UNIVERSIDAD DE PANAMÁ

VICERRECTORÍA DE INVESTIGACIÓN Y POSTGRADO

FACULTAD DE CIENCIAS DE LA EDUCACIÓN

MAESTRÍA EN DOCENCIA SUPERIOR

TESIS:

“Métodos de Fraude Cibernético en la Universidad de Panamá”

Trabajo presentado como requisito

para optar al grado de

Maestría en Docencia Superior

Profesora Asesora:

Dra. Nancy Castillo

Presentado Por:

Yeilín del Carmen Jiménez Barría

Octubre, 2024

DEDICATORIA

El presente trabajo está dedicado a mi familia, mi hijo Alessandre Bellido, a mi hermano Luis Fabián y mi esposo Javier Bellido quienes son la fuente de mi fuerza, apoyo e inspiración para llevar a cabo mis metas, gracias por estar siempre conmigo durante todo este camino. A todas las personas especiales que me acompañaron en esta etapa, aportando a mi formación profesional y como persona.

AGRADECIMIENTO

Le agradezco a Dios por ser mi guía y acompañarme en el transcurso de mi vida, brindándome salud, sabiduría y perseverancia para culminar con éxito esta meta.

A mi madre Ludiz por ser una fuente de inspiración y haberme apoyado incondicionalmente.

Agradezco a todos los docentes que, con su conocimiento y apoyo, motivaron mi desarrollo personal y profesional.

RESUMEN

Esta investigación se basa en los Métodos de Fraude Cibernético en la Universidad de Panamá, debido a la creciente digitalización y la cantidad de información confidencial que gestionan, la demanda del uso de las tecnologías y el almacenamiento de los datos personales, y con ello, para esta investigación, se logró verificar que en la actualidad, no mantienen un sistema dedicado a la prevención y detección de fraude cibernético, por lo cual están expuestos y se convierten en blancos atractivos para los ciberdelincuentes. Mi objetivo principal es realizar un análisis sobre las acciones de seguridad informática que se deberán tomar para evitar el fraude cibernético en la institución, previniendo la fuga de información de datos almacenados y custodiados dentro de la misma.

Basados en la siguiente pregunta: ¿Es importante mantener seguro nuestro entorno en donde almacenamos información y que pueda ser vulnerable a posibles ataques?

Es por ello que apliqué una encuesta a 100 personas entre profesores, estudiantes y administrativos dentro del Campus Universitario, en donde como punto clave pregunté: ¿Conocen sobre Fraude Cibernético? y de allí, segmenté las diversas preguntas que me llevó a obtener los resultados que, desde un inicio, sospechaba ya que gran parte de la población universitaria solo accede al entorno tecnológico para validar información, pero lo que no saben es que también son los principales causantes de que obtengan su información y con ella, puedan vulnerar a la institución haciéndose pasar por uno de ellos e ingresando al sistema y obteniendo las base de datos.

Como recomendación puedo indicar que se deben tomar medidas de seguridad adecuadas como plan de concientización a la comunidad universitaria, implementación de una herramienta de prevención, aplicar políticas robustas, realizar revisiones periódicas de auditoría, entre otros.

ABSTRACT

This investigation is based on Cybernetic Fraud Methods at Panama University, due to crescent digitalization and the massive amount of confidential information it manages, the demand of technology use and secure storage of personal data, this investigation was able to verify that currently do not have a dedicated system to prevention and detection of Cybernetic Fraud, so they are currently exposed and become an easy target to cybercriminals. The main goal is to make an analysis about information securities actions that need to be addressed to avoid cybernetic fraud in the institution, preventing guarded and storage personal information leakage.

Based in the following question: It is important to keep our environment safe where the information is storage and may be vulnerabilities to possible attacks?

It is for this reason a survey methodology was implemented to 100 people between, professors, student, administrative personnel from Campus, where the key question was: Do you know about Cybernetic Fraud? And from there a segmentation of diverse questions that result on an answer that I already know, because the most part of university population only access technological environment to information validation, but what they do not know is they also are the main reason that their personal information is easily obtained and the institution can be vulnerable, Anyone can impersonate your identity and access the system, violating the database information.

As recommendation, I can note that security measures must be taken as a conscientization plan to the university community, implementation of prevention tool, apply robust policies and make periodic revisions audits, among others.

PALABRAS CLAVE

- **Seguridad Informática**
- **Prevención de Ataques**
- **Protección de la Base de Datos**
- **Acciones y Medidas de Seguridad Informática**

ÍNDICE

INTRODUCCIÓN

El presente trabajo aborda el tema del fraude cibernético en la Universidad de Panamá desde una perspectiva unificada, con los aspectos más relevantes sobre conceptos, entrevistas, origen del problema y recomendaciones hechas para así evitar este delito informático. El tema del fraude cibernético es un problema muy serio, que perjudica a sus víctimas y que está presente en toda la ciudad de Panamá. Es por esta razón, que los administradores del Departamento de Tecnología de la Universidad de Panamá deben avanzar y estar a la vanguardia ante los nuevos métodos de fraude que se dan actualmente, pues de otra forma la institución estaría muy expuesta a este tipo de amenaza invisible que causa grandes pérdidas económicas. El fraude cibernético va en aumento y la institución se debe preparar para frenar estos hechos delictivos. En términos generales, en los últimos años se ha observado un aumento desmedido en el uso de los sistemas de cómputo, páginas web y uso de medios electrónicos y en consecuencia, los índices van en aumento; por tal razón, el presente trabajo muestra la forma necesaria de adoptar un sistema que sea, lo suficientemente, moderno y eficiente para encontrar las vulnerabilidades que se van generando con el tiempo y así poder actuar de una forma fácil y rápida antes de que ocurra el incidente. Para entender mejor esta problemática tan ingeniosa, pero dañina para la institución se abordan, a continuación, conceptos muy importantes para el tema en investigación.

CAPÍTULO I: FUNDAMENTACIÓN

1.1 PLANTEAMIENTO DEL PROBLEMA

Esta investigación trata sobre el fraude cibernético, debido a la creciente demanda del uso de las tecnologías y el almacenamiento de los datos personales en la Universidad de Panamá, en la misma se logró verificar que, actualmente, la Universidad de Panamá no mantiene un sistema dedicado a la prevención y detección de fraude en tiempo real y con ello, están expuestos a que los ataques tomen diferentes formas y afecten de manera distinta los datos almacenados en la institución, pero que ciertamente son de gran magnitud.

Debido a la creciente dependencia de mantener los datos en línea para almacenar y acceder a la información importante, los ciberdelincuentes pueden explotar las vulnerabilidades de seguridad en los equipos de la institución conectados a internet para acceder y robar información confidencial, realizar actualización de datos fraudulenta y hasta dañar los sistemas informáticos de la institución.

¿Asegurarse de contar con las herramientas y que el sistema de manejo de fraude cibernético cumpla con las características necesarias será particularmente importante?

Ilustración 1: Prevención de Fraude Cibernético

1.2 JUSTIFICACIÓN

Los fraudes cibernéticos están evolucionando, constantemente, debido a que los criminales utilizan su ingenio para sortear y vulnerar las medidas de seguridad que se han implementado. Un ejemplo claro, sería el caso de la Universidad de Panamá que puede utilizar medidas de seguridad muy rigurosas para proteger los datos de todos los estudiantes, profesores y administrativos de la institución, pero el criminal puede conseguir el acceso para poder entrar y sortear la barrera de seguridad implementada; aquí, es donde entra en juego el tema de ingeniería social, cuyo objetivo es hacerse pasar por el estudiante, administrativo o profesor, y ante esta acción, el sistema informático de la Universidad no puede validar o certificar que la persona que está ingresando los datos de usuario y contraseña registrados sea verdaderamente la persona dueña de esa información, por tanto, se da cabida a casos de suplantación de identidad o robo de datos.

Actualmente nos encontramos en este punto, porque el fraude cibernético ha avanzado tanto que ya no está hecho para vulnerar sistemas débiles como la clonación de una tarjeta de banda magnética, sino que es un fraude desarrollado para engañar a las personas apropiándose de la información para poder acceder a su información personal y luego, utilizar suplantación de identidad. He aquí donde se debe hacer conciencia y advertir sobre los peligros de internet, las computadoras y demás dispositivos electrónicos que pueden acceder a los sistemas. No se debe confiar, fácilmente, en nadie que solicite información privada, principalmente usuarios, contraseñas y cédula, etc.

Entonces, es preciso resaltar que, para los casos de fraude cibernético, la Universidad de Panamá utiliza este tipo de sistemas, en donde su principal preocupación no debe ser la

seguridad del sistema propiamente, sino que los criminales no obtengan la información confidencial almacenada en su base de datos.

Los ciberdelincuentes utilizan diversas técnicas y herramientas para obtener acceso no autorizado a los sistemas informáticos y dispositivos conectados a Internet. Estas técnicas pueden incluir el phishing, el malware, el ransomware, suplantación de identidad y otras tácticas de ingeniería social, de las cuales se puede ser objetivo.

Ilustración 2: Ciberdelincuentes intentando acceder a los datos sensitivos

La institución podría ser blanco de ataques informáticos ya que los ciberdelincuentes pueden:

- Obtener acceso no autorizado al sistema o información confidencial para fines de espionaje o robo de datos.

Ilustración 3: Ingeniería Social es uno de los métodos más utilizados para poder ingresar al sistema y lograr obtener información confidencial

- Los ciberdelincuentes podrían distribuir malware o virus para interrumpir el funcionamiento normal del sistema informático o para robar información confidencial.

Ilustración 4: El malware interrumpe el funcionamiento normal del sistema informático y roba información confidencial

- Los ciberdelincuentes podrían realizar intentos de phishing o suplantación de identidad para obtener información de la institución.

Ilustración 5: Phishing es uno de los métodos utilizados para poder ingresar al sistema y lograr obtener información confidencial

- Los ciberdelincuentes podrían realizar ataques de denegación de servicio (DDoS) para interrumpir la operación del sitio web o servicio en línea de la Universidad de Panamá.

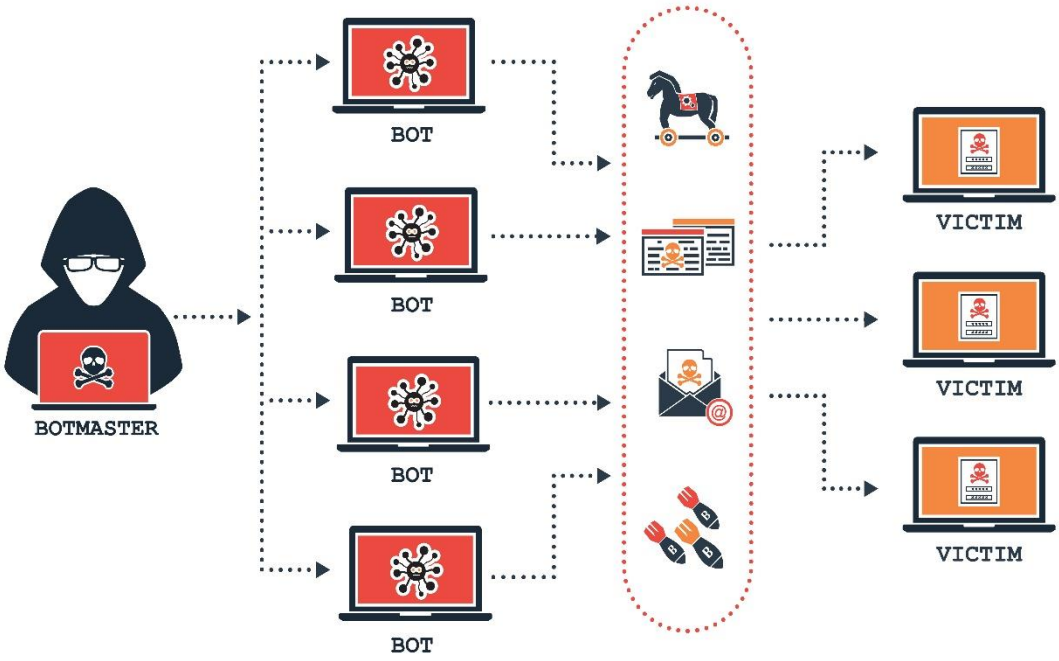

Ilustración 6: Un ataque DDoS (Distributed Denial of Service) es un tipo de ciberataque en el que se busca interrumpir el funcionamiento normal de un servidor, servicio o red, sobrecargándolo con una cantidad masiva de tráfico proveniente de múltiples fuentes

- Los ciberdelincuentes podrían explotar vulnerabilidades de software o hardware.

1.3 OBJETIVOS DE LA INVESTIGACIÓN

1.3.1 Objetivo Específico

- Identificar los tipos de fraudes cibernéticos más comunes que afectan a los estudiantes, docentes y personal administrativo de la Universidad de Panamá, tales como el phishing, el robo de identidad y el acceso no autorizado a sistemas universitarios.

- Evaluar la eficacia de las políticas de seguridad informática y los protocolos de prevención de fraude cibernético implementados en la Universidad de Panamá, con el fin de determinar áreas de mejora en la protección de la información sensible y en la respuesta ante incidentes de seguridad.

1.3.2 Objetivo Generales

- Analizar los principales métodos de fraude cibernético utilizados en la Universidad de Panamá, identificando las vulnerabilidades tecnológicas y organizacionales que permiten su ocurrencia y su impacto en la seguridad de la información académica y administrativa.
- Proponer medidas preventivas y correctivas para mitigar los riesgos asociados al fraude cibernético en la Universidad de Panamá, fomentando la educación sobre ciberseguridad entre estudiantes, personal docente y administrativo, y fortaleciendo las políticas de protección de datos.

1.4 DELIMITACIÓN

Esta investigación se enfoca solamente en el caso de fraude cibernético en la Universidad de Panamá, con un tiempo aproximado de 17 meses en donde se investigaron los diversos métodos de fraudes cibernéticos que se puedan dar dentro de la institución.

1.5 LIMITACIONES

En esta investigación la principal limitación fue la información reducida compartida por la institución ya que los datos almacenados, sobre su infraestructura, están limitados al uso únicamente de los empleados de la Universidad de Panamá.

CAPÍTULO II: MARCO REFERENCIAL

2.1 ANTECEDENTES

En la actualidad, la era digital ha permitido una gran cantidad de beneficios en cuanto a la comunicación y el intercambio de información en todo el mundo; sin embargo, este avance tecnológico también ha dado lugar a nuevas formas de delincuencia, conocidas como fraudes cibernéticos.

Estos delitos incluyen actividades como el phishing, el robo de identidad, el acoso cibernético y el fraude en línea, entre otros.

Un primer antecedente corresponde a un artículo titulado “Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad”, donde se aborda el avance de las ciberamenazas dentro de América Latina, y se establece que las principales amenazas son ataques dirigidos por malware para robar información sensible o confidencial, utilizando técnicas como “spear-phishing” o ”watering hole” y además el autor nos habla de cómo los troyanos dirigidos al fraude bancario aumentaron considerablemente, donde el 97% de las entidades financieras recibieron al menos un ataque y de estos, el 37% resultaron exitosos.

Por otra parte, hacen un análisis sobre la capacidad de comprensión de los entes reguladores sobre el tema, la debilidad de las regulaciones existentes y la necesidad de modificarlas, así como su grado de impacto en la esfera de la seguridad pública y nacional.

La investigación, previamente mencionada, demuestra cómo en América Latina, en general, existe un gran atraso en cuanto al establecimiento de los ciberdelitos a nivel legal, y aporta una visión del grado de importancia que tiene este dentro de un país; apoya nuestra investigación mostrando cuán necesario es conocer quiénes son las personas encargadas de manejar esta nueva forma de delinquir usando el ciberespacio como herramienta y medio, unido a eso, también muestran la importancia de comprender y analizar los procesos tomados por estos, para conocer la efectividad de sus acciones, mejorar y prever las situaciones que pueden poner en riesgo al público.

Por otro lado, el artículo "Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad", es una investigación centrada en las acciones delictivas en el ciberespacio, esta analiza los puntos de vista de diversos autores acerca de la aparición del ciberdelito en temas de terrorismo, generando así el llamado "ciberterrorismo", además intenta explicar el cómo las naciones han reaccionado ante estas situaciones, y realiza toda esta explicación haciendo un recorrido que va desde la conceptualización y análisis del concepto de "ciberespacio" y sus amenazas, hasta las consecuencias que este ha provocado en distintas naciones y organizaciones, para terminar mostrando la visión estratégica de defensa de los estados y las líneas de actuación que se utilizan en España y Europa para contrarrestar su efecto destructivo en la sociedad actual. La investigación citada explica el impacto que puede tener la ciberdelincuencia dentro de un país y cómo esta, es cada vez más común y cambiante; además, plantea uno de los modelos más comunes de prevención de incidentes de seguridad y hace especial énfasis en cómo los estados de gobierno deben mantenerse en constante revisión para lograr prevenir dichos incidentes y, por otro lado,

también tener la capacidad de tomar decisiones de seguridad conociendo el estado actual de su ciberespacio.

Por último, en el artículo “Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios”, sus autores abordan toda el área de los ciberdelitos, conceptualizando cada uno de estos, estableciendo sus riesgos y tipología para así pasar al tema de la impunidad en la administración de justicia sobre los delitos informáticos. Este trabajo de investigación está centrado en delitos que afectan a las empresas, ya sea en su reputación o ingresos y concluye en que cada día los delitos informáticos van aumentando tanto en tipo como en tamaño y es necesario instaurar un sistema de seguridad tal que permita resguardar la información sensible de las personas sin ningún tipo de riesgo de vulneración.

En este marco teórico, se evidencia la importancia de estudiar la incidencia de los ciberdelitos y la eficacia de las regulaciones implementadas en Panamá, para determinar si estas medidas están siendo efectivas en la prevención y control de los ciberdelitos dentro del país.

Es por esto que la investigación realizada nos habla sobre los métodos de fraude cibernético dentro de la Universidad de Panamá y la forma en la que la institución puede prevenir los mismos implementando controles adecuados, evitando incidentes de seguridad.

Los incidentes de seguridad se pueden definir como un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones y amenazar la seguridad de la información.

Es decir, son el conjunto de sucesos posibles que pueden comprometer la integridad de la información que se encuentra resguardada en algún tipo de base de datos y que afectaría tanto al usuario dueño de la información como a la institución encargada de protegerla.

Ciclo de vida de la gestión de incidentes: la mayoría de los estándares de referencia para la gestión de incidentes describen una serie de etapas a seguir para un manejo adecuado de los mismos, que se resume en una etapa de preparación (pre-incidente), una etapa de detección del incidente, otra etapa en la que se toman las decisiones correspondientes a la contención, erradicación y recuperación ante el incidente, y por último una etapa de actividad post-incidente.

A continuación, se describe un poco cada etapa mencionada:

Planificación y preparación: se centra en llevar a cabo todas las acciones necesarias para la preparación ante un incidente de seguridad, esta etapa engloba: plan de gestión de incidentes, procedimientos de actuación, política de seguridad de la información, establecimiento del equipo de respuesta a incidentes de seguridad, concienciación y formación sobre la gestión de incidentes, implantación y mantenimiento de los elementos de monitorización de eventos de seguridad, simulacros del plan de gestión de incidentes,

definición de la taxonomía de incidentes de seguridad, plan de intercambio de información y comunicación con terceros y formación permanente del equipo humano.

Detección y reporte: esta fase consta de: recopilación de información, tanto interna como externa a través de los mecanismos establecidos en la etapa anterior, identificar las actividades anómalas, registrar y notificar el incidente en caso de confirmarse.

Respuesta: se continúa con la investigación del incidente siendo necesario en ocasiones llevar a cabo una recopilación y análisis de evidencias para ampliar la información de la que se dispone, de forma que las decisiones que se tomen en esta etapa sean las más adecuadas, proporcionadas y ágiles. Esta fase pasa por las siguientes subetapas: contención del incidente, erradicación del incidente y recuperación tras el incidente.

Lecciones aprendidas: esta etapa ayuda a identificar tanto las carencias como los puntos fuertes de las etapas llevadas a cabo, así como pone de manifiesto posibles mejoras en protección y ciberdefensa de la organización; sus objetivos son: identificación de mejoras ante los planes, políticas, procedimientos, etc. Evaluación de la efectividad, agilidad y desempeño del equipo de respuesta ante incidentes, identificación de mejoras ante los sistemas de monitorización y obtención de información.

Cierre del incidente: Actividad post-incidente. El incidente de seguridad no se dará por finalizado hasta haber identificado las lecciones aprendidas y haya un plan para llevarlas a cabo.

Procedimiento de respuestas: Las organizaciones deben disponer de un procedimiento global de gestión de incidentes de seguridad de la información cuyo objetivo sea establecer las directrices generales para la gestión de incidentes de seguridad, con el fin de prevenir y mitigar el impacto de estos. Este procedimiento deberá cubrir al menos los siguientes elementos clave:

- Declaración de compromiso de la gestión.
- Propósito y objetivos del procedimiento. Alcance del procedimiento; a quién y a qué se aplica y bajo qué circunstancias.
- Definir qué se considera incidente de seguridad y sus consecuencias dentro del contexto de la organización.
- Criterios de clasificación para un incidente de seguridad.
- Criterios para evaluar la criticidad de un incidente de seguridad.
- Estructura organizativa y delimitación de roles, responsabilidades y niveles de autoridad.
- En este punto se debería incluir de forma clara la autoridad del equipo de respuesta ante incidentes (por ejemplo, para confiscar equipos, inspeccionar tráfico, descifrarlo o no, etc.)
- Contactos. Deberán estar siempre actualizados y probados (que los números de teléfono sean los correctos, los correos electrónicos adecuados, etc.).

Por consiguiente, se puede apreciar que la gestión general de los incidentes de seguridad es bastante estructurada, y que para intentar prever un ataque a nivel mayor y estar realmente preparados para ello, se tienen que realizar una serie de procedimientos y un trabajo en conjunto entre distintas entidades que permita la elaboración de un plan estratégico donde se establezcan todas las posibles medidas a tomar considerando los recursos disponibles.

Entes reguladores en Panamá

En Panamá, existen varios entes reguladores encargados de combatir los ciberdelitos y proteger la seguridad en línea. Uno de los principales es la Dirección de Investigación Judicial (DIJ), que forma parte de la Policía Nacional y se encarga de investigar y prevenir delitos informáticos, también está la Autoridad Nacional para la Innovación Gubernamental (AIG), que tiene como objetivo promover la innovación y el uso de tecnologías de la información y comunicación en el sector público, y a su vez, prevenir y combatir los ciberdelitos, otro de los entes creados para atender estos conflictos es el CSIRT Panamá, el cual se encarga de dar respuesta a incidentes de seguridad en Panamá y "entre sus objetivos están la prevención, tratamiento, identificación y resolución de ataques a incidentes de seguridad sobre los sistemas informáticos que conforman la infraestructura crítica del país y el acceso a la información de parte de los ciudadanos de Panamá".

Estos entes reguladores trabajan de manera coordinada y apoyándose en lo establecido dentro del código penal para garantizar un entorno seguro y confiable en línea para los ciudadanos panameños.

A continuación, se podrán observar a detalle las regulaciones antes mencionadas.

Código Penal: Delitos contra la Seguridad Informática. Dentro del código penal en el título VIII, capítulo I de la ley sobre delitos contra la seguridad informática, hace referencia a los artículos 285 donde se establece que "Quien indebidamente ingrese o utilice una base de datos, red o sistema informático será sancionado con dos a cuatro años de prisión". Art. 286 "Quien indebidamente se apodere, copie, utilice o modifique los datos en tránsito o contenidos en una base de datos o sistema informático, o interfiera, intercepte, obstaculice o impida su transmisión será sancionado con dos a cuatro años de prisión" y Art. 287 "Las conductas descritas en los artículos 285 y 286 se agravarán de un tercio a una sexta parte de la pena si se cometen contra datos contenidos en bases de datos o sistema informático de: Oficinas públicas o bajo su tutela, Instituciones públicas, privadas o mixtas que prestan un servicio público, Bancos, aseguradoras y demás instituciones financieras y bursátiles".

División de Ciberdelito de la Dirección de Investigación Judicial (DIJ). Es una unidad especializada encargada de investigar los delitos informáticos y de alta tecnología. Esta división es responsable de llevar a cabo investigaciones sobre delitos cometidos a través de redes informáticas, como el robo de datos, el acceso no autorizado a sistemas informáticos, el phishing, la suplantación de identidad, el grooming, entre otros.

El aumento en el uso de la tecnología y la interconexión global ha creado nuevas formas de delitos que requieren de una respuesta especializada. La División de Ciberdelitos

de la DIJ fue creada en 2010, en respuesta a la creciente necesidad de combatir este tipo de delitos, desde entonces, la unidad se ha especializado en la investigación y persecución de los delitos informáticos y ha desarrollado técnicas y metodologías específicas para este propósito.

ANTAI: Ley 81 de Protección de Datos Personales. El 29 de marzo de 2021 entró en vigor la Ley de Protección de datos personales en la República de Panamá. Esta Ley tiene por objeto establecer los principios, derechos, obligaciones y procedimientos que regulan la protección de datos personales, considerando su interrelación con la vida privada y demás derechos y libertades fundamentales de los ciudadanos, por parte de las personas naturales o jurídicas, de derecho público o privado, lucrativas o no, que traten datos personales en los términos previstos en esta ley.

Esta ley posee 46 artículos en donde se aborda el nuevo manejo de la información; entre ellos, se pueden mencionar:

- Los principios rectores del tratamiento de datos personales, como transparencia, legalidad, finalidad, calidad, proporcionalidad y responsabilidad.
- Los derechos de los titulares de los datos personales, como el derecho de acceso, rectificación, cancelación y oposición, así como el derecho a ser informados sobre el tratamiento de sus datos.
- Las excepciones al consentimiento para el tratamiento de datos personales.
- Las obligaciones de los responsables del tratamiento de datos personales, incluyendo la implementación de medidas de seguridad adecuadas para proteger los datos personales y la

obligación de informar a los titulares de los datos sobre el tratamiento de sus datos y sus derechos.

- Las transferencias internacionales de datos personales y su protección.
- La creación de la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI) y sus competencias en la protección de datos personales.
- Las sanciones por el incumplimiento de la Ley 81, incluyendo multas, cierre temporal o definitivo de la empresa y otras medidas que considere pertinentes la autoridad competente.

La proclamación de esta ley se puede considerar un pequeño avance dentro de todo el camino que queda por recorrer en Panamá para lograr ser un país seguro y bien estructurado dentro del área de la seguridad informática, la creación de una ley especial que proteja, establezca protocolos y sancione conductas inapropiadas o directamente delictivas relacionadas con la vulneración de datos personales es de gran aporte a la legislación panameña, ya que, el robo de datos o de información sensible para atacar o extorsionar a la personas y empresas es uno de los ciberdelitos más comunes en el mundo y existe una gran necesidad de crear medidas que permitan contrarrestar de alguna forma toda esta ola creciente de ataques para así poder brindarle seguridad a los usuarios o algún tipo de respaldo.

El Código Penal de la República de Panamá, aprobado mediante Ley 14 del 18 de mayo de 2007, en su Título VIII, sobre los delitos contra la "Seguridad Jurídica de los Medios Electrónicos" regula los delitos contra la seguridad informática.

Del artículo 289 al 292 regula las siguientes conductas delictivas y sus respectivas penas:

a) Ingresar o utilizar de bases de datos, red o sistemas informáticos.

b) Apoderar, copiar, utilizar o modificar datos en tránsito o contenidos en bases de datos o sistemas informáticos, o interferir, interceptar, obstaculizar o impedir la transmisión.

Además, determina ciertas conductas como circunstancias agravantes que aumentan la pena de prisión.

Un antecedente significativo de fraude cibernético en Panamá ocurrió en 2020, cuando varias instituciones bancarias del país fueron víctimas de un ciberataque masivo. En este caso, los ciberdelincuentes utilizaron técnicas de phishing y suplantación de identidad para obtener credenciales de acceso a cuentas bancarias y realizar transacciones fraudulentas. Se estima que los atacantes lograron desviar fondos de numerosas cuentas antes de que los bancos detectaran la actividad sospechosa.

Este ataque puso en evidencia la vulnerabilidad de los sistemas financieros en el país y la necesidad urgente de mejorar las medidas de ciberseguridad, como la implementación de autenticación multifactorial y mejores sistemas de monitoreo en tiempo real. También resaltó la importancia de educar a los usuarios sobre los peligros de los correos electrónicos maliciosos y otras formas de ingeniería social utilizadas para engañar a las víctimas.

El caso impulsó a las autoridades panameñas a intensificar sus esfuerzos para combatir el fraude cibernético, con la creación de equipos especializados y la colaboración con organismos internacionales para fortalecer las capacidades de defensa ante estos ataques.

Otro antecedente importante de fraude cibernético en Panamá ocurrió en 2018, cuando el Banco Nacional de Panamá fue blanco de un ataque cibernético que resultó en un robo millonario. Los atacantes lograron vulnerar los sistemas del banco mediante técnicas de phishing y acceso no autorizado, desviando fondos hacia cuentas fraudulentas. Aunque el monto exacto no fue revelado en ese momento, se informó que se trataba de una suma significativa.

Este incidente llevó a la Superintendencia de Bancos de Panamá a reforzar las medidas de ciberseguridad en el sistema financiero del país, exigiendo la implementación de mejores protocolos de autenticación y monitoreo de transacciones. Además, el ataque subrayó la necesidad de aumentar la concienciación sobre las tácticas de ingeniería social que los ciberdelincuentes utilizan para comprometer cuentas y sistemas Este caso impulsó a varias instituciones en Panamá a revisar y fortalecer sus infraestructuras tecnológicas y su capacidad de respuesta ante incidentes cibernéticos, reconociendo la creciente amenaza de los fraudes cibernéticos en la región.

Ya comprendido los antecedentes mencionados y las regulaciones que se mantienen dentro del país, en esta investigación nos basamos únicamente en los métodos de fraude cibernético dentro de la Universidad de Panamá.

2.2 CONCEPTUALIZACIÓN

Se realizó la investigación de patrones que se observan dentro de la institución, como el uso de herramientas por parte de los delincuentes para obtener información necesaria de su objetivo, así como las consecuencias económicas y reputacionales que conlleve.

Este trabajo se enfocó en prevenir y combatir el fraude cibernético mediante una propuesta con soluciones, tales como medidas de seguridad informática aplicando herramientas en tiempo real, campañas de concientización y creando un equipo de trabajo para controlar y detectar de manera efectiva el ataque.

2.3 TEORÍAS

La tecnología ha avanzado tanto que se encuentra relacionada intrínsecamente con el diario vivir de las personas y de la institución, por lo tanto, esto es de suma importancia debido a que el progreso, el desarrollo y la productividad dependen de la tecnología.

A medida que los avances en tecnología informática se desarrollan y la influencia que estos tienen en los ámbitos de la vida social, también se desarrollan acciones ilícitas que se

conocen como fraudes cibernéticos y que se han vuelto cada vez más frecuentes y sofisticados.

Las víctimas están siendo engañadas a través de la "ingeniería social", que es el proceso de manipulación de personas a través de técnicas psicológicas y habilidades sociales para lograr objetivos específicos. Estos incluyen, pero no se limitan a: recopilar información, acceder a sistemas o realizar actividades más sofisticadas, que pueden o no ser en beneficio de la persona objetivo.

La manipulación psicológica a la víctima mediante engaño tiene como objetivo principalmente que la persona comparta información privada (usuario, contraseña, credenciales, etc.) o que ejecute acciones para vulnerar los sistemas (instalar o ejecutar algún programa, deshabilitar funciones de seguridad). En estos casos, se destaca que la víctima de este tipo de engaños por parte de los delincuentes no está consciente de lo que está haciendo, pues tienen plena confianza de una tercera persona, que supuestamente los está ayudando a resolver un falso problema de seguridad en la cuenta y por ende la víctima comparte información confidencial pensando que se está comunicando con un representante de la institución. Este tipo de engaño sucede de manera rápida, la víctima al brindar plena confianza no toma las medidas de seguridad necesarias, pensando que le están ayudando a proteger sus datos.

Para prevenir el fraude cibernético es importante crear un entorno digital seguro y confiable en el que la institución pueda almacenar información de manera segura sin tener que preocuparse por los ciberataques. Esto se logra estableciendo normas y estándares

comunes para la seguridad cibernética y mediante la investigación y el desarrollo continuo de nuevas tecnologías y soluciones de seguridad para hacer frente a las amenazas emergentes a las que se enfrenta la institución.

Existen teorías importantes a considerar para controlar el fraude cibernético. Algunas de ellas incluyen:

- Integridad: Esto implica asegurarse de que los datos y sistemas estén protegidos contra manipulaciones o alteraciones no autorizadas.
- Confidencialidad: Esto se refiere a la protección de los datos y sistemas contra el acceso no autorizado.
- Disponibilidad: Esto implica asegurarse de que los sistemas y servicios estén disponibles y operativos cuando se necesiten.
- Autenticación: Esto conlleva la verificación de la identidad de los usuarios y dispositivos para evitar accesos no autorizados.
- Autorización: Esto se refiere a la asignación de permisos y niveles de acceso a usuarios y dispositivos autorizados.
- Monitoreo y registro: Esto implica el monitoreo constante de los sistemas y la recopilación de registros para identificar y prevenir el fraude.
- Respuesta rápida: Esto propone tener planes y procesos en su lugar para responder rápidamente a incidentes de seguridad y minimizar el daño.

El ciberespacio es un lugar en donde suceden miles de cosas: intercambio de información, transacciones, pagos, acuerdos, conferencias, trabajo colaborativo, alimentación de bases de datos, almacenamiento de imágenes, resguardo de videos… pero también fraudes, delitos, robo de identidades, etcétera. Y, aunque muchas empresas invierten cantidades considerables en ciberseguridad para salvaguardar tanto la información, como su infraestructura tecnológica, muchas veces son errores humanos los que le abren la puerta a la ciberdelincuencia.

Por ello, es importante implementar un plan de concientización en seguridad de la información o concientización en ciberseguridad (*awareness* es como se le conoce en inglés), para dar a los colaboradores de la empresa las herramientas necesarias para reconocer cuándo están siendo el blanco de un ataque cibernético.

Ante el incremento de fraude cibernético, se deben reforzar la información a los administrativos, estudiantes y profesores sobre una serie de medidas de seguridad como:

- No dar clic en vínculos sospechosos
- No compartir datos personales por correo electrónico
- Actualizar constantemente el antivirus en los dispositivos

Lo más preocupante es que, así como las personas deberían considerar una serie de nuevos hábitos y precauciones en temas de su economía personal, deberían hacerlo con la protección de los datos y activos críticos de las manos de los ciberdelincuentes, ya que esto

requiere un enfoque multifacético. Se podría incluir la implementación de medidas sólidas de ciberseguridad, así como el monitoreo en tiempo real de los sistemas y redes en busca de signos de actividad sospechosa a través de la web oscura o el monitoreo de exposición cibernética.

El **fraude cibernético** es una actividad delictiva en la que se utilizan medios tecnológicos o informáticos para engañar o defraudar a personas, empresas o instituciones. A menudo, los delincuentes cibernéticos buscan obtener información personal o financiera, contraseñas, o datos personales, con el fin de llevar a cabo actividades fraudulentas. Este tipo de fraude puede ocurrir a través de una variedad de métodos, como el phishing, malware, ransomware, ataques de ingeniería social, y más.

¿Qué es la detección de fraude?

La detección de fraude es un conjunto de procesos y técnicas diseñadas para identificar, rastrear y prevenir el fraude. En el mundo de los negocios, el fraude, las estafas y los agentes maliciosos están haciendo daño de diversas maneras. Las compañías tienen que adoptar medidas para asegurarse de detectar y detener el fraude antes de que afecte a la empresa. Detectar el fraude es el primer paso para identificar dónde radica el riesgo. Después, puedes prevenirlo automática o manualmente.

¿Por qué es importante detectar el fraude?

Simplemente no hay forma de evitarlo: se va a necesitar software en tiempo real para la prevención y detección de fraude**.** Los ataques toman diferentes formas y afectan a los negocios de manera distinta, pero ciertamente son de gran magnitud.

El monitoreo de la web oscura implica escanearla, continuamente, en busca de información confidencial como credenciales de inicio de sesión, números de tarjetas de crédito y otros datos confidenciales, que pueden haberse obtenido a través de una violación de datos u otros medios. El objetivo del monitoreo de la web oscura es detectar la presencia de información confidencial en esta, y alertar a la institución antes de que los ciberdelincuentes puedan utilizarla.

El monitoreo de la exposición cibernética, por otro lado, implica monitorear todo Internet, incluidas las redes públicas y privadas, en busca de vulnerabilidades y posibles vectores de ataque. El objetivo del monitoreo de la exposición cibernética es identificar y evaluar los riesgos que plantean estas vulnerabilidades y tomar las medidas adecuadas para mitigarlos.

El fraude cibernético en la Universidad de Panamá es parte de un problema principal que afecta a mayor magnitud debido a que dentro de la institución se almacenan datos personales de estudiantes, profesores y administrativos. En Panamá se ha experimentado un aumento significativo en los delitos informáticos, que incluyen fraudes, ataques de phishing, y el acceso no autorizado a sistemas. Según datos recientes, los ciberataques en Panamá han aumentado en un 113% en el último año, afectando tanto a individuos como a instituciones,

incluyendo universidades que manejan datos personales de estudiantes, profesores y personal administrativo.

En particular, los ataques de ingeniería social y el uso de técnicas como el ransomware y la suplantación de identidad son comunes. Las instituciones educativas, debido a la creciente digitalización y la cantidad de información confidencial que gestionan, se convierten en blancos atractivos para los ciberdelincuentes.

La falta de formación adecuada en ciberseguridad y la ausencia de medidas robustas de prevención agravan la situación.

Es crucial que la Universidad de Panamá implemente programas de ciberseguridad robustos que incluyan la protección de datos, monitoreo constante de redes, capacitación en buenas prácticas digitales, y estrategias de respuestas rápidas para minimizar el impacto de posibles ciberataques.

La informática está hoy presente en casi todos los campos de la vida moderna. Con mayor o menor rapidez todas las ramas del saber humano se rinden ante los progresos tecnológicos, y comienzan a utilizar los sistemas de información, para ejecutar tareas que en otros tiempos realizaban manualmente.

Vivimos en un mundo que cambia rápidamente. Antes, podíamos tener la certeza de que nadie podía acceder a información sobre nuestras vidas privadas. La información era solo una forma de llevar registros. Ese tiempo ha pasado, y con él, lo que podemos llamar intimidad. La información sobre nuestra vida personal se está volviendo un bien muy

cotizado por las compañías del mercado actual. La explosión de las industrias computacionales y de comunicaciones ha permitido la creación de un sistema, que puede guardar grandes cantidades de información de una persona y transmitirla en muy poco tiempo. Cada vez más y más personas tienen acceso a esta información, sin que las legislaciones sean capaces de regularlos.

Los progresos mundiales de las computadoras, el creciente aumento de la capacidad de almacenamiento y procesamiento, la miniaturización de los chips de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, así como la investigación en el campo de la inteligencia artificial, ejemplifican el desarrollo actual definido a menudo como la "era de la información", a lo que con más propiedad, podríamos decir que más bien estamos frente a la "ERA DE LA INFORMÁTICA".

Por tanto, abordar el estudio de las implicaciones de la informática en el fenómeno delictivo resulta una cuestión apasionante para quien observa el impacto de las nuevas tecnologías en el ámbito social.

La investigación de delitos cibernéticos es importante porque actividades como la piratería, el fraude y el robo de identidad pueden tener consecuencias muy peligrosas para las personas, las empresas y la seguridad nacional. Una investigación eficaz ayuda a reconocer y evitar a los ciberdelincuentes para proteger la propiedad digital y mantener la seguridad en línea.

Los investigadores de delitos informáticos deben seguir aprendiendo nuevas habilidades y herramientas para rastrear y prevenir eficazmente los delitos en línea, ya que la tecnología cambia constantemente y surgen nuevas amenazas.

La investigación de delitos informáticos consiste en encontrar y detener actividades maliciosas que ocurren en computadoras y dispositivos digitales. Implica el uso de herramientas y métodos especiales para examinar delitos como piratería informática, phishing, malware, violaciones de datos y robo de identidad. Las personas que realizan este trabajo se denominan investigadores de delitos informáticos. Buscan cuidadosamente pruebas que las fuerzas del orden puedan utilizar para atrapar a las personas que cometen estos delitos.

Para las personas y las empresas, investigar los delitos informáticos es muy importante para protegerlas de las amenazas cada vez mayores que suponen estos delitos. También garantiza la justicia para las víctimas. Investigar estos delitos es muy importante porque siguen evolucionando y pueden tener consecuencias peligrosas para cualquier persona, incluidos los gobiernos y las empresas.

En un mundo cada vez más digitalizado, la inversión en ciberseguridad se ha convertido en una prioridad para empresas de todos los tamaños e industrias. Sin embargo, a pesar de los avances tecnológicos y las herramientas sofisticadas que se implementan, los incidentes de ciberseguridad siguen siendo frecuentes y se estima que en más de un 90% de los ciberataques interviene el factor humano.

Es común escuchar que los usuarios son el punto más débil en la ciberseguridad. En lugar de ver a los usuarios como un riesgo, debemos empoderarlos y educarlos para que se conviertan en la primera línea de defensa contra las ciberamenazas.

Los ciberatacantes utilizan técnicas de ingeniería social, como mensajes de texto fraudulentos, códigos QR engañosos, mensajes de WhatsApp, llamadas engañosas que logran manipular a las personas. Estas técnicas continúan evolucionando y logran poner en jaque cualquier estrategia para la ciberdefensa que no haya considerado al usuario como parte fundamental de este proceso, sin importar cuánto se invirtió en los controles y servicios tecnológicos, subrayando la importancia de la concientización y la formación continua de los usuarios como la última y mejor línea de defensa.

Tradicionalmente, la concientización en ciberseguridad consistía en charlas aburridas y poco efectivas, donde los asistentes apenas prestaban atención. Este enfoque ha demostrado ser ineficaz, especialmente para aquellos sin conocimientos técnicos. La clave está en transformar estas sesiones en experiencias interactivas y relevantes para todos.

En este informe nos basamos en una investigación que se realizó en la Universidad de Panamá, en donde mediante una encuesta aplicada a 100 personas dentro del Campus entre profesores, estudiantes y administrativos logramos obtener resultados valiosos que implican tomar una serie de acciones para prevenir el Fraude Cibernético en la institución.

Esta investigación cuenta con recomendaciones que deberán ser aplicadas en la Dirección de Tecnología de Información y Comunicación, en donde trabajan alrededor de 53

administrativos que llevan la grandiosa tarea sobre los procesos de tecnológicos de la institución.

Sobre la historia de la Dirección de Tecnología y Comunicación se puede destacar que en 1965 la Universidad de Panamá fundó el Centro de Cómputo con el propósito de que los procesos de investigación fueran fortalecidos con modernas tecnologías; más tarde, el Centro de Cómputo automatizó la matrícula universitaria centralizando la misma, en un proceso computacional; además, cambió su infraestructura basada en equipos de computadoras y periféricos por arquitecturas abiertas.

Ilustración 7: Dirección de Tecnología de la Información y Comunicación (DITIC)

En 1995, se crea la Red Nacional de Información Universitaria integrando a las Facultades, Centros Regionales, Extensiones Docentes y Unidades Administrativas, además de la integración a Internet y la implementación de nuevos sistemas tendientes a acelerar los procesos informáticos tanto académico como administrativos.

Luego, el 17 de abril de 1996, mediante reunión extraordinaria No.8-96 del Consejo Administrativo, se aprueba la reestructuración del Centro de Cómputo Electrónico y surge la Dirección de Informática, con modificaciones en la estructura organizacional y no así en la estructura de puestos y las funciones asociadas.

La Dirección de Informática era una Unidad Administrativa, compuesta por los departamentos de Desarrollo de Sistemas, Producción y Soporte Técnico; dedicada a brindar servicios y productos informáticos a la comunidad universitaria.

A partir de este redireccionamiento de actividades, con el pasar del tiempo y la evolución de la tecnología surge una nueva y renovada razón de ser orientada al servicio, por lo que se hace necesario un cambio en esta Unidad Administrativa que incluya no solo aspectos relacionados con su estructura organizacional, sino también una definición precisa de funciones tendientes a fortalecer los servicios informáticos mediante la puesta en operación de nuevos sistemas, el mejoramiento y optimización de los existentes, la incursión en la utilización de nuevas tecnologías comprometidas con la calidad, la implementación de las mejores prácticas de las organizaciones en materia de calidad y seguridad de la información y sobre todo alineados con los objetivos de la Universidad de Panamá que buscan ubicarnos como una Institución educativa moderna y al día con los cambios que la tecnología propone.

Es así como el Consejo Administrativo en reunión No. 16-16 celebrada el 7 de septiembre de 2016, aprobó la reestructuración de la Dirección de Informática convirtiéndola

en la Dirección de Tecnología de la Información y Comunicación (DITIC) con una estructura organizacional acorde a la nueva realidad.

La nueva estructura organizacional se compone de cinco departamentos, cuatro secciones, una coordinación y una unidad a saber:

- Departamento de Administración de Proyectos.
- Departamento de Diseño y Desarrollo de Sistemas con dos secciones: Sistemas de gestión y Sistemas académicos.
- Departamento de Administración de la Infraestructura de Comunicaciones.
- Departamento de Soporte, Microinformática y Mesa de Servicio con dos secciones: soporte técnico y mesa de servicio.
- Departamento de Administración de Sistemas Corporativos y Centro de Proceso de Datos.
- Además, se crea la Unidad de Seguridad Informática y la Coordinación Administrativa.

La Dirección de Tecnología de la Información y Comunicación (DITIC) es una Unidad adscrita a la Rectoría, en donde laboran profesionales calificados para brindar servicios y productos informáticos a la comunidad universitaria. En esta Dirección, reposa uno de los activos más valiosos de la Institución, “La Información”; así como convergen todas las líneas que brindan el servicio de comunicación de Datos y Voz.

Las principales funciones de la institución son:

- Desarrollar sistemas automatizados para el manejo de la información, en el área Académica, de Investigación, Extensión y Administrativa, de acuerdo con solicitudes presentadas por los usuarios.
- Brindar mantenimiento a los sistemas creados de tal manera que se garantice su utilización eficiente, por parte de los usuarios.
- Diseñar, instalar, mantener y administrar las redes de comunicación de datos de la institución.
- Implementar métodos y procedimientos, que garanticen la seguridad e integridad de la información existente en los medios en que se almacene.
- Asesorar a todas las dependencias universitarias en los requerimientos y selección de recursos computacionales.
- Brindar apoyo técnico a la docencia, investigación, extensión, difusión y servicios.
- Promover el desarrollo y difusión de la tecnología informática, a todos los niveles universitarios.
- Coordinar y asesorar a los usuarios en la explotación eficiente de la información que generan los recursos informáticos en producción.

Uso de la Tecnología como Apoyo Administrativo, con ello se simplifican los procesos y se logra realizar las gestiones de manera más eficiente con el uso de la tecnología. Entre estas podemos mencionar:

Ilustración 8: Correspondencia en Línea

Con esta plataforma se agiliza el proceso y controla las actividades relacionadas al manejo de la correspondencia, acortando los tiempos y minimizando el uso de papel.

Auditoría Interna

Con este sistema se lleva el registro, control y seguimiento de todas las auditorías que realice la Dirección General de Auditoría Interna a nivel nacional, preservando los bienes, actos y transparencia de la Institución.

Ilustración 9: Agenda Única

Herramienta Digital que permite a toda la comunidad universitaria conocer los eventos culturales, académicos y deportivos de la Institución.

Proyecto desarrollado en conjunto con la Dirección General de Planificación Universitaria.

Ampliación de Ancho de Banda

Ampliación del Ancho de Banda de Internet de 150Mbps a 1000Mbps en el Campus, ampliación del Ancho de Banda de Internet en los Centros Regionales Universitarios de 20Mbps a 100Mbps y ampliación, del Enlace MPLS de Datos de 50Mbps a 220Mbps

Ilustración 10: Renovación Tecnológica

Con este proyecto se reemplazaron 852 equipos de computadoras de los laboratorios de las diferentes Facultades, Centros Regionales Universitarios y Extensiones de la Universidad de Panamá

Diseño de Procesos

Se priorizaron los procesos de mayor impacto para simplificar los trámites académicos, como, por ejemplo:

- Solicitud de confección de diplomas
- Solicitud de emisión de créditos
- Registro de convalidaciones

- Retiro e inclusión de asignaturas
- Solicitud de ingreso de profesores de banco de datos
- Solicitud de evaluación de títulos

Plataforma Intranet

Este proyecto consistió en el diseño y desarrollo de una plataforma sobre la red informática interna que facilite el acceso tanto a información como servicios para uso de los funcionarios (Administrativos y Profesores) de la Universidad de Panamá, basada en los estándares de Internet.

Ilustración 11: INTRANET

Se están trabajando en otros proyectos tales como:

- Certificación en línea de Entrega de Calificaciones
- Renovación de la Plataforma de Virtualización de Software
- Renovación de Hosting - Sistema de Contingencia IDC Externo
- Plataforma de Antivirus
- Plataforma Office 365
- Adquisición de Licencia Web para las aplicaciones de Oracle
- Capacitación de Bonita Software
- Capacitación de personal de Infraestructura en Base de Datos
- Renovación de Seguridad Perimetral.

Actualmente, la Dirección cuenta con una herramienta de monitoreo de Redes y Base de Datos.

La herramienta permite visualizar en tiempo real la actividad de los dispositivos conectados a la red, así como los enlaces y el consumo de ancho de banda a nivel nacional de forma gráfica, además nos permitirá levantar estadísticas para optimizar el rendimiento de esta, verifica la sección de monitoreo y consumo de los recursos de la Base de Datos.

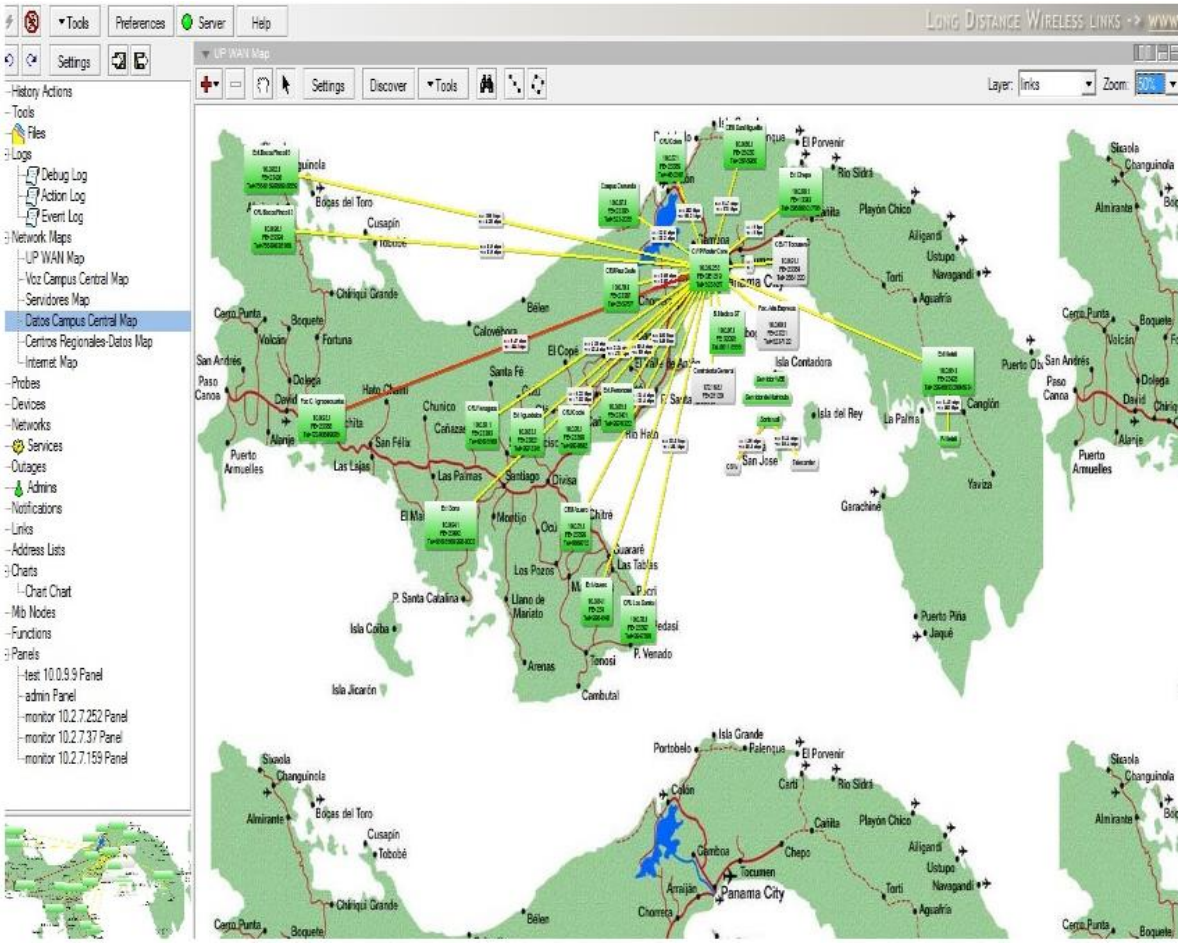

Ilustración 12: Herramienta de Monitoreo Actual

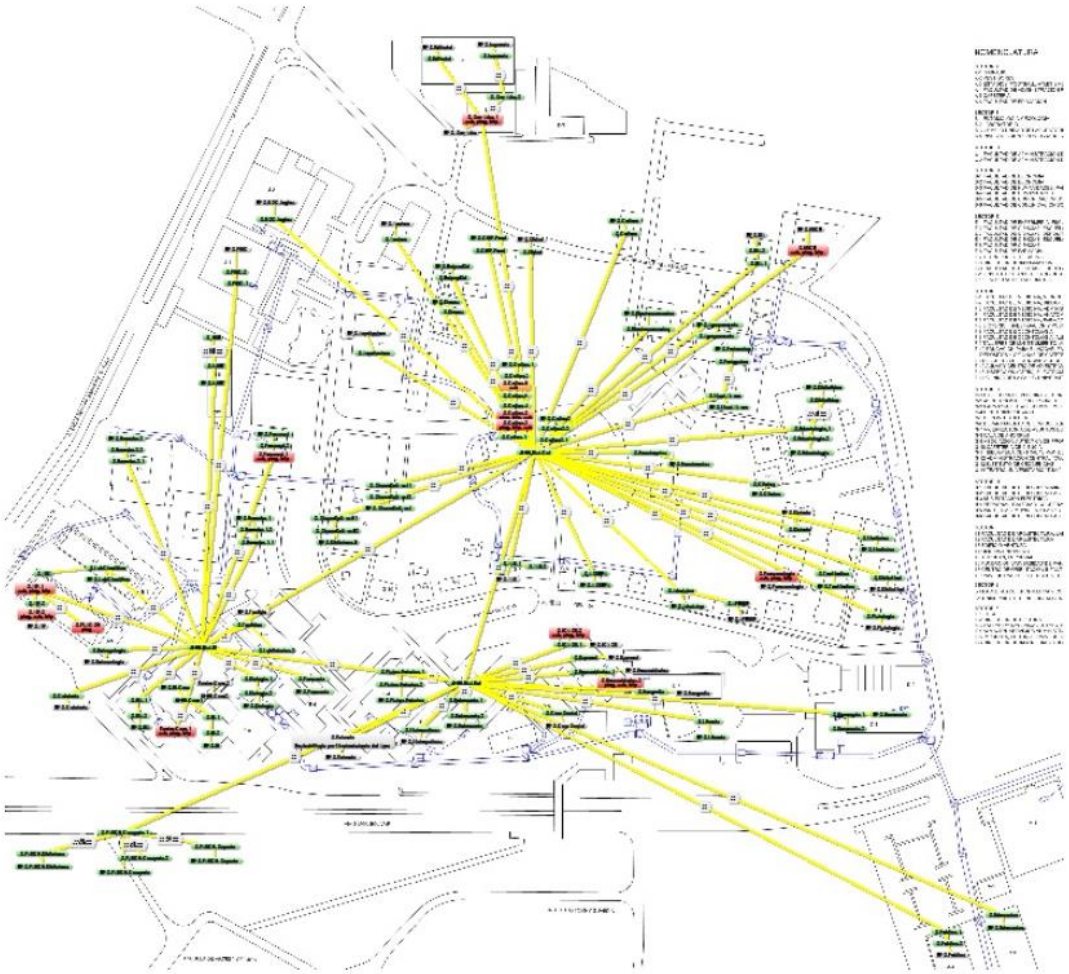

Ilustración 13: Diagrama de Interconexión

CAPITÚLO III: METODOLOGÍA

3.1 Hipótesis

La implementación de una visión general para la prevención del fraude cibernético en la Universidad de Panamá puede reducir significativamente los riesgos asociados, ya que la protección robusta de la información, junto con sistemas de detección temprana y medidas preventivas como contraseñas fuertes y autenticación de dos factores, disminuirá los incidentes de violación de datos y accesos no autorizados.

Además, un plan de respuesta rápida minimizaría el impacto de los ataques, mientras que la educación continua sobre riesgos cibernéticos aumentará la concienciación entre estudiantes, administrativos y profesores, reduciendo errores humanos.

Adicionalmente, la implementación de evaluaciones periódicas permitirá identificar brechas de seguridad y mejorar las medidas existentes, creando un entorno más seguro para toda la institución.

3.2 Variables

Las variables de estudio no han sido modificadas o alteradas, ya que, dentro de la investigación las variables estudiadas han sido observadas y analizadas, pero no se ha interferido de ninguna forma con las mismas, se busca establecer, un estadístico que permita conocer la incidencia del fraude cibernético en la Universidad de Panamá para desde ahí analizar la efectividad de las nuevas metodologías de prevención a utilizar en la institución.

3.2.1 Variables Independientes

Las variables independientes son aquellas que se implementan para reducir el riesgo de fraude cibernético. Estas son las acciones y estrategias de la visión global de ciberseguridad que afectan a las variables dependientes (resultados).

Protección de la información: las medidas tecnológicas de seguridad ya implementadas (cifrado, acceso restringido, protección de datos sensibles).

Detección temprana: los sistemas de monitoreo y alertas en tiempo real (software de detección de intrusiones, análisis de comportamientos anómalos).

Prevención proactiva: las políticas de contraseñas fuertes, autenticación multifactorial, y herramientas de prevención de fraude.

Respuesta rápida: la existencia de un plan de acción para incidentes de ciberseguridad, incluyendo equipos dedicados a la respuesta rápida.

Educación y concienciación: los programas de capacitación que se mantienen para estudiantes, profesores y personal administrativo en prácticas de prevención de fraude cibernético.

Evaluación y mejora continua: las auditorías regulares y actualizaciones de sistemas y políticas de seguridad que, actualmente, existen.

3.2.2 Variables Dependientes

Estas variables dependen de la implementación de las medidas descritas en la hipótesis.

Las variables que se podrán implementar serían:

Reducción en el número de incidentes de fraude cibernético: Cantidad de fraudes cibernéticos reportados antes y después de la implementación del enfoque de ciberseguridad.

Nivel de protección de datos personales: Grado de seguridad en la protección de datos personales de estudiantes, profesores y personal administrativo.

Tiempo de detección de amenazas: Rapidez con la que se detectan actividades sospechosas o ataques cibernéticos.

Eficiencia en la respuesta a incidentes: Tiempo y efectividad de la respuesta ante un ataque o intento de fraude cibernético.

Nivel de conciencia y conocimiento sobre ciberseguridad: Nivel de formación y concienciación en ciberseguridad entre los estudiantes, profesores y el personal administrativo.

Evaluación y mejora continua: frecuencia y efectividad de las evaluaciones de seguridad para identificar y corregir vulnerabilidades.

Estas variables dependientes pueden ser medidas mediante auditorías de seguridad, encuestas de percepción, registros de incidentes y análisis de tiempos de respuesta, entre otros indicadores que evalúan el impacto de la visión global de ciberseguridad.

3.3 Diseño de la Investigación

El diseño que se abordó es de tipo no experimental transversal, puesto que es aquel en el que el investigador no manipula directamente las variables independientes, sino que observa y mide los fenómenos tal como se presentan en su ambiente natural. Al mismo tiempo se considera descriptiva y de campo ya que es el proceso que se usa en el método científico, y sirve para la extracción de información y datos de la realidad, usando técnicas de recolección, como las encuestas.

3.4 Instrumentación

Como parte del proceso de investigación se logró realizar una encuesta a un grupo de estudiantes, administrativos y profesores de la institución. Imagen de encuesta, ver anexo.

CAPÍTULO IV: RESULTADOS

4.1 DESCRIPCIÓN DE LOS RESULTADOS

Con base en los resultados obtenidos podemos determinar que gran parte de los administrativos, profesores y estudiantes están en riesgo de ser víctimas de fraude cibernético debido a las falencias que se mantienen en el sistema y el poco conocimiento sobre el tema.

La gran mayoría de los entrevistados no conocía muy a fondo los términos que son utilizados en ciberseguridad. Las encuestas indican que debemos hacer un esfuerzo significativo en educación y concienciación a todos los usuarios de la institución, ya que es importante educarlos sobre los riesgos del fraude cibernético y cómo pueden protegerse. Así como implementar el uso de herramientas de seguridad factibles para evitar ser foco de este tipo de ataques.

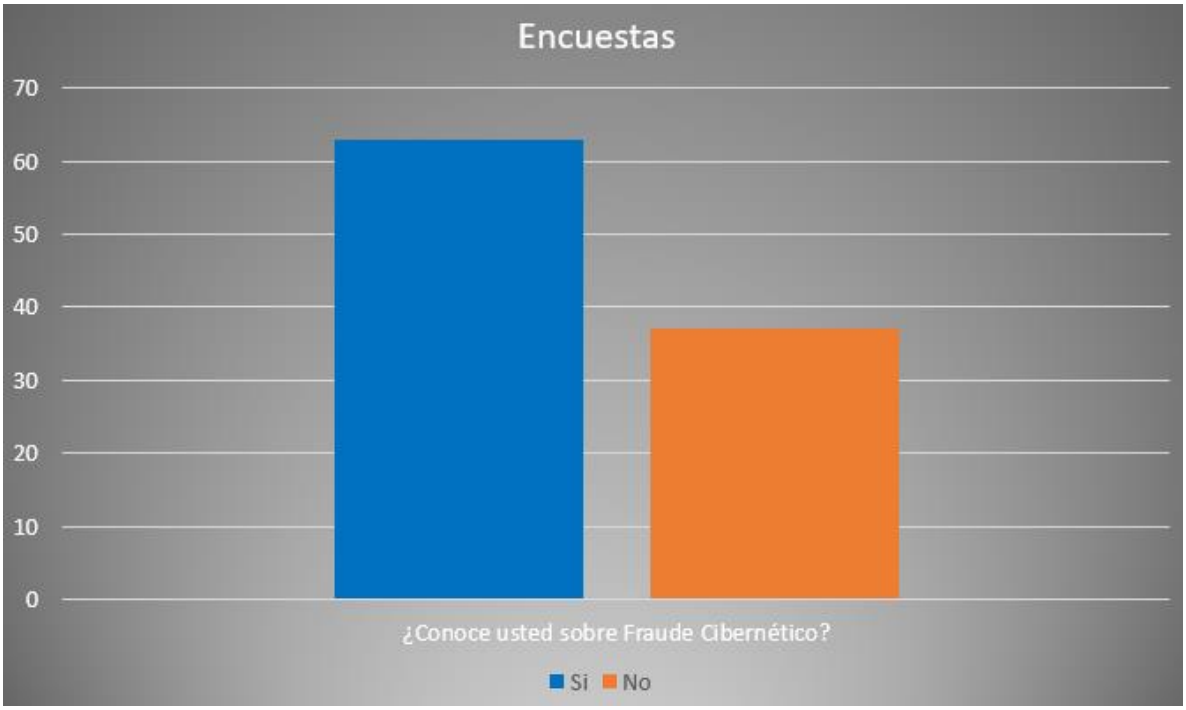

Ilustración 14: ¿Conoce usted sobre fraude cibernético?

Como podemos observar en la gráfica solo el 63% de los encuestados (que representa 63 personas) respondieron que conocen sobre fraude cibernético, y el 37% de los encuestados (que representa 37 personas) respondieron que no conocen sobre fraude cibernético.

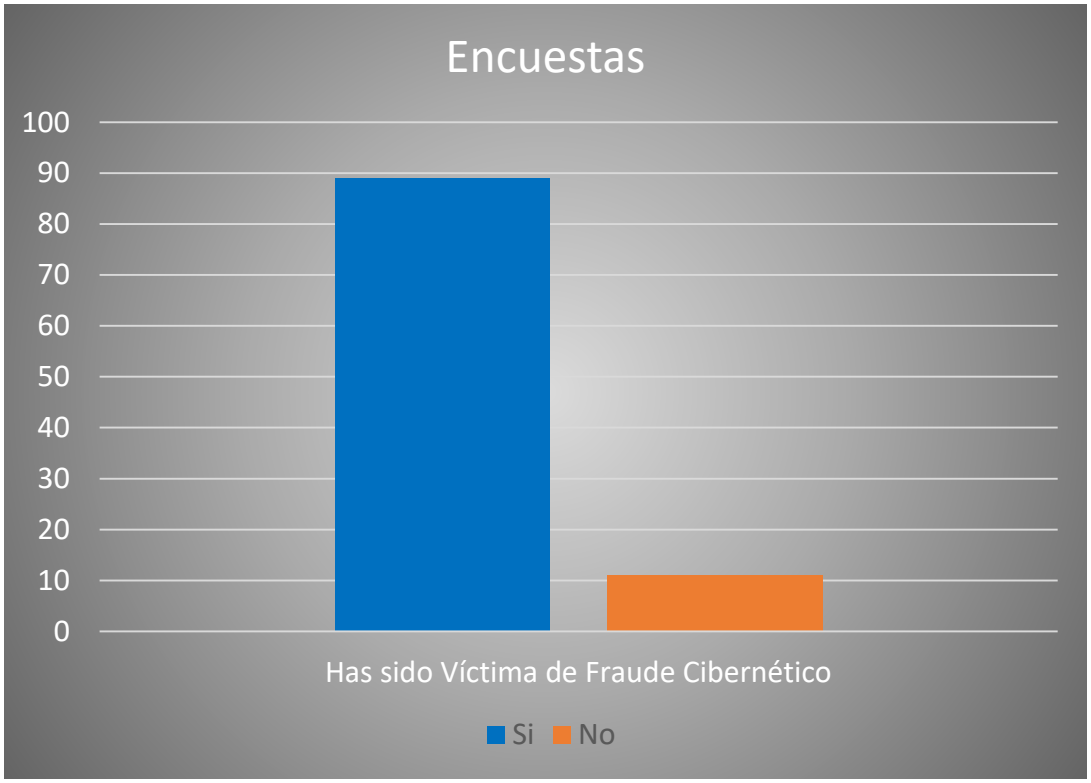

Ilustración 15: ¿Has sido víctima de fraude cibernético?

Como podemos observar en la gráfica solo el 89% de los encuestados (que representa 89 personas) respondieron que han sido víctimas de fraude cibernético, y el 11% de los encuestados (que representa 11 personas) respondieron que no han sido víctimas de fraude cibernético.

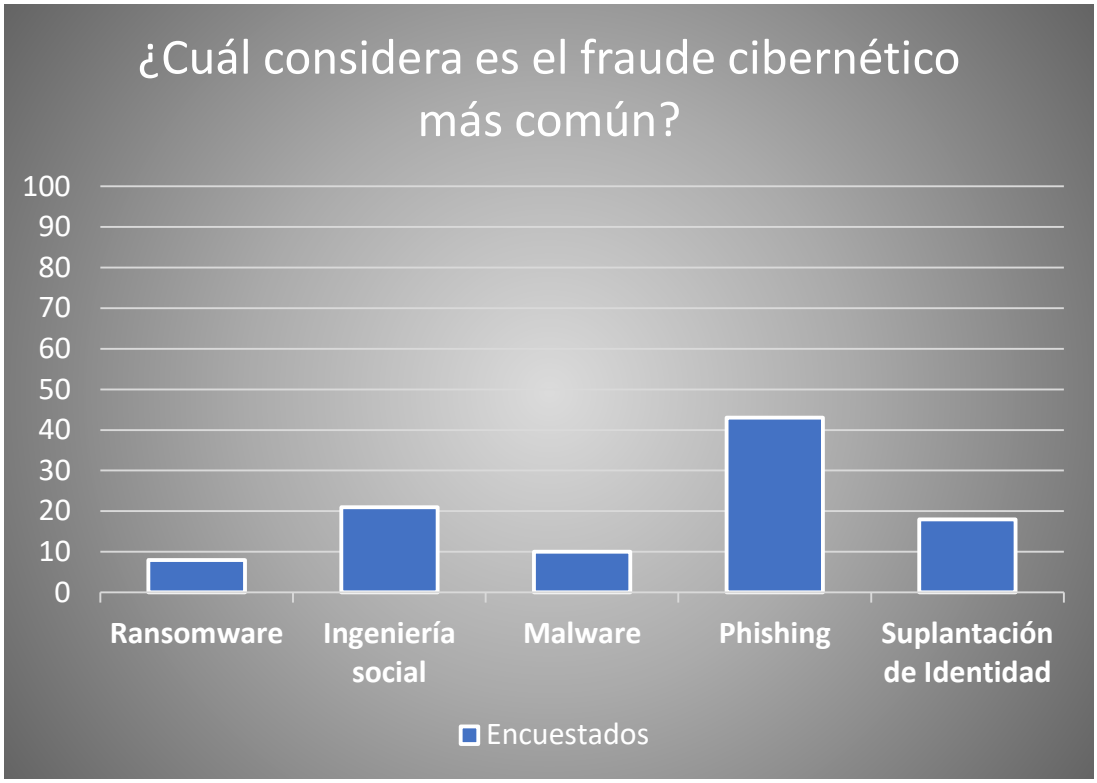

Ilustración 16: ¿Cual considera es el fraude cibernético más común?

Como podemos observar en la gráfica solo el 43% de los encuestados (que representa 43 personas) respondieron que el fraude más común es el phishing, el 21% (que representa 21 personas) respondieron que el fraude más común es la Ingeniería Social, el 18% (que representan 18 personas) respondieron que el fraude más común es la suplantación de identidad y el 8% (que representa 8 personas) respondieron que el fraude más común es el ransonware.

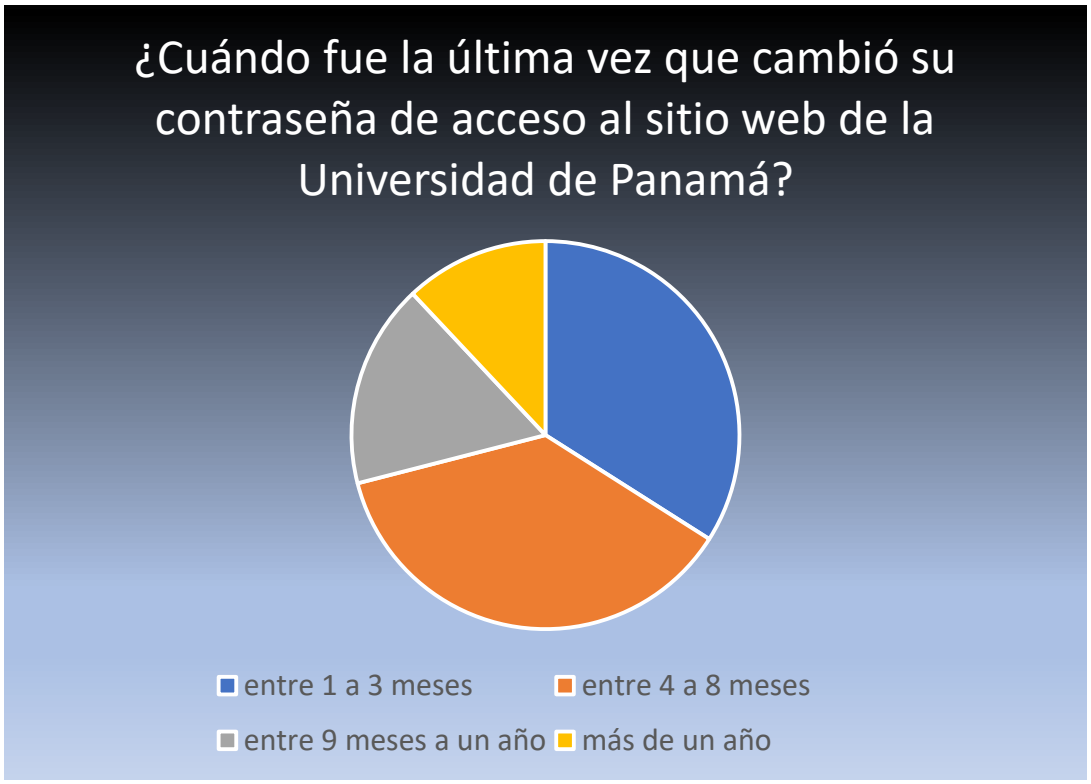

Ilustración 17: ¿Cuándo fue la última vez que cambio su contraseña de acceso al sitio web de la UP?

Como podemos observar en la gráfica solo el 37% de los encuestados (que representa 37 personas) respondieron que han cambiado su contraseña hace 4 a 8 meses, el 34% de los encuestados (que representa 34 personas) han cambiado su contraseña hace 1 a 3 meses, el 17% de los encuestados (que representa 17 personas) han cambiado su contraseña hace 9 a un año, y el 12% de los encuestados (que representa 12 personas) han cambiado su contraseña hace más de 1 año.

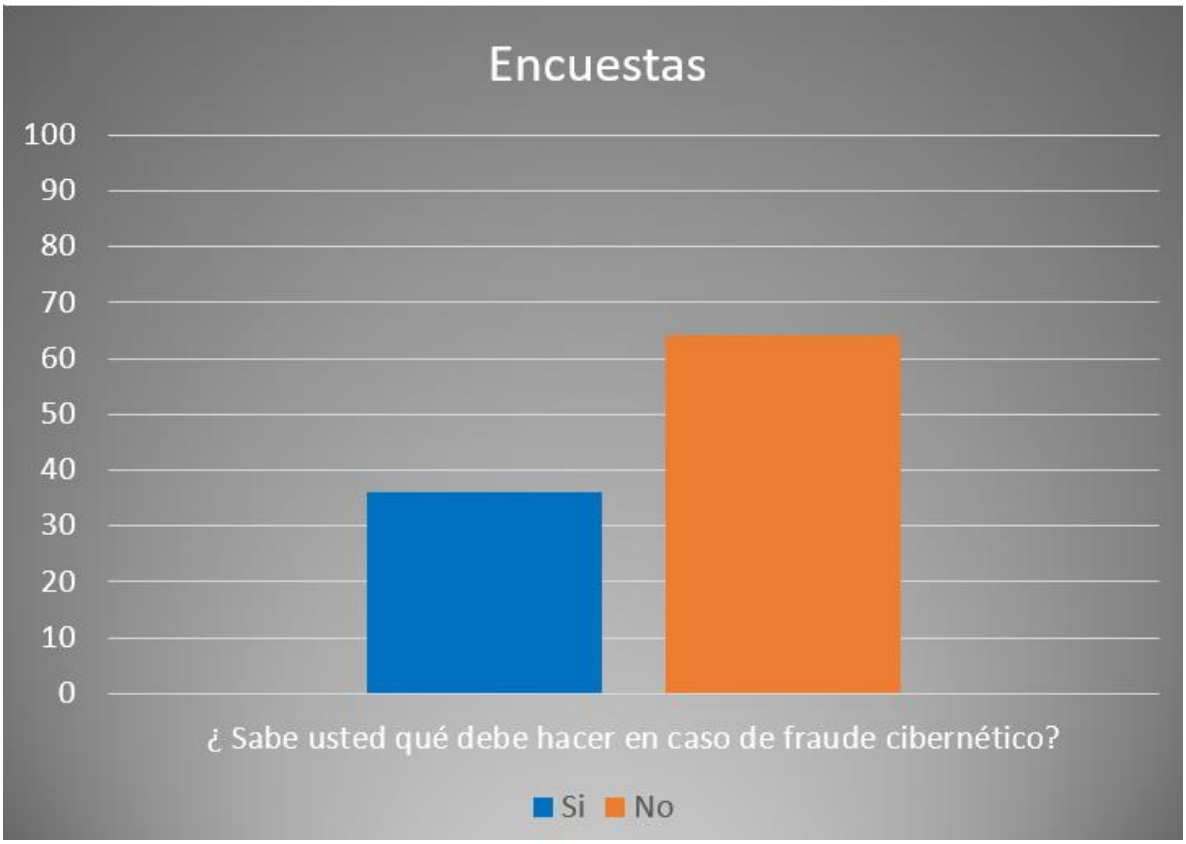

Ilustración 18: ¿Conoce usted que debe hacer en caso de fraude cibernético?

Como podemos observar en la gráfica solo el 64% de los encuestados (que representa 64 personas) respondieron que han sido víctimas de fraude cibernético, y el 36% de los encuestados (que representa 36 personas) respondieron que no han sido víctimas de fraude cibernético.

4.2 ANÁLISIS DE LOS RESULTADOS

Con estos resultados se puede observar que se necesita implementar un sistema de prevención de fraude que involucre toda la institución, así como realizar un arduo trabajo con los usuarios para concientizarlos sobre fraude cibernético, ya que es fundamental para protegernos de posibles ataques informáticos dentro de la institución.

El resultado de esta encuesta sobre fraude cibernético nos lleva a sacar un análisis de diversas formas y correlacionar los resultados, dependiendo de los objetivos específicos de la encuesta y del análisis de los datos.

Primeramente, nos debemos basar en identificar las principales formas de fraude cibernético. En la encuesta se incluyeron preguntas sobre los tipos de fraude cibernético que las personas han experimentado o sobre los tipos de fraudes que conocen; basándonos en resultados pudimos apreciar que el phishing es el tipo de fraude cibernético más comúnmente experimentado, esto podría indicar la necesidad de una mayor educación sobre cómo detectar y evitar el phishing.

Otro de los análisis generados es evaluar la efectividad de las medidas de seguridad que actualmente se tienen, como, por ejemplo, si la encuesta encontró que la mayoría de las personas utilizan contraseñas débiles y no las cambian en un tiempo prudente y adicionalmente no se utiliza el multifactor de autenticación, esto podría indicar la necesidad implementar mejores controles de seguridad.

Como resultado podemos precisar que hay una necesidad de medidas de protección adicionales para combatir este problema, por lo cual plantearemos una propuesta basada en resultados y análisis que nos lleven a encontrar medidas más fuertes y eficaces.

V. DISCUSIÓN DE RESULTADOS

5.1 CONCLUSIONES

Los sistemas de prevención de fraude cibernético es uno de los elementos vitales con los que debería contar la Universidad de Panamá, debido a la gran cantidad de datos confidenciales almacenados bajo su custodia, incluida la información de identificación personal, registros financieros y otros tipos de información privada. La institución debe adoptar medidas proactivas constantemente para protegerse contra el uso indebido o el robo de datos a nivel interno, el robo de datos a nivel externo y contra la amenaza de los ataques de malintencionados de los ciberdelincuentes para acceder a su base de datos.

Las políticas y los procedimientos de prevención de fraude cibernético adecuados permiten gestionar la protección de sus recursos físicos y financieros, su reputación, su posición legal, sus empleados y otros activos tangibles e intangibles de manera efectiva.

Uno de los mayores beneficios del monitoreo de la exposición cibernética es la detección temprana de amenazas. Al monitorear las posibles amenazas y vulnerabilidades, se puede detectar y responder a posibles ataques antes de que se conviertan en un problema. Esto puede ayudar a prevenir filtraciones de datos, minimizar el impacto de los incidentes de seguridad y reducir el riesgo de pérdidas financieras o daños a la reputación.

El fraude cibernético es una creciente amenaza en el mundo digital que afecta a individuos, empresas y organizaciones de todo tipo. Este tipo de fraude incluye actividades ilícitas como el robo de identidad, el phishing, el malware y otras formas de manipulación

para obtener datos sensibles sin autorización. Las consecuencias del fraude cibernético pueden ser devastadoras.

Como conclusión de los resultados obtenidos en esta investigación se puede determinar que las medidas de seguridad cibernética deben enfocarse en la prevención antes que en la respuesta a los incidentes. Esto incluye implementar herramientas como autenticación multifactorial, sistemas de monitoreo y auditorías periódicas para detectar y prevenir ataques. Además de que uno de los factores más importantes en la lucha contra el fraude cibernético es la educación, los administradores de los sistemas deben estar constantemente informados sobre las nuevas tácticas de los delincuentes y cómo proteger la información personal que está bajo la custodia de la institución, esto es clave para mitigar los riesgos de fraude cibernético. Esto incluye el cifrado de datos sensibles y la implementación de políticas de acceso seguras.

En caso de un ataque, una respuesta rápida y eficaz es esencial para minimizar el impacto. Contar con un plan de acción para incidentes cibernéticos ayuda a reducir los daños y a restaurar la seguridad lo antes posible.

El fraude cibernético es una amenaza en constante evolución, y la mejor defensa es una visión general que combine tecnología avanzada, educación continua y una cultura de seguridad proactiva. La institución debe adaptarse rápidamente a las nuevas amenazas para proteger tanto sus activos como la información confidencial que manejan.

5.2 RECOMENDACIONES

Para prevenir el fraude cibernético es recomendable implementar las siguientes medidas dentro de la institución:

- Implementar una herramienta de uso medido para el área de tecnología dedicado a las validaciones en tiempo real, con sistemas de detección de fraude utilizando inteligencia artificial y análisis de datos para detectar comportamientos sospechosos en los diversos accesos al sistema de la institución.

- Implementar controles de autenticación de multifactor (MFA) para acceder a sistemas críticos, reduciendo el riesgo de accesos no autorizados para obtener datos sensitivos de la institución o su base de datos.

- Implementar políticas robustas de seguridad, desarrollando y actualizando constantemente políticas basadas en accesos y uso de las plataformas, estas políticas deben estar claras, accesibles y de obligatorio cumplimiento. La política debe incluir prácticas recomendadas de seguridad cibernética y las responsabilidades de los usuarios para garantizar la seguridad de los activos.

- Realizar revisiones periódicas de auditoría de los sistemas y aplicaciones para identificar posibles fallas o vulnerabilidades y poder corregirla a tiempo.

- Organizar sesiones de capacitación a los estudiantes, administrativos y profesores para que conozcan los diferentes tipos de fraude cibernético y cómo detectarlos. Es importante que esta capacitación sea impartida por un experto en ciberseguridad o un profesional de TI para garantizar que la información sea precisa y actualizada.

- Enviar publicaciones informativas en la intranet para educarlos sobre los diferentes tipos de fraude cibernético. Las publicaciones en la intranet pueden ser una forma efectiva de recordar a los usuarios sobre los riesgos del fraude cibernético. Estos mensajes pueden incluir consejos prácticos sobre cómo protegerse en línea y cómo identificar las señales de advertencia de posibles fraudes.

- Realizar pruebas regulares de seguridad para detectar posibles vulnerabilidades en su sistema y evaluar su efectividad en caso de un ataque cibernético. Las pruebas de seguridad pueden incluir pruebas de penetración y simulaciones de ataques cibernéticos.

BIBLIOGRAFÍA

Libros:

- **Ciberseguridad: consejos para tener vidas digitales más seguras, autora: Mónica Valle**

- **Ethical Hacking, Un enfoque metodológico para profesionales, autores: Ezequiel Martín Sallis, Claudio Bernardo Caracciolo y Marcelo Fabián Rodríguez. Fue publicado en 2010 por Alfaomega Grupo Editor en Buenos Aires, Argentina.**

- **Análisis práctico de malware, autor: Raúl Acosta Bermejo.**

- **AIG. "Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructura Crítica," 2013.**

- **The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age, autor: Adam Segal, publicado en 2016.**

- **Malware Data Science, autores: Joshua Saxe y Hillary Sanders, publicado en 2018.**

- **Ingeniería social: la ciencia de la piratería humana, autor: Christopher Hadnagy, publicado en 2010.**

- **M. Moreno García. "Gestión de incidentes de ciberseguridad, 1". RA-MA Editorial, 2022.**

- **Modelado de amenazas, autor: Frank Swiderski.**

- **The Cyber Effect, autora: Mary Aiken.**

- **D. Fernández Bermejo y G. Martínez Atienza, Ciberdelitos. Barcelona: Ediciones Experiencia, 2020.**

- **Ciberseguridad, autor: Lester Evans.**

- **Hacking Exposed 7: Network Security Secrets and Solutions, autores: Joel Scambray, Stuart McClure, George Kurtz.**

- **El arte de la invisibilidad, autores: Robert Vamosi, Kevin Mitnick.**

- **Código Penal Acusatorio de Panamá. Título VIII, Cap. I Delitos contra la Seguridad Informática. Artículos 285-286-287, pág. 52-53**

- **ANTABI. "Ley 81 de Protección de Datos Personales". 2021.**

INFOGRAFÍA

- **https://cert.pa/**
- **https://somosimpactopositivo.com/**
- **https://www.educapanama.edu.pa/**
- **https://panamacibersegura.gob.pa/**
- **https://www.martesfinanciero.com/**
- **https://www.cronup.com**
- **https://www.semantic-systems.com/**
- **https://www.fortinet.com/lat/resources/cyberglossary/internet-fraud**
- **https://www.larepublica.co/ciberseguridad**

- **https://revistabyte.es/**
- **https://www.microsoft.com/es-es/security**
- **https://www.abc.es/tecnologia/internet/ciberseguridad/**
- **https://blog.uvirtual.org/**
- **https://aig.gob.pa/documentos/**
- **https://elibro.net/es/ereader/**
- **https://www.antai.gob.pa/reglamentan-ley-81-de-proteccion-de-datos-personales/**
- **https://www.up.ac.pa/intranet**

ANEXOS

Encuesta Realizada:

1. ¿Conoce usted acerca del fraude cibernético?

- Sí
- No

2. ¿Ha sido víctima de algún tipo de fraude cibernético?

- Sí
- No

3. ¿Cuál considera es el fraude cibernético más común?

- Ransomware
- Ingeniería social
- Malware
- Phishing

- Suplantación de identidad

4. *¿Cuándo fue la última vez que cambió su contraseña de su acceso al sitio web de la Universidad de Panamá?*

   - entre 1 a 3 meses
   - entre 4 a 8 meses
   - entre 9 meses a un año
   - más de un año

5. *¿Conoce usted qué debe hacer en caso de ser víctima de fraude cibernético?*

   - Sí
   - No

GLOSARIO

- Phishing: un tipo de fraude que involucra correos electrónicos falsos, sitios web y mensajes de texto que parecen provenir de fuentes confiables para robar información personal y financiera.
- Malware: software malicioso que infecta dispositivos y redes para robar información o controlarlos a través de una red de bots.
- Ransomware: un tipo de malware que bloquea el acceso a los datos y exige un rescate para recuperarlos.
- Fraude de identidad: el uso no autorizado de información personal, como nombres, números de seguro social y números de tarjetas de crédito para cometer delitos.
- Estafas de correo electrónico empresarial (BEC): un tipo de fraude en el que los delincuentes se hacen pasar por empleados de una empresa para engañar a los destinatarios para que realicen transferencias de dinero a cuentas falsas.
- Ingeniería social: técnicas de manipulación psicológica utilizadas por los delincuentes para engañar a los usuarios para que revelen información confidencial o realicen acciones no deseadas.
- MFA: la autenticación multifactor (MFA) agrega una capa de protección al proceso de inicio de sesión. Cuando se accede a una cuenta o aplicación, los usuarios deben pasar por una verificación de identidad adicional; por ejemplo, tienen que escanear su huella digital o especificar un código que reciben en su teléfono.

ÍNDICE DE FIGURAS