

Maestría en ciberseguridad

Trabajo Fin de Maestría

Guía para implementar buenas prácticas de la ISO 27032 en las pymes de Quito – Ecuador

Autor: Edwin Andres Cifuentes Bolaños

Localidad, ciudad, país

Profesor: Dr. Rodrigo Cadena Martínez

Mes y año

Resumen

En la presente investigación se diseñó una guía para la implementación de las buenas prácticas de la norma ISO 27032 en las pymes de Quito – Ecuador para la generación de mecanismos de alertas ante posibles ataques en el ciberespacio, para ello, se hizo necesario diagnosticar la situación actual de las buenas prácticas de la norma ISO 27032 en estas pymes, buscando antecederse ante posibles ataques en el ciberespacio, posteriormente, se definieron criterios para la evaluación de la implementación de las buenas prácticas de ciberseguridad en la unidad de estudio de acuerdo a la norma, por último, se establecieron los lineamientos para la implementación de los controles y seguimiento a la implementación de las buenas prácticas de ciberseguridad de acuerdo a la norma. El enfoque del presente trabajo tuvo carácter descriptivo con enfoque documental, usando como marco de referencia el COBIT, por tanto, el tipo de investigación fue proyectiva. Para el desarrollo del trabajo investigativo se plantearon cuatro fases, donde se indagó en la página oficial de la ISO cómo se encuentran las empresas pymes en Ecuador y su implementación de buenas prácticas de la norma ISO 27032, se definieron los criterios para las buenas prácticas, se revisaron los numerales de la norma, y, por último, se diseñó la guía indicando los lineamientos a seguir. Se concluye que en Quito – Ecuador son pocas las empresas pymes que aplican esta norma y están certificadas, por lo que se les sugiere tomar esta investigación como referencia para disminuir los ciberataques.

Palabras clave: ciberseguridad, Norma ISO 27032, ciberataques.

Abstract

In the present investigation, a guide was designed for the implementation of good practices of the ISO 27032 standard in SMEs in Quito - Ecuador for the generation of alert mechanisms for possible attacks in cyberspace, for this, it was necessary to diagnose the current situation of good practices of the ISO 27032 standard in these SMEs, seeking to anticipate possible attacks in cyberspace, subsequently, criteria were defined for the evaluation of the implementation of good cybersecurity practices in the study unit according to the standard, finally, guidelines were established for the implementation of controls and monitoring of the implementation of good cybersecurity practices according to the standard. The focus of this work was descriptive with a documentary approach, using COBIT as a reference framework, therefore, the type of research was projective. For the development of the research work, four phases were proposed, where the official ISO website was investigated how SMEs in Ecuador are doing and their implementation of good practices of the ISO 27032 standard, the criteria for good practices were defined, the numerals of the standard were reviewed, and finally, the guide was designed indicating the guidelines to follow. It is concluded that in Quito - Ecuador there are few SME companies that apply this standard and are certified, therefore, it is suggested that they take this research as a reference to reduce cyber attacks.

Keywords: cybersecurity, ISO 27032 Standard, cyberattacks.

Dedicatoria

Me gustaría dedicar esta tesis principalmente a Dios, porque sé que todo este esfuerzo y dedicación es gracias a Él. Para mis padres Alfonso y Edith, por su comprensión y por su ayuda en todo momento y mucho más en los momentos difíciles, a mi Mamita a quien admiro siempre porque me ha enseñado a ser lo que soy a nunca rendirme y en especial a siempre luchar por mis sueños. A mis hermanos Pao y Luis, quienes me han apoyado siempre nunca me han dejado solo y que a pesar de todas las dificultades siempre hemos estado juntos.

Agradecimientos

Al finalizar un trabajo tan arduo y con muchas dificultades, solo me queda agradecer a Dios y a todas las personas que siempre han estado para poder cumplir con este tan anhelado sueño, agradecer a la universidad por abrirme las puertas a esta formación que es online, pero que, si no tienes la dedicación de hacerlo, de estudiar y prepararte no lo haces y eso queda únicamente en la voluntad de cada persona.

Quiero agradecer a mi novia Carito, porque ella ha sido un pilar fundamental en mi vida, quien me ha apoyado en todo momento y sobre todo quien a estado para mí en cada paso de mi vida.

Índice de Contenido

RESUMEN ..... **II**

ABSTRACT ..... **III**

DEDICATORIA ..... **IV**

AGRADECIMIENTOS ..... **V**

ÍNDICE DE CONTENIDO ..... **VI**

ÍNDICE DE TABLAS ..... **VIII**

ÍNDICE DE FIGURAS ..... **IX**

1. MARCO INTRODUCTORIO **1**

1.1. ANTECEDENTES 1

1.2. PROBLEMA DE INVESTIGACIÓN 3

1.3. JUSTIFICACIÓN 5

1.4. ESTABLECIMIENTO DE HIPÓTESIS Y OBJETIVOS 6

2. MARCO TEÓRICO **7**

2.1. ESTADO DEL ARTE 17

2.2. MARCO EMPÍRICO 26

2.2.1. Hipótesis *26*

2.2.2. Objetivos de la investigación *27*

2.2.2.1. Objetivo General 27

2.2.2.2. Objetivos específicos 27

3. METODOLOGÍA **28**

3.1. DISEÑO Y TIPO DE INVESTIGACIÓN 28

3.2. POBLACIÓN Y MUESTRA 28

3.3. VARIABLES Y OPERACIONALIZACIÓN 28

3.3.1. Variable independiente *28*

3.3.2. Variable dependiente *29*

3.4. FASES DE DESARROLLO DEL TRABAJO 29

4. RESULTADOS **31**

4.1. FASE 1. IDENTIFICAR LA ORGANIZACIÓN 31

4.2. FASE 2. DEFINIR CRITERIOS PARA LA IMPLEMENTACIÓN DE LAS BUENAS PRÁCTICAS. 33

4.3. FASE 3. REVISAR LOS NUMERALES DE LA NORMA 37

4.4. FASE 4. DISEÑAR LA GUÍA PARA LA IMPLEMENTACIÓN DE LA NORMA 39

5. CONCLUSIONES 46

6. RECOMENDACIONES 48

7. REFERENCIAS BIBLIOGRÁFICAS 49

Índice de Tablas

Tabla 1. *Comportamiento del sector TIC* 18

Tabla 2. *Información de la empresa* 35

Tabla 3. *Numerales ISO 27032* 38

Tabla 4. *Numeral 7* 39

Tabla 5. *Numeral 8* 40

Tabla 6. *Numeral 9* 40

Tabla 7. *Numeral 10* 42

Tabla 8. *Numeral 11* 42

Tabla 9. *Numeral 12* 43

Tabla 10. *Numeral 13* 43

Índice de figuras

Figura 1. *Elementos del ciberespacio* 8

Figura 2. *Calidad Total según el Modelo Deming, P. (1951)* 14

Figura 3. *Fases del desarrollo del trabajo* 30

Figura 4. *Implementación ISO 27001 a nivel mundial* 32

Figura 5. *Implementación ISO 27001 a nivel de Latinoamérica* 32

Figura 6. *Principios básicos del COBIT* 34

Figura 7. *Estructura de la app Cyber CAT* 37

1. Marco introductorio

1.1. Antecedentes

Las Tecnologías de Información y Comunicación (TIC's) son herramientas inmersas en la cotidianidad de las personas. Así mismo, cualquier empresa, sin importar su fin y/o tamaño, las requieren. Por ello, la implementación de estas son uno de los recursos indispensables en las pymes, para de esta manera tratar de minimizar la brecha digital existente.

Uno de los países que desea invertir en las TIC's es Ecuador, ya que necesita mejorar la productividad a nivel empresarial, siendo la capacitación en esta área primordial. Actualmente, indica Párraga (2017), existe en las pymes un bajo nivel de adopción de nuevas tecnologías, en comparación con otros países latinos, como Costa Rica, Argentina y Chile, lo que limita por supuesto su competitividad. Integrar las TIC's en las operaciones diarias del nivel empresarial permitiría mantenerse al día con las tendencias del mercado, generando mayores rendimientos.

Si bien es cierto, estos tipos de avances traen muchas ventajas a las personas y empresas, no se puede dejar de lado la sensibilidad de la información de posibles ataques, por lo que, resguardar su seguridad requiere ser un objetivo primordial en toda organización, para generar confianza en sus clientes.

Al respecto, Zuñiga et al. (2020) exponen que la ciberseguridad en las pymes es un tópico a tomar en cuenta, estos autores realizaron indagaciones, donde aseveran que son varias las ciudades ecuatorianas, especialmente Guayaquil y Quito, que han adoptado a las TIC's para promoción de sus servicios y productos, usando para ello plataformas digitales, como redes sociales, tiendas en línea y marketing digital.

Adoptar estas estrategias ha generado muchos beneficios al comercio local. Esto queda respaldado, según los autores precitados, en un informe nacional, que indican que estas ciudades (Guayaquil y Quito) albergan el 77% de establecimientos que emplean herramientas digitales en sus operaciones comerciales, mientras que ciudades como Ambato, Portoviejo y Cuenca, representan un foco importante en adopción de esas nuevas tecnologías, pero el resto del país muestra menos penetración.

En este sentido, la organización KPMG, la cual es una de las redes más importantes a nivel global que agrupa diferentes firmas de servicios profesionales en más de 156 países, realizó un estudio sobre ciberseguridad, dentro del cual se plasman actores de amenazas, los cuales son: crimen organizado, *stackeholders* o que tengan información de interés y primordial, Hacktivistas y el Estado.

En el caso del crimen organizado, es uno de los actores que amenaza a cualquier organización de forma externa e internamente. Por ello, concientizar sobre la ciberseguridad a los empleados es una de las actividades fundamentales en las pymes, ya que ayudará a minimizar los ataques perpetrados por personas o empleados que gocen de acceso privilegiado.

En este sentido, los Hacktivistas son uno de los actores que representan una amenaza creciente para las organizaciones a nivel mundial, y lo más peligroso, es que su motivación es ideológica y buscan perpetrar los diferentes sistemas informáticos.

Por ello, para el Estado, representa un verdadero reto, un desafío complejo, sobre todo si no se tiene claridad en las normas regulatorias en el ámbito de ciberseguridad, aunado a falta de controles adecuados, quedando así expuestos cualquier organización de naturaleza privada o pública.

En función de lo anterior, se trató de ubicar qué se estaba haciendo en Ecuador con respecto a los controles de seguridad, en este sentido, un informe emanado por el Banco Mundial, junto con el Ministerio de Telecomunicaciones (2022) de ese país, dejó sentado que, en Ecuador, tanto en el sector público como privado, está adoptando una variedad de medidas de seguridad informática.

Por lo que, los actores involucrados, desde los usuarios finales a grandes instituciones, están implementando controles técnicos como parches de software de seguridad, antivirus y sistemas de gestión de contraseñas. Aunado a esto, las organizaciones están realizando inversiones para fortalecer la seguridad física para sus centros de datos, así como en la realización de copias de seguridad de forma periódica.

Del anterior informe ya mencionado, se desprende también el énfasis que está teniendo Ecuador en implementar estándares internacionales como la ISO 27002 y la EGSI vo2, buscando, de esta forma, mejorar los controles técnicos. Las referidas normas dan directrices y/o mejores prácticas a las organizaciones interesadas para que disminuyan el impacto de los ciberataques.

A pesar de lo anterior, no se tiene una guía que ayude a las pymes en Quito - Ecuador a evitar posibles ataques cibernéticos, de allí la necesidad de una guía que incentive las buenas prácticas promulgadas en la norma en estudio. De esta manera, se lograría generar mecanismos de alertas ante posibles ataques en el ciberespacio y lograr los pasos fundamentales para establecer controles que ayuden a robustecer los niveles de seguridad.

1.2. Problema de investigación

La seguridad de la información, junto con la tecnología, son temas que están evolucionando de manera constante, y es uno de los puntos más críticos y álgidos en las diferentes empresas, sin distinción del tamaño o tipo de negocio. En este sentido, el portal

especializado en ciberseguridad Esginnova Group (2021) hace énfasis en la protección de datos, confidencialidad, integridad y disponibilidad de la información.

Para estos especialistas, la seguridad de la información es un conjunto de prácticas destinadas a proteger los datos de una organización contra cualquier acceso no autorizado. Los datos e información que manejan las empresas, en la mayoría de los casos, son sensibles, representando activos valiosos que sustentan las operaciones diarias de cualquier entidad.

De esta manera, la seguridad de la información necesita garantizar la confidencialidad, integridad y disponibilidad de los datos. Por ello, abocarse a esta área resulta un pilar fundamental en cualquier negocio para el éxito empresarial.

En este sentido, las pymes, como una modalidad de organización empresarial en cualquier país, no escapa de estar a la vanguardia tecnológica y de ser sensible en el tema de ciberseguridad. Al respecto, en el caso que compete al presente trabajo de investigación, las pymes en Ecuador representan una fuente de generación de empleos importantes, las cuales apalancan la economía del país. Hecho validado, según datos de INEC (2020), donde en el país existen cerca de 882.265 empresas (CAF, Banco de Desarrollo de América Latina y el Caribe, 2023, p. 23).

Estas organizaciones, como cualquier otra, no dejan de tener sistemas de información interconectados que ofrecen diferentes servicios a sus clientes. Para ello, se hace necesario acceder a información en diferentes plataformas, en donde diariamente se realizan varias transacciones electrónicas financieras en diferentes canales asociados a entidades de comercio.

De esta manera, gracias a la tecnología y la modernización, la información relevante de las pymes, como de sus clientes, pueden quedar expuestas, por ello Duran (2020) refiere que el auge del comercio electrónico en estos últimos años ha incrementado de manera

exponencial el número de transacciones financieras digitales. Observando con preocupación, que, a pesar de los avances en sistemas de seguridad, la falta de conocimiento de los usuarios sobre la táctica de los ciberdelicuentes, los convierte en blancos fáciles para fraudes electrónicos. Estas estafas, aunque a menudo parecen sencillas, pueden tener graves consecuencias financieras. De allí la relevancia de que los usuarios estén informados sobre las últimas amenazas y como protegerse.

Es así como con el presente proyecto se busca dar un aporte en las pymes de Quito – Ecuador, con el fin de responder o mitigar incidentes informáticos bajo los estándares de la norma ISO 27032, permitiendo responder de manera oportuna ante un posible ciberataque.

1.3. Justificación

Las pymes son una de las organizaciones que a nivel económico tratan de dar un aporte significativo. De esta manera, buscan estar a la vanguardia en el uso de las TIC’s, para así crecer con la fomentación de las innovaciones e incrementar sus ventajas competitivas.

Lo anteriormente descrito, estaría incompleto si a través de las pymes no se buscará garantizar la ciberseguridad, ofreciendo a clientes y usuarios integridad y confiabilidad en un recurso tan sensible como la información. Recurso al cual se accede mediante diferentes medios tecnológicos, que pueden ser objeto de un ciberataque.

De esta manera, con la presente investigación se apoyaría a las pymes en Quito – Ecuador al proveerles de una guía sencilla que ayude a incentivar las buenas prácticas impulsadas en la ISO 27032 en este tipo de organización, así podrían establecer requerimientos necesarios para ser adoptadas, permitiendo generar mecanismos para identificar posibles riesgos de la información en la web, lo que pudiera afectar sus operaciones. Es importante resaltar que se ofrecerán lineamientos basados en esta norma ISO, pero ningún control es 100% efectivo para resguardar la información.

1.4. Establecimiento de hipótesis y objetivos

La hipótesis general de base planteada para la presente investigación es:

"Si se diseña e implementa una guía basada en las buenas prácticas de la norma ISO 27032 en las pymes de Quito, Ecuador, se mejorará significativamente la capacidad de estas empresas para detectar y responder a amenazas cibernéticas, lo que se reflejará en un aumento en la eficacia de sus mecanismos de alerta y en una reducción del riesgo de ataques en el ciberespacio".

Dentro de los objetivos de la investigación que abordará el presente proyecto están:

Objetivo general: "diseñar una guía para la implementación de las buenas prácticas de la norma ISO 27032 en las pymes de Quito – Ecuador para la generación de mecanismos de alertas ante posibles ataques en el ciberespacio".

Objetivos específicos:

A) Diagnosticar la situación actual de las buenas prácticas de la norma ISO 27032 en las pymes de Quito – Ecuador para antecederse ante posibles ataques en el ciberespacio.

B) Definir criterios para la evaluación de la implementación de las buenas prácticas de ciberseguridad en las pymes de Quito – Ecuador de acuerdo a la norma ISO 27032.

C) Establecer los lineamientos para la implementación de los controles y seguimiento a la implementación de las buenas prácticas de ciberseguridad de acuerdo a la norma ISO 27032.

2. Marco teórico

La denominada Sociedad Postindustrial necesariamente tiene implícita las TIC’s, las cuales son de uso común en las actividades desarrolladas en el sector empresarial, lo que les ha valido beneficios en pro de mejorar su eficiencia.

Las TIC’s, por tanto, remarcan un nivel de importancia en la vida cotidiana y empresarial indiscutible. Estas son definidas por Rodríguez (2009) como técnicas que ayudan a la comunicación en todos los ámbitos, y afianza Pacheco et al. (2019) que las TIC son una de las estrategias empresariales que impulsan los negocios y afianzan los procesos fundamentales en las organizaciones, sin importar su ámbito.

Las mismas representan herramientas que canalizan la información de diferentes maneras, valiéndose para ello de instrumentos (hardware/ software) que tratan los datos a ser enviados y recibidos de manera eficaz. Es mediante el uso inadecuado de las TIC’s que se puede vulnerar la información, de allí la importancia de la ciberseguridad, la cual puede ser entendida como una disciplina que tiene inmersa políticas, estrategias y procedimientos que buscan implementar medidas de seguridad para prevenir bien sea daños, sustracciones o alteraciones de cualquier recurso informático en una empresa, además, necesariamente requiere garantizar un correcto funcionamiento de esos recursos (Jaramillo, 2015).

Por tanto, proteger los sistemas de información de ataques cibernéticos es en sí la finalidad de la seguridad informática. Para ello, se requiere entender que el activo más importante de cualquier empresa es la información, por ende, demanda estar debidamente protegido. Lo que resulta indispensable en cualquier negocio que use las TIC`s, porque son cada vez mayores las amenazas y vulnerabilidades a las que se está expuesto.

Dichas vulnerabilidades pueden quedar reducidas si se implementan controles adecuados, que es en sí la finalidad de la seguridad de la información. Tal como indica

Rentería (2013), es una disciplina que necesariamente requiere del diseño de normas, procedimientos, técnicas y métodos que hagan a los sistemas de información confiables y seguros. Si bien esto es cierto, en el ciberespacio no se está exento de sufrir vulnerabilidades, por lo que se ameritan tomar las medidas necesarias para evitar los riesgos y amenazas de ciberataques.

En este sentido, Machín y Gazapo (2016) hacen hincapié que el ciberespacio está conformado por cuatro elementos a saber (ver Figura 1): datos, tecnologías de computación, tecnologías de información de análisis y tecnología de información de interacción.

Figura 1.

Elementos del ciberespacio



Fuente: Machín y Gazapo (2016)

Para estos autores, cuando cualquiera de estos cuatro elementos del ciberespacio es vulnerado, se está frente a un ciberataque, siempre y cuando la finalidad sea manipular o tener acceso indebido a la información de un tercero. Dejando plasmado en su estudio, que estos

ataques virtuales están impactando de manera significativa en servicios críticos e infraestructuras pertenecientes a los Estados que conforman la Unión Europea.

Esto ha llevado a que las organizaciones y las unidades encargadas del área de TI amplíen la visión actual en el tema de seguridad, por lo que no basta seguir centrando la atención solo en la infraestructura tecnológica de los datacenters, se necesitan ver elementos adicionales como personas y servicios publicados en la red, los cuales tienen inmersos entornos TIC's, siendo necesario identificar riesgos para implementar controles que permitan la continuación de las operaciones en las organizaciones (Internet Security Auditors, 2018).

Según Machín y Gazapo (2016), existen diversos tipos de ataques, entre los cuales destacan:

A) **Acceso físico**, es cuando el perpetrador tiene acceso a las instalaciones y logra, entre otras cosas, hacer un apagado manual de algún equipo, bien sea de forma remota o presencial; logra interrumpir el suministro eléctrico; hace vandalismo; descubre vulnerabilidades gracias a que logra monitorear la red sin tener autorización; roban discos duros u otros dispositivos de hardware de almacenamiento permanente, entre algunos aspectos.

B) **Interceptación de comunicaciones**, en este aspecto, el perpetrador tiene como objetivo recabar información para acceder de manera indebida, de esta forma penetra en los sistemas, y se da en casos específicos como falsificación de identidad, en este sentido, es muy común usar la técnica de phishing para simular una identidad y acceder a una página o a una app con un usuario existente; es común ver robos de perfiles y secuestro de sesión, imposibilitando al verdadero usuario volver a entrar a sus cuentas; la alteración de mensajes o

redireccionamiento también es una táctica usada por estos malhechores, en este caso hacen uso de virus troyanos o simulan que son correos de confianza.

C) **Denegaciones de servicio**, son ataques que ocurren en cualquier tipo de sistema computarizado, también se puede suscitar en una red, lo que provoca la imposibilidad de acceder a los usuarios reales a la red e interrumpiendo un servicio o un recurso. El objetivo primordial que busca el perpetrador es imposibilitar el buen funcionamiento de los servicios, así aprovecha las debilidades del protocolo TCP/IP e igualmente de las inconsistencias del software ubicado en el servidor.

D) **Intrusiones**, se considera toda actividad que tenga como objetivo interrumpir o hacer un mal uso de los sistemas. Para Carbajal et al. (2006) las intrusiones se pueden dar para mal uso o intrusiones anómalas. Las primeras se basan en ataques cuando se identifican las vulnerabilidades de un sistema, para ello se requiere de auditorías y reportes que arrojen información fiable. Para el segundo caso, se detectan anomalías en el uso del sistema, monitoreando si existen comportamientos inusuales e identificando cualquier actividad sospechosa. Este tipo de ataque busca dar acceso a un personal no autorizado a sistemas informáticos, dando privilegios para obtener información privada. Para ello, se pueden valer de técnicas como análisis de puertos, elevación de privilegios y ataques malintencionados.

Es de hacer notar, que los ataques informáticos son ocasionados por delincuentes que hacen un estudio de su víctima, por ello, se exponen las modalidades de perpetración y vulneración, centrándose en dos grandes aspectos, ingeniería social y skimming.

La ingeniería social es una modalidad que estudia el comportamiento de la posible víctima, para ello se valen de técnicas psicológica que inciten a las personas a ciertos

comportamientos que conlleve a la divulgación de datos privados en línea, como información financiera o datos en línea.

Para el portal especializado de antivirus AVAST (2022), la ingeniería social se puede dar de diferentes formas, siendo alguna de las más comunes el Phishing, Vishing y Smishing. El Phishing, como uno de los más comunes ataques que hacen los perpetradores, es el más usado, y busca ganar la confianza de las posibles víctimas. La mayoría de las veces, se hace uso de medios comunes de comunicación como lo son los correos electrónicos, diseñados de tal manera que obtienen información sensible, como financiera o personal, lo cual los ayuda a penetrar otros sistemas.

En el caso del Vishing, que no es más que el Phishing, pero usando como medio de comunicación la voz, es uno de los más sofisticados, donde el perpetrador trata de ganar la confianza de su posible victima mediante llamadas telefónicas, para esto falsifican los números y hacen que parezcan reales. En este ámbito, es muy común que los agresores se hagan pasar por personal informático de entidades bancarias. De igual forma, hacen uso de cambiadores de voz, así logran ocultar su verdadera identidad.

En otras modalidades de ataques está el Smishing, que también es otro derivado de ataque tipo Phishing, en este sentido se usa un simple SMS o mensaje de texto, solicitando a las posibles víctimas hacer acciones específicas que conlleven a generar vulnerabilidades. A menudo, se mandan enlaces maliciosos donde los usuarios deben pulsar clic o se les indica que requieren llamar a números específicos. En cualquiera de esos casos, se le solicita a la víctima que revele información sensible, casi siempre personal, y la usan para acceder a otro tipo de aplicaciones.

Es de destacar que el Phishing es una de las metodologías más sencillas usadas hoy en día para generar vulnerabilidades en los sistemas. Por ello, el perpetrador busca identificarse

como una persona específica para obtener ciertos datos que permitan el acceso a información privilegiada. De aquí radica la importancia de educar y prevenir a la sociedad en general de los peligros a sufrir vulnerabilidades en internet.

En Ecuador, el Phishing es el principal delito informático, representando, según informe emanado de ESET (2022), como se cita en Primicia (2024), un riesgo para organizaciones y empresas en un 70%. Dicho informe coincide con la alerta arrojada por el Observatorio de Derechos Digitales (S.F.), como se cita en Primicia (2024), sobre "una nueva ola de ataques phishing sin precedentes en el país". Dicha organización indica que los agresores ahora están "recurriendo a técnicas nunca antes vistas para evitar ser detectados, dejando expuesta a una gran cantidad de personas" (Primicia, 2024, párr. 3).

Tanto el Vishing como el Smishing son otras dos modalidades que son de uso frecuente en Ecuador. Para el Vishing, el ciberdelincuente contacta a la víctima vía voz digital, haciéndose pasar por algún especialista o funcionario, quien de manera progresiva sustrae datos financieros y personales sensibles. Es de hacer notar que, para lograr su cometido, el delincuente tiene varios contactos con la víctima, valiéndose del poder de convencimiento. Con el Smishing, sucede que la intervención es mediante mensaje de texto vía celular. Lo que ha de tenerse especial cuidado en que, cualquiera sea la técnica usada, no suministrar datos por ninguna vía, sin antes estar seguros que la procedencia es confiable.

En función de los diversos ataques a que son expuestos tanto personas naturales como jurídicas, surge la necesidad de implementar procedimientos, políticas, recursos humanos y técnicos, siendo esto la base del estándar ISO 27032, formando parte de las normas ISO 27000.

Es de destacar que esta norma no es certificable, a pesar de ello, busca brindar buenas prácticas para mejorar el manejo de la seguridad de la información en las empresas. En este

sentido, la norma toma en cuenta diferentes aspectos a considerar cuando se traslada o publica información sensible, para que las personas involucradas puedan identificar, comprender, determinar las actividades más importantes y/o críticas, y gestionar riesgos. En sí, se requiere identificar los activos, stackeholders y roles usados en el ciberespacio, para establecer controles y/o políticas que brinden una adecuada seguridad a la empresa.

La suscitada norma establece lineamientos a seguir, que no son más que sugerencias o recomendaciones, pautas o instrucciones que proporcionan orientación y dirección en una situación específica a resolver. Dichos lineamientos, en líneas generales, son responsabilidad de ser elaborados por autoridades o expertos en la materia, para eso se valen de las buenas prácticas que en este caso la Norma ISO 27032 esboza.

Los lineamientos resultan entonces una herramienta para dar dirección y orientación a todos los interesados en un área en específico, y de esta manera, puedan ayudar en la calidad y consistencia de las buenas prácticas a emplearse en los procedimientos, para lo cual se seguirá el estándar ISO 27032.

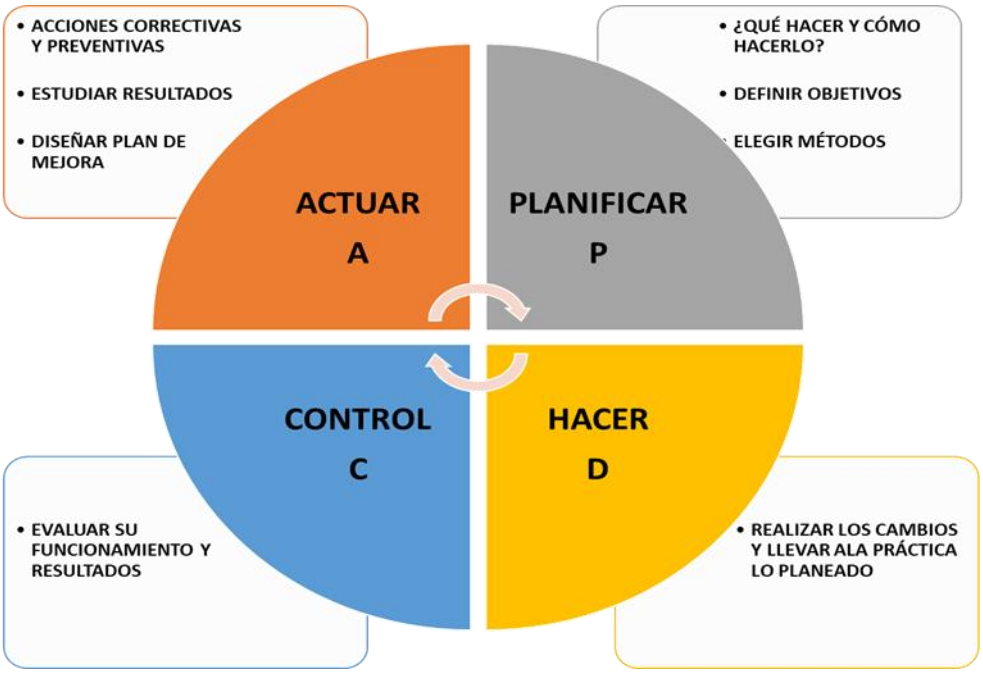
Para poder plantear lineamientos, se hace necesario indicar qué metodología seguir. En el caso de las normas ISO, por excelencia, se maneja bajo la metodología de PDCA o Metodología de Mejora Continua de Proceso. Esta consiste en un método debidamente estructurado y sistematizado que busca, de manera constante, que se identifique y mejore el desarrollo de los procesos dentro de las empresas.

Su fundamento no es más que el ciclo planteado por Deming (ver Figura 2), muy conocido como el ciclo PDCA, que significa: Planificar, Hacer, Verificar y Actuar. El mismo va en pro de la mejora continua de procesos para lograr básicamente eficacia, eficiencia y calidad. Dicha metodología tiene un enfoque cíclico y busca los procesos de las empresas en los que se pueden realizar mejoras, todo parte de identificar problemas y dar solución. Este

ciclo es una metodología conformada por actividades que introducen pequeños cambios, para obtener en los procesos optimizaciones constantes y graduales, siendo su mejora de manera sistemática y centrándose en la calidad (UNIR Revista, 2020).

Figura 2.

Calidad Total según el Modelo Deming, P. (1951)



Fuente: Deming (1951), citado por Limache (2022).

Tal como deja ver la figura 2, esta metodología consta básicamente de cuatro etapas, las cuales se describen a continuación:

PLAN: en esta fase se diagnostica la situación actual de la organización, para ello se requiere identificar los problemas, definir objetivos, ver oportunidades de mejora y dar prioridad a lo que la empresa necesite (Realyvásquez, 2018).

DO: esta fase corresponde a la ejecución tanto de actividades como de planes de acción según los objetivos indicados en la etapa anterior, para ello se hace necesario entender lo establecido, y que los stackeholders o partes interesadas estén preparados para ello.

CHECK: acá se verifican los resultados alcanzados en cada actividad implementada en la etapa anterior, por lo que se hace necesario constatar el antes y después, para así validar si ocurrieron o no mejoras, y si por supuesto los objetivos fueron logrados (Realyvásquez, 2018).

ACT: como última etapa se halla desarrollar propuestas de soluciones para que las mejoras se puedan normar, siempre que los objetivos hayan sido logrados, lo importante es estar alerta por si se detecta alguna anomalía.

En cuanto a la seguridad de la información, se tienen presente aspectos normativos y legales que se abocan a nivel nacional e internacional. Los mismos necesitan ser considerados por las empresas y quienes sean responsables de su seguridad.

Entre los aspectos legales tratados destacan:

- A nivel internacional: el Convenio sobre Ciberdelincuencia, Budapest 2001, el cual establece una política penal común para proteger a los ciudadanos de la cibercriminalidad.
- A nivel nacional: la Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos, 2022, es popularmente conocida como Ley 67. En materia legal, significó un gran avance, ya que se incluyeron varias figuras penales punibles alusivas a los ilícitos informáticos.

Este avance no se dio solamente en Ecuador, ya que países como Venezuela y Colombia también hicieron lo propio y promulgaron como ley especial en materia de delitos informáticos, lo cual se ha hecho necesario por el marco en el cual se desenvuelven las sociedades actuales.

En el caso de Ecuador, no así de los otros países, los delitos tipificados en la Ley 67 se incluyeron en el Código Penal como ilícitos informáticos, los cuales reposan en los artículos

57 al 60, estableciendo penalidades en materia informática en función de los medios usados. Donde los agravantes y atenuantes irán en función de las causales en que haya incurrido el agresor.

Es de resaltar que, el Estado Ecuatoriano para el período 2022 – 2025 aprobó una nueva “Estrategia Nacional de Ciberseguridad”. Allí se plantean 6 pilares fundamentales como objetivos estratégicos, entre los que destacan: estructuración del marco de ciberseguridad nacional, fortalecimiento de la capacidad que se tenga frente a ataques cibernéticos, fortalecimiento del marco legal para la ciberseguridad, protección de la infraestructura nacional de información y formación de profesionales en ciberseguridad (CAF, Banco de Desarrollo de América Latina y el Caribe, 2023).

En el informe presentado por el Banco de Desarrollo de América Latina y el Caribe, en el 2023, destaca que en cuanto al manejo de incidentes cibernéticos el país no posee ni las capacidades ni los recursos para dar una respuesta acorde, esto es a nivel nacional. De igual forma, no existe un registro donde estén asentados los incidentes cibernéticos y sus categorías.

Se hace necesario resaltar que para el 2015, cuando fue promulgada la Ley Orgánica de Telecomunicaciones, se creó ARCOTEL, quien es el órgano encargado de regular todo en esta materia. En este sentido, para la gestión de incidentes y vulnerabilidades informáticos en el ámbito organización se establecieron lineamientos mediante una normativa técnica bajo en Nº 2018 – 0652, donde se incluye un catálogo de incidentes y niveles para priorizarlos.

La normativa se enfoca en el sector financiero, ya que es uno de los más vulnerables a sufrir ataques, por lo que presentan un alto número de incidentes informáticos o digitales. En el caso de este sector, es la Superintendencia de Bancos el ente encargado de obligar a toda entidad bancaria a reportar los incidentes, entre estos los cibernéticos que imposibiliten el

acceso a sus servicios. Pero, salvo el sector financiero, se genera la duda si las otras organizaciones públicas y privadas están obligadas o no a reportar incidentes cibernéticos.

2.1. Estado del arte

Las TIC's han sido una de las herramientas fundamentales para que tanto a nivel personal como organizacional se haya dado la sociedad de la información. Dentro de los aspectos que más destacan, han sido permitir que el mundo empresarial se internacionalizará, lo que facilitó el comercio mediante internet. De esta manera, una de las unidades de negocio más impactadas han sido las pymes a nivel mundial, ya que han tenido incremento en sus transacciones comerciales, lo que las ha obligado a ser más competitivas en todos los sectores económicos.

En este sentido, las pymes a nivel latinoamericano no escapan a la realidad antes planteada, ya que las mismas han sido impactadas por el desarrollo e implementación tecnológico, lo que trae razonablemente diferentes riesgos en uno de sus principales activos, la información.

La importancia de este recurso es reconocida mundialmente, por ello, en el 2005, la Organización de Naciones Unidas (ONU) auspició una Cumbre Mundial que denominó de la Sociedad de la Información (CMSI). Desde ese momento hasta ahora, todos los países suscritos a la misma han tratado de implementar diferentes estrategias para minimizar el impacto de la brecha digital existente.

A pesar de lo anterior, la concepción de este tipo de sociedad es de vieja data, lo que se evidencia con el autor Peter Drucker, que antes de los años 80 ya vislumbraba este tipo de modalidad económica. Al respeto, Drucker planteó la era Post – industrial, donde los principales recursos serían la información y el conocimiento, naciendo de esta manera activos intangibles en el modelo empresarial que son de carácter estratégico (Drucker, 1993).

De allí que enmarcados en una sociedad donde la información y conocimiento son recursos estratégicos que requieren ser gestionados, resulta esta gestión una tarea ardua, por estar frente a activos con características especiales, que crece y se multiplica de forma exponencial, por ello, el papel que ha jugado la tecnología en este ámbito, ha sido crucial.

En este sentido, el Banco Mundial realizó un informe que buscaba medir diferentes aspectos de las TIC's en varios países. El mismo llevo por nombre *The Little Data Book on Information and Communication Technology 2017*, y se plasma en la siguiente tabla, en la cual se puede observar que hasta el 2010 fue que se hizo este tipo de estudio donde se medían mediante indicadores diferentes aspectos como son económicos, sociales, eficiencia, entre otros.

Tabla 1.

Comportamiento del sector TIC

Comportamiento del sector	Mundo		Europa y Asia Central		Latinoamérica y Caribe		Ecuador		
	2006	2010	2006	2011	2006	2010	2006	2010	Media del grupo
ACCESO									
Suscripciones a telefonía fija (por cada 100 habitantes)	194	172	24	251	176	185	125	144	215
Suscripciones a telefonía celular móvil (por cada 100 habitantes)	34	782	616	1,325	431	1,072	465	1,022	843
Suscripciones a banda ancha (por cable) fija (por cada 100 habitantes)	344	775	11	1,042	15	766	2	137	834
Hogares con ordenador (%)	273	362	278	449	164	379	179	27	352
Hogares con acceso a Internet (%)	188	303	199	37	99	303	25	115	251
UTILIZACIÓN									
Tráfico de voz internacional, total (minutos/suscripción/mes)	ns/nc	ns/nc	ns/nc	ns/nc	ns/nc	ns/nc	ns/nc	53	32
Tráfico móvil nacional (minutos/suscripción/mes)	ns/nc	ns/nc	ns/nc	113	43	94	ns/nc	1,344	1,379
Uso de internet por particulares (%)	158	302	129	421	165	392	6	29	341
CALIDAD									
Población con acceso a red celular móvil (%)	67	93	91	ns/nc	90	98	80	93	99
Suscripciones a banda ancha (por cable) fija (% del total de internet)	497	784	15	939	55	853	195	408	69

Comportamiento del sector	Mundo		Europa y Asia Central		Latinoamérica y Caribe		Ecuador		
	2006	2010	2006	2011	2006	2010	2006	2010	Media del grupo
Conexión internacional a Internet con banda ancha (bit/s por usuarios de internet)	4857	29020	1409	35793	1258	20010	2485	8254	9037
ACCESIBILIDAD									
Subcestas de telefonía fija ($ al mes)	ns/nc	113	ns/nc	66	ns/nc	7	ns/nc	141	98
Subcestas de telefonía celular móvil ($ al mes)	ns/nc	144	ns/nc	102	ns/nc	17	ns/nc	138	149
Subcestas de banda ancha fija ($ al mes)	ns/nc	257	ns/nc	128	ns/nc	195	ns/nc	202	176
MERCADO									
Exportaciones de bienes TIC (% sobre el total de la exportación de bienes)	138	111	11	11	96	88	2	1	155
Importaciones de bienes TIC (% sobre el total de la importación de bienes)	14	127	6	51	137	129	111	63	15
Exportaciones de servicios TIC (% sobre el total de exportación de bienes)	7	93	129	201	228	324	ns/nc	ns/nc	58
APLICACIONES									
Índice de medida Web del Egovernment (0-1, 1-mayor presencia)	45	41	47	48	47	46	48	46	46
Servidores seguros de Internet (por millón de habitantes)	647	1,837	55	48	105	361	4	197	201

Fuente: MINTEL – CONSULTRANS (2017)

Del anterior informe se desprende que las TIC's realmente han mejorado el sector empresarial de manera indiscutible, lo que ha impactado desde las multinacionales hasta las pymes. Por lo que, mientras más se use la tecnología en las pymes mayor será el impacto que tendrá en otras esferas.

En función de lo anteriormente expresado, reviste la importancia de implementar estrategias y planes para proteger los datos de las pymes, así como la información sensible a ser vulnerada. En ciertas ocasiones, son varios los factores que inciden en que este tipo de organizaciones no tomen medidas a tiempo frente a vulnerabilidades o amenazas, tal vez por

desconocer cuales son los factores críticos a ser afectados y/o las buenas prácticas que se pueden seguir.

Si bien es cierto, los ciberataques se van adaptando a las nuevas tecnologías, surgiendo otras modalidades de perpetrar a las empresas, también lo es la imperante necesidad de estar en constante alerta. En este sentido, la ISO ha propuesto buenas prácticas mediante la ISO 27032, que tratan de mitigar las vulnerabilidades y riesgos de las empresas.

En esta línea de investigación, Paredes (2022) propone una guía de implementación de políticas de control para mitigar los ciberataques basados en el modelo carding en la COAC "RIOBAMBA LTDA.". El propósito de la investigación fue plantear lineamientos que sirvan de guía ante posibles ataques cibernéticos, para ello, comparó dos metodologías, ENISA y APCERT. Como técnicas de recolección de datos usó la encuesta y la entrevista, esta última aplicada al personal del área de sistemas de la institución.

La autora centró su trabajo en el sector bancario, el cual es uno de los más atacados a nivel mundial, y sobre el que se tratan de aplicar las mejores estrategias para identificar vulnerabilidades y mitigar riesgos, por las consecuencias que trae a las entidades financieras, que no es más que la pérdida de credibilidad.

Dentro de los resultados arrojados, obtuvo en identificación y análisis de los riesgos un 40% y 21% la efectividad de planes de ciberseguridad. En el caso de la comparación realizada entre metodologías, ENISA alcanzó 19 puntos, es decir, 95% de los criterios evaluados, a diferencia de APCERT, que logró 15 puntos, que es un 75%. De esta forma, la investigadora seleccionó la metodología ENISA para evitar ataques basados en el modelo Carding.

En este sentido, ese trabajo investigativo destaca que con la aplicación de su propuesta se ayuda en la ciberseguridad, tratando así de minimizar el impacto de modalidades de

Carding recurrente en las entidades financieras, como fueron el Cash – Out, Skimming, Malware Wootkit y el Phishing. Por ello, sugiere mantener al personal capacitado para proteger así las áreas sensibles en las empresas y evitar los ciberataques.

Así mismo, la seguridad de la información es abordada por Lykhova (2022) en un artículo científico, donde expone la problemática de la ciberseguridad como un tema complejo y la multidisciplinariedad está presente. En la investigación se hicieron uso de métodos propios de las ciencias jurídicas, entre los que destacan el derecho comparado, la estadística y la revisión documental, los cuales fueron indispensables para analizar el marco legal vigente y los estándares nacionales e internacionales establecidos en esa materia.

Los autores destacan la relevancia de la ciberseguridad, la cual visualizan como un fenómeno, que tiene características propias que pueden ir variando en función de la realidad, pero en sí, se percibe su grado de incertidumbre, dinamismo y multidimensionalidad. Todo esto obliga a estar alerta en este tema, ya que para abordarlo lo mejor es mediante un equipo multidisciplinario. De lo anterior se desprende la importancia que han puesto las organizaciones abocadas a normalizar, centrando su atención especialmente en los sistemas de gestión de la seguridad de la información.

Como conclusión destacada se encuentra que la seguridad de la información va más allá de meros aspectos legales o técnicos, su tratamiento es sumamente complejo. Las fronteras en este tema realmente no están delimitadas, y, por tanto, garantizar el resguardo de la información debe ser un objetivo estratégico de toda organización.

La información puede ser vulnerada por agresores valiéndose de diferentes medios, en este sentido, Duran (2020) hizo un estudio interesante enfocado a la modalidad CARDING, esbozando: características, modos de perpetración y vulneración de la ciberseguridad.

Para ello, el autor hizo una recopilación y organización de la información, describiendo de manera detallada los principales elementos de seguridad informática que se ven vulnerados, en este sentido, hizo uso de la investigación documental. Parte de los aspectos resaltantes están las generalidades y características de la conducta asociada al cibercrimen, las cuales realmente se han dado a conocer aún más hoy en día por el incremento del uso de redes sociales.

En esta investigación, el autor se enfoca específicamente en la modalidad del Carding, delito enfocado al fraude que usa como medio del hecho punible las tarjetas de crédito y/o débito, y que afecta directamente a las entidades bancarias. Para ello, el agresor hace uso de la ingeniería social para ganar la confianza de su posible víctima y obtener datos personales y financieros.

En este aspecto, llama la atención que este delito ha venido en ascenso a nivel mundial, por lo que los Estados han tratado de poner especial cuidado al tema. El investigador finaliza su indagación considerando como problemática esta temática, ya que en la actualidad se viene promoviendo el uso del dinero electrónico en el país investigado, Colombia, país que ha experimentado una ola de delito bajo esta modalidad, por lo que en esta investigación se abordan el Carding desde el punto de vista tanto empresarial como personal.

Resaltando en este trabajo, entre otros aspectos, los diferentes métodos existentes para perpetrar los delitos, los cuales pueden ser físicos y digitales, siendo indispensable diferenciar entre ellos. Es por esto, que los ciberdelincuentes deben ser estudiados de manera constante, ya que adquieren cada día más habilidades y destrezas, por lo que las autoridades competentes requieren estar alertas para resguardar la seguridad de la información. Así que, diseñar programas que busquen prevenir a las empresas la mitigación de este tipo de conductas resulta

muy relevante. De igual manera, mantenerse informado sobre las nuevas modalidades de delito que ocurren sobre todo en las entidades bancarias.

Así mismo, se ubicó el trabajo de Limache (2022), investigación realizada en la empresa LISERME S.R.L., Arequipa, Perú. El objetivo primordial fue mejorar la gestión de incidentes de seguridad de la información en la unidad de estudio. Para ello, buscó implementar la Norma Internacional ISO 27035:2016, en el año 2022.

Dentro de la hipótesis planteada se encontró que “la aplicación de esta norma tendrá un impacto positivo significativo en la gestión de incidentes de seguridad de la información” (Limache, 2022, p. 34).

El estudio realizado por el investigador fue de tipo aplicado con diseño preexperimental. En sus hallazgos, hizo evaluación de la norma en estudio usando para ello indicadores de desempeño como tiempo de respuesta, tasa de respuesta, reincidencia y satisfacción del personal.

Entre los resultados arrojados, el investigador destaca que se redujeron los tiempos en la empresa LISERME al aplicar la normativa, dando como resultados 44.25 minutos a 13.91 minutos, quedando demostrado una disminución de 68.56% en el promedio. Además, logró aumentar el nivel de satisfacción del personal del área de TI. De esta forma, sugiere aplicar sistemas de seguimientos para las acciones arrojadas, y así ayudar en la toma de decisiones a nivel gerencial.

En este mismo sentido, Guzman (2019), en su trabajo titulado *Guía para la implementación de la Norma ISO 27032*, diseñó unos lineamientos en forma de guía, estableciendo requerimientos básicos para adoptarlas en las organizaciones. Así, lograrían formar mecanismos que les permitieran a las mismas identificar riesgos con información expuesta en el ciberespacio.

El enfoque de la investigación fue de carácter cuantitativo, usando el marco de referencia COBIT para recabar información, la cual permitió identificar diferentes elementos como requerimientos indicados en la norma en estudio.

La investigadora destaca que, en el país de estudio, Colombia, las pymes hacen uso de manera creciente de las TIC's para efectuar sus operaciones diarias. De igual forma, se han incrementado de manera exponencial los ataques cibernéticos usando como medio la ingeniera social o denegación de servicios. Destacando el hecho que los perpetradores de estos delitos van desde adolescentes hasta profesionales del área.

Estos hechos han colocado en alerta a las empresas, por lo que se han abocado a incrementar sus mecanismos de ciberseguridad. Así mismo, las entidades gubernamentales, como la Policía Nacional de Colombia, han detectado incremento de ciberataques en ciudades como Cali, Medellín y Bogotá.

Dando como conclusión este trabajo que la guía ayudará a las organizaciones a diagnosticar el nivel de ciberseguridad para aplicar controles en puntos claves. Sin embargo, destaca que, en Colombia, no existen formalmente implementados lineamientos que protejan la gran cantidad de información que las empresas tienen expuestas en el ciberespacio, salvo el sector financiero que el marco legal los obliga.

Otro de los trabajos investigados es el expuesto por Gallegos (2023), quien implementó la norma ISO 27032 en la empresa RMO Contratistas Generales SAC, con el fin de mejorar la gestión de ciberseguridad. En este sentido, aplicaron la metodología de investigación orientado en un diseño pre-experimental de tipo pretest y postest, su enfoque fue cuantitativo, tipo de investigación aplicado, con un nivel explicativo. Como instrumentos de recolección de datos se hallaron la encuesta y ficha de observación, aplicados a ocho colaboradores que son la muestra obtenida.

Para la implementación de la solución, el autor usó la metodología de mejora continua planteada por Deming, por considerar que permite a la organización identificar y corregir de manera constante los problemas y deficiencias en los procesos o servicios que posee. El resultado de la prueba de hipótesis general fue inferior a 0.05 de significancia con un nivel de confianza del 95%, lo que refleja que las medidas implementadas mejoraron la gestión de ciberseguridad en RMO Contratistas Generales SAC.

Tales resultados se confirman con lo arrojado en la encuesta aplicada, donde se ha pasado de una puntuación en el nivel de seguridad en el pretest de 50% entre malo y muy malo, a un 87.5% de regular y un 12.5% a bueno. Por lo tanto, se puede concluir que la propuesta implementada dio los resultados esperados, aumentando el nivel de seguridad en los activos de información.

De lo anterior se desprende que los investigadores sugieren seguir el ciclo propuesto en su trabajo, para, de esta forma, lograr gestionar los riesgos y fortalecer los niveles de seguridad en los activos de una manera más óptima. Aunado a mantener actualizados softwares de seguridad que protejan el hardware de la empresa y evitar ciberataques como el Phishing o Ransomware. Sugieren los investigadores que los programas suministren tecnología que permita reestablecer los servicios previos a la infección del sistema, así como estar constantemente actualizados para reconocer nuevas amenazas cibernéticas y atacar cualquier vulnerabilidad.

Por último, Rojas (2023) realizó una investigación enfocada en los Marketplace de Facebook, usados en la ciudad de Cusco, Perú. Para ello se planteó como fin aplicar la norma ISO 27032 en estos sitios web durante el período 2023, buscando mejorar la seguridad de la información, ya que estos Marketplace presentaban riesgos latentes en las transacciones de comercio electrónico.

Es por ello que el investigador trató de analizar las brechas y riesgos en cuanto a la seguridad de información en estos grupos sociales, ya que los actores principales se pueden ver envueltos en posibles fraudes. Por ello, la significancia de analizar el cumplimiento para identificar posibles áreas de mejora, buscando realizar propuestas para fortalecer la privacidad y seguridad de los datos.

El tipo de investigación fue aplicada con diseño preexperimental, donde la muestra obtenida versó en 100 personas, a las cuales se le aplicó como técnica de recolección de datos la encuesta. En este sentido, el investigador evaluó tres objetivos: grado de capacitación de los usuarios, de cumplimiento de la norma ISO 27032 y análisis de los riesgos de seguridad de la información (Rojas, 2023).

Entre los resultados arrojados por la encuesta está el grado de percepción de los usuarios sobre los riesgos de seguridad, lo cual consideran alto, también que requieren ser capacitados y cumplir con lo estipulado por la norma ISO 27032, para así mejorar la seguridad de la información en los Marketplace de Facebook en el distrito de Cusco (Rojas, 2023).

2.2. Marco empírico

2.2.1. Hipótesis

Las hipótesis planteadas en el presente trabajo son las siguientes:

Alternativa (Ha): “La implementación de la norma ISO 27032 genera una mejora significativa en la seguridad de la información en las pymes de Quito – Ecuador en el año 2024”.

Nula (H0): “La implementación de la norma ISO 27032 no genera una mejora significativa en la seguridad de la información en las pymes de Quito – Ecuador en el año 2024”.

2.2.2. Objetivos de la investigación

Dentro de los objetivos de la investigación que abordará el presente proyecto están:

2.2.2.1. Objetivo General

Diseñar una guía para la implementación de las buenas prácticas de la norma ISO 27032 en las pymes de Quito – Ecuador para la generación de mecanismos de alertas ante posibles ataques en el ciberespacio.

2.2.2.2. Objetivos específicos

A) Diagnosticar la situación actual de las buenas prácticas de la norma ISO 27032 en las pymes de Quito – Ecuador para antecederse ante posibles ataques en el ciberespacio.

B) Definir criterios para la evaluación de la implementación de las buenas prácticas de ciberseguridad en las pymes de Quito – Ecuador de acuerdo a la norma ISO 27032.

C) Establecer los lineamientos para la implementación de los controles y seguimiento a la implementación de las buenas prácticas de Ciberseguridad de acuerdo a la norma ISO 27032.

3. Metodología

El enfoque dado al presente trabajo de investigación es de carácter descriptivo con enfoque documental, ya que se recabó información usando como marco de referencia el COBIT, logrando identificar los requerimientos definidos por la norma ISO 27032, para ser aplicada en las pymes de Quito – Ecuador.

3.1. Diseño y tipo de investigación

El diseño de investigación es descriptiva, apoyada en técnicas documentales. Además, como tipo de investigación se consideró la proyectiva, que según Hurtado de Barrera (2012) busca generar soluciones a partir de un diagnóstico previo.

La idea principal de esta propuesta es elaborar una guía para la implementación de las buenas prácticas de la norma ISO 27032 en las pymes de Quito – Ecuador, y de esta manera buscar la generación de mecanismos de alertas ante posibles ataques en el ciberespacio.

3.2. Población y muestra

La población tomada en cuenta fue la denominada población referencial, la cual indica Hurtado de Barrera (2012) no es más qué “el conjunto de fuentes de las cuales se va a obtener la información respecto a la población en estudio” (p. 153). Por ello, se toma las estadísticas arrojadas por la página oficial de ISO.

3.3. Variables y operacionalización

3.3.1. Variable independiente

Aplicación de la Norma internacional ISO 27032.

Definición conceptual: La Norma ISO 27032 proporciona una guía para la gestión y mitigación de riesgos cibernéticos, buscando ayudar a las organizaciones a mantener el control sobre la información, generando confianza en los usuarios y stakeholders (Normas ISO, 2024).

3.3.2. Variable dependiente

Seguridad de la información.

Definición Conceptual: La norma ISO 27032 es primordial para la seguridad de la información en la era digital actual, proporcionando herramientas efectivas para proteger los datos y los sistemas de información, lo que ayuda a reducir de manera significativa los riesgos cibernéticos, permitiendo a las organizaciones proteger sus activos digitales de manera efectiva (Normas ISO, 2024).

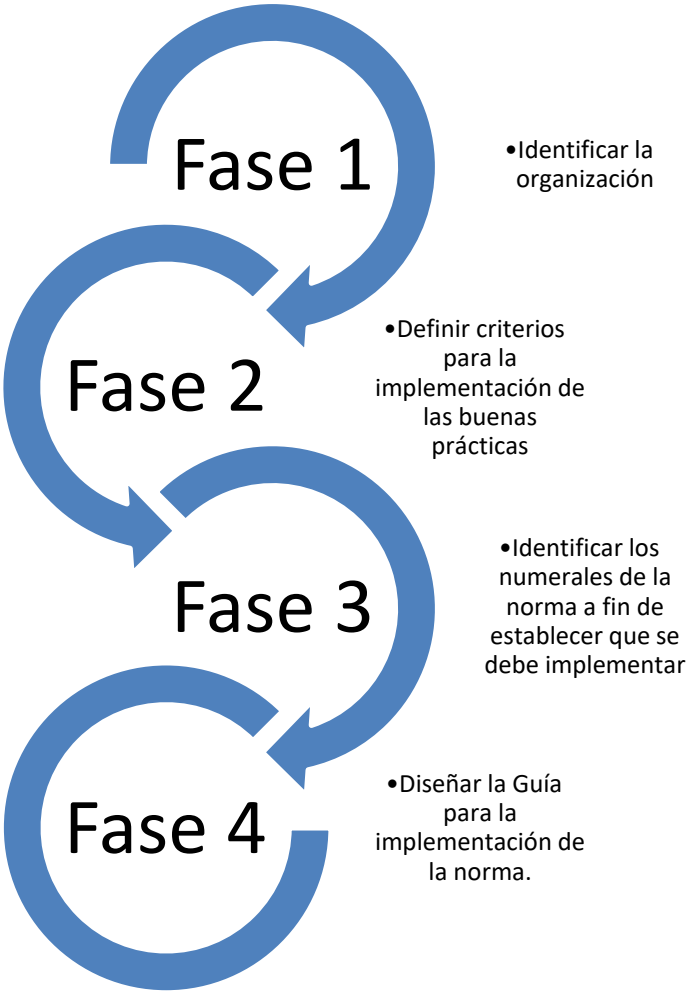
3.4. Fases de desarrollo del trabajo

Las fases planteadas de trabajo se plasman en la figura 3, la cual consta de cuatro fases que se explican a continuación:

- **Fase 1**. Identificar la organización. Se indaga según las referencias publicadas por la página oficial de la ISO cómo se encuentran las empresas pymes en Ecuador y su implementación de buenas prácticas de la norma ISO 27032, reflejando en gráficos sus datos estadísticos.
- **Fase 2**. Definir criterios para la implementación de las buenas prácticas. En este sentido, se define un formato en el cual se puedan identificar aspectos relevantes de la empresa. Luego, para definir los criterios, se toma en consideración lo indicado por la norma ISO 27032 en las organizaciones, todo con el fin de establecer el alcance de la implementación, recursos y otros.
- **Fase 3**. Revisar los numerales de la norma. Se identifican los numerales de la norma que establecen información general y orientado a lineamientos de buenas prácticas.
- **Fase 4**. Diseñar la guía para la implementación de la norma. Para ello se siguen los pasos del ciclo de Deming de Planear y Hacer.

Figura 3.

Fases del desarrollo del trabajo



4. Resultados

Para lograr alcanzar los resultados se esbozan los hallazgos según las fases planteadas.

4.1. Fase 1. Identificar la organización

Para alcanzar esta fase se necesitó en primera instancia contextualizar la norma ISO.

Contextualización de la norma ISO. Los sistemas de gestión a ser implantados en las empresas tienen un impacto, sin importar su tamaño. Para ello se requiere destinar recursos lógicos y físicos, que implican una inversión. Claro está, es muchos menos complejos implantar estos sistemas en empresas pequeñas que en grandes organizaciones, además de percibir sus beneficios de manera más plausibles las primeras, ya que al ir creciendo van adoptando buenas prácticas a través de controles que permiten mitigar riesgos.

En este sentido, las empresas con sistemas de gestión de calidad se enfocan en estructurar procesos, generando para ello procedimientos en pro de optimizar y controlar de mejor manera las operaciones y/o actividades. Pero, al adquirir nuevas tecnologías de vanguardia para competir en el mercado, se requieren controles para mitigar los riesgos.

Por ello, uno de los estándares más utilizados por las empresas son los planteados por la organización ISO, resaltando la norma 27001. Dicha organización realiza encuestas anuales, y en el caso específico que compete a este trabajo, en el país Ecuador, son pocas las empresas que se certifican en este estándar.

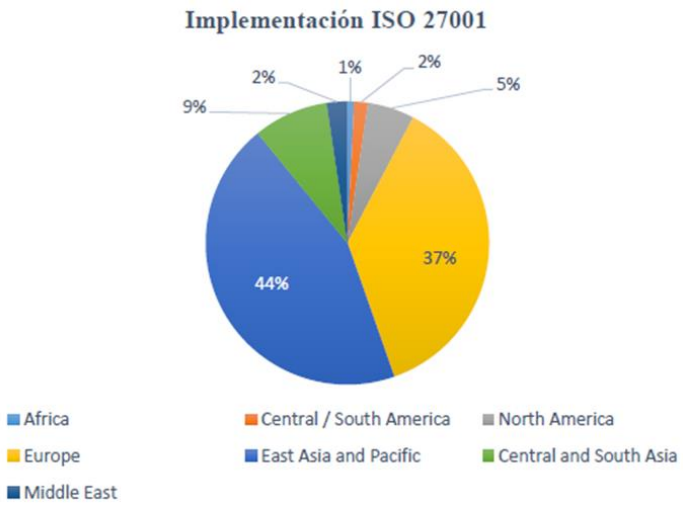
Al ver la figura 4, se percibe a nivel mundial como en la certificación de ISO 27001, para el 2022, solo 71.549 están certificadas, donde apenas el 1,6% pertenecen a América Central y Latinoamérica, siendo Ecuador el cuarto país con más certificaciones.

Así mismo, en los datos de la encuesta de la página oficial ISO indican que existen solo 28 certificaciones y 63 empresas certificadas (ver figura 5). En otras palabras, las empresas no han adoptado en su totalidad las certificaciones, y solo en algunos casos las

acogen para ser usadas como mejores prácticas o para cumplir requerimientos legales. Tal vez lo anterior esté asociado a factores como carencia de conocimiento o falta de expertos en las empresas. De lo anterior se infiere que, en la mayoría de los casos, no se tienen claro los beneficios para implementar un estándar, desconociendo las bases sólidas que proporcionan.

Figura 4.

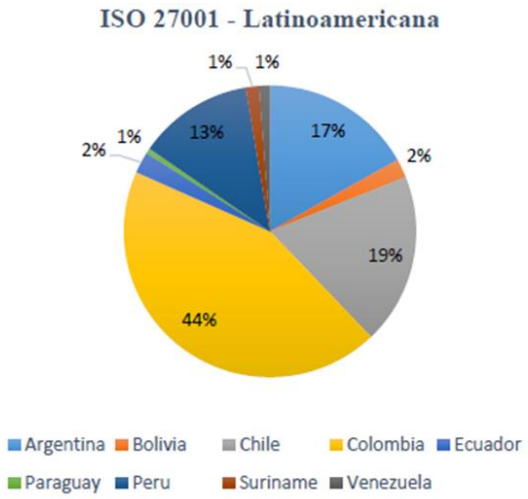
Implementación ISO 27001 a nivel mundial



Fuente: SO Survey (2022)

Figura 5.

Implementación ISO 27001 a nivel de Latinoamérica



Fuente: SO Survey (2022)

Las figuras 4 y 5 muestran que, en la mayoría de los casos, las empresas a nivel mundial no tienen como prioridad certificarse en el estándar 27001. Por lo que dejan de gozar de los beneficios que traen implícitos este tipo de normativas.

Ahora, en el caso de la ISO 27032, que es un complemento a la ISO 27001, al realizar una investigación preliminar, se conoció que las empresas en sí no tienen idea de cómo conseguir estas certificaciones. De esta manera, se plantea a continuación las pautas a tener en cuenta para implementar estas buenas prácticas.

4.2. Fase 2. Definir criterios para la implementación de las buenas prácticas.

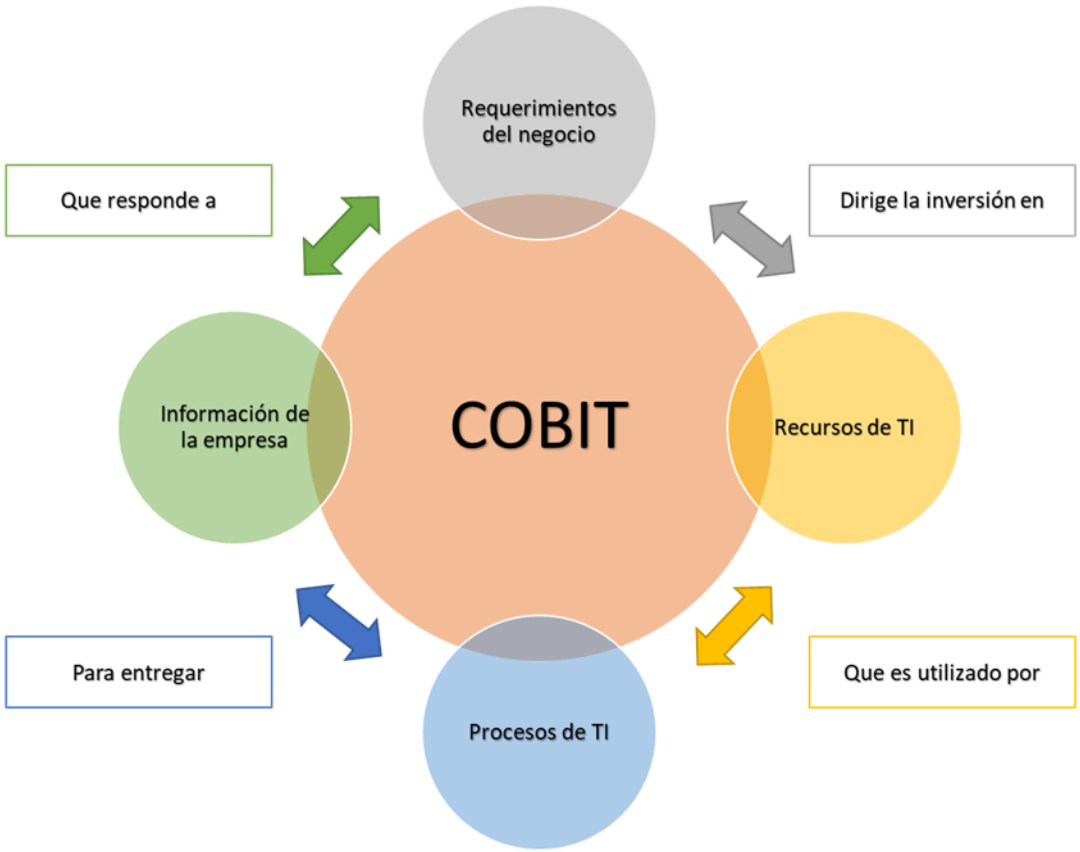
Para implementar las buenas prácticas descritas en la Norma ISO 27032, se hace necesario entender el tipo de organización a que se implementará, cuál es su misión, objetivos del negocio y si tiene o no implementado algún tipo de sistema de gestión acoplado a la norma ISO 9001 o ISO 27001. De igual manera, se necesita saber dentro de sus elementos su infraestructura tecnológica, marcos regulatorios, etc. Estos elementos van a dar un horizonte de si la empresa está preparada para hacer frente a la ciberseguridad. Es así como se sugiere:

- **Aplicación de la norma ISO 27032**: en este aspecto se debe estudiar si le conviene o no a la empresa en cuestión aplicar esta norma, para ello, se necesitará identificar los ítems a tomar en cuenta y/o aspectos que son necesarios fortalecer de lo que tengan implementado en el momento del estudio, así como lo que la norma establece como buenas prácticas.
- **Definición de los numerales de la norma**: tras decidir implementar la norma ISO 27032, es necesario definir qué numerales de la norma de adecuan al tipo de organización que estén orientados a las buenas prácticas, también se necesita definir los requerimientos para su implementación.

Siguiendo la metodología COBIT y sus buenas prácticas, se generó una plantilla para entender a la organización que se esté estudiando, esto con el fin de establecer los elementos que la conforman, como niveles de seguridad, infraestructura, entre algunos aspectos. La figura 6 muestra el ciclo donde se identifican los requisitos del negocio, recursos, procesos de TI e información de la empresa que serán usados.

Figura 6.

Principios básicos del COBIT



Fuente: Institute. CddCyeIG. COBIT 4.1. (2007).

En función de lo anterior, se plantea una plantilla (ver tabla 2), que sirva de base para entender a la organización, donde se podrán visualizar aspectos claves como misión, visión, objetivos del negocio, infraestructura, sistemas, entre otros elementos, que servirán de sustento en la implementación de la norma ISO 27032.

Tabla 2.

Información de la empresa

Información de la empresa	
Objetivo: Recabar información preliminar de la empresa para establecer tamaño, tipo de empresa, tipo de tecnologías, entre otros elementos que ayudarán a determinar el mejor camino para la implementación de las buenas prácticas de la ISO 27032	
Información General	
Nombre de la empresa	
Sector al que está dirigido	
Tipo de empresa	
Objetivos del negocio	
Misión	
Visión	
Número de procesos	
Número de empleados	
Información Alta dirección	
¿Es importante el tema de seguridad?	
¿Apoyan a las otras dependencias para el tema de seguridad?	
¿Están capacitados en el tema de seguridad?	
Estructura de TI y Seguridad	
Informarse sobre la estructura de empresa a nivel de TI y seguridad	
Áreas de TI	
Especialistas de seguridad de la información	
Áreas de riesgos	
Descripción tecnológica	
Informarse sobre los servicios tecnológicas y sistemas de la empresa	
Número de Sistemas	
Número de sistemas propios	
Número de sistemas tercerizados	
Número de servicios prestados	
Seguridad informática y de la información	
Informarse sobre los mecanismos de seguridad con los que cuenta la organización	
Software	
Hardware	
Mecanismos de seguridad para el acceso a internet	
Mecanismos de cifrado para transferencia de información	
Indicar para cada sistemas y servicio identificado los mecanismos de seguridad	
Controles lógicos	
Roles y perfiles definidos para acceso a los sistemas	
Cuentan los sistemas con procedimientos para su implementación frente a los cambios	
Procesos definidos para asignar roles y usuarios	

Políticas establecidas de acceso para los sistemas de información cuando se conectan a una red diferente a la de la empresa	
Mecanismos definidos para dar acceso a terceros a los sistemas de información	
Marco legal/ Cumplimiento	
Informarse sobre el marco legal en el cual la empresa se desenvuelve para lograr identificar que regulación tomar como referencia para implementar las buenas prácticas de Ciberseguridad	
Leyes	
Decretos	
Circulares	
Sistemas de Gestión Implementados	
Informarse sobre si tienen sistemas de gestión implementados y si están certificados	
ISO 27001	
ISO 9001	
Otro	
Manejo de Incidentes	
Tiene implementado un sistema para manejo de incidentes	
Tiene políticas establecidas para el manejo de incidentes de seguridad	
Concientización y Capacitación	
Cuentan con campañas periódicas para la concientización sobre ataques cibernéticos	
Cuentan con un cronograma de capacitación para la ciberseguridad	
Dan seguimiento a los temas de capacitación y/o concientización	

La plantilla de la Tabla 2 permitirá al evaluador conocer la situación actual de la empresa a evaluar. Luego, se necesita identificar y establecer cuál es el nivel de ciberseguridad que tiene esa empresa. De esta manera, se sugiere usar algún tipo de herramienta tecnológica, en esta investigación se indagó y se consiguió que la organización KPMG tiene disponible una aplicación móvil free que permite hacer diagnósticos en los aspectos de interés. Dicha app tiene como nombre Cyber CAT, y es de fácil acceso e instalación.

Cyber CAT tiene como objetivo poner a disposición de las organizaciones una herramienta que les permita autoevaluarse con respecto a la seguridad de la información, en este sentido, KPMG (2017) refiere sobre esta app “proporciona una cuantitativa visión de la

cibernética actual, exposición al riesgo y recomendaciones para fortalecer la postura de seguridad" (p. 3).

En este sentido, la autoevaluación con la herramienta se hace enfocándose en dos aspectos fundamentales, exposición al riesgo el primero, preparación de la empresa frente a los incidentes. Para ello, se evalúan elementos como: gobierno, gestión de riesgo cibernético, respuesta a investigación de incidentes, (KPMG, 2017) esto proveerá como insumos lecciones aprendidas que mitiguen en los procesos críticos los impactos (ver figura 7).

Figura 7.

Estructura de la app Cyber CAT



Fuente: KPMG (2017)

4.3. Fase 3. Revisar los numerales de la norma

La ISO 27032 propone buenas prácticas en el área de ciberseguridad, permitiendo a las empresas implementarlas. Los elementos a tomar en cuenta para establecer los criterios para la implementación de la presente guía son los proporcionados por la app Cyber CAT, entre los que destacan: Gobierno, Administración de Riesgo, Protección de terceras partes, Operación y Continuidad., Monitoreo y Detección, Conciencia, Respuesta e Investigación, y Administración del Cumplimiento (KPMG, 2017)

Con lo expuesto, se trata de brindar a la empresa tips claves para identificar y conocer las debilidades en puntos clave, y así buscar fortalecerlos mediante las mejores prácticas brindadas por la norma ISO 27032, en función de ello, se esgrime los 13 numerales presentes en la norma (ver tabla 3):

Tabla 3.

Numerales ISO 27032

Numeral	Descripción
1	Alcance
2	Aplicabilidad
3	Referencias
4	Términos
5	Abreviaturas
6	Generalidades
7	Partes interesadas en el Ciberespacio
8	Activos en el Ciberespacio
9	Amenazas contra la seguridad del Ciberespacio
10	Roles de las partes interesadas en la Ciberseguridad
11	Directrices para los interesados
12	Controles de Ciberseguridad
13	Marco del intercambio de información y la coordinación

Fuente: Normas ISO (2024)

La tabla 3 presenta los numerales generales de la norma en estudio, los cuales serán base para la presente guía. En este sentido, se requiere contar con lo siguiente:

A) Apoyo de la alta dirección, con el fin de garantizar que la implementación sea efectiva.

B) Especialista en el área seguridad de la información y ciberseguridad.

C) Equipo interdisciplinario en la empresa en estudio, haciéndose indispensable manejen el tema de tecnología, procesos TI, de igual forma, uno de estos miembros debe ser experto en la evaluación de riesgos para apoyar los procesos para cada uno de los activos.

D) Políticas y procedimientos de la empresa en los cuales se puede conocer cada uno de los procesos, actividades y activos involucrados (Internet Security Auditors, 2018).

4.4. Fase 4. Diseñar la Guía para la implementación de la norma

Para validar los numerales, se ha de tener en cuenta los campos requerimiento/ descripción, haciendo la salvedad que los numerales del 1 al 6 son proporcionados para conocer la norma, por lo que no se requiere implementarlos, la guía se enfocará en los numerales del 7 al 13, que se ven reflejados cada uno de manera respectivas en las tablas de la 4 a la 10.

Tabla 4.

Numeral 7

Numeral 7 - Partes interesadas en el Ciberespacio	
Objetivos	Identificar los stakeholders dentro de la empresa
Requerimientos	Para esta norma los interesados en el ciberespacio se clasifican en dos grupos: • Los consumidores, esto incluye personas naturales y jurídicas sean con fin público como privado. • Proveedores, se requiere incluir a los proveedores de servicios de Internet y de servicios de aplicaciones.
¿Cómo implementar?	
La empresa necesita establecer un documento o formato donde se solicite a cada dependencia un listado de funcionarios y proveedores.	
Se requiere consolidar el listado, para ello clasifique consumidores y proveedores	
Para cada grupo establecer lo siguiente: • Si son Consumidores: • Indique procesos y/o actividades que realiza. • Indique Sistemas o Servicios de información que usan. • Indique el impacto de los servicios en su proceso, tomando en cuenta si es alto, medio o bajo. • Si son Proveedores: • Indique tipo de Proveedor, si es crítico o no crítico. • Liste cada servicio prestado, establezca si son servicios en la nube, internet u otro y describa cada uno, también indique si el servicio se brinda en la empresa con las herramientas de la misma o en las instalaciones del proveedor. • Cuáles procesos soporta.	

Fuente: Adaptado de Normas ISO (2024)

Tabla 5.

Numeral 8

<table>
<tr><td colspan="2">Numeral 8 - Activos en el Ciberespacio</td></tr>
<tr><td>Objetivos</td><td>Identificar activos dentro de la empresa</td></tr>
<tr><td>Requerimientos</td><td>Un activo es algo que tiene valor para un individuo o una empresa. Existen varios tipos de activos, dentro de los cuales se incluyen, pero no se limitan a:
a) la información;
b) software;
c) físico;
d) los servicios;
e) las personas, sus cualificaciones, habilidades y experiencia, y
f) los activos intangibles, como la reputación y la imagen.
Para los fines de esta norma nacional, los activos en el Ciberespacio se clasifican en las siguientes clases:
Personal
Organizacional.
Para ambas clases, un activo también puede ser clasificado como:
Activo físico, cuya forma existe en el mundo real
Activo virtual, que solo existe en el Ciberespacio y no se puede ver o tocar en el mundo real.</td></tr>
<tr><td colspan="2">¿Cómo implementar?</td></tr>
<tr><td colspan="2">Identifique:
• Información necesaria para la ejecución del proceso y/o servicio
• Aplicaciones requeridas para gestionar esa información
• Alojamiento de las aplicaciones
• Dónde se almacena la información
• Si las aplicaciones dependen o son administradas por un tercero
• Por donde se transmite la información (por red local o por medio de internet)</td></tr>
<tr><td colspan="2">Realice un inventario de cada activo, tenga en cuenta los siguientes aspectos:
• Nombre
• Procesos asociados
• Categoría a la que pertenece: Hardware, Software, Servicio, Personas, otros.
• Ubicación (Virtual - Físico)
• Tipo: Tercerizado o Propio.
• Criticidad: Alto, Medio o Bajo.
<table>
<tr><td>Nº</td><td>Activos</td><td>Procesos</td><td>Categoría</td><td>Ubicación</td><td>Tipo</td><td>Criticidad</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td colspan="2">Validar lo arrojado con en el numera A8 – Gestión de Activos de la norma ISO 27001.</td></tr>
</table>

Fuente: Adaptado de Normas ISO (2024)

Tabla 6.

Numeral 9

Numeral 9 - Amenazas contra la seguridad del ciberespacio	
Objetivos	Identificar posibles amenazas a las cuales la empresa puede estar expuesta en el Ciberespacio.
Requerimientos	Para establecer las amenazas se necesitan tener identificados los activos que interactuaran en el Ciberespacio. Las amenazas al Ciberespacio se pueden dividir en dos áreas claves: Activos personales: Refiere a aspectos de identidad que pueden tener que ver con la fuga o robo de información personal.

Numeral 9 - Amenazas contra la seguridad del ciberespacio	
	Activos de la organización: Intrusiones que se pueden hace por varios medios de malhechores.

¿Cómo implementar?

Amenazas

Ubicar alguna referencia de catálogo de amenazas para su identificación. Se supiere en este caso tomar del Ministerio de Hacienda y Administraciones Públicas de España la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html y lo indicado por la norma técnica (No. 2018-0652) de Ecuador que establece lineamientos sobre gestión de incidentes y vulnerabilidades.

Del inventario obtenido en el ítem 8, identificar las amenazas a las cuales se ven expuestos cada uno de los activos. Es necesario se tome en cuenta lo indicado por el catálogo definido como referencia, e identificar vulnerabilidades clasificándolas entre físicas y lógicas.

Nº	Activos	Amenazas

Identificar aplicaciones y/o servicios expuestos en el ciberespacio, establecer vulnerabilidades a las amenazas, así como los impactos que esto genera.

Nº	Activos	Amenazas	Vulnerabilidad

Una vez identificadas las amenazas, especificar posibles agresores que podrían generar un ataque, ejemplo: Ex empleado, Empleado, Hacker, otro.

Nº	Activos	Amenazas	Vulnerabilidad	Posible Agresor

Para cada amenaza establezca niveles de impacto. Tome como referencia el siguiente esquema de calificación:

Incidencia de la Amenaza	Valor de la dimensión del activo			
	0	1	2	3
Sin incidencia	0	0	0	0
Incidencia baja	0	1	2	3
Incidencia media	0	2	3	4
Incidencia alta	0	3	4	5

En función de este cuadro evaluar cada amenaza de acuerdo al impacto en los pilares de la información, llene lo siguiente:

Amenaza	Impacto Confidencialidad	Impacto Integridad	Impacto Disponibilidad

Vulnerabilidades

Identificar de las labores diarias desempeñadas, a qué proceso está asociado, e indicar las vulnerabilidades en el Ciberespacio.

A cada amenaza identificada, establecer las vulnerabilidades a las cuales se ve expuestas.

En caso de existir vulnerabilidades técnicas, es primordial se ejecute un análisis de vulnerabilidades por parte de un tercero para los canales y sistemas de información.

Estar inscrito en bases de vulnerabilidades y/o amenazas, con el fin de alimentar el inventario e implementar una solución efectiva.

Clasificar las vulnerabilidades identificadas de acuerdo a la criticidad del activo evaluado, así se podrá establecer prioridades para la implementación de controles.

Fuente: Adaptado de Normas ISO (2024)

Tabla 7.

Numeral 10

<table>
<tr><th colspan="2">Numeral 10 - Roles de las partes interesadas en la Ciberseguridad</th></tr>
<tr><td>Objetivos</td><td>Definir los roles que desempeñan los stakeholders.</td></tr>
<tr><td>Requerimientos</td><td>Cada stakeholders identificado requiere desempeñar un rol activo en su respectivo uso y desarrollo de Internet.</td></tr>
<tr><th colspan="2">¿Cómo implementar?</th></tr>
<tr><td colspan="2">Para cada stakeholders identificado en el numeral 7, establecer roles, tome en cuenta: incidencia que tienen dentro de la operación, específique tipo de actores, directos o indirectos.
<table>
<tr><td>Nº</td><td>Interesado</td><td>Rol</td><td>Tipo de actor</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>
Tomar como referencia las planteadas en el numeral 10 de la ISO27032, como son:

Los roles de los consumidores pueden incluir, pero no se limitan a, los siguientes:
Usuarios de aplicaciones generales del Ciberespacio o usuario general;
Comprador/vendedor, que participa en la colocación de productos y servicios en sitios de subastas en línea y del mercado para los compradores interesados y viceversa;
Blogger y otro contribuyente de contenidos;
Proveedor independiente de aplicaciones (IAP) dentro de un contexto de aplicación;
Miembro de una organización;
Otros roles

Validar lineamientos con la norma ISO27032 – numeral 10, con el fin de identificar los roles de acuerdo a tipo de stakeholders.</td></tr>
</table>

Fuente: Adaptado de Normas ISO (2024)

Tabla 8.

Numeral 11

<table>
<tr><th colspan="2">Numeral 11 - Directrices para los interesados</th></tr>
<tr><td>Objetivos</td><td>Indicar lineamientos para definir directrices, los cuales deberán abarcar las tres áreas principales que presenta el numeral 11.</td></tr>
<tr><td>Requerimientos</td><td>Las tres áreas de este capítulo se centran en:
Seguridad para los consumidores
Gestión de riesgos de seguridad de la información interna de la empresa.
Requisitos de seguridad mínimo que los proveedores deberán especificar para que los consumidores apliquen.</td></tr>
<tr><th colspan="2">¿Cómo implementar?</th></tr>
<tr><td colspan="2">Para la implementación de este numeral, se necesita la evaluación y tratamiento de riesgos, por ello tomar en cuenta lo siguiente:
Seleccionar metodología para identificar y evaluar riesgos.
Validar el estándar ISO 31000 (plantea principios y directrices genéricas sobre la gestión de riesgos).
Verificar la ISO/IEC 27005 – Gestión de riesgos de seguridad de la información (Da directrices y procesos para la gestión de riesgos de seguridad de la información en una empresa).</td></tr>
<tr><td colspan="2">Establecer la matriz de calificación de riesgos, para ello tomar en cuenta la metodología de riesgos seleccionada.</td></tr>
<tr><td colspan="2">Al identificar y evaluar riesgos tomar en consideración lo especificado en el numeral 11 de la ISO27032. Esto contribuirá a establecer controles de una mejor manera para la administración de Ciberseguridad de la empresa.</td></tr>
<tr><td colspan="2">Del inventario de activos del numeral 8, identificar:
Posibles riesgos a los que se pueden ver expuesto esos activos,
Establecer posible factor que los genera (Personas, Procesos, Sistemas, otros),</td></tr>
</table>

Identificar los stakeholders internos o externos para establecer una causa raíz e impacto.
Validar los lineamientos que se establezcan según marco jurídico vigente en el país según el sector de la empresa en estudio

Fuente: Adaptado de Normas ISO (2024)

Tabla 9.

Numeral 12

Numeral 12 - Controles de Ciberseguridad	
Objetivos	Parametrizar lineamientos para diseñar controles, los cuales ayudarán a mitigar el impacto de los riesgos previamente identificados.
Requerimientos	Identificados los riesgos de Ciberseguridad, se procede a la redacción de los lineamientos apropiados, así como los controles de Ciberseguridad que soportan a los requisitos de seguridad.
¿Cómo implementar?	
Tomar en cuenta las aplicaciones e infraestructura, en este sentido son varios los elementos como proveedores, servidores u usuarios finales, todos estos ya fueron identificados en numerales anteriores (7-11).	
Definir políticas con el fin de regular la información de la empresa, bien que vaya a ser administrada en el Ciberespacio, o es su defecto compartido entre los usuarios. Para ello se sugiere que los lineamientos tengan como mínimo los siguientes aspectos: • Actualizaciones de seguridad. • Capacitación y concientización de forma periódica. • Lineamientos para la clasificación y categorización de la información inmersa en cada proceso. • Evaluación periódica de cada desarrollo ad hoc que estén en el ciberespacio. • Monitoreos de información y de accesos. Para ello especificar cómo sería en el caso de servidores y apps.	
Validar lineamientos presentes en la norma ISO27032, específicamente en su numeral 12.	

Fuente: Adaptado de Normas ISO (2024)

Tabla 10.

Numeral 13

Numeral 13 - Marco de intercambio y Coordinación de la información	
Objetivos	Identificar los lineamientos pertinentes para el intercambio de información en el ciberespacio
Requerimientos	Establecer un sistema para el intercambio y coordinación de la información que ayude a preparar una respuesta a los eventos e incidentes de Ciberseguridad.
¿Cómo implementar?	
La norma establece claramente unas condiciones a considerar para implementar este numeral, los mismos se detallan a continuación: • En función de toda la información recabada de los ítems anteriores, identificar qué información se recibe y/o envía en el ciberespacio, estableciendo que medios se utilizan para ello (aplicación, FTP, WEB, otro) que categorización tiene la información (Alta, media, baja, confidencial, publica, otros). • Según lo anterior, para cada medio usado y tipo de información se hace necesario identificar: riesgos, amenazas, vulnerabilidades, así como cualesquiera otros elementos asociados. El objetivo fundamental es identificar los elementos esenciales en los que la información que se comparte en el ciberespacio se pueda ver comprometida. • Realizar la evaluación de riesgos según la metodología seleccionada por la empresa. En este sentido, es fundamental ubicar los riesgos que resulten más críticos, de esta manera se podrán	

Numeral 13 - Marco de intercambio y Coordinación de la información
generar controles que permitan mitigar impactos en varios ámbitos como financieros o jurídicos, u otros pertinentes. • Identificar políticas o normas para el tratamiento de esta información.

Fuente: Adaptado de Normas ISO (2024)

Para implementar esta norma tomar en cuenta la metodología del ciclo de Deming, como es:

- **PLAN**: esta etapa fue descrita en la fase 1, donde se plantea la forma de abordar la norma ISO en estudio, se indaga sobre la empresa a estudiar y se propone una plantilla, con esto se busca conocer la unidad de estudio e identificar a las partes involucradas en el ámbito cibernético, se hace indispensable hacer un inventario de activos de información con sus respectivas amenazas y vulnerabilidades para reconocer el impacto por cada una de ellas y realizar la gestión de riesgos respectiva, tal como lo indica el numeral 8 de la norma ISO 27032.
- **DO**: en esta fase de ‘hacer’ se aplicará una evaluación de riesgos, para ello se inicia con la descripción de los roles de las partes interesadas en la ciberprotección, se plantean las directrices con respecto al tratamiento de los riesgos encontrados que busque alcanzar los objetivos de control propuestos, se necesita tomar en cuenta los recursos presentes y responsabilidades de los encargados para continuar con la elaboración de controles propuestas por la ISO 27032.
- **CHECK**: en esta fase de ‘verificar’ se necesita ejecutar la monitorización constante y revisión a tiempo de posibles incidentes de seguridad. Por ello, es vital la concientización de los encargados de la empresa para reconocer posibles amenazas y evitar que se efectúe.
- **ACT**: en esta fase ‘actuar’ se activa cuando culmina el periodo de prueba, se evalúan los resultados y las oportunidades de mejora en la empresa con respecto a la fase

anterior, además de realizar cada cierto tiempo medidas correctivas con respecto a la norma ISO 27032.

5. Conclusiones

La ciberseguridad es uno de los temas que más ocupa a nivel mundial a todas las organizaciones, siendo las pymes las más vulneradas, tal vez por falta de implementación de buenas prácticas como las indicadas por la norma ISO 27032, de allí que en este trabajo investigativo se buscó como objetivo primordial diseñar una guía que fomentará la implementación de estas buenas prácticas en las pymes de Quito – Ecuador.

Para ello, se desarrolló la investigación en cuatro grandes fases, en la fase 1 se indagó, según las referencias publicadas por la página oficial de la ISO, cómo se encuentran las empresas pymes en Ecuador, y si las mismas implementaban o no buenas prácticas de la norma ISO 27032, en este sentido, se reflejaron gráficos con datos estadísticos que son fuente de esta organización ISO, indicando que a nivel mundial son pocas las pymes que se hayan certificadas en la ISO 27001, por lo que se puede inferir que, en la mayoría de los casos, no tienen las empresas claro los beneficios para implementar un estándar, desconociendo las bases sólidas que proporcionan. Es de destacar en este punto que la norma en estudio, la ISO 27032, es un complemento de la ISO 27001, y dentro de las revisiones realizadas se conoció que las empresas en sí no tienen idea de cómo conseguir estas certificaciones.

En la fase 2 se definieron los criterios para la implementación de las buenas prácticas de la norma en estudio, por lo cual, la pyme que desee incorporar esta norma requiere estudiar previamente si le conviene o no acatarla, para ello deberá realizar un diagnóstico y determinar qué aspectos desea fortalecer de lo que tengan implementado en el momento del estudio, así como lo que la norma establece como buenas prácticas. En el caso de decidir implementarla, requieren definir qué numerales adecuar a su tipo de organización., así como los requerimientos. Para hacer el trabajo menos laborioso de quien decida implementar, en este trabajo se planteó una planilla siguiendo los principios básicos del COBIT que ayude a

entender a la organización que se vaya a estudiar, esto con el fin de establecer los elementos que la conforman, como niveles de seguridad, infraestructura, entre algunos aspectos.

Es necesario entender que siempre que se desee implementar unas buenas prácticas de ISO, y sobre todo esta que se estudió, es indispensable entender el tipo de organización a que se implementará, cuál es su misión, objetivos del negocio y si tiene o no implementado algún tipo de sistema de gestión acoplado a la norma ISO 9001 o ISO 27001, para poder tomar una decisión con base firme.

Además de hacer uso de plantilla planteada, que ayudará al evaluador en su diagnóstico, se necesita identificar y establecer cuál es el nivel de ciberseguridad que tiene esa empresa, para esto, se sugiere hacer uso de algún tipo de herramienta tecnológica. En este trabajo se sugiere usar la aplicación móvil free “Cyber CAT” de la organización KPMG, que permite hacer diagnósticos en los aspectos de interés.

Para la fase 3, se revisaron los numerales de la norma, tomando en cuenta los criterios de ciberseguridad manejados por la herramienta Cyber CAT, como fueron: Gobierno, Administración de Riesgo, Protección de terceras partes, Operación y Continuidad., Monitoreo y Detección, Conciencia, Respuesta e Investigación, y Administración del Cumplimiento. En función de ello, se seleccionaron 13 numerales a aplicar para el diseño de la norma.

Por último, se diseñó la guía en la fase 4, tomando en consideración los criterios seleccionados. Es de destacar, que la guía se enfocó en los numerales del 7 al 13. Planteándose siete tablas en total, donde se describe el objetivo del numeral, como los requerimientos necesarios y cómo llevarlo a cabo. Para implementar esta norma, se hace necesario tomar en cuenta la metodología del ciclo de Deming.

6. Recomendaciones

Entre las recomendaciones se plantean las siguientes:

- Antes de tomar la decisión de implementar las buenas prácticas de la Norma ISO 27032 valide que cuenta con el apoyo de la alta dirección de la empresa en estudio, para así garantizar que la implementación sea efectiva.
- El experto seleccionado para hacer uso de la presente guía, si no es experto en el área de ciberseguridad, se le sugiere buscar especialistas que lo orienten a realizar en primera instancia un buen diagnóstico, para luego determinar qué criterios de la norma en estudio desea aplicar.
- Para aplicar una norma como la ISO 27032, se necesita contar con un equipo multidisciplinario, que manejen los procesos de TI y seguridad de la información, así como tener implementado política y procedimientos que todos manejen.

7. Referencias bibliográficas

Agencia de Regulación y Control de las Telecomunicaciones. ARCOTEL. (2018, 31 de julio). *Normativa técnica sobre servicios de telecomunicaciones* (No. 2018-0652). https://www.gob.ec/sites/default/files/regulations/2018-10/ARCOTEL-2018-0652-2018-07-31-TELECOMUNICACIONES-MATRIZ.pdf

AVAST. (2022). *Ingeniería social y cómo protegerse*. AVAST. https://www.avast.com/es-es/c-social-engineering.

CAF - Banco de Desarrollo de América Latina y el Caribe. (2023). *Pymes en Ecuador: Un análisis detallado*. https://scioteca.caf.com/bitstream/handle/123456789/2132/CAF_PYMES_ECUADOR.pdf?sequence=9&isAllowed=y#:~:text=Para%202020%2C%20hab%C3%ADan%20846%20265,el%207.6%20%25%20del%20parque%20empresarial.

Carbajal, O. Y. (2006). Sistemas de detección de intrusos (IDS): Seguridad en Internet. *Polibits*, (34), 31 - 33. https://www.redalyc.org/pdf/4026/402640447006.pdf

Drucker, P. F. (1993). *La sociedad poscapitalista.* Editorial Suramericana.

Durán, J. (2020). *Principales características, modos de perpetración y vulneración de la seguridad informática a través de la modalidad carding* [Trabajo de grado, Universidad Nacional Abierta y a Distancia UNAD]. Repositorio Institucional – UNAD. https://repository.unad.edu.co/bitstream/handle/10596/34366/jduranpa.pdf?sequence=1&isAllowed=y

Esginnova. (2021, 03 de marzo). ¿Qué es la seguridad de la información y cuántos tipos hay? *PMG SSI*. https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/

Gallegos, M. (2023). *Implementación de la norma ISO 27032 en una empresa contratista* [Tesis de grado, Universidad Tecnológica del Perú]. Repositorio Institucional – UTP. https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/8141/M.Gallegos_A.Valencia_Tesis_Titulo_Profesional_2023.pdf?sequence=1&isAllowed=y

Garduño, T. (2009). *Guía Técnica para elaborar o actualizar Lineamientos*. Procuraduría Federal del Consumidor. https://www.profeco.gob.mx/juridico/Documentos/CGA/Manuales/GT-EAL-610.pdf

Guzmán, S. (2019). *Guía para la implementación de la norma ISO 27032* [Tesis de grado, Universidad Católica de Colombia]. Repositorio Institucional – Universidad Católica de Colombia. https://repository.ucatolica.edu.co/server/api/core/bitstreams/9ff18d8b-4832-448c-8325-0b4a839b90a6/content

Hurtado de Barrera, J. (2012). *Metodología de la Investigación.* Quirón.

Information Systems Audit and Control Foundation (ISACF). (2007). *COBIT 4.1: Framework for Enterprise Control*. ISACF.

Internet Security Auditors. (2018). *Consultoría para la Implementación de un Marco de Ciberseguridad ISO/IEC 27032*. Isec Auditors. https://www.isecauditors.com/consultoria-csf-iso-27032

Jaramillo, C. A. (2015). *Metodología para evaluar, detectar riesgos y vulnerabilidades en redes informáticas* [Tesis de grado, Universidad Politécnica Salesiana]. https://dspace.ups.edu.ec/handle/123456789/7910

KPMG. (2017). *KPMG Cyber CAT.* https://assets.kpmg.com/content/dam/kpmg/qm/pdf/fs-cyber-cat-app-flyer-2017.pdf

KPMG. (2018). *Building Cyber Resilience in Asset Management, Thought Leadership, Cyber security risk radar*. https://assets.kp

mg.com/content/dam/kpmg/bm/pdf/2018/07/building-cyber-resilience-in-asset-management.pdf

Limache, Y. (2022). *Aplicación de la norma ISO 27035:2016 para la gestión de incidentes de seguridad de la información en LISERME S.R.L.* [Tesis de grado, Universidad Católica de Santa María]. Repositorio Institucional – Universidad Católica de Santa María. https://repositorio.ucv.edu.pe/handle/20.500.12692/102422

Lykhova, S. S. (2022). International and national standards on societal information security. *Revista Científica General José María Córdova, 20*(38), 247-264. https://revistacientificaesmic.com/index.php/esmic/article/view/898/845

Machín, N. (2016). La ciberseguridad como factor crítico en la Unión Europea. UNISCI: *Revista UNISCI*, (42), 41 - 51. https://www.ucm.es/data/cont/media/www/pag-89564/UNISCIDP42-2NIEVA-MANUEL.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información de Ecuador. (2022). *Diagnóstico de las capacidades de ciberseguridad.* https://www.telecomunicaciones.gob.ec/wp-content/uploads/2023/05/DIAGNO%CC%81STICO-DE-LAS-CAPACIDADES-DE-CIBERSEGURIDAD-Ecuador-Diciembre-2022_compressed.pdf

MINTEL – CONSULTRANS. (2017). *Little Data Book on Information and Communication Technology*. https://www.itu.int/pub/D-IND-LDB/es

Monje, C. (2011). *Metodología de la investigación cuantitativa y cualitativa: Guía didáctica*. Universidad Surcolombiana. https://www.uv.mx/rmipe/files/2017/02/Guia-didactica-metodologia-de-la-investigacion.pdf

ISO/IEC. (2024). *Tecnología de la información — Técnicas de seguridad — Gestión de la continuidad del negocio* (Norma ISO/IEC 27032:2024). Ginebra, Suiza: Organización Internacional de Normalización. https://normasiso.org/norma-iso-27032/

Observatorio de Derechos Digitales. (s.f.). *Derechos Digitales*. https://www.derechosdigitales.org/

Pacheco, D. (2019). Las TIC como estrategia competitiva en la gestión empresarial. *Revista de Administración, 35*(2), 125-140. https://revistaenfoques.org/index.php/revistaenfoques/article/view/72

Paredes, K. (2022). *Guía de implementación de políticas de control para mitigar los ciberataques basados en el modelo carding en la COAC "Riobamba Ltda."* [Tesis de grado, Universidad Nacional de Chimborazo]. http://dspace.unach.edu.ec/bitstream/51000/8918/1/Paredes%20D.%2C%20%20Karen%20V.%20%282022%29%20GU%C3%8DA%20DE%20IMPLEMENTACI%C3%93N%20DE%20POL%C3%8DTICAS%20%281%29.pdf

Párraga, L. (2017). La *implementación de las tecnologías de la información y comunicación en las PYMES de la zona 4 del Ecuador y su impacto en la competitividad empresarial* [Tesis de grado, Universidad Nacional Mayor de San Marcos]. https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/7612/Parraga_zl.pdf?sequence=3&isAllowed=y

Primicias. (2024, 25 de marzo). Noticia: Ecuador encabeza el listado de países en la región con más ataques de phishing. *Primicias*. https://www.primicias.ec/noticias/tecnologia/ecuador-deteccion-ataques-phishing/

Realyvásquez, A. K. (2018). Applying the Plan-Do-Check-Act (PDCA) cycle to reduce the defects in the manufacturing industry: A case study. *Applied Sciences, 8*(11), 2181. https://doi.org/10.3390/app8112181

Rentería, F. (2013). *Inicio y evolución de la seguridad informática en el mundo* [Trabajo de grado, Universidad Piloto de Colombia]. http://polux.unipiloto.edu.co:8080/00001532.pdf

Rodríguez, E. (2009). Ventajas e inconvenientes de las TIC en el aula. En Rodríguez (Eds.), *Cuadernos de Educación y Desarrollo* (pp. 33 – 35). Centro Educativo de Cádiz, España. https://www.eumed.net/rev/ced/09/emrc.htm

Rojas, J. (2023). *Aplicación de la norma internacional ISO 27032 para la seguridad de la información en los marketplaces de Facebook, Cusco 2023* [Tesis de grado, Universidad César Vallejo]. Repositorio Institucional – UCV. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/113071/Rojas_MJJ-SD.pdf?sequence=1&isAllowed=y

Sampieri, R. H. (2010). *Metodología de la investigación*. McGraw-Hill.

ISO Survey. (2022). *ISO Survey of certifications to management system standards*. https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

Superintendencia de Servicios de Certificación Electrónica (SUSCERTE). (2022, abril). *Introducción a la gestión de riesgos y amenazas en la seguridad informática*. Módulo 05 del curso: Gestión de Riesgo. [Material del curso en línea]. https://aulavirtual.suscerte.gob.ve/mod/book/view.php?id=4089&chapterid=8103

UNIR. (2020). La mejora continua busca mejorar la calidad y la eficiencia a través de pequeños cambios que implican a todos los procesos y empleados de una compañía.

La mejora continua busca mejorar la calidad y la eficiencia a través de pequeños cambios que implican a todos los procesos y empleados de una compañía. *Revista UNIR*. https://www.unir.net/ingenieria/revista/mejora-continua/

Zuñiga, A.R., Serrano, I.M., y Molina, L.J. (2020). Seguridad de la información en las PYMES de Quevedo. *Journal of Business and Entrepreneurial Studies, 4*(2), 232-241. https://journalbusinesses.com/index.php/revista/article/view/97/221#info