Estructura del documento para la estructura del Resumen Analítica Especializado -RAE

Tamaño de letra: 12

Tipo de letra: Arial

Interlineado: Sencillo

Borrar letra de color gris*

Fecha de Realización:	11/06/2023
Programa:	Especialización en Seguridad Informática
Línea de Investigación:	Infraestructura tecnológica y seguridad de redes
Título:	ANALIZAR LAS POLÍTICAS Y LOS CONTROLES BÁSICOS DE SEGURIDAD DE LA INFORMACIÓN EN FUNCIÓN DE LAS NUEVAS NECESIDADES QUE TIENEN LAS PYMES DEL SECTOR COMERCIAL EN TIEMPOS COVID-19
Autor(es):	Rodriguez Arteaga Gabriel Felipe
Palabras Claves:	Ciberseguridad, COVID-19, PYMES, Resiliencia, Seguridad, Vulnerabilidad.
Descripción:	La siguiente monografía consiste en la revisión de diferentes estudios y/o documentos acerca del manejo de la ciberseguridad en tiempos de COVID para el sector PYME La condición actual del COVID-19 donde obligo a las pequeñas y medianas empresas a resurgir o a cambiar su modo de operación más apoyado en las tecnologías de información, claramente el factor de seguridad informática juega un papel fundamental en la cual es nuevo para muchas organizaciones y es de vital importancia que contextualicen y robustezcan el ámbito de la seguridad informática y a su vez integrado dentro de sus estrategias organizacionales. Ya se ha visto en los primeros meses de la Covid-19. “Los delincuentes no han dejado pasar la oportunidad y muchos de los incidentes que se vienen observando desde el inicio de la pandemia están relacionados directamente con una mala implementación de las políticas de seguridad y de una configuración incorrecta de los accesos remotos o los permisos de los usuarios en una red corporativa” La implementación de políticas y controles fundamentadas en las buena prácticas y estándares como la ISO 27001 y la ISO 27002 son

	estrategias claves para que las PYMES se mantenga en pie y existentes, para un futuro que claramente es una nueva realidad que hace dos años no pensábamos que fuera de esta forma.

Fuentes bibliográficas destacadas:

- Albors, J.: "Tendencias 2021: ¿qué nos depara un futuro in-cierto en materia de ciberseguridad?" https://blogs.protegerse.com/2020/12/04/tenden-cias-2021-que-nos-depara-un-futuro-incierto-en-mate-ria-de-ciberseguridad. Diciembre.
- ALLUE, Marta; DELGADO, Boris; FERNÁNDEZ, Carlos Manuel. Privacidad de la información: clave en la transformación digital de la era COVID-19. AENOR: Revista de la normalización y la certificación, 2020, no 362, p. 5-8.
- Busselen, M.(2020): "Por qué el ciberdelito sigue siendo un desafío empresarial preocupante en un mundo blo-queado por COVID". www.crowds-trike.com/blog/why-cybercrime-remains-a-worrying-business-challenge-in-a-covid-lockdown-world. Sep-tiembre.
- CARPENTIER, Jean-François. *La seguridad informática en la PYME: Situación actual y mejores prácticas*. Ediciones ENI, 2016.https://www.enter.co/empresas/la-alternancia-creara-mas-vulnerabilidades-en-los-dispositivos/
- CASTELLANOS VEGA, Carlos Jacinto, et al. Modalidades de cibercrimen en tiempos de Pandemia Covid-19 en Bogotá (Colombia).
- Deloitte (2020): "El estado de la ciberseguridad en España: Digitalización, teletrabajo y ciberataques en tiempos de pandemia". www2.deloitte.com/es/es/pages/risk/arti-cles/estado-ciberseguridad.html
- LEMA, Luis López. La gestión de la información durante etapas de teletrabajo en la época de la COVID-19. Perspectivas, n. 3, 2020.
- MONTOYA CORREA, Tatiana; MOLANO LUJÁN, Andrés. Diseño de un esquema de seguridad informática para PYMES, como la primera línea de defensa para la protección contra amenazas de Ransomware, utilizando los lineamientos de la norma ISO27001: 2013. 2018
- RATTI BITTINGER, Gabriela María. Desarrollo de una guía de controles de ciberseguridad para la protección integral de la PYME. 2017.
- RISS, Boris Delgado; SÁNCHEZ, Carlos Manuel Fernández. Las mejores prácticas ISO contra el Covid-19 y crisis futuras. Revista SIC: ciberseguridad, seguridad de la información y privacidad, 2020, vol. 29, no 140, p. 94-96.
- Vera, J. M. (2021). Ciberseguridad post-Covid : ¿Qué papel jugará la ciberinteligencia frente a los cisnes negros digitales que llegarán tras la vacuna? Journal of Economic & Business Intelligence. 3, 11–23.

Contenido del documento:	El documento consta de 8 partes, donde la primera parte corresponde a la definición del problema, la segunda parte a la justificación, la tercera parte a la definición de los objetivos tanto general como específicos, la cuarta parte a los marcos de referencia que tienen alcance a la revisión documental del monografía, la quinta parte corresponde al desarrollo de los objetivos en función a la problemática identificada, la sexta parte a las conclusiones, la séptima parte a las recomendaciones generales y la octava parte a la bibliografía de la monografía.
Marco Metodológico:	Revisión documental de diferentes estudios en cuanto a las estrategias durante la pandemia COVID-19 en temas de ciberseguridad y seguridad de la información aplicadas a las PYMES.
Conceptos adquiridos :	Después de las revisiones documentales se identifica la importancia que tienen la ISO 27001 y 27002 para la implementación tanto de políticas y controles de ciberseguridad y seguridad de la información para cualquier tipo de organización, contextualizando los pilares fundamentales y básicos para la implementación de un SGSI, también se identificaron las principales amenazas y vulnerabilidades que existen en la actualidad tanto en el ciberespacio como en las actuales infraestructuras tecnológicas. La implementación de Políticas y controles claves para mitigar riesgos inherentes tan básicos donde muchos de ellos se encuentran por defecto en las PYMES.
Conclusiones:	Políticas como la administración y gestión de perfiles, política gestión de acceso y de privilegios, políticas en cuanto a los requerimientos mínimos como un antivirus actualizado, una conexión segura sobre internet (VPN) permiten definir lineamientos de cumplimiento obligatorio en las PYMES conllevando a la implementación y ejecución de una barrera por defecto básica para asegurar los principales activos tecnológicos de la organización en un escenario de COVID-19 y posterior a las nuevas necesidades de la resiliencia. La revisión documental nos permite identificar las bases en cuanto a políticas, procedimientos y controles las cuales fueron determinadas por el uso

	común y repetitivo en las diferentes revisiones las cuales permitieron determinar los aspectos mínimos que se deben aplicar y que deben considerar a las PYMES del sector comercial en Colombia, controles y procedimientos tan básicos como la implementación de VPN para el trabajo remoto, el cifrado de información en la transmisión de correos electrónicos, la implementación de un antivirus, la implantación de políticas de seguridad, entre otros son las claves para un mínimo de defensa que deben tener considerar las PYMES del sector comercial, siendo este uno de los más afectados durante la Pandemia del COVID-19, su modelo de negocio era uno de los que más estaban lejos de las automatizaciones y de la tecnología 2.0 y fueron obligado a transformarse de una manera muy rápida para la continuidad de sus operaciones donde su costo de impacto negativo fue demasiado alto porque no consideraron las barreras de seguridad mínimas que deberían haberse implementado una vez iniciara la pandemia.