Artículo 8. Continuidad de negocio, análisis de la exposición al riesgo de ataques cibernéticos en empresas micro y pequeñas de la región Atlautla, Ozumba y Amecameca.

Business continuity, an analysis of risk exposure to cybernetic attacks on micro and small businesses in the region of Atlautla, Ozumba y Amecameca.

AUTORES
Angélica Ramos
Elizabeth Torres Ramos
Abigail Alonso Reyes
Laura Segundo Gil

Resumen

El estudio cuantitativo de diseño descriptivo-correlacional se realizó a partir de datos recolectados en la investigación anual 2020 de la Red de Estudios Latinoamericanos en Administración y Negocios (Relayn) de una muestra de 401 directivos de micro y pequeñas empresas de los municipios de Atlautla, Ozumba y Amecameca Estado México, con el objetivo de ponderar su exposición al riesgo de ataques cibernéticos medido a través de la relación entre la incorporación tecnológica y la implementación de software de seguridad informática con la intención de inferir su impacto en la continuidad de negocio. Se encontró una relación directa entre las variables de estudio, con r = 0.725.

Palabras clave
Ataques cibernéticos, continuidad de negocio, micro y pequeña empresa, riesgo, seguridad informática

Abstract

This quantitative research of descriptive-correlational design was performed with data recollected during the annual investigation of Latin American Studies Network in Business and Administration (Relayn) in 2020 from a sample consisting of 401 micro and small business directors from the municipality of Atlautla, Ozumba and Amecameca, Mexico State with the objective of weighing vulnerability of cybernetic attacks measured by the relationship between incorporation of technology and implementation of computer security software with the intention of inferring the impact it has on a businesses continuity. A direct relationship was found among study variables, with r = 0.725.

Keywords
Cybernetic attacks, business continuity, micro and small businesses, risk, computer security software.

Introducción

Los ataques cibernéticos y violación de datos, los cortes de tecnologías de la información y telecomunicaciones, ocupan el segundo y tercer lugar, respectivamente, del ranking de las principales amenazas identificadas por los especialistas en continuidad de negocio para el próximo año (Business Continuity Institute, 2021).

El 2020 fue un año que vino a recordar a las organizaciones la importancia de estar preparadas ante la ocurrencia de eventos inesperados que pueden representar interrupciones en sus operaciones y

afectar la continuidad de negocio, entendida como la capacidad que tiene una organización para conservar la operación de sus funciones principales durante y después de haber acontecido un desastre, tema que lleva décadas de ser abordado mediante diversas metodologías, pero que aún resulta poco familiar para empresas micro y pequeñas que, sin duda, no están exentas del impacto de acontecimientos imprevistos como desastres naturales, fallos internos, accidentes, ataques cibernéticos, interrupción de energía, desastres financieros e incluso crisis sanitarias que pondrían en riesgo la operación de la empresa y con ello la continuidad del negocio.

Ante los inminentes riesgos a los que está expuesta toda organización, han surgido diferentes enfoques para su tratamiento, partiendo de la teoría de la gestión integral del riesgo, que en la década de los noventa tomó especial relevancia, derivada de algunas catástrofes en instituciones financieras; posteriormente, fue dirigida hacia otros sectores, al tiempo que han surgido diversas propuestas metodológicas.

El *British Standard Institute* y la *International Organization for Standardization* han propuesto estándares para la implementación de un sistema para la gestión de la continuidad del negocio, el BS-25999-1 y BS-25999-2 *Sistema de Gestión de Continuidad del Negocio,* y la norma ISO 22301:2012 *Seguridad de la Sociedad – Sistema de Gestión de Continuidad del Negocio* (Lojan, 2017, párr. 1), respectivamente.

Ambos estándares implican el diseño de estrategias que se integran en el llamado Plan de Continuidad de negocio (BCP, por sus siglas en inglés), cuyo objetivo es "establecer las estrategias y procedimientos que deben ser implementados por un equipo interdisciplinario que provee el direccionamiento requerido, soporte, equipamiento, metodologías y estándares para garantizar la continuidad en las operaciones críticas" (Rodríguez, 2020, p. 1), abordando diferentes aspectos como evaluación,

comunicación de la crisis, respuesta inicial, recuperación y reanudación de las operaciones de la organización.

La continuidad del negocio es aquella capacidad estratégica y táctica que tiene la organización para anticiparse a cómo dará respuesta ante la posible ocurrencia de incidentes e interrupciones del negocio para continuar con las operaciones a un nivel definido previamente, lo cual implica la identificación de los factores de riesgo, la definición de estrategias y los planes para garantizar la operación de la empresa con el fin de proteger los intereses de las partes interesadas. La continuidad de negocios implica la gestión de incidentes y, por ende, la gestión de riesgos. Becerra et al. (2021) señalan que la continuidad de negocio "permite a las organizaciones identificar eventos potenciales que amenazan su normal funcionamiento y provee un marco para desarrollar la capacidad de recuperación y de responder ante estas situaciones de manera efectiva" (p. 4).

Los riesgos se producen tanto a causa de factores internos como externos, pueden ser de origen natural, de errores humanos o inherentes a la naturaleza de la actividad de la empresa. Mora (2018) destaca amenazas que representan riesgos de tipo tecnológico como "los ataques, virus, malware y pérdida de información" (p. 1). En la medida en que existe una mayor apropiación del uso de la tecnología por parte de las organizaciones, sin importar su tamaño, dichas amenazas se hacen más latentes. "[…] los ataques a los sistemas informáticos han aumentado, como consecuencia a los avances en los servicios y modelos de comunicaciones e información y el auge de las nuevas Tecnologías de la Información y la Comunicación, el uso continuo y generalizado a nivel global de la Internet […] [por ello] las organizaciones están expuestas día a día a amenazas tanto internas como externas que ocasionan robo de identidad e información, bases de datos, información sensible de clientes, pérdida de credibilidad y daños financieros que pueden afectar la sostenibilidad de la entidad" (Tejena-Macías, 2018, pp. 232-233).

En las pequeñas y medianas empresas (pymes) en México, se han identificado cuatro principales riesgos que amenazan su desarrollo, entre ellos destacan "los ciberdelitos, al ser víctimas del robo de información valiosa y ahorros, sin saber con certeza el motivo de la acción o incluso, las implicaciones comerciales debido a la vulnerabilidad de los datos" (*Expansión*, 2017, párr. 4).

Resulta pertinente ponderar la exposición al riesgo de ataques cibernéticos de las mypes de los municipios de Atlautla, Ozumba y Amecameca, medido a través de la relación entre la incorporación tecnológica y la implementación de software de seguridad informática para inferir su impacto en la continuidad de negocio, considerando que, en México, 98.8% del total de organizaciones son de tamaño micro y pequeño y que 99.5% de la unidades económicas de los municipios de estudio pertenece a la misma estratificación (INEGI, 2021).

Además, resulta un tema de interés actual debido a que a partir de la pandemia por COVID-19, las empresas han enfrentado un escenario crítico que las pone ante un elevado riesgo de continuidad de negocio y que, dadas las condiciones del confinamiento, se han visto obligadas a incursionar en el uso de las Tecnologías de la Información y la Comunicación (tic) como una estrategia de supervivencia, lo cual sin duda trae consigo exposición al riesgo de ser víctimas de delitos informáticos, así como de pérdida de información.

Revisión de la literatura

Desde la década de 1970, la administración de la continuidad de negocio (BCM, por sus siglas en inglés), señala Nieto (citado en Becerra et al. 2021), "ha evolucionado como una forma de gestión de crisis en respuesta a los riesgos técnicos y operativos que amenazan la recuperación de una organización frente a peligros e interrupciones". (p. 4). Uno de los primeros antecedentes es la obra Planificación de la

continuidad, escrito por Ronald Ginn, en el cual señala la importancia de desarrollar habilidades que permitan la recuperación de las organizaciones ante la posible presencia de desastres. En la década de 1990, el acontecer de algunas catástrofes en importantes empresas financieras revelaron la necesidad de implementar acciones para administrar los riesgos.

En 2003, la *British Standards Institution* (BSI) publicó el lineamiento PAS 56, el cual estableció a manera de guía los principios, terminología y el proceso para implementar un sistema de gestión de continuidad de negocio, recomendando un conjunto de buenas prácticas para anticiparse a posibles eventualidades. En 2006, la BSI divulgó el lineamiento BS 25999-1 con el objetivo de enmarcar un punto de referencia uniforme en las buenas prácticas de la gestión de continuidad de negocio (BCM, por sus siglas en inglés), que consideraba las necesidades de todas las partes interesadas. En 2007, el mismo instituto publicó el estándar BS 25999-2, orientado a la certificación y auditoría mediante un modelo para la gestión de continuidad del negocio que estuvo vigente hasta 2012.

En 2012, la *International Organization for Standardization* (ISO, por sus siglas en inglés) publicó la norma ISO 22301:2012 "*Seguridad de la Sociedad-Sistemas de gestión de la continuidad del negocio* – Requisitos, que "establece el código de un conjunto de buenas prácticas para la gestión de continuidad del negocio" (Lojan, 2017, párr. 1), dicho estándar enfatiza en el liderazgo de la alta dirección buscando que exista compatibilidad entre la gestión de continuidad del negocio y la dirección estratégica de éste, así como "la integración de los requerimientos de la norma en el plan de negocios y la comunicación de la importancia de una eficaz gestión de la continuidad del negocio " (Lojan, 2017, párr. 2).

Existe una amplia literatura sobre el tema de continuidad de negocio, la mayoría pone énfasis en los estándares para su gestión

mencionados con anterioridad. En el tema de continuidad de negocios por el riesgo de ataque cibernético en el ámbito internacional enfocado en pequeñas y medianas empresas, se encontró el estudio de Sampedro et al. (2019) denominado *Percepción de seguridad de la información en las pequeñas y medianas empresas en Santo Domingo*, con el objetivo de "identificar el conjunto de acciones preventivas y correctivas aplicadas en las pequeñas y medianas empresas (pymes) del Ecuador, provincia de Santo Domingo de los Tsáchilas" (p. 421). El estudio se realizó en una muestra de 96 unidades económicas, encontrando que "un alto porcentaje de pymes tiene establecidas acciones preventivas y correctivas, pero no las aplican, exponiendo su vulnerabilidad ante cualquier intento de alteración, pérdida o robo de información" (p. 422).

En el contexto nacional se encontró el trabajo de investigación de Ortiz, Palencia y Alvarado (2020), coincidente en el tema de la continuidad de negocio, no así en el enfoque de riesgos informáticos o riesgos de ataques cibernéticos, ya que el objetivo fue examinar si "existen diferencias en las intenciones de continuidad de los micronegocios encabezados por hombres y mujeres y cómo el sexo afecta al impacto de las características de los micronegocios en México sobre sus intenciones de permanencia en el mundo empresarial". El estudio se llevó a cabo con los resultados de Encuesta Nacional de Micronegocios 2012 del Instituto Nacional de Estadística y Geografía (Inegi), en donde se encontró que "el sexo del microempresario tiene un efecto moderador en las intenciones de continuidad del micronegocio" (p. 1).

Si bien se ha escrito mucho sobre el tema de continuidad de negocios, ciberataques, riesgo informático y seguridad informática, en la revisión de la literatura se aprecia la falta de estudios en el contexto nacional y local que aborden el tema de la presente investigación con un enfoque a micro y pequeñas empresas.

Metodología

El estudio es cuantitativo de diseño descriptivo-correlacional de corte transversal. Se utilizaron los datos recolectados en la investigación anual 2020 de la Relayn.

El objetivo de la investigación es ponderar la exposición al riesgo de ataques cibernéticos de las micro y pequeñas empresas de los municipios de Atlautla, Ozumba y Amecameca, medido a través de la relación entre la incorporación tecnológica y la implementación de software de seguridad informática para inferir su impacto en la continuidad de negocio.

Las preguntas de investigación son:

¿Las micro y pequeñas empresas de los municipios de Atlautla, Ozumba y Amecameca están expuestas al riesgo de ataques cibernéticos que afecten la continuidad de negocio?

¿Existe una relación directa entre la incorporación tecnológica y la implementación de software de seguridad informática por las micro y pequeñas empresas de los municipios de Atlautla, Ozumba y Amecameca?

H_0 . No hay relación directa entre la incorporación tecnológica y el uso de software de seguridad informática y hay alta exposición al riesgo de ataque cibernético.

H_i. Hay relación directa entre la incorporación tecnológica y el uso de software de seguridad informática y hay baja exposición al riesgo de ataque cibernético.

Variable independiente: incorporación tecnológica (IT)

Definición conceptual. Representa la implementación de nuevas tecnologías, uso de datos, maquinaria, dispositivos, software y sensores en actividades de administración y operación de la empresa; "dispositivos, herramientas, equipos y componentes electrónicos capaces de manipular información que soportan el desarrollo y crecimiento económico de cualquier organización" (Cano-Pita, 2018, p. 502).

Definición operacional. Se conformó una variable agrupada con el software PSPP a partir de cinco ítems en escala de Likert de 1 a 5 puntos, que sumados alcanzan valores de 5 (sin incorporación tecnológica) a 25 (con incorporación tecnológica). Los ítems fueron tomados de la sección Mype 4.0 del instrumento diseñado por Relayn para la investigación anual *Innovación y Mype 4.0 en la micro y pequeña empresa de Latinoamérica* (Posada, Peña & Aguilar, 2020).

Los ítems considerados para la agrupación de la variable "incorporación tecnológica" se enlistan a continuación:

44b. Computadora, tableta o algún dispositivo electrónico para administrar la empresa.

44c. Equipo o software especializado en el giro de la empresa.

44d. Página de internet o redes sociales para mostrar el catálogo de productos o servicios.

44e. Cobro automático por internet de algunas ventas.

44f. Dispositivos electrónicos para hacer cobros con tarjeta en el establecimiento.

Variable dependiente: software de seguridad informática (SSI)

Definición conceptual. Se refiere al uso de programas de aplicación especializados en "proteger la integridad y la privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos a los que está expuesta" (Baca, 2016, p. 12).

Definición operacional. Se utilizaron los datos del ítem 44i tomado de la sección Mype 4.0 del instrumento diseñado por Relayn para la investigación anual *Innovación y Mype 4.0 en la micro y pequeña empresa de Latinoamérica* (Posada, Peña & Aguilar, 2020), el cual se refiere a:

44i. Software especializado que brinde seguridad en terminales, portal de internet, puntos de venta, dispositivos móviles y sistemas administrativos.

Validación

La fiabilidad de la variable agrupada se comprobó mediante alfa de Cronbach (Tabla 8.1), en la cual se aprecia un nivel de consistencia interna alta, la cual se respalda con el análisis de las estadísticas del total de ítems (Tabla 8.2).

Tabla 8.1

Estadísticas de fiabilidad.

Alfa de Cronbach	N de elementos
0.91	5

En la Tabla 8.2 se muestra el análisis de los ítems y su impacto en el alfa de Cronbach al eliminar algún ítem, en donde se confirma el alto nivel de fiabilidad interna.

Tabla 8.2

Estadísticas de total de ítems.

Ítems	Correlación total-ítem corregida	Alfa de Cronbach si se borra el elemento
44 b. Computadora, tableta o algún dispositivo electrónico para administrar la empresa	0.7	0.9
44c. Equipo o software especializado en el giro de la empresa	0.77	0.88
44d. Página de internet o redes sociales para mostrar el catálogo de productos o servicio	0.79	0.88
44e. Cobro automático por internet de algunas ventas	0.8	0.88
44f. Dispositivos electrónicos para hacer cobros con tarjeta en el establecimiento	0.77	0.89

La población del estudio son empresas y organizaciones formales e informales de tamaño micro y pequeño que operan en los municipios de Atlautla, Ozumba y Amecameca, ubicados al oriente del Estado de México. Para efectos del presente estudio, se retoma la definición de micro y pequeña empresa de Posada, Aguilar y Peña (2016), entendiendo por mype "cualquier organización con fines de lucro que tiene al menos una persona trabajando para un patrón y que cuenta con un máximo de 50 trabajadores".

Entre las características económicas de la zona de estudio destaca la presencia de 6 929 unidades económicas, de las cuales 53% se dedica al

comercio, 36% pertenece al sector servicios y 10% a la industria. Respecto a la actividad comercial, 50% es al menudeo (INEGI, 2021), destacando principalmente tiendas de abarrotes y misceláneas, farmacias, papelerías, carnicerías, pollerías, verdulerías y recauderías, panaderías, tiendas de regalos, de ropa, muebles y artículos de limpieza y varios.

La muestra fue estratificada e integrada por 401 unidades económicas de los tres municipios; el instrumento fue aplicado por alumnos inscritos a los programas de licenciatura en Administración y gestión de pequeñas y medianas empresas, y licenciatura en Administración y gestión empresarial de la Universidad Politécnica de Atlautla.

La aplicación se realizó entre los meses de marzo a mayo de 2020, a directivos de empresas y organizaciones con las características señaladas; se entiende por directivo a "aquella persona que toma la mayoría de las decisiones en la organización" (Posada, Aguilar y Peña, 2016). La validación de los cuestionarios aplicados estuvo a cargo del grupo de investigación. Para el análisis de datos se utilizaron tablas de frecuencias y cálculo de correlación de Pearson.

Resultado

Análisis descriptivo

En el análisis de frecuencia de las variables de estudio (Tabla 8.3) se observa que 35.30% de los directivos encuestados sí ha incorporado el uso de nuevas tecnologías, uso de datos, maquinaria, dispositivos, software y sensores en actividades de administración y operación de la empresa, sin embargo, sólo 20.90% utiliza algún software especializado que brinde seguridad en terminales, portal de internet, puntos de venta, dispositivos móviles y sistemas administrativos, lo que indica que existe

una brecha entre dichas variables, dando lugar a la exposición al riesgo de ataques cibernéticos.

Otro aspecto a destacar es que 30.80% considera que no necesita la incorporación de tecnologías para la operación y administración de la empresa, mientras que 32.80% de los encuestados tampoco considera necesaria la implementación de software para la seguridad informática.

Tabla 8.3

Frecuencias de variables IT-SSI

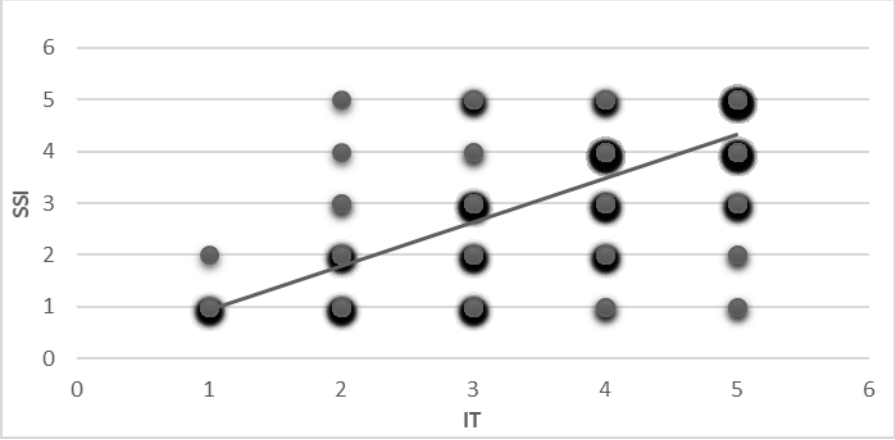
Escala	Incorporación tecnológica		Software de seguridad informática	
	Frecuencia	Porcentaje	Frecuencia	Porcentaje
No lo ha incorporado	17	4.20	58	14.40
No hay interés en incorporarlo	38	9.50	52	12.90
Podrá incorporarlo	80	19.90	75	18.70
No lo necesita	124	30.80	132	32.80
Lo ha incorporado	142	35.30	84	20.90

Análisis correlacional

En cuanto a la relación de las variables de estudio, el gráfico de dispersión (Figura 8.1) anticipa una relación positiva de baja a alta.

Figura 8.1

Diagrama de dispersión de variables.



El resultado encontrado, con cálculo del coeficiente de correlación, confirma la brecha entre dichas variables que se observó en el análisis de frecuencias.

Se obtuvo una correlación de Pearson de 0.725 a un nivel significancia de 0.05 (tabla 4), lo que significa que existe una relación directa alta entre la incorporación tecnológica y el uso de software de seguridad informática, lo cual permite ponderar que existe bajo grado de exposición al riesgo de ataques cibernéticos, ya que en la medida en que la relación de las variables sea 1 a 1, supondría que cada directivo que incorpora el uso de tecnologías de la información y las comunicaciones a la operación o administración de su empresa, estaría implementando también el uso de software especializado en seguridad informática, minimizando con ello su exposición al riesgo de ataques cibernéticos y menor riesgo de afectar la continuidad de negocio.

Tabla 8.4

Correlación de Pearson IT-SSI.

		Incorporación tecnológica	**Software de seguridad informática**
Incorporación t ecnológica	Correlación de Pearson	1	0.725(a)
	N	401	401
Software de seguridad informática	Correlación de Pearson	0.725(a)	1
	N	401	401

(a) Nivel de significancia 0.05

Discusión

Resulta importante señalar que existen diferentes metodologías para la medición del riesgo, en su mayoría, enfocadas a cumplir las normas y los estándares para la implementación de sistemas para la gestión de la continuidad del negocio, o bien, para la gestión del riesgo, en los cuales se parte de la identificación de los eventos de riesgo que afectan la seguridad informática y se evalúa su probabilidad de ocurrencia e impacto.

Cabe señalar que el estudio que aquí se presenta no retoma los lineamientos establecidos por los estándares mencionados, ya que utiliza el instrumento y los datos recolectados para la investigación anual 2020 de la Relayn; una medición que podría estar a discusión, pero que sin duda permea información interesante respecto al contexto de las mypes de la zona de estudio en términos de continuidad de negocio derivado de las amenazas por su incursión en el uso de las Tecnologías de la Información y de la Comunicación en actividades de administración y operación de las empresas, que puede ser el parteaguas para futuras investigaciones con diseños apegados a la normatividad existente.

En ese sentido, es importante mencionar que se identificó como una limitante la interpretación de la variable Software especializado para brindar seguridad que el director de la empresa pudo dar al momento de contestar el instrumento, ya que, por la naturaleza de éste, no hay un segundo o tercer ítem que robustezca la indagación en el tema de ciberataques, lo cual podría generar un sesgo en los resultados obtenidos.

Respecto a las conclusiones de otras investigaciones, se coincide con Sampedro et al. (2019) en torno a la importancia de emprender "acciones para concientizar a los directivos de las pymes sobre la necesidad de invertir en seguridad de la información y las acciones necesarias en función del tipo de empresa y actividad" (p. 422), así mismo, sobre el argumento de que "a medida que las pymes denotan un

crecimiento o implementan sistemas informáticos como estrategia competitiva quedan más expuestas a los ciberataques" (p. 428).

Conclusiones

Se rechaza la hipótesis nula de acuerdo con el resultado del coeficiente de correlación *r* de Pearson de 0.725, por tanto, se acepta la hipótesis alternativa indicando que hay una relación directa alta entre las variables incorporación tecnológica y uso de software de seguridad informática y hay baja exposición al riesgo de ataque cibernético, lo cual permite inferir que son bajas las amenazas en la continuidad de negocio derivadas de ataques, virus, malware y pérdida de información.

Si bien se alcanzó el objetivo de la investigación de ponderar la exposición al riesgo de ataques cibernéticos de las mypes de los municipios de Atlautla, Ozumba y Amecameca, medido a través de la relación entre la incorporación tecnológica y la implementación de software de seguridad informática para inferir su impacto en la continuidad de negocio, dando respuesta a las preguntas de investigación, es importante destacar que los datos fueron recopilados en un momento en el cual comenzaba el confinamiento por la pandemia de COVID-19, ante el cual las empresas han enfrentado un escenario crítico que las ha obligado a tener una mayor incursión en el uso de las tecnologías de la Información y de la Comunicación como una estrategia de supervivencia, lo cual, sin duda, habrá cambiado su exposición al riesgo de ser víctimas de delitos informáticos, así como la amenaza de continuidad de negocio, por lo que resultaría interesante no sólo realizar una nueva medición bajo el escenario actual, sino además generar propuestas de acciones que coadyuven a disminuir su exposición al riesgo y a incorporar prácticas para la gestión de la continuidad de negocio.

Asimismo, es pertinente fomentar la concientización sobre la importancia de contar con acciones dirigidas a gestionar el riesgo de exposición a ciberataques entre aquel porcentaje de directivos que ha incorporado las tecnologías en su empresa, pero que aún no cuenta con software, herramientas o planes que coadyuven a minimizar su exposición a dicho riesgo.

Referencias

Baca, G. (2016). *Introducción a la seguridad informática*. México: Patria.

Becerra, R., Benavides, J., Camacho, H. & Obando, C. (2021). Evolución y modelos de implementación de sistemas de gestión de continuidad del negocio. *Signos, Investigación en Sistemas de Gestión*, *13*(2). Recuperado de https://doi.org/10.15332/24631140.6669

Business Continuity Institute.+ (2021). *BCI Horizon Scan Report 2021* (pp. 40, 55). Recuperado de https://www.bsigroup.com/localfiles/en-gb/iso-22301/resources/bci-horizon-scan-report-2020.pdf

Cano-Pita, G. (2018). Las tics en las empresas: evolución de la tecnología y el cambio estructural en las organizaciones. *Revista Científica Dominio de las Ciencias*, *4*(1), 499-510. Recuperado de https://dialnet.unirioja.es/descarga/articulo/6313252.pdf

Expansión (2017, octubre 24). 4 puntos de riesgo más comunes en las Pymes. Recuperado de https://expansion.mx/bespoke-ad/2017/10/24/4-puntos-de-riesgo-mas-comunes-en-las-pymes

Instituto Nacional de Estadística y Geografía (Inegi) (2021). *Directorio Estadístico Nacional de Unidades Económicas (Denue).* Recuperado de https://www.inegi.org.mx/app/mapa/denue/default.aspx

Lojan, E. (2017). Modelo de evaluación de gestión de continuidad del negocio basado en la Norma ISO 22301. *Espacios, 38* (54), 16. Recuperado de https://www.revistaespacios.com/a17v38n54/a17v38n54p03.pdf

Mora, D. (2018). *Plan de continuidad de negocio como base del éxito organizacional* (pp. 1-8). Universidad Piloto de Colombia. Recuperado de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4635/00004908.pdf?sequence=1&isAllowed=y

Ortiz, J., Picazzo, E. & Alvarado, E. (2020). Diferencias entre hombres y mujeres en los determinantes de las intenciones de continuidad de los micronegocios en México. *Acta Universitaria*, *30*(2020), 1- 15. Recuperado de http://repositorio.ugto.mx/bitstream/20.500.12059/3253/1/Diferencias%20entre%20hombres%20y%20mujeres%20en%20los%20determinantes%20de%20las%20intenciones%20de%20continuidad%20de%20los%20micronegocios%20en%20M%C3%A9xico.pdf

Posada, R., Aguilar, O. C. & Peña, N. B. (2016). *Análisis sistémico de la micro y pequeña empresa en México.* México: Pearson Educación.

Posada, R., Peña, N. B., & Aguilar, O. C. (2020). Resultados generales del estudio de innovación e industria 4.0 en micro y pequeñas empresas de Latinoamérica. En Ó. C. Aguilar, N. B. Peña, R. Posada, A. Fernández, A. Reyes, J. C. Demesa & M. Á. Gómez (Eds.), *Innovación e industria 4.0 en las micro y pequeñas empresas en América Latina* (Tomo 1). Ciudad de México: McGraw-Hill.

Rodríguez, C. (2020). *La importancia de un plan de continuidad de negocio* Recuperado de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/9547/La%20importancia%20de%20un%20plan%20de.pdf?sequence=1&isAllowed=y

Sampedro, C. R., Machuca, S. A., Palma, D. P. & Carrera, F. A. (2019). Percepción de seguridad de la información en las pequeñas y medianas empresas en Santo Domingo. *Investigación Operacional*, *40*(3), 421- 428. Recuperado de http://www.invoperacional.uh.cu/index.php/InvOp/article/view/685

Tejena-Macías, M. (2018). Análisis de riesgos en seguridad de la información. *Polo del Conocimiento*, *3*(4), 230-244. Recuperado de https://www.isotools.org/2019/10/18/analisis-y-evaluacion-de-riesgos-de-seguridad-de-la-informacion-identificacion-de-amenazas-consecuencias-y-criticidad/