



UNIVERSIDAD DE MARGARITA
SUBSISTEMA DE DOCENCIA
DECANATO DE INGENIERÍA Y AFINES
COORDINACIÓN DE INVESTIGACIÓN

**EVALUACIÓN DE LOS NIVELES DE SEGURIDAD Y CONTROL QUE
DEBE CUMPLIR UNA PYME EN RELACIÓN A SUS SERVIDORES
LOCALES Y REDES ALÁMBRICAS E INALÁMBRICAS**

Elaborado por: Hanna Karam Cárdenas
Tutor: Ing. Hiram González Gómez

El Valle del Espíritu Santo, diciembre de 2021

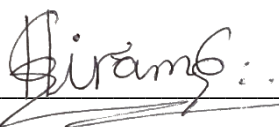


UNIVERSIDAD DE MARGARITA
SUBSISTEMA DE DOCENCIA
DECANATO DE INGENIERÍA Y AFINES
COORDINACIÓN DE INVESTIGACIÓN

CARTA DE APROBACIÓN DEL TUTOR

En mi carácter de Tutor del Trabajo de Investigación presentado por el ciudadano **HANNAH WADIH KARAM CARDENAS**, cedula con el número: **V.-18.549.354**, para optar al Grado de *Ingeniero de Sistemas*, considero que dicho trabajo: **EVALUACIÓN DE LOS NIVELES DE SEGURIDAD Y CONTROL QUE DEBE CUMPLIR UNA PYME EN RELACIÓN A SUS SERVIDORES LOCALES Y REDES ALÁMBRICAS E INALÁMBRICAS** reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del Jurado Examinador que se designe.

Atentamente



Ing. Hiram González Gómez

El Valle del Espíritu Santo, diciembre de 2021

AGRADECIMIENTOS

Muy agradecido con mi tutor Ing. Hiram González por el tiempo y apoyo prestado en el transcurso de la investigación, así como con la Prof. Yemnel Torcat y Prof. Ana Blanco por responder siempre a mis consultas, de forma oportuna y precisa. Asimismo, quiero agradecer a mis motivadores indirectos del tema seleccionado, la Prof. Georgelys Marcano y el Prof. Flavio Rosales.

ÍNDICE GENERAL

AGRADECIMIENTOS	iii
ÍNDICE DE CUADROS	vii
RESUMEN.....	viii
INTRODUCCIÓN.....	1
PARTE I	3
DESCRIPCIÓN GENERAL DEL PROBLEMA.....	3
1.1. Formulación del problema	3
1.2. Interrogantes	7
1.3. Objetivo general	7
1.4. Objetivos específicos	7
1.5. Valor académico de la investigación	8
PARTE II	10
DESCRIPCIÓN TEÓRICA.....	10
2.1. Antecedentes	10
2.2. Bases Teóricas.....	12
2.2.1. Pequeñas y medianas empresas	12
2.2.2. Seguridad informática	14
2.2.3. Políticas de seguridad	15
2.2.4. Servidores	17
2.2.5. Redes informáticas	18
2.2.6 Sistema de gestión de la seguridad de la información	21
2.3. Bases Legales.....	22
2.3.1. Constitución de la República Bolivariana de Venezuela (publicada en Gaceta Oficial Extraordinaria N.º 36.860, de fecha 30 de diciembre de 1.999)	22
2.3.2. Ley Orgánica de Telecomunicaciones (publicada en Gaceta Oficial N.º 39.610, de fecha 7 de febrero de 2011)	22
2.3.3. Ley sobre Protección a la Privacidad de las Comunicaciones (publicada en Gaceta Oficial N.º 34.863, de fecha 16 de diciembre de 1991)	23
2.3.4. Ley sobre el Derecho de Autor (publicada en Gaceta Oficial Extraordinaria N.º 4.638, de fecha 1 de octubre de 1993)	23

2.3.5. Ley Especial Contra los Delitos Informáticos (publicada en Gaceta Oficial N.º 37.313, de fecha 30 de octubre de 2001)	23
2.4. Definición de términos	24
PARTE III	28
DESCRIPCIÓN METODOLÓGICA	28
3.1. Naturaleza de la Investigación	28
3.1.1. Tipo de investigación	28
3.1.2. Diseño de la investigación	28
3.1.3. Objeto de estudio	29
3.1.4. Acopio y selección de la información	29
3.2. Técnicas de recolección de datos	30
3.3. Técnicas de análisis de datos	30
PARTE IV	32
ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS.....	32
4.1 Identificación de los factores que se deben considerar al establecer la seguridad de los servidores locales y las redes alámbricas e inalámbricas de una pyme	32
4.2 Especificación de las normas internacionales que regulan la seguridad de los servidores locales y las redes alámbricas e inalámbricas.	38
4.2.1 Serie ISO/IEC 27000.....	39
4.2.2 COBIT	40
4.2.3 ITIL.....	42
4.3 Establecimiento de las políticas adecuadas para los servidores locales y las redes alámbricas e inalámbricas de una pyme.	46
Política 1: Sobre el SGSI	47
Política 2: Control de Accesos	48
Política 3: Gestión de los activos	49
Política 4: Seguridad sobre el talento humano.....	49
Política 5: Capacitación y entrenamiento	49
Política 6: Manejo del riesgo	50
Política 7: Seguridad física y ambiental	50
Política 8: Gestión de las redes y los sistemas informáticos	50
Política 9: Sistemas de respaldo y recuperación	51
Política 10: Servicio electrónico	51

Política 11: Gestión de los incidentes de seguridad.....	51
Política 12: Planes de recuperación ante desastres	52
CONCLUSIONES.....	58
RECOMENDACIONES	59
REFERENCIAS BIBLIOGRÁFICAS	60

ÍNDICE DE CUADROS

Cuadro 1. Criterios que debe cumplir una pyme objeto de estudio.	33
Cuadro 2. Tipos y orígenes de las amenazas a la seguridad informática.....	37
Cuadro 3. Cuadro comparativo de las normas ISO/IEC 27001, COBIT e ITIL.	454
Cuadro 4. Requisitos mínimos en TI que debe cumplir una pyme.....	533
Cuadro 5. Controles y políticas de seguridad generales establecidas para las pymes.	57

UNIVERSIDAD DE MARGARITA
ALMA MATER DEL CARIBE
COORDINACIÓN DE INVESTIGACIÓN

**EVALUACIÓN DE LOS NIVELES DE SEGURIDAD Y CONTROL QUE
DEBE CUMPLIR UNA PYME EN RELACIÓN A SUS SERVIDORES
LOCALES Y REDES ALÁMBRICAS E INALÁMBRICAS**

Autor: Hanna Karam Cárdenas
Tutor: Ing. Hiram González Gómez
Noviembre de 2021

RESUMEN

Las redes de comunicación se han convertido en una herramienta vital para la operatividad de muchas empresas; sin embargo, existe el riesgo de que personas, de forma local o remota, intenten acceder a los datos almacenados en los servidores y pongan en peligro la funcionalidad de los mismos, con especial incidencia en las pymes. Éstas últimas tienden a desconocer el valor de sus datos informáticos y, por ende, no son capaces de identificar y contrarrestar a tiempo las amenazas informáticas que puedan resultar perjudiciales. En consecuencia, el presente trabajo documental evalúa de forma crítica la gestión de seguridad de los sistemas de información y comunicación en los servidores locales y redes alámbricas e inalámbricas que debe poseer una pyme en sus niveles de infraestructura, hardware y software, empleando como referencia las normas internacionales ISO/IEC 27000, COBIT e ITIL, para describir políticas de seguridad de aplicación general en dichas empresas.

Descriptores: gestión de seguridad de la información, pyme, políticas de seguridad, servidores locales, redes alámbricas, redes inalámbricas.

INTRODUCCIÓN

La globalización ha traído grandes ventajas para la humanidad, ofreciendo una extensa y variada información al alcance de un computador conectado al internet; de esta manera, las tecnologías se convierten en un importante factor de apoyo en el desarrollo e interacción de cualquier proceso, mejorando la eficiencia en cuanto a tiempo, recursos y resultados obtenidos. Tanto es así que los procesos manuales han quedado en segundo plano, y la digitalización de la información se ha convertido en parte esencial de la vida humana, especialmente en los negocios, los cuales han tenido que acoplarse a un nuevo ritmo de vida como consecuencia del COVID-19 y, muchos de ellos, se han visto en la necesidad de implementar estrategias de trabajo a distancia para no sucumbir al cese de operaciones.

Por tanto, la digitalización de información, automatización de procesos y gestión a través de la red, se han convertido en estrategias comunes para construir organizaciones suficientemente capaces de enfrentar cualquier crisis que atente contra su operatividad, desarrollo y sustento. Sin embargo, las tecnologías también pueden amenazar la privacidad, comprometer la seguridad y causar daño a terceros cuando es utilizada con fines negativos; por lo que se hace sumamente necesario proteger los sistemas de información y el acceso a las redes de comunicación para mitigar, en la medida de lo posible, los riesgos asociados a los ataques informáticos. Entre estas organizaciones que cada vez más hacen uso de los sistemas de información e infraestructura tecnológica para gestionar sus procesos se pueden encontrar a las pymes, las cuales representan en la actualidad un importante sector de la economía; agrupando una amplia y diversificada rama, tipo y complejidad de negocios.

En este sentido, se hace necesario plantear estrategias factibles y accesibles que permitan tomar medidas efectivas para proteger los recursos tecnológicos de una pyme, en especial sus servidores locales y el acceso a las redes alámbricas e inalámbricas. Por tal motivo, la presente investigación pretende describir los principales factores a considerar al momento de evaluar la seguridad en los servidores locales y redes alámbricas e inalámbricas, así como las normas internacionales en materia de seguridad de sistemas informáticos que ayudan en el diseño de marcos de trabajo para aumentar los niveles de seguridad organizacional, especialmente en cuanto a las políticas de

seguridad se refiere. De esta manera, el presente trabajo de investigación se encuentra estructurado de la siguiente forma:

En la **Parte I**, se realiza la descripción general del problema, donde se detallan los aspectos relacionados al tema objeto de estudio y su justificación, conformado por la formulación del problema, las interrogantes, los objetivos y el valor académico de la investigación.

En la **Parte II**, se presenta la descripción teórica, donde se desarrollan los principales conceptos asociados a la investigación, constituyéndose en antecedentes, bases teóricas, bases legales y definición de términos.

En la **Parte III**, se desarrolla la descripción metodológica, donde se expone la naturaleza de la investigación, las técnicas de recolección de datos y las empleadas para analizar dichos datos.

En la **Parte IV**, se presenta el análisis e interpretación de los resultados, donde se analiza cada uno de los objetivos específicos de la investigación en base a los resultados obtenidos; lo que da paso a satisfacer el objetivo general.

En **Conclusiones y Recomendaciones**, se sintetiza, a modo de respuesta, los resultados obtenidos en la investigación, añadiendo sugerencias por parte del investigador para que sean consideradas en estudios posteriores o en implementaciones de proyectos similares.

En **Fuentes Bibliográficas**, se especifica cada uno de los distintos recursos informativos que fueron consultados durante el desarrollo de la investigación; abarcando libros, páginas web, regulaciones legales, documentos digitales, entre otros.

PARTE I

DESCRIPCIÓN GENERAL DEL PROBLEMA

De acuerdo con Arias, F. (2012:41), el planteamiento del problema “consiste en describir de manera amplia la situación objeto de estudio, ubicándola en un contexto que permita comprender su origen, relaciones e incógnitas por responder”. Por ende, en esta parte se detallará la formulación del problema, así como las interrogantes, los objetivos y el valor académico que implica esta investigación.

1.1. Formulación del problema

Las pequeñas y medianas empresas (pymes) desempeñan un papel de gran importancia en la industria nacional al tener una alta capacidad de creación de empleo y un aporte importante al producto interno bruto, correspondiente al valor total de los bienes y servicios finales producidos; además, realizan un alto porcentaje de las actividades manufactureras, constituyendo una base para la expansión de las industrias y el crecimiento económico de la nación. Según el Instituto Nacional de Estadísticas – INE (2010), las pymes en Venezuela constituían, para el año 2008, el 99,5% de las empresas operativas, mientras que las grandes empresas solo representaban el 0,5%; en la actualidad se manejan cifras similares. Así mismo, más del 75% de todas las empresas emplean algún sistema de comunicación, siendo dependientes de la tecnología, especialmente en cuanto a los sistemas de pago, ya sea por punto de venta, transferencias o mediante alguna aplicación móvil.

En vista de la dependencia de una gran cantidad de pymes respecto al uso de las redes alámbricas o inalámbricas, puesto que les permiten efectuar actividades a través de medios digitales, es necesario procurar el máximo esfuerzo para garantizar la seguridad de los datos que se manejan en los sistemas interconectados, impidiendo que sean utilizados de forma distinta a como fueron conferidos o que sean captados y modificados por personas no autorizadas; de vulnerarse alguno de ellos se pierde la seguridad que pudieran estar establecidas en estas redes.

El término seguridad implica que un agresor (amenaza) intenta obtener algún valor que se encuentra en manos de un protector; tanto agresor como protector pueden ser

solo intermediarios, y el valor puede ser algo tangible o intangible, real o imaginario. De acuerdo con Costas, J. (2014:19), la seguridad informática (SI):

Consiste en asegurar que los recursos de un sistema de comunicación de un individuo u organización sean utilizados con el objeto que decida su propietario, y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Así, la SI cuida, de forma integral y mediante distintas técnicas, tanto el hardware como el software, aunque se especializa en la protección de los datos y de la información, con el fin de obtener altos niveles de seguridad (el riesgo nunca es cero), y ofrecer herramientas y procedimientos para enfrentar (prevenir, detectar y recuperar) problemas en esta área y reducir tanto el peligro de un ataque como el daño posterior, si éste llegase a materializarse.

En vista de que el bien máspreciado en las redes informáticas son los datos, se deben cuidar los medios para acceder a ellos, los cuales son los puertos. En concordancia con López, J. (2016, párr. 2), los puertos son una interfaz desde la que se envían o reciben diferentes tipos de datos y pueden ser físicos o lógicos (puertos de red). Entonces, a través de los puertos se puede crear una especie de puente o red entre programas y dispositivos, lo que deviene en la gran importancia que presentan para la SI. En este mismo orden de ideas, una red, según Molero, L. (2013), “es un sistema de interconexión de computadoras que permite a sus usuarios compartir recursos, aplicaciones, datos, voz, imágenes y transmisiones de video”; por lo tanto, una red consiste en un conjunto de dispositivos, interconectados entre sí, a través de medios físicos o inalámbricos para compartir información y recursos (archivos, recursos de red y bases de datos).

De este modo, los dispositivos que usan la red pueden cumplir los roles de servidor (brinda un servicio para todo aquel que quiera consumirlo) o de cliente (consume uno o varios servicios de uno o varios servidores), conformando la arquitectura cliente-servidor. De igual forma existen otras arquitecturas, como la punto a punto, donde el dispositivo de red puede ser cliente y servidor al mismo tiempo.

En vista de ello, la seguridad de las redes abarca distintos niveles, englobando todos los aspectos de la infraestructura tecnológica, conformada por el hardware y el software. En cuanto al hardware, este se encuentra conformado por todos los componentes físicos

y electrónicos que forman parte de la red; el software es el conjunto de programas encargados de controlar el hardware y los servicios de redes.

Por otra parte, Tarazona, C. (2007:138) define una amenaza como “cualquier situación o evento que puede afectar la posibilidad de que las organizaciones o las personas puedan desarrollar sus actividades afectando directamente la información o los sistemas que la procesan”. De esta forma, una amenaza es cualquier elemento que comprometa el sistema, como los desastres naturales, la interrupción del servicio eléctrico o internet (para las empresas que deben poseer equipos encendidos en todo momento) y la acción humana, ya sea intencional o no intencional (errores, descuidos o desconocimiento). Por lo tanto, las amenazas implican riesgos a la seguridad de las redes, que deben prevenirse a toda costa, y en caso de materializarse, se debe buscar que el daño generado sea el mínimo posible, para luego aplicar métodos de recuperación y poder adaptar las medidas de seguridad en base a la información recabada del evento.

En vista de esto, los sistemas de comunicación tienen una vulnerabilidad, debilidad o cierta posibilidad de fallo que hay que cubrir lo más posible, para evitar que puedan ser usados por algún atacante para afectar el sistema, formulando las contramedidas apropiadas. Al respecto, Mieres, J. (2009:4) menciona lo siguiente:

Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización.

En este sentido, y de forma general, existen muchas empresas que emplean la seguridad informática para protegerse de todas las amenazas posibles, mediante el uso de medidas de control frente a las vulnerabilidades que pudieran encontrarse en un sistema. Por consiguiente, las empresas invierten constantemente en seguridad para evitar sufrir ataques informáticos y pérdidas del control de sus datos, lo cual se traduciría en pérdidas económicas. Esto último es especialmente importante en el mundo empresarial, destacando las pymes, donde los datos y la información tienden a ser uno de los activos más valiosos, y donde se deben tomar las medidas de seguridad apropiadas para evitar ser víctima de ataques informáticos.

En la actualidad, las pymes deben trabajar por conseguir un sistema fiable a nivel lógico, permaneciendo atentas a vulnerabilidades de su software, restringiendo servicios, utilizando cifrado de datos, adquiriendo software de seguridad apropiados (antivirus actualizados, sistemas *antispyware* y *firewall* complementarios o integrados), entre otras acciones que dependerán de la complejidad de las vulnerabilidades que se presenten en determinada empresa.

Martínez, J. (2015) menciona que “ninguna empresa está a salvo del espionaje informático, siendo las pymes más vulnerables a esta problemática por su mayor falta de recursos, por prestarse menos atención a la ciberseguridad y por su menor concienciación en este aspecto”. Aunque sean pequeñas o medianas empresas, no significa que no puedan tener información confidencial que se debe proteger a toda costa, sino que, además, pueden convertirse, por desconocimiento, en un puente de ataques dirigidos a otras empresas con las que mantengan relaciones comerciales y que sean de interés para el atacante. Por otro lado, las motivaciones de los *hackers* que tienen por objetivo a las pymes pueden ser muy variadas e, incluso, impulsadas por empresas competidoras, abarcando venganzas personales, el lucro por venta de información confidencial o, incluso, por simple diversión o mala intención.

Así mismo, el autor anterior (*ob. cit.*) menciona que los incidentes de seguridad en las pymes son bastante altos, describiendo que el 41% de las empresas de América Latina, en el año 2013, afirmaron haber sufrido infección por códigos maliciosos. Estos incidentes se basan en el mal uso de la infraestructura tecnológica, pudiendo centrarse en diversas causas que surgen a raíz de este hecho. Es por ello necesario procurar el máximo esfuerzo para garantizar la confidencialidad (la información solo puede ser vista por usuarios autorizados), disponibilidad (que la información sea vista cuando se desee) e integridad (que los datos no sufran cambios desautorizados) de los datos que se manejan en estos sistemas, impidiendo que sean usados de forma distinta a como fueron conferidos o que sean capturados y modificados por personas no autorizadas.

De vulnerarse alguna de las características previamente mencionadas, se pierde la seguridad establecida, pudiendo traer consecuencias nefastas para las pymes, como la pérdida de clientes o socios por temor a exponer su dinero o información confidencial, pérdidas económicas y limitaciones en el flujo normal de actividades por paradas en la

prestación de sus servicios, e incluso quiebra de la empresa por pérdida de grandes capitales e imposibilidad de reanudación de sus servicios; además de multas o demandas legales. En vista de todo lo planteado previamente, se tiene la intención de realizar una evaluación de los niveles de seguridad y control que debe cumplir una pyme con respecto a sus servidores locales y a sus redes alámbricas e inalámbricas, para garantizar la protección y seguridad de sus sistemas de comunicación.

1.2. Interrogantes

Tomando en cuenta lo expresado en el apartado anterior, es necesario plantear interrogantes que permitan llevar a cabo una investigación ordenada y acorde a la problemática abordada. Respecto a la cuestión central de la investigación, se formula la siguiente pregunta: ¿Cuáles serían los niveles de seguridad y control que debe cumplir una pyme respecto a sus servidores locales y sus redes alámbricas e inalámbricas?

En relación a la pregunta principal, se desprenden las siguientes interrogantes específicas:

1. ¿Qué aspectos se consideran al establecer la seguridad de los servidores locales y las redes alámbricas e inalámbricas de una pyme?
2. ¿Qué normas internacionales regulan la seguridad de los servidores locales y las redes alámbricas e inalámbricas?
3. ¿Cuáles políticas son adecuadas para que los servidores locales y las redes alámbricas e inalámbricas de una pyme tengan seguridad en todos sus niveles?

1.3. Objetivo general

Evaluar los niveles de seguridad y control que debe cumplir una pyme en relación a sus servidores locales y redes alámbricas e inalámbricas.

1.4. Objetivos específicos

1. Identificar los aspectos que se deben considerar al establecer la seguridad de los servidores locales y las redes alámbricas e inalámbricas de una pyme.
2. Especificar las normas internacionales que regulan la seguridad de los servidores locales y las redes alámbricas e inalámbricas.
3. Establecer las políticas adecuadas para los servidores locales y las redes alámbricas e inalámbricas de una pyme.

1.5. Valor académico de la investigación

Las actividades de las pymes conforman gran parte del motor económico del país; éstas dependen del uso de la tecnología y de los sistemas de comunicación para efectuar sus procesos y operaciones internas, sin importar su tamaño o su área de desarrollo y sector productivo, lo que conlleva al mejoramiento de su operatividad y competitividad como empresa.

El funcionamiento óptimo de todos los dispositivos y redes informáticos de las pymes son muy importantes para garantizar el control de los datos y de las operaciones que éstas realicen, evitando pérdidas económicas, operativas y de clientes. La cuestión es que existen vulnerabilidades en estos dispositivos que podrían repercutir en el acceso de personas mal intencionadas (piratas informáticos) hacia los sistemas de comunicación de determinada pyme, con el objetivo de apoderarse de los datos para algún fin posterior. También es importante señalar que la mayoría de las organizaciones tienen desconocimiento del peligro que implica no tener controles en sus distintos niveles de seguridad, como lo son el software y el hardware, incrementando el riesgo latente.

Entonces, tener controles en los niveles de seguridad de las redes informáticas y de los servidores locales podría traer mayor estabilidad logística a la empresa, aumentando su reputación y la confianza de sus empleados y clientes. Cabe mencionar que todas las pymes tienen cierta relación en cuanto a los dispositivos y redes que emplean, por lo que las conclusiones de este trabajo pudieran ser efectivas para la gran mayoría de ellas, sin importar el sector económico o productivo que ocupen.

Por otro lado, el valor académico propiamente dicho de esta investigación reside en que las conclusiones que se obtengan pueden ser provechosas para estudiantes universitarios e incluso para profesionales del área de sistemas, informática y redes, pudiendo emplear el presente trabajo como referencia para futuras investigaciones académicas. Es importante añadir que la seguridad nunca es absoluta, siempre habrá brechas en la misma, debido a que la tecnología, las técnicas y los recursos de los ciberdelincuentes siempre cambia, mejora y se adapta a las defensas existentes; por lo tanto, es necesario emplear el mayor esfuerzo en mitigar los riesgos, estableciendo medidas eficaces de prevención y corrección en todos los niveles de seguridad de una

organización, lo que conlleva a evitar, en la medida de lo posible, sufrir el daño que los perpetradores tuvieran intención de ocasionar.

PARTE II

DESCRIPCIÓN TEÓRICA

De acuerdo con García, J. (2014, párr. 4) el marco teórico “sirve para acondicionar la información científica que existe sobre lo que se va a investigar, previniendo que el investigador cometa viejos errores en el estudio a desarrollar, dándole guías de cómo hacer el estudio o a dónde dirigirlo”. En este sentido, el presente capítulo consiste en describir la teoría relacionada con el problema previamente planteado, iniciando con algunos antecedentes de la investigación, para posteriormente describir las variables más importantes del estudio; además, se mencionarán las bases legales relacionadas al tema de la investigación, acompañado finalmente de un glosario de términos.

2.1. Antecedentes

González, H. (2019), en su informe de pasantías titulado “EVALUACIÓN MEDIANTE AUDITORÍA DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN EN AMBIENTE WEB Y REDES, CON EL FIN DE DETECTAR RIESGOS Y VULNERABILIDADES DE FORMA QUE SE PUEDAN APLICAR MEDIDAS PREVENTIVAS O CORRECTIVAS OPORTUNAS EN LA EMPRESA SOUTH AMERICAN JETS”, realizó una investigación evaluativa, mediante la aplicación de una auditoría de la seguridad de los sistemas de información en ambiente web y redes, con el fin de detectar riesgos y vulnerabilidades de forma que pudiesen aplicarse medidas preventivas o correctivas oportunas en la empresa señalada.

En este sentido, el autor realizó una evaluación general de las instalaciones y de los sistemas empleados para cumplir las actividades diarias de la empresa, enfocándose en buscar debilidades en la seguridad y acceso a los equipos y redes, utilizando una metodología general de auditoría y la metodología de análisis y gestión de riesgos MAGERIT V3.0. Además, utilizó las normas internacionales ISO 27001 y 27002 para establecer cuestionarios que le permitieran evaluar de forma normativa el estado de la seguridad informática de la empresa, y, en base a los resultados obtenidos, sugerir medidas de acción preventivas y mitigantes plasmadas en nuevas políticas de seguridad. Así, este trabajo arroja valiosa información referente al uso de las normas ISO de la serie

27000 en función del fortalecimiento de la seguridad en los sistemas informáticos, así como del desarrollo de las políticas de seguridad oportunas.

Cortes, J. (2016), en su trabajo de grado titulado “AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA PANAVIDAS S.A.”, realizó una investigación exploratoria y descriptiva, aplicando pruebas de penetración a los distintos sistemas de información que formaban parte de la red WLAN de la empresa PANAVIDAS, S.A., con el objetivo de evaluar el nivel de riesgo al que se enfrentaba la seguridad informática existente, buscando en este proceso diversas vulnerabilidades y amenazas. Además, realizó una auditoría documental respecto al estado de las medidas de seguridad informáticas, para lo cual utilizó como referencia las normas internacionales ISO 27.001 y 27.002. Por último, el autor documentó unas políticas de seguridad, las cuales fueron adaptadas al nivel de complejidad de la empresa en cuestión, con el propósito de reforzar el Sistema de Gestión de la Seguridad de la Información (SGSI).

En vista de que la compañía PANAVIDAS, S.A. compete en el mercado de la construcción, y se encuentra clasificada en país de origen (Colombia) como una pyme, donde sus sistemas de comunicación están basados en redes alámbricas e inalámbricas, se le considera una referencia muy útil al momento de visualizar las vulnerabilidades que pueden detectarse después de aplicar una prueba de penetración, además de que se reflejan una serie de recomendaciones y medidas de control que debe ejecutar la empresa, en sus distintos niveles, para mitigar las debilidades halladas.

Por otro lado, Martínez, J. (2015), en su trabajo de grado titulado “SEGURIDAD DE LA INFORMACIÓN EN PEQUEÑAS Y MEDIANAS EMPRESAS”, publicado en la revista de la Universidad Piloto de Colombia, realizó una investigación documental, donde describió la forma en que las pymes abordan la seguridad de la información, señalando sus principales errores al momento de implementar un SGSI, mostrando estadísticamente cuales son los incidentes de seguridad más comunes que se cometen en América Latina y exponiendo recomendaciones basadas en la norma ISO 27001:2013, mediante el ciclo de Deming, para que una pyme pueda reforzar la seguridad en sus sistemas de información mediante la aplicación de un SGSI.

De esta forma, el trabajo anterior ofrece un amplio panorama de la seguridad en los sistemas informáticos de las pymes en varios países de América Latina, la cual muchas

veces es subestimada, relegando a segundo plano la importancia que implica para una empresa la protección de sus datos informáticos, sin contemplar el alcance de las amenazas a las que se encuentran vulnerables. Así mismo, se reflejan también dificultades que presentan las pymes para realizar inversiones tecnológicas adecuadas. Por lo tanto, este trabajo sirvió como un enfoque adaptativo para el objeto de estudio de la investigación en curso, además de que se exponen datos puntuales y relevantes en relación a errores que comúnmente pueden estar cometiendo las pymes y las medidas que se podrían implementar para mitigarlos, lo cual representa un aporte significativo.

2.2. Bases Teóricas

2.2.1. Pequeñas y medianas empresas

Zevallos, E. (2003:55), afirma que existen diversos criterios para clasificar a las microempresas y pequeñas y medianas empresas (mipyme) en América Latina, los cuales incluyen el empleo (número de trabajadores), las ventas o ingresos generados por su actividad comercial, y los activos que posea. En este sentido, países como Argentina, Chile y Panamá se enfocan en los ingresos, clasificando a las empresas como grandes cuando los montos superan los 24 millones de pesos, 2,4 millones de dólares y 2,5 millones de dólares, respectivamente. Otros países como Bolivia, Colombia, Costa Rica, México y Venezuela, priorizan el número de empleados, y, para que lleguen a considerarse grandes empresas, deben superar los 49, 200, 100, 500 y 250 empleados, respectivamente. De esta forma, puede observarse que es difícil generalizar el concepto de pyme.

En este sentido, el Instituto Venezolano de los Seguros Sociales – IVSS (2021) señala en su página web, que las microempresas poseen hasta 10 trabajadores, las pequeñas poseen de 10 a 50 trabajadores, las medianas de 50 a 250, y las grandes más de 250. Además, en el Decreto con Fuerza de Ley para la promoción y desarrollo de la pequeña y mediana industria, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 37.583, de fecha 03-12-2002, se define pyme, en el art. 3, como “toda unidad de explotación económica, realizada por las personas jurídicas que efectúen actividades de transformación de materias primas en insumos, en bienes industriales

elaborados o semielaborados (...), según lo siguiente: promedio anual de trabajadores y valor de las ventas anuales(...).”.

Esta aclaratoria delimita el concepto de pyme para los fines de la investigación, donde la misma debe ser una empresa jurídica formal, sin limitación en su objeto o desempeño comercial y productivo, que posea menos de 250 trabajadores. Lamentablemente, por sus características, las pymes no suelen durar más de dos o tres años en funcionamiento desde su creación, la cual tiende a ocurrir por necesidad ante una complicada situación económica y deseos de superación.

Armas, V., en un artículo titulado “esplendor y miseria de las pymes venezolanas”, citado por Moras, F. (2003:2), declara lo siguiente:

Las pymes, sea cual fuese su grado de desarrollo tecnológico, cumple un papel importante como generadores y distribuidores del ingreso nacional. Su capacidad para emplear mano de obra poco calificada, durante las fases iniciales de los procesos de industrialización, las convierte en factor de estabilidad social. Además, las pymes contribuyen a democratizar el capital y a distribuir regionalmente el ingreso, porque están menos concentradas en las áreas industriales. La instalación de una gran empresa en un área poco desarrollada será más beneficiosa en la medida en que se desarrolle una cadena de proveedores locales que distribuyan excedentes.

Esta declaración pretende mostrar que las pymes representan un eslabón relevante en la economía, así como un impulso en lo referente al crecimiento y desarrollo del país, generando mayor intercambio de dinero en las calles, mayor capacidad de empleo, mayor generación de oferta y demanda de bienes y servicios, y mayores impuestos para la administración pública.

Culshaw, F. (2012:1), señala que “las grandes empresas en Venezuela representan algo más del 20% del sector privado. Asimismo, informa que nueve millones de venezolanos trabajan en pymes (3,5 millones lo hacen formalmente), las cuales generan 73% del empleo del país”. La realidad nacional muestra un predominio de emprendimientos que surgen de la necesidad, que son de escasa inversión, dedicadas principalmente al sector comercio (especialmente venta de alimentos), peluquería, estética y transporte. Las iniciativas de negocios innovadores o de tecnología avanzada son menos frecuentes, pero existen y luchan por abrirse camino.

Entonces, se observa que más del 70% de las empresas en Venezuela lo representan las pymes, donde la mayoría de ellas, en ocasiones denominadas emprendimientos, suelen ser de baja inversión y sencilla instalación, que por lo general solo requieren de habilidades empíricas y semiprofesionales.

Por otro lado, Culshaw, F. (*ob. cit.*) plantea que en Venezuela existen muchas regulaciones, altos impuestos y políticas que tienden a favorecer al sector público sobre el privado, sufriendo las pymes el impacto de muchas leyes que implican una enorme carga laboral, impuestos excesivos (según sus respectivos gremios), restricciones para el acceso a divisas con fines de importación, y diversas burocracias que retrasan o impiden el financiamiento formal para su desarrollo.

En vista de ello, gran parte de las grandes empresas han logrado mantenerse debido a su fortaleza y capacidad de maniobra frente a los cambios sociales y económicos, pero muchas pymes carecen de recursos, y han tenido que abandonar el negocio. De esta forma, las pymes innovadoras presentan mayores dificultades, porque requieren inversiones mayores y los financistas privados no están dispuestos a desembolsar grandes sumas debido a las dificultades económicas que ha estado enfrentando el país en los últimos años.

2.2.2. Seguridad informática

De acuerdo con Avenía, C. (2018:7), la seguridad relacionada a los sistemas informáticos “busca minimizar los riesgos asociados con el acceso y el uso de cierta información del sistema de forma no autorizada y, en general, maliciosamente”. Este punto de vista de la seguridad implica la necesidad de evaluar y cuantificar los activos a proteger (información) y, en base a estos análisis, aplicar medidas preventivas y correctivas para disminuir los riesgos a niveles que permitan asumirlos o delegarlos. En vista de ello, se involucran cuatro acciones que siempre están inmersas en cualquier asunto de seguridad, como son: prevención, transferencia, mitigación y aceptación del riesgo.

En este sentido, Romero, M.; Figueroa, G.; Vela, D.; Álava, J.; Parrales, G.; Álava, C.; Murillo, A. y Castillo, M. (2018:13) consideran que los riesgos pueden tener múltiples orígenes, como la entrada de datos, el medio que transporta la información, el hardware que es usado para transmitir y recibir, los usuarios, y los protocolos que se estén

implementando. Entonces, la seguridad debe contemplar principalmente a los usuarios que utilizan o que tienen acceso a los sistemas de información, así como a la información misma y a la infraestructura.

De esta forma, la seguridad informática debe evitar que se viole la confiabilidad, la disposición y la autenticidad de los datos, en cualquier punto de los sistemas de comunicación en el que se encuentren, considerando como factores de riesgo a los usuarios, a los dispositivos y a la infraestructura que formen parte de cualquier sistema informático. Además, la SI debe limitar las pérdidas y conseguir la adecuada recuperación del sistema en caso de un incidente de seguridad, evitando perder el control sobre lo que ocurre, cumpliendo con las regulaciones internas de la empresa, las cuales deben estar en consonancia con el marco legal vigente. Entonces, lograr definir, mantener y mejorar la SI puede ser esencial para mantener una ventaja competitiva, a nivel del flujo de caja, rentabilidad, observancia legal e imagen empresarial.

2.2.3. Políticas de seguridad

De acuerdo con la Universidad en Internet (UNIR, 2020) “las políticas de seguridad informática consisten en una serie de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información, minimizando los riesgos que le afectan”. Estas políticas deben ser autorizadas por la alta gerencia de una empresa, donde se definen los objetivos y el alcance de la misma, así como el conjunto de controles, incluyendo procedimientos e instrucciones técnicas que recogen las medidas logísticas y organizativas que se establecen para dar cumplimiento a dicha política, y que deben implementarse.

Se puede inferir que las políticas son normas plasmadas en manuales internos de la empresa, que deben ser ajustadas al tipo y complejidad de la empresa en cuestión, y que deben ser aplicadas por los empleados y cualquier individuo con acceso a alguna sección de los sistemas de información. Además, estas políticas son útiles a la hora de auditar los sistemas de información de una empresa, por lo que deben ser concretas, claras y obligatorias.

Por otro lado, Carisio, E. (2019) señala que existen dos grupos principales de políticas de seguridad informática: las que definen lo que debe evitarse, incluyendo comportamientos y prácticas que pueden poner en riesgo los sistemas y la información,

como abrir archivos o enlaces sospechosos, compartir contraseñas o utilizar redes inalámbricas de origen dudoso; y las que definen lo que se debe hacer siempre, como cifrar archivos sensibles, implementar copias de respaldo, usar contraseñas y renovarlas de forma periódica, proteger las redes mediante VPN y proxys, e instalar antivirus y antimalwares. Además, el autor recalca la importancia de determinar el alcance de las políticas de seguridad a implantar, puesto que, en mayor o menor grado, serán una fuente restrictiva a las actividades de la organización, lo que implica realizar un balance entre las ventajas y desventajas de su aplicación.

En vista de ello, es necesario decidir si algunos servicios deben ser suprimidos para garantizar la seguridad del sistema, o, por el contrario, si algunas medidas preventivas son demasiado rigurosas e impiden prestar un servicio; además, siempre hay que considerar el costo monetario que influye en todas las decisiones, sobre todo en cuanto a la contratación de personal especializado y la adquisición de hardware y software.

Profundizando un poco más en el tema, UNIR (2020) considera que el cuerpo normativo de seguridad de la información de una organización consta principalmente de las siguientes políticas y procedimientos:

- Procedimiento de control de accesos: representa las medidas técnicas y organizativas relacionadas con los permisos de acceso a las instalaciones y sistemas que albergan la información de la organización, así como el acceso a la propia información. Los controles de acceso pueden ser físicos, donde se controlan el acceso de personas a las instalaciones de la organización (tornos, barreras, cámaras, alarmas, sistemas de apertura de puertas biométricos o por tarjeta, entre otros), o lógicos, que corresponde a los sistemas implementados para controlar el acceso de los usuarios a los distintos sistemas que albergan la información o el acceso a la propia información (la implementación de un control de acceso de equipos y usuarios a la red, la configuración de permisos de lectura y escritura sobre los propios archivos de información, sistemas de *login* en los distintos sistemas, autorizaciones de acceso remoto de los usuarios a la red a través de una VPN, entre otros).
- Procedimiento de gestión de usuarios: consiste en las instrucciones precisas a realizar para la concesión de los permisos de acceso (físicos y lógicos) que

deberían tener los usuarios (permisos mínimos y necesarios para el cumplimiento de su trabajo) a las instalaciones, sistemas y a la propia información. Este procedimiento debe definir, de forma clara y concisa, los diferentes roles y responsabilidades de los usuarios.

- Procedimiento de clasificación y tratamiento de la información: incluye las instrucciones acerca de cómo clasificar la información de acuerdo a su valor (requisitos legales, sensibilidad y criticidad para la organización), y las medidas de protección y de manipulación acorde a la clasificación de la misma.
- Procedimiento de gestión de incidentes de seguridad de la información: instrucciones para la notificación de incidentes, así como de las respuestas a los mismos con las acciones a realizar al ser detectados.
- Gestión de activos de información: corresponde al resguardo de los datos, mediante el almacenamiento seguro de copias de seguridad de la información, monitoreo de seguridad de la red, uso de antimalwares, registro y supervisión de eventos, actualización y parcheo de sistemas y equipos, entre otros.

2.2.4. Servidores

Marchionni, E. (2011:23) describe a los servidores desde el punto de vista del hardware, señalando lo siguiente:

Los servidores son equipos informáticos que brindan un servicio en la red, dando información a otros servidores y a los usuarios. Además, cualquier computador puede cumplir el rol de servidor, aunque a un nivel más profesional suelen ser equipos de mayores prestaciones y dimensiones que una computadora común. En este sentido, esta última tiene solo un procesador (pese a que sea de varios núcleos), incluyendo un disco rígido para el almacenamiento de datos con una capacidad de 250 GB a 1 TB, en tanto que la memoria RAM suele ser de 2 a 16 GB; mientras tanto, un servidor puede tener varios procesadores con varios núcleos cada uno, e incluye grandes cantidades de memoria RAM, entre 16 GB a 1 TB, o más, sumado a poseer un espacio de almacenamiento que no se limita a un solo disco duro, por lo que fácilmente puede superar 1 TB. En vista de estas capacidades, un servidor puede dar un solo servicio o más de uno.

De igual manera, Borges, S. (2020, párr. 4), explica que un servidor se encarga de despachar los datos que le son solicitados y que se encuentran almacenados en su sistema, pudiendo referirse a diferentes funciones dependiendo del propósito del

servidor: sitios web enteros, datos puntuales de una base de datos, contenido estático como imágenes o videos, entre otras muchas cosas. Para Marchionni, E. (2011:27), los servicios indispensables en una empresa son el correo electrónico, el servidor de archivos (conocido como *file server*), cuya función es almacenar gran cantidad de información para que los empleados puedan acceder a ella desde cualquier lugar de la red; servicios de respaldo de datos, de almacenamiento, de asistente de escritorio, de seguridad y de procesos.

En este sentido, un servidor puede ser un equipo informático con las características de procesamiento de un computador, que le permita prestar al menos un servicio de almacenamiento, así como también puede ser un equipo especializado con alto poder de cómputo que le permita ofrecer un gran número de servicios; todo ello dependerá de los requerimientos de la empresa, adaptados a su respectiva disposición económica y técnica para adquirir y administrar los equipos.

2.2.4.1 Tipos de servidores

Los servidores pueden clasificarse, de acuerdo a la ubicación donde se encuentran los equipos con funciones de servidor, en locales o remotos. Borges, S. (2020), indica que un servidor local, como lo dice su nombre, es un servidor que está ubicado físicamente en la misma ubicación que las personas o empresas que le dan uso, como su respectiva casa u oficina, mientras que el servidor remoto se localiza en otro lugar distante a la empresa.

Entonces, el servidor se puede ubicar dentro de la empresa, de forma local, o puede ubicarse en un centro de datos que se encargue de proporcionar un servidor a las empresas o usuarios, como en el caso del servidor remoto, el cual generalmente presta servicios web.

2.2.5. Redes informáticas

Posterior a la creación de las computadoras y a su importante uso, surgió la necesidad de interconectar diferentes dispositivos para poder compartir los diferentes recursos, lo que dio origen a una red informática. En base a ello, Barceló, J.; Íñigo, J.; Martí, R. y Perramon, X. (2004) señalan que el diseño de las redes LAN partió de un camino completamente diferente del que se siguió para las redes de gran alcance, como las redes

telefónicas pensadas para interconectar dos estaciones, debido a que se requería establecer comunicaciones “muchos a uno” y “uno a muchos”, lo que era difícil de conseguir con las redes de conmutación. Por ello se empleó la difusión con medio compartido, donde los paquetes que salen de una estación llegan a todo el resto simultáneamente. En la recepción, las estaciones los aceptan o ignoran dependiendo de si son destinatarias de los mismos o no, lo cual es gestionado mediante los diferentes protocolos de red.

Raffino, M. (2020) define una red informática como “un número de sistemas informáticos conectados entre sí mediante una serie de dispositivos alámbricos o inalámbricos; gracias a los cuales pueden compartir información en paquetes de datos, transmitidos mediante impulsos eléctricos, ondas electromagnéticas o cualquier otro medio físico”.

De acuerdo con esto, las redes informáticas surgen por la evolución tecnológica y por la necesidad de compartir todo tipo de archivo, en el menor tiempo posible y con técnicas de seguridad que ofrezcan confianza de su uso a los usuarios, pudiendo definirse estas redes como un sistema de interconexión de dispositivos electrónicos que permite a sus usuarios compartir diversos tipos de datos y recursos, como texto, audio y video.

Rodríguez, M. (2013) señala, respecto con los dispositivos relacionados a una red informática, lo siguiente:

Los dispositivos conectados a una red informática pueden clasificarse en dos tipos: los que gestionan el acceso y las comunicaciones en una red (dispositivos de red), como *módem*, *router*, *switch*, *access point*, *bridge*, entre otros; y los que se conectan para utilizarla (dispositivos de usuario final), como computadora, *notebook*, *tablet*, teléfono celular, impresora, televisor inteligente, consola de videojuegos, entre otros.

Básicamente, la red la conforman el conjunto de dispositivos y elementos que permiten el funcionamiento de la red, y los aparatos electrónicos que servirán como terminales para acceder o compartir cualquier tipo de dato con otros dispositivos que estén conectados a esa red.

Así mismo, Molero, L. (2013) menciona que la información de la red se transmite por un sistema de dispositivos autónomos de red, incluyendo impresoras (de haberlas) y aplicaciones de software, interconectados mediante comunicaciones por cable, fibra óptica u ondas de radio. El autor señala que “para intentar estandarizar un sistema de

comunicación globalizado, surge el Modelo de Interconexión de Sistemas Abiertos (OSI), de la Organización Internacional de Estandarización (ISO), el cual define siete capas: física, enlace de datos, red, transporte, sesión, presentación y aplicación”.

De igual manera, el funcionamiento general de una red se basa en que, al ser solicitada una señal desde un computador, ésta es codificada por el adaptador de red en forma de bits, para ser transmitida a través de un cable o medios inalámbricos. Para esto, se utilizan protocolos, que de acuerdo con Turolto, T. (2015:7) “son reglas o estándares que definen la sintaxis, semántica y sincronización de la comunicación, así como también los posibles métodos de recuperación de errores, y pueden ser implementados por el hardware y el software”. El modelo de protocolos más conocido e importante es el TCP/IP, que permite la comunicación entre equipos al especificar y gestionar el formateo, direccionamiento y transmisión de los datos entre un dispositivo emisor y otro receptor. Además, las tarjetas de red tienen una dirección MAC única e irrepetible, que les permite identificarse claramente para que la información llegue al receptor adecuado.

La necesidad de estandarizar protocolos y procedimientos en la transferencia de paquetes de datos, surgió de la diversidad de fabricantes de hardware que empleaban distintos mecanismos para la conexión de las redes informáticas, haciéndolo costoso, limitado e inefectivo. Entonces, OSI y TCP/IP son los modelos globales empleados por las empresas generadores de hardware y software de red referentes a los sistemas de comunicación.

2.2.5.1. Tipos de redes informáticas

Rodríguez, M. (2013) indica que los medios que permiten la conexión entre dispositivos pueden clasificarse, de acuerdo al tipo de conexión, en guiados (red alámbrica) o en dirigidos (red inalámbrica). Los primeros agrupan el cable coaxial, el cual se compone de un hilo conductor de cobre, y transporta señales eléctricas de alta frecuencia; el cable de par trenzado, que es el típico cable ethernet, con 3 pares de cables aislados y entrelazados; y la fibra óptica, que es un filamento delgado de vidrio o de plástico que transmite datos mediante pulsos de luz láser o led. Los dirigidos se encuentran conformados por las ondas de radio (*wifi* y *bluetooth*), las infrarrojas y las microondas, que es la forma en la que se conectan los modem a la red.

Las redes alámbricas son mejores cuando se necesita mover grandes cantidades de datos a altas velocidades, como medios multimedia de calidad profesional, además de que son más estables; en cambio, las redes inalámbricas permiten la conexión de múltiples dispositivos, sin necesidad de un sistema de cableado que limite el espacio y la estructura de la red física. En vista de ello, es muy común que las organizaciones tengan un diseño de red principal mediante cableado, complementado con dispositivos de emisión de *wifi*.

2.2.6 Sistema de gestión de la seguridad de la información

De acuerdo con Benjumea, O. (2012), un sistema de gestión de la seguridad de la información (SGSI) consiste en un “conjunto de políticas y procedimientos que normalizan la gestión de la seguridad de la información, bien de toda una organización o bien de uno o varios de sus procesos de negocio”. El autor señala que existen diversos estándares, marcos de trabajo o metodologías para implantar y mantener un SGSI, pero sin duda, la más empleada es la serie ISO 27000, la cual comprende todo un conjunto de normas relacionadas con la seguridad de la información, de entre las que destacan la ISO 27001 (establece el marco de trabajo para definir un SGSI, centrándose en la visión de la gestión de la seguridad como un proceso continuo en el tiempo) y la ISO 27002 (buenas prácticas para gestión de la seguridad de la información).

Desde la visión de la web ISO 27000 (2020), un SGSI es un “enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización”.

Así, los SGSI tienen una relación directa con las políticas de seguridad que se establezcan, así como con diversas normas internacionales, entre las que destacan las ISO, ITIL (Biblioteca de Infraestructura de Tecnologías de Información) y COBIT (Objetivos de Control para Tecnología de Información y Tecnologías Relacionadas). EN consecuencia, este tipo de sistemas debe ser adaptado a las características especiales de una empresa, y que estén optimizados desde el punto de vista de los recursos necesarios para implantarlos y mantenerlos.

2.3. Bases Legales

2.3.1. Constitución de la República Bolivariana de Venezuela (publicada en Gaceta Oficial Extraordinaria N.º 36.860, de fecha 30 de diciembre de 1.999)

Art. 57.- Toda persona tiene derecho a expresar libremente sus pensamientos, sus ideas u opiniones de viva voz, por escrito o mediante cualquier otra forma de expresión, y de hacer uso para ello de cualquier medio de comunicación y difusión, sin que pueda establecerse censura.

De esta forma, la ley respalda y protege a los investigadores que se ocupen de describir cualquier fenómeno o tema de estudio.

Art. 110.- El Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional.

Se observa el interés nacional por el desarrollo de la ciencia y la tecnología como herramientas e instrumentos primordiales en las principales áreas productivas y sociales, en virtud del desarrollo y crecimiento de la nación. El uso de la tecnología en las pymes permite facilitar el trabajo de las personas y de expandir nuevas actividades y negocios, lo cual es reconocido por la Constitución en este artículo, al establecer la tecnología como un instrumento fundamental para el desarrollo económico.

Art. 156.- Es de la competencia del Poder Público Nacional: (...) 28. El régimen del servicio de correo y de las telecomunicaciones, así como el régimen y la administración del espectro electromagnético (...).

Por tanto, el Estado efectuará controles y regulaciones mediante distintos instrumentos jurídicos en relación a las telecomunicaciones y al uso seguro de las redes informáticas.

2.3.2. Ley Orgánica de Telecomunicaciones (publicada en Gaceta Oficial N.º 39.610, de fecha 7 de febrero de 2011)

Art. 12.- En su condición de usuario de un servicio de telecomunicaciones, toda persona tiene derecho a: 1. Acceder en condiciones de igualdad a todos los servicios de

telecomunicaciones y a recibir un servicio eficiente, de calidad e ininterrumpido (...) 2. La privacidad e inviolabilidad de sus telecomunicaciones (...).

En este sentido, los ciudadanos naturales y jurídicos tienen la potestad de adquirir algún servicio relacionado con las telecomunicaciones, especialmente en cuanto a telefonía e internet, el cual debe permitir su uso con carácter confidencial y privado.

2.3.3. Ley sobre Protección a la Privacidad de las Comunicaciones (publicada en Gaceta Oficial N.º 34.863, de fecha 16 de diciembre de 1991)

Art. 1. La presente Ley tiene por objeto proteger la privacidad, confidencialidad, inviolabilidad y secreto de las comunicaciones que se produzcan entre dos o más personas.

De este modo, se busca garantizar la confidencialidad de los datos transmitidos en las telecomunicaciones, castigando bajo diversos mecanismos a cualquier infractor que busque tomar, sin autorización, cualquier información procedente de algún dispositivo de comunicación o de almacenamiento de los mismos.

2.3.4. Ley sobre el Derecho de Autor (publicada en Gaceta Oficial Extraordinaria N.º 4.638, de fecha 1 de octubre de 1993)

Art. 1. Las disposiciones de esta Ley protegen los derechos de los autores sobre todas las obras del ingenio de carácter creador, ya sea de índole literaria, científica o artística, cualquiera sea su género, forma de expresión, mérito o destino (...).

Art. 2. Se consideran comprendidas entre las obras del ingenio a que se refiere el artículo anterior, especialmente las siguientes: los libros, folletos y otros escritos literarios, artísticos y científicos, incluidos los programas de computación, así como su documentación técnica y manuales de uso (...).

Complementando ambos artículos, la ley protege los derechos de índole intelectual relacionados con todos los trabajos de investigación y obras originales que sean de creación de las personas, individual o colectivamente.

2.3.5. Ley Especial Contra los Delitos Informáticos (publicada en Gaceta Oficial N.º 37.313, de fecha 30 de octubre de 2001)

Art. 1. La presente Ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos

cometidos contra tales sistemas o cualesquiera de sus componentes, o de los delitos cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta Ley.

Tal como lo indica el mencionado artículo, la presente ley trata, de forma más específica, el tema de los ataques informáticos y los intentos de sabotaje empresarial a nivel de los sistemas computacionales, estableciendo límites y sanciones para todos aquellos delincuentes que infrinjan alguno de los artículos descritos en la misma.

2.4. Definición de términos

Amenaza:

“Situación o evento que puede afectar la posibilidad de que las organizaciones o las personas puedan desarrollar sus actividades afectando directamente la información o los sistemas que la procesan”. (Tarazona, 2007).

Ataque informático:

“Consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema”. (Mieres, 2009).

Bit:

“Unidad mínima de información, que puede tener solo dos valores, cero o uno”. (Oxford *Languages*).

Control:

Evaluar y supervisar que todas las actividades relacionadas a los sistemas de información y comunicación que formen parte de las pymes, se realicen cumpliendo las normas internas, estándares, procedimientos y disposiciones legales establecidas. (Definición propia).

Cracker:

“Persona que se dedica a entrar en sistemas informáticos de forma no autorizada e

ilegal para conseguir información, perturbarlos, alterar su funcionamiento, inutilizarlos con fines dañinos u otros propósitos delictivos”. (Diccionario Panhispánico del español jurídico).

Dato:

“Es una representación simbólica (numérica, alfabética, entre otros) de un atributo o característica de una entidad. El dato no tiene valor semántico (sentido) en sí mismo, pero convenientemente tratado (procesado) se puede utilizar en la realización de cálculos o toma de decisiones”. (DAC-UCLA, 2005).

Hacker:

“Persona experta en alguna rama tecnológica que accede a un sistema informático o a informaciones ubicadas en dicho sistema o en la red de comunicaciones sin permiso del titular. Se diferencia del cracker en que no causa daños o no inutiliza el sistema”. (Diccionario Panhispánico del español jurídico).

Información:

“Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno”. (DAC-UCLA, 2005).

MAC:

“Es el identificador único asignado por el fabricante a una pieza de hardware de red (como una tarjeta inalámbrica o una tarjeta Ethernet)”. (Tanenbaum y Wheterall, 2015).

Malware:

También conocido como software malicioso, es cualquier tipo de programa informático diseñado para infectar la computadora de un usuario legítimo y causarle alguna acción dañina, sin conocimiento de este usuario. (Definición propia).

Mitigar:

“Moderar, aplacar, disminuir o suavizar algo riguroso”. (RAE).

Nivel de seguridad:

Representa el estado de la seguridad en la infraestructura o área tecnológica de la organización donde se ubican los elementos de los sistemas de comunicación, incluyendo el hardware o todos los dispositivos físicos que interactúan en las redes informáticas, y el software o programas informáticos que ocupan alguna función en éstas redes. (Definición propia).

Protocolos:

“Son reglas o estándares que definen la sintaxis, semántica y sincronización de la comunicación, así como también los posibles métodos de recuperación de errores, y pueden ser implementados por el hardware y el software”. (Turolto, 2015).

Puerto:

“Interfaz desde la que se envían o reciben diferentes tipos de datos, pudiendo ser físicas o lógicas”. (López, 2016).

Pymes:

Pequeñas y medianas empresas es un tipo de clasificación de empresas en Venezuela que se refiere a poseer un número de trabajadores inferior a 250 individuos. (Definición propia).

Red alámbrica:

Utilizan cables para establecer la comunicación entre equipos, pudiendo ser cable coaxial, cable de par trenzado o fibra óptica. (Definición propia).

Red inalámbrica:

“Utilizan el aire o el espacio para poder transmitir los datos sin uso de cables, mediante ondas electromagnéticas como wifi o bluetooth”. (Proaño, 2009).

Servidores:

“Son equipos informáticos que brindan un servicio en la red, dando información a otros servidores y a los usuarios”. (Marchionni, 2011).

Servidor local:

“Es un servidor que está ubicado físicamente en la misma ubicación que las personas o empresas que le dan uso”. (Borges, 2020).

Sistemas de comunicación:

Conjunto de componentes o subsistemas que permiten la transferencia de información a través de distintos medios, entre un emisor y un receptor. Las redes informáticas forman parte de los principales sistemas de comunicación. (Definición propia).

TCP/IP:

“Es un modelo que describe un conjunto de guías generales de diseño e implementación de protocolos de red específicos para permitir que un equipo pueda comunicarse en una red. Provee conectividad de extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario”. (Turolto, 2015).

Vulnerabilidad:

“Debilidad en la tecnología o en los procesos relacionados con la información, y como tal, se considera una característica propia de los sistemas de información o de la infraestructura que los contiene”. (Tarazona, 2007).

PARTE III

DESCRIPCIÓN METODOLÓGICA

Balestrini, M (2006:125), define el marco metodológico como “la instancia referida a los métodos, las diversas reglas, registros, técnicas y protocolos con los cuales una teoría y su método calculan las magnitudes de lo real”. De esta manera, en esta parte se procede a indicar la naturaleza de la investigación, la cual implica el tipo y diseño de la investigación y la población y muestra de estudio; así como las técnicas de recolección y análisis de datos a emplear.

3.1. Naturaleza de la Investigación

De acuerdo con Balestrini, M. (2006:5), en la investigación cuantitativa “se asignan metódicamente símbolos a las características observadas sobre la dimensión que se está estudiando, o se asignan números a un objeto de conocimiento según reglas, apoyados en procesos estadísticos. que pueden introducir o no la medición”. Al pretenderse hacer un estudio objetivo, enfocándose en un área lógica como son los niveles de seguridad en los sistemas de comunicación, la presente investigación se enmarca en un enfoque cuantitativo para poder aprovechar distintos recursos de esta naturaleza en la construcción de la perspectiva teórica.

3.1.1. Tipo de investigación

Según Balestrini, M. (2006:7), en la investigación evaluativa “se propone describir y comprender las relaciones significativas entre las variables; así como el establecimiento de la secuencia causal en la situación o hecho estudiado”. La presente investigación es de tipo evaluativa, puesto que durante su desarrollo se enfocó en describir, comprender y evaluar los factores relacionados con los niveles de seguridad y control que deben aplicarse en las pymes para garantizar la seguridad, tanto en sus redes informáticas como en sus servidores locales.

3.1.2. Diseño de la investigación

Arias, F. (2012:27) define a la investigación documental como “un proceso basado en la búsqueda, recuperación, análisis, crítica e interpretación de datos secundarios, es

decir, los obtenidos y registrados por otros investigadores en fuentes documentales: impresas, audiovisuales o electrónicas”. Este diseño es aplicado en la presente investigación debido a que se necesita la recopilación de información desde distintas fuentes secundarias para permitir el desenvolvimiento de la misma; puesto que la problemática no se encuentra delimitada dentro del ámbito físico donde se pueda obtener la información *in situ*.

3.1.3. Objeto de estudio

Pedraz, M. (2002:1) señala que el objeto de estudio es “aquello sobre lo cual recae una acción, especialmente intelectual, y en la medida en que define un fenómeno o una perspectiva con la que se aborda un fenómeno, constituye uno de los requisitos que definen un campo de intervención científica”. De esta manera, el objeto de estudio representa el tema de investigación, donde se plantean cuestiones concretas que se desean desarrollar y se establecen los límites de la tarea. Por lo tanto, esta investigación está centrada en cuatro (4) temáticas principales: pymes, seguridad y control, servidores locales y redes alámbricas e inalámbricas.

3.1.4. Acopio y selección de la información

De acuerdo con Cázarez, L.; Christen, M.; Jaramillo E.; Villaseñor L. y Zamudio, L. (1999:22), el acopio de la bibliografía sobre el objeto de estudio consiste en “reunir, antes que nada, todo el material publicado o inédito sobre el mismo, ya se trate de artículos, estudios críticos, monografías, ensayos, documentos de archivo, libros, tesis, entre otros”. Para la presente investigación se consultan fuentes primarias, secundarias y terciarias, en diversos formatos digitales, como páginas web, libros, revistas científicas, trabajos de grado, documentos legales y normativas internacionales en la materia de interés, confiables en el ámbito científico y con suficientes pruebas prácticas para desarrollar los objetivos planteados. Las consultas se realizaron a través de internet mediante el uso de un computador, donde también se almacenó la información obtenida.

Además, los criterios de selección y validación de las fuentes documentales fueron los siguientes: vigencia, pertinencia, relevancia y validez de la fuente. Con respecto a la vigencia, se tomaron en consideración documentos con una antigüedad de publicación inferior a 15 años; la pertinencia se refiere a si se encuentran relacionados con alguno de

los temas centrales de la investigación; la relevancia está referida a si el documento presenta de manera novedosa la temática de estudio; y la validez de la fuente se trata de la confiabilidad de quien presenta los datos, específicamente: autores reconocidos/especializados, sitios web confiables y con fuentes fidedignas, publicaciones oficiales o recursos con enlaces de validación.

3.2. Técnicas de recolección de datos

La técnica de recolección de datos empleada fue la revisión documental, definida por Arias, F. (2012:106) como “una recopilación de ideas, posturas de autores, conceptos y definiciones, que sirven de base a la investigación”. De esta forma, en el desarrollo de la revisión documental se emplearon distintas fuentes, mencionadas previamente en el apartado de acopio y selección de la información, con el fin de recopilar información del objeto de estudio.

El instrumento utilizado fue la ficha de investigación, definida por Cázares, L., *et al.* (1999:37), como un “medio para recolectar los datos de cada libro y de cada publicación periódica que se utilizan para estudiar o para realizar un trabajo de investigación”. Entonces, la ficha de investigación es un sistema de orden para ubicar dónde está cada fuente de información consultada en el transcurso de la investigación; por ello se emplearon ficheros digitales para almacenar los documentos digitales, fichas de contenido y fichas mixtas, así como todas las anotaciones de interés en la medida que se iba desarrollando la investigación, dentro del espacio de almacenamiento de un computador.

3.3. Técnicas de análisis de datos

Los datos obtenidos fueron clasificados, registrados y esquematizados de acuerdo a la importancia y grado de pertenencia respecto a cada uno de los objetivos de la investigación. También se hizo uso de la tabulación, que consiste en agrupar datos en tablas para una presentación óptima, de acuerdo a los respectivos requerimientos. Así mismo, se emplearon técnicas deductivas basadas en el análisis crítico.

Araujo, M. (2012:1) define el análisis crítico como un “proceso de evaluación que permite al lector formarse una idea del potencial de error en los resultados de un estudio (...), no entregando una sentencia definitiva sobre la condición de verdad de los

resultados, pero dando una aproximación indirecta a ella”. De esta manera, se procede a identificar las ideas principales del autor en cada bibliografía consultada, contrastando posteriormente sus planteamientos con el criterio propio y con el criterio de otros autores, seleccionando la información más relevante y confiable, lo que facilita el abordaje del objeto de estudio.

Por otro lado, también se empleó la presentación resumida, definida por Romero, J. y Bandres, A. (2010:20) de la siguiente manera:

Consiste en dar testimonio fiel de las ideas contenidas en un texto. Esta presentación debe seguir esencialmente la estructura del texto, de manera que la persona obtenga un conocimiento completo y preciso de las ideas básicas, partiendo del resumen efectuado. Este modelo de trabajo se basa en la capacidad de síntesis del autor.

Para la presentación resumida, se procedió a leer y redactar brevemente distintos párrafos de importancia con palabras propias del investigador, aunque en algunos casos se citó textualmente, para generar información de interés que fue posteriormente reflejada en la investigación. La información a la que se aplicó esta técnica fue aquella donde la cantidad de autores que manejaban un mismo tema era mayor, generalmente cuando eran más de tres.

PARTE IV

ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

Según Balestrini, M (2006:169), “los datos, posterior a su fase de recolección, han de ser sometidos a un proceso de elaboración técnica, que permite recontarlos y resumirlos (...)”. De esta forma, el autor señala que esta fase de desarrollo del proyecto de investigación comprende la incorporación de algunos lineamientos generales para el análisis e interpretación de los datos; su codificación y tabulación y sus técnicas de presentación; buscando cumplir el objetivo de proporcionar respuesta a sus interrogantes.

Posterior a revisar, clasificar y almacenar todo el material bibliográfico consultado y adquirido para desarrollar la presente investigación, se procedió al análisis en función de los objetivos de la misma, realizando los respectivos resúmenes teóricos (presentación resumida) y análisis críticos; además, se tabuló y diagramó ocasionalmente la información para permitir una visualización más clara y resumida de los datos descritos a lo largo de esta parte.

4.1 Identificación de los factores que se deben considerar al establecer la seguridad de los servidores locales y las redes alámbricas e inalámbricas de una pyme

En el presente apartado, se realizó una delimitación del concepto pyme en cuanto a los factores que se deben considerar al establecer la seguridad en sus sistemas de comunicación y servidores locales; además se describieron los principales factores de la seguridad de la información, así como los distintos niveles que ésta abarca.

En Venezuela, una pyme se define como una organización o empresa que posee máximo 250 empleados, sin hacer referencia a algún otro factor clasificatorio, como los ingresos, el objeto social, la complejidad de sus instalaciones o la cantidad y tipos de activos que posea. Para realizar una investigación de los factores a considerar para establecer la seguridad en una pyme, es necesario establecer criterios que le permitan ser objeto de un análisis efectivo, para permitir la posible implementación de medidas de seguridad que se describirán en análisis posteriores. En este sentido, al hacer mención de la seguridad en los servidores locales y redes alámbricas e inalámbricas de las pymes, en el **cuadro 1** se establece que la misma debe poseer por lo menos un computador que

pueda cumplir funciones de servidor local, así como de dispositivos que permitan la transmisión de datos y el funcionamiento de una red LAN.

De esta manera, una pyme objeto de estudio será aquella organización que posea menos de 250 trabajadores, sin límites en cuanto a su ocupación, ingresos y ubicación, y que posea dispositivos electrónicos que permitan la comunicación con redes externas, como el internet. Por este motivo, quedan descartados los pequeños emprendimientos que se manejen de forma manual, sin datos digitales o algún sistema computacional (ya sea inventarios, órdenes de compra y pagos, entre otros). Además, es necesario señalar que el cuidado en la seguridad de una pyme es escalable al número de computadores y dispositivos de red y de servidores que posea.

Criterio	Descripción
Número de Empleados	$0 < NE < 250$
Requerimiento mínimo de equipos	Computador operativo con función de almacenamiento.
	Modem.
	Router.
Servicios	Energía eléctrica.
	Acceso a Internet.

Cuadro 1. Criterios que debe cumplir una pyme objeto de estudio.

Fuente: Elaboración propia.

En este sentido, la seguridad en los sistemas informáticos y de comunicaciones, en relación a los servidores locales y las redes alámbricas e inalámbricas, poseen el principal objetivo de proteger todos los datos disponibles en determinado sistema computacional. De acuerdo con Borghello, C. (2001), la vulneración a alguna sección de los sistemas previamente mencionados, así como de los procesos operativos de la información, podría permitir la interrupción, modificación o lectura no autorizada del comportamiento normal de los datos, en cuanto a su función y diseño original, lo que implica que se debe prestar especial atención a todos los dispositivos que formen parte de la red, así como de las formas de acceder a ellas.

Así, los datos son un activo muy valioso en las pymes, pese a que muchas veces no se valora adecuadamente debido a su intangibilidad. Se considera que existe seguridad en los servidores locales y en las redes alámbricas e inalámbricas de una pyme, cuando se protegen los siguientes aspectos fundamentales: la confidencialidad, la integridad y disponibilidad de la información. De acuerdo con Costas, J. (2014), éstos conceptos “son muy comunes en el ámbito de la seguridad y aparecen como fundamentales en toda arquitectura de seguridad de la información”, principalmente en cuanto a la protección y seguridad de datos se refiere, lo que incluye normativas relacionadas a la seguridad informática, códigos de buenas prácticas sobre gestión de la seguridad de la información y de importantes certificaciones internacionales relacionadas con la auditoría de estos sistemas. A continuación, se define cada una de ellas:

- Confidencialidad: se refiere a que la información, cuando se considera privada, solo debe poder ser accedida, procesada y comprendida por usuarios autorizados.
- Integridad: es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original.
- Disponibilidad: la información debe estar siempre disponible para poder ser procesada por personas autorizadas cuando éstas lo requieran.

Según Borghello, C. (2001), “éstas tres características son primordiales debido a que, tanto las amenazas como los mecanismos de seguridad para contrarrestarlas, suelen afectarlas de forma conjunta”. En ocasiones, dependiendo del entorno en que un sistema trabaje, se podría dar prioridad a alguno de los aspectos de seguridad descritos previamente; sin embargo, en la seguridad informática y de los sistemas de comunicación tienen el mismo nivel de importancia.

En cuanto a las áreas o niveles de atención especial para la seguridad de los datos, la seguridad de una pyme abarca la infraestructura tecnológica, conformada por hardware y software, que combinados operacionalmente brindan el soporte al flujo de la información. Como el objetivo siempre es proteger las propiedades de la seguridad de los datos (confidencialidad, integridad y disponibilidad), es necesario cuidar y prestar especial atención al acceso de los puertos físicos y lógicos de los dispositivos que forman

parte de la red, que son los canales empleados por los piratas informáticos para acceder o corromper sistemas o dispositivos ajenos. Por lo tanto, los niveles de seguridad se describen a continuación.

- **Hardware:** comprende los computadores y dispositivos físicos, así como la configuración y cableado de las redes y sus respectivos servidores. Este nivel de seguridad comprende la protección de los equipos previamente mencionados frente a los peligros físicos del entorno, como polvo, humedad excesiva, altas temperaturas, riesgo de caídas o impactos; así como de amenazas humanas que pretendan acceder al sistema mediante algún puerto físico para extraer información, o insertar algún tipo de *malware* para causar daños o intentar obtener control del sistema informático, o de alguna parte del mismo.
- **Software:** algunas de las principales amenazas, en cuanto al software, son el acceso y modificaciones no autorizadas a datos y aplicaciones. Por ende, es necesario hacer uso de la seguridad lógica, la cual se basa en la efectiva administración de los permisos y el control de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos. Borghello, C. (2001) considera que mediante ello se busca cumplir los siguientes objetivos:
 - Restringir el acceso a los programas y archivos.
 - Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviado y no a otro.
 - Que la información transmitida no sufra modificaciones no autorizadas.

Por otro lado, es imprescindible conocer el tipo de amenazas a los que está sujeto cualquier sistema que implique la interconexión de dispositivos electrónicos, para poder tomar medidas oportunas y realizar evaluaciones efectivas que permitan asegurar los aspectos de seguridad de los datos descritos previamente. Partiendo de ello, Caicedo, J. y Rojas, J. (2017) tabularon los principales tipos de amenazas que atentan contra un sistema informático, así como del origen de dichas amenazas (**ver cuadro 2**). En dicho cuadro, se clasifica el tipo de amenaza de acuerdo a situaciones determinadas, como acciones no autorizadas, amenazas humanas, acciones que comprometen la información, errores en las funciones establecidas, daño físico, eventos naturales, fallas técnicas y pérdida de los servicios esenciales; estos tipos de amenazas corresponden a

los distintos niveles de seguridad planteados previamente, ya sea ubicándose en el nivel de hardware o de software.

Con respecto a los ataques informáticos, conocer la forma en la que puede ocurrir puede ayudar a tomar medidas que mitiguen el riesgo. En una primera instancia, el atacante puede usar técnicas de ingeniería social, que se describe como el uso de argucias y engaños contra usuarios para obtener información confidencial; el *dumpster diving*, que consiste en recoger documentos con datos importantes del basurero; el *sniffing*, donde se rastrea el tráfico de datos de una red interna; y el *shoulder surfing*, que busca captar contraseñas o datos cuando algún usuario los marca en el teclado. Posterior a esa etapa de reconocimiento, el delincuente puede que obtenga información como direcciones IP, datos de autenticación o nombres de host, para explorar las vulnerabilidades, incluso usando herramientas de escaneo y mapas de red, que generalmente son empleadas también para evaluar sistemas con el fin de aumentar su seguridad.

TIPO	AMENAZAS	ORIGEN
Acciones no autorizadas	Abuso de privilegios	Accidental o deliberada
	Acceso no autorizado al sistema de información	
Amenazas humanas	Ataques de ingeniería social	Deliberada
	Ataques de piratas informáticos	
	Espionaje industrial	
	Spam	
	Terrorismo	
Compromiso de información	Hurto de equipos	Deliberada
	Intercepción de señales	
	Infección con software malicioso	Accidental o deliberada
Compromiso de las funciones	Error en el uso de los sistemas de información	Accidental
	Incumplimiento en el mantenimiento	Accidental o deliberada
Daño físico	Fuego	Accidental o deliberado
	Agua	
	Polvo, corrosión, golpes	
	Fluctuaciones de energía eléctrica	
Eventos naturales	Inundaciones	Accidental
	Terremotos	
Fallas técnicas	Mal funcionamiento del sistema de información	Accidental o deliberada
	Falla de los equipos de telecomunicaciones	
	Saturación del sistema de información	
Pérdida de los servicios esenciales	Pérdida del suministro de energía	
	Pérdida del suministro de ventilación	

Cuadro 2. Tipos y orígenes de las amenazas a la seguridad informática.

Fuente: Caicedo, J. y Rojas, J. (2017).

Posterior a ello, si el atacante encuentra alguna vía de entrada debido a una vulnerabilidad del sistema, podría emplear ataques que la exploten, como el *buffer*

overflow, que puede afectar a sistemas operativos, aplicaciones o protocolos, y se basa en sobrescribir una dirección de memoria para ingresar instrucciones mediante un código arbitrario o buffer y tomar control del sistema; la denegación distribuida de servicio, que implica la saturación de los puertos de red con múltiples flujos de información; el filtrado de *password* o secuestro de sesión para obtener credenciales desde las cookies. Luego de que el ataque ha ocurrido, el perpetrador buscará la manera de mantener el acceso en el futuro, por lo que podría usar *backdoors*, que son un tipo de troyano que mantiene una vía de acceso oculta; *rootkits*, que ocultan la presencia al control de los administradores; o troyanos, que son un tipo de *malware* que brinda acceso al equipo infectado y que se percibe inicialmente como un programa inocuo.

4.2 Especificación de las normas internacionales que regulan la seguridad de los servidores locales y las redes alámbricas e inalámbricas.

Las normas internacionales que buscan proteger la información de las empresas, frente a las diversas amenazas del entorno, surgieron especialmente para que las grandes empresas creadoras de tecnología, así como los grandes centros de inteligencia gubernamentales, pudieran crear marcos de trabajo y sistemas de control en todas las etapas de su gestión, intentando evitar principalmente la fuga de información; posteriormente, se fue extendiendo al resto de empresas en el mercado de la tecnología, e incluso a otros mercados. En este sentido, las instituciones y equipos encargados del diseño y creación de las diversas normas en relación a la gestión de seguridad de los sistemas informáticos han actualizado periódicamente su documentación para seguir los avances tecnológicos, tanto ofensivos como defensivos.

Además, han surgido, en las últimas dos décadas, guías, normas y marcos de trabajo en diferentes regiones del globo, que buscan adaptar sus necesidades particulares al proceso de gestión de la seguridad de la información. De igual manera, ha aumentado la presión a las empresas que manejan base de datos de usuarios registrados en muchos países, como es el caso de la Unión Europea con el Reglamento General de Protección de Datos (GDPR, según sus siglas en inglés), donde se exigen mínimos niveles de seguridad para poder mantenerse operativos.

En vista de lo previamente mencionado y para el interés de la presente investigación, se procedió a seleccionar las normativas internacionales en materia de seguridad de los

sistemas informáticos que más se utilizan como patrones de referencia al momento de implementar este tipo de gestión en una organización; y que también se han utilizado como base para el diseño de normas locales en materia de ciberseguridad. Por tal motivo, se ha seleccionado la norma ISO/IEC 27000 como una base general en cuanto a las medidas de seguridad informática y evaluación y control de riesgos, así como también se han seleccionado los marcos de trabajo COBIT e ITIL, como guías para establecer diseños y procedimientos que permitan implementar disposiciones apropiadas para mejorar la gestión de sistemas tecnológicos y comunicacionales en las organizaciones.

4.2.1 Serie ISO/IEC 27000

Son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO, por sus siglas en inglés) y la Comisión Electrotécnica Internacional (IEC, por sus siglas en inglés). La serie contiene prácticas recomendadas en seguridad de la información para desarrollar, implementar y mantener especificaciones para los SGSI. Principalmente incluye la norma ISO/IEC 27001, la cual establece el marco de trabajo para definir un SGSI, centrándose en la visión de la gestión de la seguridad como un proceso continuo en el tiempo; y la norma 27002 relacionada con las buenas prácticas para gestión de la seguridad de la información.

La norma ISO/IEC 27001 protege la confidencialidad, disponibilidad e integridad de los datos de una empresa, mediante un sistema de análisis de los principales riesgos y amenazas que podrían afectar a la información; además, esta norma proporciona un modelo para la creación, documentación e implantación de un SGSI, y se integra perfectamente con otros sistemas de gestión como son los sistemas de gestión de la calidad, bajo la norma ISO 9001 y los sistemas de gestión ambiental bajo la norma ISO 14001. La norma ISO/IEC 27001 es la única norma certificable de las que se incluyen en la familia ISO/IEC 27000, y se estructura de la siguiente manera:

1. Introducción.
2. Generalidades.
3. Norma para consulta.
4. Términos y definiciones.
5. Contexto de la organización.
6. Liderazgo.

7. Planificación.
8. Soporte.
9. Operación.
10. Evaluación del desempeño.
11. Mejora.

Con respecto a la norma ISO/IEC 27002, Ostec (2005) la considera como una guía completa de implementación de un SGSI, la cual establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización, lo cual incluye la selección, implementación y administración de controles, teniendo en cuenta los entornos de riesgo encontrados en la empresa. Esta norma contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios principales de control.

Benjumea, O. (2005) señala los siguientes dominios de la norma ISO 27002: la política de seguridad, los aspectos organizativos de la seguridad de la información, la gestión de activos, la seguridad ligada a los recursos humanos, la seguridad física y ambiental, la gestión de las comunicaciones y de las operaciones, los controles de acceso a la información, la adquisición, desarrollo y mantenimiento de los sistemas de información, la gestión de incidentes en la seguridad de la información, la gestión de la continuidad del negocio y los aspectos de cumplimiento legal y normativo.

Entonces, la norma ISO 27001 define cómo gestionar el SGSI, y cuáles son las responsabilidades de los participantes; además, sigue un modelo de planeación y acción continua, siendo sus puntos clave la gestión de riesgos y la mejora continua. Por otro lado, la norma ISO/IEC 27002 ofrece recomendaciones sobre qué medidas tomar para asegurar los sistemas de información de una organización, además de describir los objetivos de control (aspectos a analizar para garantizar la seguridad de la información) y especificar los controles recomendados a implementar.

4.2.2 COBIT

COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas, según siglas en inglés) es una serie de recursos que se utilizan de referencia para la gestión de tecnologías de la información (TI), y está basado en la filosofía de que los recursos TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para

proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos. Fue publicada por primera vez en 1996 por la Asociación de Auditoría y Control de Sistemas de Información (ISACA, según siglas en inglés), con el objetivo de unificar y brindar buenas prácticas a través de un marco de trabajo de dominios y procesos, y presentar las actividades de una manera manejable y lógica.

Dentro de la familia de documentos de COBIT, existe uno completamente enfocado en la seguridad de la información, el COBIT 5, publicado en 2012, donde se consolidan e integran los marcos de referencia de COBIT 4.1, constituido principalmente por el Modelo de Negocios para la Seguridad de la Información (BMIS, según siglas en inglés) y el Marco de Referencia para el Aseguramiento de la Tecnología de la Información (ITAF, según siglas en inglés). COBIT 4.1, está conformado por 34 Objetivos de Control de alto nivel, todos diseñados para cada uno de los procesos de TI, los cuales están agrupados en cuatro dominios, los cuales se equiparán a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear. Los cuatro dominios se muestran a continuación de forma más detallada:

1. Planificación y organización: cubre la estrategia que se empleará para que la TI pueda contribuir de la mejor manera al logro de los objetivos del negocio. Además, el proceso de aplicación de la visión estratégica necesita ser planificada, comunicada y administrada desde diferentes perspectivas, buscando establecer una organización y una infraestructura tecnológica apropiadas. Así, este dominio lo conforman 11 procesos: definición de un plan estratégico de TI, definición de la arquitectura de información, determinación de la dirección tecnológica, definición de la organización y relaciones de TI, administración de las inversiones en TI, comunicación de los objetivos y expectativas de la gerencia, administración de los recursos humanos, búsqueda del cumplimiento de requisitos externos, evaluación de riesgos, administración de proyectos y administración de la calidad.
2. Adquisición e implementación: este dominio cubre los cambios y el mantenimiento realizado a sistemas existentes. Consta de 6 procesos: identificación de soluciones, adquisición y mantenimiento de software de aplicación, adquisición y mantenimiento de la arquitectura tecnológica, desarrollo y mantenimiento de TI, instalación y acreditación de sistemas, y administración de cambios.

3. Soporte y servicios: hace referencia a la entrega de los servicios requeridos, que abarca las operaciones tradicionales, el entrenamiento del personal y usuarios, las normas de seguridad requeridas y otros aspectos relacionados a la continuidad. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación, y consta de 13 procesos: definición de niveles de servicio, administración de servicios prestados por terceros, administración de capacidad y desempeño, garantía de servicio continuo, garantía de seguridad de los sistemas, identificación y asignación de costos, educación y entrenamiento de usuarios, apoyo y asistencia a los clientes de TI, administración de la configuración, administración de problemas e incidentes, administración de datos, administración de las instalaciones y administración de las operaciones.
4. Monitoreo: consiste en la supervisión de los procesos a través del tiempo para medir el rendimiento y evaluar su calidad y eficiencia en cuanto a los requerimientos de control. Consta de 4 procesos: monitoreo de procesos, evaluación del control interno, obtención de certificación independiente y provisión de auditoría independiente.

4.2.3 ITIL

ITIL es el acrónimo para Biblioteca de Infraestructura de Tecnologías de la Información, según sus siglas en inglés; es un marco de trabajo que fue desarrollado a finales de 1980 por la Agencia Central de Informática y Telecomunicaciones (CCTA, según siglas en inglés) como una guía para el gobierno del Reino Unido, debido al creciente uso y dependencia de la tecnología en las organizaciones, convirtiéndose actualmente en un estándar a nivel mundial en la Gestión de Servicios de TI. Su objetivo principal es buscar la calidad en todos los procesos tecnológicos, la cual debe centrarse en que los servicios de TI se correspondan y se alineen con los objetivos del negocio, satisfaciendo de esta manera los requisitos y las expectativas del cliente. Así mismo, contiene una amplia y públicamente disponible documentación profesional sobre cómo planificar, entregar y dar soporte a las características de los servicios de TI.

De esta manera, ITIL busca dar valor a las organizaciones que lo implementan, permitiéndoles adaptarse y generar los más convenientes resultados y salidas de sus

procesos, permitiendo una adecuación en cuanto a la gestión para la entrega y operación de productos y servicios habilitados por TI. La última actualización se realizó en el 2019, con ITIL 4, donde se definió el Sistema de Valor del Servicio (SVS), el cual describe recomendaciones que pueden guiar a una organización en todas las circunstancias, independientemente de sus objetivos, estrategias, tipo de trabajo o estructura de gestión, y que abarca desde la forma y funcionalidad de la alta gerencia hasta los procesos productivos más pequeños, buscando la mejora continua.

El concepto de ITIL 4 describe cómo todos los componentes y actividades de la organización trabajan juntos como un sistema para habilitar la creación de valor; es decir, pretende mostrar cómo la mezcla de distintos componentes permite la asistencia en la conversión de demanda y oportunidades en valor, consumible por determinada organización. De esta forma, el núcleo del SVS está compuesto por la cadena de valor del servicio, 34 Prácticas, 7 principios guía, gobierno, y mejora continua.

La cadena de valor del servicio corresponde a seis actividades (planificación, involucramiento, diseño y transición, obtención y creación, entrega y soporte y mejora continua) interconectadas que una organización debe realizar para entregar productos y servicios valioso y así dar respuesta a la demanda y a las oportunidades presentadas en el entorno. En cuanto a las prácticas, son metodologías o aproximaciones para realizar una tarea o lograr un resultado que han sido comprobados como efectivos, ofreciendo la flexibilidad necesaria para adaptarse en el contexto donde se empleen, ya que indistintamente del tamaño y los recursos de la organización donde se aplique, pueden producir resultados positivos.

Adicionalmente, ITIL 4 utiliza el modelo de las 4 dimensiones de gestión de servicios de TI, permitiéndole mostrar las perspectivas que son relevantes para los componentes del SVS. Estas dimensiones abarcan a las organizaciones y personas, información y tecnología, socios y proveedores, y procesos y flujos de valor, reuniendo de esta manera todos los recursos con los que cuenta una organización, y que deben estar alineados para cumplir sus objetivos de una forma óptima.

Posterior a la descripción de la visión general de las principales normativas internacionales en materia de la seguridad de la información, se puede observar en el **cuadro 3** un contraste entre cada una de ellas.

	ISO/IEC 27001	COBIT	ITIL
DEFINICIÓN	Conjunto de normas que definen los estándares de seguridad para implantar un SGSI en una empresa.	Marco de trabajo que permite comprender el gobierno y la gestión de la TI de una empresa.	Conjunto de libros donde se encuentran documentadas las buenas prácticas para la gestión de TI.
ETAPAS DE CONSTITUCIÓN	<ol style="list-style-type: none"> 1. Planificación. 2. Implementación del SGSI. 3. Fase de control o verificación. 4. Actuación, mantenimiento y mejora. 	<ol style="list-style-type: none"> 1. Planificación y Organización. 2. Adquisición e implementación. 3. Soportes y servicios. 4. Monitoreo. 	<ol style="list-style-type: none"> 1. Estrategia del servicio. 2. Diseño del servicio. 3. Transición de servicios. 4. Operación del servicio. 5. Mejora continua del servicio.
CARACTERÍSTICAS	<ul style="list-style-type: none"> • Se centra en la gestión de riesgos para luego mitigarlos. • Se basa en la gestión de la calidad PDCA (planificar, hacer, verificar y actuar). • Consta de un sistema metódico y controlado para proporcionar seguridad. • Posee un mayor compromiso de mantenimiento y mejora de la seguridad. • Puede adaptarse a la legislación vigente y complementarse con normas como la ISO 9001 e ISO 14001. 	<ul style="list-style-type: none"> • Está basado en una revisión crítica y analítica de las tareas y actividades en TI. • Usa herramientas de implementación variadas, como guías gerenciales y de auditoría. • Mejora la comunicación y, en consecuencia, la cooperación entre auditores y administradores. • Es flexible y versátil. • Se divide en tres fases: dominio, procesos y actividades. • Está alineado con estándares de control y auditoría, como COSO, IFAC e ISACA. 	<ul style="list-style-type: none"> • Facilita la entrega de servicios TI. • Se estructura en fases, que a su vez reúnen procesos y actividades específicas. • Su enfoque es operacional. • Adapta sus procesos con la intención de encajar en empresas tanto pequeñas como grandes. • Los niveles de servicio se integran para dar transparencias a los procesos.

OBJETIVOS	Definir requisitos para un SGSI, garantizando la selección de controles adecuados para la protección de los datos.	Brindar buenas prácticas a través de un marco de trabajo de dominios y procesos, y presentar las actividades de una manera manejable y lógica.	Proporcionar las herramientas y normas que le permitan mejorar la calidad de sus servicios y procesos a cualquier organización, mejorando asimismo la satisfacción del cliente.
NIVELES DE SEGURIDAD	Abarca todos los niveles de seguridad en cuanto al hardware y software, planificando medidas de control en todas las áreas, con detalle, e integrando al personal para lograr esos objetivos.	Considera el control de accesos a los sistemas de información (hardware y software).	Incluye medidas en todos los niveles de seguridad.
SERVIDORES	Menciona acciones de control y supervisión para todos los dispositivos, incluidos servidores.	No establece particularmente seguridad para servidores.	Algunos libros de ITIL detallan medidas de seguridad para servidores.
REDES	Establece medidas de seguridad para las redes.	Establece medidas de seguridad para las redes.	Establece medidas de seguridad para las redes.

Cuadro 3. Cuadro comparativo de las normas ISO/IEC 27001, COBIT e ITIL.

Fuente: Elaboración propia.

La norma ISO/IEC 27001 es mucho más específica en materia de seguridad informática, donde se establecen políticas de seguridad y medidas de control que abarcan de forma puntual todos los niveles de seguridad de una organización, mientras que ITIL y COBIT son más generales, y se enfocan en la gestión de TI, buscando optimizar los procesos de negocio; sin embargo, nunca podría implementarse la norma

ISO/IEC 27000 sin tener una infraestructura tecnológica apropiada, la cual puede ser ajustada mediante lineamientos y estrategias de ITIL y COBIT. En cuanto a las dos últimas, ITIL se basa en orientaciones para las buenas prácticas de la gestión de servicios, mientras que COBIT se basa en los principios para monitorear y evaluar el control de la seguridad TI y de los negocios.

Con respecto a sus etapas de constitución, las normas planteadas manejan, en líneas generales, un procedimiento similar, donde inicialmente se evalúa la planificación a emplear para las acciones futuras, donde se delimitarán los activos y recursos que posee una organización para definir el diseño o pautas a implementar para optimizar su funcionamiento y resguardarlos de las amenazas internas y externas, lo cual incluye la anexión de los nuevos elementos que se hayan adquirido. Posteriormente se observa el funcionamiento de los procesos y sistemas implementados para compararlo con los objetivos iniciales planteados en la fase de planificación y diseño, y determinar si han sido cumplidos o si requieren alguna modificación. La supervisión se extenderá en el tiempo y los procesos estarán sujetos a mantenimiento.

4.3 Establecimiento de las políticas adecuadas para los servidores locales y las redes alámbricas e inalámbricas de una pyme.

Las políticas de seguridad consisten en un documento que describe las pautas y normas que deben cumplir los miembros de una organización para mantener los mínimos estándares de seguridad de los sistemas informáticos y de los sistemas de comunicación. De forma general, aplicando los criterios de inclusión de las pymes descritos previamente, se procedió a describir una serie de normas y restricciones para las personas o usuarios con acceso a los equipos y dispositivos electrónicos en la pyme respectiva, iniciando con el objetivo que se busca alcanzar y la descripción de las políticas a seguir. Además, las políticas de seguridad deben seguir unos procesos de actualización periódica sujeto a cambios organizacionales relevantes, como el aumento de personal, cambios en la infraestructura computacional, desarrollo de nuevos servicios, cambio o diversificación del área de negocios, entre otros.

La política de seguridad o SGSI aplicará a cualquier información de la pyme que esté sobre las redes de comunicaciones, así como de los sistemas de información que apoyan los servicios a clientes, proveedores y contratistas, y que se encuentre almacenada o en

tránsito. De acuerdo a la norma ISO 27001 (2013), se debe especificar el alcance que las políticas de seguridad tendrán con respecto a determinada pyme para comprender todo lo que abarcarán, recomendando la inclusión de todos los activos tecnológicos. En cuanto a los parámetros del presente estudio, se requiere incluir el número de servidores locales y de los dispositivos que permiten la transmisión de datos a través de redes alámbricas e inalámbricas.

Estas políticas van dirigidas hacia los empleados y cualquiera que tenga acceso al sistema, especialmente en cuanto al manejo de computadores con acceso a la red interna, con el objetivo de evitar errores de usuario que pongan en riesgo la seguridad del sistema y que les permita trabajar de forma integral para evitar el espionaje o ingreso malintencionado; controlando las posibles eventualidades en el funcionamiento de los programas y de la red. En base a ello, se plantean acciones y limitaciones, desplegadas a través de las siguientes políticas de seguridad:

Política 1: Sobre el SGSI

El SGSI debe ser mantenido y actualizado de manera periódica o cuando ocurran grandes cambios estructurales u organizativos que puedan dejar vacíos de planificación en las políticas vigentes. Igualmente, se deben cumplir los requisitos de funcionalidad del negocio, obligaciones con los socios y los aspectos legales. Se describen las siguientes pautas:

- Se debe establecer una metodología donde se evalúen, califiquen y traten periódicamente los riesgos. Para esto es recomendable contar con un equipo especializado en el área informática y de seguridad de las redes y los sistemas de información. La evaluación de los riesgos contempla los siguientes aspectos descritos por la norma ISO 27.001 (2013): identificar los activos de información, identificar las vulnerabilidades de los activos, determinar las amenazas que pueden generar un incidente, calcular el nivel de riesgo y realizar una estimación de los diferentes niveles de riesgo y determinar si los riesgos son aceptables y si requieren una acción siguiendo criterios de aceptabilidad previamente definidos.
- Revisar cada cierto tiempo las políticas establecidas para evaluar posibles mejoras.

- Establecer un programa de capacitación y sensibilización para los empleados, jefes y personal de seguridad, el cual debe contemplar todos los riesgos asociados a las acciones perjudiciales contra el sistema informático. En este sentido, Martínez, J. (2012), considera que es importante que los empleados conozcan los incidentes más comunes, que establezcan el uso de *password* seguros, que regulen la utilización de internet en el trabajo y que conozcan la normatividad legal del entorno, para que puedan manejar la información en el ambiente laboral de forma más segura y efectiva.

Política 2: Control de Accesos

Todos los computadores y todos los empleados con acceso a los sistemas de información deben tener privilegios específicos y un acceso mediante credenciales, que deben mantenerse en secreto. Además, de tratarse de una pyme más compleja, que se encuentre dividida por departamentos y que posea dispositivos de vigilancia, se podrán aplicar las siguientes normas:

- El área de recursos humanos, en conjunto con el de sistemas, deben trabajar coordinadamente para establecer la autorización justa y necesaria de acceso a sistema de cada empleado, así como tener la capacidad para revocar privilegios, lo cual incluirá al personal de seguridad que tenga acceso a las cámaras de seguridad (de haberlas) o a cualquier computador.
- Se deben guardar registros de seguimiento en los sistemas de información y comunicaciones.
- Se debe establecer una configuración segura, mediante VPN, para el acceso remoto al sistema.
- Mantener seguras y bien resguardadas las contraseñas y sistemas de autenticación, así como cambiar las claves periódicamente.
- Todos los usuarios deben tener credenciales únicas, y se prohíbe su divulgación a cualquier persona.

Así mismo, Martínez, J. (2005) recomienda “implementar seguridad perimetral, preferiblemente basado en hardware, ya que integran todo dentro de una misma caja: filtrado de contenido, *firewall*, antivirus, detector de intrusos, antispam, VPN, entre otras

funcionalidades”. Evidentemente todo dependerá de los recursos del que disponga y esté dispuesto a utilizar cada pyme en particular.

Política 3: Gestión de los activos

Deben ser contabilizados e inventariados todos los dispositivos, computadores, software, recursos humanos, infraestructura y todos los componentes que formen parte del SGSI, con el fin de tener un control más firme. En este sentido, la norma ISO 27.001 (2013) establece que el inventario debe hacerlo el encargado de establecer las políticas de seguridad, visitando todas las áreas de la empresa y hablando con los encargados de la misma en función de los activos previamente descritos. Asimismo, deben ser clasificados de acuerdo a su importancia y por el tipo de activo o información. Cuando el activo se trata de información, se debe dejar constancia de los propietarios o manipuladores de la misma.

Política 4: Seguridad sobre el talento humano

La organización debe tener procedimientos para el reclutamiento, selección y desvinculación del personal, cuando sea lo suficientemente grande, para lo cual:

- Los roles y responsabilidades deben estar definidos, así como las condiciones contractuales y de seguridad, incluyendo los acuerdos de confidencialidad. En este sentido, la propuesta actual impide la conexión de los *smartphones* y otros dispositivos de los empleados a la red inalámbrica de la empresa, así como llevar cualquier dispositivo de transferencia de información.
- Tener una adecuada administración de las credenciales, como se mencionó previamente.

Política 5: Capacitación y entrenamiento

Todos los empleados de la empresa deben asistir a charlas de capacitación cada 6 meses, donde se tratarán temas relacionados con la seguridad de los sistemas informáticos y la importancia de su participación en este proceso, de forma integral, para cuidar los activos de la empresa de la que forman parte. Principalmente se debe crear conciencia del uso descuidado de la web y de las consecuencias que pueden producirse

al acceder a links poco confiables o no emplear credenciales y herramientas seguras para la autenticación.

Política 6: Manejo del riesgo

Los especialistas en el área de sistemas deben implementar una metodología de riesgos, para la identificación, análisis y evaluación, así como los mecanismos de tratamiento, por lo que será necesario formalizar la metodología general de riesgos para sistemas de información y plataformas tecnológicas, definiendo los niveles aceptables de los riesgos por parte de la alta dirección, así como los roles y responsabilidades frente a los mismos.

Política 7: Seguridad física y ambiental

Son aspectos relacionados a la seguridad ocupacional, por lo que se deben tener elementos de protección física que resguarden los centros de datos y las redes en general:

- Debe existir una escalera y salida de emergencias, un extintor en cada oficina, chequeos periódicos de las tuberías de agua y de las instalaciones eléctricas.
- Debe existir poca humedad en el ambiente y temperaturas inferiores a los 15 °C.
- De ser posible implementar video vigilancia.

Política 8: Gestión de las redes y los sistemas informáticos

Todas las redes de computadores, de telecomunicaciones, sistemas informáticos, dispositivos móviles y sistemas de información deben contar con la protección adecuada ante ataques, fuga de información y accesos no autorizados:

- Se debe contar con sistemas antivirus, anti-spam y anti-espías en todos los computadores con acceso a la red local e inalámbricas.
- Todos los servicios y acceso a la red deben estar controlados, para lo cual se debe implementar control de acceso en la red y sistemas de información. Se debe proceder a configurar de forma segura las redes wifi utilizando cifrado fuerte, e implementar una rotación de contraseñas de la red inalámbrica.

Política 9: Sistemas de respaldo y recuperación

Se deben tener sistemas de respaldo y procedimientos de recuperación, protección de medios de almacenamiento y control de acceso hacia las librerías y cintas. Todos los medios removibles o de almacenamiento que no se usen se les debe eliminar su información de modo seguro (sin recuperación). En este sentido, Martínez, J. (2005) señala que “deben respaldarse copias de seguridad de los datos para mantener a salvo la información importante de la empresa, definiendo frecuencia, tipo de copia, tipos de archivos, entre otros, y establecer un procedimiento que indique como realizar la copia de seguridad correspondiente”.

Política 10: Servicio electrónico

Para todos los sistemas de servicio electrónico (servicios, bases de datos y aplicaciones web) se debe proveer mecanismos de autenticación, autorización, identificación y no repudio a través de cifrado (criptografía):

- Se debe implementar y mantener un sistema PKI (infraestructura de clave pública).
- Las firmas digitales y certificados deben estar resguardados de manera óptima, así como las llaves de cifrado.
- Los datos en las bases de datos acorde a su nivel de criticidad deben estar cifrados.
- Se debe configurar los diferentes registros de auditoría y monitoreo de transacciones en línea.

Política 11: Gestión de los incidentes de seguridad

Usualmente se aplica en pymes complejas, donde se debe contar con un proceso para la atención, detección, control, tratamiento y respuesta de incidentes de seguridad:

- Cada incidente debe alimentar las fuentes de los riesgos, con sus respectivos tratamientos.
- Todos los eventos de seguridad deben ser registrados y monitoreados hasta la solución final.
- Se debe contar con un procedimiento para la investigación forense.

Política 12: Planes de recuperación ante desastres

Se debe contar con planes para la recuperación ante desastres documentados, oficializados, divulgados y aprobados, de modo que todo el personal este enterado de las acciones técnicas a realizar en caso de fallo de la red, bases de datos, sistema operativo y aplicaciones en general. Todos los planes de recuperación ante desastres deben tener un análisis de riesgos previo.

Por otro lado, es necesario destacar que las políticas de seguridad surgen de un plan de trabajo donde interactúan los responsables de las diferentes áreas de la empresa, y donde se delimitan los recursos tecnológicos y humanos con los que se cuenta (número de dispositivos de red y equipos computacionales, cantidad de usuarios con sus niveles de acceso) para establecer un monitoreo constante de las medidas de control y políticas de seguridad establecidas. Sin embargo, una empresa que tenga intenciones de implementar un SGSI, incluyendo políticas de seguridad y control, así como medidas para optimizar todos sus sistemas de información y de comunicación, debe cumplir una serie de características básicas en cuanto a su infraestructura tecnológica, especialmente enfocada a las redes y comunicaciones, así como a la seguridad informática de éstos sistemas. Por tanto, se desglosan las siguientes características:

1. Debe poseer un inventario de todos los dispositivos, activos y recursos tecnológicos que forman parte de las redes informáticas.
2. Debe poseer delimitado su plano, topología y tipo de red, incluyendo los protocolos de red: WIFI y Ethernet.
3. Contar con un proveedor de servicios de internet eficiente.
4. Delimitar la disposición de los distintos equipos y dispositivos informáticos, tanto en las unidades de trabajo como en los sistemas de redes.
5. Delimitar los distintos sistemas informáticos que se manejan en la empresa y la forma en la que se encuentran conectados a la red, lo que incluye segmentación de red (cuando sea el caso) y el acceso a la información entre distintos equipos y departamentos.
6. Contar con programas de seguridad como antivirus y firewall.
- 7..Debe poseer procesos de copia de respaldo, así como de recuperación de la información.

Por lo tanto, cuando una empresa posee las características previamente mencionadas, es cuando se puede empezar a organizar planes de mejoras en base a las necesidades y situación en su gestión de TI, la cual se va a determinar mediante evaluaciones pertinentes al tipo y complejidad de la organización en cuestión, pudiendo definirse investigaciones preliminares o auditorías de sistemas internas. De esta manera, para que una pyme pueda establecer políticas efectivas y funcionales, primero debe realizar una adecuación tecnológica apropiada, debiendo cumplir con requerimientos mínimos de seguridad, en cuanto al hardware y software, planteados en el **cuadro 4**.

Elemento de la Red	Requisitos de Hardware	Requisitos de Software
Servidor	Debe ubicarse en un lugar cerrado y en el sitio más resguardado de la empresa; organizarlo en un rack o en un gabinete sólido.	Antivirus, firewall y sistema operativo.
Servidor, switch, router y otros dispositivos de red	Mantener a temperaturas inferiores a 25°C, usando acondicionadores de aire, a los cuales se les debe realizar un mantenimiento regular.	
	Instalar un sistema UPS para proteger y proporcionar tiempo de respaldo a los equipos TI, durante las fallas de la energía eléctrica.	
	Deben ubicarse cuidadosamente, previniendo que sufran alguna caída, golpes o corrosión.	
	Se deben ubicar en áreas lo más seguras posibles, previniendo robo, sabotaje y daños ambientales.	
Switch y Router	El cableado debe estar etiquetado y distribuido en sistemas de canaletas adheridos a la pared o al techo, o en armarios de cableado. Las conexiones deben realizarse usando conectores y <i>patch-panels</i> .	Firewall
	Poseer suficientes tomas de corriente y una infraestructura del sistema eléctrico estable.	
	Deben usarse oportunamente cables de interior y exterior para cada situación específica.	
	Poseer un proveedor de servicios de internet, con conexión estable y capacidad satisfactoria.	

Cuadro 4. Requisitos mínimos en TI que debe cumplir una pyme.
Fuente: Elaboración propia.

Posterior a la evaluación oportuna de todos los aspectos de seguridad considerados para el establecimiento de las políticas de seguridad en las pymes, descritos previamente, se procedió a puntualizar los procesos y medidas de control que deben ejercer las mismas, en todos sus niveles de seguridad, buscando la protección y resguardo de los sistemas de información, especialmente en cuanto a los servidores locales y redes alámbricas e inalámbricas. Esta información se encuentra plasmada en el **cuadro 5**, donde se expresan acciones generales para todas las pymes, especialmente enfocadas en los distintos niveles de seguridad, así como en los servidores locales y las redes alámbricas e inalámbricas, y que son controles y políticas mínimas de acción general que están sujetas a ser adaptadas para situaciones o empresas particulares, sirviendo como una guía orientativa para mejorar u optimizar la seguridad de cualquier sistema informático o comunicacional en todos sus niveles.

De esta manera puede observarse que las políticas deben ser complementadas con controles de seguridad, debido a que el factor humano carece de confianza operativa, y la funcionalidad y optimización de procesos en una pyme no puede estar sujeta al comportamiento subjetivo de los usuarios. Así, por ejemplo, las políticas relacionadas al control de accesos y a la seguridad de las contraseñas se encuentran controladas por asignación de permisos de acceso. La gestión de contraseñas es uno de los aspectos más delicados para asegurar el acceso a los sistemas de información, ocupándose de identificar los distintos equipos, servicios y aplicativos para los que es necesario activar credenciales de acceso; además, define la manera con la que se generarán las claves, su formato (longitud mínima, tipos de caracteres que deben incluir y reglas semánticas), su distribución a los usuarios y el tiempo de validez.

Posterior a haber establecido los tipos de información, los perfiles de usuarios y los grupos existentes, se pueden concretar los tipos de acceso a la información a los que se tendrá derecho, definiendo las acciones que se puedan realizar sobre la información (creación, lectura, borrado, modificación, copia, ejecución, entre otros); por lo general se otorga el mínimo privilegio en el establecimiento de los permisos.

CONTROLES Y POLÍTICAS PARA LOS SERVIDORES LOCALES Y REDES ALÁMBRICAS E INALÁMBRICAS DE UNA PYME		
NIVEL	CONTROLES	POLÍTICAS
HARDWARE	Controles físicos de acceso: puertas, racks o gabinetes con llave.	Poseer todos los recursos tecnológicos en un lugar cerrado, para cuidarlos del hurto o del acceso de personas no autorizadas.
	Definir usuarios y roles y asignar permisos de acceso.	Los dispositivos y equipos solo podrán ser manipulados por personal autorizado.
	Emplear sistemas de vigilancia con al menos 2 cámaras de seguridad, con alarma incluida.	Establecer vigilancia perimetral.
	Evaluar periódicamente el estado del cableado, verificando que esté correctamente identificado y que no presente signos evidentes de deterioro.	Organizar e identificar el cableado de red.
	Establecer procedimientos para copias de seguridad: definir periodicidad, tipo y contenido de la información a resguardar. Recordar salvaguardar al menos una copia fuera de la empresa, bajo llave o cifrada en la nube.	Resguardar periódicamente la información en discos externos o en algún medio virtual.
SOFTWARE	Instalar, configurar y actualizar las herramientas de detección de programas maliciosos.	Emplear <i>antimalwares</i> y antivirus actualizados.
	Verificar periódicamente que el <i>firewall</i> de cada dispositivo se encuentre activo y configurado apropiadamente.	Configurar y activar el <i>firewall</i> en los computadores y <i>routers</i>

	<p>Definir la manera con la que se generarán las claves, así como su formato, tiempo de validez y procedimientos para revocarlas.</p> <p>Distribuir las claves generadas a los usuarios correspondientes, considerando si esta distribución ha de ser cifrada y con qué método; y cómo se activarán las claves.</p> <p>Se pueden emplear aplicaciones de gestión de contraseñas (*).</p>	Utilizar contraseñas sólidas para iniciar actividad en cada computador y servicio web.
		No utilizar contraseñas por defecto.
		Exigir el uso de contraseñas seguras, que deben cambiarse periódicamente (cada mes), y prohibir su divulgación.
		No utilizar la misma contraseña para servicios diferentes.
		No hacer uso del recordatorio de contraseñas.
	<p>Utilizar un servidor proxy para limitar la navegación en páginas web sin certificados de seguridad, o páginas específicas.</p>	Capacitar al personal respecto a la importancia de la seguridad en el acceso a los sistemas.
		No abrir links inseguros y de baja confianza.
		No realizar descargas poco fiables e innecesarias.
		No abrir correos electrónicos de dudosa procedencia.
		No realizar descargas poco fiables e innecesarias.
	Generar correos institucionales de uso exclusivo en la pyme, para cada usuario.	No utilizar el correo personal.
	<p>Establecer rutas aisladas de conexión a la red, con un <i>firewall</i> independiente para evitar las fugas de datos o entradas difícilmente perceptibles.</p>	Proteger el acceso a las redes inalámbricas.

	En caso de aplicar teletrabajo, utilizar VPN para conexiones entrantes a la red (*).	
	Bloquear los puertos USB a través de los controladores del sistema, y gestionar un medio para solicitar permisos de acceso por parte de los usuarios.	Proteger el acceso de información a través de dispositivos extraíbles.

Cuadro 5. *Controles y políticas de seguridad generales establecidas para las pymes.*
Fuente: *Elaboración propia.*

De acuerdo a esto, se evidencia que las políticas de seguridad establecidas buscan principalmente bloquear el acceso de agentes externos hacia los sistemas físicos y virtuales, y enfoca a los servidores locales y a las redes alámbricas e inalámbricas como los elementos más importantes y de mayor valor en la organización. Así mismo, se señalaron algunas de las políticas como opcionales, debido a la necesidad de invertir gran cantidad de recursos; las mismas fueron identificadas con asterisco (*). De esta forma, se ha realizado una evaluación de los niveles de seguridad y control que debe poseer una pyme, especialmente en sus servidores locales y redes alámbricas e inalámbricas, para aumentar la protección de sus datos frente a las amenazas continuas y crecientes en este campo de la tecnología y organizacional.

CONCLUSIONES

Luego de plasmar los respectivos análisis críticos realizados en la presente investigación documental, relacionados a los sistemas de gestión de la seguridad de la información, se considera que pudieron cumplirse los objetivos planteados a cabalidad, pudiendo evaluarse los controles que debe poseer una pyme en todos sus niveles de seguridad, para poder garantizar la estabilidad de sus servidores locales y redes alámbricas e inalámbricas.

En primer lugar, se identificaron los aspectos que deben ser considerados al establecer la seguridad de los servidores locales y de las redes alámbricas e inalámbricas en una pyme, los cuales involucran a los elementos principales en la arquitectura de seguridad de los datos, es decir, su confidencialidad, integridad y disponibilidad. Además, se revisaron los niveles de seguridad correspondientes a la infraestructura, el software y el hardware, y conocimientos relacionados a las amenazas y la forma en que podrían afectar el correcto funcionamiento de los datos.

Seguidamente, se especificaron las principales normas internacionales que promueven y estandarizan procedimientos y medidas de control para la gestión de la seguridad en el sector tecnológico. Específicamente, se trabajó en base a ISO/IEC 27000, COBIT e ITIL, las cuales pueden usarse de forma complementaria y adaptativa al momento de diseñar planes de gestión de seguridad de los datos informáticos en una pyme.

Por último, se establecieron los controles y políticas de seguridad de la información recomendadas para una pyme, las cuales abarcan una serie de acciones destinadas a la protección del acceso de los diferentes niveles de seguridad contra las posibles amenazas. De esta manera, las políticas planteadas se dividieron en software y hardware, donde se establecieron acciones enfocadas al control de accesos físicos y virtuales a las redes, a la gestión de contraseñas, a la organización del cableado de red y al uso de programas de seguridad. Por lo tanto, se plantearon medidas de control, en los diferentes niveles de seguridad de una pyme, para resguardar la integridad y funcionamiento de los servidores locales y redes alámbricas e inalámbricas.

RECOMENDACIONES

Los datos y la información son activos muy importantes de cualquier organización, incluidas las pymes, por lo que nunca se debe subestimar su valor. Por esta razón, se recomienda realizar una gestión de seguridad de los sistemas de información y comunicación, estableciendo un alcance en consonancia con todos los activos de la organización, involucrando a todo el personal con acceso a los dispositivos electrónicos conectados a las redes alámbricas e inalámbricas y haciendo especial énfasis en el cuidado de los servidores locales. Además, se recomienda consultar y aplicar normas y marcos de trabajo en relación a este tema para obtener mejores resultados con la mayor efectividad posible.

Además, es necesario mencionar que las políticas de seguridad de la información en una pyme siempre deberán establecerse en concordancia con el nivel de complejidad y tipo de organización en la que se constituye, considerando los recursos disponibles y dispuestos a ser destinados en este tipo de proyectos. Por último y estrechamente relacionado con lo anterior, se recomienda adaptar diferentes estrategias, que puedan integrarse de forma eficiente, para garantizar controles mínimos en los distintos niveles de seguridad de la pyme.

REFERENCIAS BIBLIOGRÁFICAS

- Arias, F. (2012). *El proyecto de investigación. Introducción a la metodología científica*. (6ta ed.). Caracas – Venezuela: Edit. Episteme.
- Avenía, C. (2017). *Fundamentos de seguridad informática*. (1era ed.). Bogotá – Colombia: Edit. Fondo editorial Areandino.
- Araujo, M. (2012). *Fundamentos del análisis crítico: concepto de validez y condiciones básicas para el análisis*. Recuperado el 12 de julio de 2021, de <https://www.medwave.cl/link.cgi/Medwave/Series/MBE03/5293>.
- Balestrini, M. (2006). *Como se elabora el proyecto de investigación*. (7ma. ed.). Caracas - Venezuela: Edit. BL Consultores Asociados Servicios Editoriales.
- Barceló, J.; Íñigo, J.; Martí, R. y Perramon, X. (2004). *Redes de computadores*. Recuperado el 15 de junio de 2021, de https://www.andaluciaesdigital.es/c/document_library/get_file?uuid=99db7a0d-06fc-4228-9a10-668ce46ce170&groupId=20195.
- Borghello, C. (2001). *Seguridad informática: sus implicancias e implementación*. Tesis Licenciatura en sistemas. Universidad Tecnológica Nacional.
- Borges, S. (2020). *Servidor local, ¿qué es y cómo puedo instalar uno?*. Recuperado el 15 de junio de 2021, de <https://blog.infranetworking.com/servidor-local/>.
- Caicedo, J. y Rojas, J. (2017). *Diseño de un sistema de gestión de seguridad de la información para el área de infraestructura tecnológica*, de ALFAGRES, S.A. basado en la norma ISO/IEC 27001:2013. Recuperado el 08 de octubre de 2021, de <http://polux.unipiloto.edu.co:8080/00004318.pdf>.
- Carisio, E. (2019). *Políticas de seguridad informática y su aplicación en la empresa*. Recuperado el 28 de junio de 2021, de <https://blog.mdcloud.es/politicas-de-seguridad-informatica-y-su-aplicacion-en-la-empresa/>.
- Cázarez, L.; Christen, M.; Jaramillo E.; Villaseñor L. y Zamudio, L. (1999). *Técnicas actuales de investigación documental*. (3era ed.). México D.F. – México: Edit. Trillas, S.A.
- Constitución de la República Bolivariana de Venezuela*. Gaceta Oficial Extraordinaria N° 36.860 de fecha 30 de diciembre de 1.999.

- Cortes, J. (2016). *Auditoría a la seguridad de la red de datos de la empresa PANAVIAS, S.A.* Recuperado el 15 de junio de 2021, de <https://repository.unad.edu.co/bitstream/handle/10596/12014/1085267906.pdf>.
- Costas, J. (2014). *Seguridad Informática*. Recuperado el 15 de febrero de 2021, de <https://es.calameo.com/read/005748053676d1b8cf6d9>.
- Culshaw, F. (2012). Pymes venezolanas con potencial de punta de lanza. *Revista Debates IESA*. Vol. 17, N° 4. Octubre-Diciembre 2012.
- García, J. (2013). *El marco teórico*. Recuperado el 15 de junio de 2021, de <https://www.uaeh.edu.mx/scige/boletin/prepa4/n2/m4.html>.
- Ghirardi, E. (2018). *Ciberataques*. Recuperado el 24 de febrero de 2021, de <https://borealos.com/post/ciberataque-o-ataque-informatico.html>.
- Gómez, A. (2019). *Tipos de ataques e intrusos en las redes informáticas*. Recuperado el 24 de febrero de 2021, de https://www.edisa.com/wp-content/uploads/2019/08/ponencia_-_tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf.
- González, H. (2019). Informe de Pasantías: *Evaluación mediante auditoría de la seguridad de los sistemas de información en ambiente web y redes, con el fin de detectar riesgos y vulnerabilidades de forma que se puedan aplicar medidas preventivas o correctivas oportunas en la empresa South American Jets, con oficinas en el centro empresarial AB, sector playa el ángel, municipio Maneiro, Estado nueva Esparta*. Universidad de Margarita. El Valle del Espíritu Santo, Venezuela.
- Instituto Nacional de Estadística. (2010). *IV Censo Económico 2007-2008. Primeros resultados*. Recuperado el 18 de mayo de 2021, de <http://www.ucla.edu.ve/DAC/investigacion/gyg/GyG%202014/Abril%202014/2-%20RoxanaMartinezyOtro.pdf>.
- Instituto Nacional de los Seguros Sociales. (2021). *Tipos de empresas*. Recuperado el 18 de junio de 2021, de <http://www.ivss.gov.ve/contenido/Tipos-de-Empresas>.
- Ley especial contra los delitos informáticos*. Asamblea Nacional (2001). Caracas, Venezuela.
- Ley Orgánica de Telecomunicaciones*. Asamblea Nacional (2011). Caracas, Venezuela.

- Ley para la Promoción y Desarrollo de la Pequeña y Mediana Industria.* Asamblea Nacional (2002). Caracas, Venezuela.
- Ley sobre el derecho de autor.* Congreso de la República (1993). Caracas, Venezuela.
- Ley sobre protección a la privacidad de las comunicaciones.* Congreso de la República (1991). Caracas, Venezuela.
- López, J. (2016). *Puertos y protocolos.* Recuperado el 16 de febrero de 2021, de <https://nksistemas.com/curso-de-redes-parte-4-puertos-y-protocolos/>.
- Marchionni, E. (2011). *Administrador de servidores. Manual Users.* (1era ed). Buenos Aires, Argentina.
- Martínez, J. (2015). *Seguridad de la Información en pequeñas y medianas empresas (pymes).* Recuperado el 28 de febrero de 2021, de <http://polux.unipiloto.edu.co:8080/00002332.pdf>.
- Mieres, J. (2009). *Ataques informáticos. Debilidades de seguridad comúnmente explotadas.* Recuperado el 24 de febrero de 2021, de https://www.evilmfingers.com/publications/white_AR/01_Atques_informaticos.pdf.
- Molero, L. (2013). *Redes de datos.* Recuperado el 28 de febrero de 2021, de <https://www.urbe.edu/info-consultas/web-profesor/12697883/archivos/Redes%20de%20Area%20Local%20y%20Metropolitana-cd2/Contenido/RedesdeDatos.pdf>.
- Moras, F. (2003). *El marco jurídico regulatorio de las pequeñas y medianas empresas (pymes) en Venezuela.* Recuperado el 16 de junio de 2021, de <https://biblat.unam.mx/hevila/Visiongerencial/2003/vol1/no1/1.pdf>.
- Proaño, G. (2009). Estudio técnico comparativo de redes LAN alámbricas e inalámbricas. Recuperado el 16 de junio de 2021, de <http://repositorio.puce.edu.ec/bitstream/handle/22000/3756/T-PUCE-3803.pdf>.
- Raffino, M. (2020). *¿Qué son las redes informáticas?* Recuperado el 12 de julio de 2021, de <https://concepto.de/redes-informaticas/>
- Rodríguez, M. (2013). *Redes Informáticas.* Recuperado el 16 de junio de 2021, de <https://es.calameo.com/read/002718716fdc3f40d6979>.
- Romero, M.; Figueroa, G.; Vela, D.; Álava, J.; Parrales, G.; Álava, C.; Murillo, A. y Castillo, M. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.*

- Recuperado el 16 de junio de 2021, de <https://core.ac.uk/download/pdf/326424171.pdf>,
- Tarazona, C. (2007). *Amenazas informáticas y seguridad de la información*. Recuperado el 16 de mayo de 2021, de <https://dialnet.unirioja.es/servlet/articulo?codigo=3311853>.
- Turolde, T. (2015). *Definición de nodo, protocolo, TCP/IP*. Recuperado el 25 de mayo de 2021, de <https://prezi.com/ibzhvl-qmtfe/definicion-de-nodo-protocolo-tcpip/>.
- UNIR (2020). *Claves de las políticas de seguridad informática*. Recuperado el 28 de febrero de 2021, de <https://www.unir.net/ingenieria/revista/politicas-seguridad-informatica>.
- Ostec. (2005). ISO 27002: Buenas prácticas para gestión de la seguridad de la información. Recuperado el 28 de septiembre de 2021 de <https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi/>.
- Pedraz, M. (2003). *Definición del objeto de estudio en las Ciencias de la Actividad Física*. Recuperado el 28 de junio de 2021, de https://ruc.udc.es/dspace/bitstream/handle/2183/9768/CC_40_1_art_5.pdf.
- Zevallos, E. (2003). Micro, pequeñas y medianas empresas en América Latina. Revista CEPAL N° 79. Abril, 2003.