BUENAS PRÁCTICAS DE SEGURIDAD INFORMÁTICA APLICADO AL COMERCIO ELECTRÓNICO PARA LAS PYMES COLOMBIANAS ASOCIADA A LA NORMA ISO 27001:2013 ANEXO A

YENNYFER PAOLA LEAL RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2021

BUENAS PRÁCTICAS DE SEGURIDAD INFORMÁTICA APLICADO AL COMERCIO ELECTRÓNICO PARA LAS PYMES COLOMBIANAS ASOCIADA A LA NORMA ISO 27001:2013 ANEXO A

YENNYFER PAOLA LEAL RODRIGUEZ

Monografía presentada para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Yenny Stella Nuñez Álvarez
Directora

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2021

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Primeramente, dedico esta monografía a Dios quien me ha dado la sabiduría, su ayuda y conocimientos para la realización de la misma, los tutores que me han ayudado incondicionalmente para poder finalizar con éxito la presente monografía, también a mis padres quienes siempre me han apoyado en el avance de mi carrera con su paciencia, amor y motivación en todos los aspectos de mi vida.

AGRADECIMIENTOS

Agradezco a Dios por la oportunidad de estudiar y todas las habilidades que me proporciona para seguir adelante cada día, también a cada uno de los tutores y directivos de la Universidad Nacional Abierta y a Distancia UNAD quienes me han apoyado constantemente en el desarrollo y finalización de este trabajo, sin este apoyo no hubiera sido posible su culminación y presentación.

TABLA DE CONTENIDO

pág.

INTRODUCCIÓN *14*
1. DEFINICIÓN DEL PROBLEMA *15*
1.1 ANTECEDENTES DEL PROBLEMA 15
1.2 FORMULACIÓN DEL PROBLEMA 15
2 JUSTIFICACIÓN *16*
3 OBJETIVOS *17*
3.1 OBJETIVO GENERAL 17
3.2 OBJETIVOS ESPECÍFICOS 17
4 MARCO REFERENCIAL *18*
4.1 MARCO TEÓRICO 18
4.2 ANTECEDENTES O ESTADO ACTUAL 25
5 Beneficios asociados al comercio electrónico en las pymes colombianas, a partir de la literatura *28*
5.1 Tendencias del comercio electrónico durante la crisis mundial del COVID-19 28
5.2 Beneficios del comercio electrónico para las pymes colombianas 31
5.2.1 Inclusión en estrategias y proyectos del gobierno colombiano 31
5.2.2 Uso estratégico de redes sociales y aplicaciones 32
5.2.3 Uso de medios de pago electrónicos 33
5.2.4 Otros beneficios: 35
6 Riesgos relacionados con el comercio electrónico, asociados hacia las pymes colombianas. *37*
6.1 Estado de la ciberseguridad en las pymes colombianas 37
6.2 Riesgos relacionados con el comercio electrónico, asociados hacia las pymes colombianas 40
6.2.1 Desventajas del comercio electrónico 41
6.3 Realización de un análisis de Riesgos en una pyme 42
6.3.1 Elija una metodología de análisis de riesgos más adecuada para su pyme: 42
6.3.2 Defina el alcance de su análisis de riesgos: 47
6.3.3 Realice un inventario detallado de activos de acuerdo con su metodología y alcance definidos anteriormente con su valoración: 47
6.3.4 Realice el análisis de amenazas de sus activos con su respectivo impacto: 52

6.3.5 Realice la evaluación y aplicaciones de salvaguardas o controles:.....58

7 Normatividad de seguridad informática que se debe conocer en el comercio electrónico aplicado a las pymes colombianas.....58

- Ley 527 de 1999.....58
- Ley 1266 de 2008:.....59
- Decreto 1377 de 2013: 60
- Ley 1273 de 2009.....61
- Ley 1480 de 2011.....61
- Ley 1581 de 2012.....62
- Documento CONPES 4012 62
- Instrumento de evaluación MSPI.....63

8 Guía de buenas prácticas de seguridad informática en el comercio electrónico para las pymes colombianas. 63

8.1 “A.10 Criptografía, A.10.1 Controles criptográficos, A.10.1.1 Política sobre el uso de controles criptográficos, A.10.1.2 Gestión de llaves” 63
Debe crear e implementar una política sobre la aplicación de controles criptográficos en su organización:.....64
Implementar una adecuada gestión de llaves criptográficas:.....64

8.2 “A.12. Seguridad en la Operativa, A.12.2 Protección contra código malicioso, A.12.2.1 Controles contra el código malicioso” 65
8.2.1 Implemente controles para detectar, retirar y evitar códigos maliciosos: 65
8.2.2 Implemente una solución de correo electrónico que le permita configurar una adecuada seguridad en el uso de éste: 66
8.2.3 Realice jornadas de capacitación y sensibilización de los usuarios en su organización:.....67

8.3 “12.3 Copias de seguridad, 12.3.1 Copias de seguridad de la información”....69
8.3.1 Realizar políticas y procedimientos para la realización de backup y pruebas de restauración de estos:.....69
8.3.2 Implementar soluciones que permitan la realización de backup de software, bases de datos y todos los datos para recuperarse ante un desastre o ataque: 70
8.3.3 Elegir los medios para almacenar las copias de seguridad y sus condiciones de almacenamiento:.....71

CONCLUSIONES.....72

9 RECOMENDACIONES 73

10 BIBLIOGRAFÍA 75

LISTA DE TABLAS

pág.

Tabla 1: Ventajas y desventajas metodologías gestión del riesgo. 43
Tabla 2: Activos identificados en una pyme. 48
Tabla 3: Valoración del impacto en una pyme..... 50
Tabla 4: Valoración del impacto por dimensión en una pyme. 50
Tabla 5: Valoración de la probabilidad de riesgo en una pyme. 53
Tabla 6: Valoración del riesgo de activos 53
Tabla 7: Amenazas y vulnerabilidades de los activos 54

LISTA DE FIGURAS

Figura 1: Clasificación de los incidentes de seguridad.---------- 26
Figura 2: Transacciones de comercio electrónico primer semestre de 2019 y 2020 en Colombia ---------- 30
Figura 3: Plataformas de redes sociales más usadas en Colombia---------- 33
Figura 4: Mapa de amenazas en línea de Fortinet---------- 38

GLOSARIO

Activo: Se entiende como todo aquello que tiene valor para una organización, específicamente en seguridad todo lo que contiene datos. El glosario de la familia de normas ISO 27000 define “En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.”[1]

Comercio electrónico: “Es el uso de las tecnologías computacional y de telecomunicaciones que se realiza entre empresas o bien entre vendedores y compradores, para apoyar el comercio de bienes y servicios”[2]

Confidencialidad: Postigo [3] explica que solo los usuarios autorizados conocen la información lo cual evita el acceso no autorizado. El glosario de la familia de normas ISO 27000 define “Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.”

Disponibilidad: Carpentier [4] explica que este es un principio que debe permitir que las personas autorizadas puedan acceder a la información siempre que lo requieran. El glosario de la familia de normas ISO 27000 define “Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.”

Integridad: Aguilera [5] Este principio garantiza la autenticidad y precisión de la información sin importar el momento en que se solicita. Los datos no deben ser

[1] Glosario normas ISO/IEC 27000.[en línea] (2013). Consultado: 15 de noviembre de 2020.Disponible en: https://www.iso27000.es/glosario.html
[2] Halchmi, Z., Hommel, K., y Avital., O., 1996. "Electronic Commerce", The Technion-Israel Institute of Technology.
[3] POSTIGO PALACIOS, A., [en línea] 2020. Seguridad Informática. Ediciones Paraninfo, S.A
[4] Carpentier, J., 2016. La Seguridad Informática En La PYME: Situación Actual Y Mejores Prácticas. Barcelona: ENI-Ediciones.
[5] Aguilera, P., [en línea] n.d. Seguridad Informática. Madrid: Editex.

modificados o alterados sin autorización. El glosario de la familia de normas ISO 27000 define “Propiedad de la información relativa a su exactitud y completitud.”

Norma ISO 27002: Según Pandini [6] Es una norma internacional que establece una recopilación de las mejores prácticas que se pueden aplicar a través de controles para apoyar la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en las organizaciones.

Pyme: En Colombia las organizaciones se dividen en micro, pequeñas, medianas y grandes empresas. **“**El término pyme hace referencia al grupo de empresas pequeñas y medianas con activos totales superiores a 500 SMMLV y hasta 30.000 SMMLV *.”[7]

Riesgo: El glosario de la familia de normas ISO 27000 define “El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.” [8]

Seguridad informática: “Es un método que involucra todo lo que pueda contener información”[9]. Es decir, se puede incluir elementos informáticos físicos y lógicos, organizacionales, de recursos humanos, medioambientales, etc. El glosario de la familia de normas ISO 27000 define la seguridad de la información como “Preservación de la confidencialidad, integridad y disponibilidad de la información. Adicionalmente, otras propiedades como la autenticidad, la responsabilidad, el no repudio y la confiabilidad también pueden estar involucradas.”.

---

[6] Pandini, W. [en línea] (2019). ISO27002: Buenas prácticas para gestión de la seguridad de la información. Disponible en: https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi#:~:text=En%20este%20grupo%20se%20encuentra,(SGSI)%20en%20las%20organizaciones.|

[7] Bancoldex. ¿Que es una pyme?[en linea]. Bogotá.(30 de julio de 2018) [Consultado: 13 de noviembre de 2020]. Disponible en: https://www.bancoldex.com/que-es-una-pyme-1338

[8] Glosario normas ISO/IEC 27000.[en línea] (2013). Consultado: 15 de noviembre de 2020.Disponible en: https://www.iso27000.es/glosario.html

[9] Romero Castro, M., Figueroa Morán, G., Vera Navarrete, D., Álava Cruzatty, J., Parrales Anzúles, G., Álava Mero, C., Murillo Quimiz, Á. and Castillo Merino, M., 2018. INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES. 1st ed. Alicante: 3ciencias, pp.13-20.

RESUMEN

Mediante la presente monografía se expondrá las buenas prácticas de seguridad informática que las pymes colombianas deben tener en cuenta para tener un comercio electrónico seguro y confiable. Para dar cumplimiento a este objetivo se explicará la importancia de que las pymes colombianas implementen mejoras de seguridad informática en su infraestructura tecnológica involucrada en el comercio electrónico de su organización, tecnología y necesidad que cada vez es más demandada en el mercado colombiano. También se expondrá un análisis de los conceptos, sistemas de pago online, beneficios y riesgos relacionados con el comercio electrónico para que las pymes lo tengan en cuenta como una parte introductoria que dará claridad sobre el tema expuesto. Adicionalmente se recomendará la aplicación de normatividad de seguridad informática en el comercio electrónico para que las pymes estén alineadas bajo normatividad estricta y confiable en términos de seguridad para la organización, sus clientes y aliados. Finalmente se harán las recomendaciones correspondientes a las buenas prácticas que se deben aplicar en una organización para tener un comercio electrónico seguro y confiable.

ABSTRACT

This monograph will expose the good computer security practices that Colombian SMEs must consider to have a safe and reliable electronic commerce. To fulfill this objective,
It will explain the importance for Colombian SMEs to implement computer security improvements in their technological infrastructure involved in the electronic commerce of their organization, technology and need that is increasingly in demand in the Colombian market. An analysis of the concepts, online payment systems, benefits and risks related to electronic commerce will also be presented so that SMEs take it into account as an introductory part that will give clarity on the exposed subject. Additionally, the application of computer security regulations in electronic commerce will be recommended so that SMEs are aligned under strict and reliable regulations in terms of security for the organization, its clients and allies. Finally, the recommendations corresponding to the good practices that should be applied in an organization to have a safe and reliable electronic commerce will be made.

INTRODUCCIÓN

La información es considerada uno de los activos más relevantes en las organizaciones y es por esto, que se deben proteger con el fin de optimizar las operaciones en los momentos donde se puedan presentar problemas informáticos y tener el control sobre esto. Reconocer la importancia de la aplicación de buenas prácticas de seguridad informática en las pymes colombianas son de vital importancia para la supervivencia, reputación y protección de la información de estas. Es el mecanismo más eficaz que cualquier empresa debe utilizar para proteger su información, puesto que ayuda a establecer políticas, procedimientos y controles, con el fin de tener bajo control el riesgo inherente para las organizaciones al manejar cualquier tipo de información.

El aumento de la demanda en el uso del internet, redes sociales, páginas de internet para realizar todo tipo de transacciones ha introducido la necesidad de aplicar el comercio electrónico en las pymes colombianas para darse a conocer, aumentar las ventas, comercialización e internacionalización de sus productos.

Por tales razones en el presente documento monográfico se va a explicar las razones por las que es primordial para la supervivencia de una compañía la aplicación de buenas prácticas de seguridad informática en el comercio electrónico, analizando conceptos, beneficios y riesgos de este, normatividad y recomendaciones de buenas prácticas para que pueda ser implementada en las organizaciones que no cuentan con recursos para consultar esta información anteriormente mencionada.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Cada día surgen nuevas tecnologías y así mismo aumenta la demanda del uso de ellas en el mercado, a su vez también surgen técnicas de ataques de seguridad informática físicos y lógicos que amenazan la seguridad de las organizaciones. Los avances tecnológicos ciertamente facilitan la vida de las personas y compañías en el planeta, pero a su vez representan un riesgo alto de ser víctima de delitos informáticos si no se aplican buenas prácticas de seguridad informática que permitan que la organización esté preparada para defenderse frente a estos ataques.

Según Certicámara[10] los países Latinoamericanos más afectados en cuanto a delitos informáticos son Brasil, México y Perú, sin embargo, Colombia es el país más afectado por ataques de Ransomware con un 72%, siendo esto una cifra alarmante. Sugiere que las empresas deben invertir en seguridad digital de su información como un factor fundamental. Por otra parte, según la revista Dinero[11] se ha evidenciado que el 98% de pequeñas y medianas empresas en Colombia no hacen inversiones tecnológicas significativas en TIC, destacando como sus principales limitaciones de inversión la falta de conciencia sobre el impacto positivo de las TIC en la organización, falta de recursos necesarios para invertir en software y hardware, capacitación de sus empleados, entre otros factores que los hacen más vulnerables frente a delitos de seguridad informática.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cuáles son las buenas prácticas que las pymes colombianas deben tener en cuenta para mejorar la seguridad informática en el comercio electrónico?

---

[10] Certicámara S.A. Así va la Ciberseguridad y su transformación en Latinoamérica. [en línea]. Bogotá (2019). [Consultado: 13 de noviembre de 2020] Disponible en: https://blogs.portafolio.co/seguridad-informatica-certicamara-sa/asi-va-la-ciberseguridad-transformacion-latinoamerica/

[11] Revista Dinero. pymes: ausentes de tecnología. [en línea]. (2007). [Consultado: 20 de noviembre de 2020]. Disponible en:https://www.dinero.com/negocios/articulo/pymes-ausentes-tecnologia/46830

2 JUSTIFICACIÓN

Actualmente el activo más importante para cualquier tipo de organización es la información y el manejo que se le dé a la misma será clave para mantener el funcionamiento, reputación y buena relación entre socios. Según Noticias Curazao[12] informa que estudios realizados en la Universidad Nacional de Ingeniería en Perú revela que las compañías que no invierten en tecnología están cerrando y desapareciendo definitivamente, es imprescindible que las compañías adopten nuevas tecnologías para poder competir y sobrevivir en el mercado. Entre estas está el comercio electrónico como herramienta fundamental que una pyme necesita implementar para darse a conocer y vender sus productos electrónicamente. Según PWC Chile [13] las compañías al ser víctimas de delitos informáticos dan mayor importancia a la seguridad informática. A nivel general las compañías presentan fondos presupuestales de operación insuficientes, falta de liderazgo, estrategia y escasez de empleados calificados para enfocarse en la seguridad informática de las compañías. Por tales razones es indispensable que las pymes colombianas aumenten su inversión en TIC, no esperar a ser víctimas de delitos informáticos para posteriormente invertir, al contrario, debe ser un incentivo para prepararse especialmente en la aplicación de buenas prácticas de seguridad informática. Estas buenas prácticas se expondrán en la presente monografía basados en un análisis general del comercio electrónico, su normatividad y las recomendaciones correspondientes, donde se brinda una base para que una organización como lo son las pymes colombianas, que cuentan con escasos recursos económicos para invertir en esta asesoría, puedan guiarse de cómo mejorar su seguridad informática en el comercio electrónico y así buscar la preservación de los principios de la información tales como la confidencialidad, integridad y disponibilidad.

[12] LAS EMPRESAS QUE NO INVIERTEN EN TECNOLOGÍA DESAPARECERÁN EN 2020. [en línea]. (2019) [Consultado: 20 de noviembre de 2020]. Disponible en: https://noticiascurazao.com/las-empresas-que-no-invierten-en-tecnologia-desapareceran-en-2020/

[13] Mondaca, C. Seguridad de la Información: ¿invierten las empresas en TI?. [en línea]. (2020). [Consultado: 20 de noviembre de 2020]. Disponible en: https://www.pwc.com/cl/es/prensa/columnas-de-opinion/seguridad-de-la-información-invierten-las-empresas-en-ti.html

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Elaborar un documento de buenas prácticas de seguridad informática en el comercio electrónico para las pymes colombianas asociada a la norma ISO 27001:2013 Anexo A, debido a su vulnerabilidad y deficiencia dentro de sus sistemas informáticos.

3.2 OBJETIVOS ESPECÍFICOS

1. Explicar los beneficios asociados al comercio electrónico en las pymes colombianas, a partir de la literatura.
2. Analizar los riesgos relacionados con el comercio electrónico, asociados hacia las pymes colombianas.
3. Compilar la normatividad de seguridad informática que se debe conocer en el comercio electrónico aplicado a las pymes colombianas.
4. Proponer una guía de buenas prácticas de seguridad informática en el comercio electrónico para las pymes colombianas.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

Según Martínez, [14] la información es el activo más importante que tiene las organizaciones y este debe ser protegido.

La implementación de mecanismos de seguridad para la información de las pymes es de gran importancia y su protección puede lograr que dichas empresas estén protegidas ante posibles amenazas de estafas o interrupción de actividades.

Como base de éstas buenas prácticas se ha tomado el Anexo A de la norma ISO 27001:2013 que sean aplicables a comercio electrónico. También la normatividad en Colombia que aplique a la protección de datos y comercio electrónico que haya lugar.

Adicionalmente a continuación se describirá algunas definiciones claves para tener claridad durante el desarrollo de los objetivos de la presente monografía entre los cuales se tienen:

Comercio electrónico: "El comercio electrónico a través de Internet se refiere a cualquier forma de transacción comercial en la que las partes involucradas interactúan electrónicamente por medio de la World Wide Web, y no por un contacto físico directo. Hace referencia a la compra y venta de bienes y servicios a través de los sitios comerciales en la Web."[15]

[14] Security Report ESET Latinoamérica 2020. [en línea]. Welivesecurity.com. 2020, nro.8. [Consultado: 19/04/2021]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf

[15] Acacia. MODELO DE MARKETING POR INTERNET DE EMPRESA. [en línea]. [Consultado: 20 de noviembre de 2020]. Disponible en: http://acacia.org.mx/busqueda/pdf/MODELO_DE_MARKETING_POR_INTERNET_DE_EMPRESA.pdf

“Podríamos definir una e-commerce como una tienda virtual. Un método de compraventa que utiliza Internet como medio para realizar transacciones y contactar con sus consumidores. No solo mediante una página web, sino también a través de las redes sociales. Estas suponen una fuente informativa con mucho impacto, y permiten acercarte y conocer más a tu público objetivo.”[16]

Analizando los conceptos mencionados se puede afirmar que el comercio electrónico puede definirse de modo general como un método más eficaz para el proceso de comercialización, compra, venta y toda la publicidad relacionada con los bienes, productos y/o servicios que brinda una organización a través de Internet, de esta manera se elimina contacto físico entre compradores y vendedores y aumenta la competitividad, calidad, compra y venta sin límite de horarios ni lugar específico.

Por tanto, el comercio electrónico permite el uso de las tecnologías de la información y las comunicaciones para todas las actividades comerciales, marketing, reducir costos y de esta manera favorece en gran medida las pymes para su reconocimiento en el mercado, cercanía con los clientes y proveedores.

Pymes: Es la abreviación que contiene las micro, pequeñas y medianas empresas en Colombia. De acuerdo con el decreto 957 de 2019 [17]éstas se clasifican de acuerdo con el número de empleados totales, valor de sus ventas brutas anuales y sus activos totales. Los valores de los criterios anteriormente mencionados son basados en el sector

[16] IEBSCHOOL. ¿Qué es ecommerce y cómo crear tu propio comercio electrónico? [en línea] (3 de marzo de 2020) [Consultado: 30 de noviembre de 2020]. Disponible en: https://www.iebschool.com/blog/comercio-online-ecommerce/

[17] COLOMBIA. MINISTERIO DE DESARROLLO ECONÓMICO. Decreto 2269 (16, noviembre, 1993). Por el cual se organiza el sistema nacional de normalización, certificación y metrología [en línea]. Bogotá, D.C, 2019. 7 p. [Consultado: 22 de abril de 2021]. Disponible en: https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%20957%20DEL%2005%20DE%20JUNIO%20DE%202019.pdf

económico en la cual la empresa desarrolle su actividad descritos en la sección 2 del mismo decreto.

Estas empresas son muy importantes para la economía colombiana puesto que contribuyen con el 28% del PIB, el 67% del empleo y el 37% de la producción del país.[18] Estas compañías fueron las más afectadas durante la pandemia del COVID-19 debido a los confinamientos estrictos en el país lo cual les obliga a cerrar sus empresas físicas y tener pérdidas económicas considerables, algunas les ha llevado a cerrar definitivamente y otras a evolucionar a través de la crisis a la transformación digital como el e-commerce.

Seguridad informática: Para comprender la importancia que tiene la seguridad de la información en cualquier organización, es necesario comprender primeramente el concepto de seguridad de la información y la diferencia con seguridad informática. Estos términos suelen confundirse ya que son terminologías similares pero que tienen orientaciones diferentes frente a sus objetivos.

El principal objetivo de la seguridad informática es el de proteger y resguardar la información integral (física y digital) de una organización o persona en particular. La seguridad informática únicamente protege y resguarda los datos almacenados en medios informáticos o digitales.[19]

Bajo estas premisas, la información para poder ser protegida y resguardada es necesario aplicar las mejores medidas de seguridad y las buenas prácticas informáticas de las cuales se va a profundizar en la presente monografía, y así lograr la protección integral de todos los datos e información importantes de esa organización o persona a defender.

[18] Hoyos-Estrada, S., & Sastoque-Gómez, J. (2020). Marketing Digital como oportunidad de digitalización de las PYMES en Colombia en tiempo del COVID – 19. Revista Científica Anfibios, 3(1), 39-46. https://doi.org/10.37979/afb.2020v3n1.60

[19] La Seguridad de la Información: Historia, Terminología y Campo de acción [blog]. Disponible en: https://blog.desdelinux.net/seguridad-información-historia-terminologia-campo/

La seguridad informática es vital para garantizar la continuidad de los negocios, por tal razón, a la información que se desea proteger se le debe garantizar los tres principios de la seguridad de la información tales como su confidencialidad, autenticidad y disponibilidad.

Principios de la seguridad de la información [20],[21]

Confidencialidad: Principio que garantiza que solamente el personal autorizado pueda acceder a la información. De esta manera se busca que la información sea accedida o divulgada a sistemas o personal no autorizado.

¿Cómo garantizar este principio?

- Implementar mecanismos de control de acceso a la información
- La no divulgación de usuarios y contraseñas de los usuarios que acceden a la información
- Implementación de políticas de cambio de contraseña periódicamente, uso de contraseñas robustas y múltiples factores de autenticación.
- Mecanismos de expiración de sesiones en las aplicaciones o sistemas donde se encuentre la información a proteger
- Eliminación o desecho de información inadecuada, es decir, sin destruirla previamente.

¿Qué sucede si este principio no se cumple?

[20] Seguridad de la información: ¿qué principios necesitan conocer las empresas? [blog] (2020). Disponible en: https://blogmexico.comstor.com/seguridad-de-la-información-que-principios-necesitan-conocer-las-empresas

[21] Firma-e.com. 2014. Pilares De La Seguridad De La Información: Confidencialidad, Integridad Y Disponibilidad | Firma-E. [online] Disponible en: <https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-información-confidencialidad-integridad-y-disponibilidad/>.

La primera consecuencia radica en que la información esté expuesta, por ende, se puede ser víctima de delitos informáticos tales como fuga de información, robo o divulgación. Como consecuencia de estos delitos el propietario de la información puede tener grandes pérdidas financieras, credibilidad y confianza por parte de sus socios o clientes y adicionalmente puede enfrentar procesos judiciales por exposición o mala manipulación de los datos personales.

Integridad: Principio que garantiza que la información se encuentre en su estado original, intacta, sin alteraciones o modificaciones no autorizadas. De esta manera el dueño de la información podrá tener certeza que la información almacenada no esté corrupta, dañada o modificada sin autorización.

¿Cómo garantizar este principio?

- Implementar un control de acceso basado en roles y privilegios
- Realizar backups de la información y sistemas digitales
- Realizar adecuado almacenamiento de la información cuando está en medios físicos
- Reforzamiento de la infraestructura tecnológica de la organización
- Implementar sistema de control de cambios
- Implementar firma digital
- Encriptación de los datos

¿Qué sucede si este principio no se cumple?

La información se podrá perder por algún factor externo o de falla en donde se encuentre almacenada, se podrá modificar sin control por tales razones no se puede tener garantía para mantenerla intacta y la organización no podrá confiar en la información almacenada o si los datos son reales.

Disponibilidad:

Es el principio de la información que garantiza que la información esté disponible todo el tiempo sin interrupciones para acceder a ella en el momento en que se necesite y requiera acceder a ella.
¿Cómo garantizar este principio?

- Implementar sistemas de backups eficientes, como alta disponibilidad en la infraestructura tecnológica
- Implementar infraestructura tecnológica en la Nube o Hibrida
- Tener un plan de recuperación de desastres eficiente

¿Qué sucede si este principio no se cumple?

No se podrá reaccionar o proceder frente a desastres o daño de infraestructura, no se podrá garantizar la continuidad de las operaciones del negocio y se podrán prolongar los periodos de indisponibilidad para acceder a la información cuando se necesite.

Historia

Para comprender aún más la importancia de la seguridad de la información se podrá visualizar una corta visualización de la historia.

La seguridad de la información no es un término que haya nacido desde la época moderna de la tecnología, desde el inicio de nuestra historia hasta la actualidad, se ha buscado proteger la información desde el arte llamado Criptografía. A continuación, se describe los principales Hitos del inicio de la historia de la seguridad de la información:

Hitos importantes criptográficos a. C.:[22]

- En los años 1500 a. C. se buscaba proteger una tableta Mesopotámica que contenía una fórmula cifrada para producir un vidriado cerámico.
- En los años 500-600 a. C. existían los libros hebreos sagrados de los profetas y la historia de los reyes de Israel tales como David, Salomón, Ezequías, Jeremías, Ezequiel, y estaban escritos con un cifrado sencillo usando la inversión del alfabeto.

Hitos importantes criptográficos d. C.:

- En el año 855 se conoció el primer libro de criptografía en el medio oriente.
- En el año 1500 Se aplico la criptografía en la diplomacia de Italia.
- En el año 1917 Se desarrolló la cinta aleatoria de un solo uso, único sistema criptográfico seguro de la época.
- En el año 1923 Durante la segunda guerra mundial, se usó la máquina de rotores "Enigma", Alemania la usó para sus comunicaciones encriptadas y que el país enemigo no pudiera descifrar sus estrategias de guerra.

Hitos importantes aparición de delincuentes informáticos:[23]

- En el año 1903 aparece el primer hacker de la historia llamado Nevil Maskelyne que interceptó una transmisión de telégrafo inalámbrico.
- En el año 1972 aparece el primer Phreaker llamado John Draper quien descubrió que un silbato que regalaban en las cajas de cereales "Cap'n Crunch" se podía

[22] La Seguridad de la Información: Historia, Terminología y Campo de acción. [blog] Disponible en: https://blog.desdelinux.net/seguridad-información-historia-terminologia-campo/
[23] Encyclopedia.kaspersky.es. 2020. Una Breve Historia Sobre El Hackeo. [online] Disponible en: <https://encyclopedia.kaspersky.es/knowledge/a-brief-history-of-hacking/>

modificar a la misma frecuencia que usaba AT&T para entrar en modo operador y así poder navegar y hacer llamadas gratuitas.

- En el año 1978 Kevin Mitnick utiliza la ingeniería social para burlar el sistema de tarjetas de autobuses de Los Ángeles, y en 1979 accedió a un sistema informático donde robó un software de Arca.
- En el año 1999 Jonathan Joseph James accedió y robó información de la NASA y el Pentágono en Estados Unidos a través de un Sniffer en una puerta trasera de un servidor donde extrajo mensajes y credenciales de acceso a ordenadores militares.
- En el año 2002 Hackers no identificados atacan 13 servidores del dominio raíz de Internet para tumbar el servicio de los DNS de Internet.

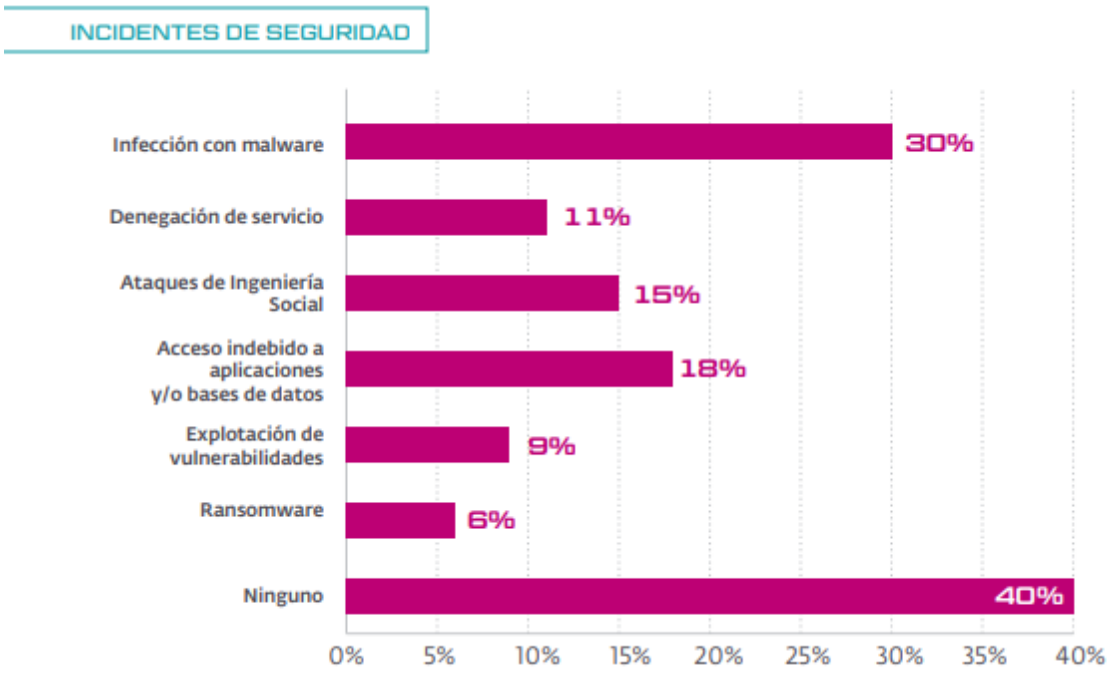
En los años siguientes hasta hoy los ataques son diarios y constantes a nivel mundial, en esta cronología solo se dan los hitos más importantes en el inicio de la historia.

4.2 ANTECEDENTES O ESTADO ACTUAL

Los incidentes de seguridad cada día han venido aumentando, y son las pymes las más afectadas, puesto que dichas organizaciones son las que menos importancia o interés tienen para implementar mecanismo de defensa que les ayuden a proteger su información.

Para el año 2020 las infecciones de malware y códigos maliciosos, el fraude interno y externo y la explotación de vulnerabilidades, fueron los incidentes de seguridad más recurrentes y es la priorización de dicha investigación, lo que resalta la buena función de tener protegida la información. Los problemas cibernéticos seguirán existiendo, y es responsabilidad de cada empresa, proteger su información, como su activo más valioso.

Figura 1: Clasificación de los incidentes de seguridad.



Fuente: Security Report ESET Latinoamérica 2020. [en línea]. Welivesecurity.com. 2020, nro.8. [Consultado: 19/04/2021]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf

En la figura 1 se puede evidenciar que la mayoría de las empresas presentaron infecciones con malware, con intenciones maliciosas y como segundo lugar el acceso indebido a aplicaciones y/o bases de datos, que básicamente hace referencia a suplantaciones de identidad o ataques dirigidos.

También según cifras de la CCIT y la policía nacional de Colombia, aumentó en un 54% el número de delitos informáticos denunciados. Además de esto, los delitos informáticos más denunciados en Colombia son Phishing, suplantación de identidad, malware y fraudes bancarios. Las cifras son preocupantes, 717 pymes reportaron ataques de Ransomware exitosos en 2019, esto porque según la misma investigación refleja que el 83% de las pymes no tienen implementados o son carentes de políticas y procedimientos para poder responder ante la vulneración o prácticas que vallan en contra de las políticas de seguridad de la información en sus organizaciones. Del mismo modo, los ataques a

través de malware crecieron en un 612% en el año 2019 y finalmente 170 empresas reportaron ataques de denegación de servicio distribuido o DDoS exitosos que afectaron los servicios que les brindan a sus clientes.

Según sus recomendaciones afirman “El 60% de las pequeñas y medianas empresas, no pueden sostener sus negocios más de seis meses luego de sufrir un ciberataque importante. Esto demuestra que los factores en torno a los Ciberataques a PYMES en Colombia comprometen seriamente los activos económicos e impactan asuntos estrictamente legales y de cumplimiento de las compañías.”[24]

Todo esto nos demuestra lo vulnerables que están las empresas y la importancia que toma proteger su información, ya que están expuestas y esto puede traer grandes consecuencias, como el robo del dinero en las cuentas, robo de información importante, la congelación de las actividades y un sin número de problemáticas hasta el cierre total de sus actividades por no poderse recuperar ante este tipo de incidentes.

[24] Informe de las tendencias del Cibercrimen en Colombia 2019-2020.Bogotá D.C. CCIT.org.co. Octubre 29 de 2019. [Consultado: 19/04/2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

5 BENEFICIOS ASOCIADOS AL COMERCIO ELECTRÓNICO EN LAS PYMES COLOMBIANAS, A PARTIR DE LA LITERATURA.

Son muchos los beneficios que acompaña la implementación del comercio electrónico para el aporte económico y para el sostenimiento de las pymes colombianas en el país. Según el Tiempo,[25] en el año 2020 Colombia alcanzo cifras inesperadas en el aumento significativo de comercio electrónico en el país por causa del COVID-19, se alcanzó más de 222 millones de transacciones en línea por causa del comercio electrónico lo que impulso la economía de las pymes colombianas y el país. Para el año 2021 el gobierno de Colombia presupuesta 290 millones de transacciones por causa del comercio electrónico en el país.

5.1 TENDENCIAS DEL COMERCIO ELECTRÓNICO DURANTE LA CRISIS MUNDIAL DEL COVID-19

En diciembre del año 2019 se descubre el inicio de una nueva cepa de coronavirus en Wuhan, China llamado COVID-19. Este virus causa problemas respiratorios graves, insuficiencia renal y hasta la muerte en algunos casos. Además, es una enfermedad infecciosa y se transmite rápidamente entre un ser humano y otro con solo cercanía o contacto físicos con un infectado, causando en un alto porcentaje de población el contagio del virus y así mismo la muerte de la mayoría de la población. Esta infección se extendió rápidamente hasta llegar a todo el planeta en el 2020 y ocasiona el inicio de una grave crisis mundial por la muerte de su población rápidamente, el colapso de la capacidad máxima de atención en los hospitales, ausencia de equipos, medicinas y personal médico para la atención de la enfermedad.

[25] El Tiempo. Comercio electrónico en Colombia proyecciones del 2021: 290 millones de transacciones, la meta del país en 'e-commerce'. [sitio web]. Bogotá, Colombia. (07 de marzo de 2021).[Consultado: 28 de abril de 2021].Disponible en:https://www.eltiempo.com/tecnosfera/novedades-tecnologia/comercio-electronico-en-colombia-proyecciones-del-2021-571657

“El nuevo Coronavirus (COVID-19) ha sido catalogado por la Organización Mundial de la Salud como una emergencia en salud pública de importancia internacional (ESPII). Se han identificado casos en todos los continentes y, el 6 de marzo se confirmó el primer caso en Colombia.”[26] Por esta razón a nivel mundial fueron restringidos los vuelos internacionales, se obliga el uso de mascarillas, distanciamiento social, se restringe las exportaciones e importaciones no esenciales, se tomaron medidas de cuarentena de la población donde se prohibía la salida de los hogares a la población y los comercios solo podían abrir los más esenciales como es de alimentación y medicina. Las personas que incumplieran estos decretos y su salida a las calles no fueran esenciales y no contempladas en los decretos eran sometidas a sanciones económicas fuertes.

Por lo anteriormente descrito, la economía en Colombia entró en una grave crisis, todos los sectores económicos tuvieron crisis por no poder seguir ofreciendo sus servicios y productos al mercado y esto causa a su vez altos índices de desempleo, según el DANE [27] la tasa de desempleo en Colombia en el mes de mayo fue de 21.4%, lo que representa 10,9% más que el mismo mes del 2019 y en octubre fue de 16,8%, lo que representa un aumento de 6.4% comparándose con el año 2019.

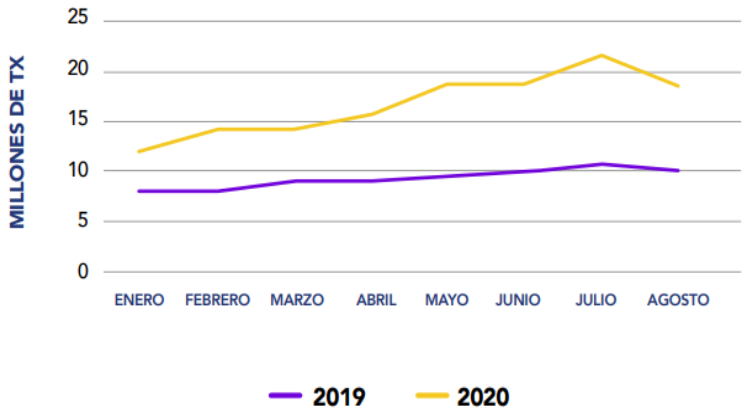
Esta crisis forzó a los negocios y pymes de todos los sectores en Colombia a reinventarse para poder sobrevivir en el mercado laboral y la crisis económica del momento. Según la CCCE [28] el cierre de los canales físicos de atención al público para ventas y/o servicios y el confinamiento de la población colombiana, obligaron a que la población usara canales

[26] MINSALUD. CORONAVIRUS (COVID-19). [en línea] [Consultado: 15 de diciembre de 2020] Disponible en:
https://www.minsalud.gov.co/salud/publica/PET/Paginas/COVID-19_copia.aspx
[27] DANE. Empleo y desempleo. [en línea] (30 de noviembre de 2020). [Consultado: 16 de diciembre de 2020].
Disponible en: https://www.DANE.gov.co/index.php/estadisticas-por-tema/mercado-laboral/empleo-y-desempleo
[28] CCCE. Informe: comportamiento del eCommerce en Colombia durante 2020 y perspectivas para 2021. [en línea] (13 de octubre de 2020). [Consultado: 16 de diciembre de 2020].
Disponible en:
https://www.ccce.org.co/gestion_gremial/informe-comportamiento-del-ecommerce-en-colombia-durante-2020-y-perspectivas-para-2021/

virtuales para realizar todo tipo de movimientos y transacciones y así mismo que las organizaciones usaran medios digitales para seguir ofreciendo sus productos y servicios. De esta manera se puede concluir que el comercio electrónico se vuelve vital para vendedores y compradores.

Según la CCCE "Al comparar el mismo periodo entre enero y agosto de 2019 y de 2020, se evidenció un crecimiento acelerado en las transacciones realizadas a través del comercio electrónico en Colombia. Particularmente, en enero de 2020 el número de transacciones de compra realizadas a través de este canal creció el 52.2% respecto a enero de 2019. Por su parte, para julio de 2020, el número de transacciones, respecto a julio de 2019, creció 100.4%. Sin embargo, para agosto de 2020, el crecimiento en el número de transacciones en comparación con agosto de 2019 se redujo a 78.8%."[29]

Figura 2: Transacciones de comercio electrónico primer semestre de 2019 y 2020 en Colombia



Fuente: CCCE.ORG.CO. 2020. Informe-comportamiento-y-perspectiva-ecommerce-2020-2021. [Consultado: 15 de diciembre de 2020] Disponible en: https://www.ccce.org.co/wp-content/uploads/2020/10/informe-comportamiento-y-perspectiva-ecommerce-2020-2021.pdf

En la figura 2 se puede apreciar que la digitalización de las organizaciones y comercios en el país ocasiona un aumento significativo en el comercio electrónico y las medidas tomadas por el gobierno de contención del COVID-19.

[29] Informe comportamiento del ecommerce en Colombia durante 2020 y perspectivas para 2021. [pdf]. CCCE. [Consultado 10 de diciembre de 2020]. Disponible en: https://www.ccce.org.co/wp-content/uploads/2020/10/informe-comportamiento-y-perspectiva-ecommerce-2020-2021.pdf

Colombia Fintech [30] afirma que muchas pymes y negocios en Colombia están aprovechando las nuevas oportunidades que la crisis sanitaria y económica ha desatado en el país para realizar sus ventas y atención al cliente a través de medios electrónicos y digitales. Existen varias alternativas para ejecutar el comercio electrónico como los Marketplace y proveedores de plataformas de comercio electrónico con procesos eficientes y manejo de publicidad de los productos y/o servicios, inventario, pedidos, clientes, proveedores, entre otros.

5.2 BENEFICIOS DEL COMERCIO ELECTRÓNICO PARA LAS PYMES COLOMBIANAS

Como se observa anteriormente por la emergencia sanitaria y económica a nivel mundial, el comercio electrónico va en un aumento acelerado y junto con ello la importancia en la economía del país, por ende, el gobierno nacional de Colombia también ha implementado algunas estrategias y proyectos para que las pymes y empresas colombianas puedan aprovechar y así sus negocios se sostengan y aporten positivamente en la reactivación económica del país.

5.2.1 Inclusión en estrategias y proyectos del gobierno colombiano

Uno de estos proyectos es realizado e incentivado por el ministerio de las TIC en Colombia[31] llamado “Vende Digital”, la cual es una plataforma de Marketplace donde se les apoya en la creación y funcionamiento de tiendas virtuales a pymes y comerciantes colombianos durante un año, además de esto se les facilita un proceso de formación de estas herramientas digitales a través de asesorías personalizadas y material didáctico

[30] Colombiafintech. E-commerce, un aliado clave durante el coronavirus. [en línea] (08 de septiembre de 2020) [Consultado: 17 de diciembre de 2020]. Disponible en: https://www.colombiafintech.co/novedades/e-commerce-un-aliado-clave-durante-el-coronavirus

[31] Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Vende Digital: lleva tu negocio a otro nivel. [sitio web]. Bogotá, Colombia. [Consultado: 01 de mayo de 2021]. Disponible en: https://vendedigital.mintic.gov.co/754/w3-channel.html

para que además que brindarles el conocimiento les están dando las herramientas para que implementen una estrategia de comercio electrónico efectivo.

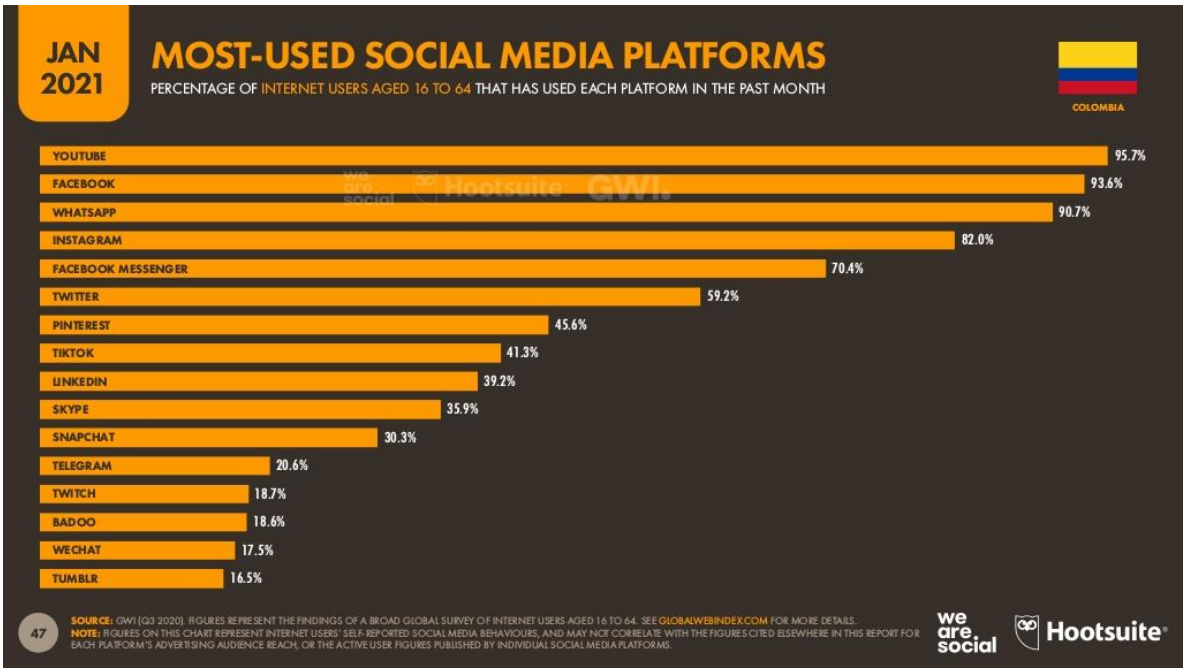
Otro proyecto realizado e incentivado por ProColombia respaldado por el ministerio de Comercio, Industria y Turismo [32] llamado “Colombia a un clic”, donde reconoce que para las pymes colombianas tienen una necesidad de la implementación del comercio electrónico como una herramienta para realizar ventas en líneas y llevarlas a ventas a nivel mundial. ProColombia realizó alianzas con Amazon, Mercadolibre, Linio y Dafiti donde buscan beneficiar pymes colombianas para que ingresen a estas plataformas y realicen ventas en línea a todo el planeta. Además de brindarles estos canales de ventas también les brindan a través de Amazon procesos de acompañamiento para realizar el seguimiento a sus negocios y marketing digital para que su estrategia de comercio sea más efectivo y así mismo logren impulsar sus ventas a mediano plazo sin límites geográficos.

5.2.2 Uso estratégico de redes sociales y aplicaciones

Las pymes pueden potencializar también el uso de aplicaciones de videoconferencia y redes sociales como mecanismos para realizar campañas de mercadeo más accesibles y flexibles para los consumidores, esto es útil para que los compradores obtengan información sobre los productos y servicios que ofrecen los empresarios en las pymes colombianas y así mismo éstas puedan obtener información de los clientes de carácter estadística, encuestas e información que los visitantes suministren a voluntad propia que permita mejorar la publicidad a través de los portales web, servicios, la calidad de estos y personalizar los mismos dependiendo los nichos de mercado.

[32] Ministerio de Comercio, Industria y Turismo. ProColombia lanzó ‘Colombia a un clic’ para impulsar el e-commerce. [sitio web]. Bogotá, Colombia. (03 abril de 2019). [Consultado: 01 de mayo de 2021]. Disponible en: https://www.mincit.gov.co/prensa/noticias/industria/procolombia-lanzo-colombia-a-un-clic-para-impulsar

Figura 3: Plataformas de redes sociales más usadas en Colombia



Fuente: Kemp, Simon. Digital 2021: Local Country Headlines. 27 de enero de 2021. Most-Used Social Media Platforms. [Consultado: 06 de mayo de 2021] Disponible en: https://datareportal.com/reports/digital-2021-local-country-headlines?utm_source=Reports&utm_medium=PDF&utm_campaign=Digital_2021&utm_content=Dual_Report_Promo_Slide

En la Figura 3 se puede visualizar las cifras mostradas en el informe anual de Marketing Digital Colombia 2021, donde se visualiza las redes sociales con más uso en el país las cuales encabezan la lista Youtube, Facebook, Whatsapp e Instagram. De esta manera las pymes podrán enfocar sus esfuerzos publicitarios en estas plataformas con base en las estadísticas dadas y a través de plataformas de monitoreo en tiempo real.

5.2.3 Uso de medios de pago electrónicos

Otro beneficio de igual importancia tanto para las pymes como para los compradores es la implementación de medios de pago electrónicos donde ya no se necesita tener efectivo para realizar una compra, haciéndolo un método más seguro, cómodo y adaptado a las necesidades de los clientes.

A través de los medios electrónicos de pago se puede ofrecer a los clientes una mayor calidad en el servicio prestado en cuanto al tiempo óptimo para realizar la compra, pago electrónico, atención y asesoría en línea y tiempos óptimos de despacho y entrega del producto y/o servicio.

En Colombia existen múltiples formas de pago en línea dentro de los cuales se destacan:

- Pago a través de cuenta de ahorros/corriente con tarjeta débito o tarjeta crédito.
- Existen agencias que facilitan el sistema de pagos como lo son PSE, REDEBAN, CREDIBANCO o tarjetas de una entidad bancaria.[33]
- Pagos a través de efectivo a través de Baloto, Efecty o RedServi
- Proveedores de servicios de pago en línea como Paypal, PayU, Mercado pago, entre otras donde los clientes pueden elegir múltiples formas de pago en línea donde confíen mayormente y además de esto contempla buenas prácticas de seguridad informática y manejo de los datos para evitar fraudes y estafas tanto para compradores como vendedores.[34]

Uno de los beneficios inmersos al usar plataformas de medios de pago electrónico al ser contratados en una pyme es que brindan seguridad tanto a vendedores como compradores durante las transacciones de compra y venta ejercido en el comercio electrónico porque aplican la normatividad referente a la protección del consumidor y sus datos durante las transacciones, esto mediante técnicas y buenas prácticas de seguridad informática aplicadas a las transacciones realizadas en los portales destinados para ello. Esta seguridad mencionada se logra a través de la implementación de protocolos de comunicación seguros como lo son el protocolo SET (Secure Electronic Transaction)

[33] SIC. Estudios de Mercado. [en línea]. [Consultado: 5 de diciembre de 2020]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/promocion_competencia/Estudios_Economicos/Estudios_Economicos/Estudios_Mercado_E-commerce.pdf

[34] JIMENEZ, David. Pasarelas de Pago en Colombia: ECOMMERCE [en línea]. DigitalJourney. (1 de octubre de 2020). [Consultado: 05 de mayo de 2021]. Disponible en: https://digitaljourney.com.co/pasarelas-de-pago-en-colombia/

[35]que es muy usado para los pagos con tarjetas débito o crédito puesto que usa algoritmos criptográficos y hash que juntos garantizan los principios de la seguridad de la información así:

1. La privacidad, puesto que la información de las tarjetas usadas por los clientes no es revelada ante la pyme o comercio donde se realiza el pago y el banco a su vez no tiene el detalle de su compra.
2. La autenticación, que con el uso de certificados y firmas electrónicas se garantiza la autenticación tanto del comercio como del cliente titular del medio de pago para evitar suplantaciones, fraudes y el no repudio de la transacción.
3. La confidencialidad mediante la transmisión de la información segura al aplicar técnicas de cifrado y la integridad mediante el uso de hash que garantiza que el mensaje no ha sido modificado inescrupulosamente durante la transmisión.

5.2.4 Otros beneficios:

Además de los beneficios del comercio electrónico anteriormente descritos tanto para los compradores, vendedores e intermediarios también se destacan:[36] [37]

- Disponibilidad de acceso y comercialización de productos y/o servicios desde cualquier lugar del planeta las 24 horas del día, solo es necesario acceso a Internet para acceder a éstos.

[35] Geeksforgeeks.Protocolo de transacciones electrónicas seguras (SET).[sitio web].(19 de junio de 2018)[Consultado: 30 de mayo de 2021] Disponible en: https://www.geeksforgeeks.org/secure-electronic-transaction-set-protocol/

[36] UNIVERSIDAD DE CUENCA FACULTAD DE INGENIERIA MAESTRIA EN TELEMÁTICA. Implementación de un prototipo de tienda virtual sobre plataforma Linux para realizar transacciones de comercio electrónico seguro. [en línea] (30 de julio de 2010) [Consultado: 05 de diciembre de 2020]. Disponible en: https://dspace.ucuenca.edu.ec/bitstream/123456789/2530/1/tm4396.pdf

[37] Gil Carmona Yessika Tatiana. BENEFICIOS DEL E-COMMERCE EN LAS PYMES COLOMBIANAS DURANTE LA COVID-19. [en línea]. Universidad Militar Nueva Granada. Bogotá, Colombia.2020. [Consultado el 6 de diciembre de 2016]. Disponible en:https://repository.unimilitar.edu.co/bitstream/handle/10654/37014/Yessika%20Tatiana%20Gil%20Carmona.pdf?sequence=1&isAllowed=y

- Se mitiga la congestión de puntos de atención físicos, largas filas y tiempos de espera para que los consumidores puedan adquirir los productos y/o servicios
- Los consumidores podrán tener acceso fácil a la información de los productos, diferentes vendedores, calidades, precios y seleccionar lo que más convenga.
- Disminución de costos operativos y de infraestructura para las pymes, ahorros de costos de alquileres de sitios físicos, locales, almacenes, sueldos de vendedores, publicidad física de los productos y/o servicios, y a su vez permite bajar los costos en los productos, manejar un marketing digital y permite ser más competitivo.
- Aumento en las ganancias sobre los productos y/o servicios ofrecidos.
- Facilita las investigaciones de mercado por parte de las pymes, existen herramientas de análisis de tendencias en el mercado para analizar y gestionar adecuadamente grandes volúmenes de datos.
- Facilidades de adopción de un modelo E-commerce en la PYME puesto que se puede bancarizar fácilmente y no requiere un monto alto de capital.
- Modernización del negocio, mayor visibilidad e inclusión en la adopción de herramientas TIC que le permitan a la pyme estar a la vanguardia y competitividad en el mercado actual.
- Optimización de tiempos en servicios de asesoría y atención al cliente
- Aumento considerable de los clientes en cualquier ubicación geográfica y reconocimiento a través de mayor visibilidad de su publicidad a través de los diferentes medios de comunicación, especialmente Internet.
- Optimización de tiempo, dinero y productividad puesto que los recursos humanos a través de alternativas como teletrabajo y alternancia.

6 RIESGOS RELACIONADOS CON EL COMERCIO ELECTRÓNICO, ASOCIADOS HACIA LAS PYMES COLOMBIANAS.

6.1 ESTADO DE LA CIBERSEGURIDAD EN LAS PYMES COLOMBIANAS

Health, H**,** una empresa colombiana importante que provee servicios tecnológicos para entidades del sector salud plantea que: [38] **"**En Colombia según el Centro Cibernético Policial (CCP), el 87% de las empresas víctimas de incidentes digitales no denuncian estos incidentes y los sufren por falta de programas de prevención.". Las organizaciones que sufren ataques cibernéticos prefieren guardar su reputación y no ser expuestas ante los medios y por ende no denuncian. Sin embargo, las compañías que sufren este tipo de delitos sufren pérdidas económicas cerca de 4.000.000.000 COP por sanciones, gastos legales, multas, perdidas o daños en su infraestructura.

El Tiempo [39] en un artículo se refiere que en el año 2019 se reportaron más de 28.000 ciberataques en Colombia donde los más denunciados son ataques con Ransomware, Malware, Phishing, robo informático, suplantación de identidad, fraude de pagos online, donde Bogotá lidera los ataques con 5.308, luego Cali (1.190) y Medellín (1.186).

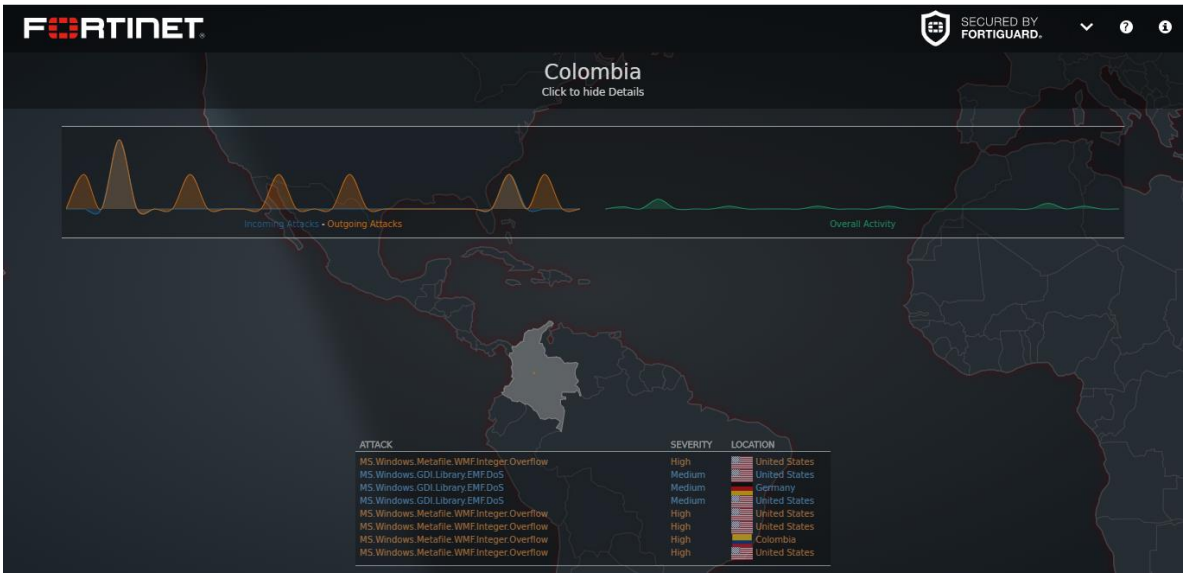
Las pymes colombianas actualmente son los más afectados frente a los diferentes tipos de ataques cibernéticos donde se lideran a través de la técnica de Ingeniería social con un 90% de afectación, 80% con correos fraudulentos, 60% con suplantación de identidad, 53% con el enmascaramiento de correos electrónicos y el 37% con la contaminación de páginas y aplicaciones web. Las pérdidas económicas por este tipo de delitos rondan entre los 300 y 5.000 millones de pesos.

[38] Health, H., 2019. 5% De Las Empresas colombianas Han Perdido Hasta Cuatro Mil Millones Por Ciberataques. [online] Heon.com.co. Disponible en: <https://www.heon.com.co/index.php/news/item/241-ataques-ciberneticos-colombia>

[39] El Tiempo. 2019. En 2019 Se Reportaron Más De 28.000 Casos De Ciberataques En Colombia. [online] Disponible en: <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790>

Según se accedió al mapa de amenazas de Fortinet, una marca líder en el mercado de la ciberseguridad se visualiza los ataques que están ingresando al país cada segundo que son numerosos:

Figura 4: Mapa de amenazas en línea de Fortinet



Fuente: Threatmap.fortiguard.com. 2020. Fortinet Threat Map. [Consultado: 28 de noviembre de 2020] Disponible en: <https://threatmap.fortiguard.com/>

En la figura 4 se logra ver en tiempo real a Colombia resaltado en blanco y los ataques que están siendo detectados a través de Fortiguard (solución de Fortinet), también en la parte superior de la imagen se pueden visualizar los ataques entrantes y salientes en una gráfica y en la parte inferior se puede ver la descripción del ataque, la severidad y el lugar. En esta imagen se puede identificar que en Colombia en el instante de la toma de la imagen estaba siendo atacada con un ataque llamado "MS.Windows.Metafile.WMF.Integer.Overflow".[40]. Este ataque hace referencia al aprovechamiento de una vulnerabilidad de desbordamiento de pila en sistemas

[40] LABORATORIOS FORTIGUARD. MS.Windows.Metafile.WMF.Integer.Overflow. [sitio web].Enciclopedia de amenazas.[Consultado: 15 de febrero de 2021]. Disponible en: https://www.fortiguard.com/encyclopedia/ips/11314

operativos Microsoft Windows a través de un archivo WMF[41] (Es un metarchivo del sistema operativo Windows que contiene comandos de programación necesarios para imágenes y dibujo sobre el cual funciona el paquete office de Microsoft y extensiones de imagen) personalizado por el atacante y así conseguir ejecutar códigos maliciosos remotamente en esos sistemas vulnerables.

Según la Revista Dinero y ESET Latinoamérica, las empresas colombianas en el año 2020 han tenido un aumento de delitos informáticos del 59% frente al año 2019, la infección de malware es la más frecuente. [42]

Las falencias identificadas más frecuentes por parte de ESET Latinoamérica son la falta de políticas de seguridad, la no clasificación de la información corporativa y no contar con planes de continuidad del negocio.

Según CCIT [43] la ciberdelincuencia se ha incrementado por el COVID-19 reportando un total de 17.211 delitos informáticos, 59% más que el 2019. Cifras alarmantes teniendo en cuenta que por cuenta del COVID-19 las pymes colombianas por causa del COVID-19 que ha afectado gran parte de la economía colombiana, se han visto forzadas al teletrabajo y ventas por Internet lo que, si no se tienen adecuadas prácticas de seguridad de la información pueden ser víctimas de delitos informáticos con pérdidas millonarias los cuales afecta hasta llegar a la quiebra de algunas compañías.

[41] WMF (Windows Metafile).[sitio web].online-convert.com.[Consultado: 31 de mayo de 2021]. Disponible en: https://www.online-convert.com/es/formato-de-archivo/wmf

[42] Empresarial, C., 2020. Ciberataques En América Latina: ¿Están Expuestas Las Empresas colombianas? [online] ¿Qué tan seguras están las empresas colombianas ante ciberataques? Disponible en: <https://www.dinero.com/tecnologia/articulo/que-tan-seguras-estan-las-empresas-colombianas-ante-ciberataques/296519>

[43] CCIT - Cámara colombiana de Informática y Telecomunicaciones. 2020. Empresas colombianas Cada Vez Más En La Mira De Los Ciberdelincuentes. [online] Disponible en: <https://www.ccit.org.co/noticias/safe-presenta-mejores-practicas-para-el-fortalecimiento-de-la-ciberseguridad-empresarial/>

6.2 RIESGOS RELACIONADOS CON EL COMERCIO ELECTRÓNICO, ASOCIADOS HACIA LAS PYMES COLOMBIANAS.

Como se describió anteriormente son muchas las ventajas y beneficios que obtienen las pymes colombianas al implementar comercio electrónico en sus negocios, pero además de estos beneficios se debe tener en cuenta que también existen riesgos que conllevan el uso de la infraestructura tecnológica, tales como las páginas web, servidores, computadores, bases de datos, una correcta gestión de los datos y los sistemas informáticos que la almacenan, entre otro tipo de activos tecnológicos.

Los riesgos más comunes en los activos informáticos usados durante el ejercicio del comercio electrónico son:

- **Fallas en la infraestructura tecnológica debido a falta de evaluación y gestión de riesgos:** La falta de evaluación y adecuada gestión de los riesgos que conlleva usar una infraestructura tecnológica en una pyme y el no dar la importancia suficiente al aseguramiento de esta trae muchas consecuencias. La principal es ser víctima de delitos informáticos graves de los cuales no pueda recuperarse y deba cerrar definitivamente su negocio. La falta de aplicación de buenas prácticas de seguridad informática en las organizaciones o vendedores en las plataformas virtuales o páginas web exponen tanto al vendedor como al consumidor ser víctimas de fraudes, suplantaciones entre otros delitos informáticos.

- **Ser víctimas de delitos informáticos:** Existen varios tipos de delitos informáticos enumerados en la ley colombiana de delitos informáticos 1273 de 2009, la cual tiene sanciones y consecuencias para el delincuente informático. Es necesario que las pymes tengan conocimiento que desde el momento en que un sistema informático almacene su información y que hablando del tema del comercio electrónico en Colombia se implemente la infraestructura tecnológica necesaria para poder operar sus ventas a través de Internet se exponen al riesgo de ser

víctimas de delitos informáticos con consecuencias graves si no son identificados y mitigados los riesgos de forma correcta.[44]

Otras de las consecuencias son de parte de los clientes, la perdida de respeto y credibilidad al buen nombre de algún vendedor, por suplantación, disponibilidad de productos inexactos, productos de calidad diferente a los que se ofrece, inexactitud en los datos de los clientes, entre otros factores que afectan la credibilidad y buen nombre de la organización.[45]

También se hace necesario la inversión de recursos importantes en la aplicación de medidas de seguridad informática suficientes para proteger la información de transacciones en línea y datos personales de sus clientes para mitigar los riesgos de delitos informáticos. Por ejemplo, la no actualización del portal donde se ofrecen los servicios web causa fallas técnicas, indisponibilidad de productos y perdida de ventas.

6.2.1 Desventajas del comercio electrónico [46]

- Dependencia completa del Internet y acceso a las TIC en la empresa.
- Por la facilidad de acceso a las tecnologías para ofrecer productos y/o servicios se puede ser víctima de fraudes de compañías inexistentes o ilegales.

---

[44] ARANGO GRANADA, Luisa Fernanda. Comercio Electrónico, Los Riesgos Que Enfrenta América Latina Para Su Masificación. [en línea]. Trabajo de grado para optar por el título de Administradora de Negocios. Medellín. Universidad De San Buenaventura Seccional Medellín. Facultad De Ciencias Empresariales. Administración De Negocios.2013.76 p.[Consultado: 01 de mayo de 2021]. Disponible en: http://bibliotecadigital.usb.edu.co/bitstream/10819/2598/1/Comercio_Electronico_Riesgos_Arango_2013.pdf

[45] UNIVERSIDAD DE CUENCA FACULTAD DE INGENIERIA MAESTRIA EN TELEMÁTICA. Implementación de un prototipo de tienda virtual sobre plataforma Linux para realizar transacciones de comercio electrónico seguro. [en línea] (30 de julio de 2010) [Consultado: 05 de diciembre de 2020]. Disponible en: https://dspace.ucuenca.edu.ec/bitstream/123456789/2530/1/tm4396.pdf

[46] PEÑA JIMENEZ, Yuber Javier. Comercio electrónico ventajas y desventajas. [en línea]. Bogotá D.C. Universidad Cooperativa de Colombia. Facultad de ciencias administrativas y económicas. Noviembre de 2019. [Consultado: 21 de abril de 2021]. Disponible en: https://repository.ucc.edu.co/bitstream/20.500.12494/16999/3/2019_Comercio_electronico_ventajas.pdf

- Falta de cultura por parte de los consumidores en el buen uso de las tecnologías para adquirir los productos y buenas prácticas de seguridad en los sistemas de pagos en línea disponibles y seguros.
- Se necesita de un presupuesto asignado para invertir en la creación de páginas y aplicaciones web optimas y seguras para sus clientes.
- Es necesario la inversión de recursos como tiempo y dinero importantes para promocionar profesionalmente sus productos y servicios.
- La rentabilidad por venta online puede ser inferior a las ventas presenciales puesto que el vendedor en la mayoría de las ocasiones debe realizar los envíos gratuitos asumiendo estos costos y en su mayoría en mensajería expresa para la atención oportuna del cliente, así mismo las comisiones que deben pagarse por venta en las aplicaciones usadas como mediadores en las transacciones, asumir costos derivados de devoluciones o daños durante el transporte.
- No se puede comercializar online cualquier tipo de producto y/o servicio y dependiendo del mismo limita los tipos de clientes y su ubicación geográfica.

6.3 REALIZACIÓN DE UN ANÁLISIS DE RIESGOS EN UNA PYME

En las pymes es necesario la realización de un análisis de riesgos que le permita entender sus activos informáticos, las vulnerabilidades, riesgos y amenazas a los que están expuestos para poder realizar una aplicación de controles que le ayude a mitigarlos y así estar más conscientes del riesgo de sus activos.

A continuación, se dará las pautas para aplicar un análisis de riesgos en una pyme:

6.3.1 Elija una metodología de análisis de riesgos más adecuada para su pyme:

Existen múltiples metodologías para la gestión del riesgo, a continuación, en la tabla 1, se explica las más usadas con sus ventajas y desventajas:

Tabla 1: Ventajas y desventajas metodologías gestión del riesgo.

Metodología de gestión del riesgo	Ventajas	Desventajas
MAGERIT[47]	▪ Es una metodología completa, para realizar el análisis, al igual que la gestión del riesgo. ▪ Este análisis puede ser cualitativo y cuantitativo. ▪ No requiere autorización para su uso dado que es libre. Los activos de la organización se segmentan en grupos para poder identificar los riesgos asociados y así mismo tomar las medidas necesarias para mitigar éstos. ▪ El archivo de inventarios es extenso en la referencia de las amenazas, tipos de activos y detalle de la información.	▪ Es costosa porque se deben convertir todos los valores a valores económicos. ▪ Se queda corto en cuanto a la información del inventario con relación a las políticas. ▪ No tiene en cuenta los procesos, recursos y vulnerabilidades como modelo a seguir.
CRAMM[48]	▪ Quien implementa es un grupo interdisciplinar de la empresa ▪ Ha sido usado en 23 países, es decir, que es una metodología internacional. ▪ Posee varias herramientas de aplicación de la metodología ▪ "Identifica y clasifica los activos de TI."[5] ▪ "Evalúa el impacto empresarial"[5].	▪ El costo del mantenimiento y la implementación del análisis es muy alto. ▪ Debe ser profesionales calificados y experimentados para el uso de la herramienta. ▪ Las revisiones completas se pueden dar tras mucho tiempo y aumenta la impresión de papel. ▪ Puede darse resultados insignificantes por las revisiones

[47] MARTOS, Fernando. Centros Hospitalarios de Alta Resolución de Andalucía-Auxiliares Administrativos. [en linea]. Primer Edición. España.2006. 195 p. [Consultado: 27 de mayo de 2021]. Disponible en: https://books.google.com.co/books?id=SmwP1cZdI4cC&pg=PA195&dq=LA+METODOLOG%C3%8DA+MAGERIT+3.0&hl=es&sa=X&ved=0ahUKEwiK5d7u_KTJAhUJWCYKHadoB14Q6AEIJTAC#v=onepage&q=LA%20METODOLOG%C3%8DA%2 0MAGERIT%203.0&f=false

[48] RIESGOS INFORMÁTICOS. [sitio web]. CRAMM. Marzo de 2014. [Consultado: 27 de mayo de 2021]. Disponible en: http://antonioinformatico.blogspot.com/2014/03/cramm.html

	▪ "Realiza el análisis de riesgos cuantitativo y cualitativo"[5]. ▪ Facilita la certificación de BS 7799 e ISO 17999	minuciosas que hace en el sistema
OCTAVE[49]	▪ Es un programa completo porque dentro de su modelo aplicativo el análisis lo hace a: procesos, dependencias, activos, vulnerabilidades, recursos, amenazas y salvaguardas. ▪ Es una metodología en que se puede gestionar y dirigir la evaluación de riesgos a través de un equipo que multitarea ▪ Este método esta focalizado en las fases de análisis y gestión del riesgo. ▪ Se puede inclusive involucrar a todo el personal.	▪ "No tiene como objetivo de seguridad el principio de No repudio de la información"[6]. ▪ Al utilizar grande volumen de documentos para el análisis hace de este proceso algo tedioso y complejo. ▪ Requiere de conocimientos técnicos importantes y complejos. ▪ "No es clara la definición de los activos de información"[6].
ISO 27005[50]	▪ Mayor aceptación por ser una metodología de estándar internacional ▪ Para monitorear y revisar riesgos utiliza una cláusula orientada totalmente a este proceso. ▪ Al realizar la justificación de riesgos se genera la aceptación el mismo. ▪ Todos los análisis son cuantitativos	▪ No tiene las herramientas o técnicas comparativas de ayuda para el caso de la implementación. ▪ No se puede certificar. ▪ No detalla la forma para valorar las amenazas.
ISO 31000[51]		

[49] DUQUE, Blanca. Metodologías de Gestión del Riesgo.[en línea] Auditoria. Universidad de Caldas, facultad de ingeniería. [Consultado: 27 de mayo de 2021]. Disponible en: https://auditoriauc20102mivi.wikispaces.com/file/view/Metodolog%C3%ACas+deGesti%C3%B2n+de+Riesgos.pdf

[50] VELASCO C. Ricardo. Gestión del riesgo basado en la norma ISO/IEC 27005:2009. [en línea] Universidad Piloto de Colombia. Enero de 2016. [Consultado: 28 de mayo de 2021]. Disponible en: http://polux.unipiloto.edu.co:8080/00002323.pdf

[51] Ventajas de implementar ISO 31000. [sitio web] Gestión Colombia.8 de abril de 2014. [Consultado: 27 de mayo de 2021]. Disponible en: https://gestioncolombiaconsultores.wordpress.com/2014/04/08/ventajas-de-implementar-iso-31000/

	▪ Esta metodología permite identificar las amenazas y oportunidades. ▪ Aumenta la seguridad y la confianza en los procesos. ▪ Mejora el aprendizaje organizacional. ▪ Reduce costo en implementación. ▪ Permite el análisis de incidencias. ▪ Permite un adecuado registro de los datos de los procesos en la organización.	Dificultad al cambio: Algunas empresas no pueden poner en práctica este tipo de métodos.
NIST 800-30[52]	▪ Facilita la certificación de BS 7799 e ISO 17999 ▪ Mayor aceptación por ser una metodología de estándar internacional. ▪ Bajo costo en cuanto al riesgo que se analiza y es solventado. ▪ En esta metodología se pueden asegurar todos los sistemas de información que procesan y trasmiten la información. ▪ Presenta de forma resumida la información de pruebas técnicas de seguridad con su respectiva evaluación y recomendaciones.	En esta metodología no se tiene en cuenta los activos ni sus respectivos procesos.
MEHARI[53]	• Esta metodología es de acceso público y aplicable para todo tipo de organizaciones.	• Solo se enfoca en los principios de la información como son su integridad, confidencialidad y disponibilidad.

[52] ELITE FORMACIÓN. Método de análisis de riesgos NIST SP 800-30. [sitio web]. Abril de 2018. [Consultado: 27 de mayo de 2021]. Disponible en: http://elite-formacion.blogspot.com/2018/04/metodo-de-analisis-de-risgos-nist-sp.html

[53] ALEMÁN NOVOA, H., & Rodríguez Barrera, C. Vista de Metodologías para el análisis de riesgos en los SGSI [en línea]. Publicaciones e Investigación. [Consultado: 28 de mayo de 2021]. Disponible en: https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874#:~:text=Las%20metodolog%C3%ADas%20Octave%2C%20MAGERIT%2C%20Mehari,riesgos%20m%C3%A1s%20robusto%20y%20eficiente.

	• Proporciona unos mecanismos para la gestión de riesgos alineada con ISO/IEC 27005:2008 • En todo su contexto es un procedimiento de para auditar e identificar vulnerabilidades y basados en ellos realizar una evaluación de riesgos	• Los controles se realizan en la gestión de los riesgos
CORAS[54]	• Provee una librería de casos que se pueden reutilizar • Se basa en la elaboración de modelos para el análisis de riesgos. • Tiene edición grafica basados en Microsoft Visio donde se diseñan los modelos de lenguaje • Proporciona unas pautas de trabajo orientado a sistemas críticos.	• No contempla dependencias ni procesos en la organización
EBIOS	• Proporciona guías y herramientas de código libres enfocada a gestores del riesgo de TI • Promueve una comunicación asertiva dentro de la organización entre sus empleados y sus aliados estratégicos de negocios • Se alinea con los últimos estándares de las normas ISO 27001, 27005 y 31000 • Herramienta de negociación, argumentación y arbitraje.	• Tiene características de herramientas de soporte y no de modelo de SGSI

Fuente: Elaboración propia.

Posterior a elegir la metodología debe seguir las pautas que dicte la misma. Para hacer una ejemplificación en términos generales de un análisis de riesgos en una pyme colombiana en tecnología y el comercio electrónico, se va a simular una pyme que elige la metodología MAGERIT.

[54] Análisis y valoración de los riesgos: Metodologías. [en línea]. 2011. [Consultado: 28 de mayo de 2021]. Disponible en: https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-8.pdf

6.3.2 Defina el alcance de su análisis de riesgos:

Es muy importante antes de iniciar con un análisis de riesgos conocer el alcance que el mismo va a tener, para continuar con el ejemplo se va a elegir que este análisis de riesgo va a tener únicamente alcance en el departamento de tecnología de la pyme, ya que el comercio electrónico usa 100% servicios digitales que dependen de la tecnología para su funcionamiento por ende se elige este alcance.

6.3.3 Realice un inventario detallado de activos de acuerdo con su metodología y alcance definidos anteriormente con su valoración:

Debe realizar el inventario de todos los activos que tengan valor para la pyme y por ende deban protegerse. Según MAGERIT [55] los activos son elementos o funciones en un sistema informático que sean vulnerables ante daños o ataques que sean significativos para una organización. Para poder categorizar los activos se debe tener en cuenta aquellos esenciales para el funcionamiento de la pyme por la información que contiene y los servicios prestados a la misma, se sugiere documentar el nombre del activo, el responsable, el tipo y su respectiva valoración.

A continuación, se enumera los tipos de activos en la metodología MAGERIT [56]:

[D] DATOS
[K] CLAVES CRIPTOGRAFICAS

[55] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. [en línea] Portal de Administración Electrónica Gobierno de España. Libro I-método. (2012). [Consultado: 29/05/2021] Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

[56] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. [en línea] Portal de Administración Electrónica Gobierno de España. Libro II-Catalogo de elementos. (2012). [Consultado: 29/05/2021] Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

[S] SERVICIOS

[SW] SOFTWARE

[HW] EQUIPAMENTO INFORMÁTICO

[COM] REDES DE COMUNICACIONES

[Media] SOPORTE DE INFORMACIÓN

[AUX] EQUIPAMENTO AUXILIAR

[L] INSTALACIONES

[P] PERSONAL

Para el ejemplo, en la tabla 2 se determinan los siguientes activos:

Tabla 2: Activos identificados en una pyme.

ACTIVOS DE INFORMACIÓN [1]											
No.	**DATOS DEL ACTIVO DE INFORMACIÓN**	**TIPO[57]**									
	Nombre del activo de información	[D] DATOS	[K] CLAVES CRIPTOGRAFICAS	[S] SERVICIOS	[SW] SOFTWARE	[HW] EQUIPAMENTO INFORMÁTICO	[COM] REDES DE COMUNICACIONES	[Media] SOPORTE DE INFORMACIÓN	[AUX] EQUIPAMENTO AUXILIAR	[L] INSTALACIONES	[P] PERSONAL
1	[backup] Copias de seguridad	X									
2	[email] Correo electrónico corporativo			X							
3	[idm] Administración de usuarios y contraseñas			X							

[57] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. [en línea] Portal de Administración Electrónica Gobierno de España. Libro II-Catalogo de elementos. (2012). [Consultado: 29/05/2021] Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

4	[av] Antivirus				X						
5	[print] Servidor físico					X					
6	[ftp] Servicio de FTP			X							
7	[file] Servidor de archivos FTP				X						
8	[san] Digitalización de documentos							X			
9	[www] Pagina web			X							
10	[www] Dominio de correo			X							
11	[www] Dominio de página web			X							
12	[dbms] Motor de base de datos				X						
13	[www] Lenguaje de programación de página web				X						
14	[site] Oficina de tecnología									X	
15	[firewall] Cortafuegos					X					
16	[pc] Equipo de computo					X					
17	[os] sistema operativo usado en los equipos de computo				X						
18	[switch] Switch					X					
19	[ipphone] Teléfonos IP					X					
20	[WIFI] Red WIFI						X				
21	[LAN] Red LAN						X				
22	[Internet] canal de ancho de banda dedicado						X				
23	[idm] Servidor DHCP			X							
24	[printed] Información impresa							X			
25	[int] Información impresa	X									
26	[HW] Servidor físico					X					
27	[USB] Memorias USB							X			

Elaboración propia. Referencia de Fuente: [1] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. [en línea] Portal de Administración Electrónica Gobierno de España. Libro II-Catalogo de elementos. (2012). [Consultado: 29/05/2021] Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

También se debe valorar cada activo identificado de acuerdo con su criticidad dentro de la pyme y así mismo su necesidad de protección. Este riesgo se puede medir basado en el impacto y la probabilidad, en este momento se va a evaluar el impacto, la probabilidad se evaluará en el siguiente paso donde se identifiquen las amenazas. Para el ejemplo se realiza la valoración de las dimensiones y el impacto basados en las tablas 3 y 4.

Tabla 3: Valoración del impacto en una pyme.

IMPACTO DEL RIESGO [2]			
	Nomenclatura	**Categoría**	**Valoración**
Impacto	MA	**Muy Alto**	4
	A	**Alto**	3
	M	**Medio**	2
	B	**Bajo**	1
	MB	**Muy Bajo**	0

Fuente:[2] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. [en línea] Portal de Administración Electrónica Gobierno de España. Libro I-método. (2012). [Consultado: 29/05/2021] Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

Basados en la tabla 3, se debe realizar la valoración de acuerdo con las dimensiones que menciona la metodología MAGERIT para los activos que son "la autenticidad, trazabilidad, confidencialidad, integridad y disponibilidad"[58]. Para el ejemplo en la tabla 4 se realiza la siguiente valoración cualitativa:

Tabla 4: Valoración del impacto por dimensión en una pyme.

VALORACION CUALITATIVA DE ACTIVOS POR DIMENSIONES [3]		
No.	**DATOS DEL ACTIVO DE INFORMACIÓN**	**DIMENSION[59]**

[58] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. [en línea] Portal de Administración Electrónica Gobierno de España. Libro I-método. (2012). [Consultado: 29/05/2021] Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

[59] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. [en línea] Portal de Administración Electrónica Gobierno de España. Libro I-método. (2012). [Consultado: 29/05/2021] Disponible en:

	Nombre del activo de información	Autenticidad (B / M /A / MA/ MB)	Trazabilidad (B / M /A / MA/ MB)	Confidencialidad (B / M /A / MA/ MB)	Integridad (B / M /A / MA/ MB)	Disponibilidad (B / M /A / MA/ MB)
1	[backup] Copias de seguridad	MA	B	MA	MA	MA
2	[email] Correo electrónico corporativo	MA	B	MA	MA	MA
3	[idm] Administración de usuarios y contraseñas	MA	B	MA	MA	MA
4	[av] Antivirus	B	B	MA	MA	MA
5	[print] Servidor físico	B	B	MA	MA	MA
6	[ftp] Servicio de FTP	MA	B	MA	MA	MA
7	[file] Servidor de archivos FTP	B	B	MA	MA	MA
8	[san] Digitalización de documentos	B	B	MA	MA	MA
9	[www] Pagina web	MA	B	MA	MA	MA
10	[www] Dominio de correo	MA	B	MA	MA	MA
11	[www] Dominio de página web	MA	B	MA	MA	MA
12	[dbms] Motor de base de datos	B	B	MA	MA	MA
13	[www] Lenguaje de programación de página web	B	B	MA	MA	MA
14	[site] Oficina de tecnología	B	B	MA	B	MA
15	[firewall] Cortafuegos	B	B	MA	MA	MA
16	[pc] Equipo de computo	B	B	MA	MA	MA
17	[os] sistema operativo usado en los equipos de computo	B	B	MA	MA	MA
18	[switch] Switch	B	B	MA	MA	MA
19	[ipphone] Teléfonos IP	B	B	MA	MA	MA
20	[WIFI] Red WIFI	B	B	MA	MA	MA
21	[LAN] Red LAN	B	B	MA	MA	MA

http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

22	[Internet] canal de ancho de banda dedicado	B	B	MA	MA	MA
23	[idm] Servidor DHCP	MA	B	MA	MA	MA
24	[printed] Información impresa	B	B	MA	MA	MA
25	[int] Información impresa	MA	B	MA	MA	MA
26	[HW] Servidor físico	B	B	MA	MA	MA
27	[USB] Memorias USB	B	B	MA	MA	MA

Elaboración propia. Referencia de Fuente: [3] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. [en línea] Portal de Administración Electrónica Gobierno de España. Libro I-método. (2012). [Consultado: 29/05/2021] Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

6.3.4 Realice el análisis de amenazas de sus activos con su respectivo impacto:

Las amenazas según MAGERIT [60] es todo aquello que cause daños o perdidas a los activos de su organización, la metodología los clasifica en los más comunes en general así:

[N] Desastres naturales
[I] De origen industrial
[E] Errores y fallos no intencionados
[A] Ataques intencionados

Hay que tener en cuenta que estas amenazas no afectan a la vez a todas las dimensiones de cada activo, cada una de las mencionadas tienen unas categorías de amenazas que mencionan la dimensión que afecta. Es necesario realizar la calificación de la probabilidad que las amenazas sean efectuadas en los activos, en la tabla 5 se indica cómo se evaluará en la metodología la probabilidad:

[60] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. [en línea] Portal de Administración Electrónica Gobierno de España. Libro I-método. (2012). [Consultado: 29/05/2021] Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

Tabla 5: Valoración de la probabilidad de riesgo en una pyme.

PROBABILIDAD DEL RIESGO [4]			
	Nomenclatura	**Categoría**	**Valoración**
Probabilidad	MA	**Seguro**	4
	A	**Probable**	3
	M	**Posible**	2
	B	**Poco probable**	1
	MB	**Muy raro**	0

Fuente: [4] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. [en línea] Portal de Administración Electrónica Gobierno de España. Libro I-método. (2012). [Consultado: 29/05/2021] Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

Así mismo es necesario identificar las vulnerabilidades que es todo lo que hace débil a un activo y esto puede ser explotado por una amenaza para que se ejecute un daño en éste. De esta manera se puede analizar si ya existen medidas que mitiguen esta vulnerabilidad o de reforzarla para que no se efectúe la amenaza en el mismo.

En la tabla 6 se puede apreciar que entonces el resultado de la valoración de un riesgo sobre un activo es el resultado de medir el impacto vs probabilidad tal cual lo define MAGERIT en su guía de técnicas.

Tabla 6: Valoración del riesgo de activos

VALORACIÓN DEL RIESGO [5]						
IMPACTO	**MA**					
	A					
	M					
	B					
	MB					
RIESGO		**MB**	**B**	**M**	**A**	**MA**
		PROBABILIDAD				

Fuente:[5] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. [en línea] Portal de Administración Electrónica Gobierno de España. Libro III-Guía de técnicas. (2012). [Consultado: 29/05/2021] Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

Para el ejemplo en la tabla 7 se mostrará dicha identificación mencionada anteriormente:

Tabla 7: Amenazas y vulnerabilidades de los activos

Activos de Información	Nombre del activo de información	Amenazas metodología MAGERIT	Vulnerabilidades
[D] DATOS	[backup] Copias de seguridad	[E18] Destrucción de información	El personal puede perder la información por mala configuración o manipulación de las copias de seguridad
[S] SERVICIOS	[email] Correo electrónico corporativo	[E19] Fugas de información	El usuario sin intención puede revelar información confidencial a personal no autorizado a través de correo electrónico.
[S] SERVICIOS	[idm] Administración de usuarios y contraseñas	[A5] Suplantación de la identidad del usuario	Una persona inescrupulosa puede adquirir credenciales de autenticación de alguien en la pyme, suplantarlo y así adquirir los privilegios del usuario suplantado.
[SW] SOFTWARE	[av] Antivirus	[E21] Errores de mantenimiento / actualización de programas (software)	Problemas en el mantenimiento del software que este actualizado y funcionando en las maquinas.
[S] SERVICIOS	[ftp] Servicio de FTP	[A5] Suplantación de la identidad del usuario	Un atacante se hace pasar por usuario autorizado para acceder al servicio y a los datos contenidos en él. Deficiente protocolo de cifrado de información.
[SW] SOFTWARE	[file] Servidor de archivos FTP	[A15] Modificación deliberada de la información	Algún usuario puede modificar la información guardada en el servidor FTP. Divulgación, secuestro y modificación de la información.
[Media] SOPORTE DE INFORMACIÓN	[san] Digitalización de documentos	[E15] Alteración accidental de la información	Puede existir la modificación de la información digitalizada con datos erróneos.
[S] SERVICIOS	[www] Pagina web	[E1] Errores de los usuarios	Los usuarios pueden presentar errores en la manipulación de la página web.

[S] SERVICIOS	[www] Dominio de correo	[E2] Errores del administrador	Puede existir una mala operación de la herramienta por parte del administrador.
[S] SERVICIOS	[www] Dominio de página web	[E2] Errores del administrador	Puede existir una mala operación de la herramienta por parte del administrador.
[HW] EQUIPAMENTO INFORMÁTICO	[firewall] Cortafuegos	[E2] Errores del administrador	El firewall podría contar con la configuración de fabrica la cual no segmenta las redes ni tampoco autoriza o deniega conexiones entrantes y salientes de la red LAN y WAN.
[HW] EQUIPAMENTO INFORMÁTICO	[pc] Equipo de computo	[E25] Pérdida de equipos	Se puede perder los equipos al no tener control de inventarios y asignación de estos.
[SW] SOFTWARE	[os] sistema operativo usado en los equipos de computo	[E8] Difusión de software dañino	El usuario puede propagar a otros equipos o la red de la institución de forma inocente software malintencionado desde sus equipos infectados
[HW] EQUIPAMENTO INFORMÁTICO	[switch] Switch	[A11] Acceso no autorizado	Un usuario puede conectarse directamente al equipo y acceder abusivamente a información o configuraciones.
[HW] EQUIPAMENTO INFORMÁTICO	[ipphone] Teléfonos IP	[A7] Uso no previsto	Puede usarse con fines personales por quien tenga acceso al teléfono.
[COM] REDES DE COMUNICACIONES	[WIFI] Red WIFI	[A14] Interceptación de información (escucha)	Un atacante desde cualquier acceso a la red WIFI alrededor o dentro del centro podrá monitorear la red y extraer información
[COM] REDES DE COMUNICACIONES	[LAN] Red LAN	[A9] [Re-]encaminamiento de mensajes	Si la configuración de la red lógicamente no está segmentada, es más fácil el redireccionamiento de paquetes de toda la red a destinos fraudulentos.
[COM] REDES DE COMUNICACIONES	[Internet] canal de ancho de banda dedicado	[E24] Caída del sistema por agotamiento de recursos	Puede ocurrir una caída de Internet por falta de control en el uso del recurso.

[HW] EQUIPAMENTO INFORMÁTICO	[HW] Servidor físico	[I7] Condiciones inadecuadas de temperatura o humedad	El servidor puede tener condiciones de climatización poco óptimas.
[S] SERVICIOS	[idm] Servidor DHCP	[A24] Denegación de servicio	Puede colapsar este servicio por no haber una adecuada configuración lógica en la red.
[L] INSTALACIONES	[site] Oficina de tecnología	[A11] Acceso no autorizado	Puede presentarse accesos no autorizados al no tener un sistema de seguridad físico que restrinja el acceso a personal no permitido.
[D] DATOS	[int] Información impresa	[E1] Errores de los usuarios	Personas pueden dar información incompleta, errónea, falsa o manipular incorrectamente la información.
[S] SERVICIOS	[www] Pagina web	[A4] Manipulación de la configuración	Se puede realizar ataques para suplantar un servidor legítimo y así obtener información de los usuarios que visitan la página web.
[HW] EQUIPAMENTO INFORMÁTICO	[pc] Equipo de computo	[A8] Difusión de software dañino	Se puede instalar un malware en el equipo que pueda difundirse rápidamente por la red y ejecutarse comandos remotos por el atacante sin control.
[HW] EQUIPAMENTO INFORMÁTICO	[firewall] Cortafuegos	[A6] Abuso de privilegios de acceso	Se puede vulnerar el ingreso al dispositivo obteniendo las credenciales de acceso por cualquier tipo de ataque y obtener y cambiar la configuración de este.
[HW] EQUIPAMENTO INFORMÁTICO	[switch] Switch	[A14] Interceptación de información (escucha)	Se puede obtener la información que está viajando a través de software que permita escuchar el tráfico y descifrarlo.
[HW] EQUIPAMENTO INFORMÁTICO	[switch] Switch	[E19] Fugas de información	Un atacante no autenticado puede generar reenvío de tráfico.

[P] PERSONAL	[backup] Copias de seguridad	[A30] Ingeniería social (picaresca)	El personal puede perder la información por mala configuración o manipulación de las copias de seguridad
[S] SERVICIOS	[www] Pagina web	[A15] Modificación deliberada de la información	Ataque de malware a la página con el fin de crear interrupción del servicio, modificación de información y/o pérdida completa de la misma
[S] SERVICIOS	[email] Correo electrónico corporativo	[A8] Difusión de software dañino	El usuario sin conocimiento puede generar apertura de enlaces que permiten ingreso de malware
[L] INSTALACIONES	[site] Oficina de tecnología	[N2] Daños por agua	Puede presentarse daño de los equipos, por falta de mantenimiento del sistema de aire acondicionado.
[L] INSTALACIONES	[site] Oficina de tecnología	[N1] Fuego	El cuarto de servidores si no cuenta con un sistema adecuado de regulación de energía, por tanto, se aumentan las probabilidades de ocurrencia de accidentes.
[Media] SOPORTE DE INFORMACIÓN	[USB] Memorias USB	[E2] Errores del administrador	Al no bloquear los puertos USB los usuarios pueden extraer información a través de los equipos, vital para la empresa.
[SW] SOFTWARE	[dbms] Motor de base de datos	[E15] Alteración accidental de la información	Puede existir alguna modificación en la base de datos de la pyme
[SW] SOFTWARE	[www] Lenguaje de programación de página web	[E20] Vulnerabilidades de los programas (software)	Puede existir errores en el código fuente de la aplicación
[SW] SOFTWARE	[www] Lenguaje de programación de página web	[E19] Fugas de información	Se puede revelar información por ataques al Código fuente

Elaboración propia y referencia de fuente:[5] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. [en línea] Portal de Administración Electrónica Gobierno de España. Libro II-Catalogo de elementos. (2012). [Consultado: 29/05/2021] Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

Posteriormente se realizan los cálculos que emite la metodología en cuanto a los cálculos de riesgo, criticidad y gestión, así mismo los niveles de aceptación del riesgo para así mismo hacer el debido tratamiento de riesgos.

6.3.5 Realice la evaluación y aplicaciones de salvaguardas o controles:

Es necesaria la implementación de salvaguardas o controles basados en la norma ISO 27001 Anexo A para mitigar estos riesgos identificados, para conocer las buenas prácticas para la aplicación de dichas salvaguardas remitirse al capítulo 4.

7 NORMATIVIDAD DE SEGURIDAD INFORMÁTICA QUE SE DEBE CONOCER EN EL COMERCIO ELECTRÓNICO APLICADO A LAS PYMES COLOMBIANAS.

El comercio electrónico como actividad de comercialización de bienes y/o servicios donde se utiliza las TIC como herramienta principal para poder llevar a cabo esta actividad, también es necesario alinearse a las diversas leyes y normas que regulen esta actividad y así mismo hacer del comercio electrónico más seguro y confiable para compradores, vendedores e intermediarios. A continuación, se recomendará las leyes y normas que se deben tener en cuenta para la implementación de comercio electrónico en una pyme colombiana.

- **LEY 527 DE 1999** [61] **:** Esta es la ley de comercio electrónico colombiana donde se introduce el reglamento para la gestión de los datos referentes al comercio electrónico, firmas digitales y también entidades de certificación.

  En esta ley se solidifica el desarrollo del comercio electrónico en Colombia donde se reconoce entre los conceptos principales: comercio electrónico, sistemas de información, entidades de certificación, firma digital e introduce la validez jurídica

[61] Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. Agosto 21 de 1999. Diario Oficial No 43673.

y probatoria de los mensajes de datos entendidos en la ley como “La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax”[62] lo cual abre la puerta a la validez jurídica y probatoria con igualdad tanto a los datos contenidos en los medios digitales como los tradicionales físicos e introduce el uso de las TIC como medios legales y controlados para hacer comercio electrónico. También la ley en su artículo 29 [63] otorga facultades a la Superintendencia de Industria y Comercio (SIC) para que autorice a las entidades de certificación dentro del marco de comercio electrónico, con base en las condiciones especificadas en dicha ley en todo el territorio nacional.

De esta manera se puede establecer esta ley como base para tener en cuenta por parte de las pymes colombianas y sus clientes, tal como Rincón plantea que los consumidores y empresarios pueden superar algún obstáculo relacionado con la seguridad de la jurídica, si se establecen atributos propuestos y aplicados por otras normas y que permitieron garantizar la disponibilidad, confidencialidad e integridad de la información con el fin de dar un tratamiento semejante donde se relacione además el buen uso de medios electrónicos. [64]

- **LEY 1266 DE 2008:** Esta ley estatutaria más comúnmente conocida como Ley de Habeas Data [65] donde se brindan todas las regulaciones sobre los datos privados

[62] Articulo 2 Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. Agosto 21 de 1999. Diario Oficial No 43673.
[63] Articulo 29 Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. Agosto 21 de 1999. Diario Oficial No 43673.
[64] Rincón Cárdenas Erick. Uso de medios electrónicos (I). La Ley 527 de 1999 como instrumento normativo suficiente. Legis Ámbito jurídico. [en línea] (12 de junio de 2017) [Consultado: 31/03/2021]. Disponible en: https://www.ambitojuridico.com/noticias/tic/uso-de-medios-electronicos-i-la-ley-527-de-1999-como-instrumento-normativo-suficiente
[65] Ley 1266 de 2008.Por medio de la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en base de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diciembre 31 de 2008.Diario Oficial No 47.219.

de los ciudadanos almacenados en bases de datos de entidades de diferentes tipos de actividades que sean usadas con fines comerciales, publicitarios, entre otras.

Es importante tener esta ley en cuenta para la aplicación en el comercio electrónico de las pymes colombianas, puesto que al hacer transacciones de compra y venta de productos y/o servicios, se obtienen datos de información personal de los usuarios que interactúan en las transacciones antes dichas y así mismo entra en administración de la pyme esta información almacenada en sus bases de datos. De esta manera la pyme debe comprometerse con el principio de la seguridad informática que es la confidencialidad, tal como lo contempla la ley en su artículo 2. "Esta ley se aplicará sin perjuicio de normas especiales que disponen la confidencialidad o reserva de ciertos datos o información registrada en Bancos de datos de naturaleza pública, para fines estadísticos, de investigación o sanción de delitos o para garantizar el orden público."[66] De esta manera los datos personales tendrán un adecuado tratamiento siempre respetando el derecho de los ciudadanos de solicitar realizar cualquier acción sobre los datos personales que se encuentran almacenados en documentos, bases de datos y sistemas informáticos, mediante PQR'S ante las entidades y la SIC. De no cumplir con esta ley estará sujeta la pyme a sanciones dispuestas por parte de la Superintendencia de industria y comercio.

- **DECRETO 1377 DE 2013:** Este decreto está directamente relacionado con la Ley 1581 de 2012 y por ende es importante tenerlo en cuenta puesto que este decreto como menciona en su título "Que con el fin de facilitar la implementación y cumplimiento de la Ley 1581 de 2012 se deben reglamentar aspectos relacionados con la autorización del Titular de información para el Tratamiento de sus datos

[66] Articulo 2 Ley 1266 de 2008.Por medio de la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en base de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diciembre 31 de 2008.Diario Oficial No 47.219.

personales, las políticas de Tratamiento de los Responsables y Encargados, el ejercicio de los derechos de los Titulares de información, las transferencias de datos personales y la responsabilidad demostrada frente al Tratamiento de datos personales, este último tema referido a la rendición de cuentas."[67]

- **LEY 1273 DE 2009:**[68] Esta ley mejor conocida como ley de delitos informáticos agrega al código penal colombiano la protección de los datos e información almacenada en los sistemas informáticos de una organización. En esta ley se reconocen todas las acciones denominadas delitos informáticos que atenten contra los principios de la seguridad de la información almacenada en las organizaciones y sus sistemas informáticos que las contienen y enumera por cada uno de ellos las sanciones correspondientes.

- **LEY 1480 DE 2011: [69]** Esta ley mejor conocida como ley de protección al consumidor donde se garantizan sus derechos de educación, acceso a información veraz que les permita realizar elecciones acertadas frente a los productos y/o servicios que consumen, oportunidades de emitir sus opiniones e inquietudes frente a estos, y también regula la responsabilidad de las entidades frente a los consumidores. Es muy importante que en el momento de realizar la comercialización de los productos o servicios en una pyme tenga en cuenta esta ley para que pueda dar cumplimiento a los derechos de sus clientes a conocer la información adecuada de los mismos y su responsabilidad frente a la atención de sus opiniones frente a éstos.

---

[67] Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Junio 27 de 2013.Diario Oficial No 48.834.

[68] Ley 1273 de 2009.Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Enero 5 de 2009.Diario Oficial No 47.223.

[69] COLOMBIA.CONGRESO DE LA REPUBLICA. Ley 1480 de 2011. (12 de octubre de 2011). Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones. [en línea]. Bogotá D.C. Diario Oficial No. 48.220.[Consultado: 27 de mayo de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1480_2011.html

- **LEY 1581 DE 2012:**[70] Esta ley de protección de datos personales garantiza los derechos constitucionales de las personas de realizar gestiones sobre sus datos personales almacenados en los sistemas informáticos de una organización. Además de esto define una nueva categorización de los datos como sensibles que son aquellos que afectan la privacidad del titular y/o son controversiales por su exposición o mal manejo de estos, en este tipo de datos la ley prohíbe su tratamiento sin autorización firmada y explicita del titular y define otras condiciones para los mismos. También esta ley define los roles, derechos y deberes de los titulares de la información como de los encargados de tratar los datos, por ende, es importante conocer y aplicar esta ley a cabalidad para cumplir con lo demandado por esta y garantizar seguridad en el comercio electrónico para sus clientes.

- **DOCUMENTO CONPES 4012:**[71] Es un documento donde se impulsa el comercio electrónico a través de una política pública nacional que genere las condiciones técnicas y económicas para el uso del comercio electrónico y todos los temas que lo derivan tanto de ciudadanos como de las pymes en Colombia y así mismo proveer actualizaciones normativas con acuerdos institucionales que garanticen la ejecución de este documento los próximos 5 años hasta 2025. En este documento las pymes pueden visualizar de forma trasversal los procesos y acuerdos que ejecutarán las distintas entidades en materia de comercio electrónico y así mismo las actualizaciones normativas según aplique en su actividad económica.

[70] COLOMBIA.CONGRESO DE LA REPUBLICA. Ley 1581 de 2012. (18 de octubre de 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. [en línea]. Bogotá D.C. Diario Oficial No. 51.657 [Consultado: 27 de mayo de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

[71] REPÚBLICA DE COLOMBIA.CONSEJO NACIONAL DE POLITICA ECONOMICA Y SOCIAL CONPES. Documento CONPES 4012. 30 de noviembre de 2020.Politica Nacional de comercio electrónico. [en línea] Bogotá. Departamento Nacional de planeación. [Consultado: 27 de mayo de 2021]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/4012.pdf

- **INSTRUMENTO DE EVALUACIÓN MSPI**:[72] Este instrumento de evaluación es muy importante a tener en cuenta en su negocio puesto que le permitirá analizar y gestionar el estado de la implementación de los controles de seguridad informática y así mismo el diseño e implementación de un plan de seguridad de la información que mejore en gran medida sus medidas frente a la ciberseguridad.

8 GUÍA DE BUENAS PRÁCTICAS DE SEGURIDAD INFORMÁTICA EN EL COMERCIO ELECTRÓNICO PARA LAS PYMES COLOMBIANAS.

Posterior al realizar un análisis de riesgos según el capítulo 7 de este mismo documento, se debe aplicar medidas que protejan los activos de información disminuyendo de esta manera el riesgo encontrado a través de la implementación de los controles en la norma ISO 27001:2013 Anexo A.

8.1 "A.10 CRIPTOGRAFÍA, A.10.1 CONTROLES CRIPTOGRÁFICOS, A.10.1.1 POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS, A.10.1.2 GESTIÓN DE LLAVES"[73]

La criptografía es esencial para una adecuada transmisión de información en una pyme especialmente en el proceso del comercio electrónico.

Criptografía: Aguilera López [74] La criptografía es la ciencia que permite que entre un emisor y receptor puedan comunicarse de forma segura a través de mensajes que

[72] Colombia. Ministerio de Tecnologías de la Información y las Comunicaciones. Instrumento de Evaluación MSPI. [en línea]. Bogotá D.C. Disponible en: https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/#:~:text=*El%20%22Instrumento%20de%20Evaluaci%C3%B3n%20MSPI,al%20interior%20de%20las%20Entidades

[73] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología De La Información. Técnicas De Seguridad. Sistemas De Gestión De La Seguridad De La Información. Requisitos. NTC-ISO 27001.Bogotá D.C. El Instituto. 2013. 33 p.

[74] Aguilera Lopez, Purificación. Seguridad informática. Editorial Editex. (pp. 167 - 170). [Consultado el 13 de abril de 2021]. Disponible en:

únicamente sean entendibles por ellos transformando o cifrando los mensajes enviados y así mismo sea indescifrable por externos a la comunicación. Hernández L. [75] afirma que de esta manera esta ciencia usa ciertas reglas que permiten que se modifique el contenido del mensaje, no ocultan la existencia de este, pero permite que pueda recuperarse, volverse claro y entendible nuevamente para el receptor. Así mismo permite que se conserven los principios de confidencialidad, integridad, autenticidad, disponibilidad y no repudio de la información contenida en el mensaje.

Al comprender que es la criptografía y lo que le aporta a una pyme, a continuación, tendrá las recomendaciones adecuadas para poder aplicarla:

Debe crear e implementar una política sobre la aplicación de controles criptográficos en su organización: De acuerdo con la evaluación de riesgos que se realice sobre los activos, se debe definir el tipo y complejidad de algoritmo de encriptación para aplicar tanto en la transmisión de la información como en el almacenamiento de esta. También es importante definir los roles de las personas que se van a incluir durante el diseño, aprobación e implementación de esta política.

Implementar una adecuada gestión de llaves criptográficas: El documentar políticas y procedimientos de una gestión adecuada de las llaves criptográficas se vuelve indispensable para evitar ser afectados frente a las diferentes amenazas que afrontan estas llaves para descifrar, modificar y/o exponer la información transmitida.

https://books.google.com.co/books?id=Mgvm3AYIT64C&lpg=PA167&dq=que%20es%20criptografia&hl=es&pg=PA167#v=onepage&q&f=false

[75] Hernández, Luis. (2016). Criptografía. España: Editorial CSIC. (pp. 17-23) [Consultado el 13 de abril de 2021]. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/41843?page=17

8.2 "A.12. SEGURIDAD EN LA OPERATIVA, A.12.2 PROTECCIÓN CONTRA CÓDIGO MALICIOSO, A.12.2.1 CONTROLES CONTRA EL CÓDIGO MALICIOSO" [76]

Es imprescindible la aplicación de este control puesto la infección por códigos maliciosos es muy común y debe disminuirse los riesgos de ser víctimas de delitos informáticos en la organización y si es víctima el tener la facultad de recuperación, por ende, se sugiere aplicar las siguientes recomendaciones para que sea exitoso la implementación de este:

8.2.1 Implemente controles para detectar, retirar y evitar códigos maliciosos:

Instale y mantenga actualizado el software de protección de malware en todas las estaciones de trabajo de su organización: Existen múltiples soluciones en el mercado donde cada una ofrece diferentes tipos de licencias, formas de funcionamiento, precios y rendimiento. A continuación, se sugiere algunos aspectos para tener en cuenta:

- Se debe analizar rigurosamente cuales son las necesidades de la organización en cuanto al inventario de activos como computadores, servidores y estaciones de trabajo que puedan ser afectadas ante un ataque de software malicioso para de este modo poder tener claro cuáles son los requerimientos y así mismo escoger la solución más acertada en dinero y efectividad.
- Seleccione una solución de seguridad que sea eficiente evitando y eliminando todo tipo de infección de software malicioso, para esto puede analizar el porcentaje de detección y eliminación de malware activo ha realizado cada solución.
- Tenga en cuenta que la solución de seguridad debe actualizar todo el tiempo las bases de datos de software malicioso

[76] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología De La Información. Técnicas De Seguridad. Sistemas De Gestión De La Seguridad De La Información. Requisitos. NTC-ISO 27001.Bogotá D.C. El Instituto. 2013. 33 p.

- Seleccionar una solución que no afecte de forma notablemente el rendimiento de los activos seleccionados para tener esta protección [77]
- Escoger la solución de seguridad que le garantice protección en tiempo real y ataques de día cero y/o machine learning en todos sus activos seleccionados para esta protección, de esta manera estará protegido todo el tiempo y sobre todo contra malware que no se encuentre en las bases de datos de software malicioso aún.
- Preferir soluciones integrales donde incluya topo tipo de archivos, transacciones web, todas las entradas de ingreso de información nueva a su dispositivo por cualquier medio como correo, red, internet, USB, entre otros y así mismo puedan ser inspeccionadas por la solución y no tenga que implementar varias soluciones para lograr esta protección integral.[78]

8.2.2 Implemente una solución de correo electrónico que le permita configurar una adecuada seguridad en el uso de éste:

El correo electrónico es un canal indispensable para la comunicación con los clientes y proveedores en una pyme por ende es muy importante implementar medidas de seguridad que le garantice la prevención y mitigación de ataques informáticos y buena gestión de gobernanza de datos a través de este medio. Existen diversas soluciones de correo electrónico para elegir por lo cual se le sugiere tener en cuenta las siguientes recomendaciones:

- Prefiera elegir soluciones de correo electrónico en la nube y no soluciones On-premise donde la solución de correo electrónico en la organización sea realizada en un servidor local con aplicaciones locales, aunque esta solución es aceptable no es la más recomendada en cuanto costos de administración, mantenimiento,

[77] KASPERSKY. ¿Como Borrar Software Malicioso?.2021. [Consultado: 22 de mayo de 2021]. Disponible en: https://latam.kaspersky.com/resource-center/preemptive-safety/removing-malicious-code
[78] KASPERSKY. Elección de una solución antivirus.2021. [Consultado: 22 de mayo de 2021]. Disponible en: https://latam.kaspersky.com/resource-center/preemptive-safety/antivirus-choices

seguridad de la información almacenada en el mismo, entre otras desventajas que este tipo de soluciones presentan frente a las soluciones Cloud que son más seguras y eficientes en su funcionamiento con costos de acuerdo a la necesidad.[79]

- Debe tener en cuenta el tipo de licencias con el que cuenta cada proveedor puesto que la mayoría de los proveedores segmentan el tipo de licencias y soluciones que la integran de acuerdo con las necesidades, siempre debe priorizar las garantías en cuanto a la seguridad y configuraciones que ofrecen como protección de virus en los mismos, doble factor de autenticación, prevención de perdida de datos, confiabilidad, soporte, redundancia, espacio de almacenamiento, costos, entre otros factores.[80]

8.2.3 Realice jornadas de capacitación y sensibilización de los usuarios en su organización:

Es determinante para tener éxito en la implementación de medidas de seguridad informática en una empresa la sensibilización y capacitación de los empleados puesto que si esto no es tenido en cuenta pueden fallar más fácilmente todas las medidas implementadas por software y el personal de seguridad informática.

La realización de estas jornadas de sensibilización ayudará a que los empleados entiendan sus responsabilidades y deberes que desempeñan en la seguridad informática de la pyme y así mismo se fortalezcan los conocimientos y habilidades en el manejo de la información para garantizar el adecuado uso y la protección de esta. También para estas jornadas sean exitosas deben darse en lenguaje adecuado que entienda el usuario final con actividades interactivas con ejemplos

[79] RUIZ, Francisco Javier.On Premise, servidores y problemas frente a solución Cloud. [blog] Blog de Dataprius.17 de junio de 2016
[Consultado: 22 de mayo de 2021]. Disponible en:https://blog.dataprius.com/index.php/2016/06/17/on-premise-servidores-problemas-solucion-cloud/
[80] Proveedor de Servicios de Email. [sitio web] .Ryte Wiki.[Consultado: 23 de mayo de 2021].Disponible en:https://es.ryte.com/wiki/Proveedor_de_Servicios_de_Email

y demostraciones reales y fáciles de comprender para que el usuario pueda descubrir sus errores, debilidades y pueda corregirlos de forma permanente.[81]

Se sugiere que sea elaborado un plan de capacitación y sensibilización de usuarios en la pyme [82]donde se pueda estructurar y tenga unas fases claras para el personal de tecnología para la ejecución y que éstas sean consecutivas en el tiempo tales como:

- **Planificación:** Durante esta etapa es primordial identificar cuales conocimientos se desean impartir, las falencias que presentan los usuarios en temas de seguridad informática y la metodología educativa a utilizar usando sesiones interactivas, fáciles de comprender, aplicadas a la vida cotidiana y garantizando la participación del personal en actividades y evaluaciones para hacer seguimiento de estas. Este plan en este punto debe ser aprobado por los directivos y realizar las inversiones que se requieran para poder ejecutar el mismo.
- **Implementación:** En esta etapa es importante implementar estrategias para impartir dicho plan anteriormente planteado, es necesario incluir a todos los miembros de la pyme dando obligatoriedad a las sesiones para garantizar que el conocimiento llegue a todos los empleados y así mismo establecer roles que permitan identificar inasistencia y participación del personal.
- **Monitoreo y evaluación:** Posterior a la ejecución del plan es necesario revisar las evaluaciones que se debieron realizar a los usuarios para

[81] VARGAS SALCEDO, Julio Cesar. Campañas de concientización en seguridad de la información dirigidas a usuarios finales como método de ayuda para la mitigación del riesgo sobre los datos de la empresa. Fundación Universidad Piloto de Colombia. [Consultado: 23 de mayo de 2021]. Disponible en: http://polux.unipiloto.edu.co:8080/00004663.pdf

[82] PLAN DE CONCIENCIACIÓN DE SEGURIDAD INFORMÁTICA.2021.Ciberseguridad:Noticias de ciberseguridad, ciberataques, vulnerabilidades informaticas.[Consultado: 23 de mayo de 2021]. Disponible en:https://ciberseguridad.com/normativa/espana/medidas/plan-concienciacion/#Establecer_responsabilidad

identificar oportunidades de mejora en la metodología o en la información que desean conocer los usuarios y así mismo realizar mejoras constantes sobre este plan, esto debe hacerse periódicamente y utilizar mediciones que permitan conocer la efectividad de estas.

8.3 "12.3 COPIAS DE SEGURIDAD, 12.3.1 COPIAS DE SEGURIDAD DE LA INFORMACIÓN"[83]

Este control es muy importante en el ejercicio de cualquier actividad donde se usen sistemas informáticos y datos como lo son los obtenidos a través del comercio electrónico, puesto que van a garantizar tener un respaldo de todos los datos importantes y todos los sistemas informáticos en la organización que los almacena. El tener copias de seguridad es una estrategia clave según la norma ISO 27002[84] para mantener los principios de disponibilidad e integridad de la información puesto que ante ser víctimas de delitos informáticos, fallas técnicas, perdida de datos, daños físicos, entre otros, la pyme pueda recuperarse y no afectar los servicios prestados a los clientes. Para su aplicación se sugiere:

8.3.1 Realizar políticas y procedimientos para la realización de backup y pruebas de restauración de estos:

Es importante elaborar documentación y procedimientos sobre el detalle de los backup a realizar en sus activos tecnológicos que almacenen información, la periodicidad en la que se van a ejecutar, tipos de backup a ejecutar, extensiones del backup, el lugar de almacenamiento, etiquetado, políticas de tratamiento de backup y también un cronograma con las pruebas periódicas de funcionamiento de los backup realizados, todo

[83] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología De La Información. Técnicas De Seguridad. Sistemas De Gestión De La Seguridad De La Información. Requisitos. NTC-ISO 27001.Bogotá D.C. El Instituto. 2013. 33 p.

[84] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología De La Información. Técnicas De Seguridad. Código de práctica para la gestion de la seguridad de la información.NTC-ISO 27002.Bogotá D.C. El Instituto. 16 de noviembre de 2007. 144 p.

lo anterior también definiendo roles y responsabilidades en cuanto al personal que va a ejecutar estos procesos.

8.3.2 Implementar soluciones que permitan la realización de backup de software, bases de datos y todos los datos para recuperarse ante un desastre o ataque:[85]

Existen múltiples soluciones tecnológicas para la realización de copias de seguridad en sus sistemas informáticos que brindan diferentes tipos de servicios, coberturas y funcionamiento y así mismo el costo, para no excederse en presupuesto y escoger la solución más acertada para su negocio debe tener en cuenta las siguientes recomendaciones:

- Antes de elegir la solución para hacer sus copias de seguridad debe previamente haber realizado el inventario de activos tecnológicos que necesitan que se les realice copias de seguridad, su criticidad y periodicidad.
- También debe analizar y tener claro la infraestructura tecnológica de su organización sea On-premise, Cloud o hibrida[86], de esto depende el tipo de solución que se valla adoptar y si es necesaria, esto porque las soluciones Cloud en algunos de sus contratos garantizan copias de seguridad, hay que revisar las condiciones y lo contratado, de lo contrario hay que elegir el software de acuerdo con sus necesidades.
- Debe tener en cuenta los costos de acuerdo con su presupuesto y sus necesidades, hay soluciones que tiene licencias gratuitas o de uso libre cuando su

[85] CORONEL CUADROS, Daniel. Procedimiento para realizar el respaldo de información siguiendo las buenas prácticas en una empresa de Contact Center. [en línea].Universidad Católica de Colombia. FACULTAD DE INGENIERIA. PROGRAMA DE INGENIERÍA DE SISTEMAS.BOGOTA D.C.2013.138 p [Consultado: 23 de mayo de 2021]. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/860/2/PROCEDIMIENTO%20PARA%20REALIZAR%20EL%20RESPALDO%20DE%20INFORMACI%C3%93N%20SIGUI.pdf

[86] Datacenter On-Premise vs Cloud. [sitio web]. Beservices.20 de octubre de 2020. [Consultado: 25 de mayo de 2021].Disponible en:https://www.beservices.es/datacenter-on-premise-vs-cloud-n-5456-es

infraestructura no es muy grande, o existen soluciones con licencias pagas que puede aprovisionar y usar de acuerdo con su caso con mejores condiciones de funcionamiento en cuanto a licencias y coberturas, mayor capacidad de backup, manejo de encriptación de los backup entre otras configuraciones que pueda requerir en particular para garantizar mayor seguridad y eficiencia , en cualquier caso, revise las condiciones de uso, sus requerimientos y funcionamiento.

8.3.3 Elegir los medios para almacenar las copias de seguridad y sus condiciones de almacenamiento:

De acuerdo con la solución de seguridad elegida es necesario elegir los medios de almacenamiento apropiado de las copias de seguridad. Por ejemplo, [87]si su solución usa un robot físico y necesita el uso de cintas magnéticas debe elegir cintas magnéticas de calidad, definir el adecuado etiquetado, y tiempo de retención. Así mismo debe elegir si estas cintas van a estar almacenadas en sus instalaciones o si se van a almacenar en un lugar externo o si va usar ambas opciones, en todo caso debe tener todo muy bien documentado a través de bitácoras o documentos que soporten el almacenamiento de las cintas. También hay soluciones que emiten sus copias de seguridad en medios digitales como USB, discos duros externos, SAN, Cloud, entre otras opciones que también deben ser adecuadamente marcadas de acuerdo con el tiempo de retención definido, documentadas y lugar de almacenamiento adecuado si aplica.

[87] ¿Conoces todos los sistemas de almacenamiento de datos? [sitio web]. Ambit.22 de octubre de 2020. [Consultado: 25 de mayo de 2021].Disponible en:https://www.ambit-bst.com/blog/conoces-todos-los-sistemas-de-almacenamiento-de-datos

CONCLUSIONES

1. La implementación del comercio electrónico en las pymes colombianas es imprescindible para su sostenimiento y desarrollo económico y del país, por esto, el gobierno colombiano ha implementado diferentes programas que benefician a las pymes en formación académica y acompañamiento de estas durante el proceso.

2. Durante la crisis de la pandemia mundial causada por el COVID-19 la digitalización de las pymes y el comercio electrónico se ha convertido en un medio imprescindible para la compra-venta de productos y servicios ofrecidos por las pymes en Colombia, por ende, es necesario que las pymes colombianas tengan en cuenta que existen vulnerabilidades digitales cuando se usan medios electrónicos para el comercio electrónico y se deben gestionar, en consecuencia, de no hacerlo podrían incluirse dentro de este 60% de las víctimas de delitos informáticos en los últimos años, que tienen consecuencias graves hasta el cierre definitivo de sus empresas colombianas.

3. Las pymes colombianas al tener sistemas de información que administran datos de sus clientes, información de proveedores y datos sensibles de la misma organización, deben tener en cuenta que es necesario regirse bajo la normatividad colombiana para no incurrir en sanciones, evitar amenazas informáticas y mantener un buen manejo de los sistemas informáticos.

4. La implementación de buenas prácticas de seguridad informática en el comercio electrónico en las pymes colombianas es vital para la preservación del funcionamiento, continuidad del negocio y buen nombre de las organizaciones, por ende, siempre al finalizar un análisis de gestión de riesgos es necesario implementar buenas prácticas que le permitan mitigar al máximo todos los riesgos informáticos y así mismo reducir las probabilidades de que las amenazas sean materializadas.

9 RECOMENDACIONES

1. Las pymes colombianas deben implementar el comercio electrónico como medio para vender sus productos y servicios, debido a que requieren la implementación de las herramientas tecnológicas para el funcionamiento del comercio electrónico, tales como las redes sociales, correo electrónico, plataformas de comercio, entre otras, que pueden impulsar ágilmente su crecimiento y visualización entre los consumidores. Así mismo, les faculta para participar de los beneficios que trae para su sostenimiento y crecimiento, la inclusión en los distintos programas que ofrece el gobierno colombiano, brindando el acompañamiento y formación académica necesarios para que aumente el conocimiento en sus empleados y logren perfilar mejores métodos de comercio electrónico.

2. Las pymes deben implementar un plan de gestión de riesgos que les permita su análisis, gestión y mitigación de estos y así evitar al máximo que las amenazas sean materializadas ya que de no implementarse las consecuencias pueden ser irreparables para el negocio.

3. Se recomienda que las pymes colombianas que hayan implementado el comercio electrónico implementen campañas de sensibilización tanto a sus empleados como al de sus clientes, invitarlos a utilizar medios digitales para realizar sus transacciones y cómo evitar ser víctimas de delitos informáticos.

4. Se recomienda para las pymes colombianas, optar por la implementación de mecanismos que puedan proteger toda la información, es necesario y deberían ser obligatorios, ya que la información de ninguna empresa en la actualidad se encuentra 100% protegida y sin esto podría traer grandes consecuencias. Después de implementar unas buenas prácticas de seguridad de la información, se recomienda seguir retroalimentando el mecanismo y fortaleciendo, junto con personal idóneo que

ayude a completar todos los objetivos planteados para la ejecución de dicho sistema informático.

5. El gobierno, así como ha generado campañas de capacitación a las pymes sobre el uso del comercio electrónico también debe intensificarse en su uso por parte de los clientes donde se motiven a sentirse seguros en el uso de estos medios y así mismo se incrementen las transacciones de compra y venta a través de Internet y plataformas seguras de comercio.

10 BIBLIOGRAFÍA

Acacia. Modelo de marketing por internet de empresa. [en línea]. [Consultado: 20 de noviembre de 2020]. Disponible en: http://acacia.org.mx/busqueda/pdf/MODELO_DE_MARKETING_POR_INTERNET_DE_EMPRESA.pdf

Aguilera López, Purificación. Seguridad informática. Editorial Editex. (pp. 167 - 170). [Consultado el 13 de abril de 2021]. Disponible en: https://books.google.com.co/books?id=Mgvm3AYIT64C&lpg=PA167&dq=que%20es%20criptografia&hl=es&pg=PA167#v=onepage&q&f=false

Aguilera, P., [en línea] n.d. Seguridad Informática. Madrid: Editex.

Alemán Novoa, H., & Rodríguez Barrera, C. Vista de Metodologías para el análisis de riesgos en los SGSI [en línea]. Publicaciones e Investigación. [Consultado: 28 de mayo de 2021]. Disponible en: https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874#:~:text=Las%20metodolog%C3%ADas%20Octave%2C%20MAGERIT%2C%20Mehari,riesgos%20m%C3%A1s%20robusto%20y%20eficiente.

Análisis y valoración de los riesgos: Metodologías. [en línea]. 2011. [Consultado: 28 de mayo de 2021]. Disponible en: https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-8.pdf

Arango Granada, Luisa Fernanda. Comercio Electrónico, Los Riesgos Que Enfrenta América Latina Para Su Masificación. [en línea]. Trabajo de grado para optar por el título de Administradora de Negocios. Medellín. Universidad De San Buenaventura Seccional Medellín. Facultad De Ciencias Empresariales. Administración De Negocios.2013.76 p. [Consultado: 01 de mayo de 2021]. Disponible en: http://bibliotecadigital.USB.edu.co/bitstream/10819/2598/1/Comercio_Electronico_Riesgos_Arango_2013.pdf

Articulo 2 Ley 1266 de 2008.Por medio de la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en base de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diciembre 31 de 2008.Diario Oficial No 47.219.

Articulo 2 Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. Agosto 21 de 1999. Diario Oficial No 43673.

Articulo 29 Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. Agosto 21 de 1999. Diario Oficial No 43673.

Bancoldex. ¿Qué es una pyme? [en línea]. Bogotá. 30 de julio de 2018. [Consultado: 13 de noviembre de 2020]. Disponible en: https://www.bancoldex.com/que-es-una-pyme-1338

Carpentier, J., La Seguridad Informática en la pyme: Situación Actual Y Mejores Prácticas. Barcelona: ENI-Ediciones. 2016.

CCCE. Informe: comportamiento del ecommerce en Colombia durante 2020 y perspectivas para 2021. [en línea].13 de octubre de 2020. [Consultado: 16 de diciembre de 2020]. Disponible en: https://www.ccce.org.co/gestion_gremial/informe-comportamiento-del-ecommerce-en-colombia-durante-2020-y-perspectivas-para-2021/

CCIT - Cámara colombiana de Informática y Telecomunicaciones. 2020. Empresas colombianas cada vez más en la mira de los ciberdelincuentes. [en línea] Disponible en: <https://www.ccit.org.co/noticias/safe-presenta-mejores-practicas-para-el-fortalecimiento-de-la-ciberseguridad-empresarial/>

Certicámara S.A. Así va la Ciberseguridad y su transformación en Latinoamérica. [en línea]. Bogotá. 2019. [Consultado: 13 de noviembre de 2020] Disponible en:

https://blogs.portafolio.co/seguridad-informatica-certicamara-sa/asi-va-la-ciberseguridad-transformacion-latinoamerica/

Colombia. Congreso de la república. Ley 1480 de 2011. 12 de octubre de 2011. Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones. [en línea]. Bogotá D.C. Diario Oficial No. 48.220. [Consultado: 27 de mayo de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1480_2011.html

Colombia. Congreso de la república. Ley 1581 de 2012. 18 de octubre de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. [en línea]. Bogotá D.C. Diario Oficial No. 51.657 [Consultado: 27 de mayo de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Colombia. Ministerio De Desarrollo Económico. Decreto 2269. 16 de noviembre de 1993. Por el cual se organiza el sistema nacional de normalización, certificación y metrología [en línea]. Bogotá, D.C, 2019. 7 p. [Consultado: 22 de abril de 2021]. Disponible en: https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%20957%20DEL%2005%20DE%20JUNIO%20DE%202019.pdf

Colombia. Ministerio de Tecnologías de la Información y las Comunicaciones. Instrumento de Evaluación MSPI. [en línea]. Bogotá D.C. Disponible en: https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/#:~:text=*El%20%22Instrumento%20de%20Evaluaci%C3%B3n%20MSPI,al%20interior%20de%20las%20Entidades

Colombiafintech. E-commerce, un aliado clave durante el coronavirus. [en línea] 08 de septiembre de 2020. [Consultado: 17 de diciembre de 2020]. Disponible en: https://www.colombiafintech.co/novedades/e-commerce-un-aliado-clave-durante-el-coronavirus

¿Conoces todos los sistemas de almacenamiento de datos? [sitio web]. Ambit.22 de octubre de 2020. [Consultado: 25 de mayo de 2021]. Disponible en: https://www.ambit-bst.com/blog/conoces-todos-los-sistemas-de-almacenamiento-de-datos

Coronel Cuadros, Daniel. Procedimiento para realizar el respaldo de información siguiendo las buenas prácticas en una empresa de Contact Center. [en línea]. Universidad Católica de Colombia. Facultad de ingeniería. Programa de ingeniería de sistemas. Bogotá D.C. 2013.138 p [Consultado: 23 de mayo de 2021]. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/860/2/PROCEDIMIENTO%20PARA%20REALIZAR%20EL%20RESPALDO%20DE%20INFORMACI%C3%93N%20SIGUI.pdf

DANE. Empleo y desempleo. [en línea]. 30 de noviembre de 2020. [Consultado: 16 de diciembre de 2020]. Disponible en: https://www.DANE.gov.co/index.php/estadisticas-por-tema/mercado-laboral/empleo-y-desempleo

Datacenter On-Premise vs Cloud. [sitio web]. Beservices.20 de octubre de 2020. [Consultado: 25 de mayo de 2021]. Disponible en: https://www.beservices.es/datacenter-on-premise-vs-cloud-n-5456-es

Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Junio 27 de 2013.Diario Oficial No 48.834.

Duque, Blanca. Metodologías de Gestión del Riesgo. [en línea] Auditoria. Universidad de Caldas, facultad de ingeniería. [Consultado: 27 de mayo de 2021]. Disponible en: https://auditoriauc20102mivi.wikispaces.com/file/view/Metodolog%C3%ACas+deGesti%C3%B2n+de+Riesgos.pdf

El Tiempo. 2019. En 2019 Se Reportaron Más De 28.000 Casos De Ciberataques En Colombia. [en línea] Disponible en: <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790>

El Tiempo. Comercio electrónico en Colombia proyecciones del 2021: 290 millones de transacciones, la meta del país en 'e-commerce'. [sitio web]. Bogotá, Colombia. 07 de marzo de 2021. [Consultado: 28 de abril de 2021].Disponible en:https://www.eltiempo.com/tecnosfera/novedades-tecnologia/comercio-electronico-en-colombia-proyecciones-del-2021-571657

Elite información. Método de análisis de riesgos NIST SP 800-30. [sitio web]. Abril de 2018. [Consultado: 27 de mayo de 2021]. Disponible en: http://elite-formacion.blogspot.com/2018/04/metodo-de-analisis-de-risgos-nist-sp.html

Empresarial, C., 2020. Ciberataques En América Latina: ¿Están Expuestas Las Empresas colombianas? ¿Qué tan seguras están las empresas colombianas ante ciberataques? [en línea] Disponible en: https://www.dinero.com/tecnologia/articulo/que-tan-seguras-estan-las-empresas-colombianas-ante-ciberataques/296519

Encyclopedia.kaspersky.es. Una Breve Historia Sobre El Hackeo. [en linea] 2020. Disponible en: <https://encyclopedia.kaspersky.es/knowledge/a-brief-history-of-hacking/>

Firma-e.com. Pilares De La Seguridad De La Información: Confidencialidad, Integridad Y Disponibilidad | Firma-E. [en linea] .2014. Disponible en: <https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-información-confidencialidad-integridad-y-disponibilidad/>.

Geeksforgeeks. Protocolo de transacciones electrónicas seguras (SET). [sitio web]. 19 de junio de 2018. [Consultado: 30 de mayo de 2021] Disponible en: https://www.geeksforgeeks.org/secure-electronic-transaction-set-protocol/

Gil Carmona Yessika Tatiana. Beneficios Del E-Commerce En Las Pymes Colombianas Durante La Covid-19. [en línea]. Universidad Militar Nueva Granada. Bogotá, Colombia.2020. [Consultado el 6 de diciembre de 2016]. Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/37014/Yessika%20Tatiana%20Gil%20Carmona.pdf?sequence=1&isAllowed=y

Glosario normas ISO/IEC 27000. [en línea] .2013. [Consultado: 15 de noviembre de 2020]. Disponible en: https://www.iso27000.es/glosario.html

Glosario normas ISO/IEC 27000. [en línea]. 2013. [Consultado: 15 de noviembre de 2020]. Disponible en: https://www.iso27000.es/glosario.html

Halchmi, Z., Hommel, K., y Avital., O., Electronic Commerce, The Technion-Israel Institute of Technology. 1996.

Health, H., 2019. 5% De Las Empresas colombianas Han Perdido Hasta Cuatro Mil Millones Por Ciberataques. [en linea] Heon.com.co. Disponible en: https://www.heon.com.co/index.php/news/item/241-ataques-ciberneticos-colombia

Hernández, Luis. Criptografía. España: Editorial CSIC. 2016. pp. 17-23. [Consultado el 13 de abril de 2021]. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/41843?page=17

Hoyos-Estrada, S., & Sastoque-Gómez, J. Marketing Digital como oportunidad de digitalización de las Pymes en Colombia en tiempo del COVID – 19. Revista Científica Anfibios. [en linea] 2020. 3(1), 39-46. [Consultado: 23 de abril de 2021]. Disponible en: https://doi.org/10.37979/afb.2020v3n1.60

IEBSchool. ¿Qué es E-commerce y cómo crear tu propio comercio electrónico? [en línea] .3 de marzo de 2020. [Consultado: 30 de noviembre de 2020]. Disponible en: https://www.iebschool.com/blog/comercio-online-ecommerce/

Informe comportamiento del ecommerce en Colombia durante 2020 y perspectivas para 2021. [pdf]. CCCE. [Consultado 10 de diciembre de 2020]. Disponible en: https://www.ccce.org.co/wp-content/uploads/2020/10/informe-comportamiento-y-perspectiva-ecommerce-2020-2021.pdf

Informe de las tendencias del Cibercrimen en Colombia 2019-2020.Bogotá D.C. CCIT.org.co. Octubre 29 de 2019. [Consultado: 19/04/2021]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Instituto colombiano de normas técnicas y certificación. Tecnología De La Información. Técnicas De Seguridad. Sistemas De Gestión De La Seguridad De La Información. Requisitos. NTC-ISO 27001.Bogotá D.C. El Instituto. 2013. 33 p.

Instituto colombiano de normas técnicas y certificación. Tecnología De La Información. Técnicas De Seguridad. Sistemas De Gestión De La Seguridad De La Información. Requisitos. NTC-ISO 27001.Bogotá D.C. El Instituto. 2013. 33 p.

Instituto Colombiano De Normas Técnicas y Certificación. Tecnología De La Información. Técnicas De Seguridad. Sistemas De Gestión De La Seguridad De La Información. Requisitos. NTC-ISO 27001.Bogotá D.C. El Instituto. 2013. 33 p.

Instituto Colombiano De Normas Técnicas y Certificación. Tecnología De La Información. Técnicas De Seguridad. Código de práctica para la gestión de la seguridad de la información. NTC-ISO 27002.Bogotá D.C. El Instituto. 16 de noviembre de 2007. 144 p.

Jimenez, David. Pasarelas de Pago en Colombia: Ecommerce [en línea]. DigitalJourney.1 de octubre de 2020. [Consultado: 05 de mayo de 2021]. Disponible en: https://digitaljourney.com.co/pasarelas-de-pago-en-colombia/

Kaspersky. ¿Como Borrar Software Malicioso?.2021. [Consultado: 22 de mayo de 2021]. Disponible en: https://latam.kaspersky.com/resource-center/preemptive-safety/removing-malicious-code

Kaspersky. Elección de una solución antivirus.2021. [Consultado: 22 de mayo de 2021]. Disponible en: https://latam.kaspersky.com/resource-center/preemptive-safety/antivirus-choices

Kemp, Simon. Digital 2021: Local Country Headlines Most-Used Social Media Platforms. 27 de enero de 2021. [Consultado: 06 de mayo de 2021] Disponible en: https://datareportal.com/reports/digital-2021-local-country-headlines?utm_source=Reports&utm_medium=PDF&utm_campaign=Digital_2021&utm_content=Dual_Report_Promo_Slide

La Seguridad de la Información: Historia, Terminología y Campo de acción [blog]. Disponible en: https://blog.desdelinux.net/seguridad-información-historia-terminologia-campo/

Laboratorios Fortiguard. MS.Windows.Metafile.WMF.Integer.Overflow. [sitio web]. Enciclopedia de amenazas. [Consultado: 15 de febrero de 2021]. Disponible en: https://www.fortiguard.com/encyclopedia/ips/11314

Las empresas que no invierten en tecnología desaparecerán en 2020. [en línea]. 2019 [Consultado: 20 de noviembre de 2020]. Disponible en: https://noticiascurazao.com/las-empresas-que-no-invierten-en-tecnologia-desapareceran-en-2020/

Ley 1266 de 2008.Por medio de la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en base de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diciembre 31 de 2008.Diario Oficial No 47.219.

Ley 1273 de 2009.Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Enero 5 de 2009.Diario Oficial No 47.223.

Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. Agosto 21 de 1999. Diario Oficial No 43673.

Martos, Fernando. Centros Hospitalarios de Alta Resolución de Andalucía-Auxiliares Administrativos. [en linea]. Primer Edición. España.2006. 195 p. [Consultado: 27 de mayo de 2021]. Disponible en: https://books.google.com.co/books?id=SmwP1cZdI4cC&pg=PA195&dq=LA+METODOLOG%C3%8DA+MAGERIT+3.0&hl=es&sa=X&ved=0ahUKEwiK5d7u_KTJAhUJWCYKHadoB14Q6AEIJTAC#v=onepage&q=LA%20METODOLOG%C3%8DA%20MAGERIT%203.0&f=false

Ministerio de Comercio, Industria y Turismo. ProColombia lanzó 'Colombia a un clic' para impulsar el e-commerce. [sitio web]. Bogotá, Colombia. 03 abril de 2019. [Consultado: 01 de mayo de 2021]. Disponible en: https://www.mincit.gov.co/prensa/noticias/industria/procolombia-lanzo-colombia-a-un-clic-para-impulsar

Ministerio de hacienda y administraciones publicas. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. [en línea] Portal de Administración Electrónica Gobierno de España. Libro I-método. 2012. [Consultado: 29 de mayo de 2021] Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

Ministerio de hacienda y administraciones públicas. MAGERIT V.3: Metodología de Análisis y gestión de riesgos de los sistemas de información. [en línea] Portal de Administración Electrónica Gobierno de España. Libro II-Catalogo de elementos. (2012). [Consultado: 29 de mayo de 2021] Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_MAGERIT.html

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Vende Digital: lleva tu negocio a otro nivel. [sitio web]. Bogotá, Colombia. [Consultado: 01 de mayo de 2021]. Disponible en: https://vendedigital.mintic.gov.co/754/w3-channel.html

Minsalud. Coronavirus (Covid-19). [en línea] [Consultado: 15 de diciembre de 2020] Disponible en: https://www.minsalud.gov.co/salud/publica/PET/Paginas/COVID-19_copia.aspx

Mondaca, C. Seguridad de la Información: ¿Invierten las empresas en TI? [en línea]. 2020. [Consultado: 20 de noviembre de 2020]. Disponible en: https://www.pwc.com/cl/es/prensa/columnas-de-opinion/seguridad-de-la-información-invierten-las-empresas-en-ti.html

Pandini, W. ISO27002: Buenas prácticas para gestión de la seguridad de la información. [en línea]. 2019. Disponible en: https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi#:~:text=En%20este%20grupo%20se%20encuentra,(SGSI)%20en%20las%20organizaciones.

Peña Jimenez, Yuber Javier. Comercio electrónico ventajas y desventajas. [en línea]. Bogotá D.C. Universidad Cooperativa de Colombia. Facultad de ciencias administrativas y económicas. Noviembre de 2019. [Consultado: 21 de abril de 2021]. Disponible en: https://repository.ucc.edu.co/bitstream/20.500.12494/16999/3/2019_Comercio_electronico_ventajas.pdf

Plan de concienciación de Seguridad Informática. 2021.Ciberseguridad: Noticias de ciberseguridad, ciberataques, vulnerabilidades informáticas. [Consultado: 23 de mayo de 2021]. Disponible en: https://ciberseguridad.com/normativa/espana/medidas/planconcienciacion/#Establecer_responsabilidad

Postigo Palacios, A., Seguridad Informática. Ediciones Paraninfo, S.A. 2020.

Proveedor de Servicios de Email. [sitio web]. Ryte Wiki. [Consultado: 23 de mayo de 2021]. Disponible en: https://es.ryte.com/wiki/Proveedor_de_Servicios_de_Email

República de Colombia. Consejo Nacional de Política Económica y Social CONPES. Documento CONPES 4012. 30 de noviembre de 2020.Politica Nacional de comercio electrónico. [en línea] Bogotá. Departamento Nacional de planeación. [Consultado: 27 de mayo de 2021]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/4012.pdf

Revista Dinero. Pymes: ausentes de tecnología. [en línea]. 2007. [Consultado: 20 de noviembre de 2020]. Disponible en: https://www.dinero.com/negocios/articulo/pymes-ausentes-tecnologia/46830

Riesgos Informáticos. [sitio web]. CRAMM. Marzo de 2014. [Consultado: 27 de mayo de 2021]. Disponible en: http://antonioinformatico.blogspot.com/2014/03/cramm.html

Rincón Cárdenas Erick. Uso de medios electrónicos (I). La Ley 527 de 1999 como instrumento normativo suficiente. Legis Ámbito jurídico. [en línea] .12 de junio de 2017. [Consultado: 31 de marzo de 2021]. Disponible en: https://www.ambitojuridico.com/noticias/tic/uso-de-medios-electronicos-i-la-ley-527-de-1999-como-instrumento-normativo-suficiente

Romero Castro, M., Figueroa Morán, G., Vera Navarrete, D., Álava Cruzatty, J., Parrales Anzúles, G., Álava Mero, C., Murillo Quimiz, Á. and Castillo Merino, M., 2018. Introducción a la seguridad informática y el análisis de vulnerabilidades. 1st ed. Alicante: 3ciencias, pp.13-20.

Ruiz, Francisco Javier. OnPremise, servidores y problemas frente a solución Cloud. [blog] Blog de Dataprius.17 de junio de 2016. [Consultado: 22 de mayo de 2021]. Disponible en: https://blog.dataprius.com/index.php/2016/06/17/on-premise-servidores-problemas-solucion-cloud/

Security Report ESET Latinoamérica 2020. [en línea]. Welivesecurity.com. 2020, nro.8. [Consultado: 19 de abril de 2021]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf

Seguridad de la información: ¿qué principios necesitan conocer las empresas? [blog] .2020. Disponible en: https://blogmexico.comstor.com/seguridad-de-la-información-que-principios-necesitan-conocer-las-empresas

SIC. Estudios de Mercado. [en línea]. [Consultado: 5 de diciembre de 2020]. Disponible en: https://www.sic.gov.co/recursos_user/documentos/promocion_competencia/Estudios_Economicos/Estudios_Economicos/Estudios_Mercado_E-commerce.pdf

Threatmap.fortiguard.com. Fortinet Threat Map. [Consultado: 28 de noviembre de 2020]. Disponible en: https://threatmap.fortiguard.com/

Universidad de cuenca facultad de ingeniería maestría en telemática. Implementación de un prototipo de tienda virtual sobre plataforma Linux para realizar transacciones de comercio electrónico seguro. [en línea] .30 de julio de 2010. [Consultado: 05 de diciembre de 2020]. Disponible en: https://dspace.ucuenca.edu.ec/bitstream/123456789/2530/1/tm4396.pdf

Universidad de cuenca facultad de ingeniería Maestría En Telemática. Implementación de un prototipo de tienda virtual sobre plataforma Linux para realizar transacciones de comercio electrónico seguro. [en línea] .30 de julio de 2010. [Consultado: 05 de diciembre de 2020]. Disponible en: https://dspace.ucuenca.edu.ec/bitstream/123456789/2530/1/tm4396.pdf

Vargas Salcedo, Julio Cesar. Campañas de concientización en seguridad de la información dirigidas a usuarios finales como método de ayuda para la mitigación del riesgo sobre los datos de la empresa. Fundación Universidad Piloto de Colombia. [Consultado: 23 de mayo de 2021]. Disponible en: http://polux.unipiloto.edu.co:8080/00004663.pdf

Velasco C. Ricardo. Gestión del riesgo basado en la norma ISO/IEC 27005:2009. [en línea] Universidad Piloto de Colombia. Enero de 2016. [Consultado: 28 de mayo de 2021]. Disponible en: http://polux.unipiloto.edu.co:8080/00002323.pdf

Ventajas de implementar ISO 31000. [sitio web] Gestión Colombia. 8 de abril de 2014. [Consultado: 27 de mayo de 2021]. Disponible en: https://gestioncolombiaconsultores.wordpress.com/2014/04/08/ventajas-de-implementar-iso-31000/

WMF (Windows Metafile). [sitio web]. online-convert.com. [Consultado: 31 de mayo de 2021]. Disponible en: https://www.online-convert.com/es/formato-de-archivo/wmf