



OFICINA DE POSGRADOS

Tema:

PROGRAMA DE CONCIENTIZACIÓN EN SEGURIDAD DE INFORMACIÓN PARA PEQUEÑAS EMPRESAS EN LA CIUDAD DE PUYO

**Proyecto de investigación previo a la obtención del título de Magister en
Ciberseguridad**

Línea de Investigación:

Seguridad de la información

Autor:

Ing. José Luis Beltrán Aldás

Director:

Ing. Omar Salvador Gomez Gomez, PhD.

Ambato – Ecuador

Marzo 2022

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

PROGRAMA DE CONCIENTIZACIÓN EN SEGURIDAD DE INFORMACIÓN PARA
PEQUEÑAS EMPRESAS EN LA CIUDAD DE PUYO

Líneas de Investigación:

Seguridad de la información

Autor:

José Luis Beltrán Aldás



Firmado electrónicamente por:
**OMAR SALVADOR
GOMEZ GOMEZ**

Omar Salvador Gómez Gómez, Ing. PhD.

f. _____

CALIFICADOR

Paúl Hernán Zurita Llerena, Ing. MSc.

f. _____

CALIFICADOR

Paúl Fernando Bernal Barzallo, Ing. MSc.

f. _____

CALIFICADOR

Juan Carlos Acosta Teneda, P. PhD.

f. _____

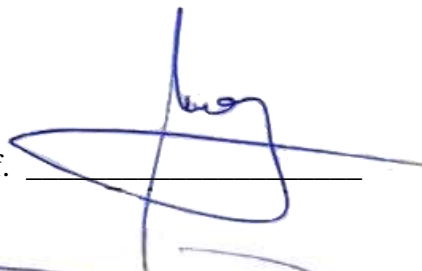
DIRECTOR UNIDAD ACADÉMICA

Hugo Rogelio Altamirano Villarroel, Dr.

SECRETARIO GENERAL PUCESA

Ambato – Ecuador

Marzo 2022


f. _____


f. _____


f. _____



DECLARACIÓN DE AUTENCIDAD Y RESPONSABILIDAD

Yo: **JOSÉ LUIS BELTRÁN ALDÁS**, con CC. **160037623-8** autor del trabajo de graduación intitulado: “PROGRAMA DE CONCIENTIZACIÓN EN SEGURIDAD DE INFORMACIÓN PARA PEQUEÑAS EMPRESAS EN LA CIUDAD DE PUYO”, previa a la obtención del título profesional de **MAGÍSTER EN CIBERSEGURIDAD**, en la **OFICINA DE POSTGRADOS**.

- 1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
- 2.- Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad.

Ambato, marzo 2022



JOSÉ LUIS BELTRÁN ALDÁS

CC. 160037623-8

AGRADECIMIENTO

Agradezco a Dios que, en virtud y presencia, ha sido guía y luz en el proceso de aprendizaje; bajo el manto de su bienestar, ha sido fundamental en este difícil año y nos ha brindado salud, paciencia e improvisada adaptación en esta nueva modalidad.

A los colegas y compañeros de la maestría, dignos profesionales que han complementado el proceso de aprendizaje con su experiencia.

A la Pontificia Universidad Católica del Ecuador, docentes y coordinadores de la maestría; mismos que han realizado un trabajo de gran esfuerzo en un periodo académico no habitual, donde se adapta a una nueva modalidad no contemplada en sus objetivos, y se ha adecuado en nuevas tecnologías y sistemas de aprendizaje para mantener la educación de calidad que la caracteriza.

A los amigos, conocidos y allegados en mi vida, que han sido motivación directa en el desarrollo de mi maestría; son testigos del esfuerzo y dedicación que día a día contemplaron la modificación de mis rutinas, salidas y encuentros que es justificado en ser un profesional que aporte conocimiento y soluciones en la sociedad.

DEDICATORIA

A mis padres, que son el pilar fundamental en el proceso de mi vida, además de ser la motivación directa para expandir nuevos conocimientos y aprendizajes en mi profesión. Su esfuerzo no ha sido en vano, al infundirme principios éticos y morales que forman parte de mi formación académica y humana, reflejan un alto grado de humildad y sacrificio. Muchas Gracias.

A todos los pequeños emprendedores de la ciudad de Puyo, motor económico y productivo, que laboran sin limitaciones y muestran su talento y servicio en pro de la sociedad.

RESUMEN

Los sistemas de información son cada día más vulnerables y se ven amenazados por la falta de concientización en crear una cultura de ciberseguridad que sensibilice en proteger datos críticos de las pequeñas empresas; su importancia radica en educar y generar conciencia sobre la seguridad de la información, que garantiza un tratamiento confiable y protegido de la información en las pequeñas empresas. El trabajo tiene como objetivo elaborar un programa de concientización en seguridad de información para el fortalecimiento de la confidencialidad, integridad y disponibilidad de información sensible de las pequeñas empresas de la ciudad de Puyo. Se trabaja con una metodología cuasiexperimental, que permita recolectar datos antes y después del estudio. Con este trabajo, se pretende establecer guías en buenos hábitos y concientización de la seguridad de la información que, sin antecedentes de trabajos realizados en la ciudad de Puyo, aporta en el desarrollo de la importancia de ciberseguridad en pequeñas empresas.

Palabras claves: sistemas de información, ciberseguridad, confidencialidad, integridad, disponibilidad, concientizar.

ABSTRACT

Information systems are increasingly vulnerable and are threatened by the lack of awareness in creating a culture of cybersecurity. To raise awareness in protecting critical data of small companies is essential; its importance for raising awareness and information security education, ensuring a reliable and protected treatment of information in small companies. The objective of this study is to develop an information security awareness program to strengthen the confidentiality, integrity, and availability of confidential information of small businesses in Puyo city. A quasi-experimental methodology will be used to collect data before and after the study. This project is intended to establish guidelines on good habits and information security awareness without precedents of similar projects done in Puyo city, so it contributes to realizing the importance of cybersecurity in small companies.

Keywords: information systems, cybersecurity, confidentiality, integrity, availability, awareness.

ÍNDICE DE CONTENIDOS

DECLARACIÓN DE AUTENCIDAD Y RESPONSABILIDAD	iii
AGRADECIMIENTO	iv
DEDICATORIA	v
RESUMEN	vi
ABSTRACT	vii
ÍNDICE DE CONTENIDOS	viii
INTRODUCCIÓN	1
CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA	4
1.1. Antecedentes	4
1.2. Ciberseguridad	7
1.3. Ataques informáticos en las <i>pymes</i>	12
1.4. Métodos de protección para la seguridad de la información	16
1.5. Plan de concientización	24
CAPÍTULO II. DISEÑO METODOLÓGICO	28
2.1. Contextualización de las pequeñas y medianas empresas (<i>pymes</i>) en la ciudad de Puyo	28
2.1.1. Justificación de las <i>pymes</i>	28
2.2. Diseño Metodológico	29
2.2.1. Diseño de la investigación	29
2.2.2. Enfoque de la investigación	29
2.2.3. Modalidad de la investigación	29
2.2.4. Técnica de la investigación	30
2.2.5. Población y Muestra	30
2.3. Método de Desarrollo	31
2.3.1. Aproximación a la solución	31

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN.....	48
3.1. Procesamiento de Datos Pre- Test y Post- Test.....	48
3.2. Análisis Descriptivo	49
3.3. Análisis Inferencial.....	50
3.4. Análisis global de datos.....	52
CONCLUSIONES.....	54
RECOMENDACIONES	55
BIBLIOGRAFÍA	56
ANEXOS	61
Anexo A. Acuerdo de confidencialidad	61
Anexo B. Formulario de diagnóstico situacional	62
Anexo C. Plan de concientización en seguridad de la información	66
Anexo D. Oficio de solicitud para aval.	73
Anexo E. Pre-Test y Pos-Tes (Formulario de evaluación).....	74
Anexo F. Promoción del programa de concientización en seguridad de información	75
Anexo H. Plataforma <i>Web</i> programa de concientización en seguridad de información.	78

INDICE DE TABLAS

Tabla 1. Distribución de las PYMES.....	5
Tabla 2. Registro de ataques.....	13
Tabla 3. Errores en el tratamiento de la información	18
Tabla 4. Clasificación de la información.....	19
Tabla 5. Estándares de la familia ISO	20
Tabla 6. Tabla de procesamiento de datos del Pre-Test y Post-Test	49
Tabla 7. Análisis Descriptivo Pre-Test y Post-Test.....	50
Tabla 8. Prueba de normalidad Pre-Test y Post- Test	51
Tabla 9. Análisis Inferencial Pre-Test y Post-Test.....	52
Tabla 10. Análisis global de resultados	53

INDICE DE FIGURAS

Figura 1. Triada de la seguridad de la información.....	8
Figura 2. Proceso de la gestión de riesgos.....	11
Figura 3. Reporte de ataques a la red en Ecuador	12
Figura 4. Formas de ataques.....	14
Figura 5. Marco de trabajo metodología Magerit.....	22
Figura 6. Procesos de la metodología ITIL	23
Figura 7. Marketing Digital	33
Figura 8. Comercio Electrónico.....	34
Figura 9. Banca en línea	34
Figura 10. Delitos informáticos	35
Figura 11. Fraudes electrónicos.....	36
Figura 12. Administración de contraseñas	36
Figura 13. Almacenamiento de contraseñas	37
Figura 14. Software de antivirus.....	38
Figura 15. Software legal.....	38
Figura 16. Dispositivos móviles	39
Figura 17. Cronograma de Actividades	41
Figura 18. Plan de concientización seguridad de la información.....	42
Figura 19. Portal Web del programa de concientización.....	43

Figura 20. Difusión publica del programa de concientización mediante <i>FanPage</i>	43
Figura 21. Pre-Test visto desde el portal <i>Web</i>	46
Figura 22. Evaluación del programa mediante Post-Test.....	47

INDICE DE GRÁFICOS

Gráfico 1. Aproximación a la solución.....	31
--	----

INTRODUCCIÓN

La era digital, ha traído grandes beneficios, mismos que han revolucionado los sistemas tradicionales de información. Con relación al área empresarial, la tecnología contribuye a una mejor disponibilidad de datos, estructura adecuada además de excelentes metodologías de negocios que son aprovechados por los administradores para una mejor toma de decisiones. No obstante, se ha minimizado la protección y resguardo de la información que serían prioridad fundamental dentro del modelo empresarial.

Los sistemas de información analizan el impacto de la adopción de tecnologías de información, en los procesos de decisión gerenciales y administrativos de la empresa. El auge y la funcionalidad; así como un amplio desarrollo referente a sistemas de información han sido empleadas por grandes y medianas empresas, mismas que se benefician de las funcionalidades cuyo objetivo es optimizar los servicios. Sin embargo, al no fomentar una cultura de seguridad de la información, esto crea un ambiente favorable en cuanto a vulnerabilidades y riesgos que son aprovechados por personas inescrupulosas para el propio beneficio o robo de información sensible muy apetecible por la competencia.

Las empresas han innovado en procesos de gestión, uso y análisis de información para una oportuna toma de decisiones, pero han excluido garantizar la seguridad de la información, donde se minimiza el uso de políticas de privacidad o planes de concienciación a sus emprendedores. En la ciudad de Puyo, las pequeñas empresas han crecido paulatinamente y son fuentes de empleo debido a la amplia gama de servicios que ofertan. Las *pymes* (pequeñas y medianas empresas), han adaptado el modelo de negocios en base a sistemas de información, mismo que permite un manejo oportuno de datos. Desde este punto, la parte de seguridad de la información se aísla del progreso y genera pérdidas por ataques dañinos como *phishing* o *malware*, así como robo de información crítica y no respaldo de datos, debido a que las gerencias evitan invertir en ciberseguridad, por considerarlo innecesario.

La carencia básica sobre seguridad en sistema de información es un inconveniente que ocasiona problemas a la organización en toda su estructura, el manejo inoportuno de la información que sin conceptos de seguridad debilita la fortaleza esencial de datos y activos lógicos para las pequeñas empresas. La debilitada cultura de ciberseguridad en el personal laboral y administrativo de las pequeñas empresas conlleva al aumento de riesgo en

protección de la información y abre oportunidades de vulnerabilidades suscitadas internamente en la organización, como el uso de claves con palabras diccionarios, ejecución de software malicioso, ingeniería social, entre otras que son problemas que suscitan en las pequeñas empresas sin medir el impacto que causan (Deutsch, 2016).

La ausencia de guías y modales de seguridad de información, así como un desmotivante y ambiguo programa, genera despreocupación en la forma de proteger los activos de información. La no detección de vulnerabilidades básicas y la falta de concientización es sus trabajadores pone en desventaja a una empresa ante sus competidores. Desde la perspectiva de Rea-Guamán, Calvo-Manzano y Feliu (2018) carecer de una guía de concientización conlleva a un robo e información crítica, caída de los servicios, e incluso llega hasta la pérdida de la imagen y prestigio de una organización.

Continuamente se evidencia un incremento en el uso de herramientas tecnológicas tanto en sistemas de gestión empresarial, como en plataformas de redes digitales para crear información crítica, misma que es susceptible de ser vulnerada y amenazada, lo que abre brechas de seguridad. Basado en este análisis ¿Al contar con un programa de concientización de la seguridad de la información, fortalece la protección de la información sensible y asegura los datos en las pequeñas empresas de la ciudad de Puyo?

Para el desarrollo del presente estudio, se parten de los siguientes objetivos:

Objetivo General: Validar el impacto del programa de concientización de la seguridad de información en el fortalecimiento de la protección de información sensible de la pequeña empresa en la ciudad de Puyo.

Objetivos Específicos:

1. Analizar teóricamente el estado del arte en seguridad de información, concientización, vulnerabilidades y educación en seguridad de información.
2. Realizar un diagnóstico de la situación actual sobre seguridades de información de la pequeña empresa de la ciudad de Puyo.
3. Diseñar un programa en fases estratégicas en sensibilización y fortalecimiento sobre una cultura de seguridad de información.

El tipo de investigación que se utiliza es cuasi experimental, basado en un estudio observacional pretest – posttest. Se aplica una encuesta de diagnóstico situacional, que mide el grado de satisfacción o rechazo del problema de investigación mediante la escala tipo Likert para evaluar la opinión y aptitud de las personas y la cultura de protección de datos en las *pymes*.

La presente investigación tiene como finalidad, desarrollar un plan de concientización de la seguridad de la información y evaluar el desempeño en una muestra representativa de una población, a través de un estudio pretest y post-test, que fortalece la educación, enseñanza y motivación de cómo proteger la información más sensible que una pequeña empresa dispone. Todo ello con la finalidad de direccionar interés en consolidar una cultura de ciberseguridad, misma que involucre a todos los activos principales que forman parte de una pequeña empresa, cuya imagen, objetivos y prestigio son necesarios para el desarrollo de la organización.

Es fundamental la necesidad de un programa de concientización debido a la falta de guías y modales sobre educación y sensibilización de seguridades de la información. Misma que, logra identificar tanto riesgos, como efectos, y en consecuencia produce una inoportuna acción del personal que está directamente involucrado con la información. Por ende, esto motiva a crear una cultura de ciberseguridad en las pequeñas empresas de la ciudad de Puyo. Dado que, permite establecer interés de parte de las organizaciones en cómo proteger la información crítica, identificar vulnerabilidades y amenazas que pongan en riesgo la disponibilidad, integridad y autenticación de datos.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Antecedentes

El creciente uso del internet mediante las redes de computadores brinda la facilidad a cada negocio ya sea pequeño, mediado o grande, para el uso de la tecnología con diversos fines como: publicidad, almacenamiento de información, ventas, control de activos, entre otros. Existen diversas empresas que hacen uso de las redes sociales para publicar los productos y promociones que poseen, esta es una estrategia efectiva en el comercio electrónico, debido a la gran demanda de usuarios conectados a internet. Estos métodos están considerados dentro del ámbito del *marketing* digital y son utilizados en su mayoría, por pequeñas y medianas empresas, a consecuencia del bajo coste en el uso de estos aplicativos.

La utilización de internet ha crecido de forma exponencial durante los últimos años y es debido a los distintos métodos de acceso a dicha tecnología. Si se realiza una reflexión, en la actualidad existen conexiones mediante plan de datos móviles 3G y 4G, así como también, servicio de navegación fija con banda ancha por fibra óptica o conexión de cobre, esto ha generado un aumento en la demanda del servicio para domicilios o negocio, la empresa de comunicaciones CISCO en su informe anual de proyección del consumo de internet realizado por Sevilla (2020) manifiesta que para el año 2023: “El 66 por ciento de la población mundial (5,300 millones de personas) serán usuarios de internet” (p.1). Esto representa una gran ventaja en el uso del internet y la red de datos para pequeñas y medianas empresas denominadas *pymes* y cuyo objetivo sea expandir sus negocios sin invertir demasiado capital.

La utilización de la tecnología no solo representa un beneficio, también, implica riesgos y amenazas ante algún ataque informático de un ciberdelincuente. Acorde al criterio de Delgado y Chávez (2018) manifiesta que:

Las *pymes* son pequeñas empresas formadas por diferentes estructuras ya sean familiares, amigos o socios quienes aportarían con capital para que la misma salga adelante en el área económica que se vaya a desenvolver, también, cuentan con el financiamiento respectivo para operar en el mercado de negocio (p. 4).

Se considerarían que las *pymes* contienen el concepto de micro, pequeñas y medianas empresas, estas se encuentran diferenciadas de acuerdo con la Cámara de Comercio de Pichincha según la Tabla 1:

Tabla 1. Distribución de las PYMES

Variables	Micro Empresa	Pequeña Empresa	Mediana Empresa	Grandes Empresas
Personal ocupado	De 1 - 9	De 10 - 49	De 50 - 199	≥ 200
Valor bruto de ventas anuales	≤ 100.000	100.001 - 1.000.000	1.000.001 - 5.000.000	> 5.000.000
Monto de activos	Hasta US\$ 100.000	De US\$ 100.001 hasta US\$ 750.000	De US\$ 750.001 hasta US\$ 3.999.999	≥ 4.000.000

Fuente: Cámara de Comercio de Quito (2017)

De acuerdo con el rango establecido para la clasificación de las *pymes*, se evidencia que dichas empresas no poseen de recursos para la implementación de un sistema de seguridad informática, debido a los altos costes que tienen. Además, de la falta de recursos económicos, existen otros factores para la deficiente protección de los recursos informáticos como:

- Los propietarios de las *pymes*, creen no ser un objetivo interesante para los ciberdelincuentes, por los ingresos que generan.
- La falta de recursos técnicos que generen una concientización acerca de este tema.
- La inexistencia de un Sistema de Gestión de Seguridad de la Información (SGSI), en el proceso interno de la organización.
- La ausencia de una política de seguridad de bajo coste orientado a las necesidades de las *pymes*.

En Ecuador existen alrededor de 179.830 *pymes* de las cuales, la provincia del Guayas abarca con un total del 32.67% que representa a un total de 58.574 empresas de este tipo, seguido de la provincia de Pichincha con un aporte del 27.95% equivalente a una cantidad de 50.269 *pymes* y por último la provincia de Manabí con un 4.69% que equivale a 8.438 empresas (INEC, 2016, p.1).

La provincia de Pastaza cuenta con alrededor de 1070 *pymes* de acuerdo con el último censo realizado por el Instituto Nacional de Estadística y Censo (INEC) en el año 2016. Las *pymes* son además un sector con mayor capacidad de abrir nuevas ofertas de empleo debido a la gran cantidad de estas, esto convierte a este sector en organizaciones con manejo de

información sensible propia de la pequeña o mediana empresa, así como también, la información personal de cada uno de sus colaboradores.

Por otra parte, en la investigación realizada por Izaguirre (2018) se pone en manifiesto el alto índice de ataques informáticos, con aproximadamente un 32% de delitos cibernéticos a nivel mundial. Entre los ataques más comunes son: por ingeniería social, *phising* o *malware*. De acuerdo con el reporte de Cybereop (2020), el 40% de los atracos informáticos son dirigidos a las pequeñas y medianas empresas, esto se debe a que, existe una vulnerabilidad latente dentro de una organización *pymes* y es el desconocimiento ante la respuesta inmediata a incidentes de este tipo. Es decir, una gran parte de propietarios o administradores de las *pymes* no manejan una conciencia clara de que hacer para prevenir ataques informáticos, o a su vez como actuar en caso de haber sufrido uno.

Como se evidencia, a pesar de no manejar recursos económicos elevados, si existe una gran cantidad de *pymes* en el país. Esto resulta muy atractivo para los ciberdelincuentes, debido a que son empresas vulnerables ante ataques sencillos, pero con capacidad de generar grandes pérdidas económicas para dicho sector. De forma adicional, el impacto ante un ciberataque en una *pyme* es mucho mayor, debido a los recursos limitados de los mismos, un ataque informático tendría una mayor afectación a los recursos y repercutiría hasta el cierre de la misma.

Las pequeñas y medianas empresas requieren herramientas que permitan a gerentes tener la suficiente confianza para la toma de decisiones en el momento de generarse riesgos de tecnologías informáticas (TI). Estas decisiones estan respaldadas mediante argumentos físicos e históricos. De manera que, “le eviten a la empresa incurrir en sobre costos y en subestimaciones o sobre estimaciones de los riesgos al momento de ser evaluados” (Flores, Arboleda & Cadavid, 2012, p. 36).

De acuerdo con el análisis de los autores, se recomienda que, toda empresa sin importar el tamaño de la misma, tendra métodos y técnicas para proteger su información ante un ciberataque. Todo ello con la finalidad de garantizar los recursos que la organización posee, estas medidas de protección son acorde a las necesidades de cada institución y a los alcances económicos que esta posea, para que no exista un perjuicio económico que afecte a la industria.

1.2. Ciberseguridad

Existe una confusión entre lo que es seguridad informática y seguridad de la información, a pesar de que estos dos términos están orientados a proteger los activos informáticos de una empresa, cada uno de ellos está orientado a ramas distintas, antes de realizar una concientización se entendera la diferencia entre cada uno de ellos:

- **Seguridad informática:** Está orientada a proteger la infraestructura y la red de comunicaciones dentro de una empresa.

La seguridad informática protege el sistema informático, trata de asegurar la integridad y la privacidad de la información que contiene. Por lo tanto, se dice que, se trata de implementar medidas técnicas que preservarán las infraestructuras y de comunicación que soportan la operación de una empresa, es decir, el hardware y el software empleados por la empresa (ISOTools Excellence, 2017, p. 1).

- **Seguridad de la información:** Es la parte de la ciberseguridad que se encarga de proteger a la información como un activo sin importar el medio en el que se encuentre. Desde la perspectiva de ISOTools Excellence (2017) menciona que: “La Seguridad de la Información integra toda la información independientemente del medio en el que esté. La seguridad informática atiende sólo a la protección de las instalaciones informáticas y de la información en medios digitales” (p.1).

De acuerdo con el concepto de ciberseguridad, la seguridad informática, así como también, la seguridad de la información, posee estructuras y conceptos diferentes. Sin embargo, trabajan en conjunto para cumplir con un mismo objetivo, el cual, consiste en disminuir los riesgos de la empresa ante un ataque informático dentro de una organización. Estos sistemas poseen un conjunto de medidas preventivas para que la empresa ya sea pequeña, mediana o grande, mantenga la confidencialidad, disponibilidad e integridad de los datos.

Es importante resaltar la clasificación que tiene la información dentro de una organización, como:

- **Crítica:** Imprescindible para la operación de la empresa.
- **Valiosa:** La información es considerada como activo y tiene un gran valor.
- **Sensible:** Esta sera accesible solo por el personal autorizado.

De acuerdo con ESET (2019):

La protección de la seguridad y la privacidad de la información confidencial de los clientes es una obligación fundamental para todas las empresas, incluye las *PYME*. La protección de datos abarca todos los controles administrativos, lógicos y técnicos necesarios para proteger la información. A la hora de desarrollar e implementar un marco para administrar la seguridad de la información dentro de una organización se suele usar la tríada C-I-D, conformada por tres conceptos fundamentales de seguridad de la información (p.1).

La tríada de la Confidencialidad, Integridad y Disponibilidad (CID) es representada de manera general en un triángulo, la razón es que los tres parámetros trabajan en conjunto para brindar la seguridad requerida por la empresa, esta interpretación se evidencia en la Figura 1, mostrada a continuación:

Figura 1. Triada de la seguridad de la información



Fuente: elaboración propia

- 1. Integridad:** Hace referencia a que la información solo será modificada por el personal autorizado y de acuerdo con previas solicitudes de cambio pedidas por la misma.

La integridad hace relación a menudo que: la información sera la misma, desde el origen de los datos, hasta el uso del cliente, sin variaciones ni alteraciones que hace uso de esa información. Por lo tanto, no se manipulara en ningún instante de la transacción Cliente- Servidor. La integridad se vera amenazada por atacantes, como por errores humanos, accidentales o intencionales (Cortes, 2016, p.1). Así, por ejemplo, una modificación de la información genera pérdidas de activos dentro del negocio.

La integridad hace uso de técnicas para la protección de información entre las cuales se cita:

- Autenticación por Firmas Digitales.
- Control de acceso a datos sensibles.
- Administración de privilegios .
- Control de regulación de comunicaciones (CRC) .
- Permisos de configuración.

Entre los ataques más comunes a la integridad de la información se tiene:

- Modificación de privilegios.
- Ataques de *SQL Injection*.
- Ataque por robo de sesión.
- Modificación de código.

2. Confidencialidad: Hace referencia a que la información sera vista solo por el personal autorizado.

La confidencialidad trata de que la información no sea revelada a usuarios no autorizados. Los atacantes tendrían acceso a la misma a travez de *Shoulder Surfing*, robo de contraseñas, romper sistemas de encriptación e ingeniería Social. El *Shoulder Surfing*, trata de mirar sobre el hombro de alguien, para ver cuáles son las teclas que presiona al ingresar una contraseña u observar algún papel o archivo que contenga la contraseña de ingreso a un sistema (Cortes, 2016 p.1). Cabe destacar que, muchas personas dejan la contraseña escrita en algún papel pegado al monitor, escritorio o en un cuaderno a vista de todo el mundo.

La confidencialidad está basada en los siguientes métodos:

- Encriptado de información.
- Uso de protección durante el tránsito de la información (*Virtual private network* VPN, *Internet Protocol security* IPsec).

Dentro de los ataques más comunes se tiene:

- *Man in the middle*.
- *Phishing*.
- Robo por contraseñas.

3. Disponibilidad: Se refiere a que la información estara disponible en cualquier momento que el usuario lo requiera.

Este punto asegura que los usuarios autorizados accedan a tiempo a sus recursos. Existen varios dispositivos dentro del sistema que estan disponibles para el acceso de la información. Como, por ejemplo: *router*, *Domain Name System* DNS, *Firewall*, *Intrusion Detection System* IDS, DHCP, Servidores, *software*, entre otros (Cortes, 2016, p.1).

La disponibilidad se basa en uso de recursos como:

- Discos duros de los servidores en modo espejo.
- Servidores con hiperconvergencia.
- Alta disponibilidad en la red de datos.
- Balanceo de carga en los servidores.
- Generación de *backups* a la información.

Esta parte de la tríada es susceptible ante ataques como:

- Inundación de ICMP.
- Inundación de paquetes UDP.
- Ataques por DOS.

ESET (2019) afirma: “Para que la seguridad de la información sea efectiva, es necesario que la empresa se comprometa a mantener la confidencialidad, integridad y disponibilidad de todos sus datos críticos, incluye los sistemas y las aplicaciones que procesan y almacenan dichos datos” (p.3).

De acuerdo con este criterio, cualquier organización sin importar su tamaño, implementa controles con el objetivo de analizar las vulnerabilidades para disminuir el riesgo ante un ciberataque. Se considera que estas son reglas relacionadas de manera directa, es decir, mientras más grande sea el riesgo en el sistema, las medidas de protección serán más robustas. La gestión de riesgos se compone de las fases mostradas en la Figura 2:

Figura 2. Proceso de la gestión de riesgos



Fuente: ESET (2019)

Desde la perspectiva de Figueroa-Suárez, Rodríguez-Andrade, Bone-Obando y Saltos-Gómez, (2017) aseguran que: “Los peligros de negocio incluyen los riesgos organizacionales, operacionales, físicos y de tecnologías de información y la comunicación (TIC)” (p.9). Mediante este criterio se obtiene un enfoque orientado a la seguridad de la información (SI), con el objetivo de conseguir los recursos que logre minimizar los riesgos en los métodos de seguridad aplicados a las *pymes*. Es importante resaltar que, estas técnicas de protección no serán vistas como un gasto, sino como una inversión para la organización. De forma adicional y los dichos autores indican que, al establecer un (SGSI) se protege al sistema de:

- Divulgación indebida de información sensible o confidencial, de forma accidental o bien, sin autorización.
- Modificación sin autorización o bien, de forma accidental, de información crítica, sin conocimiento de los propietarios.
- Pérdida de información importante sin posibilidad de recuperarla.
- No tener acceso o disponibilidad de la información si sea necesaria.

1.3. Ataques informáticos en las *pymes*

De igual forma mientras la tecnología avanza, también, lo hacen las amenazas informáticas basadas en el internet mediante las redes de comunicaciones. Esto ha llegado a convertirse en una de las principales preocupaciones, no solo para las instituciones dedicadas a la ciberseguridad, sino para todas las empresas, debido al riesgo latente en el que se encuentra la información que poseen frente a un ataque. De acuerdo con un estudio realizado por Kaspersky (2016) manifiesta que:

El 82% de las empresas a nivel mundial ha sufrido entre uno y cinco incidentes de exposición, filtración o pérdida de datos en los últimos 12 meses. Como resultado de esa clase de incidentes, el 10% de ellas perdió acceso a información crítica durante una semana y el 15% sufrió interrupciones que le impidieron realizar transacciones comerciales durante más de siete días (p.1).

En concordancia con Telefónica (2015) aseguran que precisamente: “Debido a estos riesgos latentes, la seguridad de la información se ha convertido en una auténtica prioridad por parte de empresas de toda escala, con especial énfasis en las *PYMES*, organizaciones que suelen ser más vulnerables a estos ataques” (p.1). Es por ello por lo que, si una empresa desea minimizar el riesgo contara con *software* dedicado a la protección de la infraestructura de la empresa como antivirus, cortafuegos perimetrales. Además, es importante capacitar al personal con el objetivo de prevenir vulnerabilidades como el mal uso de correo o la navegación.

En la Figura 3 se evidencia el reporte de ataques a la red de datos en Ecuador, generado por Kaspersky en el presente año:

Figura 3. Reporte de ataques a la red en Ecuador



Fuente: Kaspersky (2020)

Como se evidencia en el gráfico mostrado el Ecuador sufre alrededor de 100000 ataques en horas pico de la noche, esto es debido al alto consumo de internet que existe en el horario mencionado. En la Tabla 2 muestra el reporte de las principales infecciones a los sistemas informáticos del Ecuador.

Tabla 2. Registro de ataques

1	Intrusion.Win.MS17-010.o	78,12%
2	Bruteforce.Generic.Rdp.d	14,06%
3	Scan.Generic.PortScan.TCP	4,01%
4	Intrusion.Win.MS17-010.p	2,66%
5	Bruteforce.Generic.Rdp.a	0,78%
6	Intrusion.Win.MS17-010.cf	0,22%
7	DoS.Generic.Flood.TCPSYN	0,07%
8	Scan.Generic.PortScan.UDP	0,02%
9	Bruteforce.Generic.Rdp.c	0,02%
10	Intrusion.Win.CVE-2017-0147.sa.leak	0,02%

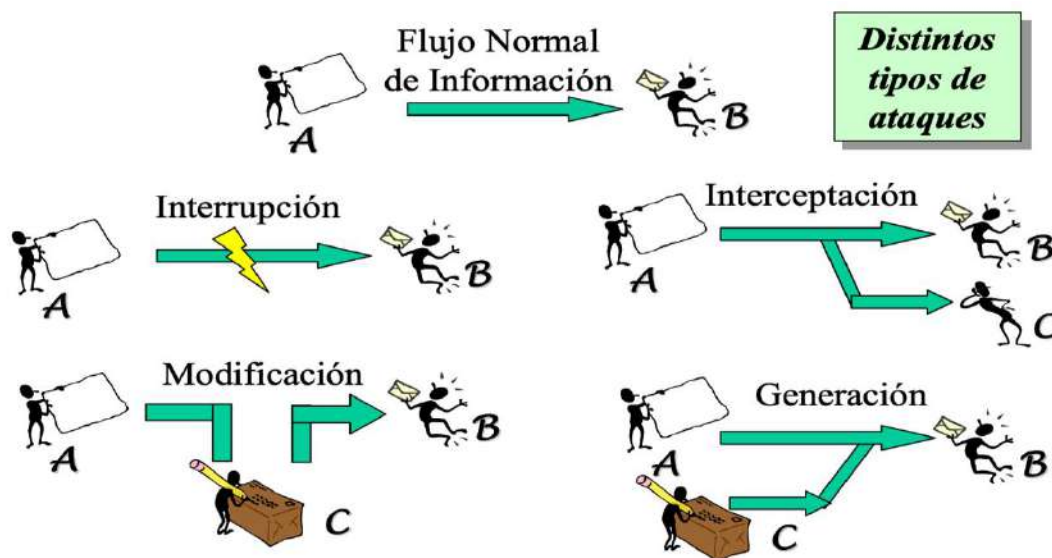
Fuente: Kaspersky (2020)

En un trabajo de investigación realizado por Gómez (2019) clasifica:

Los ataques informáticos en dos categorías los ataques activos, que producen cambios en la información y en la situación de los recursos del sistema, y los ataques pasivos, que se limitan a registrar el uso de los recursos y/o a acceder a la información guardada o transmitida por el sistema (p.1).

Estos ataques se explican de una forma más detallada en la Figura 4 presentada a continuación:

Figura 4. Formas de ataques



Fuente: Gómez (2019)

Antes estos aspectos según los reportes actuales de firmas de antivirus y empresas relacionadas con la seguridad detalladas en la introducción del artículo, el aumento de ataques de DDOS y *Malware* es evidente y para ello se utilizan redes controladas por atacantes llamadas *botnet*, que son grupos de computadores controlados por un atacante que escanearon o aprovecharon una vulnerabilidad, y que por medio de un malware lograron su control con el objetivo de distribuir otros malware o realizar ataques de DDOS (Zambrano & Guailacela, 2019, p. 9).

De acuerdo con el criterio del autor y según lo estudiado, las *pymes* no poseen la infraestructura necesaria para reducir el riesgo ante estos tipos de ataques, esto eleva el riesgo de dichos usuarios a ser atacados y vulnerada la red.

En el año 2017, el mundo se vio sorprendido ante un ataque que fue capaz de detener servicios a nivel empresarial global, este ataque fue conocido con el nombre de *WannaCry*, un programa maligno de tipo *ransomware* (*software* dañino que impide a los usuarios acceder a sus sistemas). Según el reporte generado por la Revista de Tecnología Gestión (2017) asegura que: “A pesar de que este ataque fue de índole global, el 50% de empresas vulneradas fueron a *pymes*” (p.1). Las pequeñas y medianas empresas están vulnerables a cualquier ciberataque, por lo general son víctimas de:

- **Phishing:** Está compuesto por un ataque de ingeniería social y programas o códigos con un fin maligno, usados con fines económicos por parte del atacante, el patrón usado para este tipo de ataque es el uso de correos electrónicos falsos, estos incluyen un enlace (*Uniform Resource Locator*, URL), mediante el cual, el navegador se redirige a sitio *WEB* falso.

Desde el punto de vista de Benavides, Fuertes y Sánchez (2020) indican que: “Una página de Phishing es aquella que, como cualquier página *Web*, sin permiso, alega actuar en nombre de un tercero; con la intención de confundir a los espectadores en la realización de una acción” (p. 98). Por ello, la importancia de resguardar la información.

- **Spam:** Es un tipo de ataque a través de correo electrónico. Consiste en el envío masivo de mensajes, que por lo general son promociones o anuncios que resulta inoportuno o hasta peligroso para el usuario. Frente a ello, Avast (2020) indica:

Si se define *spam* como mensajes masivos no solicitados, el *spamming* es el acto de enviar estos mensajes, mientras que a la persona que participa en esta práctica se la denomina *spammer*. La mayoría de las veces, el *spam* es de naturaleza comercial y, aunque es preocupante, no es necesariamente malicioso o fraudulento (aunque puede serlo) (p.1). Las organizaciones no permiten descuidar este aspecto.

- **Ransomware:** Es un *software* de tipo malicioso que es usado para el secuestro de información, tiene por objetivo que la víctima realice un pago por la devolución de sus datos, por lo general este pago se lo realiza por *Bitcoin*.

De acuerdo con el estudio de Aguilar y Guaita (2018), el ransomware se clasifica en tres diferentes tipos:

1. **De bloqueo:** Impide el funcionamiento normal de un dispositivo; dificulta la interacción usuario-dispositivo.
2. **De cifrado:** Cifra los archivos de una amplia gama de extensiones, y afecta información personal del usuario.

3. **De control:** Es el tipo de infección más peligroso. Accede y toma el control de sistemas completos que afecta, incluso, a empresas a nivel mundial.

1.4. Métodos de protección para la seguridad de la información

A fin de intentar disminuir las amenazas y los riesgos informáticos, existen metodologías que buscan disminuir el impacto de los ciberataques a nivel mundial. Es un conjunto de técnicas utilizadas a nivel de gerencia informática, con el objetivo de generar métodos de protección de la información de la empresa u organización. Tiene como finalidad: proporcionar una visión completa tanto de la infraestructura, así como de los datos que la institución posee. Según el criterio de EcuRed (2020) argumenta que: “Los sistemas actuales de gestión de la información se basan en gran medida en la tecnología para recopilar y presentar datos, pero el concepto es más antiguo que las tecnologías informáticas modernas” (p.1). La era digital accede con mayor facilidad a la información.

Cada organización, ya sea pequeña, mediana o grande posee información que proteger, a fin de garantizar el desarrollo normal de sus actividades empresariales se hace uso de una buena gestión de seguridad de la información (SI). El estudio estratégico usado para un correcto uso de los SI, permite generar un alto nivel de eficacia y eficiencia para la institución. En el caso de las *pymes* el uso de las SGSI es un poco limitado debido a la inversión que esta requiere, caso contrario empresas grandes no tienen inconvenientes en la implementación de este, sin embargo, el desconocimiento del tema hace que muchos empresarios no tomen en serio la gravedad de un ciberataque.

Si algún tipo de información merece una especial atención por parte de los poderes públicos, es decir, el establecimiento de una política que considere cómo será solicitada, tratada o transmitida, esa es sin duda la información personal. Más aún si el análisis masivo de datos el *Big Data* promete ser uno de los ingredientes básicos de casi cualquier negocio en casi cualquier sector económico de relevancia. Y, en efecto, ha recibido atención desde hace décadas.

Hasta ahora, protección es la palabra que orienta y casi domina, las políticas que se ocupan de la información personal. La causa es simple, la información personal entra dentro del ámbito de lo privado al que el derecho siempre ha dado el máximo amparo. También, por ello sería más preciso hablar de regulaciones que de políticas, pues el peso que en la actividad

pública han tenido acciones diferentes de las estrictamente normativas ha sido muy reducido. (Gómez, Feijóo & Martínez, 2017, p.1).

Una *pyme* está caracterizada por mantener una fluida interacción con sus clientes, a pesar de no poseer un alto número de estos, la amplia variedad de este tipo de empresas hace que, en conjunto formen una enorme cantidad de información personal de sus clientes. Por tal motivo, cada organización esta en la obligación de aplicar métodos y técnicas de protección de la información. Por otro lado, INCIBE (2020a) en su reporte manifiesta:

Gracias al uso de la tecnología, el procesamiento y almacenamiento de grandes volúmenes de datos se ha vuelto muy sencillo. En una memoria USB se almacena sin autorización, una gran cantidad de información confidencial de una empresa de tamaño mediano e incluso a través de correo electrónico se envía información confidencial de la empresa como la base de datos de clientes, con fines distintos a los permitidos (p.5).

De manera general, la falta de conocimiento en los empresarios *pymes*, hace que se cometa ciertos errores en sus empresas, los cuales, a manera de resumen se muestran en la Tabla 3 presentada a continuación:

Tabla 3. Errores en el tratamiento de la información

Información importante de la que no se realiza copia de seguridad.	Para evitar cometer este error tendremos que asegurarnos que tenemos una copia de seguridad actualizada de la información, al menos de aquella más crítica. Y comprobaremos que sabemos y que podemos recuperarla.
<p>Carpetas de red compartidas sin control de acceso.</p> <p>Usuarios que no saben dónde está la última versión de un documento.</p> <p>Usuarios que tras un cambio de puesto conservan acceso a información que, por el nuevo tipo de trabajo que van a desempeñar, no es necesaria.</p>	Estos errores se pueden evitar si hacemos que la información sólo sea accesible a quien la necesita y esté autorizado para ello. Es decir implantar un «control de accesos» .
<p>Presencia de discos duros portátiles sin que la organización conozca y tenga inventariados quién los utiliza y qué información pueden tener almacenada.</p> <p>Falta de formación de los usuarios en las herramientas que utilizan.</p> <p>Dejar que los empleados utilicen almacenamiento en la nube y su correo personal para actividades profesionales</p>	Si no se limita el uso de aplicaciones no corporativas (correo personal, almacenamiento en la nube) y se controla el uso de los dispositivos externos ni los usuarios tienen la adecuada formación, cometeremos estos errores.
Tirar los ordenadores y discos a la basura sin ningún control previo de su contenido.	Tener controlados los soportes y los equipos es esencial pues algún día dejan de ser útiles, por obsoletos o por desgaste. Es el momento de deshacerse de ellos, borrar toda la información que tenían, de forma que no quede ni rastro de su uso previo.

Fuente: INCIBE (2020a)

En este punto, se resalta que, el uso de la tecnología de manera correcta permite a las pequeñas y medianas empresas tener un desarrollo sustancial económico y a su vez generar más competitividad en el comercio de sus productos, por tales motivos se evidencia la importancia de acogerse a prevenciones y medidas que disminuya el riesgo ante un incidente de seguridad de la información. Para un correcto uso de la información es necesario diferenciar la información a tratar, esta interpretación está basada en niveles de acuerdo con su importancia y se evidencia en la Tabla 4 detallada a continuación:

Tabla 4. Clasificación de la información

CATEGORÍA	DEFINICIÓN	TRATAMIENTO
Confidencial	Información especialmente sensible para la organización. Su acceso está restringido únicamente a la Dirección y a aquellos empleados que necesiten conocerla para desempeñar sus funciones. También datos de carácter personal, en particular los de categorías especiales.	Esta información debe marcarse adecuadamente. Se deben implementar todos los controles necesarios para limitar el acceso a la misma únicamente a aquellos empleados que necesiten conocerla. En caso de sacarla de las instalaciones de la empresa en formato digital, debe cifrarse. Para los datos de carácter personal, se deben tener en cuenta la protección y garantías indicadas en la legislación sobre la materia.
Interna	Información propia de la empresa, accesible para todos sus empleados. Por ejemplo, la política de seguridad de la compañía, el directorio de personal u otra información accesible en la intranet corporativa.	Esta información debe estar adecuadamente etiquetada, y estar accesible para todo el personal. No debe difundirse a terceros salvo autorización expresa de la dirección de la empresa.
Pública	Cualquier material de la empresa sin restricciones de difusión. Por ejemplo, información publicada en la página web o materiales comerciales.	Esta información no está sujeta a ningún tipo de tratamiento especial.

Fuente: INCIBE (2020a)

Una vez establecido y clasificado cada dato de la información, se determina el riesgo a la que está sujeta, para tomar medidas de corrección. En la ejecución de este procedimiento INCIBE (2020a), recomienda basarse en cuatro pasos:

1. Conocer la información que gestiona la organización. Esto se hace a través de entrevistas y reuniones con el personal de la organización.
2. Clasificarla según su criticidad, según un criterio razonable y unificado.
3. Determinar su grado de seguridad: ¿es alto el riesgo de pérdida de información?, ¿y el de fuga o robo de información?, ¿sería alterada sin autorización?
4. Establecer las medidas necesarias para mejorar su seguridad.

El uso de esta metodología es conocido de manera general como Sistema de Gestión de Seguridad de la Información, presentan diversas guías para la implementación del mismo, sin embargo, entre las principales se tiene:

- **Estándar ISO/IEC 27000:** Al respecto Integra (2018) indica que:

Es una norma que define de qué manera se debe implantar un Sistema de Gestión de la Seguridad de la Información en una empresa u organización. Su implantación ofrece a la organización o empresa la ventaja de proteger su información de la forma más fiable posible (p.1).

Este estándar es el más utilizado por las empresas y está basado en cumplir con el objetivo de la triada de la CID, también, cuenta con un conjunto de normas dedicadas y orientadas a controlar ciertos parámetros específicos de la SGSI, los cuales, se detallan en la Tabla 5 presentada a continuación:

Tabla 5. Estándares de la familia ISO

ISO 27000	Esta estandarización contiene las definiciones y los términos que se utilizan durante toda la serie 27000.
ISO 27001	Es la norma principal de toda la serie, incluye todos los requisitos del Sistema de Gestión de Seguridad de la Información en las organizaciones.
ISO 27002	Es un manual de buenas prácticas en la que se describen los objetivos de control y las evaluaciones recomendables en cuanto a la seguridad de la información.
ISO 27003	Es un manual para implementar un Sistema de Gestión de Seguridad de la Información.
ISO 27004	En este estándar se especifican las técnicas de medida y las métricas que son aplicables a la determinación de la eficacia de un Sistema de Gestión de Seguridad de la Información y sus controles.

ISO 27005	Establece las diferentes directrices para la gestión de los Riesgos en la Seguridad de la Información.
ISO 27006	Se trata de una versión revisada de la EA-7/03 (requisitos para la acreditación de entidades).
ISO 27007	Es un manual de auditoría de un Sistema de Gestión de Seguridad de la Información.
ISO 27011	Es una guía de gestión de seguridad de la información específica para telecomunicaciones.
ISO 27031	Es una guía de continuidad de negocio basada en las tecnologías de la información y las comunicaciones. Explica los principios y conceptos de la tecnología de información y comunicación (TIC).
ISO 27032	Es un texto relativo a la ciber-seguridad. Se trata de un estándar que garantiza directrices de seguridad desde la organización ISO.
ISO 27033	Es una norma derivada de la norma de seguridad ISO/IEC 18028 de la red. Esta norma da una visión general de seguridad de la red y de los conceptos asociados.
ISO 27034	Es una guía de seguridad en aplicaciones.

Fuente: ISOTools (2020)

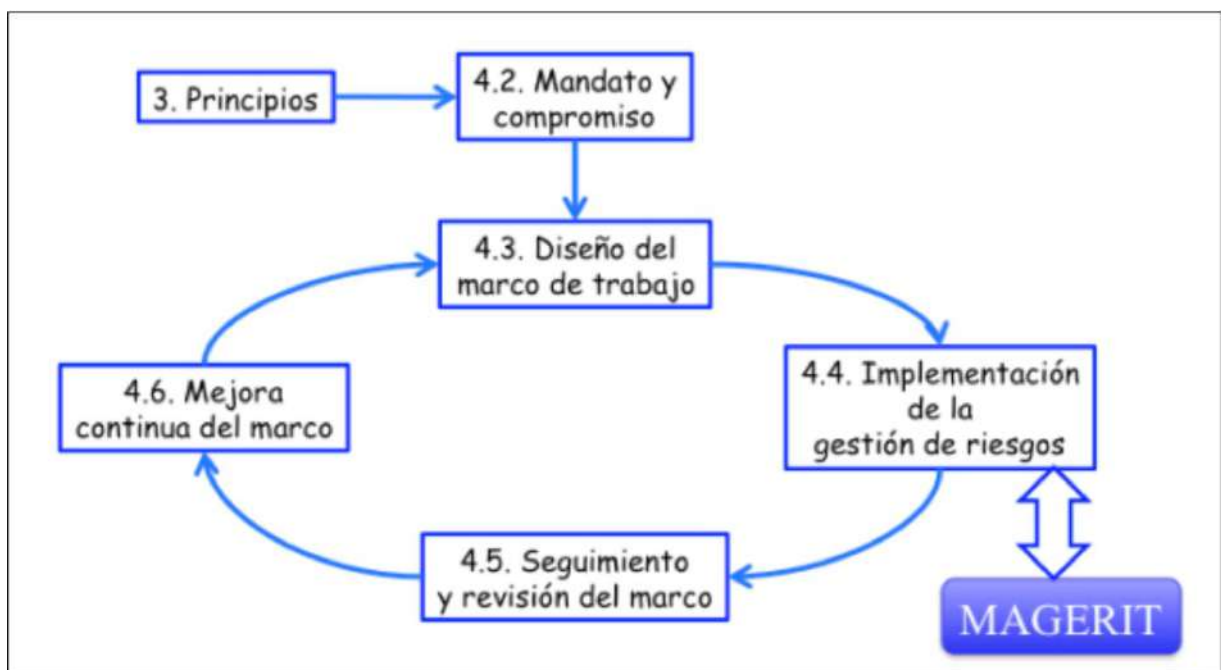
- **Metodología Magerit:** Es el acrónimo de 'Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas', creado por el Consejo Superior de Administración Electrónica (CSAE). El uso de esta metodología es de carácter público, pertenece al Ministerio de Administraciones Públicas (MAP) de España. Se elaboró Magerit porque está dirigido a los medios electrónicos, informáticos y telemáticos. Su uso en la actualidad es frecuente, lo cual, ha dado lugar al origen de ciertos riesgos que se evitan con medidas preventivas para lograr tener confianza en utilizarlos (Gaona, 2013 p.40).

Esta metodología está orientada a medir el riesgo de un sistema de información, y de esta forma recomendar medidas de protección, está basado en el siguiente proceso:

1. Estudiar los riesgos.
2. Análisis de los riesgos.
3. Recomendar medidas de protección.
4. Preparar mecanismos de evaluación.

El método de trabajo de Magerit se visualiza en la Figura 5:

Figura 5. Marco de trabajo metodología Magerit



Fuente: Gaona (2013)

- **ITIL:** En este aspecto Alberola (2013) menciona: “Es una serie de procesos que se agrupan en actividades, y que sirven de guía a las organizaciones, cada organización debe adoptar las mejores prácticas que le pueden beneficiar sin necesidad de considerar la total incorporación de los procesos” (p.13).

Es un proceso orientado a la administración y toma de decisiones en el área de los sistemas de la información y busca mantener un control de vida de los servicios, se basa en tres pilares:

1. Implementación del Proceso.
2. Creación del valor del proceso.
3. Cliente.

En la Figura 6, se visualiza cada uno de los procesos de la metodología ITIL mostrada a continuación:

Figura 6. Procesos de la metodología ITIL



Fuente: Alberola (2013)

Por otro lado, existen equipos de respuesta a incidentes de seguridad (CSIRT). Ante esto WeliveSecurity, (2015) asegura que:

Estos equipos buscan restituir las actividades con el impacto mínimo aceptable para las organizaciones. El crecimiento y la sofisticación de las amenazas informáticas plantean un nuevo panorama en el cual, algunos creen que solo es cuestión de tiempo hasta padecer las consecuencias de algún incidente de seguridad, que esta relacionado con la información. Pero, además de la comunidad de expertos e investigadores, existen equipos dedicados a responder con rapidez ante nuevos riesgos (p.1).

La necesidad de un CSIRT surge debido a tres factores fundamentales: el aumento exponencial de amenazas, generación de leyes para la protección de la información y la implementación de la gestión de riesgos. La implementación de un CSIRT a nivel de *pymes* es quizá una visión muy alejada debido al alto coste que demanda la implementación del mismo, sin embargo, esto no descarta la necesidad.

1.5. Plan de concientización

Para el estudio y la planificación del programa de concientización es necesario realizar un análisis de diferentes estudios como marco de referencia y punto de partida. De acuerdo con el criterio del Instituto Nacional de Ciberseguridad INCIBE (2020b) en su plan de concientización denominado 'Desarrollar cultura en la seguridad' afirma: “Los auténticos protagonistas de la seguridad en las empresas son los empleados, que son los que gestionan y utilizan los dispositivos tecnológicos de nuestra organización para gestionar nuestro principal activo: la información” (p.1). Este plan de concientización está basado en cuatro aspectos:

- 1. Realizar acciones de formación en seguridad para empleados:** Es importante recalcar la formación en cultura de ciberseguridad a los colaboradores de las empresas.

Tradicionalmente la seguridad de la información en las organizaciones se ha entendido como un gasto que no aporta valor al negocio. Por lo que, muy difícil ver el retorno de la inversión en medidas que no se perciben como productivas. Hasta ahora, la formación en materia de seguridad ha tenido un protagonismo casi nulo en los planes de formación de las empresas. Y si se llega a abordar, ésta se realiza de manera puntual o a un grupo reducido de empleados (INCIBE, 2020b, p.5).

El estudio planteado menciona la importancia de establecer un plan de concientización a todo el personal de una empresa, además pone en manifiesto la importancia, y en el caso de ciertos países, la formación en temas de seguridad de la información como una obligación por parte de la empresa. Estas capacitaciones están orientadas a dos ámbitos:

- a) Personal Técnico:** Es el personal que más necesita de la formación tanto teórica como práctica orientada a un grado de especialización. Se recomienda

que los administradores de los sistemas mantengan una formación constante con temas orientados a la ciberseguridad.

b) Usuarios Finales: La importancia de la capacitación a los usuarios finales se basa en que, al no mantener este personal concientizado, incurre en situaciones de riesgo a la organización. Esta capacitación esta orientado a la protección de datos de carácter personal a fin de disminuir el nivel de riesgo.

2. Establecer políticas, normativas y procedimientos de seguridad: En este aspecto “Los conocimientos adquiridos en materia de seguridad por parte del personal encargado de definir cómo se pn hacer las cosas, se plantea traducirlos en diferentes procedimientos y protocolos de actuación a seguir dentro de la organización” (INCIBE, 2020b, p. 10). Todo procedimiento estara documentado por cada etapa de desarrollo, a fin de tener un manual de cómo se trata los datos en una forma organizada y definida.

3. Supervisar que se cumplen las buenas prácticas en seguridad: Establecer estos parámetros admite que “la formación y la normalización de los protocolos de trabajo en nuestra empresa forman parte de los controles preventivos orientados a mejorar el nivel de seguridad de la organización” (INCIBE, 2020b, p. 12).

Al tener establecidas las normas y políticas de trabajo se mantiene un seguimiento constante de que son ejecutadas. Por lo que, se asigna un responsable o responsables mediante un comité representado por una dirección, para mantener un correcto uso de los recursos tecnológicos.

4. Realizar acciones de sensibilización y concienciación en seguridad para empleados: Al respecto de la concientización sea cual sea nuestro negocio, es importante que la cultura de la seguridad sea una de las bases de la filosofía de la empresa. Por este motivo, es fundamental que la Dirección se asegure de la implicación de todos los empleados (INCIBE, 2020b, p.14).

Cada usuario miembro de la organización al formar parte fundamental de la misma mantiene una formación constante acerca de los riesgos informáticos, donde se recomienda que los empleados no necesitan formación de seguridad en el sentido tradicional, sino información sobre seguridad de manera dinámica y adaptable a través de entornos web (INCIBE, 2020b).

Los temas a concientizar por parte del plan de INCIBE (2020b) están orientados a:

- Uso seguro de redes wifi.
- Uso seguro del correo electrónico.
- Prácticas de navegación segura.
- Identificación de virus y *malware*.
- Gestión de contraseñas.
- Clasificación de la información.
- Borrado seguro de la información.
- Uso de dispositivos USB.
- Seguridad en dispositivos móviles.
- Uso de programas de mensajería instantánea.
- Riesgos de las redes sociales.
- Técnicas de ingeniería social.

Por otra parte, se hace análisis del Plan de sensibilización en seguridad de la información, desarrollado por el Ministerio de Agricultura y Desarrollo Rural de Colombia en el año 2017, el cual, consta de las siguientes temáticas:

- Concepto de seguridad de la información.
- Qué es un riesgo de seguridad de la información.
- Normativa ISO27001 de gestión de seguridad de la información.
- Cómo está estructurado el sistema de gestión de seguridad de la información
- Quienes son los actores del sistema de gestión de seguridad de la información (plan de sensibilización).

Dentro de este plan de concientización se pretende además, conocer los procedimientos dentro de cada sistema de gestión de seguridad, para llegar a este objetivo se establece las fases detalladas a continuación:

- Explicación del procedimiento de clasificación y etiquetado de información.
- Explicación del procedimiento de Acceso a áreas seguras.
- Metodología de gestión de riesgos y su anexo para identificación de riesgos de seguridad (plan de sensibilización).

Dentro de estas fases se explica las amenazas más comunes conocidas como son: *Phishing*, *Ramsonware* y robo de identidad. El plan de concientización está planteado por una cantidad de actividades a fin de obtener un dinamismo y mejor captación del personal a capacitarse, entre las principales actividades se tiene:

- Campaña de sensibilización.
- Charlas y conferencias.
- Cursos.
- Concursos.
- Mensajes de correos electrónico.
- Publicaciones en pantallas.
- Elementos físicos de recordación.

Al concluir el plan plantea realizar una evaluación mediante un formulario electrónico a fin de validar el impacto y el nivel de aprendizaje y concientización generado en cada uno de los participantes del plan de concientización.

CAPÍTULO II. DISEÑO METODOLÓGICO

En cuanto a la metodología de la investigación, en esta sección se definen aspectos relacionados a la caracterización de las *pymes*, el diseño del proyecto es cuasi experimental con el uso de Pres- Test y Pos- Test. El enfoque es de tipo cuantitativo, la modalidad inductivo-deductivo. Sumado a ello, se describen las técnicas y los instrumentos utilizados, de la misma forma se exponen aspectos relacionados con la muestra.

2.1. Contextualización de las pequeñas y medianas empresas (*pymes*) en la ciudad de Puyo

En Ecuador las pequeñas empresas son el eje de la economía, a través de ellas se generan empleos. La ciudad del Puyo es la capital de la Provincia de Pastaza caracterizada por segmentos de turismo, comercio, agricultura, la industria maderera y petrolera. Además, de poseer abundantes recursos naturales, también, es el centro de grandes movimientos económicos. Es así que, por medio de los distintos barrios y su casco comercial, la población ha dedicado el comercio a diversos productos de alto consumo.

2.1.1. Justificación de las *pymes*

Muchas de las organizaciones comerciales en el cantón el Puyo no tienen bases sólidas en materia de ciberseguridad. Es decir, no toman en cuenta de forma profunda el poseer un sistema de seguridad informática y cómo gestionar dichos datos que cabe señalar, son sensibles. La inversión que realizan los altos mandos de una empresa en ciberseguridad es escasa y son las organizaciones pequeñas las más proclives a ser vulnerabilidades, debido a no concientizar sobre los ciberataques. Más bien, lo perfilan como un gasto poco rentable, y desconocen sobre los beneficios al respecto de la protección de información sensible e incluso actividades como la agricultura, ganadería o turismo dejaron de ser empíricas, para entrar en la era digital.

Las *pymes* en el cantón han cambiado la forma tradicional de negociar, para sumergirse en las redes. Dicho empuje requiere de ser dirigido en materia de ciberseguridad, por un elevado riesgo de exponer información vital de la organización, sin ser conscientes de ello. Por lo que, la información deja de ser segura, no solo a nivel local, sino también, mundial. Crear una cultura de seguridad de la información sensible abre el camino hacia un entorno adaptado a las nuevas tecnologías, que como resultado atrae inversiones y al estar en un ambiente

digital seguro, las transacciones que se ejecutan son de forma masiva. La confianza en los productos y servicios hace que las *pymes* sean canales de acceso a una economía más sólida en la ciudad del Puyo.

2.2. Diseño Metodológico

2.2.1. Diseño de la investigación

El diseño o tipo de investigación permite trazar un plan para seleccionar procesos, escenarios o grupos en la recolección de datos. Para el presente estudio, el diseño es cuasi experimental. Al respecto, Shaughnessy, Zechmeister y Zechmeister (2007) indican que: “Los cuasi experimentos comprenden cierto tipo de intervención o tratamiento y permiten realizar una comparación, pero carecen del grado de control (...) la falta de aleatorización es el sello distintivo” (p.370). Dicho de otro modo, la selección de los grupos para esta investigación no fue al azar, debido a que los sujetos o grupos ya estaban formados y están sujetos a la experimentación mediante el Pre- Test y Pos- Test.

2.2.2. Enfoque de la investigación

La investigación es cuantitativa, de modo que las variables analizadas se miden. Dicho enfoque refiere a “Estudios en los cuales los hallazgos son principalmente el producto de resúmenes y análisis estadísticos (...) produce resúmenes verbales de los hallazgos de investigación” (Shaughnessy, Zechmeister & Zechmeister, 2007, p. 44). Es decir, las mediciones cuantitativas arrojan información precisa.

Por otra parte, la investigación cuantitativa “usa la recolección de datos para probar hipótesis, con base en la medición numérica y el análisis estadístico, para establecer patrones de comportamiento y probar teorías” (Hernández, Fernández & Baptista, 2010, p. 4). En el presente estudio, este enfoque se utiliza para establecer hipótesis con la finalidad de diseñar un plan y comprobarla. Análogamente, las variables entran a una medición y se las examina mediante métodos estadísticos, hasta llegar a conclusiones relacionadas con la hipótesis.

2.2.3. Modalidad de la investigación

La modalidad de este proyecto de investigación es, inductivo- deductivo. A juicio de Prieto (2017) menciona que: “El método inductivo se desarrolla con base en hechos o prácticas particulares, para llegar a organizar fundamentos teóricos. En contraste, el método deductivo basa sus cimientos en determinados fundamentos teóricos, hasta llegar a configurar hechos

o prácticas particulares” (p.11). Por esta razón, la investigación es inductiva, para conocer la cultura de protección de datos sensibles se observó que las *pymes* son altamente vulnerables a delitos informáticos. Análogamente, se utilizó el razonamiento deductivo y la lógica para llegar a una conclusión acerca de la cultura de protección de datos en las *pymes*, una vez que se sometió a prueba las variables.

2.2.4. Técnica de la investigación

En el presente estudio, se utiliza como técnica la observación científica, descrita más adelante, y como instrumentos la encuesta dirigida a las *pymes* de la ciudad de Puyo para la obtención de los datos referentes a un diagnóstico situacional. Así también, se aplicó un cuestionario estructurado (Pre-test, Post-test) para evaluar la eficacia del programa de concientización en seguridad de información desarrollado y ejecutado a los participantes de las *pymes*.

Observación científica

Esta técnica permite explorar directamente el fenómeno de estudio. Ante esto Marradi, Archenti y Pionavi (2007) indican que: “Es el modo de establecer algún tipo de contacto empírico con los objetos/sujetos/situaciones de interés a los fines de su descripción, explicación y comprensión” (p.191). La observación científica “es más bien intencional, tiene dirección y sentido. Se observa siempre con un propósito, dado por la teoría 'desde la que' se observa” (Sánchez, 2014, p. 88). En resumen, este método de recolección de datos admite la exploración del conocimiento en cuanto a ciberseguridad en las *pymes* y actúa de manera sistemática.

2.2.5. Población y Muestra

En este estudio se contó con una base de datos de 50 *pymes* de la ciudad de Puyo, mismas que están legalmente constituidas y registradas en la Cámara de Comercio de Puyo. La población está constituida por las personas que laboran en las *pymes* y están vinculadas al uso de plataformas virtuales en pro de la organización y todas sus transacciones.

En el desarrollo de la presente investigación, se cuenta con 20 *pymes* y se selecciona un grupo de trabajo de 45 personas para el desarrollo de la intervención experimental (Programa de concientización).

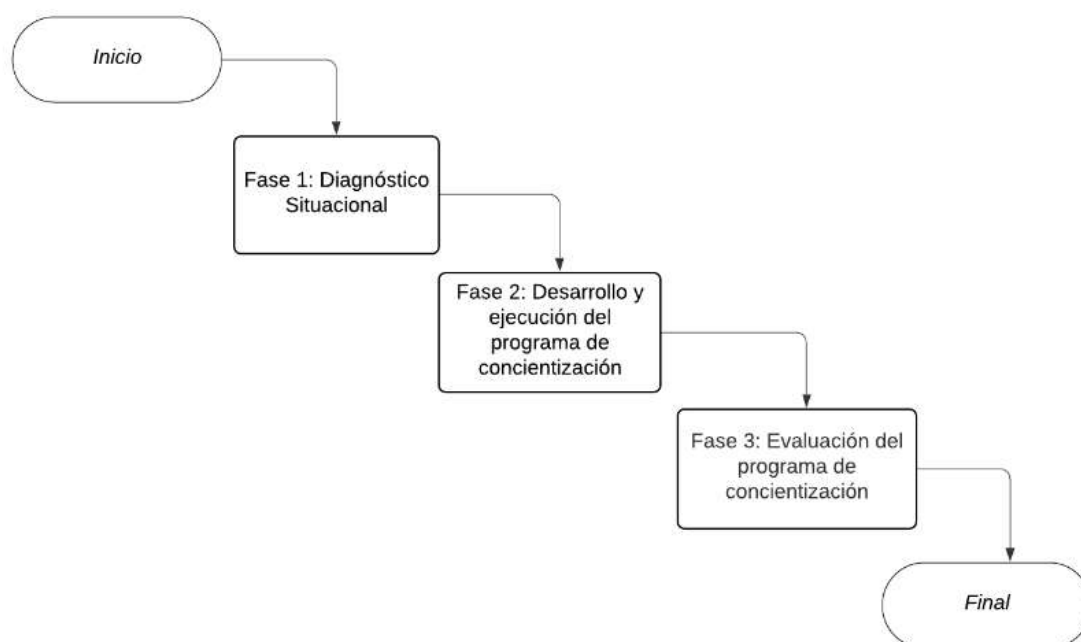
2.3. Método de Desarrollo

Para esta investigación se utiliza como metodología en el diseño del programa de concientización, un modelo estructurado en fases.

2.3.1. Aproximación a la solución

La aproximación a la solución del presente proyecto de investigación está compuesto por diferentes elementos, cuya característica principal es que, sigue una secuencia. Cada vez que finaliza una etapa se obtiene un documento o producto final, que revisado, validado y probado, sirve como aproximación y documentación de partida para la siguiente. Dicho de otro modo, este estudio es un diseño en secuencias (Ver Gráfico 1).

Gráfico 1. Aproximación a la solución



Fuente: elaboración propia

El trabajo de investigación sustenta su metodología en fases, a fin de llevar un adecuado proceso dentro del programa de concientización a desarrollar. Permite desarrollar el programa de concientización en seguridad de información, en 3 fases. La primera fase del modelo, se denomina estudio situacional o de diagnóstico (Diagnóstico situacional); la

segunda fase refiere al desarrollo del programa de concientización; y finalmente, en la tercera fase se ejecuta la evaluación del programa de concientización, cada una de ellas se detallan a continuación:

Fase 1: Estudio situacional o de diagnóstico

El análisis situacional o de diagnóstico se ejecuta con el objetivo de saber en qué situación se encuentra una organización en un momento dado, también, “determina la adecuada combinación de recursos para afrontar la solución de un problema o necesidad donde se obtiene el máximo beneficio al menor costo y riesgo posible” (Remuzgo, 2005, p. 2). En pocas palabras, es un estudio del medio en el que se desarrolla la empresa, asimismo, se toma en consideración los factores internos y externos que tienen injerencia en como se muestra la empresa en su medio. Por lo tanto, mediante este diagnóstico se conoce en qué estado se encuentran las *pymes* en la ciudad del Puyo en cuanto a cultura de seguridad de la información (ciberseguridad), y todos los factores que influyen en las mismas. Para este análisis se utilizó como instrumento la encuesta (formulario electrónico) a 5 *pymes*, descrita a continuación:

Encuesta

En referencia a la encuesta, esta es una de las técnicas más utilizadas en investigaciones, la particularidad de la encuesta es que realiza a todos los entrevistados, las mismas preguntas, en el mismo orden, y en una situación social similar. La realización de las mismas preguntas a todas las administraciones implica un mayor control sobre lo que se pregunta (Díaz, 2001, p. 13). Mediante este método se realiza una indagación sistemática de los datos requeridos de las *pymes* en cuanto a ciberseguridad. Para ello, se estructura una encuesta (formulario electrónico) de 10 preguntas donde se evalúa la cultura de protección de datos sensibles que tienen las *pymes*.

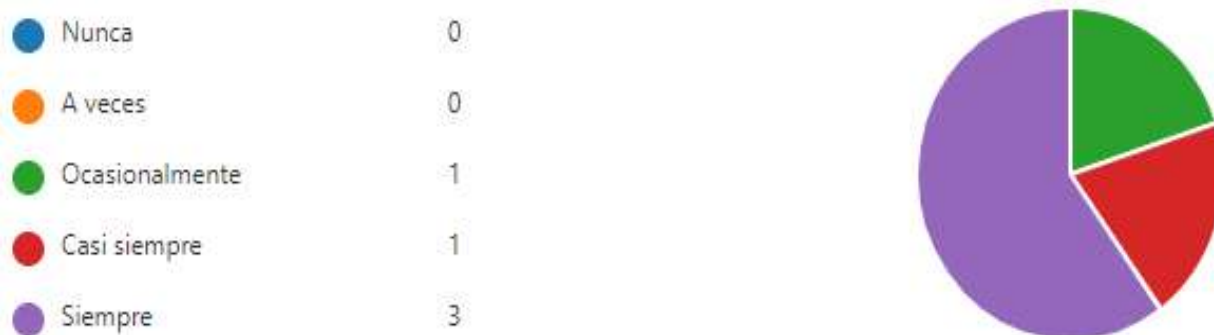
De las 10 preguntas, un grupo están orientadas a cambios de claves personales, y otro grupo de preguntas están direccionadas de manera general al conocimiento que tienen las *pymes* acerca de los diferentes ciberataques del que serían víctimas. Con esta encuesta se mide el grado de satisfacción o rechazo del problema de investigación mediante una escala tipo Likert de 5 opciones, para evaluar la opinión y aptitud de las personas en cuanto a la cultura de protección de datos. Donde a mayor puntaje, es decir, 5 puntos hay mayor cultura de

protección de datos y a menor puntaje, es decir, 1 punto es equivalente a baja cultura de protección de datos (Ver anexo B).

La encuesta de diagnóstico situacional está centralizada en 5 *pymes* estratégicas debido a su ubicación geográfica dentro de la ciudad del Puyo, así como también, por su actividad laboral. Todo ello con el objetivo de tener una mejor apreciación acerca de los riesgos informáticos a los que están sujetos las *pymes* por desconocimiento. A continuación, se expone el análisis e interpretación de los siguientes resultados:

Pregunta 1: ¿Hace uso de plataformas virtuales para promocionar su producto o servicio?

Figura 7. Marketing Digital



Fuente: elaboración propia

Análisis e interpretación

Como se evidencia en la Figura 7 los resultados de la encuesta muestran que 3 de cada 5 *pymes* hacen uso de plataformas digitales para promocionar su producto o servicio. Esto indica la acogida de la tecnología para pequeños y medianos comerciantes.

Pregunta 2: ¿Hace uso de plataformas virtuales para realizar movimientos bancarios como: cobros o pagos de un producto o servicio de su empresa?

Figura 8. Comercio Electrónico



Fuente: elaboración propia

Análisis e interpretación

Como se muestra en la Figura 8, todos los participantes hacen uso de plataformas virtuales con diferente periodicidad, para realizar movimientos bancarios dentro de las *pymes* donde laboran. Esto significa que, si se da un manejo inadecuado de dichas plataformas, estas son víctimas de fraudes electrónicos.

Figura 9. Banca en línea

Pregunta 3: ¿Cree usted que las plataformas bancarias son seguras para las diversas



transacciones que realiza su empresa?

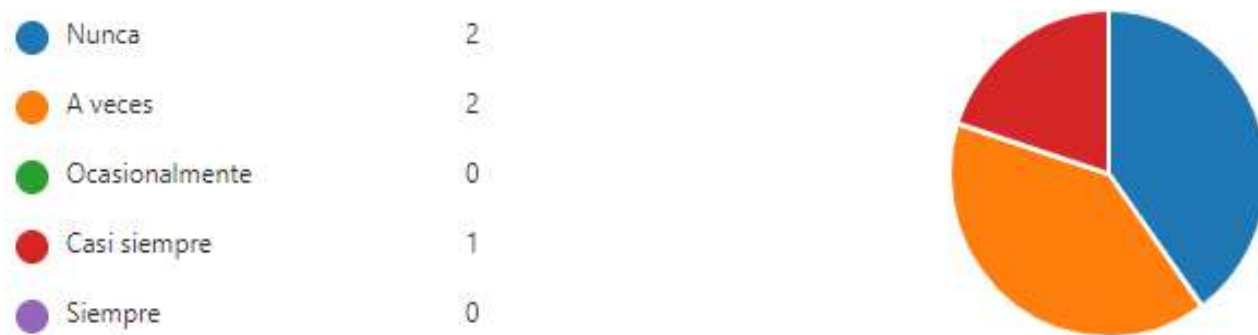
Fuente: elaboración propia

Análisis e interpretación

De acuerdo con la Figura 9 se manifiesta que, 3 de 5 *pymes* consideran que casi siempre las plataformas bancarias son seguras para realizar las diversas transacciones. Esto indica que muchas de las personas no mantienen presente los riesgos y vulnerabilidades en una transacción bancaria o riesgos de suplantación de identidad, aunque esta se muestre segura ante los ojos de la posible víctima.

Pregunta 4: ¿Ha sido víctima o ha escuchado de algún delito informático como: suplantación de identidad, *phishing*, *ransomware*, secuestro de información, robo de información, ¿otros?

Figura 10. Delitos informáticos



Fuente: elaboración propia

Análisis e interpretación

Como muestra la Figura 10 los participantes encuestados de las *pymes*, al no haber sido víctimas de un delito informático carecen de un conocimiento de las técnicas más utilizadas para fraudes electrónicos como: suplantación de identidad, *phishing*, *ransomware*, secuestro de información, robo de información, otros.

Pregunta 5: ¿Tiene conocimiento acerca de fraudes electrónicos por ingeniería social (manipulación para el robo de información confidencial del usuario)?

Figura 11. Fraudes electrónicos



Fuente: elaboración propia

Análisis e interpretación

Como se evidencia en La Figura 11, los participantes carecen de un mayor conocimiento sobre fraudes electrónicos por la técnica más utilizada que es la de ingeniería social (manipulación para el robo de información confidencial del usuario), y en esta interrogante se evidencia el desconocimiento de la misma, como un riesgo latente para dichos usuarios.

Pregunta 6: ¿Considera usted importante cambiar las contraseñas de sus plataformas electrónicas (Correo, redes sociales, celular, cajero automático, ¿Banca en línea, aplicaciones móviles bancarias, otros)?

Figura 12. Administración de contraseñas



Fuente: elaboración propia

Análisis e interpretación

Se muestra en la Figura 12 los participantes consideran importante cambiar las contraseñas de sus plataformas electrónicas (Correo, redes sociales, celular, cajero automático, Banca en línea, Aplicaciones móviles bancarias, otros). Esto indica que hay cultura de protección de confidencialidad de los datos con respecto a esta interrogante, sin embargo, es importante generar una concientización acerca de robustez de contraseñas.

Pregunta 7: ¿Usted almacena las contraseñas de las plataformas virtuales que utiliza de forma física (papel), o digital: navegador de internet, lo guardan terceros, programa externo, ¿otros?

Figura 13. Almacenamiento de contraseñas



Fuente: elaboración propia

Análisis e interpretación

En la Figura 13 indica que, en referencia a si los usuarios miembros de las *pymes* almacenan las contraseñas de las plataformas virtuales que utilizan, 3 de cada 5 usuarios almacenan sus contraseñas sin importar el riesgo que esta implica. Se considera imperativo en base a este análisis generar una concientización acerca de las amenazas presentes en un mal almacenamiento de claves.

Pregunta 8: ¿Ha instalado algún programa de antivirus en el ordenador de su trabajo (computadora)?

Figura 14. Software de antivirus



Fuente: elaboración propia

Análisis e interpretación

De acuerdo con la Figura 14, los resultados indican que, 3 de cada 5 usuarios a veces han instalado algún programa de antivirus en sus ordenadores, sin conocer el riesgo que sus equipos sean infectados por algún virus o *malware*. Evita salvaguardar la privacidad de sus datos, así como, la integridad de los mismos.

Pregunta 9: ¿Hace uso de programas piratas (software de tipo comercial con licencia adulterada) dentro de su empresa?

Figura 15. Software legal



Fuente: elaboración propia

Análisis e interpretación

La Figura 15 evidencia un correcto uso de programas con licenciamiento, esto disminuye el riesgo de ataques informáticos bajo la modalidad de *cracks* o troyanos. Sin embargo, el presente estudio considera importante enfocar una cultura de concientización acerca de la diferencia entre un *software* con licencia original y un pirata, además de cómo distinguirlos.

Pregunta 10: ¿Usted maneja información sensible de su empresa o trabajo en su dispositivo móvil?

Figura 16. Dispositivos móviles



Fuente: elaboración propia

Análisis e interpretación

Como se evidencia en la Figura 16 los resultados indican que, 4 de cada 5 usuarios, manejan información de la organización en sus dispositivos móviles, y esto amenaza la privacidad de la información digital sensible de la empresa ante un riesgo de robo o pérdida del equipo de comunicación. Con dicho resultado se observa la necesidad de inculcar en los usuarios la cultura de protección de datos.

Análisis general de resultados de diagnóstico situacional

Los resultados del diagnóstico situacional realizado a las *pymes* indican que los participantes hacen uso de plataformas virtuales para promocionar el producto o servicio que ofertan, del mismo modo realizan movimientos bancarios a través de dichas plataformas e indican bajo su perspectiva que las mismas son seguras. Además, los encuestados aseguran no haber sido víctimas de delitos informáticos, así también, carecen de mayor conocimiento sobre fraudes electrónicos en las diferentes formas de realizarlo. Por otro lado, los participantes indican la importancia de cambiar las contraseñas de las plataformas electrónicas que usan, pero el almacenamiento de la misma, lo hacen de forma que implica riesgo. Del mismo modo, los encuestados no conocen la importancia de usar antivirus en sus ordenadores a pesar de conocer cómo utilizarlos de forma adecuada.

Tras los resultados de la encuesta general realizada a los usuarios miembros de las *pymes* seleccionadas para el estudio de diagnóstico situacional, se evidencia la necesidad de crear una cultura de concientización acerca de ciberseguridad dentro de las *pymes*, mediante un programa de concientización que abarque los contenidos (temáticas) que son deficientes en los participantes, mismos que se presentan a continuación:

- Ataques y delitos informáticos.
- Técnicas de ataques informáticos más utilizados por los ciberdelincuentes.
- Correcta administración de contraseñas.
- Riesgos del uso de un software con licenciamiento ilegal.
- Técnicas de protección ante incidentes.

Una vez culminada la Fase 1 de diagnóstico situacional, procede a la siguiente, en donde cada una de las temáticas anteriormente mencionadas se desarrollan en la Fase 2 que se describe a continuación:

Fase 2: Desarrollo y ejecución del programa de concientización

Una vez ejecutado el diagnóstico situacional, se procede al desarrollo y ejecución del programa de concientización en base a los resultados obtenidos. Frente a esto, la Organización de los Estados Americanos OEA (2015) afirma: “Educar a la gente acerca de la seguridad cibernética es de suma importancia para la creación de una cultura de seguridad

cibernética. La conciencia es el primer paso hacia el desarrollo de una ciudadanía con inteligencia cibernética” (p.8). Es decir, se busca la sensibilización sobre ciberseguridad en las *pymes*, crear conciencia e influir en la conducta de las mismas. Para ello, se requiere de un mensaje memorable, que atraiga a las *pymes*, de modo que, se implante un ambiente seguro y se adapten a la propia ciberseguridad de sus datos y aliarse en la lucha contra posibles atacantes.

El programa de concientización se realizó a través de la plataforma *Zoom* (ver Anexo H), se creó un portal *Web* (ver Anexo H) con los detalles de las temáticas e información relevante a desarrollar durante el programa de concientización, además, de un *Fanpage* (ver Anexo F), invitación a las personas de las pequeñas empresas de la ciudad de Puyo (Ver Anexo F).

Cabe señalar que, el programa tuvo el aval de la Cámara de Comercio de Pastaza (Ver Anexo D). Dicho programa de concientización en seguridad de información para pequeñas empresas en la ciudad de Puyo fue ejecutado en cinco semanas, cuyas actividades se detallan, a continuación, en la Figura 17 mediante el Diagrama de Gantt:

Figura 17. Cronograma de Actividades



Fuente: elaboración propia

Cabe resaltar que, la ejecución del programa parte de la encuesta de diagnóstico situacional, cuyos resultados permitieron el desarrollo de una temática previamente definida, misma que, se encuentra detallada en la Fase 1. La investigación comprende un programa de concientización en seguridad de información impartida a 45 participantes de las *pymes* de la ciudad de Puyo. La Figura 18 muestra el plan del programa de concientización en seguridad de la información, mismo que, contiene las temáticas indicadas anteriormente. Dicho programa se aprecia con mayor detalle en el Anexo C.

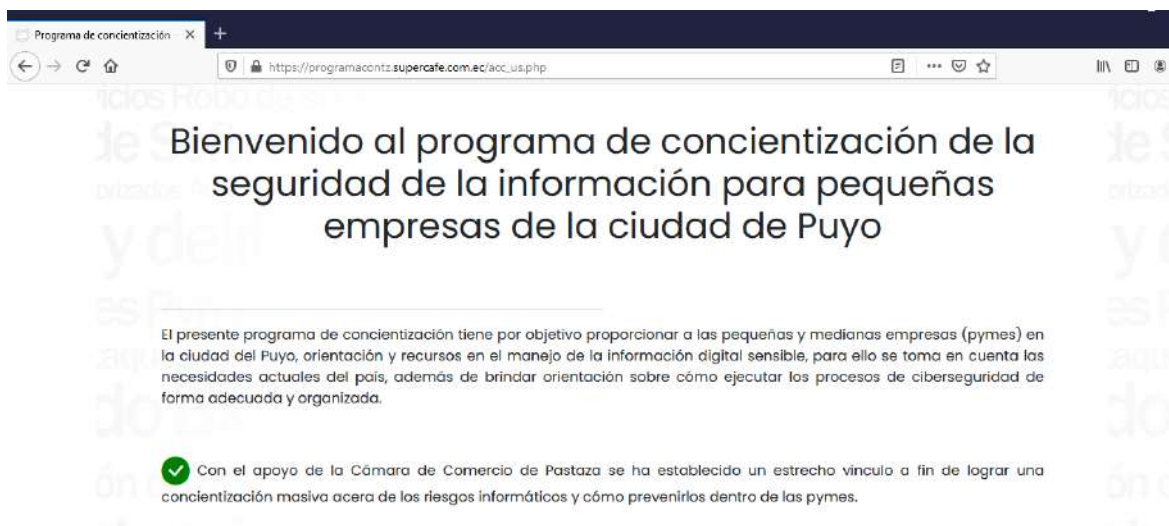
Figura 18. Plan de concientización seguridad de la información



Fuente: elaboración propia

Por otro lado, en la Figura 19 se aprecia el portal *Web* creado para el programa de concientización en seguridad de información que tiene como *link* de ingreso el siguiente enlace: https://programacontz.supercafe.com.ec/acc_us.php

Figura 19. Portal Web del programa de concientización



Fuente: elaboración propia

Del mismo modo se generó un *Fanpage* en *Facebook* del programa de concientización en seguridad de información, donde se creó contenido para publicitar el mismo y tiene el siguiente *link* de ingreso: <https://www.facebook.com/Programa-de-concientizaci%C3%B3n-de-la-seguridad-de-la-informaci%C3%B3n-107639984717059>

Figura 20. Difusión publica del programa de concientización mediante *FanPage*

Fuente: elaboración propia

Tras ejecutar el programa de concientización, es necesario proceder a la evaluación del mismo, todo ello se detalla en la Fase 3, a continuación:

Fase 3: Evaluación del programa de concientización

Para evaluar la propuesta del programa de concientización en seguridad de la información a desarrollar en el presente proyecto de titulación, se lleva a cabo un estudio Pre-Test, Post-Test. En referencia a ello, Santana (2015) menciona que:

En este diseño de investigación se utiliza un solo grupo, al cual, se le aplica un pretest, luego se procede a la intervención y finalmente, se analizan los resultados de la aplicación a través de un posttest. Ambos instrumentos, tanto el pretest como el posttest son los mismos, pero aplicados en momentos diferentes (p.14).

Para dicha evaluación, se desarrolló el instrumento para validar el programa de concientización, es decir, el cuestionario estructurado (Pre-test, Post-Test) instrumento que se detalla en el Anexo E, sumado a un Acuerdo de confidencialidad (Ver anexo A).

Del mismo modo, los datos obtenidos tras la evaluación se analizan mediante el Sistema de Análisis Estadístico SPSS versión 21. Cabe señalar que, el pretest se evalúa días antes de la implementación del programa de concientización y una vez finalizado el programa se procede a la toma del post-test. A continuación, se describe el instrumento utilizado:

Cuestionario estructurado

Al respecto de los cuestionarios Hernández, Fernández y Baptista (2010) aseguran: “Tal vez sea el instrumento más utilizado para recolectar los datos, consiste en un conjunto de preguntas respecto de una o más variables a medir” (p.217). Para validar el programa de concientización se realiza un cuestionario estructurado, es decir, un listado de preguntas que serán formuladas al participante tal y como están redactadas y en el orden en que aparecen (...) es el instrumento para recoger y agregar información proveniente de un gran número de individuos o unidades muestrales de otro tipo (por ejemplo: Empresas) (Hernández, 2001, p. 242). De modo que, para este estudio se ejecuta un pre-experimento que diferencie el dominio o no de los contenidos (pasa-falla; éxito-no éxito) y mostrar la eficacia del programa de concientización desarrollado.

Método de evaluación mediante Pre-Test y Post-Test

El Pre-test y Post-test fue elaborado según las definiciones y teorías que se encuentran en el programa de concientización en seguridad de la información descrito en la Fase 2. Dicho cuestionario evalúa mediante una escala tipo Likert de 5 opciones, donde cada número indica lo siguiente:

1. Totalmente en Desacuerdo
2. En Desacuerdo
3. Ni de acuerdo, ni desacuerdo
4. En Acuerdo
5. Totalmente de Acuerdo

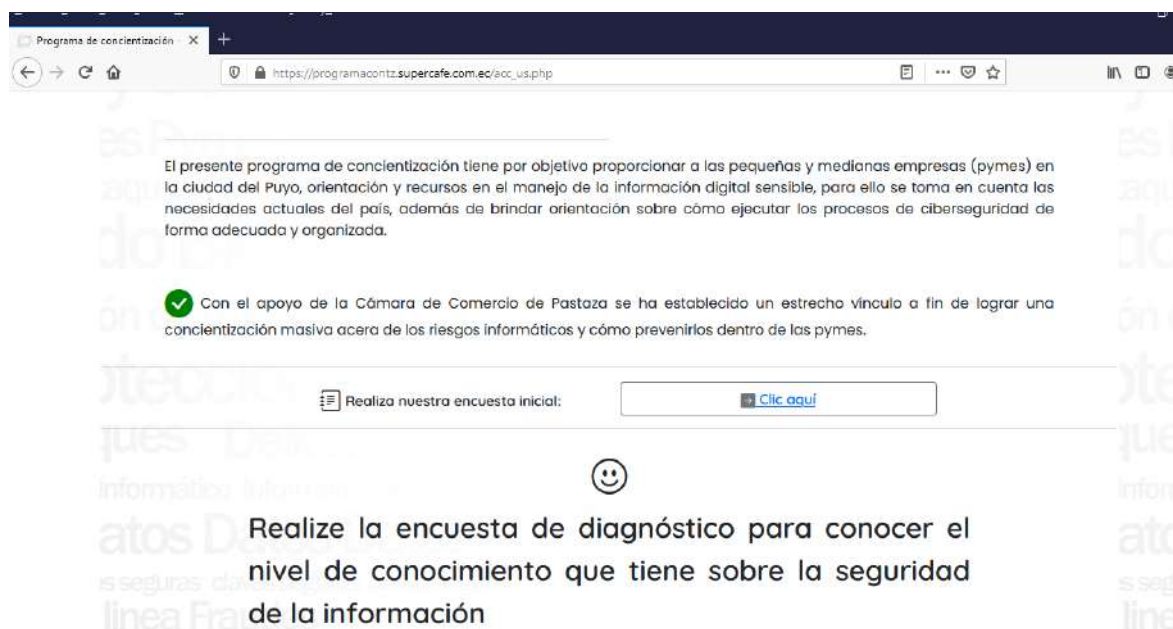
Cabe resaltar que, las preguntas son tomadas de la teoría exhibida en el programa y que fue expuesta durante la capacitación, las interrogantes se presentan a continuación:

- 1) Un ataque informático es un intento desorganizado no intencionado causado por una persona para causar daño o problemas a un sistema informático o red.
- 2) Los delitos informáticos son todas aquellas acciones ilegales, delictivas, antiéticas o no autorizadas que hacen uso de dispositivos electrónicos e internet, a fin de vulnerar, menoscabar o dañar los bienes, patrimoniales o no, de terceras personas o entidades.
- 3) El ciberataque de ingeniería social consiste en engañar al usuario para que crea que un administrador de sistema legítimo, de un banco o del gestor de sistema de la empresa para la que trabaja les pide su contraseña, pero en realidad es un hacker quien lo hace.
- 4) El ransomware es un sistema criminal creado con el objetivo de ganar dinero. Este se instala a través de enlaces engañosos incluidos en un mensaje de correo electrónico, mensaje instantáneo o sitio web.
- 5) Para crear contraseñas seguras es recomendable usar información personal que incluya palabras relacionadas con su nombre, nombres de familiares o mascotas.
- 6) No es necesario crear contraseñas más largas, que tengan al menos 8 caracteres. La probabilidad indica que es más fácil descifrar las contraseñas más largas.

- 7) En un software sin un licenciamiento adecuado, se accede a las actualizaciones del fabricante. Y si este no se actualiza, la vulnerabilidad es corregida automáticamente.
- 8) El software pirata o crackeado, viene con código malicioso escondido que es aparentemente inocente, pero en el interior de su código ejecuta acciones maliciosas.
- 9) Una red empresarial de acuerdo a su tamaño contara con *Firewall*, *Virtual Private Network* (VPN), *Surf Protection*, *Spam Filter* y Antivirus.
- 10) Los equipos de respuesta a incidentes de seguridad (CSIRT) buscan restituir las actividades con el impacto mínimo aceptable para las organizaciones ante un ciberataque.

La Figura 21 muestra la toma del Pre-Test a los participantes del programa; al ingresar al portal *Web* despliega la indicación de llenar la encuesta.

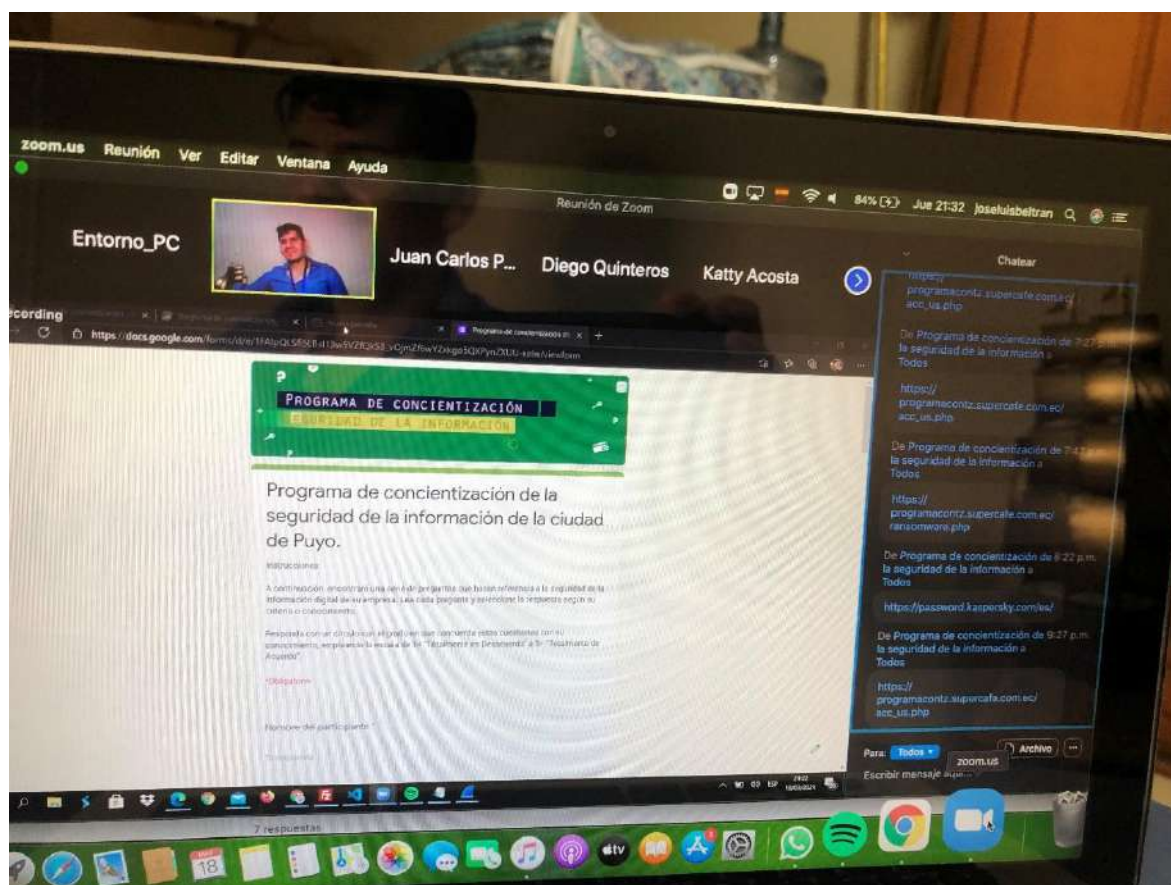
Figura 21. Pre-Test visto desde el portal *Web*



Fuente: elaboración propia

Después de ejecutado el programa de concientización en seguridad de la información mediante la plataforma *Zoom* (Ver Anexo H), acto seguido se procedió a la evaluación de la intervención, a través del Post-Test como se muestra en la Figura 22.

Figura 22. Evaluación del programa mediante Post-Test



Fuente: elaboración propia

Una vez llevado a cabo el programa de concientización, los resultados que arrojó la evaluación del mismo, se describen en el Capítulo III.

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

Tras ejecutar el Pre-Test y Post-Test, los datos obtenidos se tabularon e interpretaron mediante el Sistema de Análisis Estadístico SPSS versión 21; es un *software* estadístico que posee atributos de análisis de datos e ilustraciones gráficas para el Pre-Test y Post-Test.

Para ello, se realiza un análisis descriptivo y análisis inferencial con los datos obtenidos en el cuestionario.

3.1. Procesamiento de Datos Pre- Test y Post- Test

El Pre-Test y Post-Test es la herramienta encargada de la medición en cuanto a los conocimientos de seguridad de la información que poseen los participantes del estudio, dicho instrumento se compone de 10 ítems cuyas preguntas miden el conocimiento y tienen un valor mínimo de 1 punto (Totalmente en desacuerdo) a un valor máximo de 5 puntos (Totalmente en acuerdo) en escala de likert por cada pregunta, referente a las siguientes temáticas: ataques y delitos informáticos, técnicas de ataques informáticos más utilizados por los ciberdelincuentes, la correcta administración de contraseñas, riesgos del uso de un *software* con licenciamiento ilegal y técnicas de protección ante incidentes, con dos preguntas.

En el factor ataques y delitos informáticos, con dos ítems, el *Mín.* = 1 punto y *Máx.* = 5 puntos. En cuanto al factor, técnicas de ataques informáticos más utilizados por los ciberdelincuentes, con dos ítems, el *Mín.* = 1 punto y como *Máx.* = 5 puntos.

En el factor sobre la correcta administración de contraseñas, con dos ítems, el *Mín.* = 1 punto y como *Máx.* = 5 puntos. Seguidamente en el factor de riesgos del uso de un software con licenciamiento ilegal, con dos ítems, el *Mín.* = 1 punto y como *Máx.* = 5 puntos.

Finalmente, en el factor técnicas de protección ante incidentes, con dos ítems, el *Mín.* = 1 punto y como *Máx.* = 5 puntos.

Los datos mostrados en la Tabla 6, corresponden a los 45 participantes que son denominados casos, y obtienen un puntaje por participante a través del cuestionario aplicado antes y

después del programa de concientización, sin embargo, su calificación difiere de acuerdo al grado de conocimiento tanto en el Pre-Test como del Post-Test.

Tabla 6. Tabla de procesamiento de datos del Pre-Test y Post-Test

Casos	Puntaje Pre-Test	Puntaje Post-Test	Casos	Puntaje Pre-Test	Puntaje Post-Test
1	31	32	24	30	31
2	38	35	25	29	33
3	40	36	26	28	31
4	34	34	27	25	29
5	26	34	28	23	31
6	43	32	29	25	27
7	41	29	30	26	35
8	43	32	31	25	33
9	41	31	32	34	33
10	34	30	33	28	32
11	45	33	34	28	34
12	34	36	35	25	36
13	31	33	36	19	34
14	31	32	37	25	34
15	33	34	38	28	34
16	29	32	39	29	36
17	32	33	40	30	35
18	28	33	41	30	34
19	29	34	42	28	29
20	25	31	43	33	34
21	31	35	44	28	33
22	28	35	45	31	33
23	28	31			

Nota: Continúa en la siguiente tabla

Fuente: elaboración propia

3.2. Análisis Descriptivo

A través del análisis descriptivo, permite acercarse a un tipo de aproximación que ayuda en la interpretación del objeto de estudio, por consiguiente, proporciona un enfoque vital en describir las relaciones que suscitan entre los datos.

Las puntuaciones que se indican en la Tabla 7, corresponden a la media aritmética (*M*), la Desviación Estándar (*DT*), el puntaje mínimo (*mín.*), el puntaje máximo (*máx.*) del Pre-Test y el Pos-Test de forma total, aplicado a los participantes del estudio N=45.

Tabla 7. Análisis Descriptivo Pre-Test y Post-Test

<i>Grupo</i>	<i>N</i>	<i>M</i>	<i>DT</i>	<i>Min</i>	<i>Máx</i>
Pre- Test	45	305.111	5,40884	19	45
Post- Test	45	32,8444	2,06657	27	36

Nota: *DT: Desviación Estándar*

Fuente: elaboración propia

Se evidencia, en el Pre-Test que obtiene como valor *Mín.* = 19,00 puntos y como máximo *Máx.* = 45,00 puntos, con una media de *M* = 30,51; y una desviación típica de *DT* = 5,40. Entre la máxima y la mínima puntuación alcanzada por los participantes hay una diferencia de 26 puntos, sin duda, indican el desconocimiento de los participantes en cuanto a temas de seguridad de la información.

Por otro lado, el Post-Test aplicado a los participantes N=45 presenta un valor total *Mín.* = 27,00 puntos y como máximo *Máx.* = 36,00 puntos, con una media de *M* = 32,84 y una desviación típica de *DT* = 2,06. Entre la máxima y mínima puntuación alcanzada hay una diferencia de 9 puntos, esto quiere decir que indica cambios en cuanto al conocimiento de los participantes en temas de seguridad de la información.

3.3. Análisis Inferencial

En esta sección se realiza el análisis inferencial del Pre- Test y Pos- Test.

Pruebas de normalidad

Se realiza la prueba de normalidad según el test de Shapiro y Wilk (1965), con las muestras tanto del Pre-Test como del Post-Test que ayuda a evaluar la normalidad. Recibe un conjunto de datos y realiza la comparación con una distribución normal. Se plantea las hipótesis: Hipótesis nula (H_0): indica que la muestra se ajusta a una distribución normal; y la Hipótesis

alternativa (H_a): indica que la muestra no se ajusta a una distribución normal. Se utiliza un nivel de significancia (alfa) del 0,05.

Tabla 8. Prueba de normalidad Pre-Test y Post- Test

PRUEBAS DE NORMALIDAD PRE-TEST Y POST-TEST			
	Shapiro-Wilk		
	Estadístico	gl	Sig.(p)
Pre-Test	0.930	45	0.009
Post-Test	0.946	45	0.035

Fuente: elaboración propia

La Tabla 8 muestra la prueba de normalidad del Pre- Test y Post- Test, que a través del criterio de decisión se tiene que: si $p \leq 0.05$ se rechaza la hipótesis nula y se acepta la hipótesis alternativa, en cambio, si $p > 0.05$ se acepta la hipótesis nula y se rechaza la hipótesis alternativa. De acuerdo al resultado, se obtiene un $p=0,009$ en el Pre-Test y un $p=0,035$ en el Post-Test, esto quiere decir, las muestras tanto del Pre-Test y Post-Test no se ajustan a una distribución normal. Por lo tanto, el valor p es significativo y se concluye que esta distribución de las muestras es distinta a los de una distribución normal.

Tras realizar el Test de Shapiro-Wilk, mediante las muestras del Pre- Test y Post- Test, los resultados indican que los datos no se ajustan a una distribución normal, por lo que lo siguiente es aplicar un enfoque no paramétrico para conocer si hay diferencia entre medias de dos conjunto de datos provenientes de muestras relacionadas, que según Wilconxon (1945), si no se cumple el supuesto de normalidad, se aplica la prueba y tiene como parámetro dos conjuntos de datos: el antes y el después.

A continuación, se realiza la prueba de Wilconxon del Pre-Test y Post-Test para comparar los tipos de mediciones de una misma muestra. De esta manera, se hace el planteamiento de hipótesis donde se tiene que: $H_0: \mu_1 = \mu_2$, es decir, ambos grupos son equivalentes; no hay diferencia significativa en el Pre- Test y Pos- Test. Al contrario se tiene $H_a: \mu_1 \neq \mu_2$ donde ambos grupos son diferentes, por lo cual, si hay diferencia significativa en el Pre-Test y Post- Test. Se utiliza un nivel de significación (alfa) del 0,05.

Se aplica la prueba estadística de Wilcoxon al conjunto de muestras del Pre-test y Post - tes, que de acuerdo al criterio de decisión, si $p > 0,05$, se acepta la hipótesis nula y se rechaza la hipótesis alternativa, en cambio, si $p \leq 0,05$, se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

Tabla 9. Análisis Inferencial Pre-Test y Post-Test

<i>Estadísticos de contrastes</i>	
<i>Puntaje Pre - Puntaje Pro</i>	
Z	-3,010 ^b
Sig. asintót.	0,003

Nota: a. Prueba de los rangos con signo de Wilcoxon; b. Basado en los rangos negativos.

Fuente: elaboración propia

De acuerdo a la Tabla 9, el valor $p=0,003$; por lo tanto, se rechaza la hipótesis nula y se acepta la hipótesis alternativa, es decir, las medias entre el Pre-Test y Pos-Test son significativamente diferentes. Por consiguiente, se concluye que los dos grupos de mediciones son diferentes. Lo que implica que, el programa de concientización en seguridad de información para pequeñas empresas en la ciudad de puyo de manera integral genera mejoras en la cultura de protección de datos sensibles de las *pymes*.

3.4. Análisis global de datos

De acuerdo con los resultados obtenidos, en la evaluación posterior a la capacitación realizada a las pequeñas y mediana empresas de la ciudad del Puyo, se evidencia el interés por parte de los participantes en crear una cultura de buen manejo de la información digital personal y comercial, que dichos usuarios manejan diariamente. Por otra parte, se ha generado conocimientos al respecto de los programas de concientización en seguridad de información para *pymes*, con la finalidad de que se desarrollen nuevas investigaciones acerca del tema, y plantear posteriores propuestas para mejorar la ciberseguridad en dicho sector económico comercial.

Dicho de otro modo, los resultados del análisis estadístico descriptivo e inferencial pone en evidencia una mejora significativa de conocimiento en las temáticas tratadas. Como se evidencia en la Tabla 10.

Tabla 10. Análisis global de resultados

Temáticas	Hubo mejoras en conocimientos	No hubo mejoras en conocimientos
Ataques y delitos informáticos	X	
Técnicas de ataques informáticos más utilizados por los ciberdelincuentes	X	
Correcta administración de contraseñas	X	
Riesgos del uso de un software con licenciamiento ilegal	X	
Técnicas de protección ante incidentes	X	

Fuente: elaboración propia

El programa de concientización ejecutado ha permitido contribuir a la mejora de conocimientos en las temáticas planteadas en la investigación.

CONCLUSIONES

- El análisis teórico realizado pone en manifiesto el incremento de ataques informáticos a la seguridad de la información a nivel mundial en las empresas tanto públicas como privadas. Ecuador no está exento de dichos ataques, debido al deficiente conocimiento de las personas en temas de ciberseguridad.
- De acuerdo al diagnóstico situacional, una gran parte del sector económico, en la Provincia de Pastaza, está sustentado por alrededor de 1070 *pymes*, las cuales, presentan un bajo índice de conocimiento acerca de temáticas en cuanto a seguridad de la información y métodos de protección ante delitos informáticos.
- El diseño del programa de concientización en seguridad de la información, ha permitido que los propietarios de las *pymes* comprendan la importancia de la información que manejan. De igual forma, el programa de concientización ayudó a los participantes del estudio, a fomentar una cultura de concientización en ciberseguridad con las temáticas planteadas en base a la encuesta realizada.
- De acuerdo con los datos obtenidos en la evaluación del programa, se obtiene un valor $p=0,003$; que es menor o igual que 0,05 lo que implica que es estadísticamente significativo, por lo que se evidencia un mejor conocimiento sobre las temáticas tratadas acerca de seguridad de la información, en los participantes que formaron parte del programa de concientización en seguridad de información.

RECOMENDACIONES

- Mantener un constante flujo de conocimiento en cuanto a temáticas de ciberseguridad. De modo que, los datos digitales se mantengan protegidos ante los ataques informáticos más comunes, de acuerdo a los métodos de protección actuales.
- Replicar la investigación a otros sectores del país, a fin de realizar comparaciones en temas de cultura de seguridad de la información en la población, de tal forma que las *pymes* mejoren el tratamiento de los datos digitales sensibles que manejan.
- Realizar más campañas de concientización, sobre temas de seguridad informática, orientadas a toda la población, con el objetivo de mejorar la cultura en cuanto a este tema para disminuir los riesgos latentes en los datos sensibles de cada usuario.
- Se recomienda que, para posteriores estudios, se realicen pruebas de validación de conocimientos en los asistentes, para comprobar la viabilidad de un programa de concientización en seguridad de la información.

BIBLIOGRAFÍA

- Aguilar, D. & Guaita, F. (2018). *Evaluación de tres ataques ransomware utilizando escenarios virtuales como plataforma experimental (Tesis de pregrado)*. Recuperada de <https://dspace.ups.edu.ec/bitstream/123456789/15919/1/UPS-ST003698.pdf>
- Alberola, A. (2013). *Integración de Service Desk con Desarrollo de Software basándose en ITIL y Métodos Ágiles (Tesis)*. Recuperada de <https://riunet.upv.es/handle/10251/47907>
- Avast. (2020). *Qué es el spam: guía esencial para detectar y prevenir el spam*. Recuperado de <https://www.avast.com/es-es/c-spam>
- Barranco, J. (2001). *Metodología del análisis estructurado de sistemas* (2ª ed.). Madrid: Universidad Pontificia Comillas de Madrid.
- Benavides, E., Fuertes, W., y Sánchez, S. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura. *Cienc Tecn UTEQ*, 13(1), 97-104. doi: <https://doi.org/10.18779/cyt.v13i1.357>
- Cámara de comercio de Quito. (2017). *Clasificación de las pymes, pequeña y mediana empresa*. Recuperado de http://www.ccq.ec/wp-content/uploads/2017/06/Consulta_Societaria_Junio_2017.pdf
- Cortes, D. (2016). *Fundamentos Básicos de Seguridad de la Información*. Recuperado de <https://www.seguridadyfirewall.cl/2016/01/fundamentos-basicos-de-seguridad-de-la.html>
- Cybereop. (2020). *Casi el 70 por ciento de las pymes experimentan ataques cibernéticos*. Recuperado de <https://www.cybereop.com/blog/casi-el-70-por-ciento-de-las-pymes-experimentan-ataques-ciberneticos.html>
- Delgado, D., y Chávez, G. (2018). Las Pymes en el Ecuador y sus fuentes de financiamiento. *Revista Observatorio de la Economía Latinoamericana*, 1-18. ISSN: 1696-8352

- Deutsch, V. (2016). *Principales problemas de ciberseguridad y su solución*. Recuperado de <https://empresas.blogthinkbig.com/problemas-ciberseguridad-y-solucion/>
- Díaz, V. (2001). *Diseño y elaboración de cuestionarios para la investigación comercial*. Madrid: Esic.
- EcuRed. (2020). *Sistema de Gestión de Información*. Recuperado de <https://www.ecured.cu/EcuRed>
- ESET. (2019). *Introducción a la protección de datos*. Estados unidos: ESET, LLC y ESET, spol. s.r.o.
- Figuerola-Suárez, J., Rodríguez-Andrade, J., Bone-Obando, C., y Saltos-Gómez, J. (2017). La seguridad informática y la seguridad de la información. *Pol. Con*, 14 (2), 145-155. doi: 10.23857/pc.v2i12.420
- Florez, W., Arboleda, C., y Cadavid, J. (2012). Solución integral de seguridad para las pymes mediante un UTM. *Ing. USBMed*, 3 (1), 35-42. ISSN: 2027-5846
- Gaona, K. (2013). *Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa pesquera e industrial Bravito S.A. en la ciudad de Machala (Tesis de pregrado)*. Recuperada de <https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf>
- Gómez, A. (2019). *Tipos de ataques e intrusos en las redes informáticas*. Recuperado de https://www.edisa.com/wp-content/uploads/2019/08/ponencia_-_tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf
- Gómez, J. L., Feijóo, C., y Martínez, D. (2017). Política antes que regulación: la protección de la información personal en la era del big data. Recuperado de <https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/405/G%C3%93MEZ,%20FEIJOO%20Y%20F.%20MART%C3%8DNEZ.pdf>
- Hernández, B. (2001). *Técnicas estadísticas de investigación social*. Madrid: Díaz de Santos.

- Hernández, R., Fernández, C., y Baptista, M. (2010). *Metodología de la investigación* (5ª ed.). México: McGRAW-HILL.
- Kaspersky Lab. (2016). *Cómo abordar los desafíos de respuesta a incidentes*. Recuperado de <https://latam.kaspersky.com/blog/incident-response-report/>
- Kaspersky. (2020). *Ataques a la red. Periodo de tiempo: Día*. Recuperado de <https://securelist.lat/>
- INCIBE. (2020a). *Protección de la información*. Recuperado de <https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-informacion>
- INCIBE. (2020b). *Desarrollar cultura en seguridad*. Recuperado de <https://www.incibe.es/protege-tu-empresa/que-te-interesa/desarrollar-cultura-en-seguridad>
- INEC. (2016). *Encuesta a Empresas*. Recuperado de <https://www.ecuadorencifras.gob.ec/encuesta-a-empresas/>
- Integra. (2018). *¿Qué es la norma ISO 27000 de Seguridad de la Información?* Recuperado de <https://blog.consultoresdesistemasdegestion.es/que-es-la-iso-27000-de-seguridad-de-la-informacion/>
- ISOTools Excellence. (2017). *¿Seguridad informática o seguridad de la información?* Recuperado de <https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/>
- ISOTools Excellence. (2020). *La familia de normas ISO 27000*. Recuperado de <https://www.isotools.org/2015/01/21/familia-normas-iso-27000/>
- Izaguirre, J. (2018). Análisis de los ciberataques realizados en América Latina. *INNOVA Research Journal*, 3 (9), 172-181.
- Marradi, A., Archenti, N., y Pionavi, J. I. (2007). *Metodología de las Ciencias Sociales*. Buenos Aires: Emecé.
- Ministerio de Agricultura y Desarrollo Rural de Colombia. (2017). *Plan de sensibilización en seguridad de la información 2017*. Recuperado de https://www.minagricultura.gov.co/Furag2017/Evidencias/Pregunta%20144/1/PLA%20N%20DE%20SENSIBILIZACION%20C3%93N_2017.pdf

- Prieto, B. (2017). El uso de los métodos deductivo e inductivo para aumentar la eficiencia del procesamiento de adquisición de evidencias digitales. *Cuadernos de Contabilidad*, 18(46), 1-27. doi: <https://doi.org/10.11144/Javeriana.cc18-46.umdi>
- Rea-Guaman, A., Calvo-Manzano, J., y San Feliu, T. (2018). Prototipo para Gestionar la Ciberseguridad en Pequeñas Empresas. *13th Iberian Conference on Information Systems and Technologies (CISTI)*, 1-6. doi: 10.23919/CISTI.2018.8399252
- Remuzgo, F. (2005). *Diagnóstico Situacional de la Empresa*. Recuperado de http://geco.mineroartesanal.com/tiki-download_wiki_attachment.php?attId=371
- Revista de Tecnología Gestión. (2017). *Pymess: ¿Por qué son las más vulnerables a un ataque de hackers?* Recuperado de <https://gestion.pe/tecnologia/pymes-son-vulnerables-ataque-hackers-136731-noticia/>
- Sánchez, R. (2014). *Enseñar a investigar. Una didáctica nueva de la investigación en ciencias sociales y humanas*. México: Universidad Nacional Autónoma de México.
- Santana, I. (2015). *Diseño Cuasi-experimental (pre test/post test) Aplicado a la Implementación de Tics en el Grado de Inglés Elemental: Caso Universidad Tecnológica de Santiago Recinto Santo Domingo en el Cuatrimestre Mayo-Agosto 2015-2*. (Tesis de posgrado). doi: 10.13140/RG.2.2.20540.18565
- Sevilla, P. (2020). *El nuevo Informe Anual de Internet de Cisco pronostica que para 2023 más del 10% de las conexiones móviles globales se...* Recuperado de <https://news-blogs.cisco.com/americas/es/2020/02/21/el-nuevo-informe-anual-de-internet-de-cisco-pronostica-que-para-2023-mas-del-10-de-las-conexiones-moviles-globales-seran-con-5g/>
- Shapiro, S. S.; Wilk, M. B. (1965). "An analysis of variance test for normality (complete samples)". *Biometrika*. 52 (3-4): 591-611
- Shaughnessy, J., Zechmeister, E., y Zechmeister, J. (2007). *Métodos de investigación en psicología* (7ª ed.). México: McGRAW-HILL.
- Telefónica. (2015). *Alerta: los 4 ataques informáticos más frecuentes y cómo evitarlos*. Recuperado de <https://destinonegocio.com/pe/gestion-pe/alerta-los-4-ataques-informaticos-mas-frecuentes-y-como-evitarlos/>

- WeliveSecurity (2015). *¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes?* Recuperado de <https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/>
- Wilcoxon, Frank (Dec 1945). "*Individual comparisons by ranking methods*". *Biometrics Bulletin*. **1** (6): 80–83
- Zambrano, A., y Guailacela, F. (2019). *Análisis de la eficiencia de los IDS open source Suricata y Snort en las PYMES. (Tesis de posgrado)*. Recuperada de <http://repositorio.uees.edu.ec/bitstream/123456789/2926/1/ZAMBRANO%20BARBERAN%20ALFONSO%20%26%20GUAILACELA%20ROMERO%20FRANKLIN.pdf>

ANEXOS

Anexo A: Acuerdo de confidencialidad

Acuerdo de confidencialidad enviada a los gerentes de las *pymes* para su participación en el programa de concientización en la ciudad de Puyo, que detalla a continuación:

Figura 23. Acuerdo de confidencialidad enviada mediante correo electrónico



Fuente: Elaboración propia

Anexo B: Formulario de diagnóstico situacional

Encuesta de diagnóstico situacional sobre seguridad de información que fue enviada a los gerentes de las *pymes* de la ciudad de Puyo, donde se determinó la problemática y vulnerabilidades respecto al objeto de estudio.

ENCUESTA DIRIGIDA A LAS PYMES

PROYECTO DE DESARROLLO: PROGRAMA DE CONCIENTIZACIÓN EN SEGURIDAD DE INFORMACIÓN PARA PEQUEÑAS EMPRESAS EN LA CIUDAD DE PUYO

Objetivo: Realizar un diagnóstico de la situación actual sobre seguridad de información de la pequeña empresa de la ciudad de Puyo

Instrucciones: A continuación, usted encueasimintra una serie de preguntas que hacen referencia a la seguridad de la información digital de su empresa. Lea cada pregunta y seleccione la respuesta según su criterio o conocimiento.

1. ¿Hace uso de plataformas virtuales para promocionar su producto o servicio?

1. Nunca

2. A veces

3. Ocasionalmente

4. Casi siempre

5. Siempre

2. ¿Hace uso de plataformas virtuales para realizar movimientos bancarios como: cobros o pagos de un producto o servicio de su empresa?

1. Nunca

2. A veces

3. Ocasionalmente

4. Casi siempre

5. Siempre

3. ¿Cree usted que las plataformas bancarias son seguras para las diversas transacciones que realiza su empresa?

1. Nunca

2. A veces

3. Ocasionalmente

4. Casi siempre

5. Siempre

4. ¿Ha sido víctima o ha escuchado de algún delito informático como: suplantación de identidad, *phishing*, *ransomware*, secuestro de información, robo de información, otros?

1. Nunca

2. A veces

3. Ocasionalmente

4. Casi siempre

5. Siempre

5. ¿Tiene conocimiento acerca de fraudes electrónicos por ingeniería social (manipulación para el robo de información confidencial del usuario)?

1. Nunca

2. A veces

3. Ocasionalmente

4. Casi siempre

5. Siempre

6. ¿Considera usted importante cambiar las contraseñas de sus plataformas electrónicas (Correo, redes sociales, celular, cajero automático, Banca en línea, Aplicaciones móviles bancarias, otros)?

1. Nunca

2. A veces

3. Ocasionalmente

4. Casi siempre

5. Siempre

7. ¿Usted almacena las contraseñas de las plataformas virtuales que utiliza de forma física (papel), o digital: navegador de internet, lo guardan terceros, programa externo, otros?

1. Nunca

2. A veces

3. Ocasionalmente

4. Casi siempre

5. Siempre

8. ¿Ha instalado algún programa de antivirus en el ordenador de su trabajo (computadora)?

1. Nunca

2. A veces

3. Ocasionalmente

4. Casi siempre

5. Siempre

9. ¿Hace uso de programas piratas (software de tipo comercial con licencia adulterada) dentro de su empresa?

1. Nunca

2. A veces

3. Ocasionalmente

4. Casi siempre

5. Siempre

10. ¿Usted maneja información sensible de su empresa o trabajo en su dispositivo móvil?

1. Nunca

2. A veces

3. Ocasionalmente

4. Casi siempre

5. Siempre

Anexo C: Plan de concientización en seguridad de la información

Hace referencia a los objetivos, los alcances, la planificación, los temas abordar y cronogramas de actividades con la finalidad de hacer conocer el estudio de investigación al presidente de la cámara de comercio de Pastaza y sea socializado con los socios.

El plan de concientización está firmado y sellado por la misma entidad.

Figura 24. Portada del plan de concientización



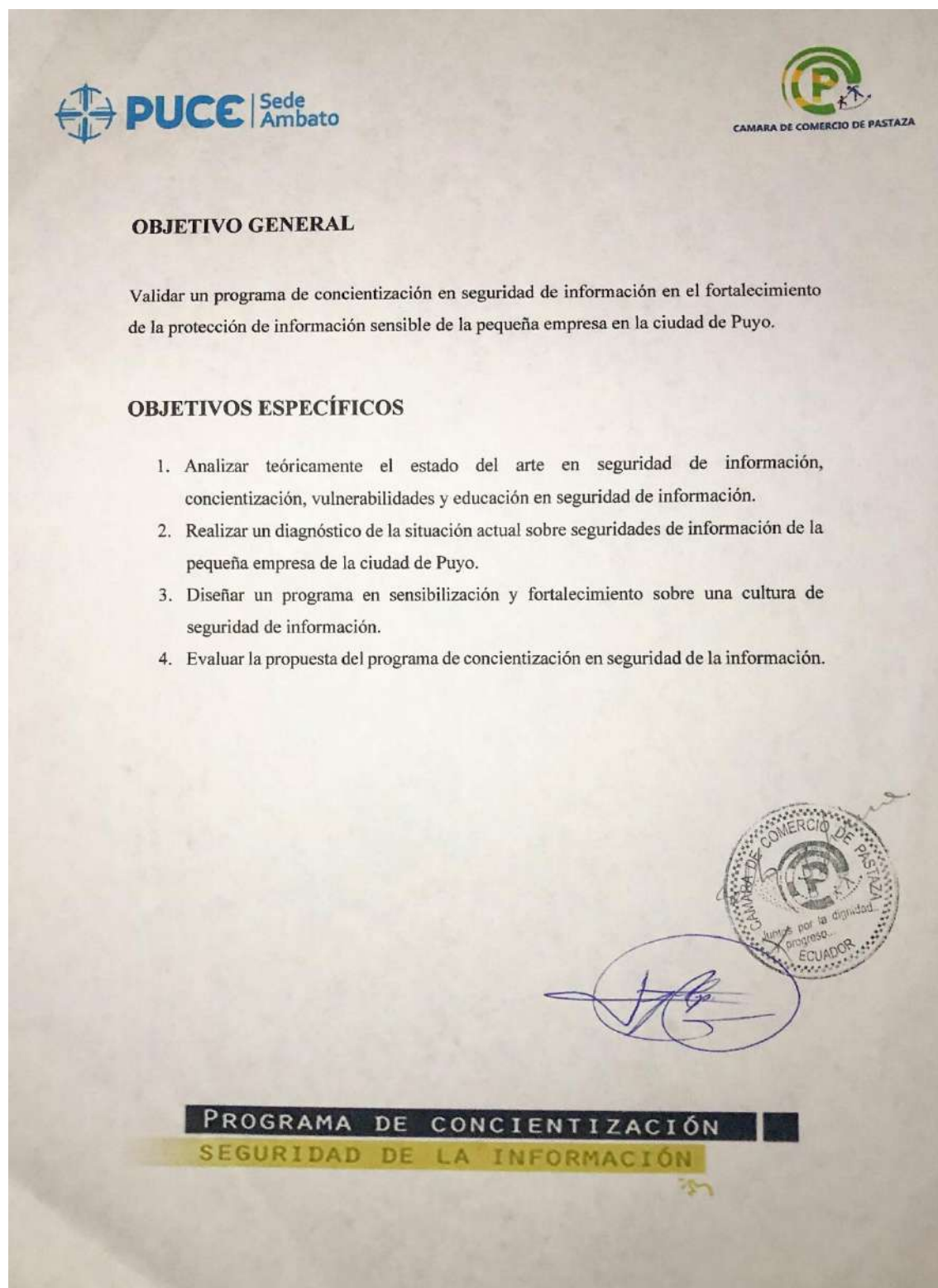
Fuente: elaboración propia

Figura 25. Planificación del desarrollo de programa de concientización



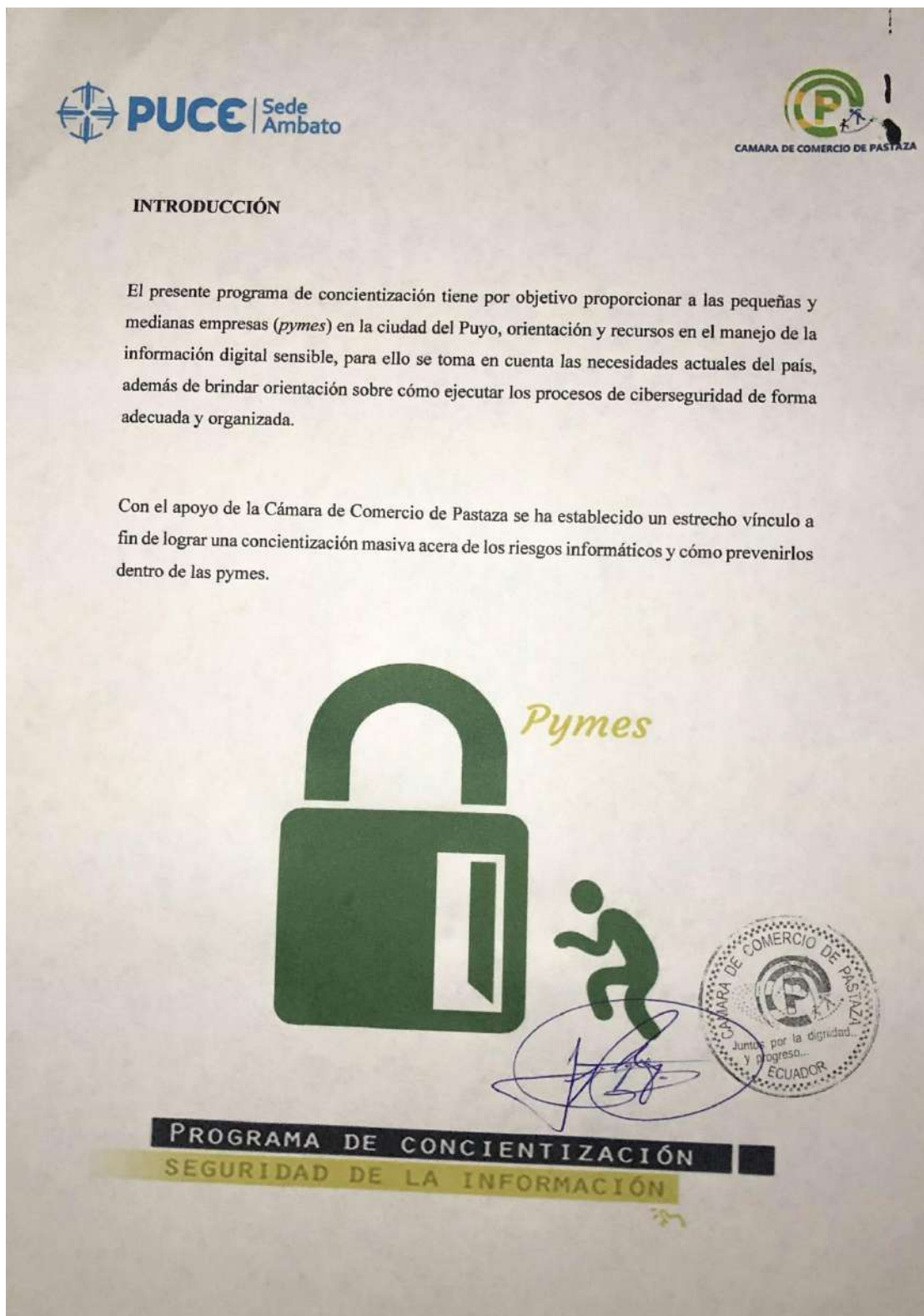
Fuente: elaboración propia

Figura 26. Objetivo general y objetivos específicos del plan de concientización



Fuente: elaboración propia

Figura 27. Introducción del contenido del plan de concientización



Fuente: elaboración propia

Figura 28. Alcances y propósitos del plan de concientización



MISIÓN

Crear una cultura de concientización y conocimiento acerca del adecuado manejo de la información digital sensible de las pequeñas y medianas empresas en la ciudad del Puyo, así como también métodos de prevención y respuesta a incidentes ante los diversos tipos de delitos informáticos.

VISIÓN

A través del programa de concientización se busca disminuir el riesgo latente ante un ataque cibernético a las *pymes*, así como también dar un nuevo enfoque a través del conocimiento adquirido sobre la importancia que tiene la ciberseguridad en la actualidad.

ALCANCE

El presente programa de concientización, tiene por alcance capacitar a los usuarios de las *pymes* con el apoyo de la Cámara de Comercio de Pastaza de modo que se cree una cultura de protección de datos.



Fuente: elaboración propia

Figura 29. Materiales y herramientas para ejecución del programa de concientización



MATERIALES

El presente programa de concientización hace uso de las siguientes herramientas:

Para participantes

- *Hardware*
 - Ordenador portátil o de escritorio con acceso a internet
 - Smartphone (teléfono inteligente) con acceso a internet
 - Tablet o Ipad con acceso a internet
- *Software*
 - Plataforma Facebook

Para el instructor

- *Hardware*
 - Ordenador portátil con acceso a internet
- *Software*
 - Sistema Operativo Kali Linux (virtualizado)
 - Sistema Operativo CentOS Linux (virtualizado)
 - Plataforma Wordpress
 - Servicio de Hosting
 - Plataforma Office 365



Fuente: elaboración propia

Figura 30. Cronograma de actividades del plan de concientización



Planificación de actividades

El presente plan de concientización está diseñado para 4 semanas y en cada una de ellas hay diferentes actividades a cumplirse, además, se dará por culminado cuando se haga la entrega de los certificados a los participantes.

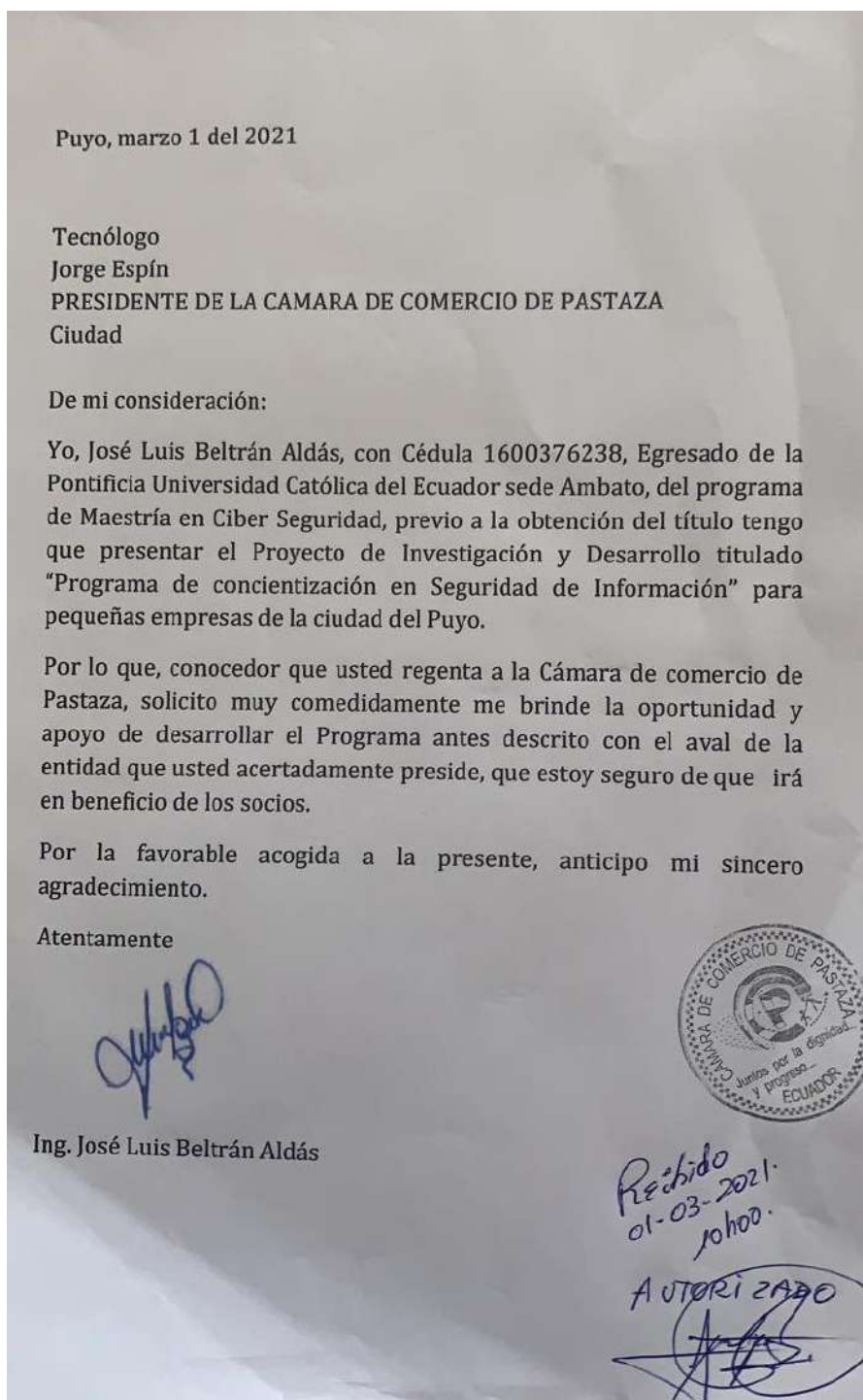


Fuente: elaboración propia

Anexo D: Oficio de solicitud para aval.

Documento que se adjunta y cerciora que se cumplió con el trámite pertinente, para contar con la respectiva autorización para el desarrollo del presente estudio de investigación sobre el programa de concientización de la seguridad de la información.

Figura 31. Formato de solicitud para el aval de capacitación a la cámara de comercio de Pastaza



Fuente: elaboración propia

Anexo E: Pre-Test y Pos-Tes (Formulario de evaluación)

Cuestionario de evaluación a los participantes del Programa de concientización, donde determinamos el nivel de conocimiento antes y después del estudio.

Figura 32. Cuestionario del Pre-Test y Post-Test

CIBERSEGURIDAD EN LAS PYMES

Instrucciones: Responda con un círculo con el grado en que concuerda estas cuestiones con su conocimiento, empleando la escala de 1= "Totalmente en Desacuerdo" a 5= "Totalmente de Acuerdo".

1. Totalmente en Desacuerdo
2. En Desacuerdo
3. Ni de acuerdo, ni desacuerdo
4. En Acuerdo
5. Totalmente de Acuerdo

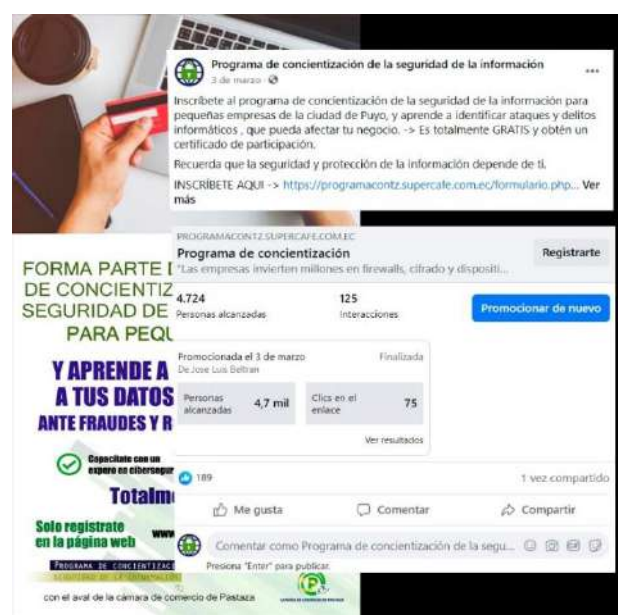
N		1	2	3	4	5
1	Un ataque informático es un intento desorganizado no intencionado causado por una persona para causar daño o problemas a un sistema informático o red.	1	2	3	4	5
2	Los delitos informáticos son todas aquellas acciones ilegales, delictivas, antiéticas o no autorizadas que hacen uso de dispositivos electrónicos e internet, a fin de vulnerar, menoscabar o dañar los bienes, patrimoniales o no, de terceras personas o entidades.	1	2	3	4	5
3	El ciberataque de ingeniería social consiste en engañar al usuario para que crea que un administrador de sistema legítimo, de un banco o del gestor de sistema de la empresa para la que trabaja les pide su contraseña, cuando en realidad es un hacker quien lo hace.	1	2	3	4	5
4	El ransomware es un sistema criminal creado con el objetivo de ganar dinero. Este se puede instalar a través de enlaces engañosos incluidos en un mensaje de correo electrónico, mensaje instantáneo o sitio web.	1	2	3	4	5
5	Para crear contraseñas seguras es recomendable usar información personal que incluya palabras relacionadas con su nombre, nombres de familiares o mascotas.	1	2	3	4	5
6	No es necesario crear contraseñas más largas, que tengan al menos 8 caracteres. La probabilidad indica que es más fácil descifrar las contraseñas más largas.	1	2	3	4	5
7	En un software sin un licenciamiento adecuado, se puede acceder a las actualizaciones del fabricante. Y si este no puede actualizarse, la vulnerabilidad será corregida automáticamente.	1	2	3	4	5
8	El software pirata o crackeado, viene con código malicioso escondido que es aparentemente inocente pero en el interior de su código ejecuta acciones maliciosas.	1	2	3	4	5
9	Una red empresarial dependiendo de su tamaño deberá contar con Firewall, Virtual Private Network (VPN), Surf Protection, Spam Filter y Antivirus.	1	2	3	4	5
10	Los equipos de respuesta a incidentes de seguridad (CSIRT) buscan restituir las actividades con el impacto mínimo aceptable para las organizaciones ante un ciberataque.	1	2	3	4	5

Anexo F: Promoción del programa de concientización en seguridad de información

Se utilizó las redes sociales para promocionar e invitar a pequeñas y medianas empresas en la ciudad de Puyo, a ser participes en el programa de concientización en seguridad de información, además se utilizó material impreso de publicidad los mismos que fueron entregados personalmente.

Link de ingreso: <https://www.facebook.com/Programa-de-concientizaci%C3%B3n-de-la-seguridad-de-la-informaci%C3%B3n-107639984717059>

Figura 33. Publicidad y anuncios sobre el programa de concientización a través de *Facebook*



Fuente: Elaboración propia

Figura 34. Invitación a los propietarios y trabajadores de pequeñas y medianas empresas a formar parte de programa de concientización



Fuente: Elaboración propia

Figura 35. Diseño de publicidad digital para promoción del programa de concientización



Que tan seguras son tus contraseñas ?
Navegas en canales seguros
Ha escuchado sobre Ingeniería social
Secuestro de datos ?

Aprende a identificar ataques y delitos y protege tus datos

Inscríbete es gratis! www.programacontz.supercafe.com.ec

PROGRAMA DE CONCIERTIZACIÓN
 SEGURIDAD DE LA INFORMACIÓN

con el aval de la cámara de comercio de Pastaza



FORMA PARTE DEL PROGRAMA DE CONCIERTIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA PEQUEÑAS EMPRESAS

Y APRENDE A DAR SEGURIDAD A TUS DATOS E INFORMACIÓN ANTE FRAUDES Y ROBOS INFORMÁTICOS

✓ Capacitate con un experto en ciberseguridad ✓ Obtén tu certificado de participación

Totalmente gratis!!

Solo regístrate en la página web www.programacontz.supercafe.com.ec

PROGRAMA DE CONCIERTIZACIÓN
 SEGURIDAD DE LA INFORMACIÓN

con el aval de la cámara de comercio de Pastaza

<https://www.>



INSCRÍBETE → NAVEGAS
EN EL PROGRAMA DE CONCIERTIZACIÓN

✓ Capacitate con un experto en ciberseguridad
ES TOTALMENTE GRATIS

<http://www.>



SEGURO
DE LA SEGURIDAD DE INFORMACIÓN

✓ Obtén tu certificado de participación
CUPOS LIMITADOS

Fuente: Elaboración propia

Anexo H: Plataforma Web programa de concientización en seguridad de información.

Dentro del desarrollo y ejecución del modelo de aproximación a la solución contempla la fase 2, se ha construido una plataforma web dinámica, innovadora y de fácil uso dirigida a los participantes inscritos en el programa de concientización para fortalecer la cultura de ciberseguridad. *Link de ingreso:* <https://programacontz.supercafe.com.ec/>

Figura 36. Portada principal del programa de concientización



Fuente: Elaboración propia

Figura 37. Formulario de inscripción

Fuente: Elaboración propia

Se ingresa a la portada principal a los participantes donde se encuentra la accesibilidad de la información, así mismo encontrar la Visión, la Misión, los alcances, temáticas y desarrollo de las mismas de una manera eficaz.

Link de ingreso: https://programacontz.supercafe.com.ec/acc_us.php

Figura 38. Portada principal de los participantes

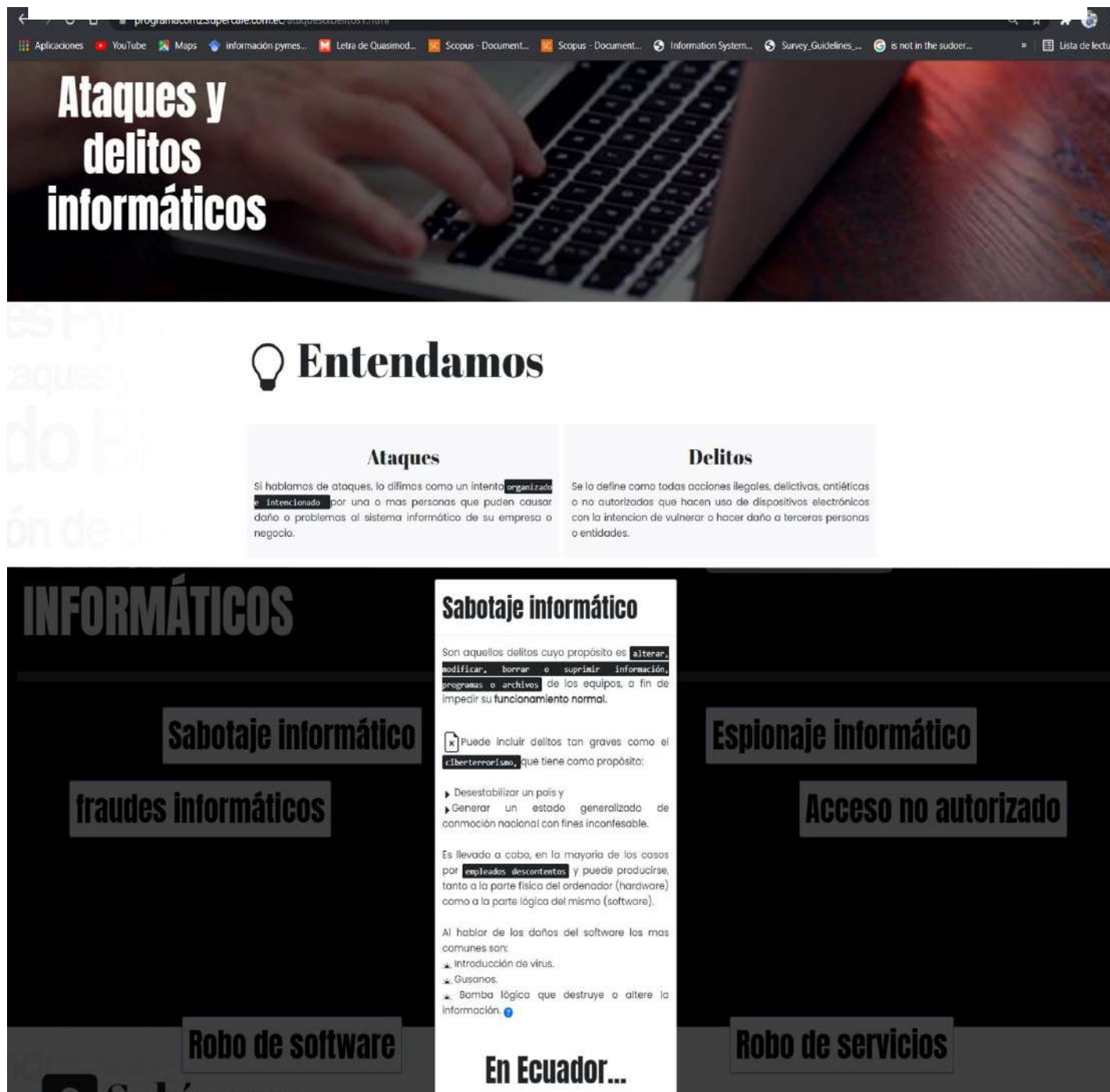


Fuente: Elaboración propia

La página *web* trata sobre ataques y delitos informáticos que contiene conceptos, nociones y referencias sobre como identificarlos, así mismo, se pretende que el participante comprenda y fortalezca su nivel de conocimiento dentro del programa de concientización.

Link de ingreso <https://programacontz.supercafe.com.ec/ataques&delitos1.html>

Figura 39. Página *web* sobre ataques y delitos informáticos



Fuente: Elaboración propia

La página *web* trata sobre técnicas de ataques informáticos más utilizados por los ciberdelincuentes. Se explica las amenazas y vulnerabilidades que están expuestas las empresas, al no saber identificar qué tipo de técnicas usan y como afecta a la integridad de las mismas.

Link de ingreso <https://programacontz.supercafe.com.ec/tecnicas&ataques.html>

Figura 40. Página *web* sobre Técnicas de ataques informáticos más utilizados



Técnicas de ataques informáticos más utilizados

Los ataques informáticos representan una de las amenazas más grandes que existen para las empresas y el mundo actualmente, afecta por igual a individuos particulares, **microempresas** e incluso estados y naciones.

Debido a esto, las medidas de seguridad informática se han convertido en prioritarias, especialmente para aquellas empresas o entidades que dependen casi al 100% de internet para realizar sus operaciones.

Ransomware

¿Que es? Tipos de Ransomware Como Protegerse:

Este tipo de malware es el más peligroso, debido a que secuestra su información o impide el acceso a cambio de pago por liberar o habilitar los datos. Actualmente los pagos se lo realizan a personas con identidades ocultas o desconocidas, a través de métodos de pagos por criptomonedas o transferencias electrónicas.

Como puede infectarse?

Uno de los métodos más comunes es a través del spam malicioso o correo electrónico no deseado, generalmente remiten empresas, bancos o cooperativas que no somos clientes y anexas archivos pdf, ofertas o links externos a otros servicios.

La publicidad maliciosa es uno de los métodos más comunes, generalmente suelen usar redes sociales o aplicaciones móviles, que al hacer click en aquella publicidad lleva a un acceso externo o ejecuta cierto programa en modo off line sin que la víctima este enterada.

Phishing **Ingeniería social**

Fuente: Elaboración propia

Figura 41. Página *web* sobre correcta administración de contraseñas



La página *web* trata sobre riesgos del uso de *software* con licenciamiento ilegal. Se instruye sobre las consecuencias que conlleva al descargar o instalar un programa o *software* sin licencia en las empresas, y el efecto negativo que genera como: problemas legales, robo de información sensible, intromisión, etc.

Link de ingreso <https://programacontz.supercafe.com.ec/riesgossoftwareilegal.html>

Figura 42. Página *web* sobre riesgos del uso de un *software* con licenciamiento ilegal



Riesgos del uso de un software con licenciamiento ilegal

Según datos de Play-it-safe.net, la unidad de Digital Crimes de Microsoft, el 61% de ordenadores adquiridos con software pirata tienen algún tipo de virus o malware.

Introducción

Debido a lo fácil que es navegar y bajar contenido en internet, es muy común que las empresas elijan usar o descargar software sin licencia. En algunos casos se requiere como una alternativa puntual y resuelve una necesidad espontánea, pero en otros casos tiene como fin una acción premeditada y hasta maliciosa.

Ten encuenta que la usar software pirata no solo cometes un delito legal, sino tambien puede traer graves consecuencias tanto a sus empresas como a información personal.

Usar software pirata no es una opción viable para cualquier tipo de negocios, puede estar sujeta a multas por no cumplir obligaciones legales y abrir una puerta para la infección del sistema de información de su empresa, por causa de malware alojado en sus aplicaciones.

NO A LA PIRATERIA

Riesgos al usar Software sin licencia

Creemos que al utilizar software ilegal es un beneficio grande para nuestra empresa, debido a que no pagamos impuestos de ley, ni la misma

Fuente: Elaboración propia

La página web trata sobre Técnicas de protección ante incidentes. Aborda sobre cómo proteger y dar respuesta ante ataques informáticos para minimizar la cantidad y repercusión de los incidentes de seguridad.

Link de ingreso <https://programacontz.supercafe.com.ec/tecnicasproteccionincidentes.html>

Figura 43. Página web sobre técnicas de protección ante incidentes



The screenshot shows a web browser window with the URL programacontz.supercafe.com.ec/tecnicasproteccionincidentes.html. The page has a dark blue header with the title "Técnicas de protección ante incidentes" in large white letters. Below the header, there is a paragraph of text, a central graphic with a magnifying glass over a bar chart, and a list of statistics on the right. At the bottom, there are two sections: "Que es?" and "Quienes lo ejecutan?".

A medida que exponemos nuestros datos online, a través de canales de redes sociales, emails con archivos adjuntos, etc. aumenta la posibilidad de ser víctimas de una filtración de datos u otros ataques.

La respuesta a este problema no es dejar de usar internet, pero las empresas necesitan prestar atención a las vulnerabilidades de Seguridad, implementar medidas preventivas y generar estrategias que limiten el daño posible, si esas medidas fallan.

Maidana ofrece algunas estadísticas interesantes basadas en una encuesta en Latinoamérica:

- El 60 % de personas dice haber sufrido un ataque de phishing
- Un 40 % reconoce haber sufrido de ingreso a sus ordenadores
- El 44 % reconoce de borrados de archivos
- Un 54 % dice haber sufrido ataques para manipular sus sistemas
- El 76 % opina que los ataques informáticos son más sofisticados,
- El 69 % de las empresas dicen que sus empleados están concienciados de los riesgos de sufrir un ataque informático,

Que es?
Es el encargado de desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información. Analiza, verifica y planifica planes en torno a la seguridad global de redes y ordenadores de una empresa u organización.

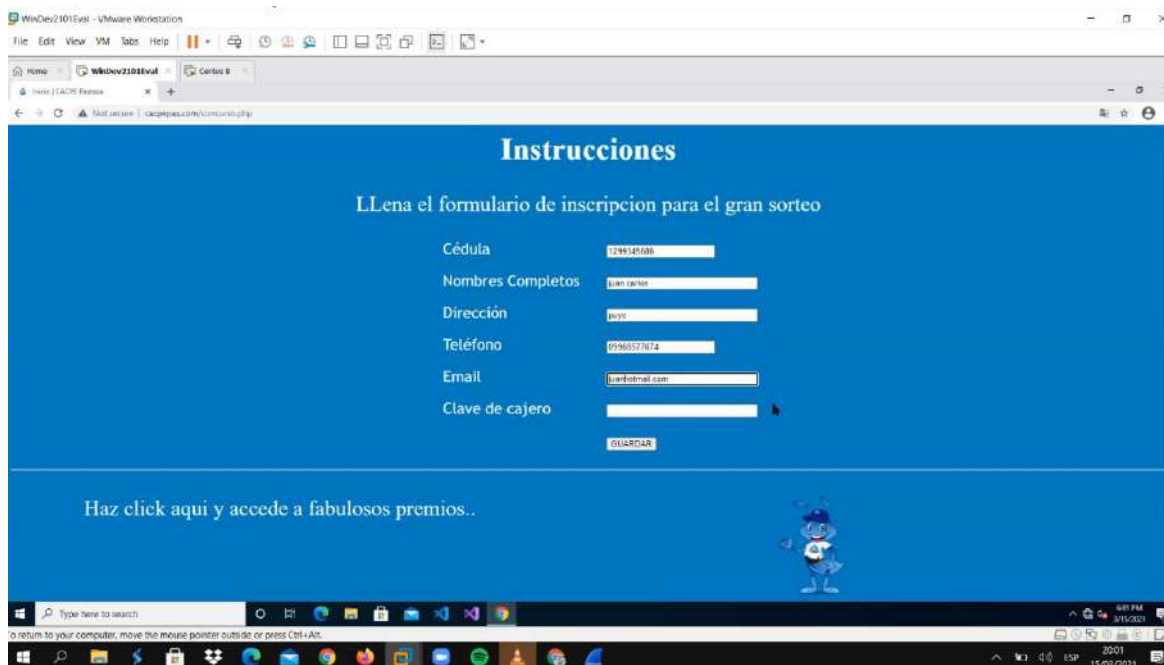
Quienes lo ejecutan?
Un grupo de expertos que tienen amplio conocimiento y experiencia, entorno a la seguridad en tecnologías de la información.

Fuente: Elaboración propia

Dentro del desarrollo de la capacitación del programa de concientización, se realizaron pruebas en entornos virtualizados, esto con la finalidad que el participante sea capaz de reconocer y entender como suceden estos ataques en entornos reales.

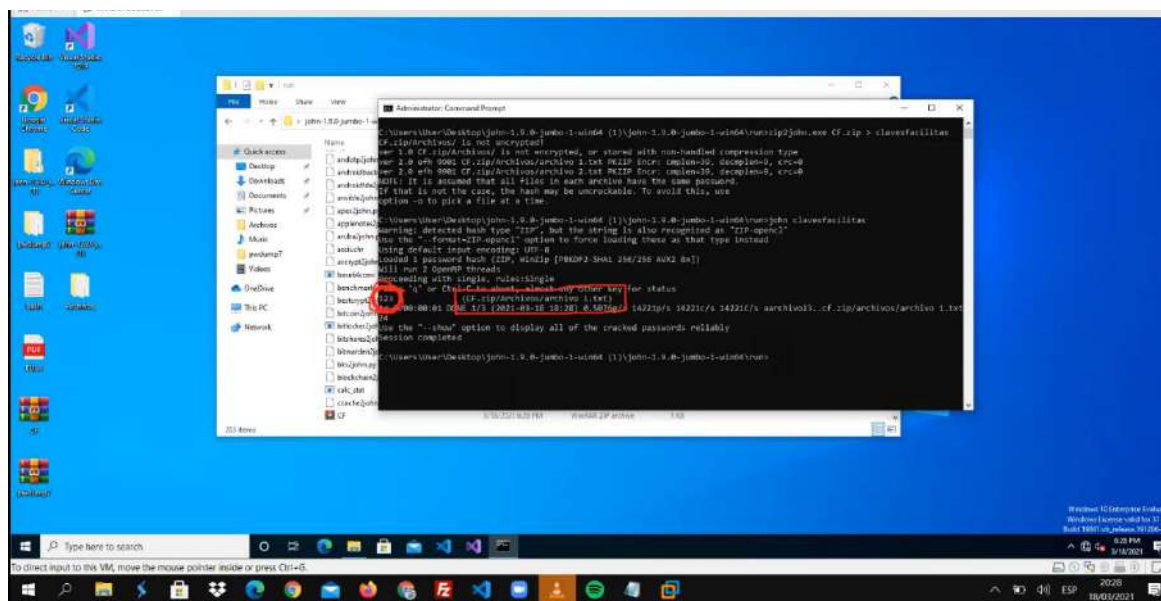
Se utilizó *software* de virtualización *VMware Workstation 15 Pro*, *CentOS 8* (Servidor web de pruebas) y *Windows 10* (Usuario para verificación en pruebas).

Figura 44. Delito informático a cliente *Windows*, para sustracción de datos mediante *phishing*.



Fuente: Elaboración propia

Figura 45. Comprobar la robustez de contraseñas en archivos



Fuente: Elaboración propia

Culminado el Programa de concientización en seguridad de la información, se procedió a entregar un certificado de participación a los asistentes, mismo que se encuentra abalizado por el presidente de la Cámara de Comercio de Pastaza y el Instructor, quienes dan fe de participación y agradecimiento.

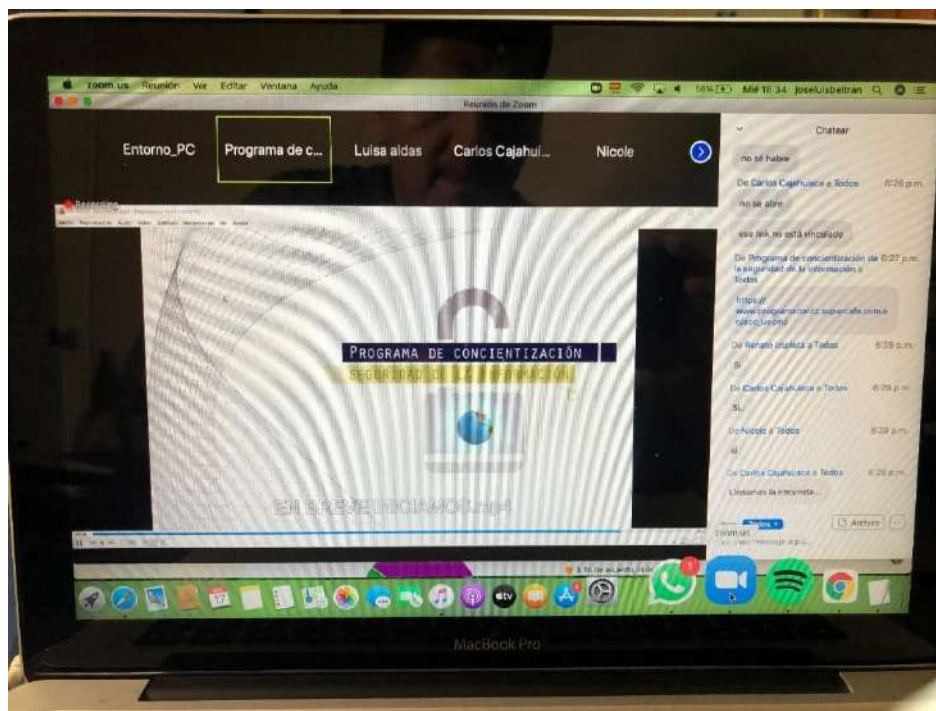
Figura 46. Formato del certificado entregado a los participantes



Fuente: Elaboración propia

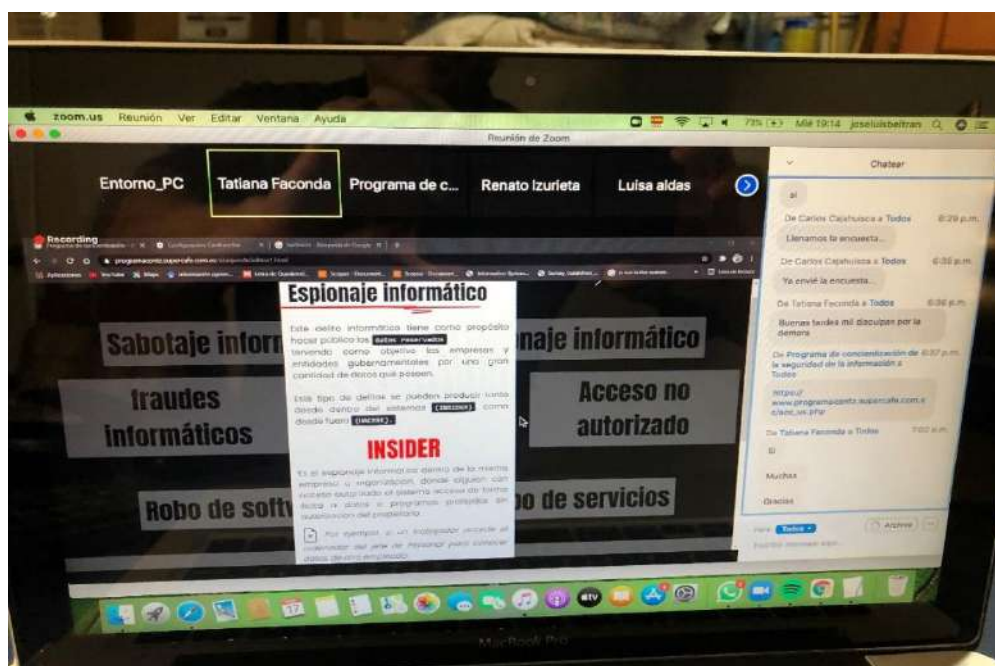
Dentro del Desarrollo del Programa, se evidencia la utilización de la herramienta electrónica Zoom, de la capacitación virtual realizada a los participantes del programa de concientización en seguridad de la información.

Figura 47. Bienvenida a los participantes del programa de concientización



Fuente: Elaboración propia

Figura 48. Capacitación a los participantes sobre ataques y delitos informáticos



Fuente: Elaboración propia