información, sea que lo desarrollen internamente o que lo compren a la medida, deberán contar con una metodología y estándares claros para el desarrollo y administración de estos sistemas. La capacitación y mejora continua permitirá accionar anticipadamente para llevar un control de qué información se debe respaldar. Las bases de datos y códigos fuente son lo mínimo recomendable. | (Anchundia Betancourt, 2017), (Bruycker & Darville, 2017), (NCSA, 2018) |

El capital humano es el factor fundamental para la transformación cultural (Díaz, 2021). Se requiere una estrecha cooperación entre los colaboradores, la gestión formativa y la gerencia de todas las áreas y funciones de la organización (Vergara-Romero et al., 2021). Para la adecuada implementación de este protocolo, se sugiere complementar con las siguientes dos dimensiones:

### 4.1 Involucrar a la dirección de la pyme

Tal como lo establece la norma ISO/IEC 27000, una de las bases fundamentales sobre las cuales hay que iniciar un proyecto de este tipo es el apoyo claro y decidido de la dirección de la organización, ya que el cambio de cultura y concientización que implica el proceso hace necesario el impulso constante de las autoridades. Es necesario sensibilizar a los directivos y avanzar en las iniciativas de las empresas para fortalecer la ciberseguridad en línea con la digitalización (Gobierno de Japón, 2021).

### 4.2 Formación del personal

La principal amenaza que afecta la seguridad de la información de una pyme es el desconocimiento del concepto mismo (Inoguchi & Macha, 2017). De la Rosa (2019) explica que la ciberseguridad dentro de una empresa sigue el modelo de una cadena, que se rompe por su eslabón más débil; en el caso de la ciberseguridad, sabemos

que ese eslabón son los colaboradores. Es todo un reto conseguir que el colaborador esté plenamente identificado con acciones para la protección de los datos de la organización, pero se puede lograr a través de la sensibilización, la capacitación y la divulgación y mejora continua.

#### *4.2.1 Sensibilización*

Ramírez Montealegre (2016) recomienda tener programas de concientización en ciberseguridad en las pymes, dándoles un enfoque práctico y tangible que ayude a identificar situaciones de riesgo y pueda aportar en las decisiones y acciones. De la Rosa (2019) pide sensibilizar al personal sobre los riesgos cibernéticos, para que todos y cada uno de los colaboradores se autoperciban como parte fundamental de la ciberseguridad de la empresa, creando una cultura consciente del riesgo. Casi cualquier colaborador puede proporcionar una puerta abierta a la red de una organización, y los ciberdelincuentes lo saben (NCSA, 2018); por ello, es indispensable que los colaboradores también lo entiendan.

#### *4.2.2 Capacitación*

Navarro Uriol (2020) indica que cada colaborador debe proteger su puesto de trabajo, por lo que se le debe capacitar sobre el manejo seguro del correo electrónico, sitios web, dispositivos móviles, teletrabajo, redes sociales, unidades USB, etcétera. Debido a los ataques relacionados con errores humanos, como *phishing* u otras técnicas de ingeniería social (Palafox-Pascual, 2019), es primordial capacitar también sobre ingeniería social, para que los colaboradores conozcan los tipos de engaños, tretas y artimañas (Borghello, 2009) de los ciberdelincuentes, los cuales se orientan a que el usuario comprometa al sistema y revele información valiosa a través de acciones que van desde un clic hasta atender un llamado telefónico, los cuales pueden derivar en la pérdida de información confidencial.

#### *4.2.3 Divulgación y mejora continua*

Martínez y Blanco (2020) recomiendan generar una estrategia de difusión del programa de gestión de la seguridad que se va a implementar, ya que se requiere que todos los que integran la organización participen para producir un nivel de seguridad. Las personas son una gran debilidad en la ciberseguridad, pero cuando se involucran y se capacitan correctamente, pueden convertirse en la primera línea de defensa contra los atacantes (Ponsard et al., 2019); por ello, es necesario que las pymes comuniquen y refuercen constantemente a sus colaboradores sobre estos temas para crear una cultura de ciberseguridad mediante la formación continua y la actualización de las herramientas tecnológicas utilizadas.

## 5. CONCLUSIONES

La ciberseguridad no ha sido una alta prioridad para la mayoría de las pymes (Benz & Chatterjee, 2020), aun cuando la mayoría de ellas parecen tener un nivel de conciencia sobre la importancia de la ciberseguridad. Al observar las estadísticas de ataques, continúa habiendo fallas. Una primera explicación es que las medidas de seguridad se perciben como demasiado complejas, lentas y que requieren un alto nivel de conocimientos técnicos sobre los sistemas de informática. Otra razón es la dificultad para pasar de la concientización inicial a la emergencia de una cultura de ciberseguridad interna, debido a la falta de recursos, tales como dinero, tiempo y experiencia (Ponsard et al., 2019).

Las escasas medidas de seguridad de la información, la poca capacitación del personal de la empresa y las deficientes políticas de seguridad informática en las pymes han tenido un impacto negativo en el desarrollo de sus actividades comerciales (Zuña Macancela et al., 2019). La gerencia, al momento de gestionar sus riesgos, también tiene que enfocarse en el aspecto informático, pues debe ser consciente del riesgo tecnológico, las amenazas cibernéticas y las deficiencias de los sistemas informáticos, ya que estos elementos también ponen en peligro el cumplimiento de los objetivos organizacionales y, por ende, la continuidad del negocio (Peralta Zuñiga & Aguilar Valarezo, 2021).

Las pymes se colocarían en la ruta para evolucionar de una etapa de concientización del riesgo a la construcción de una cultura de ciberseguridad si hicieran una adecuada utilización de los recursos escasos para salvaguardar la confidencialidad, integridad y disponibilidad del activo más valioso: la información. La transición de las pymes no es un proceso rápido, pero la implementación de este protocolo básico es un paso firme para construir una cultura de ciberseguridad.

## REFERENCIAS

Abu-Nimeh, S., Nappa, D., Wang, X., & Nair, S. (2007). A comparison of machine learning techniques for phishing detection. En *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit* (pp. 60-69). https://doi.org/10.1145/1299015.1299021

Anchundia Betancourt, C. E. (2017). Ciberseguridad en los sistemas de información de las universidades. *Dominio de las Ciencias*, *3*(3), 200-217. https://dialnet.unirioja.es/servlet/articulo?codigo=6102849

Australian Cyber Security Centre. (2021). *Personal cyber security: Next steps guide*. https://www.cyber.gov.au/acsc/view-all-content/guidance/personal-cyber-security-next-steps-guide

Bartesaghi, I., & Weck, W. (Eds.). (2022). *Los efectos de la digitalización, inteligencia artificial, big data e industria 4.0 en el trabajo de las pymes en Latinoamérica*. Konrad-Adenauer-Stiftung e. V.; Universidad Católica del Uruguay. https://www.kas.de/en/web/regionalprogramm-adela/single-title/-/content/losefectos-de-la-digitalizacion-inteligencia-artificial-big-data-e-industria-4-0-en-eltrabajo-de-l

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, *63*(4), 531-540. https://doi.org/10.1016/j.bushor.2020.03.010

Borghello, C. (2009). *El arma infalible: la ingeniería social*. ESET. https://www.eset-la.com/pdf/prensa/informe/arma_infalible_ingenieria_social.pdf

Bruycker, M., & Darville, C. (2017). *Cyber security guide for SME*. Centre for Cyber Security Belgium. https://ccb.belgium.be/en/document/guide-sme

BSI. (2022). Cybersecurity confidence for the SME. *BSI Blog*. https://www.bsigroup.com/enGB/blog/Small-Business-Blog/cybersecurity-confidence-for-the-sme/

Cabezas Juárez, I. C. (2020). *Implementación de un framework de ciberseguridad compuesto por normas y controles para proteger la información de las pequeñas y medianas empresas en Lima* [Tesis de grado, Universidad de San Martín de Porres]. Registro Nacional de Trabajos de Investigación. https://renati.sunedu.gob.pe/handle/sunedu/2847596

Cherepanov, A., & Lipovsky, R. (2017, 12 de junio). *Industroyer: Biggest threat to industrial control systems since Stuxnet*. WeLiveSecurity. https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrialcontrol-systems-since-stuxnet/

Cortés Aldana, D. G. (2016). *Firewalls de nueva generación: la seguridad informática vanguardista* [Tesis de grado, Universidad Piloto de Colombia]. Re-Pilo. http://repository.unipiloto.edu.co/handle/20.500.12277/2719

Cuenca, J. (2016). *Firewall o cortafuegos*. Universidad Nacional de Loja. https://www.researchgate.net/publication/295256426_FIREWALL_O_CORTAFUEGOS

Cybersecurity and Infrastructure Security Agency. (2021). *Cyber essentials starter kit*. https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Starte r%20Kit_03.12.2021_508_0.pdf

De la Rosa, J. (2019). *Ciberseguridad para pymes* [Trabajo de fin de grado, Universidad de Valladolid]. Universidad de Valladolid, Repositorio Documental. https://uvadoc.uva.es/handle/10324/38735

Díaz, M. (2021). *Estado de la ciberseguridad en la logística de América Latina y el Caribe.* Comisión Económica para América Latina y el Caribe, serie Desarrollo Productivo n.° 228. https://repositorio.cepal.org/handle/11362/47240

Eggers, F. (2020). Masters of disasters? Challenges and opportunities for SMEs in times of crisis. *Journal of Business Research*, *116*, 199-208. https://doi.org/10.1016/j.jbusres.2020.05.025

ENISA. (2021). *Guía de ciberseguridad para pymes*. The European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/report-files/smes-leaflettranslations/enisa-cybersecurity-guide-for-smes_es.pdf

ESET. (2022, 2 de junio). *Threat Report T1 2022*. https://www.welivesecurity.com/wp-content/uploads/2022/06/eset_threat_report_t12022.pdf

Faith, M., Leiva, J. C., & Mora, R. (2022). Las pymes en Costa Rica. En I. Bartesaghi & W. Weck (Eds.), *Los efectos de la digitalización, inteligencia artificial, big data e industria 4.0 en el trabajo de las pymes en Latinoamérica*. Konrad-Adenauer-Stiftung e. V.; Universidad Católica del Uruguay. https://www.kas.de/en/web/regionalprogramm-adela/single-title/-/content/losefectos-de-la-digitalizacion-inteligencia-artificial-big-data-e-industria-4-0-en-eltrabajo-de-l

Fernández, M. C., & Puig, P. (2022). *Los desafíos del comercio electrónico para las PyME: principales claves en el proceso de digitalización*. Banco Interamericano de Desarrollo. https://publications.iadb.org/es/los-desafios-del-comercio-electronico-para-las-pyme-principales-claves-en-el-proceso-de

Gobierno de Japón. (2021). *Cybersecurity for all*. https://www.nisc.go.jp/pdf/policy/kihons/cs-senryaku2021-en-booklet.pdf

Gutiérrez-Cárdenas, J. M., & Orihuela, L. L. (2016). Filogenia de *malware* orientada al análisis de librerías. *Interfases*, *9*, 67-86. https://doi.org/10.26439/interfases2016.n009.1241

Horn, A. (2017, 11 de diciembre). Cybersecurity should be a top concern for middle-market companies. *SmallBizDaily*. https://www.smallbizdaily.com/cybersecurity-middlemarket-companies/

Iao, K. (2021, 23 de abril). What is a remote desktop protocol attack? *Paubox*. https://www.paubox.com/blog/what-is-remote-desktop-protocol-attack/

Inoguchi, A., & Macha, E. L. (2017). *Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las pymes del Perú, 2016* [Tesis de grado, Universidad San Ignacio de Loyola]. https://repositorio.usil.edu.pe/handle/usil/2810

Kovac, R. (2022, 2 de junio). *Foreword ESET Threat Report T1 2022*. https://www.welivesecurity.com/wpcontent/uploads/2022/06/eset_threat_report_t12022.pdf

Lara, J. F. (2022, 22 de agosto). Costa Rica recibió 513 millones de intentos de ciberataques en primer semestre. *La Nación*. https://www.nacion.com/el-pais/servicios/costarica-recibio-513-millones-de-intentos-de/YFLBY3DU55GRDJGL76NGX4V6UQ/story/

Maggi Murillo, G., & Gómez Gómez, O. S. (2021). Estudio preliminar sobre conocimiento de ciberseguridad en usuarios de PYMEs: caso de estudio en Riobamba. *Perspectivas*, *3*(2), 45-53. https://doi.org/10.47187/perspectivas.vol3iss2.pp45-53.2021

Mao, J., Bian, J., Tian, W., Zhu, S., Wei, T., Li, A., & Liang, Z. (2018). Detecting phishing websites via aggregation analysis of page layouts. *Procedia Computer Science*, *129*, 224-230. https://doi.org/10.1016/j.procs.2018.03.053

Marchand-Niño, W.-R., & Ventocilla, E. J. V. (2020). Modelo Balanced Scorecard para los controles críticos de seguridad informática según el Center for Internet Security (CIS). *Interfases*, *13*, 57-76. https://doi.org/10.26439/interfases2020.n013.4876

Martínez, J. A., & Blanco, L. X. (2020). *Recomendaciones de buenas prácticas de ciberseguridad en Pymes para la generación de soluciones de detección de intrusos usando Snort* [Tesis de grado, Universidad Autónoma de Bucaramanga]. https://repository.unab.edu.co/handle/20.500.12749/13911

Messmer, E. (2008, 29 de junio). *Tech Talk: Where'd it come from, anyway?* PCWorld. https://web.archive.org/web/20121016035507/https://www.pcworld.com/article/147 698/tech.html

Moncada Vargas, A. E. (2020). Comparación de técnicas de *machine learning* para detección de sitios web de *phishing*. *Interfases*, *13*, 77-103. https://doi.org/10.26439/interfases2020.n013.4886

Morales, F., Toapanta, S., & Toasa, R. M. (2020). Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información. *Revista Ibérica de Sistemas e Tecnologias de Informação*, *E27*, 553-565. https://www.researchgate.net/publication/339956501_Implementacion_de_un_sistema_de_seguridad_perimetral_como_estrategia_de_seguridad_de_la_informacion

National Cyber Security Alliance. (2018). *The cybersecurity awareness toolkit*. https://staysafeonline.org/wp-content/uploads/2018/09/SMB-Toolkit-FINAL.pdf

Navarro Uriol, C. (2020). *Estrategias de ciberseguridad: el caso de la pequeña y mediana empresa* [Trabajo de fin de grado, Universidad de Zaragoza]. Zaguan. Repositorio Institucional de Documentos. https://zaguan.unizar.es/record/101988/files/TAZ-TFG2020-1242.pdf?version=1

Orellana, F. D. (2020). *Cybersecurity incident response capabilities in the Ecuadorian small business sector: A qualitative study* [Tesis de doctorado, Northcentral University, School of Business and Technology Management]. ProQuest Dissertations & Theses Global. http://www.proquest.com/pqdtglobal/docview/2466034020/abstract/6BDCDD913D 1D469EPQ/1

Organización Internacional para Estandarización & International Electrotechnical Comission (2018). *ISO/IEC 27000*. https://www.normasiso.net/wpcontent/uploads/2016/10/iso-27000.pdf

Palafox-Pascual, L. (2019). *NUTRIA: "Una metodología de ciberseguridad para pymes en entornos industriales"* [Tesis de maestría, Universidad Internacional de La Rioja]. Re-Unir. Repositorio Digital. https://reunir.unir.net/handle/123456789/9422

Peralta Zuñiga, M. L., & Aguilar Valarezo, D. N. (2021). La ciberseguridad y su concepción en las PYMES de Cuenca, Ecuador. *Contabilidad y Auditoría*, *53*, 99-126. https://ojs.econ.uba.ar//index.php/Contyaudit/article/view/2061

Ponsard, C., Grandclaudon, J., & Bal, S. (2019). Survey and lessons learned on raising SME awareness about cybersecurity. En *Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP)* (pp. 558-563). https://doi.org/10.5220/0007574305580563

Ramírez, C., & González, J. C. (2020). *Guía de controles y buenas prácticas de ciberseguridad para mipymes* [Trabajo de grado, Tecnológico de Antioquia Institución Universitaria]. Repositorio Digital TDEA. https://dspace.tdea.edu.co/handle/tdea/1394

Ramírez Montealegre, B. (2016). *Medición de madurez de ciberseguridad en pymes colombianas* [Tesis de maestría, Universidad Nacional de Colombia]. Repositorio Institucional. Biblioteca Digital. https://repositorio.unal.edu.co/handle/unal/57956

Semrau, T., Ambos, T., & Kraus, S. (2016). Entrepreneurial orientation and SME performance across societal cultures: An international study. *Journal of Business Research*, *69*(5), 1928-1932. https://doi.org/10.1016/j.jbusres.2015.10.082

Vergara-Romero, A., Márquez Sánchez, F., Sorhegui-Ortega, R., & Olalla-Hernández, A. (2021). Capital humano: actor central para la sostenibilidad organizacional. *Revista Venezolana de Gerencia*, *26*(93), 297-307.

Weinelt, B. (2016). *Digital transformation of industries*. World Economic Forum. https://www.weforum.org/reports/digital-transformation-of-industries/

World Economic Forum. (2022). *Global Cybersecurity Outlook 2022*. https://www.weforum.org/reports/global-cybersecurity-outlook-2022/

Zuña Macancela, E. R., Arce Ramírez, Á. A., Romero Berrones, W. J., & Soledispa Baque, C. J. (2019). Análisis de la seguridad de la información en las PYMES de la ciudad de Milagro. *Universidad y Sociedad*, *11*(4), 487-492. http://scielo.sld.cu/scielo.php?script=sci_abstract&pid=S2218362020190004004 87&lng=es&nrm=iso&tlng=en