UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS

FRAUDES INFORMÁTICOS Y SU INCIDENCIA EN LA SEGURIDAD DE LOS DOCENTES Y ESTUDIANTES DE LA UCACUE, EXTENSIÓN CAÑAR.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA DE SISTEMAS

AUTOR: TANIA ESTEFANIA CHALÁN GUAMÁN.

DIRECTOR: ING. CRISTIAN HUMBERTO FLORES URGILES

CAÑAR - ECUADOR

2022

DIOS, PATRIA, CULTURA Y DESARROLLO

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE TECNOLOGÍAS DE LA INFORMACION Y COMUNICACIÓN

CARRERA DE SISTEMAS

FRAUDES INFORMÁTICOS Y SU INCIDENCIA EN LA SEGURIDAD DE LOS DOCENTES Y ESTUDIANTES DE LA UCACUE, EXTENSIÓN CAÑAR.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA DE SISTEMAS

AUTOR: TANIA ESTEFANIA CHALÁN GUAMÁN.

DIRECTOR: ING. CRISTIAN HUMBERTO FLORES URGILES

CAÑAR - ECUADOR

2022

DIOS, PATRIA, CULTURA Y DESARROLLO

Declaratoria de Autoría y Responsabilidad

Tania Estefania Chalán Guamán portador(a) de la cédula de ciudadanía Nº **0302893557**. Declaro ser el autor de la obra: "**Fraudes informáticos y su incidencia en la seguridad de los docentes y estudiantes de la UCACUE, extensión Cañar."**, sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cuenca, **22 de septiembre de 2022**

F: .....

Srta. TANIA ESTEFANIA CHALAN GUAMAN

CI: 0302893557

CERTIFICADO

Certifico que le presente trabajo fue desarrollado por el estudiante: **TANIA ESTEFANÍA CHALAN GUAMÁN**, bajo mi supervisión.

Ing. Cristian Flores Urgilés

DIRECTOR DEL TRABAJO DE TITULACIÓN UNIVERSIDAD CATÓLICA DE CUENCA EXTENSIÓN CAÑAR

APROBACIÓN DE TRIBUNAL DE GRADO

El tribunal designado por el honorable consejo directivo de la Universidad Católica de Cuenca Extensión Cañar, Facultad de Ingeniería de Sistemas instalado para receptar la sustentación del trabajo final de investigación con el tema "Fraudes informáticos y su incidencia en la seguridad de los docentes y estudiantes de la UCACUE, extensión Cañar", transcurrido el tiempo reglamentario procede a consignar la calificación de (___/100).

Cañar, _____, de_____, del 202_

_____ _____

PRESIDENTE DIRECTOR

_____ _____

DELEGADO SECRETARIO

DEDICATORIA

A Dios por haberme permitido llegar hasta este punto de mi vida por ayudarme a aprender de mis errores y mejorar como persona.

A mi Jefa Dolly Paredes por el apoyo brindado día a día en mi carrera Universitaria y de forma especial a mi hijo Joan Chalán por ser la razón de mi vida, mi inspiración y mi motivo para seguir adelante y superarme cada día más.

A mis padres José Chalán y Carmen Guamán por apoyarme de forma incondicional, ayudarme a cumplir mis metas y sueños por haberme forjado como la persona que soy actualmente.

También dedico con un profundo sentimiento a mis hermanas Mariana, Claudia, Jhulissa y Sofía y a mis cuñados Victor Barahona y Adonis Alvarez por el apoyo moral por ser fuente de motivación para culminar con mis estudios y formarme profesionalmente y a toda mi familia que es lo más valioso que Dios me ha dado.

AGRADECIMIENTO

Un agradecimiento a la Universidad Católica de Cuenca por permitirme convertirme en una profesional, gracias a cada docente de la carrera de Ingeniería de Sistemas extensión Cañar, quienes formaron parte de este proceso, gracias por su paciencia y enseñanzas.

De manera especial al Ingeniero Cristian Flores Urgiles, director de mi trabajo de titulación por el tiempo asignado a mi persona por su gran apoyo y guía para la formación de mi carrera, también a todos los catedráticos de la facultad de sistemas gracias por la sabiduría que me transmitieron durante mis años de estudio.

RESUMEN

La presente investigación tiene por objetivo, analizar los fraudes informáticos y su incidencia en la seguridad de los docentes y estudiantes de la UCACUE, extensión Cañar. Los objetivos planteados para llevar a cabo el presente estudio fueron: 1) Realizar encuestas para medir el nivel de seguridad que existe al momento de utilizar medios tecnológicos, 2) Analizar los diferentes fraudes informáticos y como inciden en los usuarios el impacto de estos actos en la vida social y en la tecnología, 3) Determinar los diferentes factores que influyen en el fraude informático. La investigación surge debido a que actualmente se ha visto un incremento en los casos de fraudes informáticos, generando preocupación debido a la importancia de la información que se maneja por medio de las redes. Por ello el análisis de algunos de estos actos ilícitos es primordial, ya que en muchas ocasiones es realizada con gran facilidad, aprovechado el desconocimiento de las personas, la ingenuidad al entregar información personal para beneficiarse económicamente. El análisis de incidencia se realizó por medio de la aplicación de encuestas y una matriz de riesgo utilizando la metodología MAGERIT, determinando los activos en base a la encuesta realizada, así como también las amenazas que puedan afectar a estos. Los resultados demostraron que las amenazas suplantación de identidad - Phishing y la divulgación de información - Caballo de Troya son fraudes que se presentan con más frecuencias en los medios tecnológicos, donde alrededor del 60% entre docentes y estudiantes son víctimas de este tipo de delito.

Palabras Clave: fraudes informáticos, tecnología, información, metodología magerit.

ABSTRACT

This research aims to analyze computer fraud and its impact on the security of teachers and students of UCACUE, Cañar campus. The objectives of this study were: 1) To conduct surveys to measure the level of security that exists when using technological means, 2) To analyze the different computer frauds and how the impact of these acts on social life and technology affects users, 3) To determine the different factors that influence computer fraud. The research arises because there has been an increase in computer fraud cases, generating concern due to the importance of the information handled through the networks. For this reason, analyzing some of these illicit acts is essential since, on many occasions, it is carried out with great ease to exploit people economically, taking advantage of their lack of knowledge and naivety when handing over personal information. The incidence analysis was carried out through surveys and a risk matrix using the MAGERIT methodology, determining the assets based on the study conducted and the threats that may affect them. The results showed that Phishing (identity theft) and Trojan Horse (spreading of information) are the most frequent technological media fraud, where about 60% of teachers and students are victims of this type of crime.

Keywords: computer fraud, technology, information, magerit methodology.

e-ISSN: 2588-1000

Pro Sciences

Revista de Producción, Ciencias e Investigación

FRAUDES INFORMÁTICOS Y SU INCIDENCIA EN LA SEGURIDAD DE LOS DOCENTES Y ESTUDIANTES DE LA UCACUE, EXTENSIÓN CAÑAR.

Computer fraud and its impact on the safety of teachers and students at UCACUE, Cañar extension.

Tania Estefanía Chalan Guamán [1]
Cristian Humberto Flores Urgilés[2]
Categoría profesional, Universidad Católica de Cuenca, Ecuador
techalang57@est.ucacue.edu.ec
chfloresu@ucacue.edu.ec
ORCID

INTRODUCCIÓN

El avance tecnológico, ha permitido que la informática sea un instrumento indispensable para la sociedad y el mundo con infinitas posibilidades de cambio, desarrollo y aumento en los distintos procesos laborales, comunicaciones, educación, etc. Con este crecimiento surge también la delincuencia informática, mediante el uso y la explotación inadecuada de la tecnología, con fines lucrativos, provocado el fraude informático considerado como uno de los delitos más graves que ha causado grandes desfalcos financieros.

Actualmente los fraudes informáticos están en constate crecimiento, esto ha provocado que todos los días existan miles de personas víctimas en diferentes delitos y muchos de

Ingenieria en Sistemas

estos casos han quedado en la impunidad ya que es dificultoso identificar o descubrir a los autores de estos hechos.

Por lo tanto, es necesario que las instituciones u organizaciones comiencen a tomar conciencia sobre temas de seguridad informática y apliquen estrategias, mecanismos, controles u otro tipo de actividades que ayuden a minimizar los riesgos de convertirse en víctimas de los delitos informáticos.

Siendo conscientes del incremento considerable de los casos de fraudes informáticos, ha causado preocupación debido a la importancia de la información que manejan los docentes y estudiantes de la UCACUE, extensión Cañar, surge la necesidad de realizar la presente investigación. Sin embargo, eliminar definitivamente los actos delictivos es un hecho imposible, más existe la posibilidad de prevenirlo y con esto poder reducir el impacto a la comunidad educativa.

BASES TEORICAS

Seguridad Informática

La seguridad informática se define como la disciplina encargada de buscar salvaguardar la integridad de la información, en funcionamiento de los sistemas informáticos, en si su función principal es proteger todo lo que es valioso para la institución ya sea infraestructura o datos. (Maribel, 2012, pág. 17)

Delito

"El delito es el hecho humano previsto de modo típico por una norma jurídica sancionada con penalización en sentido estricto, lesivo o peligroso para los bienes o intereses considerados merecedores de la más; enérgica tutela y expresión reprobable de la personalidad del agente, tal cuál es el momento de su comisión". (Ruiz Cruz, 2016, p. 8)

Delito informático

El delito informático implica actividades criminales que los países tratan de encuadrar en figuras típicas como robos, hurtos, fraudes, estafa, sabotaje, etc. Sin embargo, debe destacarse que los usos crecientes de las técnicas informáticas han proporcionado nuevos delitos, lo que han generado, a su vez, la necesidad de regulación jurídica (Ribero Corzo, 2016, pp. 27-28).

Delitos Informáticos en el Ecuador

En Ecuador, como en todos los países, existen delitos informáticos. No se encontró evidencia de estadísticas sobre delitos informáticos sobre olvidos o canjes de contraseñas para realizar algún mal a una persona u organización. Sin embargo, si se encontró información sobre de delitos de robo de contraseña en Internet (López Vallejo, 2017, pág. 37).

"En la actualidad, en el Ecuador cuenta con Leyes que sancionan este tipo de delitos con penas de privación de libertad, los mismos que están reconocidos en el Código Orgánico Integral Pena (COIP)" (Ramirez, 2017).

Los delitos informáticos reconocidos son:

- Pornografía infantil – 13 a 16 años de prisión.
- Violación del derecho a la intimidad – de uno a tres años de prisión
- Revelación ilegal de información de bases de datos – de uno a tres años de prisión
- Interceptación de comunicaciones – de tres a cinco años de prisión
- Pharming y Phishing – de tres a cinco años de prisión
- Fraude informático – de tres a cinco años de prisión
- Ataque a la integridad de sistemas informáticos – de tres a cinco años de prisión
- Delitos contra la información pública reservada legalmente – de tres a cinco años de prisión
- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones – de tres a cinco años de prisión.

Ilustración 1 Delitos Informáticos Fuente: (Ramirez, 2017)

Tipos de delitos informáticos

Gestión de TI es el proceso de supervisión de todos los asuntos relacionados con las operaciones y recursos de tecnología de la información dentro de una organización.

La ONU distingue 3 tipologías de delito informático, las que han sido aceptadas por la mayoría de la doctrina especializada, estas son:

Fraude Informático

"Conductas que consisten en la manipulación ilícita, a través de la creación de datos falsos o la alteración de datos o procesos contenidos en sistemas informáticos, realizada con el objeto de obtener ganancias indebidas" (Garzon Tapia & Vizuete Gallardo, 2013, p. 13).

El fraude se produce al ingresar datos de manera ilegal, para lo cual el ciberdelincuente debe tener alto nivel de conocimientos informáticos, llevando suponer que el mismo puede ser u empleado de una0 empresa que tiene acceso a sistemas o redes de información clasificada en donde puede ingresar y alterar datos para generar información falsa beneficiando al delincuente (Chungata Cabrera, 2015, p. 33).

Tipos de fraudes Informáticos

Existen varias maneras de cometer fraudes informáticos, entre ellas se mencionan las siguientes:

- **Manipulación de los datos de entrada**

Conocido también como sustracción de datos o manipulación del input, es el más común de los delitos informáticos ya que es fácil de cometer y difícil de descubrir.

Este tipo de fraude no requiere de conocimientos técnicos de informática y es realizable por cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos (Garzon Tapia & Vizuete Gallardo, 2013, p. 14).

- **Manipulación del programa.**

"Son todos los programas o códigos de computadora cuya función es dañar un sistema y dañar la computadora sin el conocimiento de su dueño, con finalidades muy diversas" (Pico Llerena, 2012, p. 80).

- **Manipulación de datos de salida**

  Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común, es el fraude a través de los cajeros automáticos; el mismo que se realiza mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.

  "Este delito comprende abusos o interferencias en el funcionamiento de un sistema de tratamiento automatizado de datos, con la intención de obtener un provecho y causar un perjuicio económico" (Avila, 2010, pág. 72).

- **Phishing**

Esta es una modalidad de estafa diseñada con la finalidad de robarle la identidad. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes (Pico Llerena, 2012, p. 79).

- **Spyware (Sustracción sin el conocimiento de la víctima)**

Los programas Spyware sirven para que el sujeto activo pueda sustraer datos del ordenador de la víctima con diversos fines, normalmente son datos sensibles y podría utilizarse para acceder a cuentas bancarias y códigos de tarjetas de crédito, con el riesgo que ello supone (Gonzales Suarez, 2014, p. 9).

Falsificación

Este delito es particularmente fraudulento, puesto que el autor sabe cómo lograr su objetivo, mediante la utilización de computadora con el fin de alterar o modificar mensajes de datos, documentación o cualquier información contenida en el ordenador.

La falsificación por medio de la informática se subdivide en:

- Falsificación por medio
- Como instrumento

Daños a Datos

"Hace referencia a las conductas consistentes en generar daño por medio de virus, gusano, acceso no autorizado por hacker o cracker".

Metodología de Análisis de Riesgos

- **Margerit**

Es una de las metodologías más utilizadas que permite el análisis de gestión de riesgos de los Sistemas de Información; fue creada por el Concejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información siguiendo la terminología de la norma ISO 31000 (Molina Miranda, 2015, p. 15).

- **ISO 27005**

Consiste en el establecimiento del contexto, evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo, comunicación y consulta del riesgo, supervisión y revisión del riesgo. Este proceso poder ser iterativo para la evaluación del riesgo y/o actividades de tratamiento del riesgo. Un enfoque iterativo para realizar la evaluación del riesgo puede aumentar la profundidad y el detalle de la evaluación en cada iteración (Banda Santisteban, 2019, p. 31).

- **Octave**

"OCTAVE es la metodología de Evaluación de Amenazas Operacionalmente Criticas, Activos y Vulnerabilidades para agilizar y optimizar el proceso de evaluación de riesgos de seguridad de la información alineados a los objetivos y metas de la organización" (Molina Miranda, 2015, p. 16).

METODOLOGÍA

Enfoque de la investigación

La presente investigación tendrá un enfoque mixto, por las siguientes consideraciones:

El enfoque cualitativo porque se considerará la participación de las personas dentro de la realidad del problema y así interpretar la imagen de la situación actual en su contexto.

Cuantitativo por lo se utilizará técnicas de recolección de datos estadísticos, y ofrecerá una forma clara para hacerse entender, poniendo énfasis en los resultados.

Nivel de investigación

Para la presente investigación se ha considerado el nivel descriptivo puesto que permite analizar el problema, mediante la delimitación de tiempo y espacio construyendo el análisis crítico, contextualización y los antecedentes investigativos.

También se consideró el uso del nivel exploratorio y la aplicación de un análisis de riesgo mediante la matriz de Magerit, para ello, se contará con la participación de los estudiantes y docentes de la Universidad Católica de Cuenca Extensión Cañar, con el fin de analizar los fraudes informáticos y su incidencia en la seguridad.

La información analizada en el presente estudio fue en base a una encuesta aplicada a los docentes y estudiantes de la UCACUE Extensión Cañar, las mismas que fueron respondidas a través de la herramienta Google Forms.

Población y muestra

En la presente investigación la población está conformada por 32 docentes y 440 estudiantes de la UCACUE, extensión Cañar, para el desarrollo del presente estudio se tomará una parte de la población mencionada, es decir se calculará una muestra finita para la aplicación de la encuesta. La muestra será obtenida mediante la aplicación de la formula estadística.

$$n = \frac{N * Z_\alpha^2 * p * q}{e^2 * (N-1) + Z_\alpha^2 * p * q}$$

Donde:

n= tamaño de la muestra buscado

N= Tamaño de la población o universo

e = Error de estimación máximo aceptado

Z= Parámetro estadístico en función del nivel de confianza

p= Probabilidad de que ocurra el evento estudiado.

q= (1 – p) = Probabilidad de que no ocurra el evento estudiado

Con un nivel de confianza del 95% y el margen de error del 5% se obtuvo la muestra de 206 estudiantes y 30 docentes a las cuales se les realizara la encuesta.

Gestión de riesgos (MAGERIT) para determinarla incidencias de fraudes informáticos.

La metodología MAGERIT cumple con una serie de fases para el análisis de riesgo.

La fase 1 consta de la identificación y valoración de los activos, las cuales los tipos de activos a ser evaluados fueron obtenidos del libro de Magerit versión 3.0 y la calificación de los mismos se realizó en base a lo que dicta la metodología, otorgándole un valor para cada dimensión de seguridad (Disponibilidad, Integridad, Confidencialidad, Autenticidad, trazabilidad) por activo, guiado en la escala de valoración determinada en la tabla Nº 1, el valor final se obtiene mediante una sumatoria de las dimensiones.

Tabla 1: Dimensión de valoración de los Activos

Bajo	1
Medio	2
Alto	3
Muy Alto	4
Critico	5

La fase 2 consta de la identificación y valoración de las amenazas, en esta fase se identifica las amenazas por cada tipo de activo, la valoración se lleva acabo de acuerdo a la lo expuesto en la tabla Nº 2, en dónde se tendrá que calificar el impacto y probabilidad de ocurrencia de dichas amenazas, en lo que respecta al valor del factor de Exposición se obtiene de la multiplicación del impacto por probabilidad.

Tabla 2: Valoración de Impacto y probabilidad por niveles.

Insignificante	**1**	**Improbable**	**1**	**FE = I*P**
Menor	**2**			
Moderado	**3**	**Probable**	**2**	
Mayor	**4**			
Catastrofico	**5**	**Casi Seguro**	**3**	
Impacto		Probabilidad		Factor de Exposición

La fase 3 consta de determinación del riesgo, para ello se realiza un cálculo matemático (Multiplicación) entre el activo y el factor de exposición, el rango o nivel de riesgo se basa en la tabla de intervalo que se muestra a continuación, tabla Nª 3.

Tabla 3: Descripción de los intervalos para determinar el nivel de Riesgo

R= VA*FE	
Bajo	1--37
Medio	38--74
Alto	75--111
Critico	112--375
RIESGO	

Con el cumplimiento de estas fases se logra determinar el nivel de incidencias de las diferentes amenazas que se puedan presentar en el manejo de los medios tecnológicos.

RESULTADOS

Encuesta

El rango de edad de los estudiante y docentes encuestados fue de 18 a 65 años, se obtiene como resultado el 83% en las edades entre los 18 a 35 siendo el porcentaje más alto de los encuestados, un 13% en las edades entre 36 a 45 años y un 4% en las edades de 46 a 65 años.

La mayor parte de las personas encuestadas responden que WhatsApp es la red social más utilizada en la actualidad con un 35%, seguida de Facebook en la que también interactúan con un porcentaje de 26%, TikTok con 20% y Instagram con 13%. El 56% de los estudiantes y docentes encuestados, mencionan que sus contactos no les piden permiso para subir a las redes sociales una foto o video en el que se encuentre incluido, el 35% responde que a veces les piden permiso, sin embargo, solo 9% misiona que sus contactos si les piden permiso al momento de subir una foto o video.

Con respecto al comportamiento de estas redes sociales, los encuestados están consciente del peligro que se pueda presentar, de acuerdo a la encuesta el 61% admiten que aceptan solicitudes de amistada solo de las personas que les parecen conocidos, el 35% admiten que aceptan solicitudes de amistad solo a los que conocen en persona, y el 4% acepta todas las solicitudes así no los conozca.

En cuanto a la seguridad para el ingreso a estas redes sociales, se obtiene que el 85% cumple con en el uso correcto de las contraseñas y el 5% no cumple con lo establecido en las políticas. Con lo que respecta al tiempo de cambio de contraseña el 56 % menciona que realizan el cambio cada vez que la aplicativo se lo pida. El 46% responde que utiliza el gestor de contraseñas de google para ciertas aplicaciones, lo que sería una ventaja, pero al mismo tiempo presenta inconvenientes en el uso de la misma, debido a que se puede presentar fallos en el servicio y esto podría afectar a las contraseñas guardadas.

En lo que respecta a los incidentes en las redes sociales el 68% de los encuestados mencionan que no han sufrido hackeo en sus cuentas, el 20 % menciona que si han sufrido de hackeo. El 40% entre estudiantes y docentes admiten que fueron víctima de virus, software malicioso que se instalaron en sus equipos informáticos al ingresar a ciertos sitios web.

Al navegar en las redes sociales, algunos de los encuestados mencionan que han tenido problemas, entre ellas con un 12% han sufrido intentos de fraude, el 8% indican que han perjudicado su imagen, su vida laboral y social. El 20% han sido víctima de fraude informático, el 64% de los encuestados creen que los delincuentes cometen fraudes informáticos con el fin de causar daños económicos y el 36% por causar daño moral a las personas.

Ante el tipo de fraude informático más común, el 43% entre docentes y estudiantes creen que es el robo de credenciales bancarias, ya que la finalidad de los mismos es causar daños económicos, mientras que el 24% menciona que el robo de cuenta de las redes sociales es el más común, de manera que, mediante la suplantación de identidad pueden llegar a engañar a cualquier persona y lograr su objetivo.

En cuanto al respaldo de información de diferentes dispositivos electrónicos, el 56% menciona que, si realizan el respectivo respaldo en caso de que la información se vea afectada por algún ataque, virus o en su defecto perdida del dispositivo. En lo que respecta al proceso de respaldo el 64% responde que a veces lo realizan de forma continua y el 20% si realiza respaldos de forma continua, es decir que ellos establecen cronogramas con fechas y hora en la que deben realizar el respectivo proceso.

Las tecnologías de la información y comunicación abarcan sin duda el ordenador y sobre todo el internet, ya que son medios que permiten el almacenamiento, recuperación y comunicación de la información, a más de ellos es el medio por el que los atacantes cometen distintos delitos, por lo que toda información almacenada debe estar protegido, de acuerdo a la encuesta el 64% afirman que toman medidas necesarias para proteger la información que almacenan e intercambian en internet, también afirman que si reciben SMS o E-mails desconocidos el 60% lo elimina, con el fin de no correr riesgo al abrirlos.

Análisis de Riesgo mediante MAGERIT

Con los resultados obtenidos en el análisis de la encuesta, se determinaron variables que fueron tomadas como activos para el desarrollo de la matriz de MAGERIT, en donde se

determinó las amenaza más comunes y peligrosos en cada activo. Los resultados se reflejan en la siguiente tabla Nº4.

Tipo de activo	Codigo	Activo	Dimenciones de Valoracion						Bajo 1 Medio 2 Alto 3 Muy Alto 4 Critico 5	Catalogo de Amenazas	Calculo del Riesgo							
			Disponibilidad	Integridad	Confidencialidad	Autenticidad	Trazabilidad	TOTAL /25			Insignificante 1 Menor 2 Moderado 3 Mayor 4 Catastrofico 5	Improbable 1 Probable 2 Casi Seguro 3	FE = I*P		R= VA*FE Bajo 1--37 Medio 38--74 Alto 75--111 Critico 112--375	
										Amenazas	Impacto	Probabilidad	Factor de Exposición	RIESGO		
[SW] Software - Aplicaciones informáticas	A1	Facebook	4	5	3	2	2	16		Error en aceptar solicitudes de amistada a personas extrañas o desconocidas	5	3	15	240		
										Suplantacion de identidad del usuario	5	4	20	320		
										Destruccion de informacion	4	3	12	192		
										Divulgacion de infromacion	5	3	15	240		
	A2	WhatsApp	4	5	3	2	2	16		Suplantacion de identidad del usuario	5	3	15	240		
	A5	Instagram	4	5	3	2	2	16		Suplantacion de identidad del usuario	5	3	15	240		
[D] Datos / Información	A6	Datos personales	4	4	5	3	3	19		Divulgación de información	5	3	15	285		
										Suplantación de la identidad del usuario	4	3	12	228		
										Fugas de información	5	2	10	190		
[K] Claves criptográficas	A7	Contraseña	3	4	5	4	2	18		Fugas de información	4	3	12	216		
										Acceso no autorizado	5	3	15	270		
										Suplantación de la identidad del usuario	5	2	10	180		
[HW] Equipamiento informático (hardware)	A9	Telefono Celular	4	4	4	2	2	16		Robo	4	3	12	192		
										Emanaciones electromagnéticas	5	3	15	240		
[COM] Redes de comunicaciones	A11	Internet	5	5	5	4	3	22		Suplantación de la identidad del usuario	4	3	12	264		
										Fallo de servicios de comunicaciones	4	2	8	176		
[P] Personal	A12	Estudiantes	5	5	2	2	2	16		Fuga de informacion	4	3	12	192		
										Extorsión	5	3	15	240		
	A13	Docentes	5	5	3	2	2	17		Ingeniería social (picaresca)	5	3	15	255		

La suplantación de identidad y la divulgación de información son unas de las amenazas más comunes que se presentan en algunos tipos de activos como son: Software -

Aplicaciones informáticas, Datos / Información, Claves criptográficas, Redes de comunicaciones. En cuanto al tipo de actico Personas en las que están inmersos los estudiantes y docentes el análisis dio como resultado que la fuga de información, la extorción y la ingeniería social son las amenazas más críticas que se pueden presentar en el manejo de las redes de comunicación.

DISCUSIÓN

El estudio refleja que tanto docentes como estudiantes han sido víctima de algún tipo de fraude informático, para ello y en base a la matriz de riesgo se analiza cada una de las amenazas que se encontraron en un nivel de riesgo crítico.

Suplantación de identidad de usuario, es una de las amenazas con mayor nivel de criticidad, debido a que, con el crecimiento del internet, las redes sociales, etc., provoca que personas con intenciones maliciosas tenga más oportunidades de ocupar la identidad de otra, a este tipo de conducta se le considera un delito o fraudes informáticos conocido como Phishing, siendo el principal objetivo de este tipo de delito, obtener información personal ya sea del estudiante o docentes a través de engaños (suplantación de identidad). "Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventana emergentes" (Maribel, 2012, pág. 95). Se determina que el 28% entre docentes y estudiantes, responden E-mails sin verificar si estos provienen de fuentes confiables y 37% Ingresan a sitios sugeridos por ventanas emergentes, lo cual provoca ser víctima de este tipo fraude.

Divulgación de información otra de las amenazas con un nivel de riesgo alto, consiste en exponer y difundir un contenido o varios contenidos que pueden ser de interés público, hoy en día existen herramientas con las cuales se puede divulgar cualquier contenido, dichas herramientas pueden ser manejadas a través del fraude informático conocido como Caballo de Troya el cual se encarga de "ocultar un programa informático en un computador ajeno, para ejecutar acciones no autorizadas" (Herrera & Salinas, 2015, pág. 174). Estas acciones pueden ser como: hacer público una foto, video o información que comprometa su Integridad. El 37% de los encuestados afirman que al navegar en internet e ingresar a diferentes sitios web han sido víctimas de software maliciosos, la ejecución de dichos software por simple curiosidad trae grabes consecuencias, la incidencia de dicho fraude es alto puesto tanto docentes como estudiantes cuentan con información en

sus dispositivos electrónicos, la misma que puede ser aprovechado por estos atacantes con el fin de obtener algún beneficio.

Fuga de información es una amenaza que consiste en perder la confidencialidad de la información ya sea de una empresa o individuo, mediante la obtención de la misma por parte de personas no autorizadas, esta conducta va relacionada con el delito de Ingeniería social, es un tipo de fraude que hace uso de técnicas para engañar a los usuarios, los estudiantes y docentes pueden ser víctima de dicho delito, debido a que carecen de poco conocimiento y no saben con certeza cuál es la mejor manera de proteger su información, dando paso a que terceros con engaños pueden obtener información que les pueda perjudicar. Influyen factores como: Uso excesivo de las redes sociales, login y password visibles para terceras personas, Información importantes anotadas en hojas volantes que pueden ser desechados, etc.

Extorción es una de las amenazas que se presenta habitualmente en los adultos (Docentes), consta de un delito informático que a través del uso de un medio digital el atacante obliga a las personas mediante amenazas a realizar actos ilícitos con la intención de producir un perjuicio de carácter patrimonial o bien del sujeto pasivo, la mayoría de los casos se presentan al navegar en internet y en las redes sociales, el nivel de incidencia de este delito resulta preocupante, ya que el 67% de los encuestados afirma aceptar solicitudes de personas que creen conocer, sin ser conscientes de que los atacantes puedan estar suplantando identidad de una persona conocida, el cual solicite información de carácter personal y estas puedan ser utilizados para ser extorsionados.

CONCLUSIONES

Con la aplicación de la encuesta a los estudiantes y docentes de la Universidad Católica de Cuenca Extensión Cañar y el análisis de la misma, se determina el alto grado de desconocimiento respecto a todas las amenazas informáticas que se encuadran dentro de los conocidos como fraudes informáticos, las cuales representan un riesgo a la integridad física, moral y económica de los estudiantes y docentes de la UCACUE.

De acuerdo al análisis realizado en la matriz de MAGERIT, se determina que las mayores amenazas se encuentran asociadas a la perdida de información personal como (Fotos, videos, documentos confidenciales), siendo esta la suplantación de identidad, divulgación de información, fuga de información, robo, etc., con un nivel de riesgo crítico, en base al análisis de riesgo de estas amenazas, se determinó los métodos con mayor incidencia que se encuentran dentro de la categoría de los fraudes informáticos tales como: Pishing, Caballo de Troya, Ingeniería Social, Extorción, Datos falsos o engañosos, que afecta a los sistemas informáticos y personas.

La falta de conocimiento en el manejo de medios tecnológicos por parte de los estudiantes y docentes, provoca que sean víctima de fraudes informáticos, en base al estudio el más común en los jóvenes es el fraude conocido como Pishing (Engaño), estas se presentan en su gran mayoría en las redes sociales, por medio de la aceptación de solicitudes de amistad de personas desconocidas, debido a esta acción los jóvenes pueden ser víctimas de otro tipo de delitos como: Acoso, Ciberbullying, Sexting, etc. Otro de los fraudes más comunes fue la Extorción (Fines Económicos), esto se presenta habitualmente en las personas adultas (docentes), ya que aprovechan las vulnerabilidades en el manejo de los medios tecnológicos, quedando expuestos a que los criminales obtienen toda información confidencial y amenazar con exponerla a menos que le cancele cierta cantidad de dinero.

BIBLIOGRAFÍA

Chungata Cabrera, A. M. (04 de 03 de 2015). *dspace.ucuenca.edu.ec.* Obtenido de http://dspace.ucuenca.edu.ec/bitstream/123456789/21321/1/TESIS.pdf

Avila, C. H. (01 de 01 de 2010). *dspace.ucuenca.edu.ec.* Obtenido de https://dspace.ucuenca.edu.ec/bitstream/123456789/2673/1/tm4391.pdf

Banda Santisteban, J. C. (22 de 10 de 2019). *tesis.usat.edu.pe.* Obtenido de tesis.usat.edu.pe: https://tesis.usat.edu.pe/bitstream/20.500.12423/2159/1/TM_BandaSantistebanJose.pdf

Garzon Tapia, P. N., & Vizuete Gallardo, M. F. (08 de 04 de 2013). *repositorio.utc.edu.ec.* Obtenido de http://repositorio.utc.edu.ec/bitstream/27000/139/1/T-UTC-0066.pdf

Gonzales Suarez, M. (13 de 05 de 2014). *digibuo.uniovi.es.* Obtenido de https://digibuo.uniovi.es/dspace/bitstream/handle/10651/27824/TFM_Gonzalez%20Suarez%2C%20Marcos.pdf?sequence=3&isAllowed=y

Herrera, J. V., & Salinas, Y. C. (2015). LOS DELITOS INFORMÁTICOS Y SU PENALIZACIÓN EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL ECUATORIANO. *SATHIRI*, 171-194. Obtenido de https://revistasdigitales.upec.edu.ec/index.php/sathiri/article/view/404

López Vallejo, M. R. (2017). Hacking ético. Vulnerabilidad de Sistemas Operativos en el acceso por contraseñas. *Revista Publicando*, 31-51. Obtenido de https://revistapublicando.org/revista/index.php/crv/article/view/407/pdf_259

Maribel, P. L. (01 de 11 de 2012). *repositorio.uta.edu.ec.* Obtenido de https://repositorio.uta.edu.ec/bitstream/123456789/2899/1/Tesis_t763si.pdf

Molina Miranda, M. F. (10 de 07 de 2015). *www.dit.upm.es.* Obtenido de http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf

Pico Llerena, E. M. (16 de 11 de 2012). *repositorio.uta.edu.ec.* Obtenido de https://repositorio.uta.edu.ec/bitstream/123456789/2899/1/Tesis_t763si.pdf

Ramirez, R. (27 de 12 de 2017). *www.policia.gob.ec*. Obtenido de https://www.policia.gob.ec/delitos-informaticos-establecidos-en-el-coip-y-como-prevenirlos/

Ribero Corzo, S. M. (04 de 11 de 2016). *repository.unab.edu.co.* Obtenido de https://repository.unab.edu.co/bitstream/handle/20.500.12749/1305/2016_Tesis_Ribero_Corzo_Sylvia_Margarita.pdf?sequence=1&isAllowed=y

Ruiz Cruz, C. A. (01 de 12 de 2016). *dspace.unl.edu.ec.* Obtenido de dspace.unl.edu.ec: https://dspace.unl.edu.ec/jspui/bitstream/123456789/17916/1/Tesis%20Lista%20Carolin.pdf

Trabajo de Titulación

Tema:

Fraudes informáticos y su incidencia en la seguridad de los docentes y estudiantes de la UCACUE, extensión Cañar.

Unidad Académica

Tecnologías de la Información y la Comunicación

Carrera

Ingeniera de Sistemas

Alumna

Tania Estefanía Chalán Guamán.

Tutor:

Ing. Cristian Humberto Flores Urgiles

Abril – Agosto-2021

Cañar, 22 de abril de 2021

Ingeniero

Leopoldo Pauta Ayabaca, Msc.

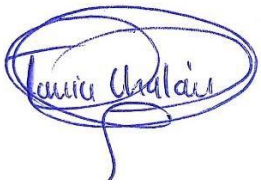
DECANO DE LA UNIDAD ACADÉMICA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Ciudad.

Yo, **TANIA ESTEFANIA CHALAN GUAMAN**, con número de identificación **0302893557**, alumna de la carrera de Ingeniería de Sistemas, solicito por su intermedio a Consejo Directivo la aprobación del tema de tesis **"FRAUDES INFORMÁTICOS Y SU INCIDENCIA EN LA SEGURIDAD DE LOS DOCENTES Y ESTUDIANTES DE LA UCACUE, EXTENSIÓN CAÑAR.",** proponiendo como tutor de la misma al Ing. Cristian Humberto Flores Urgiles, el tema propuesto está considerado su desarrollo en décimo ciclo, ya que estaré matriculado en la Unidad de Titulación.

Por la atención que Ud. y el Honorable Consejo Directivo le brinden a la presente, anticipo mis sentimientos de consideración y estima para cada uno de Uds.

Atentamente;



Srta. TANIA ESTEFANIA CHALAN GUAMAN

Estudiante de Ingeniería de Sistemas, extensión Cañar
CI: 0302893557

Anexo: Formato del Anteproyecto.

A. TÍTULO
Fraudes informáticos y su incidencia en la seguridad de los docentes y estudiantes de la UCACUE, extensión Cañar.

B. DOMINIO, LÍNEA Y ÁMBITOS DE INVESTIGACIÓN			
Tecnologías de Información y Comunicación	**Ciencias exactas, naturales y tecnológicas**	Analítica de Datos	
		Ingeniería de Software	
		Algoritmos computacionales	
		Inteligencia de negocios	
		Gobierno de Ti	
		Auditoria y seguridad informática	X
		Simulación	

C. PLANTEAMIENTO DEL PROBLEMA

En la actualidad las tecnologías de la información y las comunicaciones están cambiando a la sociedad y al mundo, al mejorar la productividad en las industrias tradicionales, revolucionar los procesos laborales. Este crecimiento rápido también ha desencadenado nuevas formas de delincuencia informática, como son los fraudes informáticos y las diferentes formas de manipulación y como la seguridad de la información es afectada por estos delitos informáticos.

Por eso el presente trabajo se basa en un análisis a través de encuestas para medir las cualidades de como manejan las tecnologías docentes y estudiantes de la Universidad Católica de Cuenca Extensión Cañar. Con el fin de precautelar la seguridad y evitar que se cometan fraudes informáticos y que tan inmersos son a caer en manipulaciones.

D. OBJETIVO GENERAL

Analizar los fraudes informáticos y su incidencia en la seguridad de los docentes y estudiantes de la UCACUE, extensión Cañar.

E. OBJETIVOS ESPECÍFICOS

1. Realizar encuestas para medir el nivel de seguridad que existe al momento de utilizar medios tecnológicos.
2. Analizar las diferentes fraudes informáticos y como inciden en los usuarios el impacto de estos actos en la vida social y en la tecnología.
3. Determinar los diferentes factores que influyen en el fraude informático

F. JUSTIFICACIÓN

Históricamente los Delitos Informáticos tuvieron su origen, a finales de la segunda guerra mundial, en donde a través de las armas de guerra ya sean estas nucleares o químicas comenzaron a encontrar e investigar nuevas formas de poder vulnerar a los estados que se encontraban en conflicto unos con otros, es decir ya comenzaron a través de la investigación tecnológica a atacar a equipos de telecomunicaciones de los países, para así poder dejarlos sin derecho a pedir ayuda, refuerzo o armamento o mejor dicho sin acceso o derecho a comunicarse para protegerse.

Estos avances dieron lugar a la creación del primer satélite artificial llamado SPUNIK, creado por la EX UNION SOVIETICA (04 de octubre de 1957), quienes tomaron el liderazgo más pronto que los Estados Unidos de América, y ya habían anunciado al mundo sobre una carrera inter espacial. Dos años más tarde los Estados Unidos de América crean el departamento ADVANCED RESEARCH PROJECTS

AGENCY (arpa), traducido en español agencia de proyectos de investigación avanzada, con lo que marcó el comienzo del uso de las Comunicaciones Globales, manejado exclusivamente por intelectuales de élite.

Debido a que con el crecimiento de la tecnología, también se ha incrementado el mal uso de la misma y han aparecido una serie de actos ilícitos, a los que se han denominado de manera general "delitos informáticos", Es así que una vez que el campo del Internet comenzó a recorrer el mundo, también la delincuencia informática tomo piso y recorrió varios sectores tanto públicos como privados, donde hoy en día el uso de estas tecnologías que tanto bien hizo a la sociedad en lo que tiene que ver a la comunicación a través del ciberespacio comienza a perjudicar a la misma, tornándose en un factor gravemente controlable, es decir, como la ciencia y la tecnología están al alcance de todos no se puede prevenir o mejor dicho la intención de prevenir a estos ciber-delincuentes hoy en día es más difícil y se necesita de muchos recursos estatales para poder frenar estos abusos que son cometidos a través de las máquinas manipuladas y premeditadas por el ser humano.

Llegando a lo que hoy se conoce como delitos transnacionales, aunque el mismo no se encuentra aún normado, pero que en algunas legislaciones de algunos países, ya se lo está tipificado como delito transnacional ya que su potencial incursión en el mundo está causando grandes pérdidas, ya sean estas de carácter económico, como también de carácter personal, que afectan de manera general a la sociedad como lo es en el campo de los servicios de primera necesidad en los que se encuentran aeropuertos, hospitales, juzgados, instituciones bancarias llegando a un punto mayor como lo es el

terrorismo y la delincuencia organizada con la que se opera desde varios países para manipular y desatar un perjuicio a los estados. [1]

G. ALCANCE

Analizar los diferentes Fraudes informáticos y su incidencia en la seguridad de los docentes y estudiantes de la UCACUE, extensión Cañar.

H. CONCEPTOS RELACIONADOS

Fraudes

Conductas que consisten en la manipulación ilícita, a través de la creación de datos falsos o la alteración de datos o procesos contenidos en sistemas informáticos, realizada con el objeto de obtener ganancias indebidas. [2]

formas de fraude:

- **Manipulación de los datos de entrada. -**

Este tipo de fraude informático, conocido también como sustracción de datos, representa el delito informático más común, ya que es fácil de cometer y difícil de descubrir. El mismo, que no requiere conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

- **Manipulación de programas.-**

Es muy difícil de descubrir y a menudo pasa inadvertido, debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas.

- **Manipulación de los datos de salida. -**

Se efectúa fijando un objetivo al funcionamiento del sistema informático. Elejemplo más común, es el fraude a través de los cajeros automáticos; el mismo, quese realiza mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas. Sin embargo, en la actualidad se usa equipos y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito. [2]

- **Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:**
    - Acceso ilícito a sistemas informáticos.
    - Interceptación ilícita de datos informáticos.
    - Interferencia en el funcionamiento de un sistema informático.
    - Abuso de dispositivos que faciliten la comisión de delitos.
- **Delitos informáticos:**
    - Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.

- Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.

- **Delitos relacionados con el contenido:**
  - Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

- **Ataques que se producen contra el derecho a la intimidad:**

Delito de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos. (Artículos del 197 al 201 del Código Penal)

- **Infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor:**

Especialmente la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas. (Artículos 270 y otros del Código Penal)

- **Falsedades:**

Concepto de documento como todo soporte material que exprese o incorpore datos. Extensión de la falsificación de moneda a las tarjetas de débito y crédito. Fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad. (Artículos 386 y ss. del Código Penal)

- **Sabotajes informáticos:**

Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos. (Artículo 263 y otros del Código Penal)

- **Fraudes informáticos:**

Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito. (Artículos 248 y ss. del Código Penal)

- **Amenazas:**

Realizadas por cualquier medio de comunicación. (Artículos 169 y ss. del Código Penal)

- **Calumnias e injurias:**

Cuando se propaguen por cualquier medio de eficacia semejante a la imprenta o la radiodifusión. (Artículos 205 y ss. del Código Penal)

- **Pornografía infantil:**

Entre los delitos relativos a la prostitución al utilizar a menores o incapaces con fines exhibicionistas o pornográficos. [4]

Seguridad de red

La seguridad de red se refiere a cualesquiera actividades diseñadas para proteger la red. En concreto, estas actividades protegen la facilidad de uso, fiabilidad, integridad y seguridad de su red y datos. La seguridad de red efectiva se dirige a una variedad de amenazas y la forma de impedir que entren o se difundan en una red de dispositivos. ¿Y cuáles son las amenazas a la red? Muchas amenazas a la seguridad de la red hoy en día se propagan a través de Internet. Los más comunes incluyen:

- Virus, gusanos y caballos de Troya
- Software espía y publicitario

- Ataques de día cero, también llamados ataques de hora cero
- Ataques de hackers
- Ataques de denegación de servicio
- Intercepción o robo de datos
- Robo de identidad [5]

I. TRABAJOS RELACIONADOS

Para el presente proyecto se toma como referencia los siguientes trabajos y se puntualizara los temas que nos servirán.

Un estudio realizado en la Universidad Nacional de Loja modalidad de estudios a distancia carrera de Derecho La presente investigación denominada ““ANÁLISIS DE LOS DELITOS INFORMÁTICOS Y SU VIOLACIÓN DE LOS DERECHOS CONSTITUCIONALES DE LOS CIUDADANOS” tiene como objeto dar una visión clara sobre los delitos informáticos en especial sobre la violación de los derechos constitucionales de los ciudadanos, que se generan por la utilización de las tecnologías de la información y de la comunicación, como el correo electrónico, transacciones financieras, comercio electrónico y la utilización de las redes sociales; se analiza y conceptualiza la naturaleza de las Infracciones Informáticas y sus tipificaciones de acuerdo a sus características principales y se establecen alternativas de soluciones para sancionar los delitos informáticos y evitar la vulneración de los derechos constitucionales del ofendido. [3]

Documento que servirá para el análisis de los diferentes delitos informáticos existentes y como se vulneran los derechos.

De la misma manera una tesis realizada en la Universidad Técnica de Cotopaxi Unidad Académica de Ciencias Administrativas y Humanísticas, trabajo de Investigación sobre el tema: "LOS DELITOS INFORMÁTICOS Y SU PERJUICIO EN LA SOCIEDAD" se establece la conceptualización respectiva del tema, generalidades asociadas al fenómeno, estadísticas mundiales sobre delitos informáticos, el efecto de éstos en diferentes áreas, como poder minimizar la amenaza de los delitos a través de la seguridad, aspectos de legislación informática, y por último se busca unificar la investigación realizada para poder establecer el papel de la Ley Penal frente a los delitos informáticos. [4]

Tesis que se utilizada para tomar en cuenta definiciones teóricas y cuáles son las diferentes formas de minimizar los fraudes informáticos.

J. METODOLOGÍA

El método a utilizar en el presente trabajo de investigación será cualitativa y descriptiva porque vamos a medir las acciones de los docentes y estudiantes al momento de trabajar con la tecnología y cuáles son las vulnerabilidades en su seguridad y descriptiva de como ellos puedan evitar fraudes informáticos y no caigan en manipulaciones.

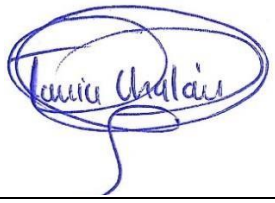
K. CRONOGRAMA DE ACTIVIDADES																						
N°	ACTIVIDAD	MES I				MES II				MES III				IV				V				
		S1	S2	S3	S4	S 1	S2	S 3	S 4	S1	S 2	S3	S4	S 1	S 2	S 3	S 4	S1	S 2	S 3	S4	MEDIOS DE VERIFICACIÓN
1	**Realizar un estudio teórico sobre los diferentes fraudes informáticos**																					
	Buscar Información en la Bases de Datos	X	X																			Hojas de Word con los links de los documentos encontrados
2	**Analizar las diferentes opciones que influyen a la hora de realizar fraudes informáticos**																					
	Realizar investigaciones de los diferentes factores que influyen en la manipulación para realizar los fraudes informáticos			X	X																	Hojas de word con los links de fraudes informáticos y las diferentes formas de fraude
3	**Realización de una encuesta a estudiantes y alumnos de la UCACUE extensión Cañar**																					
	Realizar encuestas					X																Encuestas
	Analizar los datos obtenidos						X															Encuestas
4	**Realizar un breve análisis de lo que está pasando los docentes y estudiantes para poder definir cuales los puntos débiles en su seguridad.**																					
	Análisis de la seguridad																					En base a las encuestas y documentos analizados

L. DECLARACIÓN FINAL
Los abajo firmantes declaramos bajo juramento que el proyecto descrito en este documento no ha sido presentado a otra institución nacional o internacional para su financiamiento, no causa perjuicio al ambiente, es de nuestra autoría y no transgrede norma ética alguna.

M. PARTICIPANTES	
DIRECTOR:	Ing. Danny Andrade Cárdenas
ESTUDIANTE 1	Tania Estefanía Chalán Guamán

N. FIRMAS DE RESPONSABILIDAD	
Lugar:	Cañar
Fecha:	09/03/2021

Firmas:



Nombre: Ing. Cristian Humberto Flores Urgiles CC: 0301638375 **Director del Proyecto**	Nombre: Tania Estefanía Chalán Guamán C.C.: 0302893557 **Estudiante / Egresado**

O. APROBACIÓN	
Firmas:	
Nombre: CC: **Primer Par Revisor**	Nombre: C.C.: **Segundo Par Revisor**

P.REFERENCIAS

REFERENCIAS

[1] F. Riofrío, *Los Delitos Informáticosy su Tipificación en la Legislación Ecuatoriana,* A, 2012.

[2] P. N. G. TAPIA, «“El FRAUDE INFORMÁTICO: VALORACIONES TÉCNICO-JURÍDICAS”,» Latacunga, 2006.

[3] D. M. C. Vallejo, «DerechoEcuador.com,» [En línea]. Available: https://www.derechoecuador.com/.

[4] C. FURENSIC, «COMPUTER FURENSIC,» [En línea]. Available: https://www.delitosinformaticos.info/delitos_informaticos/definicion.html.

[5] E. d. Expertos, «VIU UNIVERSIDAD INTERNACIONAL DE VALENCIA,» 21 03 2018. [En línea]. Available: https://www.universidadviu.com/int/actualidad/nuestros-expertos/tres-tipos-de-seguridad-informatica-que-debes-conocer.

[6] C. A. R. Cruz, «“ANÁLISIS DE LOS DELITOS INFORMÁTICOS Y SU VIOLACIÓN DE LOS DERECHOS CONSTITUCIONALES DE LOS CIUDADANOS”,» Loja, 2016.

[7] A. S. B. Eduardo, «“LOS DELITOS INFORMÁTICOS Y SU PERJUICIO EN LA SOCIEDAD”,» Latacunga, 2012.

UNIVERSIDAD CATÓLICA DE CUENCA
COMUNIDAD EDUCATIVA AL SERVICIO DEL PUEBLO

SOLICITUD PARA:

Beca o ayuda económica, Justificación de faltas ,Justificación de pruebas, Justificación de trabajos, Justificación de lecciones, Justificación de prácticas, Licencia eventual, Examen postergado, Examen supletorio, Segunda matrícula, Tercera matrícula, Matrícula especial, Matrícula extraordinaria, Record académico, Hojas certificadas, Examen suficiencia, Tutorías, Rectificación de nombres, Malla curricular, Reposición de título, Otros

Fecha: 04 - 07 - 2022

Dirigido a: Ing Priscila Ruiz Mgs.
Coordinadora del Campus Cañar.

Solicitante: Tania Chalán

Carrera: Ingeniería de Sistemas

Año/Ciclo: Paralelo:

Asunto: Solicito Comedidamente autoria aplicación de Encuesta como parte de mi trabajo de Titulación, a Docentes y Estudiantes del Campus Cañar

Solicitante

Constancia de Presentación.- Fecha: Cañar, 04 de Julio de 2022

Hora: 15' 12

Resolución:

Notificado 05-07-2022

Universidad Católica de Cuenca EXTENSIÓN CAÑAR COORDINADOR GENERAL

Universidad Católica de Cuenca EXTENSIÓN CAÑAR SECRETARÍA CATÓLICA DE CUENCA

Valor $ 5,00

N° 0229904

Universidad Católica de Cuenca

Articulo

INFORME DE ORIGINALIDAD

9%	9%	0%	3%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	kwaas.org Fuente de Internet	1 %
2	docplayer.es Fuente de Internet	1 %
3	bibliotecadigital.icesi.edu.co Fuente de Internet	1 %
4	core.ac.uk Fuente de Internet	1 %
5	repository.unab.edu.co Fuente de Internet	1 %
6	journalprosciences.com Fuente de Internet	1 %
7	Submitted to Universidad Autónoma de Aguascalientes Trabajo del estudiante	1 %
8	searchdatacenter.techtarget.com Fuente de Internet	1 %
9	alteridad.ups.edu.ec Fuente de Internet	

1 %

10	cienciadigital.org Fuente de Internet	1 %

Excluir citas	Activo	Excluir coincidencias	< 1%
Excluir bibliografía	Activo		

Pro Sciences
Revista de Producción, Ciencias e Investigación.
http://www.journalprosciences.com/index.php/ps

CONSTANCIA DE ACEPTACIÓN DE ARTÍCULO

PRO SCIENCES: REVISTA DE PRODUCCIÓN, CIENCIAS E INVESTIGACIÓN con ***ISSN: 2588-1000***, perteneciente al ***CENTRO DE INVESTIGACIÓN Y DESARROLLO PROFESIONAL***, en cabeza de su editor Joffre León-Acurio.

Hace constar:

Que, el artículo titulado: **"FRAUDES INFORMÁTICOS Y SU INCIDENCIA EN LA SEGURIDAD DE LOS DOCENTES Y ESTUDIANTES DE LA UCACUE, EXTENSIÓN CAÑAR",** de autoría de los investigadores: **Tania Estefanía Chalán Guamán, Cristhian Humberto Flores Urgiles, Cristina Mariuxi Flores Urgiles, Luis Fernando Pinos Castillo, Julio Jhovanny Santacruz Espinoza,** se presentó el 2 de septiembre de 2022 en nuestra revista para su revisión.

Se informa que el artículo fue sometido a un proceso *double–blind_peer–review*, para verificar el cumplimento de las políticas y directrices de los autores requeridas por la revista, siendo así la decisión final, **PUBLICABLE**, mismo que se visualizará en la edición Vol. 6. N° 46 (2022) diciembre.

Asimismo, se declara que actualmente la revista se encuentra incluida en: ***Latindex Catálogo 2.0; REDIB (Red Iberoamericana de Innovación y Conocimiento Científico); MIAR; Actualidad Iberoamericana; ERIHPLUS (European Reference Index for the Humanities Social Sciences); OAJI (Open Academic Journals Index); LatinREV (Red Latinoamericana de Revistas Académicas en Ciencias Sociales y Humanidades); Research Bib; BASE; PKP INDEX; Open Archives; Open AIRE Explore; ISSN (International Standard Serial Number Internacional Centre); CROSSREF (Content Registration); Signatory of DORA***.

Las ediciones de la revista se encuentran publicadas en el portal de **Pro Sciences: Revista de Producción, Ciencias e Investigación** http://www.journalprosciences.com/index.php/ps

Para constancia, se firma la presente en la ciudad de Babahoyo a los 28 días del mes de septiembre del año 2022.

Cordialmente,

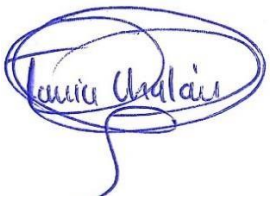
Ing. Práxedes Montiel-Díaz, MSc.
Directora
Pro Sciences: Revista de Producción, Ciencias e Investigación
Centro de Investigación y Desarrollo Profesional

(+593) 98 529 2824| editor@journalprosciences.com | http://www.journalprosciences.com/index.php/ps
Isaías Chopitea y Juan X Marcos | Babahoyo – Los Ríos - Ecuador

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Tania Estefania Chalán Guamán portador de la cedula de ciudadanía N.º 0302893557 En calidad de autor y titular de los derechos patrimoniales de trabajo de titulación" **FRAUDES INFORMÁTICOS Y SU INCIDENCIA EN LA SEGURIDAD DE LOS DOCENTES Y ESTUDIANTES DE LA UCACUE, EXTENSIÓN CAÑAR."** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos. Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de este trabajo de titulación en Repositorio Institucional de conformidad a los dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cañar, **22 de septiembre 2022**



F: …….

Tania Estefania Chalán Guamán

C.I. 0302893557