



**UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA**

Departamento de Ingeniería Comercial

**“EL ROL DE LA INTELIGENCIA ARTIFICIAL EN LOS FRAUDES
DIGITALES DENTRO DE LAS EMPRESAS: MÉTODOS, IMPACTO
Y PERSPECTIVAS FUTURAS”**

TESIS PARA OPTAR AL TÍTULO DE INGENIERA COMERCIAL

AUTORA

FRANCISCA ESTELLES OLIVARES

PROFESOR GUÍA

FRANCESCO PONTARELLI CONTRERAS

PROFESOR CORREFERENTE

MACARENA GATICA SILVA

2024

Agradecimientos

En primer lugar, quiero expresar mi más profundo agradecimiento a mi padre y madre, por su apoyo incondicional durante toda mi carrera universitaria. Extiendo este agradecimiento a toda mi familia, sobre todo a mis hermanos y hermanas, quienes me apoyaron sin dudar en cada paso del camino.

Agradezco a mis compañeras, con quienes compartí asignaturas, risas, experiencias y aprendizajes. Sin duda, fueron un apoyo fundamental para mí y siempre las recordaré con mucho cariño.

Un sincero agradecimiento a todos los profesores y profesoras que confiaron en mí y me motivaron a continuar. Destaco su labor como profesionales y su compromiso con los estudiantes. Sin duda, sus conocimientos y enseñanzas me servirán durante toda mi vida.

También, quiero agradecer a todas las personas que formaron parte de mi investigación. Su interés por colaborar fue esencial, y gracias a su participación, aprendí mucho más de lo que esperaba.

Finalmente, me gustaría agradecerme a mí misma por llegar hasta aquí y lograr todo lo que me he propuesto durante mi vida académica, reconozco que el camino no fue fácil, sin embargo, fui capaz de superar cada desafío que se presentó.

A todos, mis más sinceros agradecimientos.

Resumen Ejecutivo

El presente estudio tiene como objetivo investigar el uso de la inteligencia artificial (IA) en la realización y prevención de fraudes digitales, analizar la relación de la IA con la ciberseguridad en las empresas y conocer la percepción y perspectivas de los expertos. Se plantean propuestas que incluyen la capacidad de la IA para reducir pérdidas económicas y vulnerabilidades, la importancia del conocimiento y ética profesional en la eficacia de la IA, el potencial de la IA para fortalecer las técnicas de fraude, y la percepción crítica de empresas afectadas por fraudes sobre la necesidad de invertir en ciberseguridad.

La investigación se basa en una metodología con enfoque cualitativo basado en entrevistas semi estructuradas dirigidas a profesionales en ciberseguridad e IA, las cuales se centraron en el uso de la IA como herramienta para prevenir los fraudes digitales, así como también para efectuarlos, además del papel de la IA en la ciberseguridad de las empresas, y, por último, se abordaron sus percepciones en este ámbito.

El análisis de las entrevistas revela que la IA es eficaz en la detección y prevención de fraudes digitales, aunque su efectividad depende de la inversión y preparación interna de las empresas. La importancia del factor humano y la capacitación continua son cruciales para maximizar sus capacidades. Los expertos destacan que la IA también es utilizada para realizar fraudes más sofisticados, lo que plantea desafíos adicionales. Además, las empresas afectadas por fraudes tienden a aumentar sus inversiones en ciberseguridad, mostrando una actitud proactiva.

Y, por último, en Chile, la Ley Marco de Ciberseguridad junto con la creación de la Agencia Nacional de Ciberseguridad han establecido un gran avance en esta materia, sin embargo, existe una escasez de profesionales especializados y conciencia en las personas, por lo cual aún falta mucho por avanzar.

Palabras claves: Inteligencia Artificial, Ciberseguridad, Fraudes Digitales, Empresas, Factor humano, Perspectivas, Percepción.

Abstract

The present study aims to investigate the use of artificial intelligence (AI) in the realization and prevention of digital fraud, analyze the relationship of AI with cybersecurity in companies, and learn about the perception and perspectives of experts. Proposals are presented that include the ability of AI to reduce economic losses and vulnerabilities, the importance of knowledge and professional ethics in the effectiveness of AI, the potential of AI to enhance fraud techniques, and the critical perception of companies affected by fraud regarding the need to invest in cybersecurity.

The research is based on a qualitative approach methodology based on semi-structured interviews with cybersecurity and AI professionals, which focused on the use of AI as a tool to prevent digital fraud, as well as to carry it out, the role of AI in the cybersecurity of companies, and finally, their perceptions in this area.

The analysis of the interviews reveals that AI is effective in detecting and preventing digital fraud, although its effectiveness depends on the internal investment and preparation of companies. The importance of the human factor and continuous education are crucial to maximize its capabilities. Experts highlight that AI is also being used to carry out more sophisticated frauds, which poses additional challenges. In addition, companies affected by fraud have to increase their investments in cybersecurity, showing a proactive attitude.

And finally, in Chile, the Cybersecurity Framework Law and the creation of the National Cybersecurity Agency have established a breakthrough in this area, however, there is a shortage of professionals specialized in this area, so there is still a long way to go.

Keywords: Artificial Intelligence, Cybersecurity, Digital Fraud, Companies, Human Factor, Perspectives, Perception.

Índice

Introducción	7
Preguntas de investigación.....	8
Objetivos.....	8
1. Objetivo general	8
2. Objetivos específicos	8
Marco Teórico.....	9
1. Inteligencia Artificial.....	9
2. Fraudes digitales.....	10
3. Principales métodos de fraudes digitales.....	10
3.1 Malware.....	11
3.2 Phishing	12
3.3 Vishing.....	12
3.4 Smishing	13
3.5 Botnets	14
3.6 Ransomware.....	14
4. Ciberseguridad	15
5. Inteligencia Artificial en Ciberseguridad	16
5.1 Aprendizaje automático (ML).....	16
5.2 Aprendizaje profundo (DL).....	17
6. Medidas tomadas en Chile.....	17
7. Perspectivas y percepción	19
Propuestas	20
Metodología.....	21
1. Entrevista	22

Resultados	23
Análisis.....	35
Conclusiones.....	47
Recomendaciones.....	50
Bibliografía.....	69

Introducción

En la era de la digitalización y el avance tecnológico acelerado, la seguridad de la información y la prevención del fraude digital se han convertido en temas de vital importancia para las empresas a nivel mundial. La digitalización no solo ha transformado la forma en que las organizaciones operan y se comunican, sino que también ha creado nuevas oportunidades y desafíos en términos de ciberseguridad. La interconectividad de los sistemas informáticos y el incremento en la dependencia de tecnologías digitales han expuesto a las empresas a una variedad de amenazas cibernéticas, entre las cuales el fraude digital ocupa un lugar preponderante.

El fraude digital se refiere a una amplia gama de actividades maliciosas que tienen como objetivo engañar a las personas y organizaciones para obtener beneficios financieros o información confidencial. Estas actividades pueden incluir, entre otras, el phishing, el malware, ransomware, robo de identidad y la manipulación de datos. La sofisticación y la frecuencia de estos ataques han crecido exponencialmente, impulsando a las organizaciones a buscar soluciones innovadoras para proteger sus activos.

En este contexto, la inteligencia artificial ha emergido como una herramienta crucial en la lucha contra el fraude digital. La IA, con su capacidad para procesar y analizar grandes volúmenes de datos a velocidades inigualables, ofrece un enfoque proactivo y dinámico para la detección y prevención del fraude.

Esta investigación tiene como objetivo proporcionar un análisis del impacto de la inteligencia artificial en los fraudes digitales dentro de las empresas. A través de un análisis cualitativo, se busca conocer la eficacia de las herramientas de IA, los métodos de fraudes digitales, el impacto que tienen dentro de las empresas, además de las perspectivas de los expertos sobre la ciberseguridad.

Para lograr estos objetivos, se realizarán entrevistas con profesionales en el ámbito de la ciberseguridad y la inteligencia artificial. Estas entrevistas proporcionarán una visión profunda de las experiencias y percepciones de los expertos sobre el uso de la IA en la prevención de fraudes, así como recomendaciones para mejorar la adopción y efectividad de estas tecnologías.

Preguntas de investigación

Se plantean las siguientes preguntas de investigación

1. ¿Cuál es el impacto de la implementación de inteligencia artificial en la incidencia de los fraudes digitales dentro de las empresas?
2. ¿Cómo pueden las tecnologías de Inteligencia artificial mejorar la detección y prevención de fraudes digitales?
3. ¿Cuál es la percepción de expertos respecto al papel de la inteligencia artificial en la prevención de fraudes digitales y cuáles son sus expectativas para su desarrollo futuro en este campo?

Objetivos

1. Objetivo general

Investigar el uso de la inteligencia artificial para realizar y prevenir fraudes digitales, además de conocer su relación con la ciberseguridad dentro de las empresas y conocer las perspectivas de los expertos en este ámbito.

2. Objetivos específicos

1. Investigar los principales métodos utilizados para realizar fraudes digitales con IA y el impacto que tienen a nivel organizacional.
2. Investigar las herramientas de la IA utilizadas para detectar los fraudes digitales.
3. Investigar las medidas que se están tomando a nivel nacional para detener los fraudes digitales.
4. Conocer las perspectivas y percepción de los expertos sobre las expectativas de la IA en relación a los fraudes digitales y ciberseguridad de las organizaciones.

Marco Teórico

1. Inteligencia Artificial

Dos momentos claves que son ampliamente reconocidos como los cimientos de la Inteligencia Artificial (AI) fueron, en primer lugar, en 1951 Marvin Minsky junto a Dean Edmonds crearon la primera máquina electrónica de la historia capaz de aprender, bautizada como SNARC (Stochastic Neural Analog Reinforcement Calculator) empleaba 400 válvulas electrónicas y su mecanismo estaba basado en la simulación de redes neurales, y en segundo lugar, el test de Turing que desarrolló el matemático Alan Turing en 1950.

El test de Turing, también conocido como el "juego de imitación", como se menciona en el artículo de *“Computing Machinery And Intelligence”* de Alan Turing (A. M Turing, 1950), consiste en un escenario en el que un humano, sin saber si está interactuando con otro humano o con una máquina, formula preguntas por escrito a un tercero, quien responde también por escrito. El objetivo es que el entrevistador determine si está hablando con una máquina o con un humano. El éxito de la máquina en engañar al humano se considera como un indicio de su inteligencia. Para superar esta prueba, la máquina debe ser capaz de comprender y expresarse en lenguaje natural de manera coherente, almacenar y utilizar la información recibida, formular conclusiones, aprender del comportamiento y del entorno, y manipular objetos para responder adecuadamente.

John McCarthy, considerado como uno de los pioneros de la inteligencia artificial, define la IA como la ciencia e ingeniería de hacer máquinas inteligentes, especialmente programas informáticos inteligentes. Aunque se relaciona con la tarea similar de usar computadoras para comprender la inteligencia humana, no se limita necesariamente a métodos que sean biológicamente observables. (McCarthy, s. f.)

En 1956 McCarthy consiguió reunir en un “think tank” en Dartmouth a diez intelectuales punteros en el área para realizar un estudio de dos meses sobre la inteligencia artificial. Los temas que se trataron fueron: la automatización de los ordenadores, como programar un ordenador para que pueda utilizar el lenguaje, las redes neuronales, la teoría del tamaño del cálculo, el “machine learning”, la aleatoriedad y creatividad en las máquinas y como conseguir que las máquinas consigan realizar abstracciones (John McCarthy et al., 1955).

Del encuentro se destaca sobre todo la aportación de Newell y Simon en lo que se considera hoy en día por muchos el primer programa de IA creado, el “Logic Theorist”. Este programa era capaz no solo de pensar lógicamente sino también de interpretar y manipular símbolos. Esta reunión fue un punto de inflexión en el avance de la Inteligencia Artificial. Los participantes y sus seguidores asumieron la responsabilidad de avanzar en este campo, manteniéndose a la vanguardia durante un largo período de tiempo.

2. Fraudes digitales

El fraude digital puede adoptar muchas formas diferentes y no existe una definición uniforme en todas las jurisdicciones. Según el Banco de Pagos Internacionales, el fraude digital abarca múltiples dimensiones, por ejemplo, protección del consumidor, conducta, integridad del mercado, estabilidad financiera y, por lo tanto, es de naturaleza intersectorial (Bank for International Settlements, 2023). Según la Asociación de Examinadores Certificados de Fraude, el fraude es el uso de la propia ocupación para el enriquecimiento personal mediante el mal uso deliberado o la mala aplicación de los recursos o activos de la organización empleadora (ACFE, 2002).

La razón principal detrás del fraude es “lograr ganancias en terreno falso por medios ilegales un impacto dramático en la economía, el derecho e incluso los valores morales humanos” (Panos Alexopoulos et al., 2007). Casi todo sistema tecnológico que involucra dinero y servicios puede verse comprometido por actos fraudulentos (Almeida, 2009). Por lo tanto, los fraudes en estos sistemas se consideran delitos cibernéticos y causan enormes pérdidas financieras, además, puede reducir la confianza en la industria, desestabilizar las economías y afectar el costo de vida de las personas (West & Bhattacharya, 2016).

3. Principales métodos de fraudes digitales

Según el informe de la Interpol sobre las tendencias de la delincuencia a escala mundial (Interpol, 2022) y el informe de las principales amenazas cibernéticas realizado por la Agencia de la Unión Europea (Enisa, 2020), entre los principales delitos cometidos a nivel mundial que son de preocupación primordial se encuentran los fraudes realizados a través de malware, phishing, vishing, smishing, botnets y ransomware.

3.1 Malware

El término malware proviene de la palabra “Software malicioso” y se refiere a programas potencialmente dañinos para el usuario, que tienen como objetivo robar datos confidenciales, controlar la actividad en la PC o robar la identidad del usuario.

Según el artículo sobre amenazas emergentes en ciberseguridad (Jang-Jaccard & Nepal, 2014), existen tres categorías principales de técnicas para detectar malware, aunque hay otras formas de clasificación, la primera es basadas en firmas, la segunda se basa en anomalías y la tercera en heurísticas.

Cuando se emplea un enfoque basado en firmas, los desarrolladores escanean un archivo en búsqueda de malware, comparan la información con una base de datos de firmas de virus y luego corroboran los resultados. Si la información coincide con la de la base de datos, se considera que el archivo está infectado con un virus. Aunque este método limita la detección de malware desconocido, su ventaja principal radica en su eficacia con malware conocido.

Los métodos basados en anomalías superan las limitaciones de las técnicas basadas en firmas al permitir la detección de cualquier malware, tanto conocido como desconocido, mediante la aplicación de técnicas de clasificación a las acciones de un sistema. La mejora en la detección de actividad de malware se logra al cambiar de una detección basada en patrones a una basada en clasificación para identificar comportamientos normales o anómalos. La aplicación de IA a sistemas de detección basados en firmas y anomalías mejora la eficiencia en la detección de malware.

Por otro lado, el método basado en heurística utiliza técnicas de minería de datos y aprendizaje automático para comprender el comportamiento de un archivo ejecutable.

Asimismo, el malware puede ingresar a los sistemas a través de varias vías, como la propagación desde dispositivos previamente infectados, la persuasión de los usuarios para que abran archivos contaminados o siendo atraídos hacia sitios web que distribuyen malware.

Este tipo de software puede infiltrarse en cualquier fase del ciclo de vida de un sistema y se adapta y evoluciona constantemente, aprovechando las nuevas tecnologías emergentes y sus vulnerabilidades para evitar ser detectado.

3.2 Phishing

El phishing es una forma de intentar adquirir información confidencial, como nombre de usuario, contraseña o detalles de la tarjeta de crédito, haciéndose pasar por una entidad confiable. La mayoría de las estafas de phishing se basan en engañar al usuario para que visite un sitio web malicioso que afirma pertenecer a empresas y agencias legítimas. El usuario desprevenido ingresa información privada en el sitio web malicioso que luego es utilizada por delincuentes maliciosos. La mayoría de los métodos de phishing utilizan alguna forma de engaño técnico diseñado para hacer que un enlace en un correo electrónico (y un sitio web falsificado) parezca pertenecer a una organización legítima, como un banco conocido (Jang-Jaccard & Nepal, 2014).

Según el Informe de phishing del 2022 realizado por la Zscaler, empresa de ciberseguridad (Zscaler, 2022), Los ataques de phishing aumentaron un 29 % en 2021 en comparación con 2020, entre los cinco países que sufrieron el mayor número de ataques se encuentran Estados Unidos, Singapur, Alemania, los Países Bajos y el Reino Unido.

Además, señala que los tres principales métodos que son utilizados para realizar fraudes digitales por medio de phishing son a través de un enlace, donde el usuario hace clic en un enlace malicioso que lleva a un sitio de phishing, un archivo alojado o una instalación de malware, a través de una solicitud, en la cual se pide al usuario que envíe información confidencial que da lugar a un robo de datos, y por medio de un archivo adjunto que contiene un software malicioso.

3.3 Vishing

El artículo *“Phishing, SMiShing y Vishing: una evaluación de las amenazas contra Dispositivos móviles”* menciona que el vishing es la práctica criminal de utilizar el sistema telefónico para obtener acceso a información personal y financiera de los clientes con el propósito de cometer fraude. Los autores señalan que el vishing explota la confianza de un individuo en los servicios telefónicos, ya que la víctima a menudo no es consciente de que los estafadores pueden utilizar métodos como el suplantamiento de identidad en el identificador de llamadas y sistemas automatizados complejos para cometer este tipo de estafa. Sin embargo, a medida que el rendimiento de los ataques de phishing tradicionales

sigue disminuyendo, los estafadores han recurrido al vishing en un intento de robar números de cuenta financieros, contraseñas y otros datos personales de los usuarios. (Osei et al. 2014)

3.4 Smishing

La palabra Smishing fue utilizada por primera vez en el 2006 por David Rayhawk de McAfee (Mishra et al. 2020). Smishing debe su nombre a la tecnología de mensajería de prueba SMS (Short Message Service), implica el envío de un mensaje de texto a un teléfono móvil con el fin de persuadir al individuo para que divulgue información personal.

Al igual que en el phishing o vishing, un ataque de smishing generalmente incluye una llamada a la acción para la víctima prevista que requiere una "respuesta inmediata". Además, “el smishing está emergiendo como una herramienta de fraude preferida a nivel mundial, ya que cada vez más consumidores acceden a Internet a través de dispositivos móviles o teléfonos celulares en lugar de una computadora de escritorio o portátil tradicional” (Osei et al. 2014).

Como se menciona en el artículo “*Smishing detector*”, un mensaje de texto Smishing puede contener varias actividades maliciosas, incluyendo la inserción de URL, donde los atacantes envían mensajes de texto con enlaces incrustados y al hacer clic se puede instalar un código malicioso en el teléfono de la víctima, el usuario es redirigido a un sitio web de phishing que imita uno legítimo, solicitando información confidencial como credenciales de usuario o detalles de tarjetas de crédito o se descarga un archivo en el dispositivo, que resulta ser malware y puede llevar a actividades maliciosas posteriores.

Otra forma de Smishing que se ha posicionado son los mensajes que ofrecen cupones, descuentos o regalos gratuitos junto con un número de teléfono o dirección de correo electrónico, por el cual solicitan a las víctimas que se comuniquen con ellos a través de estos medios y luego intentan obtener sus credenciales de manera gradual. Asimismo, también existen los mensajes automáticos solicitando a la víctima que se suscriba o cancele la suscripción a un servicio, redirigiéndolos a sitios web maliciosos.

Durante el smishing, los atacantes diseñan la interfaz de usuario de manera astuta para que sea difícil para la víctima distinguir entre un sitio web legítimo y uno falso. Copian el código fuente de sitios web legítimos para crear páginas falsas que se asemejan a las legítimas.

Además, modifican las URL para que parezcan genuinas, pero en realidad conducen a sitios web o archivos maliciosos (Mishra et al. 2020).

3.5 Botnets

Un Botnet es una agrupación de dispositivos conectados en línea que ejecutan, sin el consentimiento de sus dueños, uno o más Bots, programas que realizan acciones automáticas y suelen imitar o suplantar el comportamiento humano. Debido a que cada dispositivo tiene una dirección IP única, la actividad de un Botnet involucra múltiples direcciones IP, dificultando la ubicación y la interrupción de la fuente del tráfico malicioso de Bots. Cuando se utilizan para infectar otras computadoras, los dispositivos de los destinatarios de correo no deseado pueden contribuir al crecimiento de los Botnets.

Los atacantes pueden emplear Bots maliciosos en un Botnet o red de Bots para lanzar estos ataques y ocultar su origen. Son difíciles de detectar porque requieren pocos recursos computacionales, lo que evita que interfieran con el funcionamiento normal de las aplicaciones y no levanta sospechas en el usuario. Sin embargo, las Botnets más avanzadas también pueden modificar su comportamiento para evadir la detección por parte de los sistemas de ciberseguridad de las computadoras. En la mayoría de los casos, los usuarios no son conscientes de que sus dispositivos forman parte de un Botnet y están siendo controlados por ciberdelincuentes (Capuano et al., 2022).

3.6 Ransomware

El ransomware es “un tipo de malware que retiene como rehenes los datos o el dispositivo de la víctima, amenazando con mantenerlo bloqueado a menos que la víctima pague un rescate al atacante” (IBM, 2024).

Según International Business Machines Corporation, el ransomware se clasifica en dos tipos principales: el cifrado, que encripta los datos de la víctima y solicita un rescate, y el de bloqueo de pantalla, que bloquea el acceso al dispositivo exigiendo un rescate. Estas categorías incluyen subtipos como el leakware/doxware, que roba y amenaza con divulgar datos, el ransomware móvil que afecta a dispositivos móviles y el scareware que intenta asustar a los usuarios para pagar. También hay ransomware destructivo que amenaza con destruir datos incluso si se paga el rescate.

Según un informe de ENISA sobre el ransomware, este método se ha convertido en una herramienta popular utilizada por actores maliciosos con el objetivo de causar daño a gobiernos, empresas e individuos de manera frecuente. En tales situaciones, las víctimas de ransomware pueden enfrentar pérdidas económicas significativas, ya sea al pagar el rescate exigido o al costear la recuperación de los datos afectados en caso de no cumplir con las demandas de los atacantes. Además, se señala que en la mayoría de los países, la lucha contra el ransomware enfrenta desafíos importantes, como la falta de coordinación y colaboración entre agencias y autoridades, así como la ausencia de legislación específica que penalice claramente este tipo de ataques (ENISA, 2020a).

4. Ciberseguridad

La Ciberseguridad es “el proceso de defensa de los sistemas de Tecnologías de la Información y las Comunicaciones contra una variedad de amenazas en línea” (Capuano et al., 2022). Además, “por medio de la ciberseguridad cualquier organización intenta proteger sus sistemas que se encuentran interconectados y expuestos a Internet de diversas ciberamenazas” (Alazab et al., 2022). Como bien señala Alazab, tanto personas particulares como empresas adoptan esta medida para resguardar sus centros de datos y otros servidores contra accesos no permitidos, ya que los ataques cibernéticos son una amenaza constante para las empresas y los delitos relacionados con la ciberseguridad aumentan cada año

Estas amenazas, denominadas "ataques cibernéticos", engloban actividades delictivas que buscan aprovechar vulnerabilidades en sistemas, redes o infraestructuras de información electrónica, con el fin primordial de sustraer, modificar o eliminar datos. En un contexto marcado por el aumento de estos ataques, es común hallar estrategias de intrusión que se aprovechan de la falta de preparación tanto de los sistemas como de los usuarios, con el propósito de acceder a información confidencial o comprometer la integridad de los sistemas. Dos desafíos principales en el ámbito de la ciberseguridad son entender las distintas modalidades de ciberataques y desarrollar mecanismos de protección adicionales para contrarrestarlos.

5. Inteligencia Artificial en Ciberseguridad

Existen diversos enfoques para implementar la IA en la detección de los fraudes digitales. Según Jurgovsky, los sistemas utilizados con frecuencia en el área de la ciberseguridad que buscan detectar el fraude digital se pueden dividir entre las herramientas automáticas, que se basan en reglas de detección de fraude analizando todas las nuevas transacciones entrantes y asigna una puntuación fraudulenta. Y, el proceso manual que realizan investigadores de fraude, centrándose en transacciones con una alta puntuación fraudulenta y proporcionan información binaria sobre todas las transacciones que analizaron. (Jurgovsky et al., 2018).

A través de las tecnologías que se basan en los algoritmos de la IA, destacan el aprendizaje automático y el aprendizaje profundo, los cuales han tenido eficacia para detectar amenazas desconocidas en la red, siendo un aporte significativo para la ciberseguridad.

5.1 Aprendizaje automático (ML)

El aprendizaje automático (ML) es “un subconjunto de la Inteligencia Artificial, que se centra en la implementación de algunos sistemas que pueden aprender de los datos históricos, identificar patrones y tomar decisiones lógicas con poca o ninguna intervención humana” (Wazid et al., 2022a). Es un procedimiento mediante el cual los sistemas informáticos adquieren conocimientos a partir de datos y emplean algoritmos para llevar a cabo tareas sin necesidad de ser programados de manera explícita.

Según Kotsiopoulos, las técnicas de aprendizaje automático tienen un papel crucial en diversas áreas de la ciberseguridad, especialmente en la detección y predicción de ataques. En el ámbito financiero, por ejemplo, el aumento del fraude bancario móvil ha generado pérdidas significativas. Además, señala que implementar modelos de aprendizaje automático para identificar anomalías en el comportamiento de los usuarios, como ubicaciones de inicio de sesión inusuales o transferencias de dinero sospechosas, podría ser una medida eficaz para mitigar este problema y proporcionar análisis detallados sobre la detección de anomalías en aplicaciones bancarias móviles y electrónicas (Kotsiopoulos et al., 2021).

El uso de Machine Learning en el campo de la ciberseguridad ha revolucionado la capacidad para prever y detectar amenazas de manera más efectiva que los métodos tradicionales o incluso que los sistemas basados en software avanzado, pero sin inteligencia artificial.

Además, estos modelos pueden adaptarse y mejorar continuamente a medida que se enfrentan a nuevas amenazas y patrones de comportamiento, lo que los convierte en una herramienta invaluable para proteger sistemas y redes contra ataques cibernéticos. Su capacidad para aprender de manera autónoma y su agilidad en la detección de anomalías hacen que el Machine Learning sea fundamental en la defensa contra las constantes evoluciones en el panorama de la ciberseguridad.

5.2 Aprendizaje profundo (DL)

El aprendizaje profundo (DL) es “un subcampo del ML y utiliza datos para enseñar a las computadoras cómo hacer cosas que solo los humanos son capaces de hacer en ese momento” (Truong et al., 2020). Según Wazid el aprendizaje profundo se fundamenta en un complejo conjunto de algoritmos inspirados en el funcionamiento del cerebro humano, lo que le otorga la capacidad de analizar y procesar datos no estructurados, tales como documentos, imágenes y texto. (Wazid et al., 2022b)

Según los autores, el núcleo del aprendizaje profundo es que al construir redes neuronales más extensas y entrenarlas con la mayor cantidad de datos, su rendimiento aumentará (Truong et al., 2020).

También señalan que la diferencia y ventaja más importante entre el aprendizaje automático y el aprendizaje profundo, es el gran rendimiento que tiene en grandes conjuntos de datos. La ventaja más importante de DL sobre el ML convencional es su rendimiento superior en grandes conjuntos de datos.

Por último, apuntan a que los algoritmos DL típicos que se utilizan con frecuencia en el ámbito de la ciberseguridad son las redes neuronales de retroalimentación, redes neuronales convolucionales, redes neuronales recurrentes, redes de creencias profundas, codificadores automáticos apilados, redes generativas adversarias, máquinas Boltzmann restringidas y conjunto de redes de aprendizaje profundo.

6. Medidas tomadas en Chile

Chile se incorporó, tras la aprobación por parte del Congreso Nacional el 16 de noviembre de 2016, al acuerdo internacional de uso más extendido para desarrollar la legislación de combate al cibercrimen, el cual está bajo el Convenio sobre la Ciberdelincuencia del Consejo

de Europa “Convenio de Budapest”. El cual se encuentra ratificado por 60 Estados, incluidos los Estados miembros de la Unión Europea, junto a Estados Unidos, Canadá, Australia y Japón (Achavar & Cárdenas, s. f.).

En relación a la legislación chilena, a partir del 2022 rige la Ley N°21.459, la cual adecua la legislación chilena al convenio Budapest, establece las normas sobre delitos informáticos y considera como tipos penales los ataques a la integridad de un sistema informático, el acceso ilícito, la interceptación ilícita, el ataque a la integridad de los datos informáticos, la falsificación informática, la receptación de datos informáticos, el fraude Informático y el abuso de los dispositivos (Nacional, 2022).

También, frente a este escenario versátil y progresivo de los ciberdelitos, la Policía de Investigaciones crea en marzo del año 2022, la Jefatura Nacional de Ciberdelitos (Jenaciber), de la cual dependen las Brigadas Investigadoras del Ciberdelitos Metropolitana, Valparaíso y Concepción; además del Departamento Forense Digital. Con el propósito de “responder a los desafíos que plantean las nuevas formas de delincuencia asociadas a la evolución de las tecnologías, generando las condiciones para incrementar la efectividad en la investigación criminal por parte de las unidades dependientes”(Ciberdelitos, s. f.). Con ello, se busca reforzar la acción contra los crímenes cibernéticos, teniendo en cuenta su crecimiento acelerado y ciertas particularidades, como su nivel de complejidad y la seriedad de sus repercusiones.

Además, este año se promulgó la Ley Marco Ciberseguridad, ley 21663, la cual, tal como se menciona en el artículo 1:

“La presente ley tiene por objeto establecer la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y entre éstos y los particulares; establecer los requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad; establecer las atribuciones y obligaciones de los organismos del Estado, así como los deberes de las instituciones determinadas en el artículo 4°, y los mecanismos de control, supervisión y de responsabilidad ante infracciones” (Nacional, 2024)

Las instituciones establecidas estarán obligadas por la ley 21663 a aplicar de manera permanente las medidas para prevenir, reportar y resolver incidentes de ciberseguridad.

A pesar de que se han logrado importantes avances en el marco legal, lo que también implica responsabilidades, tales como estar preparados para enfrentar ciberataques cada vez más sofisticados, sin duda aún existen muchos desafíos pendientes en la legislación en ciberseguridad en Chile.

7. Perspectivas y percepción

Según el primer Informe sobre las tendencias de la delincuencia de la Interpol, los delitos financieros y los delitos cometidos por internet son considerados como las principales preocupaciones para la policía en todo el mundo. Se espera que estos delitos aumenten en el futuro, lo que provoca una creciente preocupación por la ciberseguridad y la protección de los sistemas financieros en todo el mundo (Interpol, 2022).

Asimismo, el estudio comparativo de capacidades de seguridad de 2018 de Cisco, concluye que el 39 % de las organizaciones dependen completamente de la automatización para detectar amenazas cibernéticas, mientras que el 34 % depende completamente del aprendizaje automático y el 32 % depende completamente de la IA (CISCO, 2018). Lo que conlleva que cada vez más organizaciones confían en la automatización, el aprendizaje automático y la inteligencia artificial para automatizar la detección de amenazas.

Según Juan Carlos Zevallos, Líder de IBM Security Software para América Latina, con los ataques generados con IA, las empresas se ven presionadas hacia un nuevo panorama en el que la seguridad impulsada por IA puede elevar las defensas y la productividad a nivel humano, programático y tecnológico.

Por otro lado, el Informe anual oficial sobre delitos cibernéticos de 2019 de Cybersecurity Ventures, menciona que el ciberdelito es la mayor amenaza para todas las empresas del mundo y uno de los mayores problemas de la humanidad. Además señala que “los costos de los delitos cibernéticos incluyen daños y destrucción de datos, dinero robado, pérdida de productividad, robo de propiedad intelectual, robo de datos personales y financieros, interrupción del curso normal de los negocios después del ataque, daño a la reputación y más” (Cybersecurity Ventures, 2019).

Propuestas

Debido a la investigación realizada, se plantean las siguientes propuestas:

1. La capacidad de la IA para analizar grandes volúmenes de datos de manera rápida y precisa, identificando patrones y anomalías que podrían indicar actividades fraudulentas junto con la implementación de algoritmos de aprendizaje automático y profundo pueden mejorar la capacidad de las organizaciones para anticipar y responder a nuevas formas de fraude digital.

Por ello se propone que la implementación de tecnologías de IA en la detección y prevención de fraudes digitales puede reducir significativamente las pérdidas económicas y la vulnerabilidad de las organizaciones ante estos ataques.

2. Tras la evolución constante de las tecnologías, la inteligencia artificial se ha posicionado como una herramienta crucial para detectar y prevenir fraudes digitales, pero, a pesar de sus avances, el personal organizativo puede limitarse por la efectividad de las tecnologías.

Por lo tanto, se propone que, a pesar de las avanzadas soluciones de inteligencia artificial contra los fraudes digitales, el conocimiento y la ética profesional del personal son un factor determinante en la eficacia de las estrategias preventivas, ya que los empleados pueden potenciar significativamente las capacidades de la inteligencia artificial para proteger los activos de las empresas frente a los fraudes digitales.

3. Si bien la inteligencia artificial ha permitido detectar fraudes digitales, también ha sido utilizada para efectuar los fraudes con mayores herramientas y automatización, aumentando el riesgo de fraude para las organizaciones como los bancos y dificultando las medidas preventivas que hayan tomado.

Por ende, se propone que la inteligencia artificial permitirá fortalecer y aumentar las técnicas para emplear fraudes, lo que provocará que las medidas tomadas por organizaciones financieras estén más endeble y enfrenten pérdidas significativas.

4. Es importante contar con la capacidad para monitorear y mitigar los impactos de los ciberataques a nivel institucional y de industria, además los directores son conscientes de estos riesgos y están definiendo estrategias para enfrentarlos y mitigarlos. Esto luego de sufrir pérdidas por robos realizados con el método de phishing.

Debido a esto, se plantea que las empresas que han experimentado pérdidas financieras debido a fraudes digitales con IA tienen una percepción más crítica sobre la necesidad e importancia de inversiones adicionales en tecnologías de ciberseguridad, ya que comprenden que la implementación de métodos basados en inteligencia artificial es fundamental para protegerse eficazmente contra estos delitos cibernéticos.

Metodología

La investigación se enfoca en una metodología con enfoque cualitativo, con el fin de conocer los principales métodos utilizados para realizar fraudes digitales con IA y el impacto que provocan en las empresas, asimismo, conocer el uso de la inteligencia artificial para detectar y prevenir los fraudes digitales. Además, conocer las medidas tomadas en Chile respecto a los fraudes digitales y la percepción y expectativas de la IA y ciberseguridad en las empresas.

Como se menciona en el artículo “La metodología en la investigación cualitativa”:

“La investigación cualitativa se puede definir como la conjunción de ciertas técnicas de recolección, modelos analíticos normalmente inductivos y teorías que privilegian el significado de los actores, el investigador se involucra personalmente en el proceso de acopio, por ende, es parte del instrumento de recolección. Su objetivo no es definir la distribución de variables, sino establecer las relaciones y los significados de su objeto de estudio.” (Sanchez, 2005)

Con el fin de cumplir los objetivos propuestos, se basa la investigación cualitativa en una entrevista semiestructurada, en la cual el investigador planifica la entrevista con antelación, creando un guion que define la información temática que desea obtener. Las preguntas formuladas son abiertas, permitiendo al entrevistado añadir matices a sus respuestas, lo que enriquece la información proporcionada.

1. Entrevista

Los entrevistados serán profesionales que trabajen en el ámbito de la ciberseguridad y IA de las empresas. Para conocer sobre el uso de las herramientas de la Inteligencia artificial para efectuar los fraudes digitales y para prevenirlos, se plantean las siguientes preguntas:

En relación con la inteligencia artificial se plantean las preguntas:

1. ¿Cuál es la confiabilidad y seguridad de los procesos que utilizan IA?
2. ¿Cómo cree que la IA puede contribuir en el avance del campo de la ciberseguridad?
3. ¿Conoce algún avance que haya tenido la IA para la detección de fraudes digitales?
4. ¿Recomendaría el uso de la IA para prevenir y detectar los fraudes digitales?
5. ¿Cuál es su opinión sobre la capacidad de adaptación de las tecnologías de IA ante la evolución constante de los métodos de fraude digital?

En relación con la ciberseguridad se plantean las preguntas:

1. ¿Cuáles han sido los fraudes digitales que han aumentado en el último tiempo?
1. ¿Cómo las organizaciones pueden responder de manera efectiva ante estos ataques?
2. ¿Cuál ha sido la industria que se ha visto más afectada por los fraudes?
3. ¿Qué herramienta se está utilizando como medida de prevención y detección?
4. ¿Qué tan importante es el uso de la IA como medida preventiva?
5. ¿Qué rol que ha tomado la IA en la detección de fraudes digitales y cómo ha ido evolucionando con el tiempo?
6. ¿Podría darme ejemplos de cómo se utilizan las tecnologías de la IA para prevenir los fraudes digitales?
7. A parte del uso de la IA, ¿Qué otras medidas deberían utilizarse para prevenir los fraudes?
8. Por otro lado, ¿Cómo cree que la IA está siendo utilizada actualmente para fortalecer los métodos de fraudes digitales?
9. ¿Cuál es su visión sobre el futuro de la ciberseguridad en un contexto donde tanto los defensores como los perpetradores de los fraudes digitales están utilizando tecnologías de IA cada vez más avanzadas?
10. ¿Qué recomendaciones daría a las organizaciones que están considerando adoptar soluciones de IA para mejorar su postura de seguridad contra los fraudes digitales?

11. ¿Qué recomendaciones daría a organizaciones que han sufrido algún tipo de fraude?

Resultados

Se realizaron 9 entrevistas, cada una enfocada al uso de la IA y ciberseguridad, a continuación, se presentan los perfiles de los entrevistados y un resumen de la entrevista:

1. Michael Heavey

La entrevista número 1, fue realizada a Michael Heavey el cual es coordinador de la mesa de ciberseguridad de la comisión desafíos del futuro del senado de Chile, además de ser asesor del senador Kenneth Pugh, quien ha sido uno de los que ha traído los temas de ciberseguridad y tecnología al senado.

La entrevista se basó en los temas de ciberseguridad tanto a nivel nacional como de empresas, además de ver las herramientas y medidas utilizadas para ciberseguridad como la inteligencia artificial y otros factores humanos.

En primera instancia, Michael menciona que recientemente se aprobó la Ley Marco Ciberseguridad, que establece y fija reglas y normativas que serán aplicadas a distintas instituciones, además se crea la Agencia Nacional de la Ciberseguridad.

En relación con la IA, indica que, así como se utiliza para detectar vulnerabilidades, también se utiliza para descubrir las propias vulnerabilidades y tomar medidas para prevenir los ataques. Pero también existe un gran déficit dentro de las empresas respecto a la conciencia de la ciberseguridad, menciona y destaca que uno de los mayores desafíos en la actualidad, es capacitar al personal dentro de la organización, porque la mayoría de los ataques ocurren por las personas. Enfatiza que el factor humano es primordial para la ciberseguridad y que hace falta que las personas tengan ciberhigiene, concepto que Michael define como “las normas y prácticas para manejarse frente a un computador”.

Y, por último, señala que “hay dos tipos de empresas en el mercado, las que saben que la hackearon y las que no saben que las hackearon”, por ende, indica que hay que tomar medidas para disminuir el riesgo y los efectos, asimismo, vuelve a recalcar la importancia del factor humano dentro de las organizaciones.

2. Rolando Martínez

La entrevista número 2, fue realizada a Rolando Martínez, el cual empezó en el área de ciberseguridad como director de tecnología de varias empresas y servicios públicos, entre ellas el Registro Civil, además de los trabajos que ha realizado como gerente de ciberseguridad en una empresa que vende soluciones, certificación digital y servicios de ciberseguridad, también se ha desempeñado en el área de inteligencia artificial y fue director ejecutivo del Centro Nacional de Inteligencia Artificial (CENIA) desde el 2021 hasta el 2023. Debido a su trayectoria profesional, se encuentra al tanto de lo que ocurre respecto a la ciberseguridad y la inteligencia artificial.

En la entrevista se destacan la relación que existe entre la ciberseguridad y la IA, además, comenta una experiencia de intento de fraude digital que sufrió a través del método de Business Email Compromise (BEC) en el cual trataron de hacerse pasar por su cargo de director con el fin de que el gerente de administración y finanzas hiciera una transferencia supuestamente ordenada por él. Por otra parte, menciona los métodos para evitar los fraudes, como lo son eliminar el uso de passwords, mantener sistemas más robustos de autenticación y también trabajar con el factor humano, con el fin de disminuir el riesgo lo más posible.

También, según Rolando, el panorama de la ciberseguridad está cambiando, ya que hay bandas más especializadas y organizadas, las cuales buscan las vulnerabilidades y luego las utilizan para venderlas en mercados negros por un beneficio económico no menor. Incluso, menciona que la IA ha ayudado a realizar estos ataques por medio de hacerse pasar por la persona con la misma voz que tiene, lo cual lo hace más creíble, a pesar de que este método no se ha visto tanto, sin duda logra que los daños sean mayores.

Además, la entrevista destaca que dentro de las empresas se está tomando más importancia y se están preocupando por la ciberseguridad, luego de la Ley Marco Ciberseguridad que se promulgó, se refleja que están comenzando a informarse más sobre lo que respecta la ciberseguridad y los ataques. Sin embargo, también señala que existe un gran déficit de especialistas en esta área, por lo cual las empresas más grandes tienen mayores posibilidades para poder contratar al personal correspondiente y capacitarlos.

Asimismo, en base a su experiencia, señala que en general hay organizaciones que están bien preparadas para el fraude y otras que piensan que no les va a ocurrir y por ende no se preparan. Sin embargo, indica que esto no es un tema de que no les va a ocurrir, sino que cuándo les va a tocar, por lo mismo, recalca que la educación en ciberseguridad debe ser permanente y generar niveles de preparación efectivos para proteger los activos digitales.

3. Carlos Villagra

La entrevista número 3 fue realizada a Carlos Villagra, el cual lleva trabajando en el área de seguridad de la información de ciberseguridad cerca de 20 años, en los cuales ha tenido diversos roles, como en tecnología, soporte, consultoría, marco regulatorio e incluso Chief Information Security Officer (CISO). Por otra parte, también se destaca por ser docente de posgrado de magister de ciberseguridad en la Adolfo Ibáñez y en la Universidad de UNIAC.

Durante la entrevista, destaca el tema de la ciberseguridad dentro de las empresas, en el cual hoy en día se ha visto una evolución en este ámbito de ciberseguridad, tanto a nivel de gobierno, a nivel nacional existe un marco regulatorio, políticas, ley de ciberseguridad, entre otros como la Agencia Nacional de Ciberseguridad. Dentro de las empresas, menciona que hoy en día la ciberseguridad es un proceso más de la compañía y no tanto de tecnología de la información como era en el pasado, además, de evidenciar un cambio en las inversiones, presupuestos, personas y conocimientos dentro de la empresa.

En este mismo ámbito, el entrevistado menciona que la IA aplicada hoy en día como herramienta se puede utilizar tanto para defender como para atacar, pero menciona que hay cosas que la IA nunca va a suplir, lo cual es la dirección que lleva el director de ciberseguridad, ya que la IA es solo una herramienta que puede beneficiar, pero la persona es quien maneja la dirección que quiere tomar. Asimismo, uno de los mayores desafíos de la IA que menciona, es el factor humano, ya que trabajar con las personas es primordial para cumplir con los objetivos de ciberseguridad.

En el mismo contexto, menciona que los métodos para perpetrar un fraude por una vulnerabilidad de un sistema son las plataformas de comunicación humana, como el correo, el phishing, spam, en el cual se suplanta la identidad y a partir de ello se genera el fraude.

Al finalizar la entrevista, señala que existen dos tipos de empresas, las que saben que les pasó y las que no saben que les pasó, por ende, hay que tener en claro el nivel de madurez y estado de la ciberseguridad, ya que si no se evalúa o mide no se puede saber si está siendo atacada o no.

4. N.N

La entrevista número 4, fue realizada a un experto del área de inteligencia artificial, el cual prefirió mantener su identidad de forma anónima, sin embargo, la entrevista abarcó principalmente el uso y aplicación de la inteligencia artificial dentro de una empresa.

El entrevistado señala los beneficios de implementar procesos con la IA dentro de la empresa, destacando la reducción de tiempos de respuestas y una mejora en la seguridad, además de la implementación de varias medidas para asegurar la operativa continua y proteger los datos.

Asimismo, menciona diversos ejemplos de cómo se aplica la IA y cuales medidas hay que tomar para mantener la seguridad de los datos, destacando la importancia de realizar pruebas piloto y mantener contratos de confidencialidad con los proveedores y todo el personal de la organización, con el fin de proteger la información y datos de forma segura y con menor riesgo de ser vulnerados.

Por último, destaca la importancia del error humano, ya que, al utilizar las herramientas de IA, hay que tener una visión flexible, aceptar la posibilidad de equivocarse y ser capaces de adaptarse y seguir adelante.

5. Xavier Bonnaire

La entrevista número 5, fue realizada a Xavier Bonnaire, el cuál comenzó su trayectoria en Francia a cargo de todo lo que era el aspecto de seguridad del departamento de informática, y en Chile comenzó a desarrollar el conocimiento y capacidades en el tema de ciberseguridad, ha realizado diversas publicaciones sobre esta materia, y hoy en día se encuentra a cargo de la línea de seguridad del departamento de informática de la Universidad Técnica Federico Santa María (UTFSM), desempeñándose como docente en los cursos que se dictan sobre ciberseguridad o relacionado con ello y tiene el rol de director académico del diplomado en ciberseguridad de la UTFSM.

La entrevista abordó la trayectoria Xavier Bonnaire en ciberseguridad, los desafíos y oportunidades de la inteligencia artificial en este campo, y la importancia de mejorar la conciencia y educación sobre ciberseguridad en Chile. Se discutieron los riesgos de los ciberataques para empresas y organizaciones, así como las medidas básicas de seguridad y la creciente demanda de profesionales en el área.

En relación con cómo la inteligencia artificial se relaciona con la ciberseguridad, el entrevistado destacó que la IA puede ser beneficiosa para detectar y responder rápidamente a ataques cibernéticos, pero también puede ser utilizada por ciberdelincuentes para generar ataques automáticamente. Además, anticipó que en un futuro cercano podríamos ver una "batalla" entre sistemas de IA que generan ataques y los que defienden infraestructuras.

En base a su experiencia, señala que los desafíos de la inteligencia artificial se encuentra la dificultad de hacer predicciones y la posibilidad de una carrera entre el uso defensivo y ofensivo de la IA. También expresó preocupaciones sobre la calidad de los datos de entrenamiento, destacando que la IA podría producir respuestas erróneas si se entrena con información no confiable. Si bien, no existe una solución clara, enfatizó la importancia de controlar la calidad de los datos de entrenamiento.

Asimismo, destacó que el mayor reto no era técnico, sino la falta de conciencia general sobre los problemas de ciberseguridad, tanto a nivel personal como empresarial. Xavier indica que muchas empresas, especialmente las PYMES, no consideran la ciberseguridad como una prioridad, viéndola como un gasto en lugar de una inversión. También señaló que un ataque exitoso podría resultar más costoso que la inversión inicial en seguridad, afectando no solo las finanzas, sino también la imagen y el tiempo operativo de la empresa.

Por otra parte, se destaca la importancia de mejorar la conciencia y la educación sobre ciberseguridad en Chile, ya que existen efectos devastadores de los ataques, como el ransomware, por ende, nace la necesidad de tener respaldos en su lugar. También menciona la reciente legislación que mejoró la ciberseguridad y la creación de nuevas agencias nacionales de seguridad. Pero existe la necesidad de capacitar a los empleados sobre las mejores prácticas para poder tener una efectividad de las medidas tomadas.

Además, en la entrevista menciona casos específicos de sistemas financieros en los que las empresas se recuperaron después de ataques. Destacó que los ciberdelincuentes están moviéndose hacia empresas más pequeñas y menos protegidas, y que estos ataques están causando pérdidas financieras significativas. También mencionó el concepto de "ingeniería social", donde los atacantes crean estrés en las empresas mediante facturas impagadas o amenazas de interrumpir el servicio.

Finalmente, se menciona la importancia de la seguridad informática, enfatizando que la pregunta no es si ocurrirá un ataque exitoso, sino cuándo. Recomendó implementar medidas básicas como mantener el software actualizado, usar contraseñas complejas y autenticación de doble factor, instalar antivirus y capacitar al personal. También destacó que estas medidas, aunque no son 100% efectivas, pueden prevenir hasta el 95% de los ataques potenciales. Y, por último, señaló que la mayoría de las fallas de seguridad se deben a errores humanos, por lo que la educación y capacitación del personal son cruciales para mejorar la seguridad general.

6. Romina Garrido

La entrevista número 6 se realizó a Romina Garrido, abogada especialista en Protección de Datos Personales, además de trabajar en temas de inteligencia artificial en la Universidad Adolfo Ibáñez.

La entrevista aborda la relación entre la inteligencia artificial (IA) y la ciberseguridad, destacando cómo ambas disciplinas se complementan y enfrentan desafíos comunes. Romina, define la ciberseguridad como el conjunto de prácticas destinadas a proteger los activos de información en el ámbito digital, garantizando su integridad, confidencialidad y disponibilidad. Por otro lado, menciona que la inteligencia artificial es una tecnología que emula ciertas capacidades humanas, como el análisis y la toma de decisiones, utilizando datos como su principal insumo. En este contexto, la ciberseguridad juega un papel clave al asegurar que los datos utilizados por la IA sean confiables y estén protegidos contra alteraciones que puedan comprometer la calidad de los resultados producidos por los sistemas inteligentes.

Además, dentro de la entrevista, se destaca que la IA se ha convertido en una herramienta esencial para fortalecer la ciberseguridad en las empresas. Gracias a su capacidad para automatizar procesos repetitivos, la IA permite monitorear grandes cantidades de datos en tiempo real, identificando posibles ciberataques de manera más eficiente que los equipos humanos. Esto resulta especialmente valioso en organizaciones con recursos limitados, donde el personal de ciberseguridad no puede abarcar la totalidad de los sistemas. Sin embargo, también se reconoce que la IA puede ser utilizada con fines maliciosos, como el desarrollo de sistemas para suplantar identidades, descubrir contraseñas o realizar fraudes, lo que plantea desafíos éticos y de seguridad.

La conversación también resalta los mayores desafíos que enfrenta la ciberseguridad en las empresas hoy en día. Entre estos se incluyen la falta de presupuesto, la retención de talento especializado y la necesidad de concientizar a los directorios sobre la importancia estratégica de la ciberseguridad. Aunque existen herramientas tecnológicas avanzadas, su implementación muchas veces se ve limitada por la falta de recursos o formación del personal. Además, se subraya que la ciberseguridad debe ser entendida como una responsabilidad colectiva dentro de las organizaciones, ya que incluso los sistemas más robustos pueden ser vulnerados por errores humanos, como el manejo inadecuado de correos o archivos sospechosos.

Finalmente, se enfatiza la importancia de adoptar medidas preventivas antes de sufrir un ciberataque. Se menciona que con la entrada en vigor de la ley marco de ciberseguridad en Chile, las empresas estarán sujetas a sanciones si no cumplen con ciertos estándares mínimos. Más allá de las obligaciones legales, la ciberseguridad es esencial para proteger la reputación de las organizaciones y mantener la confianza de clientes y trabajadores. La formación y concientización en estos temas son presentadas como pilares fundamentales para enfrentar los desafíos actuales y futuros en el ámbito de la seguridad digital.

7. Giovanna Lanzarini

La entrevista número 7 corresponde a Giovanna Lanzarini, la cual realizó un diplomado en ciberseguridad y actualmente trabaja como Analista de Ciberseguridad dentro de una empresa de gran tamaño.

La entrevista se centró en las medidas de seguridad cibernética y la prevención de fraudes, destacando cómo las organizaciones manejan los riesgos digitales. Giovanna explicó que se utilizan varias herramientas para detectar comportamientos inusuales, como la descarga de programas no autorizados o la identificación de comportamientos extraños en computadoras mediante un antivirus que alerta cuando detecta procesos no habituales. Estos sistemas buscan bloquear actividades sospechosas antes de que puedan causar daños, lo que forma parte de las alertas internas y del monitoreo continuo que se lleva a cabo dentro de la empresa. Además, menciona que se utilizan herramientas especializadas para el análisis de correos electrónicos, en los que se detectan enlaces sospechosos o remitentes no confiables. A pesar de contar con estas tecnologías avanzadas, destacó que la intervención humana sigue siendo crucial, ya que los atacantes mejoran constantemente sus técnicas, haciendo que la capacidad de detección de los sistemas automatizados también deba evolucionar.

Además de las herramientas de detección, Giovanna explicó que se realiza un seguimiento de los sistemas informáticos, como servidores y computadoras de los usuarios, para asegurarse de que se mantengan actualizados. La obsolescencia de ciertos sistemas operativos puede representar una vulnerabilidad importante, ya que estos ya no reciben soporte de seguridad, lo que facilita que los atacantes exploten fallos de seguridad sin parches. Giovanna subrayó que este tipo de vulnerabilidades es monitoreado de cerca, y se realiza un análisis exhaustivo de los servidores y bases de datos para identificar cualquier anomalía en su funcionamiento que pueda ser indicativa de un ataque.

En cuanto al uso de inteligencia artificial, señala que, aunque la IA también se utiliza para detectar patrones sospechosos y prevenir fraudes, los delincuentes también están empleando IA para lanzar ataques más sofisticados y rápidos. Esto implica que la empresa debe mantenerse al día con las últimas tecnologías para protegerse, utilizando IA tanto para la prevención como para contrarrestar los métodos avanzados de los atacantes.

En términos de concientización y educación, en la entrevista se destaca la importancia de programas internos para sensibilizar a los empleados sobre los riesgos de ciberseguridad, implementando iniciativas como cursos, webinars, y campañas de simulación de phishing, en las que se evalúa la capacidad de los empleados para detectar fraudes. Este tipo de

capacitación se realiza de manera continua para garantizar que los empleados estén al tanto de las últimas amenazas y sepan cómo actuar ante ellas.

Por otro lado, menciona que la ingeniería social es una de las técnicas más utilizadas por los atacantes, quienes manipulan a las personas para obtener acceso a información confidencial. Sin embargo, los fraudes no solo ocurren a través de correos electrónicos, sino también mediante la recopilación de información en redes sociales y otras plataformas, lo que permite a los atacantes personalizar sus engaños y aumentar la probabilidad de éxito. Por lo tanto, el entrenamiento sobre cómo detectar estas técnicas se ha convertido en un aspecto esencial de la estrategia de ciberseguridad de la empresa.

Finalmente, Giovanna reflexionó sobre los desafíos futuros en el campo de la ciberseguridad. A pesar de los avances tecnológicos, la concientización del personal sigue siendo una de las mayores barreras, ya que el factor humano es el eslabón más débil en la cadena de seguridad. La educación constante es necesaria para mantener a los empleados informados y preparados para enfrentar nuevas amenazas. Por ello, a medida que los atacantes se vuelven más sofisticados, las empresas deben evolucionar junto con ellos, invirtiendo en nuevas tecnologías y entrenando continuamente a su personal para enfrentar los desafíos que surjan. La clave será mantenerse actualizados y preparados ante los cambios rápidos que caracterizan el mundo de la ciberseguridad.

8. Sebastián Berríos

La entrevista número 8 se realizó a Sebastián Berríos, ingeniero civil informático que lleva una gran trayectoria dentro de la Universidad Católica de Valparaíso, es el encargado de infraestructura, tecnología y seguridad. Durante su vida profesional, ha realizado varios diplomados en el área de ciberseguridad y actualmente se encuentra realizando clases de docencia universitaria para diplomados sobre esta materia. Por otra parte, también trabaja como consultor del área de ciberseguridad realizando computación forense, entre otras actividades.

La entrevista abordó los principales desafíos y tendencias en ciberseguridad empresarial, destacando el papel crucial que desempeña la inteligencia artificial (IA) tanto en la defensa como en los ataques cibernéticos. Según el entrevistado, en Chile se han registrado avances

significativos gracias a la implementación de leyes orientadas a proteger la infraestructura crítica. Sin embargo, aún existen importantes brechas en muchas organizaciones, debido a la falta de herramientas tecnológicas avanzadas, políticas robustas y personal debidamente capacitado. “La tecnología avanza rápidamente, pero el factor humano sigue siendo el eslabón más débil en la cadena de ciberseguridad”, menciona Sebastián, resaltando la necesidad de fomentar una cultura de prevención y capacitación constante en todos los niveles organizacionales.

Durante la entrevista, se identificaron los fraudes digitales más comunes, entre los que destacan el phishing y el ransomware. Estas modalidades de ataque no solo generan pérdidas económicas significativas, sino que también afectan de manera crítica la reputación de las empresas involucradas. “Un incidente de phishing puede comprometer la confianza de los clientes en cuestión de minutos”, agregó el experto, enfatizando la importancia de educar a los colaboradores para reconocer y manejar amenazas de este tipo.

Asimismo, se abordó cómo la IA se utiliza para crear estrategias de ataque más sofisticadas, lo que representa un desafío para las organizaciones que aún no cuentan con soluciones tecnológicas avanzadas. Por otro lado, también se destacó el potencial de la IA como una herramienta clave para detectar patrones de comportamiento inusual, automatizar respuestas y reforzar la seguridad en tiempo real. Según Sebastián, “la inteligencia artificial es una espada de doble filo; si bien puede ayudarnos a prevenir incidentes, también está en manos de los atacantes, quienes cada día desarrollan métodos más complejos”.

En cuanto a las recomendaciones, el entrevistado subrayó la necesidad de implementar mecanismos como la autenticación multifactorial, la elaboración de planes de respuesta ante incidentes y el uso de tecnologías avanzadas para la gestión de riesgos. También señaló que las empresas deben invertir en ciberseguridad no solo como una necesidad técnica, sino como una estrategia integral que garantice la resiliencia organizacional. “Invertir en ciberseguridad no es un gasto, es una inversión a largo plazo que protege tanto los activos como la reputación de la empresa”, afirmó.

Por último, la entrevista concluyó con una reflexión sobre el panorama futuro de la ciberseguridad, destacando que, aunque las amenazas continuarán evolucionando, la colaboración entre empresas, expertos y organismos gubernamentales será clave para

fortalecer las defensas digitales. “La ciberseguridad no es solo una responsabilidad tecnológica; es un compromiso colectivo que requiere esfuerzo y coordinación” menciona al finalizar la entrevista.

9. Francisco Villalobos

La última entrevista fue realizada a Francisco Villalobos, ingeniero civil electrónico colaborador de la Universidad Católica de Valparaíso, trabajando principalmente en el área de computadores en telecomunicaciones y hace 5 años que comenzó en el área de ciberseguridad. Con un enfoque en investigaciones en materia de inteligencia artificial y ciberseguridad.

La entrevista se centró en el tema de la ciberseguridad, particularmente en su relación con la inteligencia artificial (IA) y su aplicación en la protección de sistemas críticos como los de control industrial.

Según el entrevistado, uno de los principales enfoques de su investigación está en los sistemas grandes, como aquellos que controlan infraestructuras críticas, que pueden afectar económicamente a una ciudad o país si son atacados. El entrevistado señaló que los ataques a estos sistemas podrían tener consecuencias graves, incluso en términos de pérdidas humanas. "Nosotros estamos más orientados a la investigación dentro de estos sistemas, que son grandes sistemas que podrían, si caen, perjudicar a toda una ciudad o país, cierto en términos económicos y también en pérdidas humanas," menciona.

El trabajo realizado incluye el estudio de diversas técnicas de Machine Learning (ML) para la detección de ataques en sistemas, con el objetivo de evitar la generación de falsos positivos. A través del uso de algoritmos supervisados y no supervisados, así como redes neuronales, se busca identificar rápidamente un ataque para prevenir pérdidas operacionales significativas. "Lo que estamos haciendo es estudiar distintas técnicas de Machine Learning orientadas a detectar ataques y evitar falsos positivos, que al ser detectados tarde pueden generar pérdidas operacionales," explicó el entrevistado. Además, se ha trabajado en el análisis de malware y phishing, y en la implementación de soluciones biométricas para reforzar la seguridad.

Una parte clave de la conversación se centró en cómo la inteligencia artificial puede ser utilizada tanto para la protección contra los ciberataques como para la generación de estos ataques. Aunque el entrevistado y su equipo no han trabajado desde la perspectiva de los atacantes, reconoció que los hackers también están utilizando IA y herramientas automatizadas, como el ransomware inteligente, para atacar a las empresas. "La IA puede ser utilizada en ambos sentidos. Puede ser una herramienta para los atacantes y la están utilizando hoy en día, nosotros no lo hemos hecho en ese sentido," mencionó. A pesar de esto, el enfoque de su investigación sigue siendo desde la defensa, utilizando la IA y el aprendizaje automático para mejorar la seguridad de los sistemas.

En cuanto a experiencias personales con ataques, el entrevistado comentó que no ha sido víctima de un ataque directo, pero ha presenciado incidentes relacionados con ingeniería social, como el envío de correos electrónicos fraudulentos a estudiantes. En esos casos, se recomienda tener precauciones, como leer detenidamente los correos electrónicos, instalar herramientas antimalware, y utilizar métodos de autenticación multifactorial. "El ataque generalmente entra a través de las personas. El factor humano es el problema principal en ciberseguridad," subrayó el entrevistado.

En relación con los desafíos de la ciberseguridad, el entrevistado destacó el factor humano como uno de los mayores problemas. A pesar de tener tecnologías avanzadas, los errores humanos siguen siendo una puerta de entrada común para los atacantes. Por ello, la capacitación y la concientización del personal son fundamentales para mitigar estos riesgos. "Lo esencial es la capacitación al personal, y la concientización. En ese sentido, la inteligencia artificial puede ayudar a formar a las personas en el buen uso de los sistemas de ciberseguridad," explicó. Además, mencionó un proyecto en el que están trabajando que utiliza IA para crear un taller auto-instruccional, similar a un chatbot, para educar al personal sobre ciberseguridad.

El entrevistado también habló sobre el contexto normativo y legal en torno a la ciberseguridad. Señaló que, aunque las leyes y políticas de seguridad cibernética están comenzando a fortalecerse, hay una tensión entre la necesidad de proteger los sistemas y las restricciones legales que enfrentan los profesionales de la seguridad, como los hackers éticos. A medida que la IA se utiliza cada vez más, también surgen preocupaciones sobre su mal

uso. "La IA puede generar beneficios, pero también puede causar inconvenientes. Hemos visto casos de ataques de ransomware, phishing, y otros tipos de fraudes utilizando herramientas de IA," comentó el entrevistado.

Finalmente, el entrevistado ofreció recomendaciones para pequeñas y medianas empresas (PYMES) que no tienen los recursos para implementar tecnologías avanzadas como la inteligencia artificial. Sostuvo que existen buenas prácticas que pueden adoptarse, como la implementación de políticas de seguridad basadas en normas como la ISO 27001. "Una PYME puede aplicar buenas prácticas de ciberseguridad, como la implementación de políticas de seguridad según la ISO 27001, para protegerse. Es importante que, aunque no se cuente con grandes recursos, las empresas sigan ciertos estándares básicos," concluyó el entrevistado.

Análisis

Luego de transcribir las entrevistas, se realizó un análisis utilizando el programa Atlas.ti. Este software permitió codificar la información y luego categorizarlos para identificar patrones y temas recurrentes, destacando los aspectos más relevantes de cada entrevista. A partir de este análisis, se organizó la información en una tabla de análisis que sintetiza la información obtenida y facilita la comparación de las respuestas de los entrevistados, incluyendo la identificación del entrevistado, el objetivo propuesto, el tema o patrones recurrentes, los hallazgos más relevantes derivados de la entrevista y por último las citas textuales de los entrevistados.

A continuación, se presenta un resumen de la tabla, destacando las citas más importantes y objetivos específicos.

Tabla 1: Resumen análisis de las entrevistas

Objetivos	Recurrentes	Hallazgos	Citas
Métodos utilizados para realizar fraudes	Phishing, Ransomware, Ingeniería social, Sistema vulnerable.	Los fraudes comunes incluyen phishing e ingeniería social. Los cuales	"Puedes tener ataques que vienen porque alguien abre mal un archivo que le llega y ese archivo viene contaminado..." "puede ser un phishing " (M. Heavey). "Me han tratado de hacer ciberataque que se trataba de hacer un fraude que se llama Business Email Compromise a mí" (R. Martínez). "¿Cuál es la

		incorporan archivos con links que activan ataques.	plataforma de comunicación tradicional empresarial? El correo, phishing, spam. En donde la gente o suplanta la identidad de alguien o captura el correo de alguien y a partir de eso generan fraude" (C. Villagra). "hay empresas más pequeñas que tuvieron problemas de ataque por algo que se llama la ingeniería social, la ingeniería social es hacerte pasar por otra persona" (X. Bonnaire). "Utilizan la ingeniería social, es una técnica de manipulación a las personas, pueden hacerlo por diferentes medios, como el Phishing, el Spear Phishing que saca un perfil personalizado de la persona desde las redes sociales u otras plataformas, llamadas telefónicas y el SMS también es muy conocido" (G. Lanzarini).
Uso de la IA para realizar fraudes	Uso de la IA para encontrar vulnerabilidades y generar ataques personalizados y sofisticados.	IA para identificar, explotar vulnerabilidades y crear códigos maliciosos, sin la necesidad de tener conocimientos de programación avanzada"	"usan las mismas herramientas de inteligencia artificial u otras que ellos van entrenando y van buscando vulnerabilidades"(M. Heavey). "Yo creo que el nivel más masivo son estos correos... hay mucha gente que cae y que están apuntados como al gran público... En ese nivel de fraude, que es como un micro fraude, la inteligencia artificial ayuda mucho más a la gente que hace el fraude que a la gente que lo detiene."(R. Martínez)."la inteligencia artificial se usa ahora para generar ataques... los ciberdelincuentes también usan ese tipo de capacidad para generar códigos maliciosos automáticamente, para detectar automáticamente algunas fallas que existen, una infraestructura tuya o de hardware o software, etcétera."(X. Bonnaire). "los hackers están utilizando esas herramientas y hay un montón de herramientas que se pueden hacer fácil sin necesariamente tener conocimiento avanzado en programación" (F. Villalobos). "Los ataques están avanzando muy rápido con el uso de la IA, la están usando mucho, por ejemplo, podrían lanzar una campaña de Phishing gigantesca y más personalizada que antes"(G. Lanzarini).

El uso de la IA para prevenir y detectar fraudes	Desarrollo y monitoreo de herramientas de IA en la detección de fraudes.	La IA ayuda en la ciberseguridad para detectar errores de programación y mejorar la defensa contra ataques sofisticados.	"el uso de la IA dentro de la tecnología de ciberseguridad es tremendamente potente...puedes tener soluciones súper rápido"(C. Villagra). "con dos meses de entrenamiento tenías los resultados que en otras ocasiones alcanzarías después de 1 año."(N.N). "la IA va a ir aprendiendo, o sea, tú tienes que desarrollar un sistema e ir entrenándolo para justamente el objetivo que tú quieres... hay todo un tema de desarrollo de liberación del algoritmo para que el algoritmo vaya aprendiendo de la situación que vaya probando y vaya generando y proponiendo soluciones." (M. Heavey). "Los grandes modelos de lenguaje, que son los que hoy día están como más en boca en términos de la inteligencia artificial...son capaces muchas veces de señalar defectos de programación que son inseguros o cosas por el estilo, lo que ayuda a los programadores a no cometer esos errores en el diseño de sus aplicaciones."(R. Martínez). "se transforma también en una herramienta para la ciberseguridad en la medida que permite automatizar procesos repetitivos bajo reglas y que te permiten detectar amenazas que probablemente con 4 o 5 personas que tú tengas en un equipo de ciberseguridad se te podría pasar"(R. Garrido). "La IA que hemos trabajado es principalmente orientado a la parte de sistemas basados en machine learning, para poder reforzar la forma de que, cómo se cuándo se recibe un ataque en un sistema rápidamente, ese ese ataque puede hacer detectado a través de distintos algoritmos supervisados, no supervisado o redes neuronales" (F. Villalobos).
--	--	--	--

Otras medidas para prevenir los fraudes digitales	Factor humano, cultura, capacitación y colaboración	Ciberhigiene dentro de la empresa, capacitación del personal y prácticas de ciberseguridad	"¿qué es lo que es la ciber higiene? Son las normas y prácticas para manejarse frente a un computador" "Gran parte, sino como 80 o 90% de los ciberataques tienen algún factor humano de por medio."(M. Heavey). " hemos estado viendo ahora que han salido tecnologías nuevas que te permiten eliminar por completo el uso de passwords y ocupar dispositivos físicos como autenticación. ...hay que sumar, por supuesto, el factor humano, hay que hacer charlas de concientización, hay que hacer ensayos"(R. Martínez). "las empresas tienen que trabajar, formación, capacitaciones, curso de inducción... el factor humano acá es súper importante la tecnología nunca va a suplir."(C. Villagra). "Entonces, educar, educar, capacitar a la gente en buenas prácticas mínima, eso no significa que te va a salvar del 100% de los ataques con esas esas medidas básicas, pero te va a salvar lo mejor de un 95%, lo que es mucho mejor que nada."(X. Bonnaire). "Hay que entender la ciberseguridad como una tarea de todos los que están en su organización, y no solamente el encargado de ciberseguridad "(R. Garrido). "es fundamental que tengamos claridad, que tenemos que trabajar en la confianza de nuestras empresas, la capacitación continua es fundamental" (S. Berríos). "Utilizar herramientas antimalware, como antivirus, tener segundo método de protección del sistema, como el uso de contraseñas robustas" (F. Villalobos).
Impacto en las empresas	Pérdida de valor e imagen y falta de preparación	No invertir en ciberseguridad provoca pérdidas económicas y reputacionales.	"Una empresa que es atacada software y es capturada, por ejemplo, su valor inmediatamente se ve resentido... inmediatamente te baja el valor de la de la acción. Tiene un efecto económico tremendo."(M. Heavey). "en ciberseguridad hay que ver el gasto en plata, pero también hay un gasto en imagen de la empresa y un gasto en tiempo, porque si tú no puedes operar durante dos semanas o más, bueno, es plata que no entra tampoco en la empresa, así que al final el balance es súper negativo"(X. Bonnaire). "Hay riesgos no solamente legales, reputacionales importantes y desconfianza con tus clientes, con tus trabajadores"(R. Garrido). "A través de una persona pueden ingresar a los datos e información de la empresa, correos,

			páginas internas, etc., las pérdidas no son mínimas, son millonarias" (G. Lanzarini). "Hoy día un ataque, un ciberataque daña la imagen que de alguna manera afecta la confianza."(S. Berríos).
Medidas tomadas en Chile	Evolución y regulaciones en ciberseguridad	Ley Marco Ciberseguridad y Agencia Nacional de Ciberseguridad	"Las organizaciones están sujetas a una ley de ciberseguridad que se promulgó recién, como este es un país sumamente legalista, en el momento que haya una ley ya todo el mundo se ordenó detrás de esos temas"(R. Martínez) "la ley Marco Ciberseguridad, que establece, primero que nada, toda una institucionalidad y una gobernanza y fija una serie de reglas y normativas que se van a ir aplicando a distintas instituciones"(M. Heavey). "hoy día a nivel país, tenemos todo un marco regulatorio en el ámbito de tecnología y puntualmente ciberseguridad, política nacional, ley de ciberseguridad, ley de delito y económico"(C. Villagra) "... y viene una terrible para el cambio, que es sobre los datos personal, esa sí que va a ser una evolución en Chile y la gran mayoría de empresas, van a estar en súper enojada con eso porque va a cambiar drásticamente los hábitos que tienen en términos de gestión de datos."(X. Bonnaire). "Basado en las nuevas políticas que Chile se ha creado ya hoy día, las organizaciones cada vez están más conscientes de la importancia de poder proteger sus activos digitales, aunque muchas aún carecen de herramientas políticas y prácticas necesarias para poder de alguna manera que defenderse" (S. Berríos). "La ley de delitos económicos incorporó los delitos informáticos dentro de aquellos delitos que pueden ser cometidos por entes y para tú no cometer delitos informáticos tienes que tener controles de ciberseguridad para que no tengas fuga de información, acceso a un debido de datos, receptación de datos, que son los delitos que son los otros delitos informados entonces."(R. Garrido).

Perspectivas de ciberseguridad	Cultura de ciberseguridad, tecnologías y controles claves	Conciencia y preparación por parte de las empresas.	"tienen que velar por la resiliencia...la resiliencia, en el fondo es la capacidad que tú tienes de volver a brindar los servicios en las condiciones que estaban antes del evento de ciberseguridad o ciberataque (M. Heavey). ""son varias las tareas que hay que hacer en forma simultánea para que el tema de ciberseguridad mejore para que el riesgo que uno tiene baje. O sea, nunca hay una empresa que esté ciento por ciento libre de tener un ciberataque."(R. Martínez). " hoy día ciberseguridad es un proceso más de la compañía, no es TI. ¿Como ha cambiado? las inversiones, los presupuestos, las tecnologías, las dotaciones, las personas, el conocimiento, la formación también es un tema reimportarte en ciberseguridad."(C. Villagra). "el mayor desafío en Chile es la concientización, es decir que no existe una cultura general a nivel país y a nivel de las personas digamos, de los problemas de ciberseguridad, de las buenas prácticas en comportamiento en internet, de la gestión de contraseña, de datos personales, etcétera."(X. Bonnaire). "la ciberseguridad va a ser un requisito para producir inteligencia artificial. Es decir, yo tengo que tener mis datos resguardados, seguros, protegerlos, porque si no la inteligencia artificial o los resultados que producen las máquinas no van a ser los óptimos ni deseados si mis datos son corruptos"(R. Garrido).” "Uno de los mayores desafíos de la ciberseguridad, es la concientización de las personas, es un factor crucial para el futuro"(G. Lanzarini).” "casi el 80 al 90% de los ataques que se generan hoy día son por falta de capacitación, son por fallas de errores humanos" "es muy importante es la comunicación entre las empresas...La ciberseguridad se comparte, no se compite"(S. Garrido).
Perspectivas de empresas	Preparación de las empresas en el futuro, presupuesto y recursos para la ciberseguridad.	Existe una gran necesidad de crear conciencia sobre la ciberseguridad y formar especialistas debido a la creciente amenaza de	"hoy día existen dos tipos de empresa, las que les pasó y las que no saben qué le pasó"(C. Villagra). "hay un dicho en ciberseguridad que dice que la pregunta no es saber si tú vas a ser víctimas de un ataque exitoso, sino que cuándo"(X. Bonnaire). "hay dos tipos de empresas en el mercado, las que saben que las hackearon y las que no saben que las hackearon. Así de claro, la reacción va a depender del daño que sufran" (M. Heavey). " a las que no están preparadas y piensan que no

		ciberataques y la falta de cultura de ciberseguridad.	les va a tocar, solamente hay que decirles de que este no es un tema que sí les va a tocar, sino que cuándo les va a tocar"(R. Martínez). "pero lo que les falta a las empresas, al menos lo que me toca ver, son áreas que son muy precarias, en general, una persona, dos personas luchando con los directorios para para que den presupuesto para el año siguiente para implementar programas, concientización, porque claro, todavía se ve como que la ciberseguridad fuera como una suerte como de inversión, no como un requisito de base para que mi empresa"(R. Garrido). "las empresas no pueden esperar a que les pase, siempre deben ser preventivos, tener la capacidad de respuesta y saber qué hacer y saber hacia dónde ir"(G. Lanzarini)." lo principal es hacer algunas charlas, talleres para poder lograr la concientización de la de las personas, porque las personas son relevantes."(F. Villalobos).
--	--	---	---

Fuente: Elaboración propia

En primera instancia, los entrevistados han resaltado la importancia y beneficio de la inteligencia artificial en la ciberseguridad, coincidiendo en que se está utilizando de manera efectiva para prevenir los ciberataques, debido a que tienen la capacidad de detectar y neutralizar posibles ataques mediante el aprendizaje continuo y el monitoreo de vulnerabilidades y amenazas. Los sistemas de IA son entrenados para identificar sus propias vulnerabilidades y proponer soluciones, además, por medio de un proceso de desarrollo constante y adaptativo, permite que las herramientas de IA se perfeccionen con el tiempo.

Un aspecto crucial señalado es que la inteligencia artificial no es una solución mágica que resolver todos los problemas de ciberseguridad de manera automática. En lugar de eso, requiere un desarrollo y liberación de algoritmos que aprendan de las situaciones a las que se enfrentan, generando y proponiendo soluciones basadas en la experiencia y el análisis continuo de datos. Este enfoque permite que las herramientas de IA evolucionen y mejoren su eficacia en la detección de amenazas.

Otro hallazgo relevante es el papel de la IA en la detección de errores de programación y en la mejora de la defensa contra ataques sofisticados. Como menciona Rolando Martínez, la IA proporciona capacidades avanzadas de procesamiento de texto y análisis de grandes volúmenes de datos, lo que resulta crucial para identificar y corregir defectos de

programación que puedan ser explotados por atacantes. Además, en el contexto de grandes hackeos y ataques industriales, señala que la inteligencia artificial se ha mostrado más beneficiosa para los defensores que para los atacantes. Sin embargo, en el caso de ataques más pequeños y masivos, como el phishing y fraudes menores, la IA también puede ser utilizada por los atacantes para mejorar la efectividad de sus tácticas.

Carlos Villagra y N.N destacan la capacidad de la IA para procesar grandes cantidades de datos rápidamente y disminuir los tiempos de respuesta. Esto demuestra que la IA puede analizar y responder a amenazas de manera mucho más rápida y eficiente que los seres humanos, permitiendo soluciones más rápidas y efectivas ante ciberataques. Asimismo, Xavier Bonnaire menciona “la inteligencia artificial es una herramienta bastante eficiente para detectar esos ataques, para ser capaz de desplegar rápidamente una respuesta”, y con ello Francisco Villalobos, resalta su experiencia con el uso de IA en sistemas basados en machine learning para reforzar la forma en que se recibe un ataque en el sistema, para tener la capacidad de actuar rápido y eficazmente.

En cuanto al uso de la IA para realizar fraudes, los atacantes emplean herramientas de IA para buscar vulnerabilidades y ejecutar ataques automatizados. Estas herramientas les permiten insertar segmentos de código malicioso y manipular sistemas de diversas maneras, incluyendo el robo de información y la implementación de ransomware. Los entrevistados destacan la capacidad de los atacantes para entrenar herramientas de IA, que luego pueden ejecutar acciones de manera autónoma y continua, incrementando la sofisticación y frecuencia de los ataques. Además, como bien menciona Francisco Villalobos, hay diversas herramientas de IA para efectuar ataques sin la necesidad de tener conocimiento sobre programación, lo que demuestra lo accesible que es realizar fraudes digitales.

De esta manera, la IA está facilitando la creación de fraudes masivos mediante correos de phishing y engaños personalizados. Los atacantes utilizan la IA para diseñar mensajes de phishing más convincentes y dirigidos a un público amplio. Estos fraudes pueden variar desde ofertas engañosas de herencias hasta solicitudes de ayuda de supuestas víctimas, la capacidad de la IA para personalizar y automatizar estos mensajes aumenta la probabilidad de éxito de fraudes.

Asimismo, los métodos utilizados para realizar fraudes digitales, más recurrentes que mencionan los entrevistados son principalmente el phishing y el ransomware. Los ataques de phishing son comunes y un aspecto destacado es que los ciberataques pueden iniciarse simplemente abriendo un archivo contaminado o a través de correos electrónicos fraudulentos, por ello algunas empresas han implementado políticas específicas para mitigar estos riesgos. El ransomware, por su parte, implica el secuestro de sistemas mediante la encriptación de datos, y los atacantes suelen exigir un rescate para devolver el acceso.

Los correos fraudulentos son un ejemplo del método comúnmente utilizado en ciberataques. Rolando Martínez menciona el caso de intento de fraude conocido como BEC, donde los atacantes se hacen pasar por altos ejecutivos para solicitar transferencia de dinero. Este tipo de ataques no solo son sofisticados en su apariencia, sino también están respaldados por herramientas avanzadas disponibles en la dark web. Además, la IA se utiliza para crear correos electrónicos engañosos y realistas, haciendo que las víctimas sean más propensas a caer en la trampa, tal como menciona Giovanna Lanzarini, los correos fraudulentos están siendo más personalizados y sofisticados que antes.

Otra técnica mencionada es el uso de la IA para replicar voces y crear videos falsos de personas pidiendo ayuda, aumentando así la credibilidad del fraude. Aunque no se ha observado una aparición reiterada de estos métodos, su existencia indica una tendencia preocupante hacia fraudes cada vez más sofisticados y convincentes.

Michael Heavey menciona que “La gente de ciberseguridad tiene como regla de oro, qué por cada 1000 líneas de código que tú tengas hay al menos 1 vulnerabilidad”, este dato indica que habrá un porcentaje de probabilidad de vulnerar el sistema y poder atacarlo. Además, el incentivo para realizar ciberataques es grande debido a la facilidad con la que pueden ser ejecutados con recursos limitados.

Las respuestas de los entrevistados en relación con el impacto de los ciberataques en las empresas reflejan una preocupación significativa por la falta de preparación y concienciación en materia de ciberseguridad en muchas empresas. Michael Heavey destaca que las empresas que no invierten adecuadamente en seguridad pueden sufrir grandes pérdidas económicas y de reputación, además la ciberseguridad no se trata únicamente de programas y tecnologías, sino también de la conciencia social y las implicancias legales. Un ataque no solo puede

afectar los activos de la empresa, sino también el valor para los accionistas y la percepción pública y la imagen de la empresa se ve perjudicada, además, en varias ocasiones sufrir un ataque, impide a la empresa continuar operando, ocasionando pérdida de tiempo y con ello un efecto negativo en las operaciones de la empresa. Un claro ejemplo de esto es el que cita Michael Heavey respecto a un banco que no invirtió lo necesario en ciberseguridad y sufrió un ataque, este caso ilustra como la falta de preparación y una mala gestión pueden llevar a una pérdida de valor significativa.

Por su parte, Romina Garrido, resalta la importancia de los riesgos para las empresas, los cuales no son solo legales, si no que genera una desconfianza en los clientes y trabajadores. Esto lo confirma Sebastián Berríos, señalando que un ciberataque afecta la confianza en la empresa, generando pérdidas millonarias.

Por otro lado, se observa un cambio positivo en la mentalidad de las empresas, la ciberseguridad está empezando a ser vista no solo como un problema reputacional, sino que se le está tomando más importancia y preocupación. Este cambio ha llevado a una mayor disposición a compartir información y a invertir en ciberseguridad, tal como mencionan los entrevistados, las grandes empresas en particular están realizando inversiones significativas en ciberseguridad para protegerse contra posibles ataques.

Pese a, se evidencia que, aunque la mentalidad está cambiando y las empresas están comenzando a tomar la ciberseguridad más en serio, especialmente aquellas que ya han sido hackeadas, todavía hay un camino por recorrer.

En relación con las medidas que se han tomado en Chile respecto a la ciberseguridad, todos los entrevistados destacan la importancia de la Ley marco de ciberseguridad, que ha establecido una estructura institucional y de gobernanza para abordar la ciberseguridad a nivel nacional. Esta ley incluye la creación de la agencia nacional de la ciberseguridad, que tiene la responsabilidad de coordinar y normatizar los aspectos relacionados con la ciberseguridad dentro del marco legal. La agencia posee facultades normativas y sancionatorias significativas, lo que refuerza su capacidad para asegurar el cumplimiento de las normativas de ciberseguridad en diversas instituciones que señala la ley.

Se refleja cómo Chile ha experimentado una evolución significativa en su enfoque hacia la ciberseguridad desarrollando un marco regulatorio que abarca leyes y políticas nacionales, como menciona Carlos Villagra, las nuevas regulaciones incluyen no solo la Ley de ciberseguridad, si no también leyes relacionadas con delitos económicos y fraudes cibernéticos. Además, mencionan que se continúa trabajando en leyes y políticas de esta materia, incluso, la más próxima es sobre los datos personales, la cual traerá consigo un cambio en los hábitos de gestión de datos de las empresas.

Si bien se menciona una conciencia generalizada sobre la importancia de la ciberseguridad entre las organizaciones en Chile, también señalan una escasez crítica de profesionales especializados en ciberseguridad. Esta falta de talento ha llevado a las empresas a buscar y formar internamente a sus equipos, así como a contratar servicios externos, lo cual es más accesible para empresas medianas y grandes, pero un desafío para las más pequeñas.

Así como se utiliza la IA como herramienta para realizar y prevenir los ataques, se mencionan otras medidas que se pueden utilizar para reforzar la seguridad y prevenir estos ataques. Estas medidas son la eliminación de passwords tradicionales y reemplazarlos con métodos de autenticación más seguros y tecnologías como dispositivos físicos de autenticación, como menciona Rolando, ya que son destacados por su capacidad para proporcionar un nivel de seguridad más robusto. Este enfoque segmenta la red y limita los accesos, lo que reduce la posibilidad de que un atacante interno comprometa sistemas críticos.

A estas medidas, Rolando Martínez señala que hay que sumar el factor humano. Este es un componente relevante para el éxito de las medidas implementadas, Michael Heavey menciona que “Gran parte, sino como 80 o 90% de los ciberataques tienen algún factor humano de por medio”. Debido a ello, el entrenamiento y la concientización del personal se consideran indispensables para la prevención del fraude digitales porque, aunque las tecnologías avanzadas de inteligencia artificial son efectivas, su efectividad se ve comprometida si las personas no actúan de manera segura.

Los entrevistados concuerdan sobre la importancia de campañas de concientización y programas de formación continua para elevar el nivel de madurez organizacional. En última instancia el factor humano es visto como decisivo, ya que la decisión final es de la persona.

Por ello, la educación continua y la preparación son cruciales para asegurar que las personas tomen decisiones informadas y seguras.

Otro termino mencionado por Michael Heavey, es la ciberhigiene, las cuales corresponden a las normas y práctica para manejarse frente a un computador, este concepto se relaciona con el factor humano y el actuar de las personas, debido a que en general, no presentan mayores conocimientos sobre qué implica, por ejemplo, dejar el computador abierto e ir a otro lugar por unos minutos. La concientización sobre la ciberhigiene busca reducir la incidencia de ataques internos, que, según indica, “Gran parte, sino como 80 o 90% de los ciberataques tienen algún factor humano de por medio.” Este dato, subraya la importancia de que el personal esté bien educado y consciente de las medidas que se están tomando respecto a la ciberseguridad.

También, la preparación y la resiliencia de las empresas se presentan como aspectos clave en la defensa contra el ciberataque. La preparación no solo implica la adopción de tecnologías, sino también la capacidad de respuesta y recuperación rápida ante incidentes, asegurando la continuidad del negocio y minimizando el impacto de los ataques.

Por otra parte, los entrevistados, señalan que el nivel de preparación varia considerablemente entre las organizaciones, mientras algunas están bien preparadas y han implementado medidas preventivas efectivas, otras confían en su buena suerte y no se preparan adecuadamente. Este enfoque pasivo es peligroso, ya que los ataques pueden ser sofisticados y prolongados, con atacantes que permanecen en las redes durante meses o años antes de ejecutar el golpe final. Por este motivo se resalta la educación continua y la conciencia sobre la ciberseguridad, además, las organizaciones deben adoptar una mentalidad proactiva y estar siempre alerta, invirtiendo en medidas preventivas y formativas para proteger sus activos digitales de manera efectiva.

Como menciona Carlos Villagra, la tecnología siempre conlleva un nivel de riesgo, pero también proporciona herramientas para mitigarlo. El control adecuado de estas tecnologías es fundamental para reducir los riesgos de ciberseguridad. Las palabras de los entrevistados refuerzan la idea de que, aunque la tecnología facilita la vida, también crea nuevas brechas que deben ser gestionadas. Por ello, la ciberseguridad ha evolucionado para incluir no solo

tecnologías avanzadas, sino también inversiones, presupuestos adecuados, dotaciones de personal capacitados y una formación constante.

Respecto a las perspectivas que tienen los expertos sobre la ciberseguridad, señalan que las empresas necesitan de profesionales especializados, además de la falta de cultura de ciberseguridad es evidente y representa una debilidad significativa, ya que muchas organizaciones no están preparadas para detectar y responder a ciberataques de manera efectiva. También, se destacan la necesidad de una mejor comprensión y educación sobre ciberseguridad en todos los niveles de la empresa, las empresas deben estar conscientes de sus vulnerabilidades y adoptar una actitud proactiva preparándose para posibles ataques en todo momento.

Además, mencionan que las amenazas cibernéticas han evolucionado con bandas organizadas que ahora venden vulnerabilidades y explotan programas en la dark web. Esto ha transformado el programa de cibercrimen, pasando de ataques individuales a una industria organizada. Por eso mismo, las organizaciones deben realizar múltiples tareas simultáneamente para reducir el riesgo de ciberataques, reconociendo que nunca estarán completamente libres de estos riesgos.

Y, por último, la IA está siendo utilizada tanto para defender como para llevar a cabo ciberataques avanzados, esto incluye nuevos tipos de ataques, por ello la ciberseguridad debe evolucionar para abordar estas nuevas amenazas, integrando tecnologías avanzadas y formación especializada para anticipar y neutralizar estos ataques innovadores. Para esto es crucial estar en constante aprendizaje y, como menciona Romina Garrido, la ciberseguridad se comparte entre las empresas y no se compite.

Conclusiones

A partir del análisis de las entrevistas realizadas en el marco de esta tesis, se pueden extraer conclusiones relevantes que permiten evaluar el cumplimiento de las propuestas y los objetivos planteados. En general, las opiniones de los expertos convergen en resaltar tanto las oportunidades como las limitaciones de la inteligencia artificial en el ámbito de la ciberseguridad, particularmente en la detección y prevención de fraudes digitales.

Los entrevistados coinciden en que la IA ha demostrado ser una herramienta efectiva para la detección y prevención de fraudes digitales. La capacidad de la IA para analizar grandes volúmenes de datos rápidamente y con precisión permite identificar patrones y anomalías que podrían indicar actividades fraudulentas. Las tecnologías de aprendizaje automático y profundo facilitan la anticipación y respuesta a nuevas formas de fraude digital.

Sin embargo, aunque la IA ha reducido la vulnerabilidad y las pérdidas económicas en las organizaciones, su efectividad varía según el nivel de inversión y la preparación interna de cada empresa. Empresas que han adoptado ampliamente estas tecnologías y han invertido en capacitación continua han observado una reducción significativa en los incidentes de fraude. No obstante, en organizaciones con menos recursos o menor conciencia, la implementación de IA no siempre ha sido suficiente para contrarrestar las amenazas, lo que indica que la propuesta 1 no se cumple de manera completa.

Por otra parte, los 4 entrevistados sobre el ámbito de la ciberseguridad e IA, destacan reiteradamente que el factor humano es crucial para el éxito de cualquier estrategia de ciberseguridad. Aunque la IA proporciona herramientas avanzadas, su efectividad está directamente relacionada con el nivel de conocimiento y la ética profesional del personal de la organización. Como bien menciona Michael Heavey, aproximadamente el 80-90% de los ciberataques implica algún tipo de error humano. Por lo tanto, la educación constante del personal es indispensable para maximizar las capacidades de la IA en la protección contra fraudes digitales.

Además, el término de la ciberhigiene es mencionado como una práctica esencial que los empleados deben adoptar para minimizar riesgos, lo cual incluye hábitos seguros al usar computadoras y manejar información sensible. La formación continua y la sensibilización sobre la importancia de la ciberseguridad son fundamentales para potenciar las tecnologías de la IA y asegurar la efectividad de las estrategias preventivas, confirmando la validez de la propuesta 3.

Por otra parte, los expertos reconocen que la IA no solo es una herramienta poderosa para los defensores, sino que también está siendo utilizada por los atacantes para llevar a cabo fraudes más sofisticados y automatizados. La capacidad de la IA para replicar voces, crear videos

falsos y personalizar correos de phishing ha incrementado la efectividad de los ataques, dificultando las medidas preventivas adoptadas por las organizaciones.

A pesar de estos desafíos, las organizaciones que invierten en tecnologías de la IA y adoptan enfoques proactivos de ciberseguridad están mejor preparadas para enfrentar estos ataques. La implementación de métodos de autenticación más seguros y la segmentación de redes, junto con la formación del personal, ayudan a mitigar los riesgos. Aunque la amenaza es significativa, las empresas pueden fortalecer sus defensas a través de una combinación de tecnología avanzada y prácticas de seguridad robustas, lo que sugiere que la 3 tampoco se cumple de forma completa.

Y en relación con la propuesta 4, los testimonios de los expertos apuntan a que las empresas que han sufrido pérdidas financieras a causas de fraudes digitales con IA muestran una conciencia más clara y crítica sobre la importancia de invertir en tecnologías de ciberseguridad. Estas organizaciones comprenden mejor que aquellas que no han sido afectadas la gravedad de las amenazas cibernéticas y la necesidad de métodos avanzados, incluidos los basados en IA para protegerse eficazmente.

Los entrevistados señalan que las empresas que han sido víctimas de ciberataques son más proclives a aumentar sus inversiones en ciberseguridad, adoptando tecnologías avanzadas y desarrollando políticas más robustas para mitigar futuros riesgos. Esta percepción crítica se refleja en un cambio en la mentalidad de las empresas afectadas, que empiezan a ver la ciberseguridad no solo como una medida preventiva, sino como una necesidad fundamental para la continuidad y protección de su empresa.

Este comportamiento también se evidencia en los ejemplos proporcionados durante las entrevistas, donde empresa que sufrieron ataques significativos hicieron inversiones sustanciales en tecnologías de IA y capacitación del personal para evitar recurrencias. Por lo tanto, se puede concluir que la propuesta se cumple, ya que existe una correlación clara entre la experiencia de pérdidas financieras debido a fraudes digitales y una percepción más crítica y proactiva respecto a la necesidad de inversiones adicionales en ciberseguridad.

Finalmente, a través de la investigación se han identificado los métodos más comunes detectados en los cuales se encuentra el phishing, ransomware, replicación de voces y videos

falsos. Estos fraudes, potenciados por la IA, han generado impactos significativos en las organizaciones, incluyendo pérdidas económicas, daños reputacionales y operativos. Las empresas que no realizan inversiones adecuadas en ciberseguridad se encuentran especialmente vulnerables ante estos ataques.

Las herramientas de IA más efectivas para combatir estos fraudes incluyen sistema de aprendizaje automático y profundo, que tienen la capacidad de analizar grandes volúmenes de datos en tiempo real, detectando patrones y anomalías. Esto permite una respuesta rápida y precisa ante las amenazas, mejorando la calidad de las organizaciones para prevenir fraudes.

Por otra parte, a nivel nacional, la Ley Marco de Ciberseguridad y la creación de la Agencia Nacional de Ciberseguridad han establecido un marco institucional y de gobernanza que aborda la ciberseguridad a nivel nacional. Estas medidas, junto con las leyes relacionadas con delitos económicos y fraudes cibernéticos, han significado un gran avance en esta materia, sin embargo, aún falta mucho por avanzar.

Por último, los expertos consultados tienen una percepción positiva sobre el potencial de la IA para mejorar la ciberseguridad. Sin embargo, también reconocen las limitaciones de estas tecnologías y subrayan la importancia del factor humano. La IA se considera una herramienta poderosa que debe ser complementada con una formación continua y una cultura de ciberseguridad dentro de las empresas para poder maximizar su efectividad.

Recomendaciones

En primer lugar, se recomienda a las organizaciones invertir de manera continua en tecnologías avanzadas de IA para la detección y prevención de fraudes digitales. Además, es fundamental que inviertan en la capacitación continua de su personal para asegurar la eficacia de estas herramientas, asimismo, se destaca que no es recomendable esperar a que suceda algún ataque para tomar las medidas, ya que la pérdida puede ser mucho mayor e incluso irreparable.

Asimismo, debido a que la ciberseguridad es un campo dinámico que requiere una adaptación constante a nuevas amenazas. Las organizaciones deben estar dispuestas a innovar y adoptar nuevas tecnologías y métodos para mantenerse un paso adelante de los atacantes.

En segundo lugar, es esencial fomentar una cultura de ciberseguridad en todas las áreas de la organización, incluyendo implementación de políticas de ciber higiene, la realización de simulaciones de ciberataques y campañas de conciencia para asegurar que todo el personal entienda la importancia de las prácticas seguras.

Y, por último, a nivel nacional, es importante seguir desarrollando y actualizando el marco regulatorio relacionado con la ciberseguridad. La colaboración entre el gobierno, el sector privado y las instituciones académicas es crucial para asegurar que las leyes y políticas estén alineadas con las mejores prácticas y los avances tecnológicos.

Anexos

Anexo 1:

ANÁLISIS DE LAS ENTREVISTAS				
Entrevistado	Objetivo	Recurrente	Hallazgo	Citas
1	El uso de la IA para prevenir y detectar fraudes	Desarrollo y monitoreo de herramientas de la IA	La IA se está utilizando para desarrollar herramientas de ciberdefensa que detecten y neutralicen posibles ataques, mediante el aprendizaje y monitoreo continuo de las vulnerabilidades y amenazas.	"El uso de herramientas, yo diría que sí es relevante y se van a ir desarrollando herramientas de ciberdefensa para evitar ciberataque. Tú vas a ir perfeccionando tu propio software para ir básicamente detectando y neutralizando posibles ataques siempre y eso va a ser parte de herramientas de desarrollo" "Ahora, la inteligencia artificial va a ir aprendiendo, o sea, tú tienes que desarrollar un sistema e ir entrenándolo para justamente el objetivo que tú quieres... hay todo un tema de desarrollo de liberación del algoritmo para que el algoritmo vaya aprendiendo de la situación que vaya probando y vaya generando y proponiendo soluciones."
2	El uso de la IA para prevenir y detectar fraudes	La IA en la defensa y detección de fraudes	La IA ayuda en la ciberseguridad para detectar errores de programación y mejorar la defensa contra ataques sofisticados.	"la inteligencia artificial es una tecnología nueva que nos permite generar algunas capacidades de procesamiento de texto en general y en forma muy rápida entre la mayor parte" "Los grandes modelos de lenguaje, que son los que hoy día están como más en boca en términos de la inteligencia artificial...son capaces muchas veces de señalar defectos de programación que son inseguros o cosas por el estilo, lo que ayuda a los programadores a no cometer esos errores en el diseño de sus aplicaciones."
3	El uso de la IA para prevenir y detectar fraudes	Potencia de la IA en ciberseguridad	La IA es extremadamente efectiva en la ciberseguridad por su capacidad de procesar grandes cantidades de datos.	"el uso de la inteligencia artificial dentro de la tecnología de ciberseguridad es tremendamente potente, o sea, piensa que diría un ser humano que puede procesar una cantidad de datos finita, en un tiempo finito, inteligencia artificial, no dependiendo del tipo de potencia que tenga, dónde está montado, puedes tener soluciones súper rápido"

4	El uso de la IA para prevenir y detectar fraudes	Implementación de la IA dentro de la empresa.	Reducción de tiempos de respuesta y mejora de la seguridad	"los casos de negocio se hacían complicados con las nuevas versiones de inteligencia, lo que se demoraba 6 meses se transformaba en cuatro semanas, y cuando tú ya querías obtener resultados de alguna manera, es con algún nivel de seguridad más arriba del 80%. Ya con dos meses de entrenamiento tenías los resultados que en otras ocasiones alcanzarías después de 1 año."
5	El uso de la IA para prevenir y detectar fraudes	Uso de la IA para detección y respuesta rápida.	La IA es una herramienta eficiente para detectar ataques, desplegar respuestas rápidas y mitigar los efectos de los incidentes de seguridad.	"la inteligencia artificial va a ser un gran beneficio para lo que es la seguridad...pero hay un tema que es super complejo, que se llama la detección de ataque y la respuesta a incidentes." "ahí desde ese punto de vista, la inteligencia artificial es una herramienta bastante eficiente para detectar esos ataques, para ser capaz de desplegar rápidamente una respuesta, software, o hardware desconectar redes varias cosas, digamos. Y ahí realmente es un beneficio enorme.
6	El uso de la IA para prevenir y detectar fraudes	Monitoreo y Alertas	Automatizar procesos	"La IA puede monitorear todos los procesos y dar las alertas que son necesarias para que los encargados de ciberseguridad puedan detectar oportunamente ciberataques" "se transforma también en una herramienta para la ciberseguridad en la medida que permite automatizar procesos repetitivos bajo reglas y que te permiten detectar amenazas que probablemente con 4 o 5 personas que tú tengas en un equipo de ciberseguridad se te podría pasar"
7	El uso de la IA para prevenir y detectar fraudes	Alertas y algoritmos	Sistemas que detectan patrones.	"Se utilizan sistemas de alertas para detectar amenazas" "Hay que utilizarla al igual que los atacantes, para estar al mismo nivel e incluso mayor" "Se utilizan plataformas que detectan patrones y algoritmos, con el fin de alertar algún comportamiento extraño y tomar las medidas necesarias"
8	El uso de la IA para prevenir y detectar fraudes	Automatización y detección del malware.	Mejora en respuesta a ataques.	"mejorar detección de malware, automatizar respuestas antecedentes "

9	El uso de la IA para prevenir y detectar fraudes	Machine learning y algoritmos.	Redes neuronales que detectan ataques.	"La IA que hemos trabajado es principalmente orientado a la parte de sistemas basados en machine learning, para poder reforzar la forma de que, cómo se cuándo se recibe un ataque en un sistema rápidamente, ese ese ataque puede hacer detectado a través de distintos algoritmos supervisados, no supervisado o redes neuronales."
1	Impacto en la empresa	Perdida del valor de la empresa, falta de preparación y conciencia.	Las empresas que no invierten adecuadamente en la ciberseguridad pueden sufrir grandes pérdidas económicas y de reputación.	"La ciberseguridad no es únicamente programas, sino que también hay conciencia social, es interacción, es legal" "la mentalidad está afortunadamente cambiando. el hecho de hablar de ciberseguridad entre las empresas y de compartir información, eso ha cambiado, ya no se ve como un tema de reputacional" "Después que empezó a hacerse un poco más, más popular, más evidente que estas cosas ocurrían, la gente empezó a compartir información y hacer más sensible al tema y a invertir más, entonces ahí las empresas grandes están haciendo grandes inversiones en temas de ciberseguridad." "Una empresa que es atacada software y es capturada, por ejemplo, su valor inmediatamente se ve resentido... inmediatamente te baja el valor de la de la acción. Tiene un efecto económico tremendo."
5	Impacto en la empresa	Impacto financiero y en la imagen de la empresa.	Impacto en pérdida de imagen y tiempo de inactividad.	"en ciberseguridad hay que ver el gasto en plata, pero también hay un gasto en imagen de la empresa y un gasto en tiempo, porque si tú no puedes operar durante dos semanas o más, bueno, es plata que no entra tampoco en la empresa, así que al final el balance es súper negativo"
6	Impacto en las empresas	Recursos e inversión	Riesgos reputacionales	"falta de capacidad, presupuesto, retención del talento, inversión, porque creo que la tecnología muchas veces existe cuando uno se entera de las mayores brechas de ciberataques que hemos visto en nuestro país, en el que, en este último momento, en general por una falta de supervisión en materia de ciberseguridad, porque

				las soluciones ya estaban disponibles en el mercado, pero no se implementaron en el momento." ". Hay riesgos no solamente legales, reputacionales importantes y desconfianza con tus clientes, con tus trabajadores"
7	Impacto en las empresas	Pérdidas millonarias	Acceso a datos críticos por fallos humanos.	"A través de una persona pueden ingresar a los datos e información de la empresa, correos, páginas internas, etc., las pérdidas no son mínimas, son millonarias"
8	Impacto en las empresas	Daño reputacional.	Incremento de desconfianza.	"han causado pérdidas económicas significativas, daño a la reputación de las empresas afectadas, aumento de la desconfianza" "Hoy día un ataque, un ciberataque daña la imagen que de alguna manera afecta la confianza."
9	Impacto en las empresas	Falta de percepción del riesgo.	Subestimación de ciberseguridad.	"es un problema a veces de las empresas, porque creen que esto de la ciberseguridad es como algo que no podría afectarle "
1	Medidas tomadas en Chile	Ley Marco Ciberseguridad. Creación de agencia y normativas.	En Chile, se ha establecido una ley marco de ciberseguridad que incluye la creación de una Agencia Nacional de la Ciberseguridad.	"la ley Marco Ciberseguridad, que establece, primero que nada, toda una institucionalidad y una gobernanza y fija una serie de reglas y normativas que se van a ir aplicando a distintas instituciones, esto significa que van a ver, por ejemplo, en la ley marco se crea una Agencia Nacional de la Ciberseguridad, que coordina todos los aspectos de ciberseguridad dentro del marco legal, tiene facultades normativas sancionatorias importantes y no son pocas." "Dentro de la normativa que crea la agencia de ciberseguridad, se establece las facultades que tiene y como va a controlar y como va a normar sobre distintas instituciones, entonces se van a establecer dos conceptos, uno son los operadores esenciales y los otros son los operadores de importancia vital."
2	Medidas tomadas en Chile	Ley de ciberseguridad.	Promulgación de una ley reciente	"Las organizaciones están sujetas a una ley de ciberseguridad que se promulgó recién, como este es un país sumamente legalista, en el momento que haya una ley ya todo el mundo se ordenó detrás de esos temas."

3	Medidas tomadas en Chile	Evolución y regulaciones en ciberseguridad	Chile ha implementado un marco regulatorio sólido en ciberseguridad, incluyendo leyes y políticas nacionales.	"Pero ahora se ha dado mucho foco, entonces dos cosas, la primera, hay una evolución y la evolución se mide en madurez, y si tú lo miras hoy día a nivel país, tenemos todo un marco regulatorio en el ámbito de tecnología y puntualmente ciberseguridad, política nacional, ley de ciberseguridad, ley de delito y económico"
5	Medidas tomadas en Chile	Cambios en la legislación chilena	Ley de ciberdelincuencia y Agencia Nacional de Ciberseguridad.	"Lo que sí es un gran paso últimamente es el cambio de ley, hay varias leyes que salieron. La primera es la ley de ciberdelincuencia que tiene la ventaja de, como dicen los de la PDI, de tipificar nuevos delitos" "Hay una nueva ley Marco de Ciberseguridad, la creación de la agencia nacional de ciberseguridad y viene una terrible para el cambio, que es sobre los datos personal, esa sí que va a ser una evolución en Chile y la gran mayoría de empresas, van a estar en súper enojada con eso porque va a cambiar drásticamente los hábitos que tienen en términos de gestión de datos."
6	Medidas tomadas en Chile	Leyes y sanciones	Controles obligatorios y Ley Marco Ciberseguridad	"ya tenemos la ley marco de ciberseguridad en poco tiempo más para comenzar a regir con sanciones para ciertos sectores empresariales" "La ley de delitos económicos incorporó los delitos informáticos dentro de aquellos delitos que pueden ser cometidos por entes y para tú no cometer delitos informáticos tienes que tener controles de ciberseguridad para que no tengas fuga de información, acceso a un debido de datos, receptación de datos, que son los delitos que son los otros delitos informados entonces."
7	Medidas tomadas en Chile	Ley de ciberseguridad.	Obligación de notificar incidentes.	"Ahora se viene la ley de la ciberseguridad, con ello si o si las empresas deben avisar a la autoridad, por ello deben tener un sistema preventivo y estar preparados"

8	Medidas tomadas en Chile	Protección de activos digitales.	Falta de herramientas y prácticas.	"Basado en las nuevas políticas que Chile se ha creado ya hoy día, las organizaciones cada vez están más conscientes de la importancia de poder proteger sus activos digitales, aunque muchas aún carecen de herramientas políticas y prácticas necesarias para poder de alguna manera que defenderse. "
9	Medidas tomadas en Chile	Ley de incidentes críticos.	Plazos para informar eventos.	"la ley va a decir que, si ocurre un evento, por ejemplo, en una infraestructura crítica, la empresa tiene un tiempo para avisar y ahí tiene que protegerse de alguna forma "
1	Métodos utilizados para realizar fraudes	Phishing. Ransomware. Sistema vulnerable.	Los ciberataques se pueden producir con poca infraestructura.	"Puedes tener ataques que vienen porque alguien abre mal un archivo que le llega y ese archivo viene contaminado..." "puede ser un phishing y pasa bien a menudo, incluso las empresas ya hoy día están haciendo políticas anti-phishing" "El incentivo es muy grande porque los ciberataques tú lo puedes producir o los podías producir con muy poco, con muy poca infraestructura. Hoy día va requiriendo un poco más y, pero también están las herramientas de inteligencia artificial, pero para generar ciberataques. Incluso tú los puedes contratar en la Deep web" "El ransomware, es un tema, es un secuestro, tu secuestras el sistema y puedes hacer varias cosas"
2	Métodos utilizados para realizar fraudes	Phishing o correos fraudulentos.	Caso de ciberataque por medio de correos fraudulentos.	"Me han tratado de hacer ciberataque que se trataba de hacer un fraude que se llama Business Email Compromise a mí, donde alguien se hizo pasar por mí y en el cargo de director Ejecutivo del Cenia trató de que nuestro gerente de administración y finanzas hiciera una transferencia que estaba supuestamente ordenada por mí." "La inteligencia artificial ayuda mucho, no tanto a programar bien, como hacer correos que engañen a las personas en forma mucho más fácil. Hoy día lo pueden hacer con la misma voz de la persona, lo cual lo hace mucho más creíble, incluso se pueden hacer vídeos de

				esa persona pidiendo ayuda. No se ha visto eso en forma tan extendida como se pensó en un principio, pero sin duda son características que hacen que el tema del cibercrimen tenga cada vez más extensión y los daños sean mayores."
3	Métodos utilizados para realizar fraudes	Uso de plataformas de comunicación y phishing	Fraudes comunes incluyen phishing y suplantación de identidad a través de correos electrónicos.	"Hoy día lo que siento yo, que ocurre más común, es lo que antiguamente se llamaba el cuento del tío y para eso se utiliza mucho en las plataformas de comunicación humana. ¿Cuál es la plataforma de comunicación tradicional empresarial? El correo, phishing, spam. En donde la gente o suplanta la identidad de alguien o captura el correo de alguien y a partir de eso generan fraude"
5	Métodos utilizados para realizar fraudes	Ransomware, Phishing, ingeniería social.	Ingeniería social	"tuvimos casos en los bancos, en sistemas financieros... en el Banco Estado fue un ransomware que cifró todos los servidores del Banco para que el Banco pague un rescate y el rescate el pago es doble porque tú pagas el primer rescate para recuperar tus datos y como antes lo filtraron y tienen una copia, pagas una segunda vez para que no, no de no difundan al público, es la doble pega. El Banco de Chile fue un phishing interno que cuyo objetivo era robar plata a través del sistema de transacciones internacionales en dólares por el sistema Swift, etcétera," "El problema cuando le pasa a otra empresa, hay empresas que sí se recuperaron, hay empresas más pequeñas que tuvieron problemas de ataque por algo que se llama la ingeniería social, la ingeniería social es hacerte pasar por otra persona... en el fondo hay una usurpación por mail de algunos dominios de mail, es un poco complicado explicarlo, pero resulta una estafa final."

7	Métodos utilizados para realizar fraudes	Phishing e ingeniería social.	Archivos con links infectados que no son detectados.	"por correo mandan un Word, el cual no es detectado como amenaza porque es un archivo Word, sin embargo, dentro de este archivo viene un link infectado" "Utilizan la ingeniería social, es una técnica de manipulación a las personas, pueden hacerlo por diferentes medios, como el Phishing, el Spear Phishing que saca un perfil personalizado de la persona desde las redes sociales u otras plataformas, llamadas telefónicas y el SMS también es muy conocido"
8	Métodos utilizados para realizar fraudes	Phishing, ransomware.	Uso común en pagos digitales.	"los métodos de pago digital más comunes en general el Phishing Ransomware"
9	Métodos utilizados para realizar fraudes	Phishing por correo	Clics que activan ataques.	"A través del correo electrónico hacen clic y los atacan"
1	Otras medidas para prevenir los fraudes digitales	Factor humano	Las empresas están tomando más importancia en proteger los activos no tangibles, por ello es relevante la ciberhigiene del personal de la empresa.	"Entonces las empresas que saben, yo creo que hoy día están tomando más conciencia de la importancia de proteger los activos informáticos, que son activos, el problema es que no son tangibles" "El mayor problema que tenemos de cómo entran los ataques, es a través de la misma gente, todavía no hay una un concepto de lo que tenemos que meter mucho en la cabeza, que es lo que se llaman las ciber higiene" "¿qué es lo que es la ciber higiene? Son las normas y prácticas para manejarse frente a un computador... la gente tiene que aprender a usar y hay ciertas cosas que no tienen usar, por ejemplo, dejar abiertos los computadores cuando están trabajando y se van a tomar un café y alguien se puede meter y hacer cualquier cosa." "...ahí va generando espacios para que los potenciales ataque se produzcan. Gran parte, sino como 80 o 90% de los ciberataques tienen algún factor humano de por medio."

2	Otras medidas para prevenir los fraudes digitales	Eliminación de passwords. Factor humano	Eliminar el uso de passwords y adoptar autenticación más robusta.	"...eliminar el uso de passwords. Yo diría que eso es lo fundamental, hemos estado viendo ahora que han salido tecnologías nuevas que te permiten eliminar por completo el uso de passwords y ocupar dispositivos físicos como autenticación." "Yo diría que temas de autenticación más robusta pegan en el centro de lo que son el tema de los fraudes digitales." "...no existe un, no porque tú estés dentro de la red de la empresa eres una persona de confianza, sino que absolutamente desconfiar de todas las conexiones." "tener planificada tu red en forma segmentada, de manera que las personas que están en un lado y son usuarios no tengan acceso a los servidores que los que administran." "...hay que sumar, por supuesto, el factor humano, hay que hacer charlas de concientización, hay que hacer ensayos donde uno trata de engañar a los trabajadores de una empresa y ver cuántos caen y después analizar esa operación"
3	Otras medidas para prevenir los fraudes digitales	Formación y concientización de las personas. Factor humano	La formación y la capacitación del personal es fundamental para prevenir fraudes, ya que la tecnología sola no es suficiente	"Hacer un buen aguante, un buen campaña difusión, aumentar las capacidades de nivel de madurez de las compañías, de las organizaciones. Ese es el principal foco, por ahí yo veo que es donde está la mayor brecha y que las empresas tienen que trabajar, formación, capacitaciones, curso de inducción" "el factor humano acá es súper importante la tecnología nunca va a suplir."
4	Otras medidas para prevenir los fraudes digitales	Seguridad y colaboración	Implementación de varias medidas para asegurar la operativa continua y proteger los datos.	"tenemos varias dimensiones en las cuales manejamos condiciones que efectivamente nos permitan asegurarnos sobre la continua operativa y también asegurarnos que efectivamente estos datos no van a ser mal utilizados o evitar que sean dañados de alguna manera" "cuando empezamos a implementación hacemos piloto y en la elaboración de esas pilotos... interactuamos con los proveedores y ahí aplicamos estas condiciones, un documento, un acuerdo de confidencialidad... un alcance

				revisado por otro equipo de sistemas también validando que efectivamente las condiciones de seguridad se estén cumpliendo, y después de eso, una implementación completa, totalmente validada por los equipos de seguridad."
5	Otras medidas para prevenir los fraudes digitales	Capacitación y concientización	Capacitación del personal y concientización sobre prácticas de ciberseguridad	"un gran problema que sí a nivel de la empresa misma que la capacitación del personal, porque está bien decir que hay que hacer eso, eso, pero que, si tú no lo explicas a los empleados, si tú no lo no lo capacitas en las buenas prácticas, bueno, no sirve para nada" "Entonces el consejo, hay que prepararse, hay que informarse, hay que implementar algunas medidas que son básicas de ciberseguridad. Hay algunas cosas que son gratis, que no cuestan nada ya, tener al día el software del sistema operativo, todo el softwares que usamos, tener una política de gestión de contraseñas eficiente, no contraseñas débiles, si es que se puede implementar lo que se llama un doble factor de autenticación" "Entonces, educar, educar, capacitar a la gente en buenas prácticas mínima, eso no significa que te va a salvar del 100% de los ataques con esas esas medidas básicas, pero te va a salvar lo mejor de un 95%, lo que es mucho mejor que nada."
6	Otras medidas para prevenir los fraudes digitales	Cultura y colaboración	Inclusión organizacional	"entender la ciberseguridad como una tarea de todos los que están en su organización, y no solamente el encargado de ciberseguridad "
7	Otras medidas para prevenir los fraudes digitales	Capacitación y webinars.	Es crucial el uso de sistemas actualizados.	"Enfocarse en sus vulnerabilidades es crucial, por ejemplo, que el personal esté utilizando un computador antiguo que no tiene actualizado los sistemas de seguridad" "Programas informativos sobre ciberseguridad, recomendaciones, para que las personas tengan conocimiento y conciencia" "Realizar webinars con las personas y campañas de phishing"

8	Otras medidas para prevenir los fraudes digitales	Capacitación continua.	Confianza empresarial clave.	"es fundamental que tengamos claridad, que tenemos que trabajar en la confianza de nuestras empresas, la capacitación continua es fundamental "
9	Otras medidas para prevenir los fraudes digitales	Contraseñas robustas y antimalware	Políticas de uso adecuado	"Utilizar herramientas antimalware, como antivirus, tener segundo método de protección del sistema, como el uso de contraseñas robustas" "Políticas de seguridad para que las personas ocupen bien los sistemas "
1	Perspectivas de ciberseguridad	Preparación y resiliencia	Las empresas deben prepararse para enfrentar ciberataques mediante la implementación de sistemas de gestión de seguridad de la información y mejorando su resiliencia para recuperar servicios después de un ataque.	"ellos tienen que ir preparándose como van a enfrentar los ciberataques y para evitarlos, para enfrentar los ciberataques, la primera cosa que tienen que hacer es generar un sistema de gestión de seguridad de información." "Y segundo, tienen que velar por la resiliencia." "la resiliencia, en el fondo es la capacidad que tú tienes de volver a brindar los servicios en las condiciones que estaban antes del evento de ciberseguridad o ciberataque." "hay déficit de cultura de ciberseguridad muy grande en el país, hay déficit de especialistas, se calcula que son como 30.000 al año al año 30. O sea, hay una necesidad tremenda de especialistas de todo tipo, no solamente de desde el punto de ser programador, sino que también de entender, de administrar, de generar procedimientos de una cantidad enorme de cosas."
2	Perspectivas de ciberseguridad	Riesgo de ataque.	No hay empresa que esté 100% libre de tener un ciberataque.	"son varias las tareas que hay que hacer en forma simultánea para que el tema de ciberseguridad mejore para que el riesgo que uno tiene baje. O sea, nunca hay una empresa que esté ciento por ciento libre de tener un ciberataque." "En la medida que ocupamos computadoras y el 99,9% de las empresas sí lo hace, o que tenemos dispositivos que estén monitoreados... Entonces ahí también hay un riesgo industrial que hay que reconocer."

				"...el objetivo no es no tener riesgo. Yo diría que el objetivo es tener un riesgo lo más bajo posible"
3	Perspectivas de ciberseguridad	Tecnología y control de claves	La tecnología junto con el control adecuado es esencial para reducir los riesgos de ciberseguridad. Además de inversiones y formación.	"Por un lado, las tecnologías, toda tecnología va a tener un nivel de riesgo Pues esas brechas hoy día la manera de mirarla es ir de la mano con tecnología, pero de la mano con control, que es lo que es ciberseguridad, no es más que la exposición al riesgo o al menos cuantificarlo y disminuirlo. ¿Entonces cómo ha cambiado? Enormemente y hoy día ciberseguridad es un proceso más de la compañía, no es TI. ¿Como ha cambiado? las inversiones, los presupuestos, las tecnologías, las dotaciones, las personas, el conocimiento, la formación también es un tema reimportarte en ciberseguridad."
5	Perspectivas de ciberseguridad	Educación y cultura de ciberseguridad	Concientización y educación del personal sobre las buenas prácticas en internet y la gestión de datos personales.	"en ciberseguridad siempre se dice que la parte más débil el usuario final es el humano, de hecho, si uno piensa que la ciberseguridad se trata de resolver ese problema con tecnología, con cosas técnica y a crear un montón de cuestión, eh, la respuesta es no." "En Chile, el mayor desafío actual todavía no es algo técnico o tecnológico, lo que sea, el mayor desafío en Chile es la concientización, es decir que no existe una cultura general a nivel país y a nivel de las personas digamos, de los problemas de ciberseguridad, de las buenas prácticas en comportamiento en internet, de la gestión de contraseña, de datos personales, etcétera, etcétera." "probablemente en un futuro cercano, no muy lejano. Vamos a asistir a una especie de batalla entre la IA entre los que generan ataques y los que defienden la infraestructura tuya. Eso es lo que va a pasar, no te puedo decir en qué tiempo, porque hacer

				predicciones en ese tema es algo sumamente difíciles y todos se equivocan, pero va a llegar sí o sí"
6	Perspectivas de ciberseguridad	Requisitos y protección	Datos seguros	"la ciberseguridad va a ser un requisito para producir inteligencia artificial. Es decir, yo tengo que tener mis datos resguardados, seguros, protegerlos, porque si no la inteligencia artificial o los resultados que producen las máquinas no van a ser los óptimos ni deseados si mis datos son corruptos" "la ciberseguridad que usa la inteligencia artificial como una herramienta de gestión misma para la ciberseguridad."
7	Perspectivas de ciberseguridad	Conocimiento limitado.	Concientización como desafío clave.	"Es algo cada vez más relevante para las personas, pero no tienen conocimientos" "Uno de los mayores desafíos de la ciberseguridad, es la concientización de las personas, es un factor crucial para el futuro"
8	Perspectivas de ciberseguridad	Escasez de personal capacitado.	Evolución de amenazas constante.	"los mayores desafíos de la ciberseguridad yo creo que es la constante evolución de la amenaza, el poco personal capacitado, no tenemos mucho personal estamos al debe con profesionales en el área de ciberseguridad, y al mismo tiempo las problemáticas de integración de nuevas tecnologías." "casi el 80 al 90% de los ataques que se generan hoy día son por falta de capacitación, son por fallas de errores humanos" "es muy importante es la comunicación entre las empresas...La ciberseguridad se comparte, no se compete"
9	Perspectivas de ciberseguridad	Capacitación del personal.	Factor humano primordial.	"el factor humano es primordial, el tema de la concientización y la capacitación del personal."
1	Perspectivas en las empresas	Cultura de ciberseguridad y déficit de especialistas	Existe una gran necesidad de crear conciencia sobre la ciberseguridad y formar especialistas en	"en ciberseguridad hay una cosa que se dice, hay dos tipos de empresas en el mercado. Las que saben que la hackearon y las que no saben que las hackearon. Así de claro, la reacción va a depender del daño que sufran" "tenemos,

			el área debido a la creciente amenaza de ciberataques y la falta de cultura de ciberseguridad en las empresas.	por una parte, crear conciencia... tenemos mucho que enseñarle a la gente"
2	Perspectivas en las empresas	Preparación de las organizaciones	Organizaciones bien preparadas contra el fraude y otras que aún no se han enfrentado al problema.	"Yo diría que en general siempre hay más que las organizaciones que no han sufrido fraudes. Yo diría que hay organizaciones que están bien preparadas para el fraude y otras organizaciones que piensan que como que no les va a ocurrir y no se preparan. A las que están bien preparadas, felicitaciones, a las que no están preparadas y piensan que no les va a tocar, solamente hay que decirles de que este no es un tema que sí les va a tocar, sino que cuándo les va a tocar, cierto, y que muchas veces los ataques no ocurren de un día para otro. Los atacantes, en los casos más sofisticados, pueden estar varios meses, incluso años, dentro de las redes esperando el momento preciso donde hay más dinero en juegos o pueden sacar mayor provecho para atacar. Por lo tanto, el tema de la ciberseguridad tiene que ser un tema de educación permanente y meter la cabeza en la arena creo que no es la solución. Digamos eso es solamente te genera menos nivel de preparación del que efectivamente necesitas para proteger tus activos digitales"
3	Perspectivas en las empresas	Preparación de las empresas	Existen 2 tipos de empresas, las que han sido víctimas de fraudes y las que no se han dado cuenta de que han sido atacadas.	"hoy día existen dos tipos de empresa, las que les pasó y las que no saben qué le pasó"
4	Perspectivas en las empresas	Flexibilidad y adaptación	Tener una visión flexible, aceptar la posibilidad de equivocarse y seguir adelante	"Entonces es importante que tú tengas, o sea, a ver que los que trabajan en estos proyectos, conozcan un poco de inteligencia, porque aquí hay varias capas y que cuando conozcan un poco

				tengan la visión como para entender qué es lo que quieren hacer con ella y tengan una visión con paradigmas bastante flexibles porque hay cosas que uno cree que no se pueden hacer y sí se pueden hacer. Y también está flexibilidad de tratar de equivocarse rápido y seguir adelante rápido, como en todas las cosas."
5	Perspectivas en las empresas	Inminencia de ataques	Las empresas serán víctimas de un ataque sí o sí.	"hay un dicho en ciberseguridad que dice que la pregunta no es saber si tú vas a ser víctimas de un ataque exitoso, sino que cuándo. Esa es la pregunta, ¿cuánto tiempo más te vas a mantener sin problema? Esa es la pregunta más importante, porque si va te va a pasar, la respuesta es sí, eh solamente cuándo va a pasar"
6	Perspectivas en las empresas	Presupuesto y recursos	Percepción del gasto	"pero lo que les falta a las empresas, al menos lo que me toca ver, son áreas que son muy precarias, en general, una persona, dos personas luchando con los directorios para para que den presupuesto para el año siguiente para implementar programas, concientización, porque claro, todavía se ve como que la ciberseguridad fuera como una suerte como de inversión, no como un requisito de base para que mi empresa"
7	Perspectivas en las empresas	Presupuesto en ciberseguridad.	Preparación y respuesta esenciales.	"A nivel organizacional, es un punto clave en las empresas, destinar un presupuesto para la ciberseguridad" "las empresas no pueden esperar a que les pase, siempre deben ser preventivos, tener la capacidad de respuesta y saber qué hacer y saber hacia dónde ir"
8	Perspectivas en las empresas	Equipos pequeños.	Herramientas tecnológicas necesarias.	"la empresa en general tiene un equipo compuesto de 5 personas en el área de ciberseguridad, como mucho, por lo cual, si no utilizamos este uso de herramientas tecnológicas para poder fortalecer, créeme que no vamos a lograr nuestro objetivo"
9	Perspectivas en las empresas	Charlas y talleres.	Necesidad de CISO en grandes empresas.	" lo principal es hacer algunas charlas, ciertos talleres para poder lograr la concientización de la de las personas, porque las personas

				son relevantes." "Para las grandes empresas es necesario invertir y tener un CISO"
1	Uso de la IA para realizar fraudes	Uso de herramientas de IA para encontrar vulnerabilidades y realizar ataques.	El aumento del uso de la IA para identificar y explotar vulnerabilidades en sistemas informáticos.	"Así como tú te estás defendiendo, también los que están atacando hacen exactamente lo mismo, usan las mismas herramientas de inteligencia artificial u otras que ellos van entrenando y van buscando vulnerabilidades" "se toman los sistemas y pueden hacer lo que quieren, desde robarte información, que es bastante usual o simplemente capturar, ah, lo que se denomina un ransomware" ""algunas herramientas de inteligencia artificial, lo puedes hacer por negación de servicios, o sea empezar a pedir y los sistemas se saturan, entonces no tienen respuesta y estás bajo un ciberataque o se metieron por alguna parte, te buscaron una vulnerabilidad por un segmento de código y por ahí, por la puerta que no está protegida, por ahí se pueden meter y desarrollan un pequeño código y ese código se empieza a replicar y empieza a tomar el sistema."
2	Uso de la IA para realizar fraudes	Uso de la IA en fraudes masivos	La IA facilita la creación de fraudes masivos como correos de phishing y engaños personalizados	"Yo creo que el nivel más masivo son estos correos, que bueno, que a veces te llegan como, soy el heredero de una gran fortuna en Nigeria y quiero ocupar tu cuenta para transferir 20000000 de dólares, que uno dice que tú pides esto, pero hay mucha gente que cae y que están apuntados como al gran público... En ese nivel de fraude, que es como un micro fraude, la inteligencia artificial ayuda mucho más a la gente que hace el fraude que a la gente que lo detiene."
5	Uso de la IA para realizar fraudes	Inteligencia artificial en ciberataques	Generación de ataques y creación de códigos maliciosos	"la inteligencia artificial se usa ahora para generar ataques... los ciberdelincuentes también usan ese tipo de capacidad para generar códigos maliciosos automáticamente, para detectar automáticamente algunas fallas que existen, una infraestructura tuya o de hardware o software, etcétera." "Todos esos sistemas están entrenados con una gran

				cantidad de datos... el problema de esos entrenamientos es que la calidad de la inteligencia artificial que tú tienes al final depende muchísimo de la calidad de los datos de entrada, de los datos de entrenamiento y, por ejemplo, las que son IA generales, como chat GPT, fueron entrenar con datos también que provienen de internet, página web en todos lados." "hay un montón de datos que son, en estadística, ellos llamarían eso un poco los outliers, ese que son diferentes restos, pero que sí entran en entrenamiento y, que a veces tienen el poder entre comilla, un efecto colateral de hacer que la IA final, en algunos temas, puede o mentir o producir respuestas erróneas, ya, y ese es un gran peligro que tiene la inteligencia artificial, cómo ser capaz de controlar la seguridad de los datos de entrada, en términos de claridad, de dónde vienen, de cuál es digamos la certeza de esos datos para entender a alguien"
6	Uso de la IA para realizar fraudes	Amenazas y técnicas	Riesgos avanzados	"la inteligencia artificial también puede ser una amenaza para la ciberseguridad en la medida que son también técnicas que puede ser utilizada de manera de mala forma por una persona. "
7	Uso de la IA para realizar fraudes	Campañas personalizadas.	Avance rápido de ataques con IA.	"Los ataques están avanzando muy rápido con el uso de la IA, la están usando mucho, por ejemplo, podrían lanzar una campaña de Phishing gigantesca y más personalizada que antes"
8	Uso de la IA para realizar fraudes	Ataques sofisticados.	Falta de recursos humanos.	"los actores maliciosos, en este caso los delincuentes utilizan estas técnicas para desarrollar ataques más sofisticados. Recuerda que detrás de cada ataque no hay solamente una persona, hay un centenar de personas que hoy día están generando ataque constantemente en la infraestructura y hoy día nuestra empresa tampoco tienen mucho capital humano para poder de alguna manera de defenderse "
9	Uso de la IA para realizar fraudes	Herramientas accesibles.	Hackers sin necesidad de	"los hackers están utilizando esas herramientas y hay un montón de herramientas que se pueden hacer

			programación avanzada.	fácil sin necesariamente tener conocimiento avanzado en programación"
--	--	--	------------------------	---

Bibliografía

A. M Turing. (1950). *COMPUTING MACHINERY AND INTELLIGENCE*.

ACFE. (2002). *Report to the nation occupational fraud and abuse*.

Achavar, V. B., & Cárdenas, A. V. (s. f.). *Convenio sobre la Ciberdelincuencia: Convenio de Budapest*.

Alazab, M., Rm, S. P., M, P., Maddikunta, P. K. R., Gadekallu, T. R., & Pham, Q.-V.

(2022). Federated Learning for Cybersecurity: Concepts, Challenges, and Future Directions. *IEEE Transactions on Industrial Informatics*, 18(5), 3501–3509.

<https://doi.org/10.1109/TII.2021.3119038>

Almeida, M. P. S.-B. (2009). *Classification for Fraud Detection with Social Network Analysis*.

Bank for International Settlements. (2023). *Digital fraud and banking: Supervisory and financial stability implications*.

Capuano, N., Fenza, G., Loia, V., & Stanzione, C. (2022). Explainable Artificial Intelligence in CyberSecurity: A Survey. *IEEE Access*, 10, 93575–93600.

<https://doi.org/10.1109/ACCESS.2022.3204171>

Cibercrimen. (s. f.). Recuperado 2 de mayo de 2024, de

<https://www.pdichile.cl/instituci%C3%B3n/unidades/cibercrimen>

CISCO. (2018). *Anual Cybersecurity Report*.

Cybersecurity Ventures. (2019). *2019 Official Annual Cybercrime Report*.

ENISA. (2020a). *Ransomware*.

ENISA. (2020b). *Web-based attacks*.

Ezer Osei Yeboah-Boateng & Priscilla Mateko Amanor. (2014). *Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices*.

F53e86_entrevistapdfcopy.pdf. (s. f.). Recuperado 12 de julio de 2024, de

http://www2.uca.edu.sv/mcp/media/archivo/f53e86_entrevistapdfcopy.pdf

IBM. (2024). *What is Ransomware?* | IBM. <https://www.ibm.com/topics/ransomware>

Interpol. (2022). *Informe Anual 2022*. 20.

https://www.interpol.int/es/content/download/19843/file/INTERPOL%20%20Annual%20Report%202022_SP.pdf

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity.

Journal of Computer and System Sciences, 80(5), 973–993.

<https://doi.org/10.1016/j.jcss.2014.02.005>

John McCarthy, Marvin L. Minsky, Nathaniel Rochester, & Claude E. Shannon. (1955). A

Proposal for the Dartmouth Summer Research Project on Artificial Intelligence.

Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P.-E., He-Guelton, L., &

Caelen, O. (2018). Sequence classification for credit-card fraud detection. *Expert Systems with Applications*, 100, 234–245.

<https://doi.org/10.1016/j.eswa.2018.01.037>

Kotsiopoulos, T., Sarigiannidis, P., Ioannidis, D., & Tzovaras, D. (2021). Machine

Learning and Deep Learning in smart manufacturing: The Smart Grid paradigm.

Computer Science Review, 40, 100341.

<https://doi.org/10.1016/j.cosrev.2020.100341>

McCarthy, J. (s. f.). *WHAT IS ARTIFICIAL INTELLIGENCE?*

- Mishra, S., & Soni, D. (2020). Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis. *Future Generation Computer Systems*, 108, 803–815. <https://doi.org/10.1016/j.future.2020.03.021>
- Nacional, B. del C. (2022, junio 20). *Biblioteca del Congreso Nacional | Ley Chile*. www.bcn.cl/leychile. <https://www.bcn.cl/leychile>
- Nacional, B. del C. (2024, abril 8). *Biblioteca del Congreso Nacional | Ley Chile*. www.bcn.cl/leychile. <https://www.bcn.cl/leychile>
- Panos Alexopoulos, Kostas Kafentzis, Xanthi Benetou, Tassos Tagaris, & Panos Georgolios. (2007). TOWARDS A GENERIC FRAUD ONTOLOGY IN E-GOVERNMENT: *Proceedings of the Second International Conference on E-Business*, 269–276. <https://doi.org/10.5220/0002112602690276>
- Sanchez, M. (2005). *La metodología en la investigación cualitativa*. <https://repositorio.flacsoandes.edu.ec/bitstream/10469/7413/1/REXTN-MS01-08-Sanchez.pdf>
- Truong, T. C., Diep, Q. B., & Zelinka, I. (2020). Artificial Intelligence in the Cyber Domain: Offense and Defense. *Symmetry*, 12(3), Article 3. <https://doi.org/10.3390/sym12030410>
- Wazid, M., Das, A. K., Chamola, V., & Park, Y. (2022a). Uniting cyber security and machine learning: Advantages, challenges and future research. *ICT Express*, 8(3), 313–321. <https://doi.org/10.1016/j.icte.2022.04.007>
- Wazid, M., Das, A. K., Chamola, V., & Park, Y. (2022b). Uniting cyber security and machine learning: Advantages, challenges and future research. *ICT Express*, 8(3), 313–321. <https://doi.org/10.1016/j.icte.2022.04.007>

West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security*, 57, 47–66.

<https://doi.org/10.1016/j.cose.2015.09.005>

Zscaler. (2022). *Informe sobre el phishing 2022*.