UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TEMA:

Ciberseguridad post Covid-19 y su impacto en las pymes del Ecuador

TRABAJO DE TITULACIÓN EN MODALIDAD DE ARTÍCULO PROFESIONAL DE ALTO NIVEL

PARA LA OBTENCIÓN DEL TITULO DE: MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN

AUTOR

Ing. Gatsby Gabino Bueno Valero

TUTOR

Ing. Lídice Victoria Haz López Msia.

Santa Elena, Ecuador

Año 2022

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
MARJORIE ALEXANDRA CORONEL SUAREZ

ING. MARJORIE CORONEL SUÁREZ, Mgti
COORDINAADORA DEL PROGRAMA

Firmado electrónicamente por:
JAIME BENJAMIN OROZCO IGUASNIA

ING. JAIME OROZCO IGUASNIA, MSc
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
DANIEL IVAN QUIRUMBAY YAGUAL

LSI. DANIEL QUIRUMBAY YAGUAL, MSIA.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
LIDICE VICTORIA

ING. LÍDICE HAZ LÓPEZ, MSIA.
TUTOR

AB. VICTOR CORONEL, MGTR.
SECRETARIO GENERAL
UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por BUENO VALERO GATSBY GABINO, como requerimiento para la obtención del título de Magister en Tecnologías de la Información.

TUTOR

Firmado electrónicamente por:
LIDICE
VICTORIA

Lídice Victoria Haz López

15 días del mes de noviembre del año 2022

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

DECLARACIÓN DE RESPONSABILIDAD

Yo, Bueno Valero Gatsby Gabino

DECLARO QUE:

El trabajo de Titulación, *"Ciberseguridad post Covid-19 y su impacto en las pymes del Ecuador"* previo a la obtención del título en Magister en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, a los 15 días del mes de noviembre del año 2022

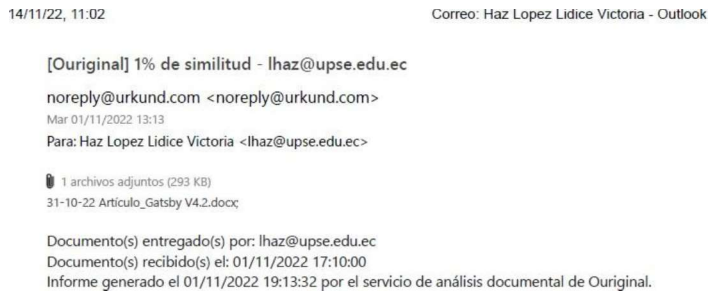
EL AUTOR

Bueno Valero Gatsby Gabino

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado *"Ciberseguridad post Covid-19 y su impacto en las pymes del Ecuador"*, presentado por el estudiante, Bueno Valero Gatsby Gabino fue enviado al Sistema Antiplagio URKUND, presentando un porcentaje de similitud correspondiente al 1%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.



14/11/22, 11:02 Correo: Haz Lopez Lidice Victoria - Outlook

[Ouriginal] 1% de similitud - lhaz@upse.edu.ec

noreply@urkund.com <noreply@urkund.com>
Mar 01/11/2022 13:13
Para: Haz Lopez Lidice Victoria <lhaz@upse.edu.ec>

1 archivos adjuntos (293 KB)
31-10-22 Artículo_Gatsby V4.2.docx;

Documento(s) entregado(s) por: lhaz@upse.edu.ec
Documento(s) recibido(s) el: 01/11/2022 17:10:00
Informe generado el 01/11/2022 19:13:32 por el servicio de análisis documental de Ouriginal.

TUTOR

Firmado electrónicamente por:
LIDICE
VICTORIA

Lídice Victoria Haz López

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

AUTORIZACIÓN

Yo, Bueno Valero Gatsby Gabino

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de artículo profesional de alto nivel con fines de difusión pública, además apruebo la reproducción de este artículo académico dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, a los 15 días del mes de noviembre del año 2022

EL AUTOR

Bueno Valero Gatsby Gabino

Ciberseguridad post Covid-19 y su impacto en las pymes del Ecuador

Cybersecurity post Covid-19 and its impact on pymes in Ecuador

Gatsby Bueno[1]
Universidad Estatal Península de Santa Elena, Ecuador
gatsby1303@hotmail.com
ORCID 0000-0001-6969-1987

Lídice Haz [2]
Universidad Estatal Península de Santa Elena, Ecuador
lhaz@upse.edu.ec
ORCID 0000-0003-1291-1875

RESUMEN

La digitalización de las empresas es una estrategia de negocios que promueve la innovación y mejoramiento de los servicios e incrementa su competitividad en el mercado. La pandemia del Covid-19 sin duda alguna ha marcado un antes y un después destacando la urgencia de la tecnificación de los negocios con el fin de diseñar y aplicar estrategias de ciberseguridad. Es por ello, que las empresas necesitan asegurar el correcto funcionamiento de la infraestructura tecnológica mediante la implementación de mecanismos de ciberseguridad que permitan diagnosticar los posibles errores o fallas técnicas y administrativas sobre los sistemas y la información. Este trabajo describe cómo las pymes perciben y administran la ciberseguridad en el contexto de la post-pandemia Covid-19. Para esto, se realizó una investigación bibliográfica de tipo cualitativa, y la aplicación de una encuesta dirigida a representantes de pymes ecuatorianas. El objetivo fue identificar el interés de las empresas por implementar mecanismos de ciberseguridad en sus sistemas de cómputo en la post-pandemia. En general, los resultados permitieron identificar las debilidades de los recursos tecnológicos con mayor exposición a riesgos y amenazas por falta de conocimiento, errores u omisiones en el manejo de la ciberseguridad. Finalmente, se describe un conjunto de buenas prácticas de ciberseguridad basado en normas internacionales ISO 27001 y COBIT 5.0 referidos a la seguridad de la información y seguridad informática. Estas prácticas incluyen controles de mitigación para contrarrestar los efectos de los riesgos que afectan a la integridad, disponibilidad y confidencialidad de información.

PALABRAS CLAVE
Ciberseguridad, Pymes, Postpandemia, Covid-19, Activos de información.

[1] Ingeniero en Networking y Telecomunicaciones
[2] Ingeniera en Sistemas Computacionales, Máster en Seguridad Informática

ABSTRACT
The digitization of companies is a business strategy that promotes innovation and improvement of services, increasing their competitiveness. The Covid-19 pandemic has undoubtedly marked a before and after, highlighting the urgency of the modernization of business in order to design and apply cybersecurity strategies. That is why companies need to ensure the proper functioning of the technological infrastructure by implementing cybersecurity mechanisms that allow possible errors or administrative and technical failures on systems and information to be diagnosed. This work describe how PYMES perceive and manage cybersecurity in the context of the post-Covid-19 pandemic. For this, a qualitative bibliographical research was carried out, and the application of a survey addressed to representatives of Ecuadorian PYMES. The objective was to identify the interest of companies in implementing cybersecurity mechanisms in their computer systems after the post-pandemic. In general, the results made it possible to identify the weaknesses of the technological resources with greater exposure to risks and threats due to lack of knowledge, errors or omissions in the management of cybersecurity. Finally, a set of good cybersecurity practices based on international standards ISO 27001 and COBIT 5.0 referring to information security and computer security is described. These practices include mitigating controls to counteract the effects of risks that affect the integrity, availability and confidentiality of information.

KEYWORDS
Cybersecurity, PYMES, Post-pandemic, Covid-19, Information assets.

INTRODUCCIÓN

En la actualidad, las empresas enfrentan nuevos desafíos para incrementar sus negocios y ser competitivos. Los sistemas de información y comunicación son parte fundamental para el funcionamiento de los procesos del negocio. Es así, que se encuentran integrados como soporte para el desarrollo de las actividades productivas que generan valor a una empresa u organización. La implementación de tecnología es una estrategia necesaria dado que apoyan la toma de decisiones (Buenrostro & Hernández, 2019).

El servicio de procesamiento de la información soporta la ejecución de los diferentes procesos que se encuentran automatizados para cada una de las áreas del negocio. El uso ininterrumpido de los sistemas de información y comunicación aumentan la eficacia y eficiencia de las organizaciones, facilitando la dirección y control de los procesos del negocio a través de la entrega oportuna de la información en forma y tiempo adecuados permitiendo que la gerencia cumpla con sus responsabilidades y objetivos (Pabón, 2018).

En este sentido, las empresas buscan la integración de tecnología digital en todas las áreas del negocio. Lo cual fomenta la transformación digital en las pymes. Esto sugiere un cambio en la forma en que operan y brindan valor a sus clientes. Lograr la transformación digital brinda acceso a nuevas oportunidades de negocio, llegando a nuevos mercados y permitiendo mantenerse actualizado con aquello que ocurre fuera de su entorno (Sánchez et al. (2019); (Herencia, 2022).

Sin embargo, la transformación digital conlleva a la materialización de riesgos cibernéticos por amenazas externas o internas que pueden afectar a la seguridad de la información (Herencia, 2022). En este sentido, la ciberseguridad y la implementación de buenas prácticas de seguridad informática son una estrategia que juega un papel muy importante para hacerle frente a los ciber-riesgos (Rosa Pineño, 2019).

El sitio Hackmageddon, (2022) señala que los ciberataques en las empresas y en los gobiernos durante el año 2019 ascendieron a 1.802 eventos que comprometieron la seguridad de los sistemas e infraestructuras de cómputo de diferentes países. Según el estudio realizado por Aguilar, (2021) señala que 298 casos de ciberataques estuvo direccionados a organizaciones gubernamentales incitando ciberguerra, hacktivismo o ciberespionaje. Las vulnerabilidades que fueron explotadas afectaron la continuidad de los procesos a nivel de base de datos, información de los sistemas informáticos y tecnologías de operación de los gobiernos.

En este contexto, la pandemia del COVID-19 también aceleró la digitalización y virtualización de los procesos económicos y sociales. Esto como respuesta a las cuarentenas forzadas. Lo principal era evitar la desaceleración productiva y la posible interrupción total del sistema económico y financiero (Salazar, 2021). De acuerdo con la Comisión Económica para América Latina y el Caribe (CEPAL), las empresas más avanzadas en transformación digital tuvieron mayor capacidad de respuesta a los retos generados por durante y después de la pandemia COVID-19 y, por tanto, poseen mayor ventaja frente a aquellas que no han iniciado su proceso transformador en el uso de las TIC's y la gestión de la ciberseguridad (Reyes et al. (2020); (Alonso, 2017).

Por lo antes descrito, se describe un conjunto de buenas prácticas de ciberseguridad basado en normas internacionales ISO 27001 y COBIT 5.0 referidos a la seguridad de la información y seguridad informática. Estas prácticas incluyen técnicas y controles de

mitigación para contrarrestar los efectos de los riesgos que afectan a la integridad, disponibilidad y confidencialidad de la información.

TRANSFORMACIÓN DIGITAL DE LAS PYMES POST-COVID 19

Previo a la pandemia las pymes de todos los sectores económicos ya se encontraban implementando tecnología para la automatización de sus procesos y servicios, creando retos y oportunidades. La pandemia de COVID-19 ha creado una mayor transformación digital en todas las empresas, creando nuevas oportunidades, pero también potenciando amenazas.

La necesidad del distanciamiento social y laboral contribuyó a la adquisición de plataformas digitales y herramientas tecnológicas para que las empresas funcionen sin inconveniente durante la pandemia (Battisti et al., 2022). Por consiguiente, las pequeñas y medianas empresas (PYME) tuvieron que adaptarse a la era digital (Ragazou et al., 2022). El teletrabajo fue el mecanismo implementado para mantener la continuidad de los procesos; de tal manera que muchos trabajadores y empleados aprendieron a trabajar bajo esta modalidad, a usar la comunicación digital y las herramientas de colaboración.

De esta manera, las pymes se enfocaron en la transformación digital de sus modelos de negocios (Khurana et al., 2022). Convirtiendo esta tendencia inevitable en una fuerza que promueve el desarrollo sostenible de las empresas. Yang et al. (2021) mencionan que las pymes al realizar estos cambios tecnológicos están modificando su forma de operar. Lo que, promueve una marcada tendencia económica, comercial y financiera que ofrece nuevas posibilidades tecnológicas y oportunidades en el entorno empresarial.

Por lo tanto, la transformación digital es la forma en que las empresas integran nuevas tecnologías en todas las áreas. Promueve la innovación en el modelo comercial creando valor para los clientes. Esta transformación afecta a los procesos comerciales, las rutinas operativas y las capacidades organizativas de una empresa. Esto con la finalidad de optimizar los procesos, mejorando su competitividad y eficiencia (Stich et al., 2020).

Además, la transformación digital, también denominada “digitalización”, se refiere a la integración de las tecnologías que contribuyen a la creación de nuevas aplicaciones y sistemas que redundan en la mejora del nivel de competitividad y eficiencia de las empresas (Chatterjee et al., 2022; Hulla et al., 2021).

La transformación digital en el desarrollo empresarial está encaminado a optimizar sus métodos y facilitar las gestiones entre proveedores y clientes. Los resultados de la inversión en la innovación digital se reflejarán en las utilidades, el crecimiento en el mercado y en las ventajas competitivas. Los sistemas digitales como los ERP, las aplicaciones como CAM, CAD, y FMS, la inteligencia artificial, la sistematización en la nube, blockchain, Big Data, los desarrollo de IoT y las plataformas como EDI, la innovación abierta y el e-commerce permiten optimizar la capacidad para responder a los desafíos del mercado.

Sin embargo, las pymes se enfrentan a diversos retos para lograr esta transformación. Las pocas competencias digitales de sus empleados y propietarios, el desconocimiento de los beneficios de la digitalización, la resistencia al cambio, la falta de recurso para invertir, el grado de tecnificación del negocio, y los riesgos y amenazas cibernéticas. Todo esto, genera barreras para la evolución de las empresas y, en consecuencia, menos de la mitad de las pymes han iniciado su proceso de transformación digital, especialmente en países en desarrollo (Rojas & Bustos, 2021).

La pandemia ha tenido una combinación de impactos negativos, entre los que se destaca la automatización de los procesos y la seguridad de la información que afectan la continuidad del negocio. Para algunos sectores, la presencia física sigue siendo necesaria,

por ejemplo, en las industrias del servicio de salud, la construcción, la logística y la seguridad. Para el resto de las industrias la tecnología brinda soluciones adecuadas que pueden ser desarrolladas totalmente en la virtualidad (Xie et al., 2022).

Es por ello, que la globalización digital se incrementa en las actividades de los gobiernos, empresas, usuarios, que se convierten en blancos más atractivos para los criminales cibernéticos. Estos ciberdelincuentes aprovechan la web para mantenerse en el anonimato mientras realizan sus ataques. Es por ello que las empresas han incrementado la inversión en ciberseguridad para minimizar las probabilidades de ser víctimas de los ciberataques. Hay que tener en cuenta que los crackers consiguen la manera de burlar las medidas de seguridad para lograr acceder a información confidencial de los usuarios y con ello obtener un beneficio económico.

Gamboa, (2020) en su artículo de la Importancia de la Seguridad Informática y Ciberseguridad en el Mundo actual indica que las amenazas más devastadoras para la economía empresarial y de los usuarios durante el 2019 fueron los spams (engaños), compromiso de cuentas de email corporativas (BEC) y el fraude con argumento sentimental, representando el 47% de los delitos totales y el 65% de las pérdidas económicas, siendo el sector más vulnerable a los ataques digitales los adultos mayores a 50 años, quienes representaron el 42% de las victimas totales y el 49% de las pérdidas generadas durante el año pasado. El país con mayor porcentaje de ataques durante el 2019 fue Estados Unidos con 76,2% del total de reportes, seguido del Reino Unido con el 20,1% de los casos registrados. La inversión en ciberseguridad ha mostrado un incremento del 46,8% en los últimos 5 años hasta alcanzar la cifra de 106.600 millones de dólares durante el 2019.

En este sentido, para lograr una transformación digital favorable es necesario definir los factores básicos que influyen en la aceleración digital. A continuación, acorde con la literatura sobre el tema se presenta una lista corta de factores básicos o impulsores, que sirve de marco conceptual para evaluar los retos y oportunidades.

- Definición de políticas estratégicas para la transformación digital, con un marco institucional y de gobernanza apropiados para su coordinación y ejecución.
- Mejoramiento de la calidad de la infraestructura digital y el acceso a la conectividad.
- Desarrollo de competencias digitales en el recurso humano.
- Creación de marcos legales y regulatorios en temas como ciberseguridad, protección de datos y privacidad, y en materia de normas para la compra y venta de equipos tecnológicos.
- Creación de políticas de transformación digital sectoriales, en sectores clave tales como gobierno digital, salud, sector ambiental, sector académico y financiero.
- Generar alianzas estratégicas y de cooperación internacional.

Estos factores promueven la transformación digital. Entre más alineados e integrados estén todos estos elementos en un país, de manera que se refuercen mutuamente, más amistoso y favorable será el ambiente para propiciar la aceleración digital.

PERSPECTIVA DE LA CIBERSEGURIDAD EN LAS PYMES POST-COVID 19

La crisis sanitaria del Covid-19 afectó a todo el mundo, ocasionando que las personas se replantearan su estilo de vida. El distanciamiento social impuesto a la población generó diversos cambios en la forma de adquirir productos y servicios. El internet es el medio por el cual las empresas y las personas se relacionan en ámbitos comerciales, académicos y personales. Esto debido, a que el uso de las plataformas de comunicación contribuye con

el crecimiento y la transformación digital de las empresas; además de, aprovechar las ventajas de su facilidad de uso y acceso.

En este contexto, el desarrollo tecnológico y la tecno-dependencia de las pymes comprometen a los activos de información ante amenazas no deseadas. El estudio de (Marek, 2022) sugiere que la industria 4.0 y la pandemia han provocado cambios en el desarrollo tecnológico e innovación, situaciones económicas y restricciones en varias empresas y regiones en el mundo. Además, las pequeñas y medianas empresas (pymes) son inmaduras y más vulnerables en términos de riesgo de ciberseguridad y resiliencia. Es por ello, que la organización para la cooperación y el Desarrollo Económico (OCDE) y el Banco de Desarrollo de América Latina (CAF) (OCDE/CAF, 2019) señalaron que Las pymes de Argentina, Brasil, Colombia, Ecuador, México, Uruguay y Venezuela, generaron la cuarta parte de la producción total de la región, esto representa 99.5% de las empresas, siendo las microempresas la de mayor presencia en todos los sectores de la economía, sobre todo en el comercio, donde alcanza 92% de participación, y en otras actividades comunitarias, sociales y personales donde participa con 95%. Más del 60% del empleo formal dependen de las pymes. En general, las pymes a nivel mundial son consideradas el 90% de la economía empresarial global.

En consecuencia, las pymes deben tener la capacidad de detectar, responder y recuperarse de los ataques cibernéticos. Sin embargo, las pymes carecen de información de cómo actuar en caso de tener una amenaza digital. Es posible, que no cuenten con estrategias adecuadas de seguridad cibernética porque invierten menos en infraestructura de ciberseguridad. Esta situación, se ve reflejada en los altos índices de afectación en América Latina respecto a la gestión de la ciberseguridad. La Figura 1, muestra los porcentajes de ataques cibernéticos más frecuentes durante el 2020 y 2021, este último con un incremento del 4% respecto al año 2020. Además, de acuerdo con el Índice de Inteligencia de Amenazas X-Force de IBM Security, los países más ciber atacados en la región fueron Brasil, México y Perú. En general, el ataque más empleado por los ciberdelincuentes es el ransomware, que es el secuestro de datos a través de un tipo de software malicioso que no permite el acceso a los archivos del sistema operativo infectado, y en el que se exige una recompensa a cambio de devolver tal información.

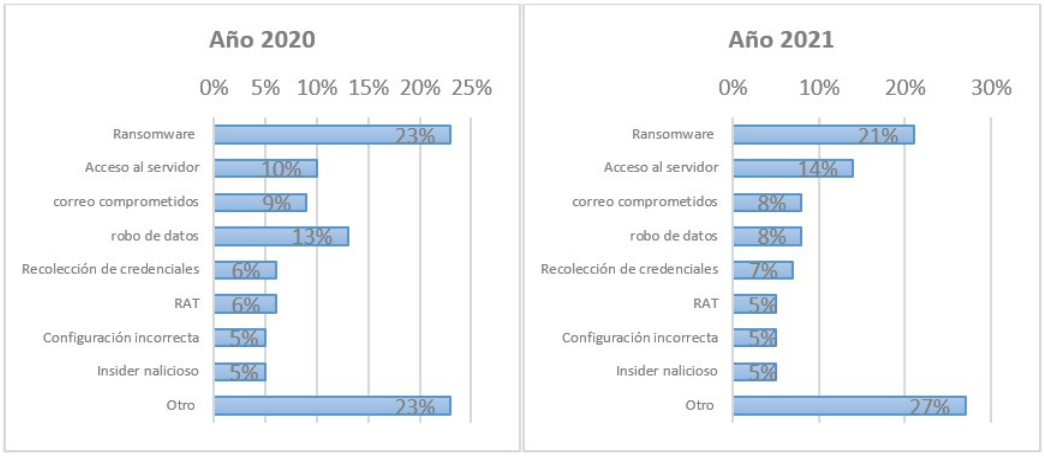


Figura 1. Ciberataques más frecuentes en América Latina 2020 vs 2021
Fuente: Índice de Inteligencia de Amenazas X-Force de IBM Security

En Ecuador, de acuerdo con las denuncias presentadas en la Fiscalía, en los años previos a la pandemia de COVID-19 se registraron diversas denuncias de delitos informáticos. En la Figura 2 se muestran las estadísticas de los delitos informáticos siendo el año 2019 el que tiene mayor número de delitos. Esto sugiere, que las infraestructuras tecnológicas y

los usuarios finales se vuelven blanco fácil de los ciberdelincuentes, y con ello la materialización de las amenazas exponiendo la seguridad y privacidad de la información.

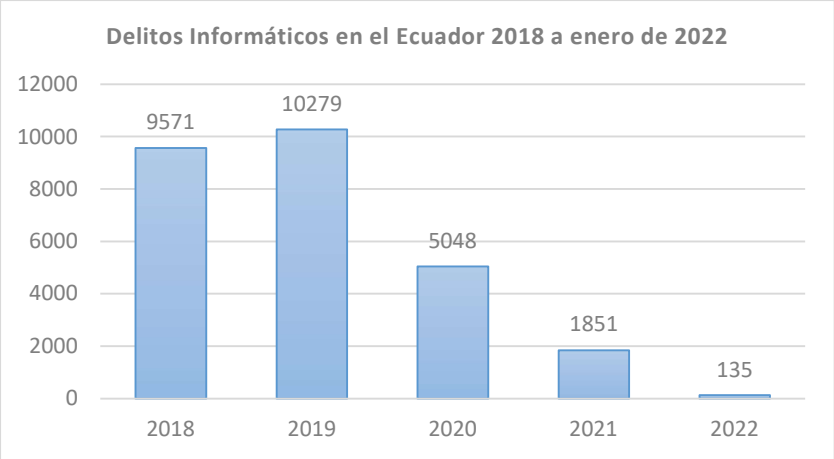


Figura 2. Delitos informáticos en el Ecuador 2018 a enero 2022
Fuente: DAI-CIBERPOL

En la Tabla 1, se muestran las denuncias registradas en la Fiscalía (FGE, 2022) según el tipo de delito cometido. Los delitos con mayor frecuencia son la suplantación de identidad con 2162 denuncias, seguido de la falsificación de documentos con 1448 denuncias, y la apropiación fraudulenta a través de medios electrónicos con 1033 denuncias. Entre otros delitos que afectan a la integridad, seguridad y disponibilidad de los sistemas informáticos de las empresas y organizaciones. Las estadísticas globales de ciberseguridad demuestran que existe un mayor índice de cometimiento de delitos; sin embargo, de forma local en Ecuador, muchas veces por desconocimiento o por evitar una mala imagen, estos delitos no se denuncian ante las autoridades; lo que, implica una falsa expectativa del manejo de la ciberseguridad.

Tabla 1. Tipos de delitos informáticos en Ecuador (FGE, 2022)

Delitos	**Frecuencia Absoluta**	**Frecuencia Relativa**
Suplantación de identidad	2162	43%
Falsificación y uso de documento falso	1448	29%
Apropiación fraudulenta por medios electrónicos	1033	20%
Acceso no concedido a un sistema informático, telemático o de telecomunicaciones	175	3%
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	85	2%
Ataques a la integridad de sistemas informáticos	51	1%
Intercepción ilegal de datos	45	1%
Transferencia electrónica de activos patrimonial	31	1%
Revelación ilegal de base de datos.	18	0%
Total	**5048**	**100%**

Las pymes se enfrentan a tres principales desafíos, a decir, (i) no tener la experiencia interna para mitigar el riesgo cibernético; (ii) restricciones presupuestarias de TI; y (iii) una falta general de comprensión de cómo protegerse contra los ataques cibernéticos (Keeper, 2018). En un estudio reciente, se encontró que los principales desafíos eran la

falta de fondos para pagar el talento, los problemas con el cumplimiento normativo y legal, y la escasez de talento disponible profesionalmente (Asti, 2017).

Asimismo, las pymes que participaron en la encuesta realizada por ESET Security Report (2021) para Latinoamérica respecto con los ataques cibernéticos; en la Figura 3, se muestra que el 60% mantiene la principal preocupación en el acceso indebido a la información, el 39% no cuenta con normativas de seguridad, y un 28% no clasifica su información. Lo que sugiere, que no existen claros controles respecto al manejo eficiente de la ciberseguridad; aun cuando ésta es considerada un factor fundamental para la protección de la infraestructura de T.I.; que, además, sirve como control de índole tecnológico en combinación e integración con controles administrativos, físicos y técnicos de la organización.

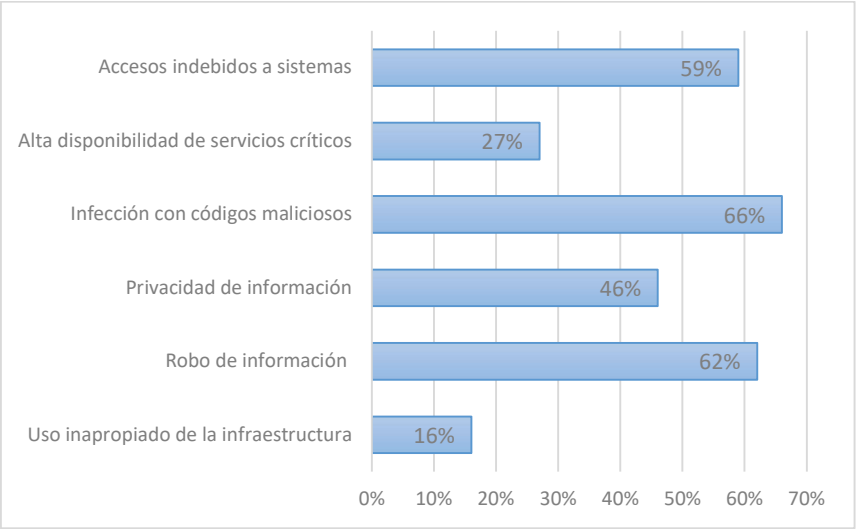


Figura 3. Principales preocupaciones de las empresas de América Latina en ciberseguridad
Fuente: ESET Security Report (2021)

En este contexto, las pymes tienen la ventaja potencial de ser pequeñas con arreglos de T.I. más flexibles. Esto, permite una mejor gestión de los desafíos que enfrentan a nivel técnico, humano, organizacional, financiero y legal. La inversión que las empresas realizan permite mejorar sus sistemas de software, hardware y servicios de seguridad, para incrementar la prevención de ser víctima de ciberataques (Piñedo, 2019). También las capacitaciones dirigidas a usuarios sobre el buen uso de las contraseñas y de las plataformas empresariales, bancarias, públicas, etc., ayudarán a prevenir la materialización de las ciberamenazas y evitar una afectación en la disponibilidad, integridad y confidencialidad de la información almacenada en los sistemas de cómputo; es decir, garantizar la ciberseguridad (CISA, 2022).

Por consiguiente, para fortalecer la cultura de ciberseguridad, se requiere principalmente que las pymes actualicen los conocimientos de seguridad informática de los empleados. Esto debido a que no cuentan con conocimientos adecuados para utilizar sus dispositivos digitales, lo que, facilita que los ciberdelincuentes tengan espacios abiertos para explotar cualquier dominio o dispositivo (Check Poinit, 2022). Estudios sugieren el desarrollo de campañas de concienciación o series de capacitaciones sobre técnicas y mecanismos de seguridad informática dirigida a los empleados y usuarios en general; ya que, son considerados el “eslabón más débil” en la cadena de ciberseguridad (Maggi & Gómez, 2021).

De la misma manera que se gestiona el conocimiento humano de la ciberseguridad; también es necesario gestionar el riesgo tecnológico. La gestión del riesgo de T.I., permite mantener una estrategia de protección y de mitigación de amenazas que asegure el mejoramiento continuo de la seguridad de la información. Los procesos críticos del negocio se soportan con el uso de la tecnología. La importancia de implementar un correcto análisis de riesgo mediante un proceso interactivo de cambios que se enmarquen en la mejora continua de las organizaciones permitirá salvaguardar la seguridad de la información (Vanegas et al., (2014). Gestionar el riesgo de T.I. permite que los empresarios pueden planear migraciones tecnológicas, detectar cuellos de botellas, analizar, evaluar y monitorear las amenazas más latentes que puedan afectar la continuidad del negocio y evitar pérdidas. Por lo tanto, los ejecutivos de las organizaciones deben priorizar las capacidades operativas en ciberseguridad y resiliencia de T.I. para impulsar los negocios en las diferentes industrias.

MÉTODOLOGÍA

Dado que se trata de evaluar cómo las empresas manejan y perciben la ciberseguridad en el contexto de la post-pandemia Covid 19; se recurrió a una investigación documental explicativa para identificar los factores claves que permitan asegurar los activos de información, en función del objetivo establecido para este estudio.

Este trabajo se realiza bajo el planteamiento del enfoque cualitativo y descriptivo, el cual se ajusta con el proceso de recolección de información cualitativa y fiable para realizar el análisis de la información obtenida.

La población de estudio está conformada por 131 representantes de pymes en el sector comercial de la ciudad de Guayaquil. Para la selección de la muestra se utilizó un muestreo no probabilístico por bola de nieve.

La técnica que se aplicó para la recolección de los datos es la encuesta mediante el diseño de un cuestionario de preguntas cerradas orientadas a obtener respuestas dicotómicas y de selección múltiple que permiten evaluar el contexto en el que las pymes gestionan la ciberseguridad.

Para el procesamiento de datos se utiliza la estadística descriptiva, mediante la elaboración de tablas y gráficos que facilitan el análisis y la interpretación de los resultados.

RESULTADOS

En esta sección, se informa y discute la información obtenida mediante la aplicación de la encuesta a los representantes de las pymes ecuatorianas. Se ha evaluado los criterios de seguridad lógica y física que aplican las empresas en sus sistemas de cómputo luego de la post-pandemia.

La población objeto de estudio está conformada por 83 hombres y 48 mujeres; en edades entre 20 y 60 años, siendo los rangos más altos entre 30 y 39 años, lo que representa el 50%; seguido del 41% en el rango de edades entre 40 y 49 años; y por último el 9% que corresponde al rango entre 20 y 29 años.

En la Figura 4, se muestra el nivel de importancia que tienen las pymes por conocer el nivel técnico de sus empleados respecto a la ciberseguridad. El 97% de los encuestados están de acuerdo y afirman que es necesario evaluar y conocer el nivel de dominio técnico que tienen los empleados respecto a la ciberseguridad. Esta información, es relevante debido a que existen muchas amenazas digitales que pueden interrumpir los procesos del

sistema computacional de las empresas; siendo la principal puerta de entrada para los cibercriminales los empleados, los mismos que son considerados el eslabón más débil de la cadena en cuanto a concienciación en ciberseguridad.

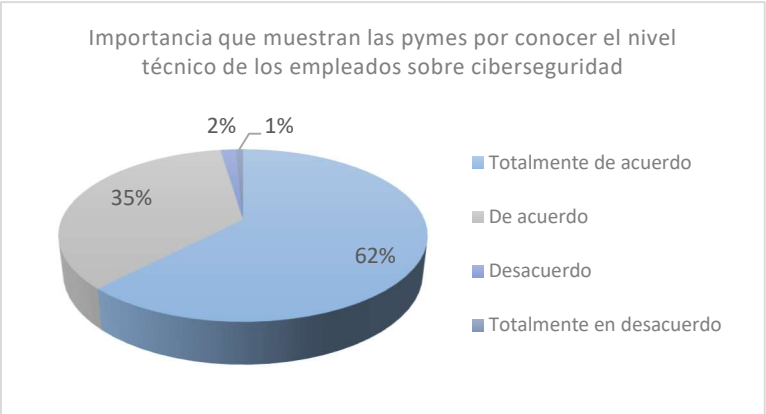


Figura 4. Importancia que muestran las pymes por conocer el nivel técnico de los empleados sobre ciberseguridad
Fuente: Elaboración propia

En la Figura 5, se muestra el nivel de identificación que pueden tener las pymes con respecto a la gestión de las amenazas cibernéticas y los procesos de mitigación para estas amenazas en su infraestructura tecnológica. El 76% menciona que tiene un nivel medio-alto en la identificación de amenazas cibernéticas. El 21% tiene un nivel bajo, y el 3% no posee ningún nivel de gestión. Las estadísticas de ciberataques diariamente se incrementan, lo que, amenaza la ciberseguridad de la empresa. Por ello, la importancia de gestionar las amenazas y los riesgos cibernéticos para evitar ser víctima de delitos informáticos que puede tener consecuencias perjudiciales, tales como, pérdidas financieras y de reputación.

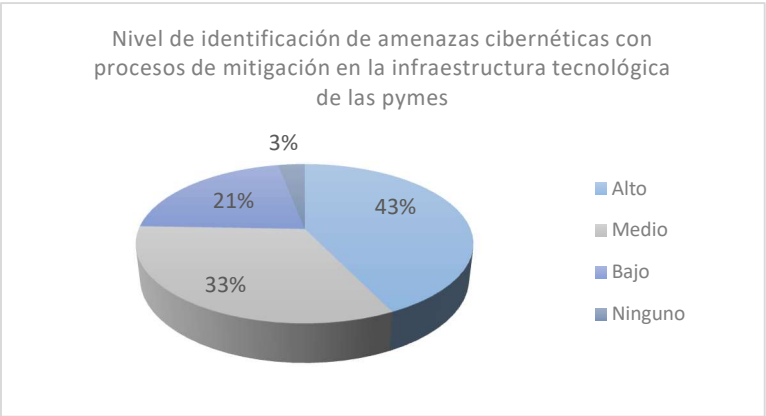


Figura 5. Nivel de identificación de amenazas cibernéticas con procesos de mitigación en la infraestructura tecnológica de las pymes
Fuente: Elaboración propia

En la Figura 6, se muestra el interés que tienen las pymes por la implementación de mecanismos de seguridad informática y de seguridad de la información, a través del uso de protocolos seguros, herramientas informáticas y actividades de gestión estratégica de ciberseguridad que permitan proteger el hardware, el software y los datos de las pymes. El 99% de los encuestados muestran interés y están de acuerdo con la importancia de implementar mecanismos de ciberseguridad. La transformación digital de las empresas, y en general, el crecimiento global de las redes y la información, impulsan el desarrollo

e innovación tecnológica de la sociedad. Esta realidad, impone la necesidad de gestionar los riesgos cibernéticos mediante la implementación de estrategias a nivel gerencial y a nivel operativo mediante herramientas de seguridad informática y de seguridad de la información.

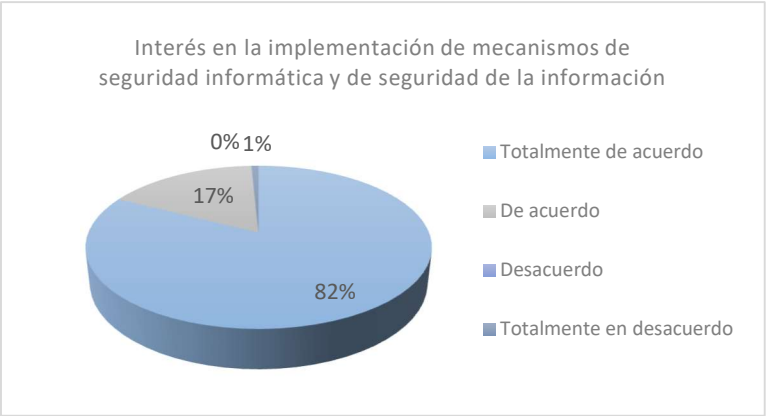


Figura 6. Interés en la implementación de mecanismos de seguridad informática y de seguridad de la información
Fuente: Elaboración propia

En la Figura 7, se muestra el interés que tienen las pymes por el uso e implementación de una guía de buenas prácticas de ciberseguridad basada en normas internacionales ISO 27000 y COBIT 5.0. El 98% de los encuestados están de acuerdo con implementar la guía de buenas prácticas de ciberseguridad. Los ataques cibernéticos afectan el normal desarrollo de las actividades del negocio comprometiendo la confidencialidad, integridad y disponibilidad de la información. Por ello, es imprescindible que las pymes sean proactivas en la gestión e implementación de controles de seguridad informática; con el fin de mitigar y contrarrestar los efectos negativos que puedan ocasionar los riesgos cibernéticos.

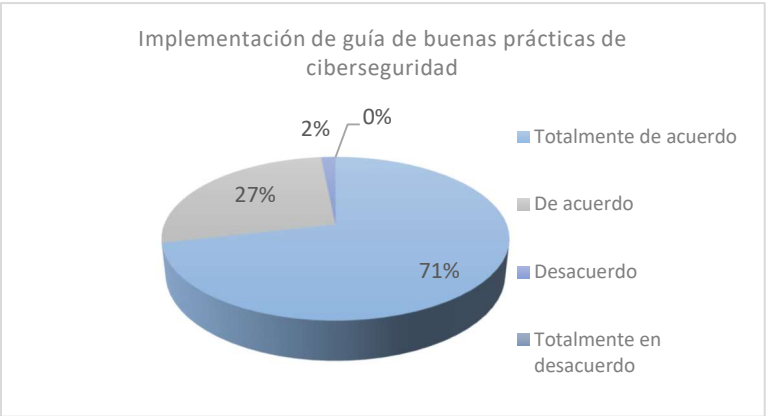


Figura 7. Implementación de guía de buenas prácticas de ciberseguridad
Fuente: Elaboración propia

Los datos recopilados en esta investigación evidenciaron que las pymes muestran preocupación por el mal uso y acceso que puedan hacer usuarios no autorizados con su activo más preciado, que es la información y los datos empresariales internos. Las principales dificultades que se han encontrado es el poco conocimiento que pueden tener sus empleados respecto al manejo de la ciberseguridad. Este panorama demuestra que las empresas fallan en lo básico; y que en realidad no cuentan con suficientes controles de seguridad ni mecanismos de defensa en términos de herramientas de seguridad

informática. Esto sugiere que las pymes busquen asesoría por métodos de seguridad para implantarlos en sus sistemas e infraestructuras de cómputo.

Desde el nivel estratégico, las pymes deben conocer cuáles son sus riesgos cibernéticos y como gestionarlos de forma adecuada; y con ello, minimizar el impacto que pueda generar en el negocio, en caso de que el riesgo se materialice. En el nivel operativo, las pymes deben gestionar la implementación de soluciones tecnológicas de ciberseguridad acorde con las tendencias actuales y con las necesidades del negocio.

Los encuestados consideran importante la creación de una guía de buenas prácticas de ciberseguridad que permita minimizar los riesgos que puedan afectar la confidencialidad, la integridad y la disponibilidad de la información, y que asegure la continuidad y rápida recuperación del negocio ante un incidente o ataque cibernético.

PRACTICAS DE CIBERSEGURIDAD PARA ASEGURAR LOS ACTIVOS DE INFORMACIÓN EN LAS PYMES

La seguridad de la información es un factor primordial que se debe manejar en los entornos empresariales y personales. La diversificación y uso de las tecnologías en distintas actividades ha generado un incremento en los ataques y amenazas cibernéticas (Miamó, 2019). En este contexto, las pequeñas y medianas empresas (pymes) mantienen una política reactiva frente a los incidentes de seguridad; es decir, deciden aplicar medidas de ciberseguridad luego de sufrir un ciberataque. Este accionar, en muchas ocasiones solo se limita en aplicar medidas para contrarrestar el ataque ejecutado; es decir, no se realiza un análisis exhaustivo de las distintas amenazas que existen en el ciberespacio, y que puedan suponer un riesgo para la organización (López Fernández, 2019).

En este sentido, es necesario asegurar los activos de información con mecanismos de ciberseguridad que permita minimizar la materialización de los riesgos que puedan afectarlos. Los activos de información son datos relacionados con la actividad de la empresa (Mintic, 2022). Entiéndase, activo de información como todo aquello que tiene valor, y que forma parte de los procesos core de las organizaciones; y por tanto, es necesario identificar, clasificar y analizar el nivel de tolerancia al riesgo; además de evaluar los controles existentes y futuros que permitan asegurar su disponibilidad, integridad y confidencialidad. Los activos de información son indispensables porque ayudan a la empresa a desarrollar sus operaciones y cumplir con los objetivos estratégicos. Para lo que, es necesario mantener un inventario actualizado de los activos identificando su tipo, proceso core que soporta, para posteriormente evaluar las amenazas y los riesgos que los pueden afectar. En la Tabla 2, se muestra una clasificación general de los activos de información con un ejemplo del activo.

Tabla 2. Activos de información

Tipos de activos de información	Activo de información
Física	Centro de cómputo Armarios Oficinas
Red/Telecomunicaciones	Hardware de T.I. Estaciones de trabajo Enlaces de datos Equipos de red Servidores físicos Portátiles
Plataformas	Sistemas operativos

Base de datos	Copias de seguridad Claves
Aplicaciones	Softwares Servicios informáticos
Información/Documentos	Correos electrónicos Pólizas Manuales Contratos
Personas	Empleados Subcontratados Externos

Para garantizar la integridad, la disponibilidad y la confidencialidad de los activos de información, es necesario implementar controles principalmente a aquellos activos con mayor criticidad y exposición a riesgos. Esto, sugiere diseñar y aplicar estrategias de seguridad de la información, herramientas y mecanismos de seguridad informática.

Es necesario que las pymes aprendan a gestionar y valorar los controles de ciberseguridad. Entendiendo que, la seguridad de la información se enfoca en el análisis y evaluación de riesgos y amenazas, implementando un plan de acción para minimizar la probabilidad de ocurrencia e impacto de dichos riesgos sobre los activos de información. El fin, es proteger la información de una organización, independientemente del lugar donde se almacene; por ejemplo, documentos físicos, discos duros, file de documentos, o incluso en la memoria de las personas que lo conocen.

La seguridad informática, tiene por objetivo evaluar y administrar las implementaciones tecnológicas para proteger la información mediante el uso de tecnologías como, software antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que articulados con prácticas de gobierno de tecnología de información, establecen la forma de accionar y asegurar las situaciones de fallas parciales o totales, cuando el activo se encuentra en riesgo.

La Figura 8, describe el nivel de gestión que tiene la seguridad de la información y la seguridad informática. Esta grafica resume que la seguridad de la información evalúa desde un nivel gerencial estratégico los diferentes riesgos a los cuales está expuesta la empresa y cómo gestionarlos para minimizar su materialización e impacto; mientras que, la seguridad informática se enfoca en aplicar las técnicas de protección para evitar ataques de agentes externos e internos.

Figura 8. Seguridad de la información vs. Seguridad informática
Fuente: Elaboración propia

En consecuencia, los activos de información requieren de la implementación de controles que garanticen la seguridad y privacidad de estos activos, y de la información. A continuación, se describen controles claves de ciberseguridad sugeridos en la norma ISO 27001, la cual provee un enfoque de trabajo para los sistemas de gestión de seguridad de la información (SGSI) con el fin de proporcionar confidencialidad, integridad y disponibilidad continua de la información, así como el cumplimiento legal; y en el marco de trabajo COBIT 5.0 para el gobierno y la gestión de las tecnologías de la información (TI) empresariales (Ilixum, 2022).

En la figura 9, se resumen los factores claves que deberían gestionar las pymes desde un nivel gerencial, estratégico y operativo. Estos factores, deben considerarse para el diseño e implementación de controles que garanticen la seguridad de los activos de información.

Ciberseguridad para pymes	
Nivel Gerencial/Estratégico	**Nivel Operativo**
•Cumplimiento legal •Políticas de seguridad de la información •Gestión de Riesgos T.I. •Planes de contingencia y continuidad del negocio	•Implantación de soluciones de seguridad informática •Seguridad en la nube •Formación y concienciación •Ejecución de auditoría técnica

Figura 9. Factores de ciberseguridad y privacidad para pymes
Fuente: Elaboración propia

Controles & buenas prácticas de ciberseguridad para pymes

A continuación, en la Tabla 3, se describen controles y buenas prácticas de ciberseguridad para las pymes. Estas recomendaciones han sido elaboradas con la ayuda de estudios sobre la Ciberseguridad en el Ecuador, una propuesta de organización de los autores Tates & Recalde (2019), en el cual plantean políticas nacionales y estrategias de ciberseguridad para proteger la infraestructura informática. Además, se considera los controles de buenas prácticas definidos en la norma internacional ISO 27001 (Sistema de Gestión de Seguridad de la Información), el marco de trabajo COBIT 5.0, y los resultados de esta investigación.

Tabla 3. Controles de ciberseguridad para pymes

Nivel	Control	Descripción
Gerencial Estratégico	*Implementación de políticas de seguridad de la información en las empresas*	Proceso de autoevaluación que determina el grado de vulnerabilidad que tienen sus plataformas e infraestructuras tecnológicas frente a los delitos informáticos especialmente aquellos basados en ingeniería social.
	Análisis de riesgos de T.I.	Identificar los riesgos de carácter tecnológico a los que está expuesta la empresa. Es decir, ejecutar un proceso de identificación, análisis, evaluación, y respuesta al riesgo mediante la implementación de controles.
	Gobernanza y gestión administrativa de las TIC.	Gestionar las TIC a través de los estatutos, reglamentos, políticas y normativas internas que sean apropiadas para la empresa, y que se enmarquen con la ley de compañía, y las legislaciones respecto a la seguridad y la privacidad de la información.
	Conformación de equipos de respuesta a incidentes.	Conformar equipos con personas que poseen la experiencia y la formación necesaria para actuar frente a incidencias y desastres que pudieran afectar la integridad, confidencialidad y disponibilidad de la información. Estos son los responsables de dar seguimiento al cumplimiento de las políticas y planes de seguridad adoptados por la institución.
	Guía de procedimientos.	Establecer mediante manuales de procedimientos bien definidos, rápidos y eficientes la recuperación de las actividades de una institución en caso de un incidente.
Operativo	*Capacitación.*	Capacitar a todo el personal que hace parte de la organización; es decir, personal administrativo y de servicios, técnicos y gerenciales en programas de ciberseguridad que ayuden a que los usuarios identifiquen los métodos de engaño más practicados por los ciberatacantes.
	Backups	Generar copias de seguridad de la información digital que se encuentra en los equipos de la empresa. Estos backups se deben realizar de forma periódica a través de dispositivos de almacenamiento externos, los cuales deben resguardarse en un lugar diferente al que contiene el origen de los datos.
	Imagen del sistema	Generar una réplica exacta del disco duro de un equipo ya configurado, a partir de instalaciones limpias. Esto con el fin de hacer recuperaciones más rápidas en caso de daño de una computadora.
	Cifrado de particiones.	Realizar cifrado de particiones principalmente en equipos portátiles para hacer ilegible la información contenida en las unidades de almacenamiento.

	Autenticación	Implementar políticas de creación de contraseñas seguras para acceder a las plataformas, sistemas, aplicaciones.
	Actualización periódica de dispositivos.	Todos los dispositivos que hacen parte de la seguridad de la información deben ser evaluados y actualizados periódicamente.
	Software y hardware de seguridad informática.	Implementación de antivirus, UTM, IDS, IPS, Firewall.
	Almacenamiento en la nube	Utilizar servicios de terceros que cuenten con las garantías necesarias para asegurar el almacenamiento externo de la información, aquí se recomienda revisar los SLA del proveedor.

La figura 10, muestra un resumen del modelo propuesto para gestionar la ciberseguridad en una pyme; basado en los controles especificados en la norma ISO 27001 y COBIT 5.0.

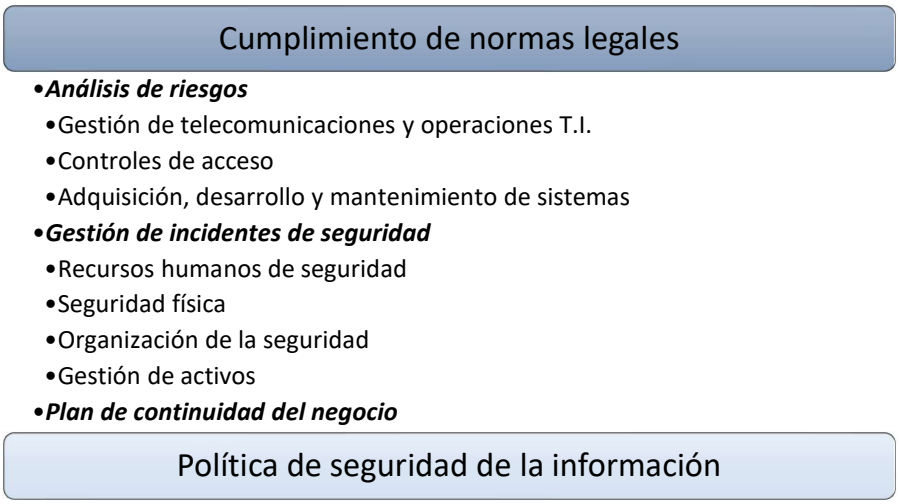


Figura 10. Modelo de gestión de la ciberseguridad para pymes
Fuente: Elaboración propia

CONCLUSIONES

La pandemia Covid -19 aceleró la transformación digital en las pymes ecuatorianas; y como parte de esta transformación la necesidad de implementar ciberseguridad enmarcándose como una estrategia de crecimiento apalancado en la tecnología. Para las empresas asegurar los activos de información es una prioridad; por lo que, es necesario invertir en tecnologías de ciberseguridad e implementar políticas de seguridad de la información para adaptarlas al trabajo remoto.

En tal sentido, las pymes perciben a la Ciberseguridad luego de pandemia Covid-19 como un proceso de mejora continua que ayudará a mitigar los riesgos cibernéticos. Las pymes consideran importante invertir en herramientas de ciberseguridad. Además, es necesario implementar herramientas de seguridad informática y estrategias de seguridad de la información enmarcadas en normas internacionales ISO 27001 y el marco de trabajo COBIT 5.0. Esto con el fin de aplicarlo en la producción de servicios

o productos que ofrecen las empresas. Lo cual, permite mejorar la rentabilidad económica mediante la transformación digital y la seguridad de la información.

En consecuencia, implementar los controles y buenas prácticas de ciberseguridad aseguran la información frente a posibles amenazas que puedan afectar a la integridad, disponibilidad y confidencialidad de la misma. Asimismo, el sistema de seguridad de la información debe ser evaluado constantemente por el departamento de TI con el fin de actualizar los sistemas tecnológicos; y revisar las vulnerabilidades y las amenazas cibernéticas. De esta manera, se determinará la presencia de los diversos riesgos en los procesos de calidad de las empresas pymes del Ecuador.

REFERENCIAS BIBLIOGRÁFICAS

Aguilar, J. (2021). Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior. *Instituto de Estudios Internacionales-Universidad de Chile.*, 169-197.

Alonso, I. (2017). La transformación digital de la empresa. Universidad de Cantabria.

Asti, A. (2017). Cyber Defense Challenges from the Small and Medium-Size Business Perspective. *Global Information Assurance Certification Paper*, 1-20.

Battisti, E., Alfiero, S., & Leonidou, E. (2022). Remote working and digital transformation during the Covid-19 pandemic: Economic financial impacts and psychological drivers for employees. *Journal of Business Research, 150*, 38-50.

Buenrostro, H. E., & Hernández, M. D. (2019). La incorporación de las TIC en las empresas. Factores de la brecha digital en las MIpymes de Aguascalientes. *Economía teoría y práctica, 50*, 101-124.

Chatterjee, S., Chaudhuri, R., Vrontis, D., & Thrassou, A. (2022). SME entrepreneurship and digitalization - the potentialities and moderating role of demographic factors. *Technological Forecasting and Social Change, 179*.

Check Poinit. (9 de 09 de 2022). *Informe de Seguridad del 2022 de Check Point Software: Magnitud de la ciberpandemia mundial.* Obtenido de https://pages.checkpoint.com/cyber-security-report-2022-spanish.html?utm_source=eblast&utm_medium=email&utm_campaign=fm_eb_22q1_latam_es_security_report

CISA. (6 de 10 de 2022). *Security Tip (ST04-001), Cybersecurity & Infrastructure Security Agency*. Obtenido de https://www.cisa.gov/uscert/ncas/tips/ST04-001

Eset. (2021). Security Report. Latinoamerica 2021. *ESET Security Report*, 1-29.

FGE. (14 de 10 de 2022). *Fiscalia General del Estado. Los delitos informáticos van desde fraude hasta espionaje.* Obtenido de https://www.fiscalia.gob.ec/los-delitos-informaticos-van-desde-el-fraude-hasta-el-espionaje/

Gamboa, J. L. (2020). Importancia de la Seguridad Informática y Ciberseguridad en el Mundo actual. *Universidad Piloto de Colombioa*, 1-12.

Gonzalo, H. (2022). *Los Ciberdelitos en el Ecuador.* Guayaquil : DAI-CIBERPOL.

Hackmageddon. (05 de 09 de 2022). *Cronologías de ataques de cibernéticos* . Obtenido de https://www.hackmageddon.com/

Herencia, C. (2022). La transformación digital y su importancia en las pymes. *Iberamerican Business Journal, 5*(2), 64-81.

Hulla, M., Herstatter, P., Wolf, M., & Rannsauer, C. (2021). Towards digitalization in production in SMEs-A qualitative study of Challenges, competencies and requirements for trainings. *Procedia CIRP, 104*.

Ilixum. (2022). *COBIT, ¿Qué Es Y Para Qué Sirve?* Obtenido de https://ilixum.com/cobit-que-es-y-para-que-sirve/

ISO 27001. (10 de 2022). *NORMA ISO 27001*. Obtenido de https://normaiso27001.es/

Keeper. (07 de 10 de 2018). 2018 State of Cybersecurity in Small & Medium Size Businesses. *Research Report*, 1-46.

Khurana, I., Dutta, D. K., & Singh Ghura, A. (2022). SMEs and digital transformation during a crisis: The emergence of resilience as a second-order dynamic capability in an entrepreneurial ecosystem. *Journal of Business Research, 150*, 623-641.

López Fernández, C. J. (2019). Desarrollo de una Guia de controles Ciberseguridad para la protección Integral de la Pyme. 79.

Maggi, G., & Gómez, O. (2021). Estudio preliminar sobre conocimiento de Ciberseguridad en usuarios de PYMEs: Caso de estudio Riobamba. *Revista Perspectiva*, 1-9.

Marek, J. (2022). Systematic technology innovation management and analysis of other forms of IP protection. *International Journal of innovation Studies*, 238-258.

Miamó, L. (2019). Detección de botnets y ransomware en redes de datos mediante técnicas de aprendizaje automático. *Doctoral dissertation, Universidad de Murcia.* .

Mintic. (2022). *Guía para la Gestión y Clasificación de Activos de información. Seguridad y Privacidad de la información*. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

Pabón, F. O. (2018). Retos y tendencias de la Ingeniería en Tecnologías de la Información y las Comunicaciones (TIC) frente al Desarrollo del Sector Productivo. *Retos, 14*, 39.

Ragazou, K., Passas, L., & Sklavos, G. (2022). Investigating the Strategic Role of Digital Transformation Path of SMEs in the era of Covid-19: A Bibliometric Analysis Using R. *Digital Transformation in SMEs: A Response to crisis, 14*.

Reyes, M., & Quispe, C. (2020). Transformación digital en la Industria 4.0 una Revisión de la Literatura. *Reserchgate*, 1-15.

Rojas-Mayta, E., & Bustos Martínez, M. (2021). La situación de las PYMES en un contexto de post pandemia. *Revista Científica FIPCAEC (Fomento de la Investigación y publicación en Ciencias Administrativas, Económicas y Contables), 6*(1), 996-1012.

Rosa Pineño, J. (2019). Ciberseguridad para PYMES. Obtenido de http://uvadoc.uva.es/handle/10324/38735

Salazar, J. M. (2021). La transformación digital y su papel en la reactivación con transformación económica y del empleo en América Latina. *XI Foro de Competitividad de las Américas*, 2-68.

Sánchez, C., Bayona, B., Prado, L., & Mendoza, E. (2019). Innovación y tecnología en el tercer sector: Paradigmas y desafíos. *Revista Colombiana de Tecnologías de Avanzada (RCTA), 1*(33), 62-68.

Stich, V., Zeller, V., Hicking, J., & Kraut, A. (2020). Measures for a successful digital transformation of SMEs. *Procedia CIRP, 93*, 286-291.

Tates, C., & Recalde, L. (2019). La ciberseguridad en el Ecuador, Una propuesta de organización . *Revista de Ciencias de Seguridad y Defensa*, 156-169.

Vanegas, D., Gonzalo, A., & Pardo, C. (2014). Hacia un modelo para la gestión de riesgo de TI en MiPymes: MOGRIT. *Red de Revista Científicas de América Latina, el Caribe, España y Portugal*, 35-48.

Xie, X., Han, Y., Anderson, A., & Ribeiro-Navarrete, S. (2022). Digital platforms and SMEs business model innovation: Exploring the mediating mechanisms of capability reconfiguration. *International Journal of Information Management, 65*.

Yang, Z., Chang, J., Huang, L., & Mardani, A. (2021). Digital transformation solutions of entrepreneurial SMEs bases on an information error-driven T-spherical fuzzy cloud algorithm. *International Journal of Information Management*. doi:https://doi.org/10.1016/j.ijinfomgt.2021.102384