Universidad Nacional Abierta y a Distancia	**FORMATO** **RESUMEN ANALÍTICO EN EDUCACIÓN - RAE**

1. Información General	
Tipo de documento	Monografía
Acceso al documento	Trabajo monográfico para optar al título de Magister en Administración de organizaciones
Título del documento	Análisis Documental para la Creación de un Equipo de Respuestas a Incidentes Informáticos orientado a Pequeñas y Medianas Empresas del Sector Económico Colombiano
Autor(es)	Katherin Andrea Franco Suarez Luis Fernando Zambrano Hernández
Publicación	Año 2021
Palabras Claves	Brechas digitales, desarrollo de capacidades, negocio, protección de datos, tecnologías de la información

2. Descripción

Actualmente las Tecnologías de la Información y la Comunicación se han transformado en un sector transversal de todos los sistemas modernos. Según el diario El País, para el año 2018 en Colombia un 96% de empresas utiliza este medio para el desarrollo de sus actividades (País, 2018). La hipótesis de este estudio monográfico plantea que, si las organizaciones no se anticipan ante potenciales riesgos de ciberseguridad se verán afectadas en su infraestructura tecnológica, ocasionada por un evento o incidente informático, el cual genera pérdidas financieras y reputacionales, acciones legales y la afectación en la continuidad de su negocio.

En virtud de lo anterior, este documento se construye teniendo como referente una metodología de investigación cualitativa, planteada a través de cuatro capítulos incluyendo los objetivos propuestos: 1. El desarrollo metodológico; 2. El estado actual de la gestión de la ciberseguridad y de la protección de los datos en las PyMES colombianas; 3. un plan estratégico que contribuya al robustecimiento de las capacidades del aseguramiento digital; 4. una propuesta tecnológica para la gestión de un evento de ciberseguridad.

Lo antes citado conlleva a la viabilidad de la creación de un Equipo de Respuesta a Incidentes Informáticos – CSIRT, que brinde servicios estratégicos para la gestión de eventos de ciberseguridad a PyMES.

Este documento está dirigido a las PyMES del sector económico colombiano, Empresas del sector de la seguridad de la información, comunidades académicas y todas las partes interesadas que estén involucradas en la reducción de brechas digitales, aportando en el desarrollo de capacidades de Ciberseguridad, fortaleciendo la sostenibilidad y la continuidad del negocio.

3. Fuentes

- BID. (2017). Impacto de los incidentes de seguridad digital. Obtenido de https://publications.iadb.org/publications/spanish/document/Impacto-de-los-incidentes-de-seguridad-digital-en-Colombia-2017.pdf
- CCIT, & PONAL. (29 de Octubre de 2019). Tendencias Cibercrimen Colombia 2019 - 2020. Obtenido de https://www.ccit.org.co/wp-content/uploads/informe-tendencias-final.pdf
- ESET. (2018). Minería de criptomonedas: respuesta a tres de las preguntas más frecuentes.

Obtenido de Welivesecurity: https://www.welivesecurity.com/la-es/2018/06/22/mineria-criptomonedas-respuesta-tres-preguntas-frecuentes/

- Espino , & Martínez . (2017). *Análisis predictivo: técnicas y modelos utilizados y aplicaciones del mismo - herramientas Open Sourceque permiten su uso.* Obtenido de UOC: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/59565/6/caresptimTFG0117mem%C3%B2ria.pdf

- FBI. (11 de Febrero de 2020). *2019 Internet Crime Report Released.* Obtenido de https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120
- Fernández, S. (2002). *Investigación cuantitativa y cualitativa. .* Coruña España: Cad Aten primaria complejo Hospitalario Juan Canalejo.

- Fregoso, c. (17 de 03 de 2021). *INTERUS*. Obtenido de Estrategias de marketing digital: https://blog.interius.com.mx/quick-wins-para-empezar-automatizar-procesos-empresa

- Freyre, C. (11 de Marzo de 2019). *El papel de la ciberseguridad en las organizaciones*. Obtenido de Escuela Argentina de Negocios: http://www.ean.edu.ar/nota/299-el-papel-de-la-ciberseguridad-en-las-organizaciones

- GCA. (2020). *Global Cybersecurity Agenda (GCA).* Obtenido de https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx
- GORDON, & LOEB. (2002). *The economics of information security .* Obtenido de ACM: https://dl.acm.org/citation.cfm?id=581274

- INCIBE. (2020). *Plan Director de Seguridad.* Obtenido de Instituo Nacional de Ciberseguridad: https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad

- ISO. (2015). *GTC-ISO-IEC 27002:2015.* Obtenido de TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. CÓDIGO DE PRÁCTICA PARA CONTROLES DE SEGURIDAD DE LA INFORMACIÓN: https://ecollection-icontec-org.bibliotecavirtual.unad.edu.co/normavw.aspx?ID=308

- *Kaspersky Lab: las brechas de seguridad ocasionadas por terceros representan un costo mayor para las empresas*. (28 de 11 de 2017). Obtenido de https://latam.kaspersky.com/about/press-releases/2017_kaspersky-lab-security-breaches
- LACNIC. (2012). *Manual básico de: Gestión de Incidentes de Seguridad Informática.* Obtenido de https://csirt.lacnic.net/wp-content/themes/warpnew/docs/manual_basico_sp.pdf

- MDAP. (2016). *Excecutive Master Project Management.* Obtenido de https://uv-mdap.com/matriz-poder-influencia-interesados

- País, E. (18 de 01 de 2018). *Diario el País*. Obtenido de https://www.elpais.com.co/tecnologia/el-96-de-las-empresas-en-colombia-utilizan-internet.html

- PONEMON. (2019). *Exclusive Research Report 2019 Global State of cybersecurity iun small and medium-size businesses*. Obtenido de https://www.keeper.io/hubfs/2019%20Keeper%20Report_Final%20(1).pdf

Universidad Nacional Abierta y a Distancia	**FORMATO**
	RESUMEN ANALÍTICO EN EDUCACIÓN - RAE

4. Contenidos

El documento se construye teniendo presente la hipótesis: “Las organizaciones que no se anticipan ante potenciales riesgos de ciberseguridad, se verán afectadas en su infraestructura tecnológica ocasionada por un evento o incidente informático, el cual genera pérdidas financieras y reputacionales, acciones legales y la afectación en la continuidad del negocio”. Esta se comprueba a través del desarrollo de cuatro capítulos: Primero se aborda el desarrollo metodológico; Seguido a esto, se establece el estado actual de la gestión de la ciberseguridad y de la protección de los datos en las PyMES colombianas; En el tercer capítulo, se presenta un plan estratégico que contribuye al robustecimiento de las capacidades del aseguramiento digital; Y, finalmente se plantea una propuesta tecnológica para la gestión de un evento de ciberseguridad

1. Metodología

Teniendo presente la línea de investigación “Gestión de las Organizaciones” y a partir de la sub línea “Planeación de las Organizaciones” (ECACEN, 2017), este estudio monográfico se construye con el fin de contribuir al reconocimiento de mejores prácticas de gobierno de TI y el impacto que estas puedan aportar a la gestión del conocimiento de una organización. Por tal motivo, como soporte metodológico para analizar los factores políticos, económicos, sociales y tecnológicos para la Creación de un Equipo de Respuestas a Incidentes Informáticos orientado a Pymes colombianas, se plantea la aplicación de la investigación Cualitativa. En relación con ello en el año de 1996 Taylor & Bogdan, indicaban que esta permite aplicar un conjunto de técnicas para recoger datos donde todos los escenarios son dignos de estudio y todos los puntos de vista son importantes. Es preciso también mencionar lo expuesto en el año 2002 por Fernández, quien platea que la investigación cualitativa intenta identificar la naturaleza profunda de una realidad, las relaciones que pueden existir y la estructura dinámica que pueda presentar.

Es así como la recopilación de información a partir de boletines generados por organizaciones que estudian la ciberseguridad, estándares y normativas planteadas por entes certificadores y estados, documentos emanados de la academia y el juicio de expertos , permite establecer un panorama que determine: el estado actual de la gestión de la seguridad en organizaciones, plantear un plan estratégico que contribuya en el robustecimiento de las capacidades de la seguridad de la información y de la protección de datos de una PyME y esquematizar un propuesta tecnológica que sirva como base para la gestión de un evento de ciberseguridad. Esto con el fin de plantear la creación de un Equipo de Respuestas a Incidentes Informáticos para el Sector de las Pequeñas y Medianas empresas del país.

2. Conclusiones

La hipótesis señalada “Las organizaciones que no se anticipan ante potenciales riesgos de ciberseguridad se ven afectadas en su infraestructura tecnológica ocasionada por un evento o incidente informático, el cual genera pérdidas financieras y reputacionales, acciones legales y la afectación en la continuidad del negocio.”, se comprueba teniendo presente lo expuesto en el capítulo uno, ya que a partir de la fundamentación teórica planteada en los marcos y el desarrollo del capítulo dos, se puede evidenciar que las pérdidas económicas debido a ataques informáticos para el año 2019 oscilaba entre 300 y 5000 millones de pesos, indicando además que la baja capacidad en recursos como talento humano capacitado y la poca inversión en ciberseguridad que las PyMES asignan en sus presupuestos es una realidad. Esto sin duda alguna afecta la continuidad del negocio ocasionando pérdidas económicas y reputacionales.

El capítulo tres, se establece un plan estratégico que contribuye en el robustecimiento de las capacidades

de ciberseguridad, que aporta a la continuidad de negocio a partir del diseño de un Plan Director de Seguridad y que se integra con una metodología para el desarrollo de proyectos como la ISO 21500. En este plan, se brindan lineamientos claros para que una organización o para que un equipo de respuestas a incidentes informáticos, cuenten con un talento humano capacitado con unos procesos definidos para la gestión de la información y la protección de los datos y con el uso de tecnologías que permitan mejorar el aseguramiento de sus entornos digitales.

Así mismo, este capítulo, soporta la necesidad de consolidar un equipo de respuestas a incidentes informáticos que brinde servicios a PyMES, teniendo presente lo planteado en la matriz de análisis de factores políticos, sociales, económicos y tecnológicos, evidenciando en esta, la necesidad de ampliar un modelo de negocio en la línea de la ciberseguridad, que impacte a las pequeñas y medianas empresas a partir del despliegue de servicios acorde a sus presupuestos y necesidades, que acompañen a este sector de la economía en el cumplimiento de la legislación y normatividad y que fortalezca como servicio externo sus infraestructuras tecnológicas con el ánimo de mejorar el estado de la ciberseguridad.

El capítulo 4, esquematiza una propuesta que sirva como infraestructura tecnológica y física para el despliegue de los servicios de un CSIRT de PyMES. Esta infraestructura se proyecta teniendo presente: Uno: Recursos mínimos locativos que permitan tener un espacio físico para la prestación de sus servicios. DOS: Recursos mínimos de hardware los cuales pueden ser considerados en un presupuesto a un costo bajo en su adquisición. TRES: El uso de herramientas de software libre lo cual termina siendo el valor agregado en términos de inversión. Es por esto por lo que un Equipo de respuestas orientado a PyMES no solo se implementa con el fin de dar cumplimiento a las exigencias normativas que se imponen en torno a la seguridad digital, sino que permite abarcar estratégicamente las necesidades de una Pequeña y Mediana Empresa con el fin de contribuir en la mejora de prácticas de gobierno de TI, generando impacto en la competitividad de la organización y en su entorno digital.

Elaborado por:	Katherin Andrea Franco Suarez Luis Fernando Zambrano Hernández

Fecha de elaboración del Resumen:	11	10	2021