Framework de ciberseguridad basado en la Norma ISO 27001 para Pymes educativas

Humberto Bonilla Dávila [1]
Ricardo Andrés Almeida Delgado [2]

Resumen

La actual coyuntura de trabajo remoto y el uso intensivo del internet hacen que la ciberseguridad sea un tema que no puede pasar desapercibido. En particular para las pymes educativas que deben integrar sus procesos a la realidad de la educación virtual, tales como el E-learning y B-Learning. Ciberseguridad es un concepto que en principio para las pymes parece difícil de implementar y/o que no lo tienen contemplado dentro de sus planes de desarrollo y presupuesto. Partiendo de ello, la investigación que aquí se presenta tuvo como objetivo orientar a la Pymes para tener una forma ordenada y fácil de implementar una política de ciberseguridad. De tal modo, se propone un Framework de ciberseguridad basado en la norma ISO-27001, a partir de la selección de un conjunto de buenas prácticas que

1 Ingeniero de Sistemas, Universidad Santiago de Cali, Estudiante; humberto.bonilla00@usc.edu.co.
2 Ingeniero informático, Advanced Diploma In Client-Server Programming, Especialista en investigación - Magister en informática, Corporación Universitaria Minuto de Dios, Docente Investigador); ricardo.almeida@uniminuto.edu.

ofrecen organizaciones dedicadas a combatir el fraude y los ataques a los activos informáticos. En este documento se selecciona un subconjunto de controles, tomando como base el estándar ISO-27001, a partir del cual se definieron controles tanto obligatorios como recomendables con los cuales las pymes educativas pueden emprender una política de ciberseguridad eficiente y accesible.

Palabras clave: políticas, prácticas, ciberseguridad, estándares, vulnerabilidad, protección, continuidad del negocio, ISO27K

Abstract

The current situation of remote work and the intensive use of the internet make cybersecurity an issue that cannot go unnoticed. For educational small and medium-sized enterprises (SMEs), that must integrate their processes into the reality of E-learning and B-Learning education. Cybersecurity is a concept that in principle for SMEs seems difficult to implement and that they do not have as a principle to contemplate within their development plans and budget. With the aim of collaborating so that SMEs have an orderly and easy way to implement a cybersecurity policy, this article proposes a cybersecurity Framework based on ISO27K, based on the selection of a set of good practices offered by dedicated organizations to combat fraud and attacks on computer assets. In this document a subset of controls is selected based on the ISO27K standard, from which both mandatory and recommended controls were defined with which educational SMEs can undertake a cybersecurity policy.

Keywords: policies, practices, cybersecurity, standards, vulnerability, protection, business continuity, ISO27K

Introducción

Estamos viviendo la denominada “Cuarta Revolución Industrial” (Centro de Comercio Internacional, 2018), la cual está introduciendo innovaciones tecnológicas, transformando la manera en

que la sociedad se relaciona e introduciendo cambios culturales y económicos. Esta revolución está penetrando todos los aspectos de la sociedad, modificando la forma en que nos comunicamos y forzando a las empresas a asimilar estas transformaciones.

La digitalización está transformando las organizaciones tradicionales, principalmente debido a la aparición de nuevos modelos de negocios soportados por procesos colaborativos. Bárcena, secretaria ejecutiva de la CEPAL, expone que "la digitalización es una herramienta clave para aumentar la productividad y la calidad del trabajo que generan las pequeñas y medianas empresas (pymes), y contribuir así a reducir la desigualdad en la región" (CEPAL, 2016).

Hoy el foco está en los datos, la conectividad y la movilidad. La empresa colombiana no escapa a estos temas; por el contrario, la velocidad de la digitalización está impulsando, dinamizando y diversificando la economía (Kannan & Li, 2017), lo que lleva a que las pequeñas empresas aceleren su ingreso al comercio electrónico para sobrevivir a la competencia y no perder mercado.

La digitalización trae consigo la presencia de los llamados hackers, quienes han afectado la integridad y el buen uso de los sistemas informáticos. Tal es el caso del ataque cibernético ransomware denominado "WannaCry" (Routledge, 2017), que tuvo presencia en varios países, como España, Reino Unido, Turquía, Ucrania, China, Brasil, México y Colombia. Este ataque afectó a empresas de diferentes sectores: ferroviarias, telecomunicaciones, universidades, hospitales, gobiernos y bancos, siendo los dos últimos los objetivos más llamativos de los atacantes.

Por otro lado, las tecnologías de la comunicación y la información (TIC), así como las redes y la conectividad, juegan un papel muy importante en el desarrollo de la llamada Revolución Industrial 4.0. Desde el punto de vista económico, el crecimiento de los negocios por internet ha impactado de forma positiva el desarrollo de diferentes mercados. Sin embargo, el crecimiento y la creciente penetración global de las TIC también han traído un aumento de las actividades ilícitas en el ciberespacio, que se describe como el entorno formado por componentes físicos y no físicos, caracterizado por el uso de computadoras y el espectro electromagnético para almacenar, modificar e intercambiar datos utilizando redes informáticas.

La problemática del crimen cibernético, el espionaje y el terrorismo a través de internet ha hecho que cada país, para proteger la infraestructura que depende del uso de las TIC, esté

adoptando e implementando estrategias nacionales de ciberseguridad (NCSS). Adoptar una NCSS tiene como objetivo garantizar un enfoque coherente a nivel nacional para asegurar el dominio cibernético, enfrentar los riesgos y reducir las amenazas a las que está expuesto cualquier estado u organización grande, mediana o pequeña, como las pymes.

Marco teórico

La ciberseguridad es un concepto compuesto que puede relacionarse con otras palabras, como ciberespacio, ciberamenazas, cibercriminales, y tiene como propósito la protección de la información digital que cohabita en los sistemas interconectados mediante procesos que implican prevención, detección, mitigación de riesgos y reacción ante cualquier problemática que amenace la confidencialidad, la integridad y la disponibilidad de la información. Puede utilizarse como sinónimo de seguridad de la información, seguridad informática o seguridad en la computación (Machín, N., & Gazapo, M., 2016).

Según exponen Machín, N., & Gazapo, M. (2016), "La relevancia de la ciberseguridad sigue viéndose incrementada debido a la aparición de una nueva ola de sistemas ciberfísicos, como los dispositivos 'inteligentes' para el hogar, vehículos autónomos y sistemas aéreos no tripulados". La protección frente a los ciber-riesgos se ha convertido, por tanto, en una prioridad para cualquier organización, sobre todo porque cada día aparecen nuevas y más sofisticadas amenazas a través de Internet (Machín, N., & Gazapo, M., 2016). Además, el primer informe de análisis de cibercrimen en Colombia de la Dirección de Investigación e Interpol de la Policía Nacional de Colombia (2017), realizado por el Centro Cibernético Policial (CCP) en alianza con la Cámara Colombiana de Informática y Telecomunicaciones (CCIT), denominado "Análisis del cibercrimen 2016-2017", muestra cómo la dinámica de los cibercrímenes y su constante evolución ha impulsado la creación de grupos delictivos que trabajan de manera cooperativa y coordinada, conformando organizaciones complejas de cibercrimen que amenazan gobiernos, empresas y personas. Estos grupos centran sus ataques en el robo de información contenida en bases de datos, la interrupción o sabotaje de servicios, y la causa de daños a la reputación de personas o empresas, lo que resulta en elevadas pérdidas monetarias.

Colombia es uno de los países latinoamericanos mejor preparados en temas de ciberseguridad; sin embargo, ha sufrido ataques que han impactado la seguridad informática empresarial, mostrando que el riesgo está latente para cualquier tipo de empresa. En 2017 se registró el ciberataque de ransomware "WannaCry", que ocurrió el 12 de mayo y se propagó rápidamente a nivel global. Como consecuencia, la información de los equipos afectados fue encriptada, y los atacantes solicitaron un rescate en bitcoins para recuperar los datos (Routledge, 2017).

La problemática es aún más relevante para las pymes educativas, que en el contexto de este documento son empresas dedicadas a la formación para el trabajo o enseñanza de idiomas. Estas empresas, con presupuestos limitados, están haciendo esfuerzos para ingresar a la era digital durante la pandemia de COVID-19, adquiriendo sistemas de información, redes, telefonía IP, conexión a Internet y otras tecnologías de hardware y software para ser competitivas en el mercado (Sabido-Domínguez, Alonso-Novelo & Barredo-Baqueiro, 2018). Sin embargo, muchas de ellas no son conscientes de que la ciberseguridad es un factor primordial y, en cualquier momento, pueden verse amenazadas por ataques cibernéticos, ya que tanto estudiantes como personal administrativo deben acceder a Internet para prestar o recibir servicios. Por lo general, desconocen los aspectos y problemas relacionados con la seguridad de la información.

Este tipo de pymes tienen poco conocimiento sobre la vulnerabilidad de sus activos informáticos y, además, no son conscientes de que los empleados son el eslabón más débil dentro de una empresa en términos de ciberseguridad. Por ello, tampoco tienen conciencia de las nuevas técnicas de hackeo o de los peligros de la web. Además, estas organizaciones suelen no contar con herramientas de seguridad adecuadas o utilizan soluciones gratuitas de firewalls o cortafuegos, sin considerar que la mayoría de ellas son versiones reducidas de productos comerciales que no cuentan con actualizaciones y, por el contrario, presentan agujeros de seguridad, lo que hace a la empresa vulnerable a los ataques cibernéticos.

Para las pymes educativas, las tecnologías digitales están modificando la forma en que prestan sus servicios y gestionan sus negocios, así como la forma en que se conectan compradores y proveedores (Sabido-Domínguez, Alonso-Novelo & Barredo-Baqueiro, 2018). La conexión de estos actores genera mejores oportunidades para algunas empresas, mientras que para

otras, representa una preocupación por la posibilidad de perder visibilidad y mercado. Esta situación deja claro que aquellas empresas que no se adapten a la revolución 4.0 tendrán menos oportunidades de prosperar en la era digital. Aunque la revolución 4.0 trae preocupaciones, las pymes deben emplear estrategias de protección para contrarrestar los ataques cibernéticos a los que están expuestas debido a la falta de presupuesto, desconocimiento, falta de infraestructura y, en general, por no contar con una estrategia de protección de la información (BMC & Forbes Insights, 2017).

Bajo estas premisas, será de gran utilidad identificar y proponer para las pequeñas empresas, en particular para las pymes del sector educativo, un conjunto de buenas prácticas de ciberseguridad que les permitan mitigar los riesgos a los cuales están expuestas, siguiendo los estándares o normas que muchas otras empresas ya están aplicando, y que los organismos nacionales e internacionales están protocolizando para que la transición hacia la revolución 4.0 no sea traumática (Jazdi, 2014). Conocer las buenas prácticas de ciberseguridad permitirá a las pymes educativas exigir que los proveedores de infraestructura garanticen la calidad de sus tecnologías, la interoperabilidad entre productos digitales, y la privacidad y seguridad de la información.

Por lo expuesto anteriormente, esta propuesta está dirigida a crear un marco de buenas prácticas en ciberseguridad basado en la norma ISO 27001 para pymes educativas. Contar con un conjunto de buenas prácticas permitirá que la dependencia tecnológica, la interconectividad requerida por la globalización y la internacionalización no sean susceptibles a amenazas contra la confidencialidad, integridad y disponibilidad de la información de cualquier organización, grande o pequeña. Este paso es necesario, ya que las pymes educativas están incorporando más tecnología digital, más conectividad a Internet para su operación y más almacenamiento de información en sus servidores, lo que aumenta el riesgo para la seguridad de la información (Flórez, 2012).

La preocupación por la ciberseguridad ha llevado a distintas organizaciones a desarrollar e implementar medidas para minimizar el riesgo al que están expuestos usuarios y empresas, grandes o pequeñas (pymes), ante las amenazas. Así lo expone el informe “Balance Cibercrimen en Colombia 2017” del Centro Cibernético Policial, que destaca el incremento del cibercrimen en el país, con un aumento del 28,3% en 2017 respecto a los resultados de 2016.

En la Séptima Cumbre Latinoamericana de Analistas de Seguridad, realizada en septiembre de 2017 en Buenos Aires (Argentina), Kaspersky reveló que América Latina experimentó un incremento del 59% en el número de ciberataques en 2017, con la salvedad de que estos son cada vez más sofisticados, potentes, con mayor alcance e impacto.

La preocupación mencionada también ha sido expresada por el "National Institute of Standards and Technology", que propuso como estrategia de protección el Framework denominado "Framework for Improving Critical Infrastructure Cybersecurity" (Contreras, 2018). Este marco se centra en el uso de gestores de negocios para dirigir las actividades de ciberseguridad y considerar los riesgos de ciberseguridad como parte de los procesos de gestión de riesgos de la organización. En este contexto, Microsoft también ha desarrollado un Framework de Políticas de Seguridad Cibernética, como una contribución de la empresa al estar en el centro de la problemática sobre ciberseguridad entre la industria y los gobiernos de todo el mundo. Microsoft ha participado en el desarrollo de las mejores prácticas en la regulación de la seguridad cibernética, desde enfoques centrados en los resultados hasta la creación de leyes sobre ciberdelitos, colaborando con la implementación de aspectos básicos de seguridad para infraestructuras críticas en los estados y la industria (Ciglic, 2017).

Autores como Santos Olmo Parra, Sánchez Crespo, Álvarez, Huerta y Fernández Medina Patón (2016) consideran que el foco central de un sistema de seguridad de la información debe estar basado en el análisis de riesgos, apoyando las propuestas de Barrientos en su tesis de 2005 de la Universidad EAFIT, titulada "Integration of a Safety Management System With an Information Quality Management System" y de Fredriksen, R., con su propuesta "The CORAS Framework for a Model-Based Risk Management Process", presentada en la 21st International Conference on Computer Safety, Reliability and Security de Safecomp en 2002. Barrientos propone realizar un análisis de la seguridad informática e identificar el grado de vulnerabilidad para determinar los aspectos a mejorar en la empresa, con el objetivo de reducir los riesgos. El CORAS Framework propone realizar un análisis de riesgos de seguridad utilizando UML2, AS/NZS 4360, ISO/IEC27001, RM–ODP6, UP7 y XML8.

Metodología

La investigación es de tipo cuantitativa no experimental, transversal de carácter exploratoria (Hernández, 2018) tal como se muestra en la siguiente figura:

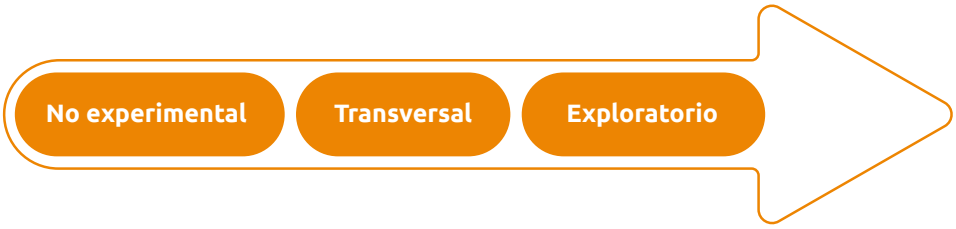

Figura 1. Fases del proceso metodológico de la investigación
Fuente. Elaboración propia

Para cumplir con el objetivo de proponer un Framework de ciberseguridad para las pymes educativas, en el desarrollo de la investigación se realizó una recopilación de información sobre cómo las empresas, y en particular las pymes educativas, deben adoptar prácticas y estrategias de ciberseguridad, así como la actitud frente a la misma, sin interferir o manipular las variables definidas, es decir, de manera no experimental.

Por otro lado, el estudio fue transversal, dado que se observaron las prácticas que aplican algunas pymes en una única ocasión, lo que llevó a definir un estudio de tipo exploratorio. Esto último se consideró lo más adecuado, teniendo en cuenta que no existe mucha información sobre el tema elegido, dirigido exclusivamente a las pymes educativas.

En cuanto a la ciberseguridad, se han mencionado diversos aspectos que pueden influir en la forma en que las MiPymes están enfrentando los problemas de seguridad de la información. Dentro de estos aspectos se incluyen problemas técnicos, humanos, organizacionales, entre otros. Esta investigación realizó una indagación holística de la ciberseguridad en las pymes educativas de Cali, cuyos resultados servirán como base para realizar estudios futuros y proporcionar lineamientos y estrategias encaminadas a mejorar las prácticas en ciberseguridad de este sector empresarial.

La población objetivo consistió en un número reducido de pymes de Cali, según la definición proporcionada por la Ley 905

de 2004. Como se mencionó anteriormente, no fue posible determinar con exactitud el número total de pymes educativas en Cali, razón por la cual se aplicaron los instrumentos necesarios a una muestra por conveniencia.

El alcance de este documento tiene como meta la creación del Framework, y se deja para un futuro trabajo la aplicación y el análisis de la efectividad de la implementación del Framework propuesto.

La investigación se desarrolló teniendo en cuenta las siguientes etapas, como se muestra en la figura 2.

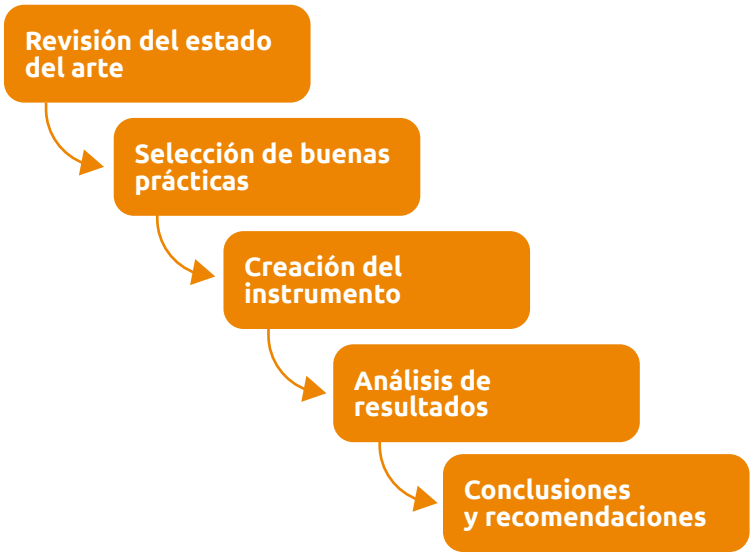

Figura 2. Etapas de desarrollo de la investigación
Fuente. Elaboración propia

Resultados y Discusión

Este apartado presenta los resultados del desarrollo de la propuesta del trabajo de investigación. Según la metodología escogida y el objetivo propuesto, se procedió con el desarrollo de cada uno de ellos.

Estado del arte de la ciberseguridad en las pymes educativas

En la investigación, se buscó ampliar y determinar el desarrollo y compromiso continuo en la ejecución de programas o parámetros de calidad requeridos para contrarrestar los problemas y situaciones relacionadas con la seguridad de la información o ciberseguridad de las pymes educativas en Cali.

Para determinar los alcances de la implementación en materia de ciberseguridad, identificando las amenazas y vulnerabilidades cibernéticas de las que puede ser víctima la institución, se procedió a obtener un conocimiento general de la institución educativa, ejecutando algunas fases importantes para el progreso de este:

- Se recolectó información de 10 organizaciones o pymes educativas a través de entrevistas con directivos, coordinadores de programas y jefes de área de tecnología, con el fin de obtener un punto de vista asertivo en cuanto al desarrollo del área en estudio.
- Se realizó una verificación y validación del estado actual de la ciberseguridad, analizando el contexto de la entidad.

Bajo esta recolección de información, se llevó a cabo el procesamiento y análisis de los datos obtenidos para obtener los insumos necesarios y realizar el diseño o elaboración de la propuesta para la implementación de buenas prácticas en ciberseguridad.

Las variables contenidas en la tabla 2, y las preguntas asociadas, se centran en la obtención de un resultado para determinar si la institución conoce y tiene implementado el concepto de ciberseguridad o parte de este, así como también las fortalezas y debilidades en cada área.

A continuación, se presenta un análisis de cada una de ellas:

Tabla 2. Cuestionario de Ciberseguridad.

VARIABLE	ÁREA	PREGUNTAS
Estructura organizacional	Organización	• ¿Cuenta la organización con un sistema SGSI? • ¿La alta dirección se ha comprometido por escrito a establecer la seguridad de la información o ciberseguridad? • ¿Existe objetivos de seguridad de información o ciberseguridad y planes para alcanzarlos? • ¿Se han definido roles y responsabilidades concretas para la seguridad de la información? • En la estructura organizacional de su empresa, ¿existe algún cargo con funciones o persona al manejo de la ciberseguridad? • ¿Se ha realizado alguna auditoría interna o externa de seguridad de información? De ser así, ¿Se ha realizado seguimiento, medición y mejora continua de la evaluación? ¿Cuál es la frecuencia de las auditorias?
Políticas, normas o practicas	Directriz	• ¿Existe una política donde se defina como utilizar las tecnologías de la información y los datos de la empresa?
	Control de acceso	• ¿Existe controles de acceso físico autorizados a los principales sistemas de tecnologías de la información, servidores y redes? • ¿Se encuentran protegidos contra daños provocados por incendios los sistemas de tecnologías de la información, servidores y redes? • ¿Cuenta con un sistema de alimentación ininterrumpida en caso de fallas de energía? • ¿El acceso como administrador está reservado solamente a los administradores? • ¿La Entidad cuenta con perfil de usuarios para acceder a los sistemas de información o datos críticos? • ¿Cómo se controla el uso de datos críticos por usuarios no autorizados?
Relevancia	Grado de importancia	• ¿La institución considera importante el concepto de ciberseguridad y todo lo que implica? • ¿En caso de tener proveedores, estos saben a quién informar la pérdida o robo

Identificar activos y análisis de riesgo	Activos	• ¿La Institución tiene identificado los activos de información (servidores, página web, correo electrónico, UPS, rack, switch)? • ¿Los activos de información tienen alguna clasificación?
	Gestión de riesgos	• ¿La institución realiza o ha realizado algún análisis de riesgos sobre los activos de información? • ¿El análisis de riesgos están enfocados a los riesgos tecnológicos?
	Amenazas y vulnerabilidades	• ¿La Institución conoce las vulnerabilidades con que cuenta los sistemas informáticos en materia de ciberseguridad? • ¿Se conoce cuáles son las amenazas más frecuentes que se presentan en el modelo de negocio?
Cultura, capacitación y entrenamiento	Personal	• ¿Se asigna algún presupuesto destinado a la ciberseguridad o seguridad de la información? • ¿Se realizan capacitaciones a los empleados de la Institución acerca de la Ciberseguridad? • ¿Los empleados de la Institución están en la capacidad de identificar algunas de las diversas amenazas cibernéticas que existe?
Tecnología	Dispositivos móviles	• ¿Se dispone de una política para el uso de dispositivos móviles? • ¿Los usuarios hacen uso de móviles personales para acceder a los datos de la Institución? • ¿Cómo se controlan y tratan los datos almacenados en estos dispositivos? • ¿En caso de robo o pérdida de un dispositivo cual es el procedimiento por seguir?
	La nube	• ¿De qué manera se asegura que el personal trabaja de forma segura? • ¿Tanto la institución como el proveedor conoce las responsabilidades en temas de la seguridad y la gestión de incidentes?
	Software	• ¿Se tiene conocimiento de todas las aplicaciones y programas del cual hace uso la Institución? • ¿La Institución cuenta con herramientas que permitan asegurar la información de su empresa? • ¿Cada cuánto tiempo se actualizan las aplicaciones y los equipos informáticos?
	Redes	• ¿Cómo se controlan los accesos a la Wi-Fi corporativa? • ¿El acceso a internet tiene medidas de protección? ¿Cómo controlan el uso de los empleados a este servicio? • ¿Cómo se controla el acceso a los servicios y aplicaciones para usuarios remotos?
	Sistemas de información	• ¿Se dispone de un listado de los sistemas de tecnologías de la información de la empresa?

Prevención	Copias de seguridad	• ¿Existe un análisis de riesgos de los sistemas de tecnologías de la información más críticos?
Planes de contingencia	Incidentes de seguridad	• ¿La institución tiene claro el concepto de incidente de seguridad? • ¿Cuentan con una gestión de incidentes de seguridad? • ¿Los usuarios pueden identificar y actuar frente a un caso de incidente de ciberseguridad?
	Continuidad del negocio	• ¿La empresa cuenta con un plan de contingencia ante un suceso de ciberseguridad? • ¿Sabe usted que debe hacer ante un evento en donde se vea comprometido la información? • ¿En caso de ataque cibernético la institución cuenta con planes de recuperación de los sistemas más críticos? • ¿Los planes de recuperación están física y lógicamente de fácil disposición en caso de emergencia? ¿Se hacen pruebas de efectividad? ¿Cada cuánto se actualiza?

Fuente. Elaboración propia

En el transcurso de la ejecución de las entrevistas, se logró observar que de las 10 pymes entrevistadas, solo 4 tenían un control adecuado. Las otras 6 presentaban poco control y descuido en el acceso al espacio donde se localizan los servidores. Se pudo observar que, inclusive, los responsables del área dejaban la puerta de acceso sin seguro, y en varias oportunidades, personal de la entidad e incluso estudiantes tuvieron la oportunidad de ingresar sin ningún tipo de control.

Otro aspecto que llama la atención es que, en la mayoría de las pymes educativas, la persona responsable del área de TIC también realiza la atención de soporte técnico. Esta labor incrementa sus funciones y disminuye la posibilidad de avanzar en la implantación de procedimientos que ayuden a garantizar la seguridad de la información y los activos informáticos.

De acuerdo con el resultado del cuestionario de la tabla 2, en 8 de las áreas TIC, se evidenció que no cuentan con un cronograma, plan definido u objetivo concreto de desarrollo de actividades sobre el tema de ciberseguridad.

Prácticas de Ciberseguridad Aplicables a las Pymes

Para dar cumplimiento al objetivo propuesto, inicialmente se procedió a realizar una investigación documental sobre qué organizaciones, empresas o entidades estaban trabajando sobre

el tema de ciberseguridad. Así, se encontró que algunos de los principales estándares de gestión de la seguridad han incorporado dentro de sus procesos el análisis y la gestión del riesgo, como lo hace ISO/IEC27005, que respalda los conceptos expuestos en la norma ISO/IEC27001 e ISO/IEC27002. También se encontró que se hace referencia a la seguridad en la norma ISO/IEC2000/ ITIL y COBIT, este último una metodología para el control de los proyectos de tecnología, los flujos de información y los riesgos que implica la falta de controles adecuados en los mismos.

El uso de buenas prácticas en ciberseguridad evita los posibles daños e incidencias que se puedan presentar en los sistemas de información, garantizando la gestión de los riesgos, minimizando las pérdidas y asegurando el uso correcto de los recursos.

En (OSIseguridad, 2015) se encuentra la frase: "Nunca abrirías tu hogar a un desconocido. ¿Por qué permites que cualquiera entre en tu vida digital?". Así mismo, Eugene Howard Spafford, experto en seguridad informática, dice que no es posible lograr un sistema completamente seguro y afirma: "El único sistema seguro es aquel que está apagado, en el interior de un bloque de hormigón protegido en una habitación sellada rodeada por guardias armados, y aun así, tengo mis dudas".

Para lograr un nivel adecuado de ciberseguridad, es necesario abarcar no solo el ámbito técnico, sino también un conjunto de elementos que proporcionen un mejor desempeño en ciberseguridad en la empresa. Entre estos se contemplan:

- **Sector técnico**: compuesto por los sistemas, dispositivos, software o hardware que permiten la seguridad.
- **Sector organizacional**: compuesto por la normatividad que hace referencia al cumplimiento de la seguridad, como normas ISO, políticas, buenas prácticas, que apoyan el ámbito técnico.
- **Sector legislativo**: dedicado al cumplimiento de la legislación vigente en materia de ciberseguridad.
- **Sector humano**: hace referencia a todo el proceso de formar y concienciar a los usuarios y personal de la empresa en el uso responsable de los equipos y la importancia de la seguridad.

Para garantizar la protección de los tres pilares fundamentales de la información, es de vital importancia identificar el tipo de información manejada y los procesos involucrados en la mis-

ma. Lo anterior, con el fin de desarrollar estrategias (SGSI) que impidan el riesgo constante en que se encuentra expuesto el activo más vital de una institución.

La investigación documental permitió observar que, aunque en todos los países hay preocupación por la problemática de la ciberseguridad, existe en España un conjunto de organizaciones que, junto con el gobierno español, han impulsado el trabajo específicamente con las pymes. Por esta razón, se han escogido como apoyo para el presente trabajo las siguientes entidades:

- **CEPREVEN**: creada en 1975, es una asociación sin ánimo de lucro que impulsa la prevención, el intercambio de informaciones entre organismos, entidades y personas físicas. Se dedica al mejoramiento y capacitación de todos los involucrados en la prevención y protección de riesgos mediante cursos de formación, consultoría y publicaciones especializadas.
- **CEPYME**: organización confederativa e intersectorial, de ámbito nacional, para la defensa, representación y fomento de los intereses de las pymes y del empresario autónomo.
- **UNESPA**: llamada Asociación Empresarial del Seguro, representa a más de 200 entidades aseguradoras y reaseguradoras que conforman al menos el 96% del volumen de negocio asegurador español.
- **CCN-CERT**: es la Capacidad de Respuesta a Incidentes del Centro Criptológico Nacional Español, adscrito al Centro Nacional de Inteligencia, cuyas funciones se pueden consultar en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia.
- **INCIBE**: es el denominado Instituto Nacional de Ciberseguridad de España, una organización dependiente del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, y consolidada como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y sectores estratégicos.
- **CESG**: es el sitio web del grupo de seguridad electrónica de comunicaciones que garantiza la seguridad de la comunicación del Gobierno Español.

- **ISO27K**: es una solución de mejora continua que permite el desarrollo del Sistema de Gestión de Seguridad de la Información (SGSI), que permite evaluar riesgos o amenazas que pueden poner en peligro la información tanto propia como de terceros. Además, permite eliminar o minimizar el peligro mediante el establecimiento de los controles y estrategias más adecuadas.

En la Tabla 3, se condensan un conjunto integral de las buenas prácticas en ciberseguridad de la información, que pueden ser aplicadas a las pymes educativas de Cali, debido a su relevancia e impacto. Estas prácticas se catalogan según la organización o entidad que las recomienda, el tipo de práctica y se asocian con referencia a si la norma ISO27K incluye o no ese tipo de práctica.

Tabla 3. Prácticas de Ciberseguridad aplicables a las pymes educativas.

Práctica / Fuente	CEPYME / CEPREVEN / UNESPA	CCN-CERT	INCIBE	CESG	ISO27K
Política y Normatividad de ciberseguridad / Cultura de ciberseguridad	X	X	X		X
Seguridad de los datos / Cifrar información sensible	X	X			X
Seguridad en la red / Redes de forma segura	X		X	X	X
Software de seguridad / protección contra malware	X	X	X	X	X
Información en tránsito (Correo electrónico – Navegador web)	X		X		X
Protección de dispositivos móviles	X			X	X
Actualizaciones	X	X	X		X
Gestión de riesgos				X	X
Incidentes	X			X	X

Formación personal (Educación y concien-cia del usuario)	X			X	X
Control de acceso (privilegios de usuario)	X		X	X	X
uso de contraseñas		X			X
Copias de seguridad periódicas		X	X		X
Revisiones regulares		X			X
Continuidad del negocio			X		X

Fuente. Elaboración propia

Partiendo de la Tabla 3 y añadiendo otras normas como COBIT (5) y NIST 800-53 (5), se observa que existen diversas normas, estándares y guías que cubren diferentes elementos de la ciberseguridad. La situación problemática para las pymes surge al momento de aplicar alguna de estas, ya que las pequeñas empresas no cuentan ni con el presupuesto ni con el conocimiento necesario para implementarlas.

Este panorama se complica aún más para las pymes debido a que muchas de las normas o estándares disponibles están orientados a la gestión de las TIC, y algunas de ellas se enfocan únicamente en la seguridad de la información, mientras que otras están más centradas en la estrategia del negocio y menos en la seguridad.

Este escenario lleva a las pymes a la necesidad de contar con una guía o framework que, dado sus limitados recursos, sea la solución más adecuada y, a su vez, fácil de aplicar.

Framework de Seguridad Aplicable a las Pymes

En el apartado anterior se mencionó que existen diversas normas, guías y estándares dedicados a cubrir diferentes aspectos de la ciberseguridad, y que el reto para las pymes radica en tomar la decisión de aplicar alguna de ellas. Este documento propone que las normas ISO27K podrían ser una solución viable y, en este sentido, se presenta cómo las buenas prácticas propuestas por las entidades españolas y la norma ISO27K se

pueden asociar para la construcción del framework propuesto, tal como se muestra en la Tabla 3.

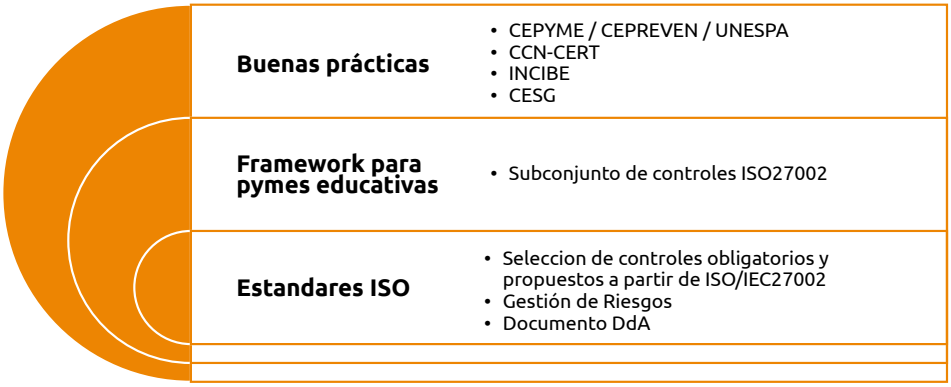

Figura 3. Buenas prácticas aplicables a las pymes educativas.
Fuente. Elaboración propia

ISO27001:2013 es un estándar universal que, además, permite obtener una certificación. Por otro lado, la ISO 27002 contiene una amplia cantidad de controles, que pueden ser excesivos para una pyme. Lo más destacable de la ISO27001 es que es aplicable a cualquier organización, sin importar su tamaño, y permite a la organización aplicar solo lo que necesite, siempre y cuando primero realice un análisis de riesgos. Esto significa que las pymes educativas podrán seleccionar únicamente los controles que consideren necesarios y adecuados para su organización.

Dado que el objetivo de este artículo es proporcionar un framework de buenas prácticas de ciberseguridad para las pymes educativas, se estudió la lista de controles más relevantes y se seleccionaron aquellos que, según la Tabla 3, se consideran aplicables a las pymes, basados en las normas ISO/IEC 27K.

Partiendo de la premisa de que la ISO27002 ofrece una gran cantidad de controles, se seleccionaron aquellos de más fácil aplicación para las pymes educativas, siempre con la premisa de que la gestión de riesgos es la base fundamental para el control de la seguridad en cualquier organización.

Cuando una pyme educativa decide implementar un estándar de gestión de seguridad de la información para proteger sus activos, la gestión de riesgos debe ser el punto de partida de su política. Esto implica superar barreras o comentarios negativos como: “tiene costos muy altos que no podemos asumir”, “¿por

qué hacerlo si no tenemos ataques diarios?", "siempre respondemos rápidamente a cualquier incidente", "si se dedican tantos recursos a la seguridad, ¿cómo podremos realizar las operaciones diarias?". Estos comentarios son típicos de la alta dirección de cualquier pyme educativa cuando se le presenta la necesidad de aplicar una política de seguridad.

La gestión de riesgos generalmente consta de las siguientes fases:

a. Análisis de los riesgos
b. Identificación de los elementos del análisis de riesgo
c. Análisis de los resultados

Teniendo en cuenta que la implementación de una política de seguridad para las pymes debe comenzar con un análisis de riesgos, la recomendación es seguir las fases descritas, tal como se muestra en la Figura 4, para emprender una política de ciberseguridad.

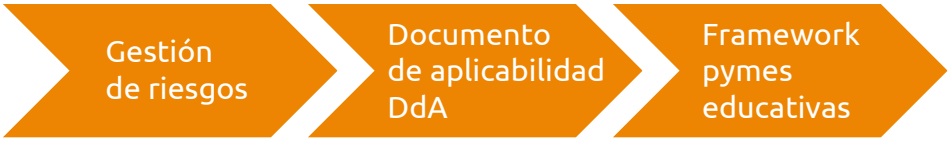

Figura 4. Fases de aplicación de Framework pymes educativas.
Fuente. Elaboración propia.

De la Figura 4 se observa que, antes de aplicar el Framework propuesto, es necesario crear el documento de aplicabilidad y realizar la gestión de riesgos. Las fases de gestión de riesgos se describieron en el apartado anterior, y el Documento de Aplicabilidad (DdA) se ilustra a continuación.

Documento de Aplicabilidad (DdA)

Toda política de seguridad debe contar con un Documento de Declaración de Aplicabilidad (DdA), ya que este constituye el vínculo entre la gestión de riesgos y la implementación de la

política. Este documento debe incluir los controles a aplicar y cómo se llevará a cabo la implementación de los mismos. Además, forma parte de la lista de documentos obligatorios para el cumplimiento de la norma ISO/IEC 27001.

El Documento de Declaración de Aplicabilidad (DdA) permite a toda organización:

- Identificar los controles requeridos para regulaciones, contratos con proveedores, procesos internos, entre otros.
- Justificar la aplicación de los controles incluidos y la exclusión de otros
- Describir cómo se aplican los controles seleccionados o excluidos, y además especificar la política, el procedimiento o el proceso de aplicación.
- Programar auditorías internas o externas para la validación y seguimiento de la política de seguridad de la información.
- Trabajar de manera sistemática y organizada.

Un documento DdA tiene una estructura y formato similar a los propuestos en la Tabla 4, como se verá a continuación, dado que no existe un modelo único.

Tabla 4. Modelo de formato documento DdD

Código Control	Seleccionado	Motivo selección	Implementado	Motivo exclusión	Referencia
A6.1.1	✓	Se requiere definir los roles y responsabilidades del recurso humano que trabajan en la pyme	✓		
A15.2.2	✗			Los proveedores no disponen acceso a los activos ni existe una gestión de servicios con ellos.	

Fuente: Elaboración propia

Como se mencionó anteriormente, las organizaciones que guían las buenas prácticas de seguridad y ciberseguridad para las pymes, como las referidas en el apartado 3.2, cumplen de alguna manera con los aspectos establecidos en la norma ISO/IEC 27002:2013. Por esta razón, si una pyme está interesada en obtener la certificación ISO 27001, deberá tener en cuenta que existe un número determinado de controles que deben aplicarse de forma obligatoria, mientras que otros son solo recomendables.

La selección de controles para el Framework propuesto incluirá solo aquellos que se consideran obligatorios para el cumplimiento de la ISO/IEC 27001:2013, junto con un conjunto de controles recomendables que facilitan la implementación de una política de ciberseguridad, como se muestra a continuación:

Tabla 4. Modelo de formato documento DdD

5.1 Dirección de gestión para la seguridad de la información	**ISO27001**
Proporciona dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos de negocio, leyes y regulaciones relevantes.	
5.1.1 Políticas para la seguridad de la información	Obligatorio
5.1.2 Revisión de las políticas para seguridad de la información	Obligatorio
6.1 Organización interna	
Establecer un marco de trabajo de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.	
6.1.1 Roles y responsabilidades para la seguridad de información	Recomendado
6.1.2 Separación de deberes	Recomendado
6.1.3 Contacto con las autoridades	Recomendado
6.1.4 Contacto con grupos de interés especial	Recomendado
6.1.5 Seguridad de la información en la gestión de proyectos	Recomendado
6.2 Dispositivos móviles y teletrabajo	
Asegurar la seguridad del teletrabajo y el uso de los aparatos móviles.	
6.2.2 Teletrabajo	Recomendado
7.1 Previo al empleo	
Asegurar que los empleados y los contratistas comprenden sus responsabilidades y que sean adecuadas para los roles para los que son considerados.	
7.1.1 Selección	Recomendado
7.1.2 Términos y condiciones del empleo	Obligatorio
Asegurar que los empleados y contratistas conocen y cumplen con sus responsabilidades de seguridad de la información.	

7.2.1 Responsabilidades de la dirección	Recomendado
7.2.2 Toma de conciencia, educación y formación en la seguridad de la información	Recomendado
7.2.3 Proceso disciplinario	Recomendado
7.3 Terminación o cambio de empleo	
Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.	
7.3.1 Terminación o cambio de responsabilidades de empleo	Recomendado
8.1 Responsabilidad por los activos	
Identificar activos organizativos y definir responsabilidades de protección apropiadas.	
8.1.1 Inventario de activos	Obligatorio
8.1.2 Propiedad de los activos	Recomendado
8.1.3 Uso aceptable de los activos	Obligatorio
8.1.4 Devolución de activos	Recomendado
8.2 Clasificación de la información	
Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.	
8.2.1 Clasificación de la información	Recomendado
8.2.2 Etiquetado de la información	Recomendado
8.2.3 Manejo de activos	Recomendado
8.3 Manipulación de media	
Prevenir la divulgación, modificación, eliminación o destrucción no autorizada de la información almacenada en los medios.	
8.3.1 Gestión de medios removibles	Recomendado
8.3.2 Eliminación de los medios	Recomendado
8.3.3 Transferencia de medios físicos	Recomendado
9.1 Requisitos de negocio para el control de acceso	
Limitar el acceso a la información y las instalaciones de procesamiento de la información.	
9.1.1 Política de control de acceso	Obligatorio
9.1.2 Política sobre el uso de los servicios de red	Obligatorio
9.2 Gestión de acceso de usuarios	
Asegurar el acceso de usuario autorizado y prevenir el acceso no autorizado a los sistemas y servicios.	
9.2.1 Registro y cancelación del registro de usuarios	Recomendado
9.2.2 Suministro de acceso de usuarios	Recomendado
9.2.3 Gestión de derechos de acceso privilegiado	Recomendado
9.2.4 Gestión de información de autenticación secreta de usuarios	Recomendado

9.2.5 Revisión de los derechos de acceso de usuarios	Recomendado
9.2.6 Retiro o ajuste de los derechos de acceso	Recomendado
9.3 Responsabilidades de los usuarios	
Asegurar que los usuarios sean responsables para la salvaguarda de la información de autenticación.	
9.3.1 Uso de la información de autenticación secreta	Recomendado
9.4 Control de acceso a sistemas y aplicaciones	
Prevenir el acceso no autorizado a los sistemas y aplicaciones.	
9.4.1 Restricción de acceso a la información	Recomendado
9.4.2 Procedimiento de ingreso seguro	Recomendado
9.4.3 Sistema de gestión de contraseñas	Recomendado
9.4.4 Uso de programas utilitarios privilegiados	Recomendado
9.4.5 Control de acceso a códigos fuente de programas	Recomendado
10.1 Controles criptográficos	
Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticación y/o la integridad de la información.	
10.1.1 Política sobre el uso de controles criptográficos	Recomendado
10.1.2 Gestión de claves	Recomendado
11.1 Áreas seguras	
Prevenir el acceso físico no autorizado, daños e interferencias a las instalaciones de procesamiento de información e información de la organización.	
11.1.1 Perímetro de seguridad física	Recomendado
11.1.2 Controles físicos de entrada	Recomendado
11.1.3 Seguridad de oficinas, recintos e instalaciones	Recomendado
11.1.4 Protección contra amenazas externas y ambientales	Recomendado
11.1.5 Trabajo en áreas seguras	Recomendado
11.1.6 Áreas de carga y descarga	Recomendado
11.2 Equipos	
Prevenir la pérdida, el daño, el robo o el compromiso de los activos y la interrupción de las operaciones de la organización.	
11.2.1 Ubicación y protección de los equipos	Recomendado
11.2.2 Servicios de suministro	Recomendado
11.2.3 Seguridad del cableado	Recomendado
11.2.4 Mantenimiento de equipos	Recomendado
11.2.5 Retirada de activos	Recomendado
11.2.6 Seguridad de equipos y activos fuera de las instalaciones	Recomendado
11.2.7 Eliminación segura o reutilización de equipos	Recomendado

11.2.8 Equipos de usuario desatendidos	Recomendado
11.2.9 Política de escritorio y pantalla limpios	Recomendado
12.1 Procedimientos operacionales y responsabilidades	
Asegurar operaciones correctas y seguras de las instalaciones de procesado de la información.	
12.1.1 Procedimientos operacionales documentados	Obligatorio
12.1.2 Gestión de cambios	Recomendado
12.1.3 Gestión de capacidad	Recomendado
12.1.4 Separación de los ambientes de desarrollo, pruebas y operación	Recomendado
12.2 Protección contra códigos maliciosos	
Asegurar que la información y las instalaciones de procesado de la información están protegidas contra los códigos maliciosos.	
12.2.1 Controles contra códigos maliciosos	Recomendado
12.3 Copias de respaldo	
Proteger contra la pérdida de datos.	
12.3.1 Respaldo de información	Recomendado
12.4 Registro y monitorización	
Registrar eventos y generar evidencias.	
12.4.1 Registro de eventos	Obligatorio
12.4.2 Protección de la información de registro	Recomendado
12.4.3 Registros del administrador y del operador	Obligatorio
12.4.4 Sincronización de relojes	Recomendado
12.5 Control de software operacional	
Asegurar la integridad de los sistemas operacionales.	
12.5.1 Instalación de software en sistemas operativos	Recomendado
12.6 Gestión de la vulnerabilidad técnica	
Prevenir la explotación de las vulnerabilidades técnicas.	
12.6.1 Gestión de las vulnerabilidades técnicas	Recomendado
12.6.2 Restricciones sobre la instalación de software	Recomendado
12.7 Consideraciones sobre auditorias de sistemas de información	
Minimizar el impacto de las actividades de auditoría en los sistemas operacionales.	
12.7.1 Información controles de auditoría de sistemas	Obligatorio
13.1 Gestión de seguridad de las redes	
Asegurar la protección de la información en redes y en las instalaciones de procesado de la información de soporte.	

13.1.1 Controles de redes	Recomendado
13.1.2 Seguridad de los servicios de red	Recomendado
13.1.3 Separación en las redes	Recomendado
13.2 Transferencia de información	
Mantener la seguridad de información transferida dentro de la organización y con cualquier entidad externa.	
13.2.1 Políticas y procedimientos de transferencia de información	Recomendado
13.2.2 Acuerdos sobre transferencia de información	Recomendado
13.2.3 Mensajería electrónica	Recomendado
13.2.4 Acuerdos de confidencialidad o de no divulgación	Obligatorio
14.1 Requisitos de seguridad de los sistemas de información	
Asegurar que la seguridad de la información es una parte integral de los sistemas de información en todo el ciclo de vida. Esto además incluye los requisitos para los sistemas de información los cuales proporcionan servicios sobre redes públicas.	
14.1.1 Análisis y especificación de requisitos de seguridad de la información	Obligatorio
14.1.2 Seguridad de servicios de las aplicaciones en redes publicas	Recomendado
14.1.3 Protección de transacciones de los servicios de las aplicaciones	Recomendado
14.2 Seguridad en los procesos de desarrollo y soporte	
Asegurar que la seguridad de la información está diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información	
14.2.1 Política de desarrollo seguro	Recomendado
14.2.2 Procedimientos de control de cambios en sistemas	Recomendado
14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Recomendado
14.2.4 Restricciones en los cambios a los paquetes de software	Recomendado
14.2.5 Principios de construcción de sistemas seguros	Recomendado
14.2.5 Principios de construcción de sistemas seguros	Obligatorio
14.2.6 Entorno de desarrollo seguro	Recomendado
14.2.7 Desarrollo contratado externamente	Recomendado
14.2.8 Pruebas de seguridad de sistemas	Recomendado
14.2.9 Prueba de aceptación de sistemas	Recomendado
14.3 Datos de prueba	
Asegurar la protección de los datos utilizados para las pruebas.	
14.3.1 Protección de datos de prueba	Recomendado
15.1 Seguridad de la información en las relaciones con los proveedores	

Asegurar la protección de los activos de la organización que son accesibles por los proveedores.	
15.1.1 Política de seguridad de la información para las relaciones con proveedores	Obligatorio
15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores	Recomendado
15.1.3 Cadena de suministro de tecnología de información y comunicación	Recomendado
15.2 Gestión de la prestación de servicios con los proveedores	
Mantener un nivel acordado de seguridad de la información y entrega de servicios de acuerdo con los acuerdos con los proveedores	
15.2.1 Seguimiento y revisión de los servicios de los proveedores	Obligatorio
15.2.2 Gestión de cambios en los servicios de proveedores	Recomendado
16.1 Gestión de incidentes y mejoras de seguridad de la información	
Asegurar un enfoque consistente y efectivo para la gestión de los incidentes de seguridad de la información, incluyendo la comunicación sobre eventos y debilidades de seguridad.	
16.1.1 Responsabilidad y procedimientos	Recomendado
16.1.2 Reporte de eventos de seguridad de la información	Obligatorio
16.1.3 Reporte de debilidades de seguridad de la información	Obligatorio
16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Obligatorio
16.1.5 Respuesta a incidentes de seguridad de la información	Obligatorio
16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información	Recomendado
16.1.7 Recolección de evidencia	Recomendado
17.1 Continuidad de seguridad de la información	
La continuidad de la seguridad de la información debe integrarse en los sistemas de la gestión de la continuidad del negocio de la organización.	
17.1.1 Planificación de la continuidad de la seguridad de la información	Recomendado
17.1.2 Implementación de la continuidad de la seguridad de la información	Obligatorio
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Recomendado
17.2 Redundancias	
Asegurar la disponibilidad de las instalaciones de procesado de la información.	

17.2.1 Disponibilidad de instalaciones de procesamiento de información	Recomendado
18.1 Cumplimiento con los requisitos legales y contractuales	
Evitar incumplimientos de obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con cualquier requisito de seguridad.	
18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	Obligatorio
18.1.2 Derechos de propiedad intelectual	Recomendado
18.1.3 Protección de registros	Recomendado
18.1.4 Privacidad y protección de datos personales	Recomendado
18.1.5 Reglamentación de controles criptográficos	Recomendado
18.2 Revisiones de seguridad de la información	
Asegurar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización.	
18.2.1 Revisión independiente de la seguridad de la información	Obligatorio
18.2.2 Cumplimiento con las políticas y normas de seguridad	Obligatorio
18.2.3 Revisión del cumplimiento técnico	Obligatorio

Fuente. Elaboración propia basada en ISO27002

La anterior tabla representa el Framework producto de la investigación para las pymes educativas, teniendo presente que este tipo de organizaciones tienen dificultades similares para implementar una política de seguridad, en el mismo se han enumerado los controles obligatorios y recomendables para que cada una de ellas pueda hacer su apropiación del documento en el momento de hacer la implementación.

Cabe recordar que en la tabla 4 se explican los requisitos para aplicar el Framework, los cuales son: hacer gestión de riesgos, tener construido el documento de aplicabilidad y aplicar el Framework.

Conclusiones

Para las pymes educativas, las tecnologías digitales y la revolución 4.0 han transformado la manera en que prestan sus servicios. Sin embargo, esta revolución también ha generado preocupaciones en cuanto a la ciberseguridad, lo que hace ne-

cesario implementar estrategias de protección para contrarrestar los ciberataques a los que están expuestas. Esto ocurre debido a factores como la falta de presupuesto, desconocimiento, insuficiencia de infraestructura y, en general, la carencia de una estrategia para proteger la información.

La preocupación por los problemas de ciberseguridad expuestos en este documento ha llevado a diversas organizaciones a desarrollar y proponer buenas prácticas que minimicen el nivel de riesgo al que se enfrentan las pymes, como es el caso de las organizaciones españolas mencionadas en este trabajo.

Desde la perspectiva del trabajo realizado, se logró correlacionar las buenas prácticas propuestas por diversas entidades con el estándar ISO/IEC 27002, a partir del cual se seleccionaron los controles aplicables para que una pyme del sector educativo implemente una política de ciberseguridad.

El desarrollo del trabajo permitió identificar que, antes de aplicar el Framework propuesto, se debe realizar un análisis de riesgos y elaborar un Documento de Aplicabilidad (DdA), elementos esenciales sin los cuales no es recomendable iniciar una política de ciberseguridad.

Como trabajo futuro, se sugiere aplicar el Framework en una o varias pymes del sector educativo para validar la eficacia y facilidad de uso del instrumento propuesto.

Referencias

BMC & Forbes Insights. (2017). *Enterprise's re-engineer security in the age of digital transformation. CIOs and CISOs need a new security model to close today's security gaps and effectively wage cyber warfare*.

Centro de Comercio Internacional. (2018). *Ecosistemas empresariales para la era digital*. Ginebra, Suiza: Arancha González. Recuperado de http://www.intracen.org/uploadedFiles/intracenorg/Content/Publications/SMECO2018ExecutiveSummarySP.pdf

Ciglic, K. (2017). *Cybersecurity policy framework: A practical guide to the development of national cybersecurity policy* (1st ed.). Redmond, WA: Microsoft.

Contreras, J. (2018). Developing a framework to improve critical infrastructure cybersecurity (Response to NIST Request for Information Docket No. 130208119-3119-01).

SSRN Electronic Journal. https://doi.org/10.6028/NIST.CSWP.04162018

Dirección de Investigación e Interpol-Policía Nacional de Colombia. (2017). *Amenazas del cibercrimen en Colombia 2016-2017* (pp. 1-12). Bogotá: Policía Nacional de Colombia. Recuperado de https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Flórez, W., Arboleda, C., & Cadavid, J. (2012). Solución integral de seguridad de las pymes mediante un UTM. *Ing. USBMed, 3*(1). Recuperado de http://web.usbmed.edu.co/usbmed/fing/v3n1/v3n1a4.pdf

Hernández Gracia, J. (2018). Tipos de investigación. *Boletín Científico de la Escuela Superior de Atotonilco de Tula, 5*(9). https://doi.org/10.29057/esat.v5i9.2885

Kannan, P. K., & Li, H. (2017). Digital marketing: A framework, review, and research agenda. *International Journal of Research in Marketing, 34*(1), 22-45. https://doi.org/10.1016/j.ijresmar.2016.11.006

Machín, N., & Gazapo, M. (2016). La ciberseguridad como factor crítico en la seguridad de la Unión Europea. *Revista UNISCI, (42)*, 47-68.

Jazdi, N. (2014). Cyber-physical systems in the context of Industry 4.0. *2014 IEEE International Conference on Automation, Quality and Testing, Robotics*. https://doi.org/10.1109/aqtr.2014.6857843

Routledge. (2017). The WannaCry ransomware attack. *Strategic Comments, 23*(4), vii-ix. https://doi.org/10.1080/13567888.2017.1335101

Sabido-Domínguez, T., Alonso-Novelo, V., & Barredo-Baqueiro, G. (2018). Transformación e innovación en las organizaciones (TIO): El uso de las tecnologías de la información y comunicación en las pymes, como herramienta para crear ventajas competitivas. *RECI Revista Iberoamericana de las Ciencias Computacionales e Informática, 6*(12), 213. https://doi.org/10.23913/reci.v6i12.74

Santos Olmo Parra, A., Sánchez Crespo, L., Alvarez, E., Huerta, M., & Fernández Medina Paton, E. (2016). Methodology for dynamic analysis and risk management on ISO27001. *IEEE Latin America Transactions, 14*(6), 2897-2911. https://doi.org/10.1109/tla.2016.7555273