Oscar Moratto
Colombia

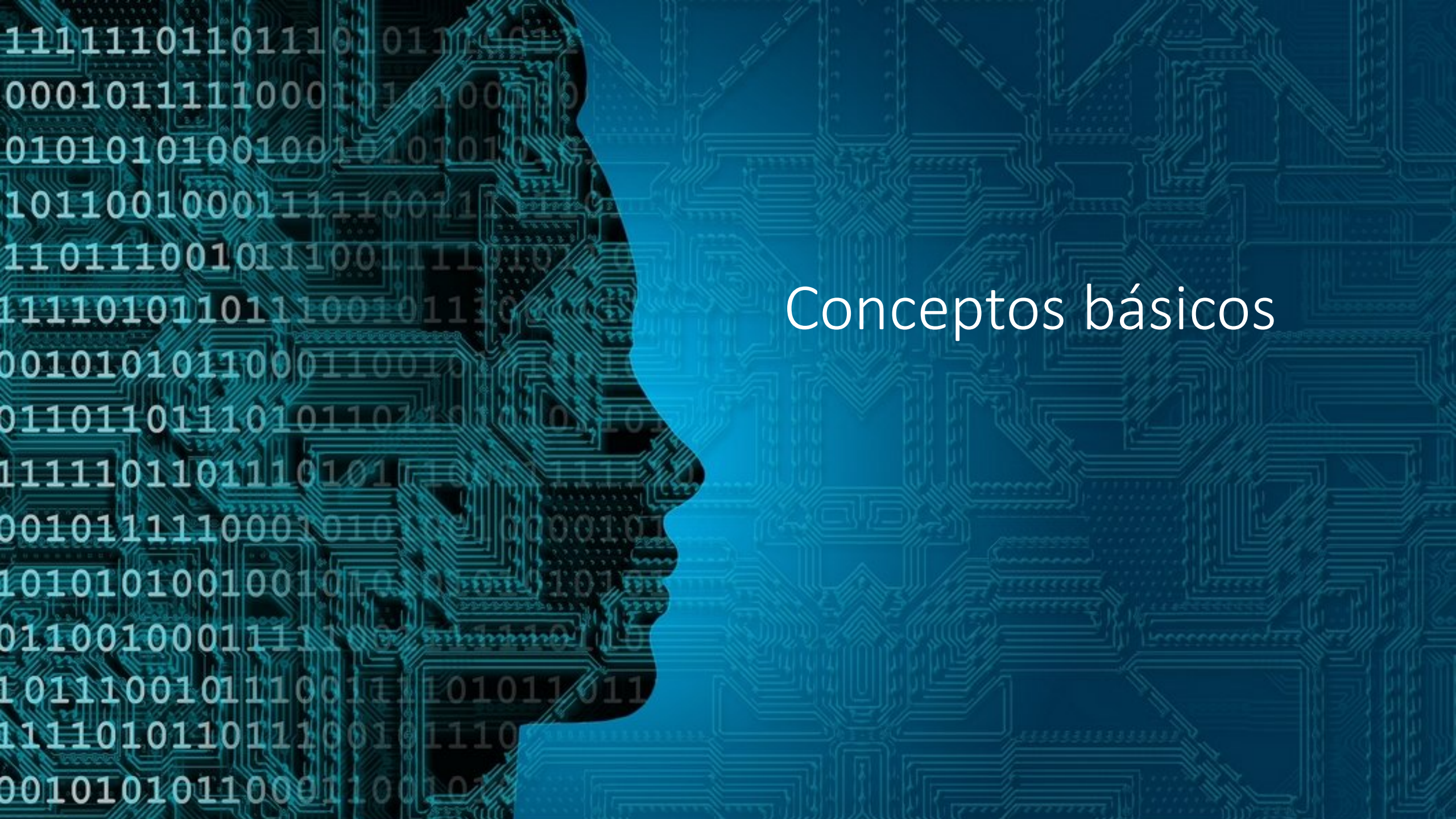
Roy Gava
Suiza

Gonzalo Vila
Argentina

Taller: Aplicación de Machine Learning e Inteligencia Artificial para la gestión de factores de riesgo

Agenda

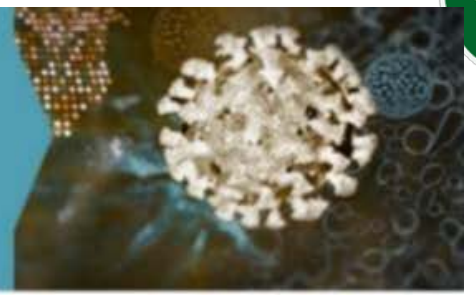
Tema	Observaciones
Introducción	Qué es la inteligencia artificial? IA, Machine Learning, Deep Learning ML: aprendizaje supervisado, aprendizaje no supervisado, aprendizaje por refuerzo La importancia de la IA en las labores de cumplimiento Limitaciones de la IA : ataques adversos, profundización de sesgos, etc.
Machine Learning: Aprendizaje No Supervisado	Que los asistentes comprendan en qué consiste el aprendizaje no supervisado Taller: https://www.naftaliharris.com/blog/visualizing-k-means-clustering/ https://www.naftaliharris.com/blog/visualizing-dbscan-clustering/
Usos de aprendizaje no supervisado en cumplimiento y antifraude	Presentar distintos casos de uso de aprendizaje no supervisado en cumplimiento (p.e. segmentación, clusterización de transacciones, clusterización de wallets crypto) y en antifraude (detección de operaciones anormales, NLP, etc.)
Break	
Machine Learning: Aprendizaje Supervisado	Que los asistentes comprendan en qué consiste el aprendizaje supervisado Taller entrenar un modelo de imágenes: https://teachablemachine.withgoogle.com/train/image
Usos de aprendizaje supervisado en cumplimiento y antifraude	Presentar distintos casos de uso de aprendizaje supervisado en cumplimiento (p.e. clasificación de alertas - triage, reconocimiento de texto - onboarding digital, reconocimiento facial - onboarging digital) y en antifraude (evaluación de riesgo de clientes - p.e teniendo en cuenta información de redes sociales, bureaus de crédito, etc.)
LLM (chatGTP y otros)	Entender cómo funciona un modelo LLM Taller: Uso de modelos LLM para generacion de imágenes para perfiles falsos en redes sociales https://boredhumans.com/text-to-image.php
Usos antieticos de IA	Presentar distintos usos antiéticos e ilegales de IA Deepfakes, fraude de voz, etc Dilemas éticos de uso de tecnología



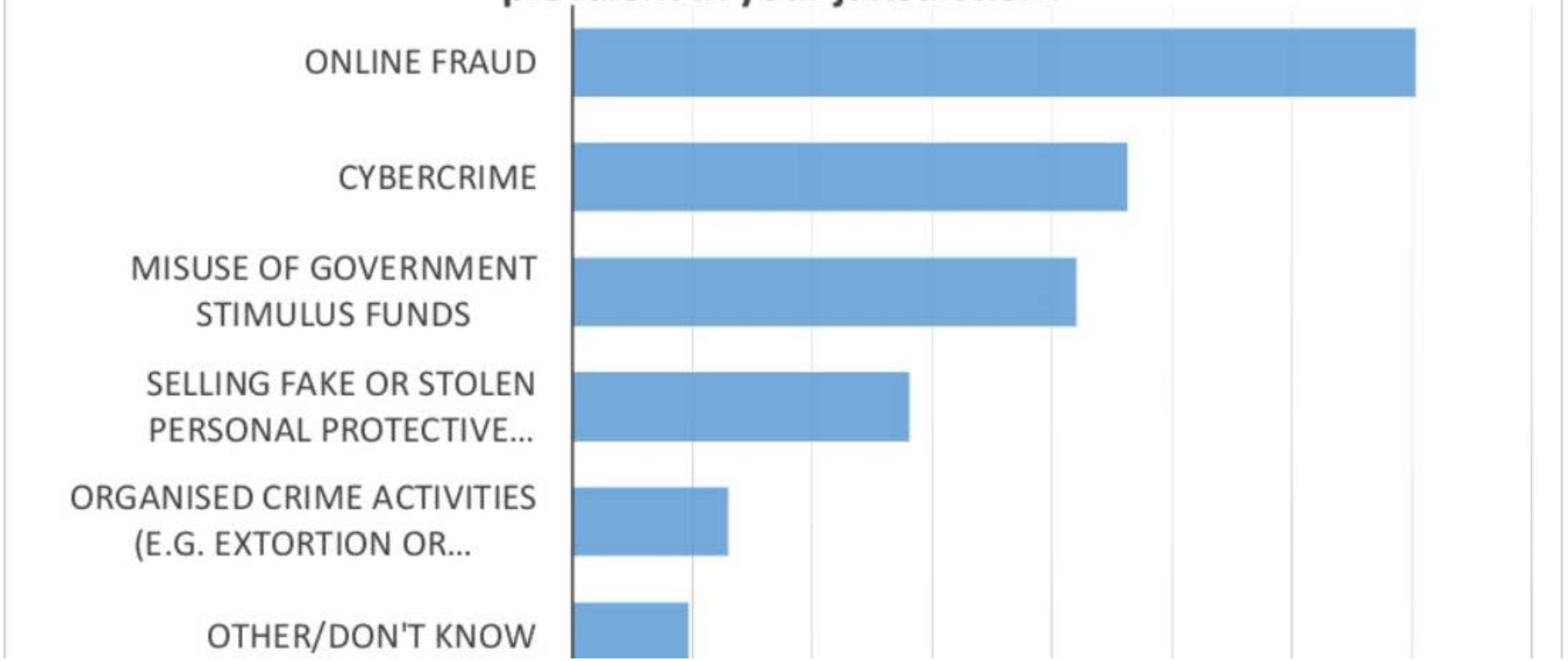
Conceptos básicos

FATF

COVID-19 and the Changing Money Laundering and Terrorist Financing Risk Landscape



Which COVID-19 related crime do you think has been the most prevalent in your jurisdiction?



FATF webinar slides on the Impact of COVID-19 on the Detection of Money Laundering & Terrorist Financing

The Impact of COVID-19 on the Detection of Money Laundering & Terrorist Financing

Poll results question 1

1. As a result of the COVID-19 pandemic, what do you think are the biggest challenge(s) facing the private sector and public authorities when detecting money laundering and terrorist financing? Choose one or more of the following. (Multiple choice)

Remote working or staff absences affecting capacity	(250/674) 37%
Decreased prioritisation of anti-money laundering due to economic downturn	(235/674) 35%
Changing financial profile of individuals and companies, making it harder to detect anomalies	(260/674) 39%
Changing behaviour of individuals and companies due to increase in online activity	(369/674) 55%
New or emerging money laundering risks	(340/674) 50%

FATF

The Impact of COVID-19 on the Detection of Money Laundering & Terrorist Financing

Poll results question 3

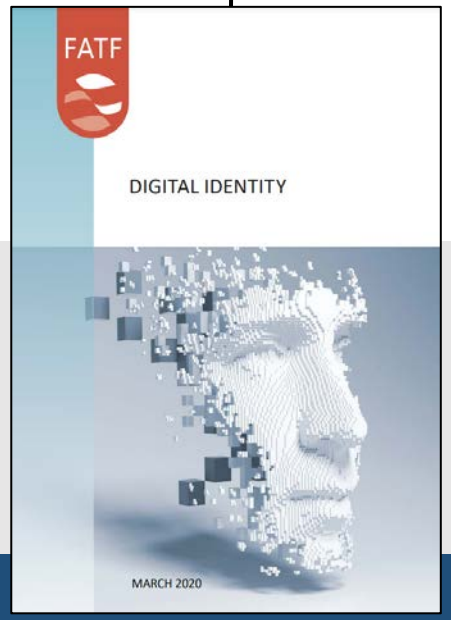
1. What do you think the longer-term consequences of the pandemic might be on tackling money laundering and terrorist financing, for both the private sector and public authorities? Choose one or more of the following. (Multiple choice)

Need for better adaptability of tools used to detect money laundering and terrorist financing	(391/610) 64%
The increase in use of digital tools	(387/610) 63%
Economic downturn leading to long-term decrease in prioritisation of anti-money laundering and counter terrorist financing	(117/610) 19%
Economic downturn leading to increased prioritisation of anti-money laundering and counter terrorist financing by governments in order to recover the proceeds of crime	(152/610) 25%
Need for better public and private sector coordination and sharing of information in order to respond to significant events	(454/610) 74%

Documentos del GAFI

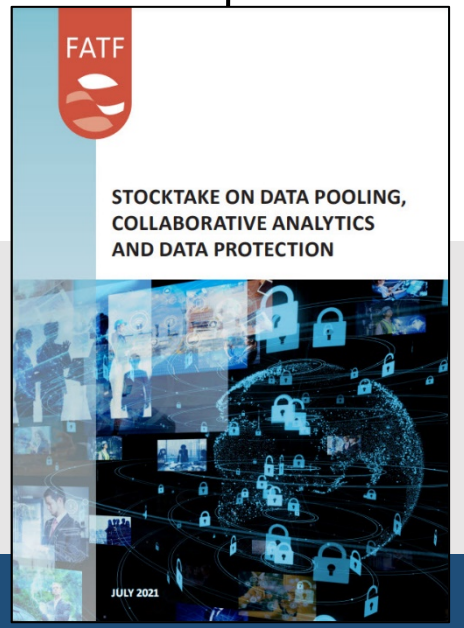
Reporte de los Ministros de Finanzas y Gobernadores de Bancos Centrales del G20 Sobre las Llamadas Monedas Estables

Identidad Digital

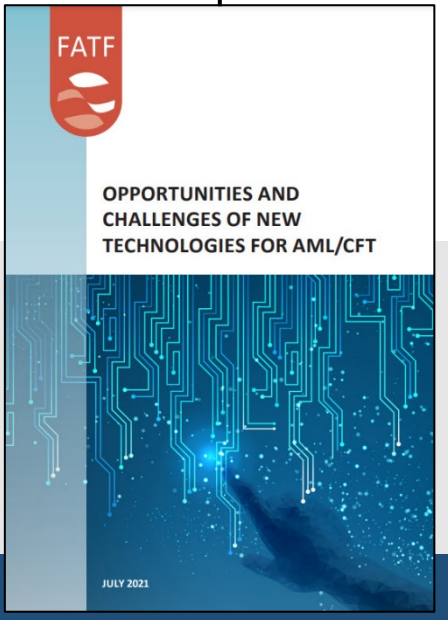


Activos Virtuales y Proveedores de Activos Virtuales

Balance Sobre Datos Comunes, Análisis Colaborativo y la Protección de los Datos



Oportunidades y Desafíos de las Nuevas Tecnologías para el ALD/CFT



TÉCNICAS COMUNES

SISTEMA DE PREVENCIÓN

XI Congreso de Prevención de Lavado de activos de las Américas

CPLDFT 11 CPLDAMERICAS.COM 2023

EVALUACION DE CUMPLIMIENTO NORMATIVO » EVALUACIÓN DE EFECTIVIDAD Y CALIDAD DEL SISTEMA

PROGRAMA DE PREVENCIÓN

PILARES

HERRAMIENTAS DE GESTIÓN DE RIESGOS

ESTRUCTURA DE CONTROL Y GOBIERNO CORPORATIVO

PROCEDIMIENTOS DE DEBIDA DILIGENCIA

SISTEMA DE MONITOREO Y REPORTE DE OP.SOSPECHOSA

1°
- MATRIZ RIESGO ENTIDAD
- MATRIZ RIESGO CLIENTE
- MATRIZ RIESGO TERCERAS PARTES

2°
- AREA DE CONTROL – COMPLIANCE INTEGRAL
- NORMAS/MANUALES INTERNOS
- EVALUACION PERIODICA DEL SISTEMA DE PREVENCION

3°
- ONBOARDING DIGITAL – ALTAS NO PRESENCIALES
- IDENTIFICACIÓN Y REQUERIMIENTO DE INFORMACIÓN EN VIRTUD DEL RIESGO
- BIG DATA – INTELIGENCIA ARTIFICIAL BÚSQUEDA FUENTES PUBLICAS

4°
- PERFIL OPERATIVO – TRANSACCIONAL – PROSPECTIVO
- ALERTAS AUTOMATIZADAS
- REPORTES SISTEMÁTICOS DE INFORMACIÓN
- CALIDAD EN LOS REPORTES DE OPERACIONES SOSPECHOSAS

FLUJOS DE FONDOS ILICITOS

EVASION FISCAL
USD 3.2 BILLONES

FRAUDE
USD 4.7 BILLONES

CORRUPCION
USD 2.6 BILLONES

SOBORNO
USD 2.5 BILLONES

CIBERDELITOS
USD 6 BILLONES

CRIMEN ORGANIZADO
USD 1.6 BILLONES

USD 2.7 BILLONES

- CONTRABANDO FALSIFICACIÓN
- TRAFICO DE DROGAS
- TRAFICO DE MIGRANTES
- TRAFICO ILEGAL DE ORGANOS
- TALA ILEGAL
- TRAFICO HUMANO
- MINERIA ILEGAL
- PESCA ILEGAL
- COMERCIO ILEGAL DE VIDA SILVESTRE
- ROBO DE PETROLEO CRUDO
- TRAFICO DE PROPIEDAD CULTURAL

2018

USD 11.6 BILLONES

VS.

2022

USD 21.7 BILLONES

CONVERGENCIA
DELITOS FINANCIEROS

XI Congreso de Prevención de Lavado de activos de las Américas

FRAUDE

ACFE™ Association of Certified Fraud Examiners

ANALIZA EL COSTO, LAS VICTIMAS, LAS INDUSTRIAS OBJETO DE FRAUDE

2504

CASOS DE FRAUDES EVALUADOS

125

JURISDICCIONES

PERDIDA PROMEDIO POR CASO ESTUDIADO DE FRAUDE

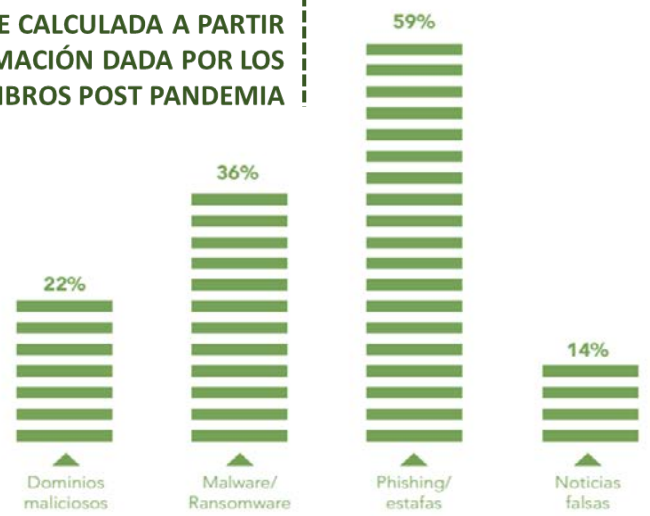
USD 1.509.000

EL 5% DE LOS INGRESOS DE CADA EMPRESA SE PIERDEN POR FRAUDE.

CIBERDELITOS

ENCUESTA MUNDIAL DE INTERPOL SOBRE CIBERDELINCUENCIA DISTRIBUCIÓN POR REGIONES DE LOS PAÍSES QUE HAN RESPONDIDO

PROPORCIÓN DE LAS PRINCIPALES CIBERAMENAZAS VINCULADAS CON EL DELITO DE FRAUDE CALCULADA A PARTIR DE LA INFORMACIÓN DADA POR LOS PAÍSES MIEMBROS POST PANDEMIA



COSTO CIBERCRIME

U$S 10.5 BILLONES ANUALES

2025

UNITED STATES DEPARTMENT OF THE TREASURY

FinCEN

FINANCIAL CRIMES ENFORCEMENT NETWORK

The proliferation of cyber-events and cyber-enabled crime represents a significant threat to consumers and the U.S. financial system. The Financial Crimes Enforcement Network (FinCEN) issues this advisory to assist financial institutions in understanding their Bank Secrecy Act (BSA) obligations regarding cyber-events and cyber-enabled crime. This advisory also highlights how BSA reporting helps U.S. authorities combat cyber-events and cyber-enabled crime.

Through this advisory FinCEN advises financial institutions on:

I. Reporting cyber-enabled crime and cyber-events through Suspicious Activity Reports (SARs);

II. Including relevant and available cyber-related information (e.g., Internet Protocol (IP) addresses with timestamps, virtual-wallet information, device identifiers) in SARs;

III. Collaborating between BSA/Anti-Money Laundering (AML) units and in-house cybersecurity units to identify suspicious activity; and

IV. Sharing information, including cyber-related information, among financial institutions to guard against and report money laundering, terrorism financing, and cyber-enabled crime.

This Advisory should be shared with:

- *Cybersecurity units*
- *Network administrators*
- *Risk departments*
- *Fraud prevention units*
- *BSA/AML management*
- *AML intelligence units*
- *AML analysts/investigators*

For the purpose of this advisory:[1]

Cyber-Event: An attempt to compromise or gain unauthorized electronic access to electronic systems, services, resources, or information.

Cyber-Enabled Crime: Illegal activities (e.g., fraud, money laundering, identity theft) carried out or facilitated by electronic systems and devices, such as networks and computers.

- Debe presentar un ROS incluso si el ciber evento no es exitoso (basta con solo saber, sospechar o tener motivos para sospechar que el ciber evento tenía la intención o podía afectar una transacción a través de la institución financiera)
- Las unidades ALD/CFT no tienen la obligación de contar con personal / sistemas dedicados a la ciberseguridad
- Las unidades ALD/CFT no tienen la obligación de tener conocimiento en ciberseguridad pero deben trabajar en colaboración con la unidad ciberseguridad
- Los sujetos obligados pueden compartir información sobre ciber eventos entre ellas

ackers robaron US$10 millones en atac Banco de Chile

so sería el mayor **ciberataque** sufrido por un banco chileno, y se suma a otros contra uciones financieras en la región y el mundo

Mexican Banks Suffer Un

Seguro | https://www.pymnts.com/news/security-and-risk/2018/mexican-banks-cybersecurity-cyberattack-spei/

PYMNTS.com

SECTIONS TODAY'S NEWS RETAIL B2B OPINION INDEXES TRACKERS PYMNTSLIVE PAY-OLOGY RESOURCE CENTER

SECURITY & FRAUD

Five Or More Mexican Banks Suffer Unauthorized Transfers

By PYMNTS

Posted on May 14, 2018

TRENDING RIGHT NOW

APPLE

Apple Close To $1 Trillion In M
With Amazon Close Behind

SECURITY & FRAUD

Credit Card Data Stolen In Chil
Attack

https://www.pymnts.com/apple/2018/apple-amazon-stock-one-trillion-retail/

Desktop Libraries ES

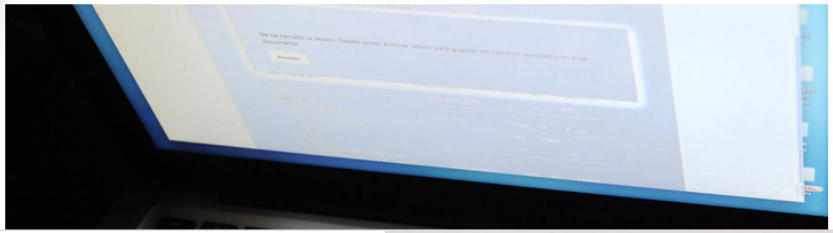
Servicios

Conti usó a Costa Rica para crear nuevos grupos de ‘hackers’

País fue prueba de banda criminal para un proceso de reestructuración interna; el fin principal no era obtener dinero con la extorsión, según analistas en ciber

Por José Andrés Céspedes

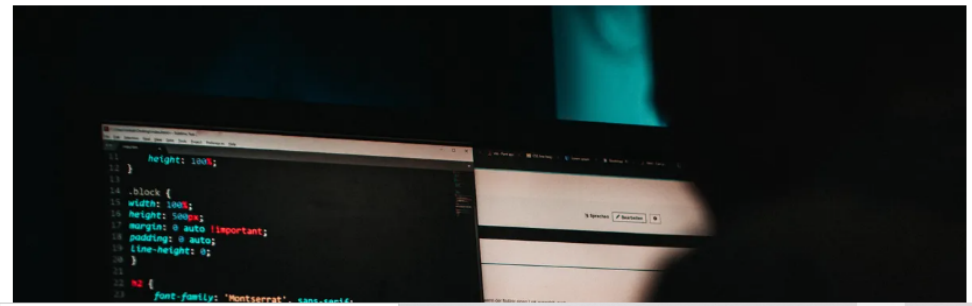
18 de julio 2022, 12:34 PM



Tecnología & Innovación

Conti, el ciberataque que puso en aprietos a Costa Rica y amenaza con expandirse a los gobiernos de A. Latina

El grupo ruso que se especializa en vulnerar plataformas públicas, secuestrando datos y sistemas, obligó a declarar el Estado de Emergencia en Costa Rica. Expertos advierten que este puede ser solo uno de muchos otros ataques a entidades oficiales de países como Perú, Chile y México, entre otros.



Tipos de ciberataques

- Advanced Fee
- Business Email Compromise (BEC)
- Botnet
- Confidence/Romance Fraud - Fraude de confianza/romance
- Credit Card Fraud/Check Fraud - Fraude con tarjeta de crédito/fraude con cheque
- Crimes Against Children - Delitos contra los niños
- Data Breach - Violación de datos
- Employment - Empleo
- Extortion – Extorsión
- Government Impersonation - Suplantación de identidad del gobierno
- Harassment/Stalking - Acoso
- Identity Theft – Robo de identidad
- Investment – Inversión
- Lottery/Sweepstakes/Inheritance - Lotería/Sorteo/Herencia
- Malware – Software Malicioso
- Non-Payment/Non-Delivery - Falta de pago/falta de entrega
- Overpayment - Sobrepago
- Personal Data Breach - Violación de datos personales
- Phishing
- Ransomware
- Real Estate- -Bienes Raíces
- SIM Swap - Intercambio de SIM
- Spoofing - Suplantación de identidad
- Tech Support – Soporte Técnico
- Threats of Violence - Amenazas de violencia

Hola @VisaArgentina necesito desconocer un cargo que no me corresponde, hace semanas que llamo y no me atienden, tampoco me responden por mail. Pueden comunicarse conmigo?

13:36 · 31/1/22 · Twitter Web App

1 Me gusta

Visa Argentina 🇦🇷 @visachattar · 2h

En respuesta a @delosmechi

Buenas tardes👋 Bienvenidos al Centro de Atención Virtual 📱 de Visa Argentina🇦🇷 Ante cualquier reclamó, duda o Inconveniente sobre Nuestros Servicios o Productos💳, Déjanos un Número Alternativo de Línea📲 para que un Asesor/a, Tomé la Comunicación

Twittea tu respuesta

Ciberseguridad en las finanzas 4.0

UCA ESCUELA DE NEGOCIOS
Facultad de Ciencias Económicas

UCA ESCUELA DE NEGOCIOS
Facultad de Ciencias Económicas

Confianza

Los delincuentes se aprovechan de la naturaleza humana y la hacen jugar en contra

Ciberseguridad en las finanzas 4.0

UCA ESCUELA DE NEGOCIOS
Facultad de Ciencias Económicas

Ciberseguridad en las finanzas 4.0

UCA ESCUELA DE NEGOCIOS
Ciencias Económicas

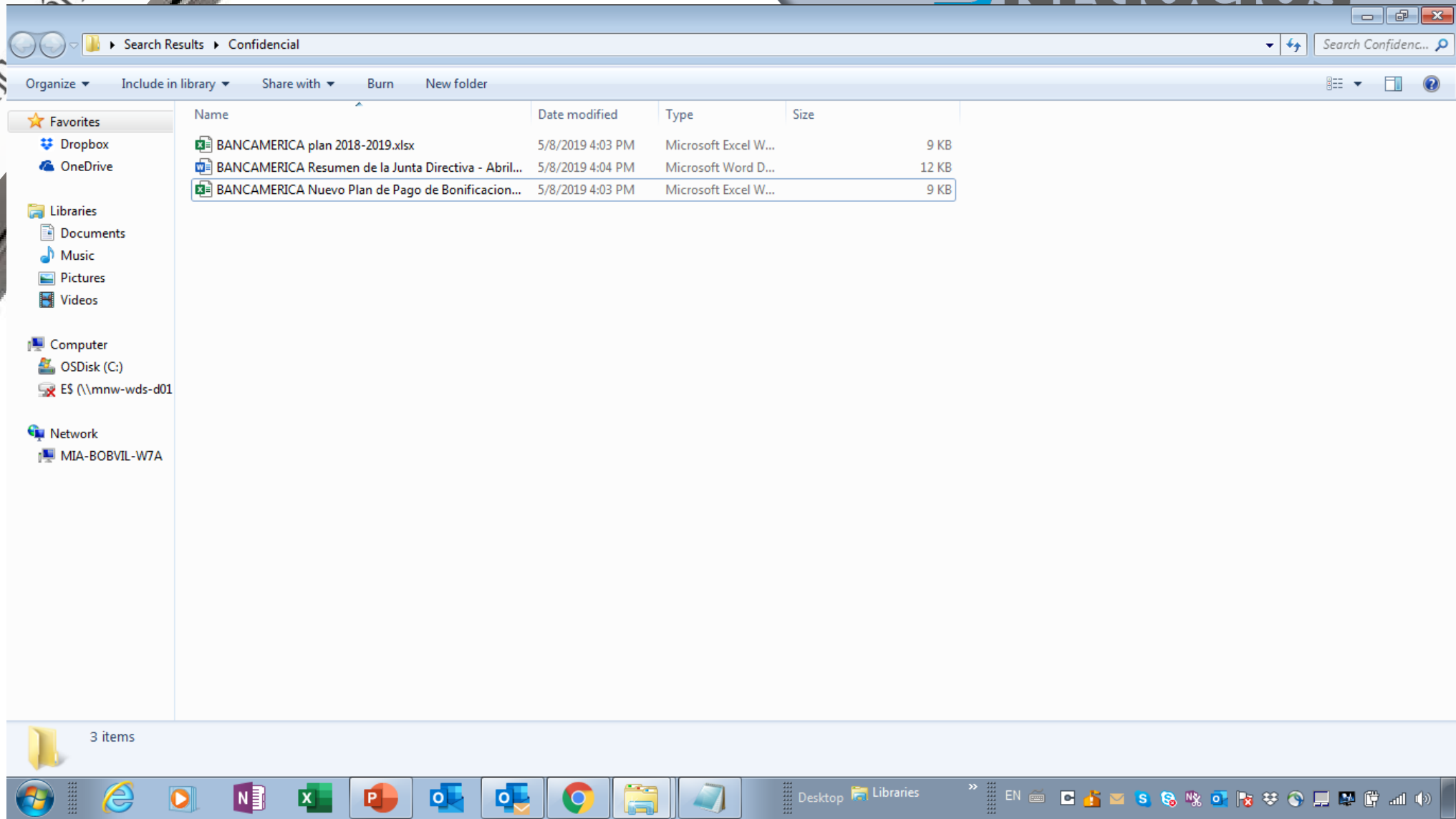
Ciberseguridad en las finanzas 4.0

UCA ESCUELA DE NEGOCIOS
Facultad de Ciencias Económicas

Ciberseguridad en las finanzas 4.0

UCA ESCUELA DE NEGOCIOS
Facultad de Ciencias Económicas

UCA ESCUELA DE NEGOCIOS

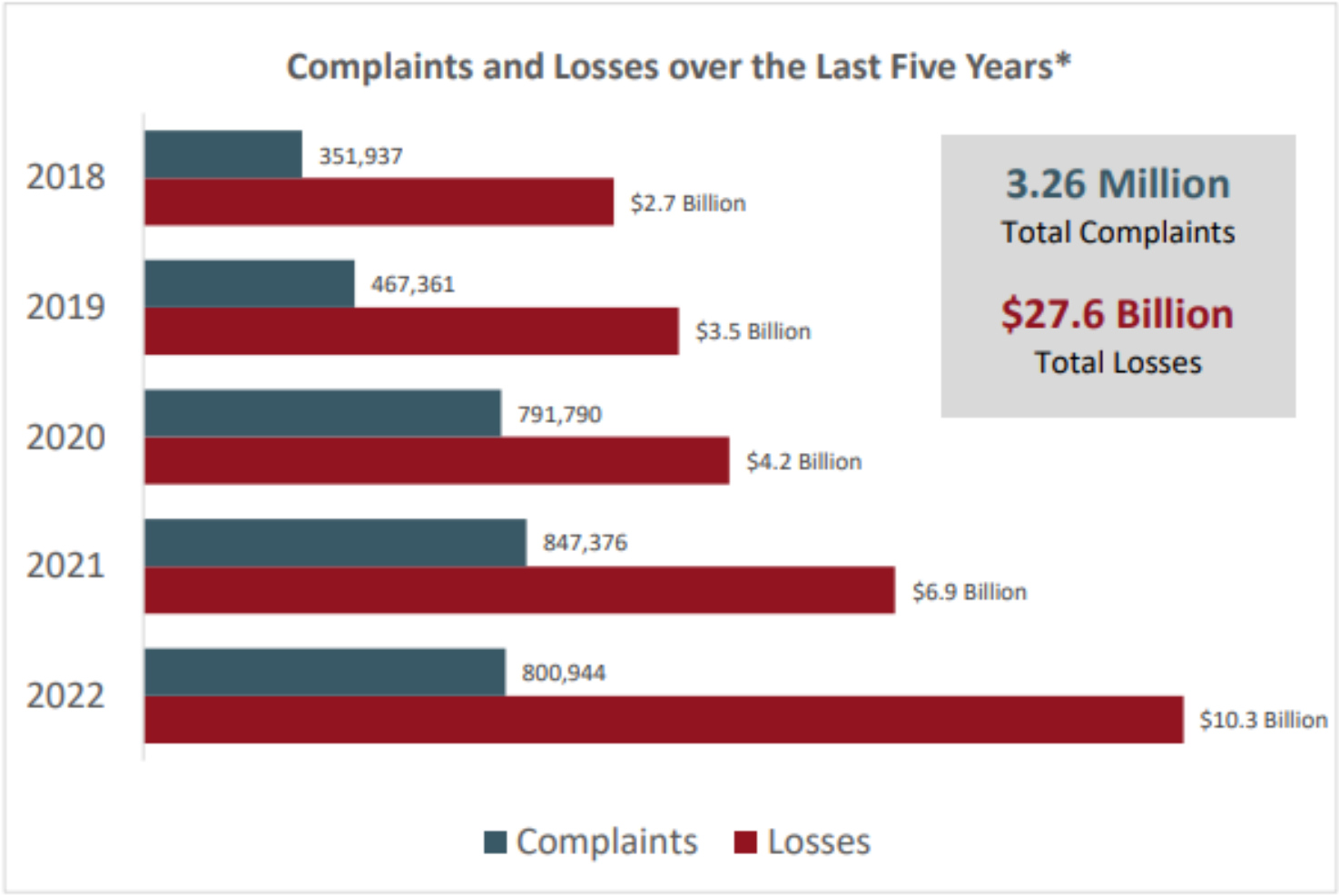



FEDERAL BUREAU of INVESTIGATION
Internet Crime Report
2022
INTERNET CRIME COMPLAINT CENTER

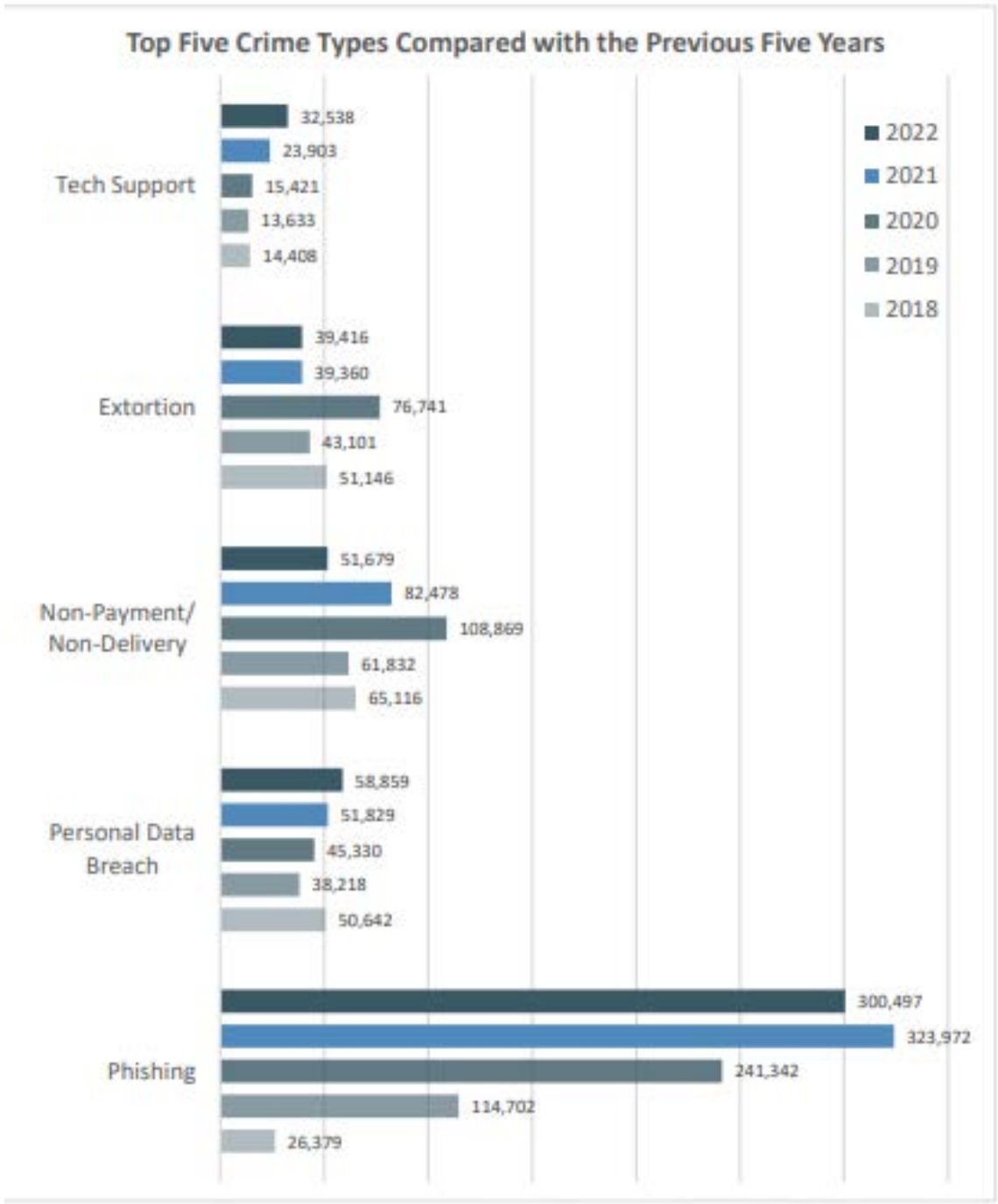
En los últimos cinco años, el IC3 ha recibido un promedio de 652.000 denuncias al año. Estas quejas abordan una amplia gama de estafas por Internet que afectan a las víctimas en todo el mundo.

LAST FIVE YEARS

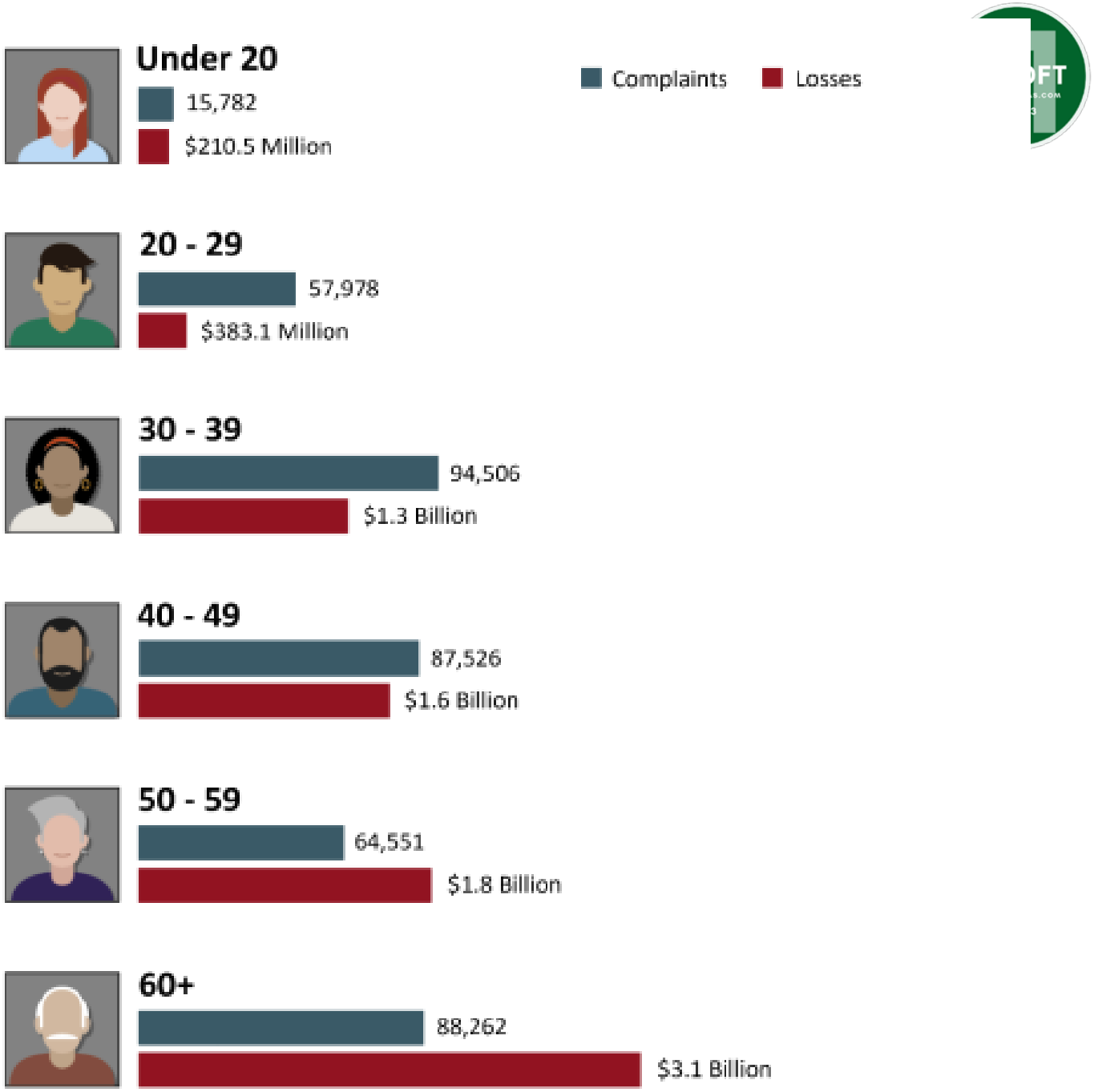
Over the last five years, the IC3 has received an average of 652,000 complaints per year. These complaints address a wide array of Internet scams affecting victims across the globe.[3]



Los 5 delitos principales en comparación con los cinco años anteriores

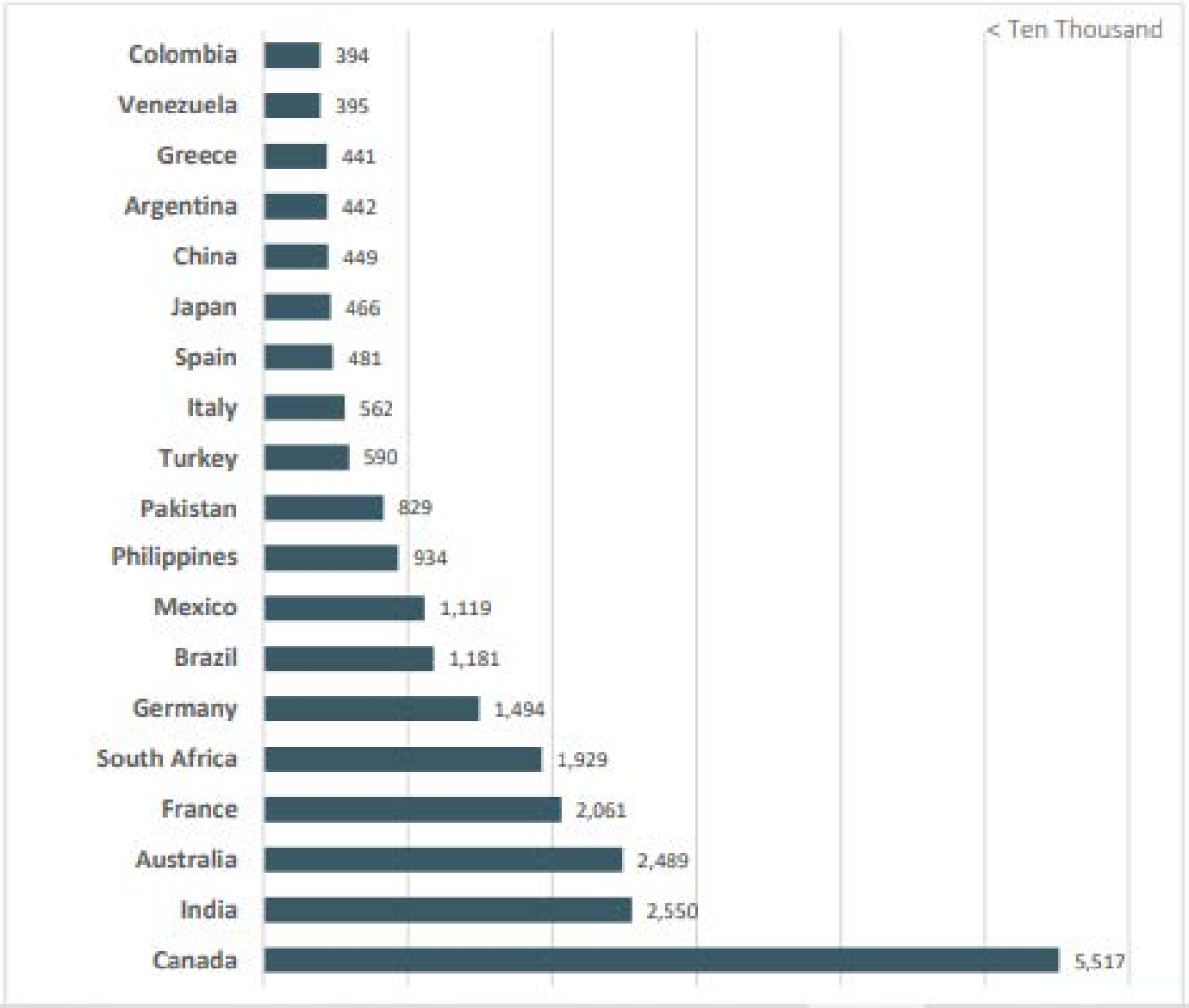


Víctimas por rango etario en 2022



2022 - TOP 20 INTERNATIONAL VICTIM COUNTRIES[18]

Compared to the United States



BUSINESS EMAIL COMPROMISE (BEC) En 2022, el IC3 recibió 22.000 denuncias por Business Email Compromise (BEC)/ Email Account Compromise (EAC) con pérdidas de casi US$ 2.700 millones.

BEC es una estafa sofisticada dirigida tanto a empresas como a personas que realizan transferencias de fondos. La estafa se lleva a cabo con frecuencia cuando un sujeto compromete cuentas de correo electrónico comerciales legítimas mediante ingeniería social o técnicas de intrusión informática para realizar transferencias de fondos no autorizadas.

La pandemia de COVID-19 y las restricciones a las reuniones presenciales provocaron aumentos en las prácticas de teletrabajo o comunicación virtual. Estas prácticas de trabajo y comunicación continuaron en 2022, y el IC3 ha observado el surgimiento de esquemas BEC/EAC más nuevos que explotan esta **dependencia de las reuniones virtuales** para instruir a las víctimas para que envíen transferencias electrónicas fraudulentas. Lo hacen al comprometer el correo electrónico de un empleador o director financiero, como un CEO o CFO, que luego se usaría para solicitar a los empleados que participen en plataformas de reuniones virtuales. En esas reuniones, el estafador **insertaría una imagen fija del CEO sin audio, o un audio "falso" a través del cual los estafadores, actuando como ejecutivos de negocios, afirmarían que su audio/video no funcionaba correctamente**. Luego, los estafadores usarían las plataformas de reuniones virtuales para instruir directamente a los empleados para que inicien transferencias electrónicas o usarían el correo electrónico comprometido de los ejecutivos para proporcionar instrucciones

RANSOMWARE (SECUESTRO DE DATOS)

En 2022, el IC3 recibió 2.385 denuncias identificadas como ransomware con pérdidas de más de US$34 millones. El ransomware es un tipo de software malicioso, o malware, que cifra los datos en una computadora, dejándola inutilizable. Un ciberdelincuente malintencionado retiene los datos como rehenes hasta que se paga el rescate. Si no se paga el rescate, los datos de la víctima no estarán disponibles. Los ciberdelincuentes también pueden presionar a las víctimas para que paguen el rescate amenazando con destruir los datos de la víctima o con revelarlos al público.

Aunque los ciberdelincuentes usan una variedad de técnicas para infectar a las víctimas con ransomware, los correos electrónicos de phishing, la explotación del Protocolo de Escritorio Remoto (RDP) y la explotación de vulnerabilidades de software siguieron siendo los tres principales vectores de infección iniciales para los incidentes de ransomware informados al IC3. Una vez que un actor de amenazas de ransomware obtiene la ejecución del código en un dispositivo o acceso a la red, puede implementar el ransomware.

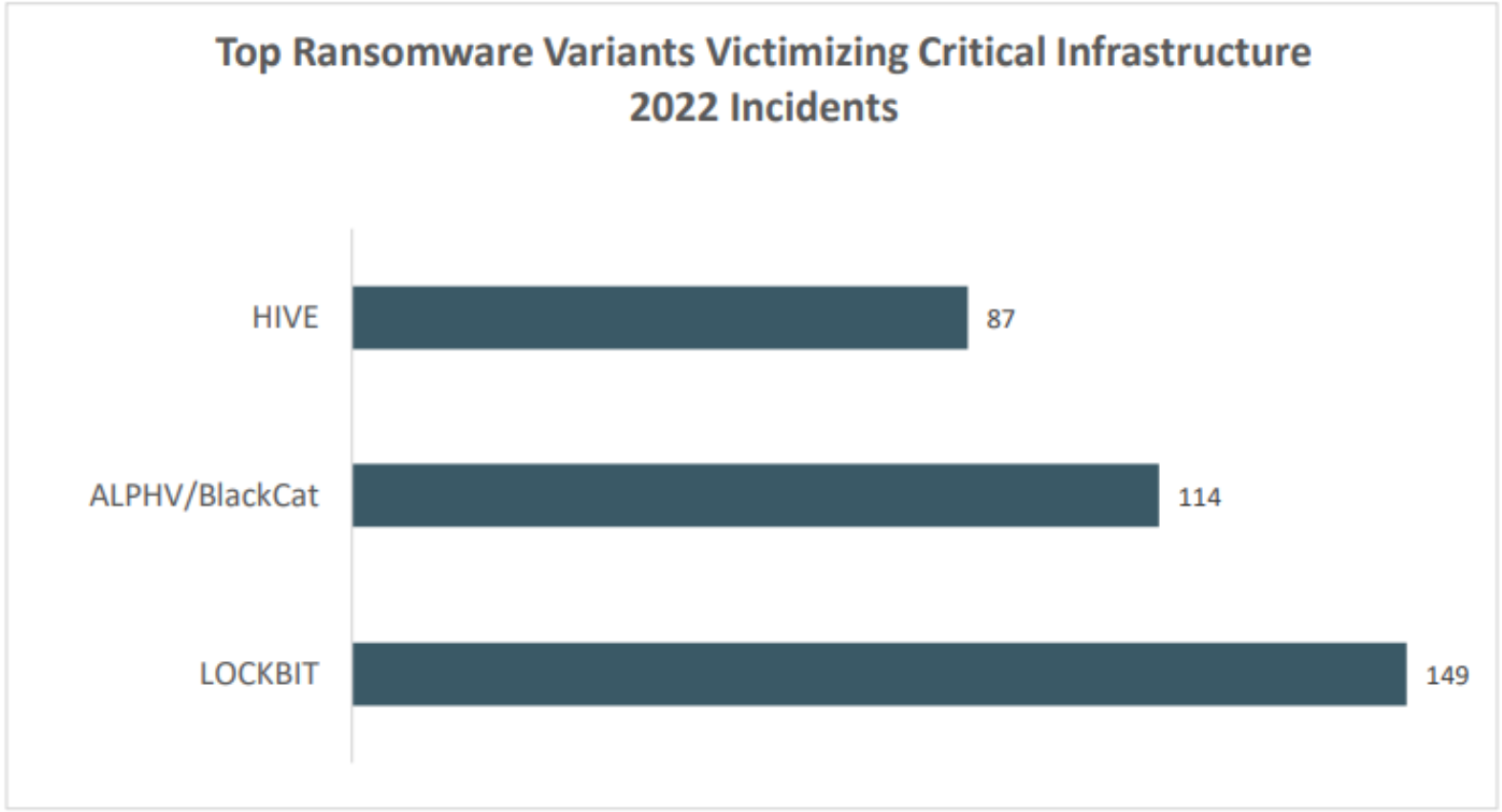
Acciones inmediatas que se pueden tomar para protegerse de un ransomware:

- Actualizar el sistema operativo y software.
- Implementar capacitación de usuarios y ejercicios de phishing para crear conciencia sobre los riesgos de enlaces y archivos adjuntos sospechosos.
- Si se utiliza el Protocolo de Escritorio Remoto (Remote Desktop Protocol RDP) supervisión constante.
- Realizar una copia de seguridad offline de todos los datos.

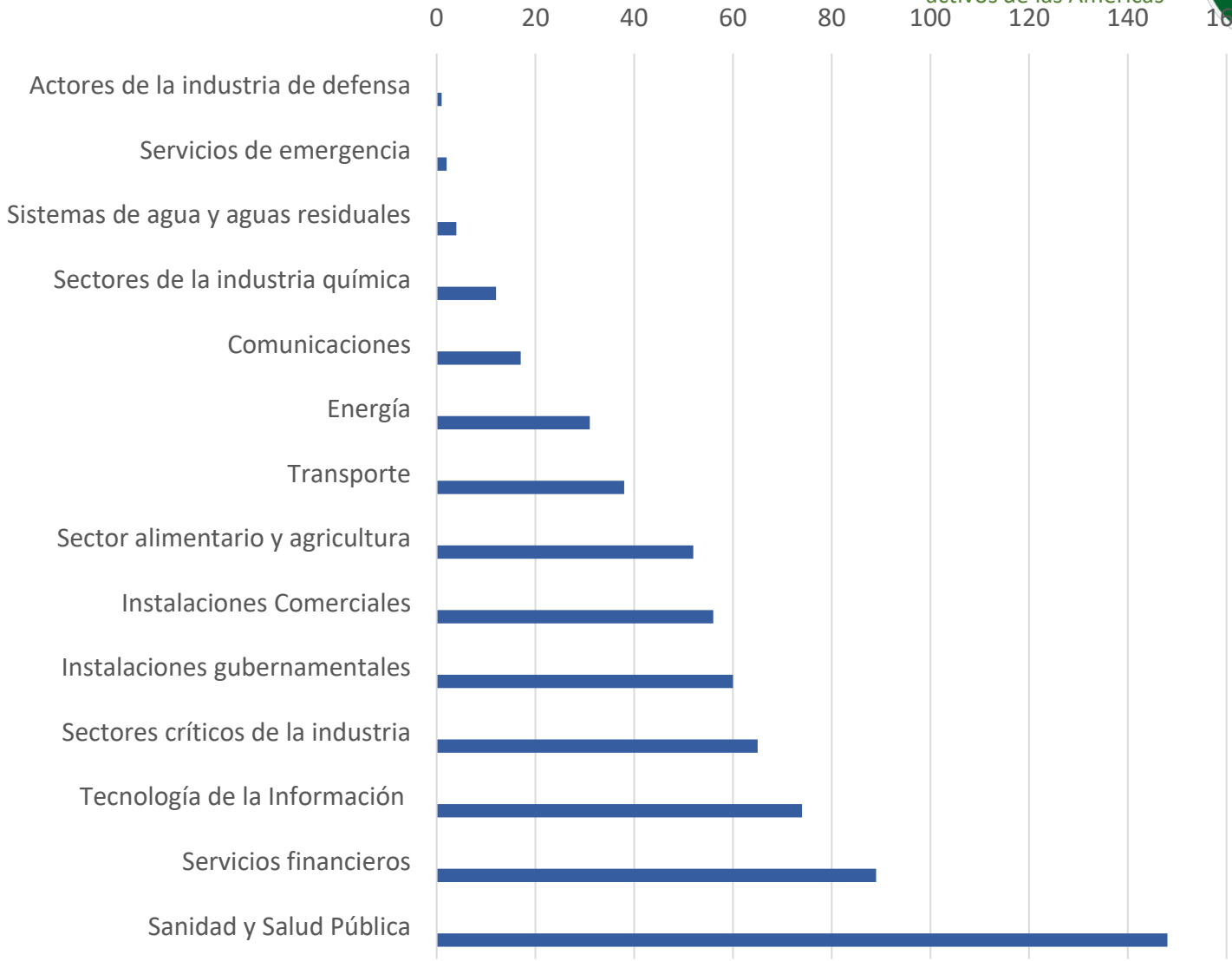
Principales variantes de ransomware que victimizan infraestructura crítica

Incidentes 2022

The three top ransomware variants reported to the IC3 that victimized a member of a critical infrastructure sector were Lock bit, ALPHV/Blackcoats, and Hive.[11]



Sectores víctimas de ransomware



2022 CRIME TYPES

By Victim Count			
Crime Type	*Victims*	*Crime Type*	*Victims*
Phishing	300,497	Government Impersonation	11,554
Personal Data Breach	58,859	Advanced Fee	11,264
Non-Payment/Non-Delivery	51,679	Other	9,966
Extortion	39,416	Overpayment	6,183
Tech Support	32,538	Lottery/Sweepstakes/Inheritance	5,650
Investment	30,529	Data Breach	2,795
Identity Theft	27,922	Crimes Against Children	2,587
Credit Card/Check Fraud	22,985	Ransomware	2,385
BEC	21,832	Threats of Violence	2,224
Spoofing	20,649	IPR/Copyright/Counterfeit	2,183
Confidence/Romance	19,021	SIM Swap	2,026
Employment	14,946	Malware	762
Harassment/Stalking	11,779	Botnet	568
Real Estate	11,727		

*Descriptors**			
Cryptocurrency	31,310	Cryptocurrency Wallet	20,781

*These descriptors relate to the medium or tool used to facilitate the crime and are used by the IC3 for tracking purposes only. They are available as descriptors only after another crime type has been selected. Please see Appendix

2022 CRIME TYPES continued

By Victim Loss			
Crime Type	*Loss*	*Crime Type*	*Loss*
Investment	$3,311,742,206	Lottery/Sweepstakes/Inheritance	$83,602,376
BEC	$2,742,354,049	SIM Swap	$72,652,571
Tech Support	$806,551,993	Extortion	$54,335,128
Personal Data Breach	$742,438,136	Employment	$52,204,269
Confidence/Romance	$735,882,192	Phishing	$52,089,159
Data Breach	$459,321,859	Overpayment	$38,335,772
Real Estate	$396,932,821	Ransomware	*$34,353,237
Non-Payment/Non-Delivery	$281,770,073	Botnet	$17,099,378
Credit Card/Check Fraud	$264,148,905	Malware	$9,326,482
Government Impersonation	$240,553,091	Harassment/Stalking	$5,621,402
Identity Theft	$189,205,793	Threats of Violence	$4,972,099
Other	$117,686,789	IPR/Copyright/Counterfeit	$4,591,177
Spoofing	$107,926,252	Crimes Against Children	$577,464
Advanced Fee	$104,325,444		

*Descriptors***			
Cryptocurrency	$2,496,196,530	Cryptocurrency Wallet	$1,349,090,883

LAST THREE-YEAR COMPLAINT LOSS COMPARISON

By Victim Loss						▼ ▲ = Trend from previous Year
Crime Type	**2022**		2021		2020	
Advanced Fee	**$104,325,444**	▲	$98,694,137	▲	$83,215,405	▼
BEC	**$2,742,354,049**	▲	$2,395,953,296	▲	$1,866,642,107	▲
*Botnet	**$17,099,378**	▲	N/A		N/A	
Confidence Fraud/Romance	**$735,882,192**	▼	$956,039,739	▲	$600,249,821	▲
Credit Card/Check Fraud	**264,148,905**	▲	$172,998,385	▲	$129,820,792	▲
Crimes Against Children	**$577,464**	▲	$198,950	▼	$660,044	▼
Data Breach	**$459,321,859**	▲	$151,568,225	▲	$128,916,648	▲
Employment	**$52,204,269**	▲	$47,231,023	▼	$62,314,015	▲
Extortion	**$54,335,128**	▼	$60,577,741	▼	$70,935,939	▼
Government Impersonation	**$240,553,091**	▲	$142,643,253	▲	$109,938,030	▼
*Harassment/Stalking	**$5,621,402**		N/A		N/A	
Identity Theft	**189,205,793**	▼	$278,267,918	▲	$219,484,699	▲
Investment	**$3,311,742,206**	▲	$1,455,943,193	▲	$336,469,000	▲
IPR/Copyright and Counterfeit	**$4,591,177**	▼	$16,365,011	▲	$5,910,617	▼
Lottery/Sweepstakes/Inheritance	**$83,602,376**	▲	$71,289,089	▲	$61,111,319	▲
Malware	**$9,326,482**	▲	$5,596,889	▼	$6,904,054	▲
Non-Payment/Non-Delivery	**$281,770,073**	▼	$337,493,071	▲	$265,011,249	▲
Other	**$117,686,789**	▲	$75,837,524	▼	$101,523,082	▲
Overpayment	**$38,335,772**	▲	$33,407,671	▼	$51,039,922	▼
Personal Data Breach	**$742,438,136**	▲	$517,021,289	▲	$194,473,055	▲
Phishing	**$52,089,159**	▲	$44,213,707	▼	$54,241,075	▼
Ransomware	**$34,353,237**	▼	$49,207,908	▲	$29,157,405	▲
Real Estate	**$396,932,821**	▲	$350,328,166	▲	$213,196,082	▼
*SIM Swap	**$72,652,571**		N/A		N/A	
Spoofing	**$107,926,252**	▲	$82,169,806	▼	$216,513,728	▼
Tech Support	**$806,551,993**	▲	$347,657,432	▲	$146,477,709	▲
*Threats of Violence	**$4,972,099**		N/A		N/A	

Aspectos principales del Programa de Cumplimiento de un Sujeto Obligado

UCA ESCUELA DE NEGOCIOS
Facultad de Ciencias Económicas

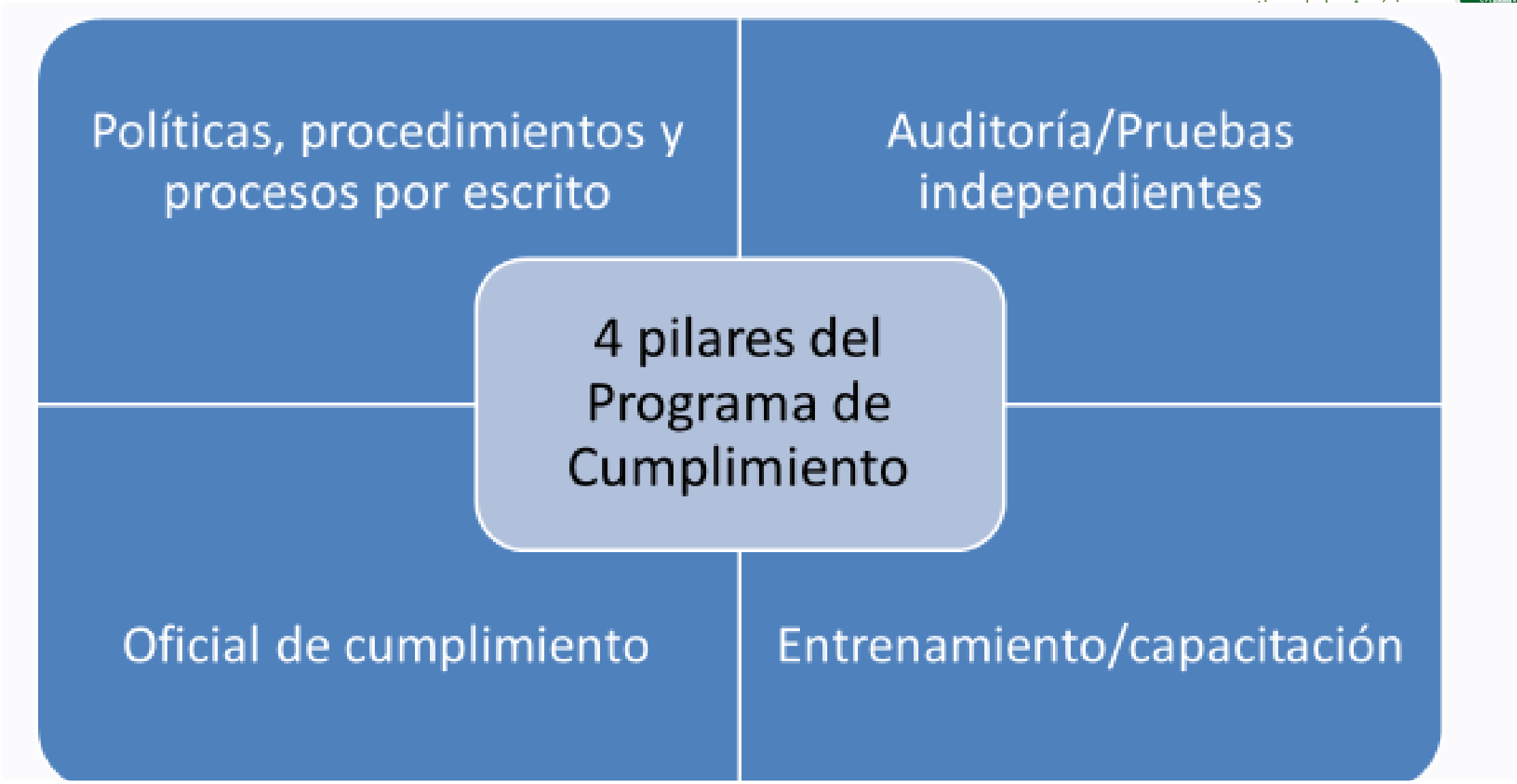
Sujetos obligados a cumplir con la normativa ALD/CFT y sus principales obligaciones

- Panorama General del Cumplimiento

Procesos y controles para cumplir con las leyes, regulaciones, y otros requisitos gubernamentales y estándares internacionales

Las obligaciones regulatorias se vuelven más **complejas y globales**

Existe una tendencia hacia la unificación de la "gestión o administración del riesgo de delitos financieros"


Políticas, procedimientos y procesos por escrito
Auditoría/Pruebas independientes
4 pilares del Programa de Cumplimiento
Oficial de cumplimiento
Entrenamiento/capacitación

Conceptos novedosos?

1916

SOME METHODS FOR CLASSIFICATION AND ANALYSIS OF MULTIVARIATE OBSERVATIONS

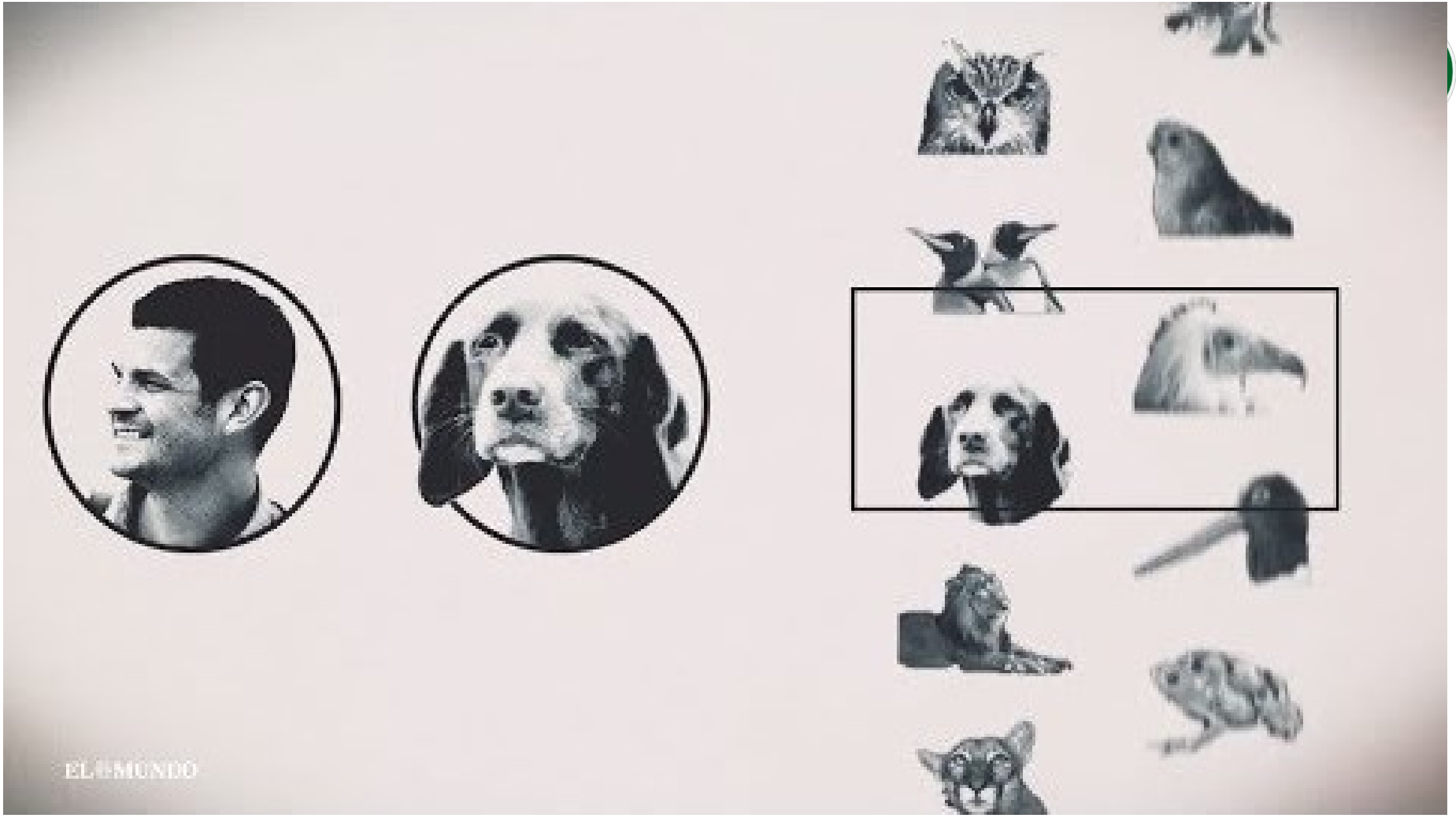
J. MacQUEEN
University of California, Los Angeles

1. Introduction

The main purpose of this paper is to describe a process for partitioning an N-dimensional population into k sets on the basis of a sample. The process, which is called 'k-means,' appears to give partitions which are reasonably efficient in the sense of within-class variance. That is, if p is the probability mass function for the population, $S = \{S_1, S_2, \cdots, S_k\}$ is a partition of E_N, and u_i, $i = 1, 2, \cdots, k$, is the conditional mean of p over the set S_i, then $w^2(S) = \sum_{i=1}^{k} \int_{S_i} |z - u_i|^2 \, dp(z)$ tends to be low for the partitions S generated by the method. We say 'tends to be low,' primarily because of intuitive considerations, corroborated to some extent by mathematical analysis and practical computational experience. Also, the k-means procedure is easily programmed and is computationally economical, so that it is feasible to process very large samples on a digital computer. Possible applications include methods for similarity grouping, nonlinear prediction, approximating multivariate distributions, and nonparametric tests for independence among several variables.

In addition to suggesting practical classification methods, the study of k-means has proved to be theoretically interesting. The k-means concept represents a generalization of the ordinary sample mean, and one is naturally led to study the pertinent asymptotic behavior, the object being to establish some sort of law of large numbers for the k-means. This problem is sufficiently interesting, in fact, for us to devote a good portion of this paper to it. The k-means are defined in section 2.1, and the main results which have been obtained on the asymptotic

1954



https://www.youtube.com/watch?v=NSf3o-wxtQ0

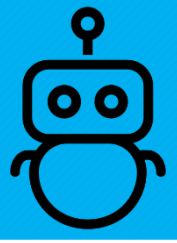
Conceptos básicos

XI Congreso de Prevención de Lavado de activos de las Américas

Inteligencia Artificial, Machine Learning y Deep Learning

Inteligencia Artificial

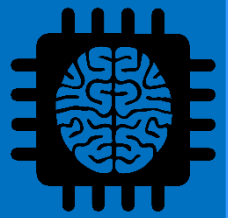
" … is a technique which allows the machines to act like humans by replicating their behavior and nature"



1950

Machine Learning

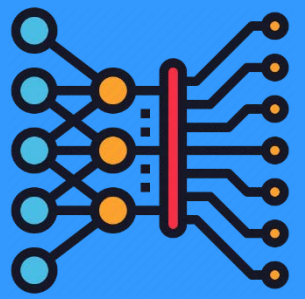
"It allows the machines to learn and make predictions based on its experience(data)"



1990

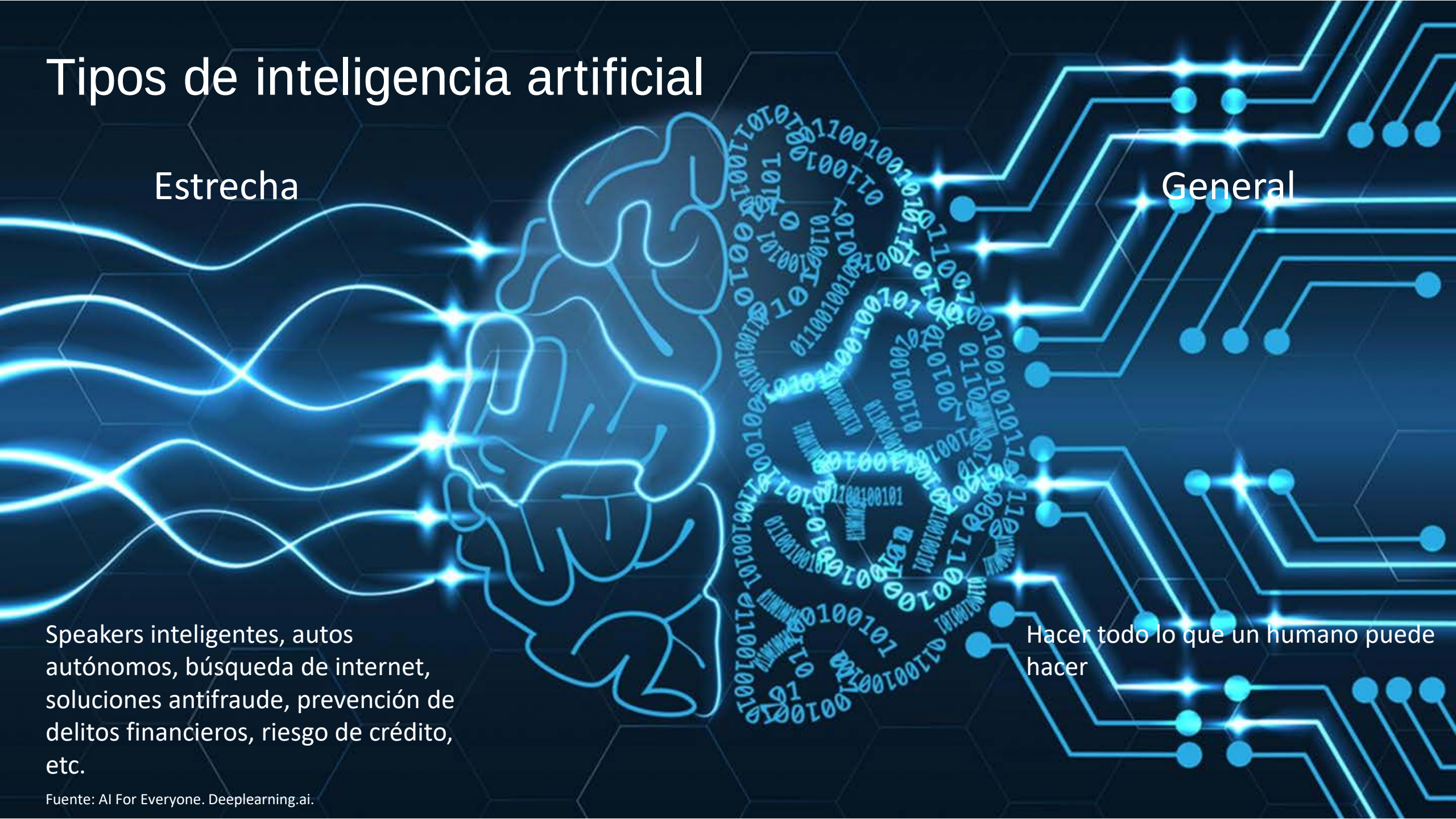
Deep Learning

"… is a particular kind of machine learning that achieves great power and flexibility by learning to represent the world as nested hierarchy of concepts or abstraction"



2010

Tipos de inteligencia artificial



Estrecha

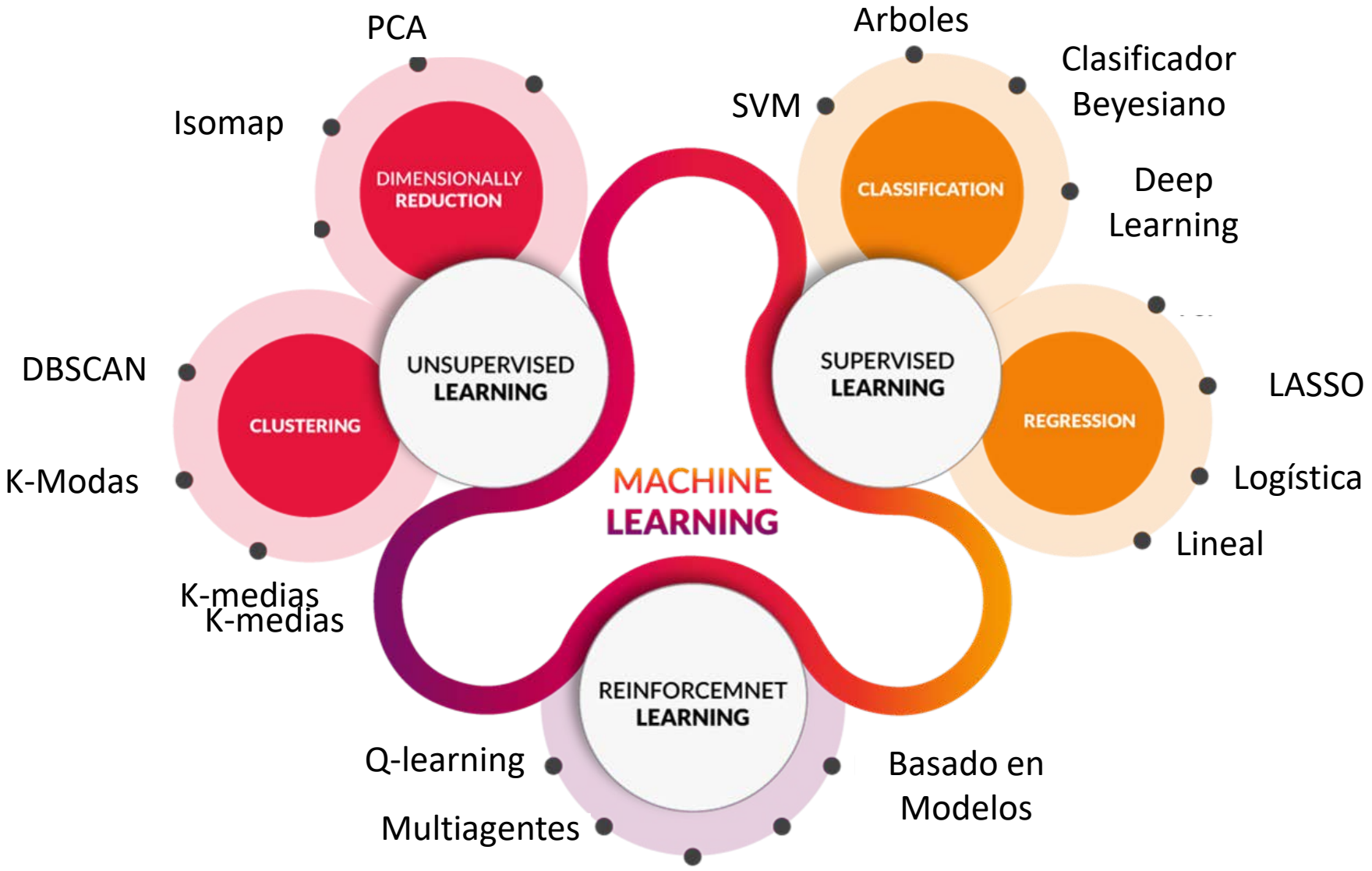
Speakers inteligentes, autos autónomos, búsqueda de internet, soluciones antifraude, prevención de delitos financieros, riesgo de crédito, etc.

General

Hacer todo lo que un humano puede hacer

Fuente: AI For Everyone. Deeplearning.ai.

Aprendizaje supervisado vs aprendizaje no supervisado

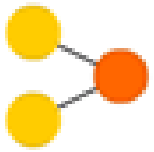


A mostly complete chart of

Neural Networks

- Backfed Input Cell
- Input Cell
- Noisy Input Cell
- Hidden Cell
- Probablistic Hidden Cell
- Spiking Hidden Cell
- Output Cell
- Match Input Output Cell
- Recurrent Cell
- Memory Cell
- Different Memory Cell
- Kernel
- Convolution or Pool

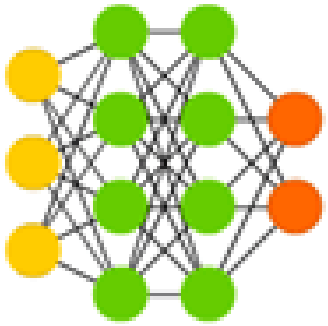
Perceptron (P)



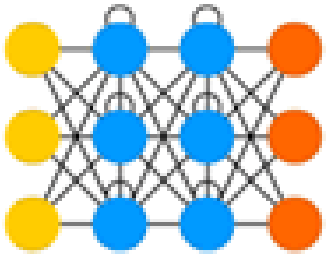
Feed Forward (FF)

Radial Basis Network (RBF)

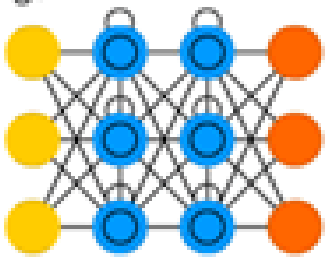
Deep Feed Forward (DFF)



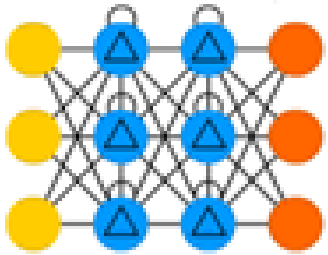
Recurrent Neural Network (RNN)



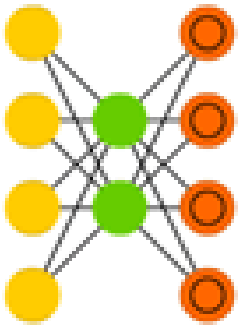
Long / Short Term Memory (LSTM)



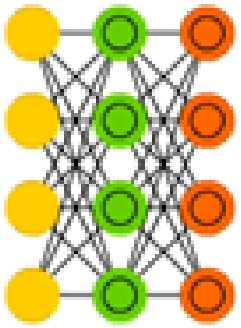
Gated Recurrent Unit (GRU)



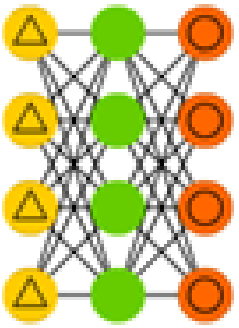
Auto Encoder (AE)



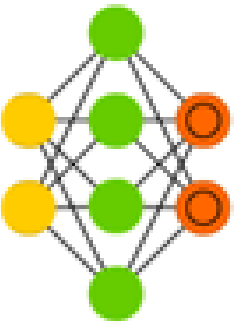
Variational AE (VAE)

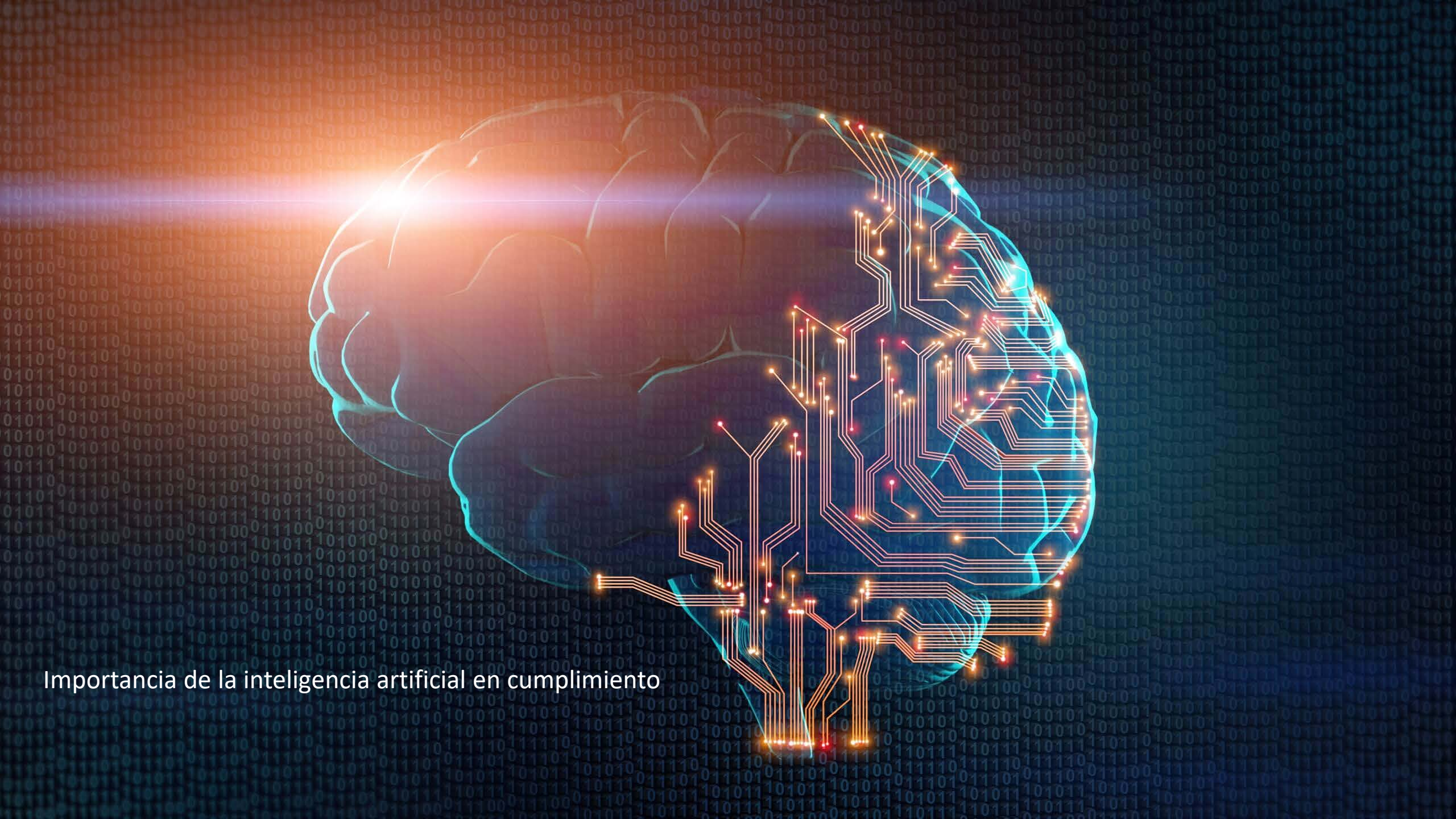


Denoising AE (DAE)

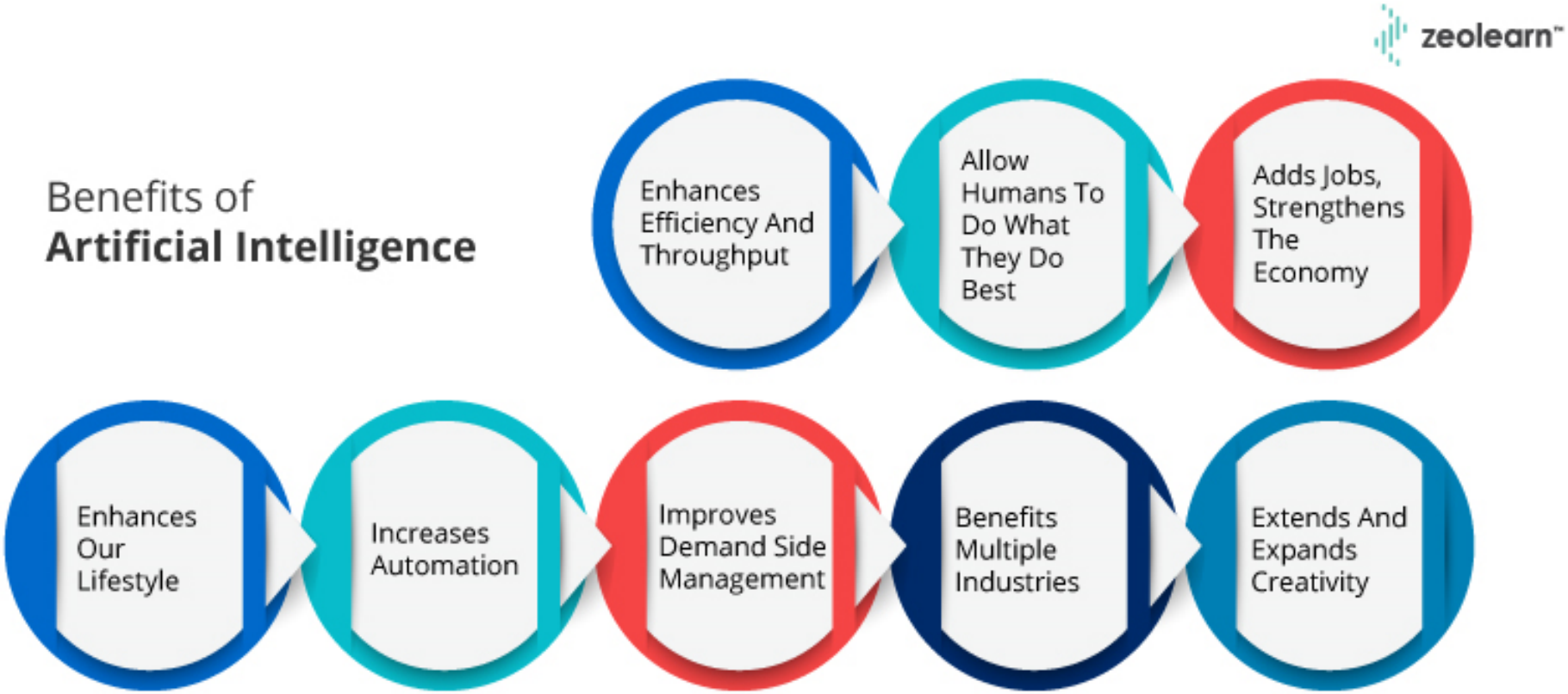


Sparse AE (SAE)

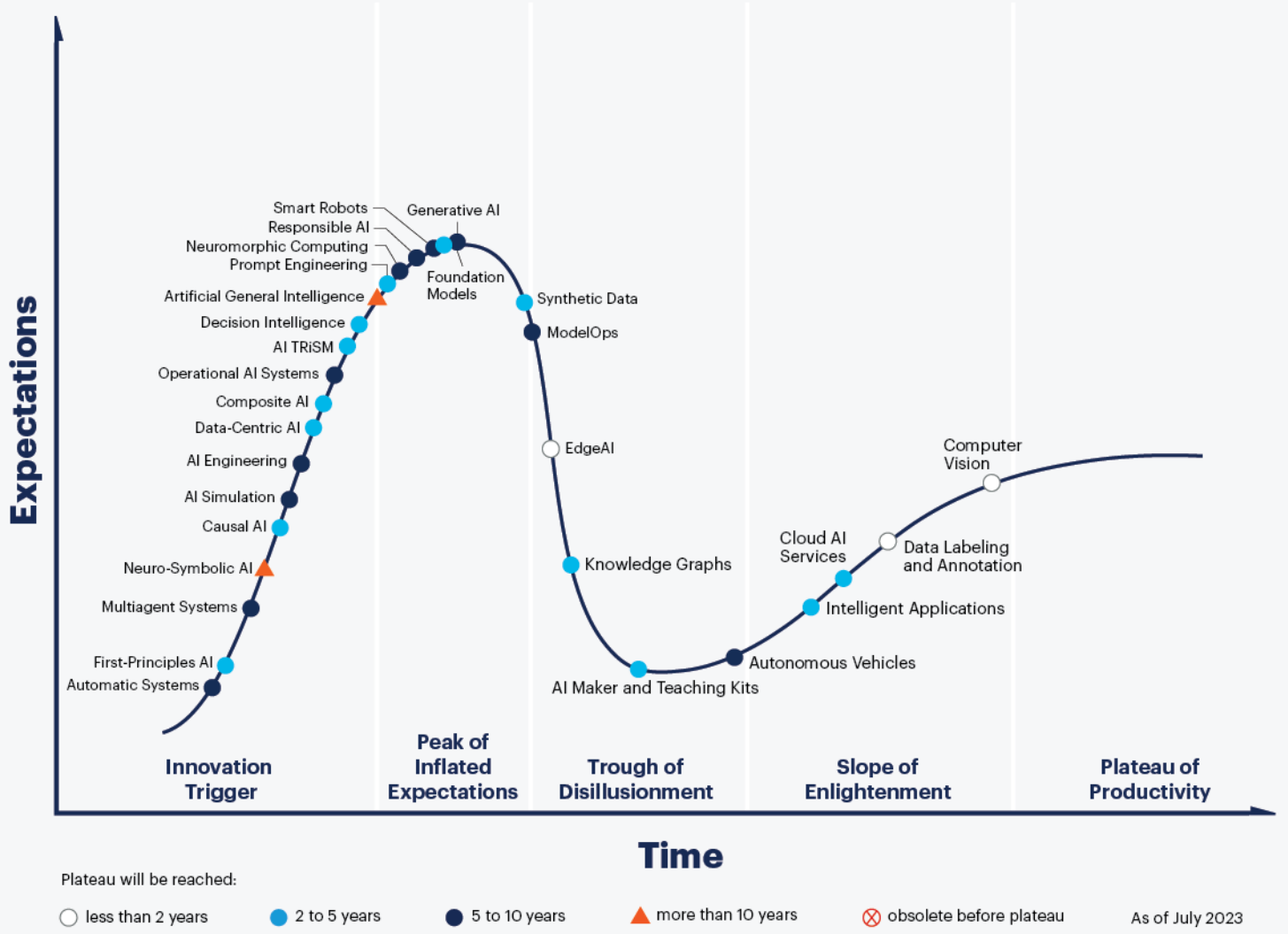



Importancia de la inteligencia artificial en cumplimiento

Importancia de la inteligencia artificial en cumplimiento



Hype Cycle for Artificial Intelligence, 2023



gartner.com

https://www.gartner.com/en/articles/what-s-new-in-artificial-intelligence-from-the-2023-gartner-hype-cycle

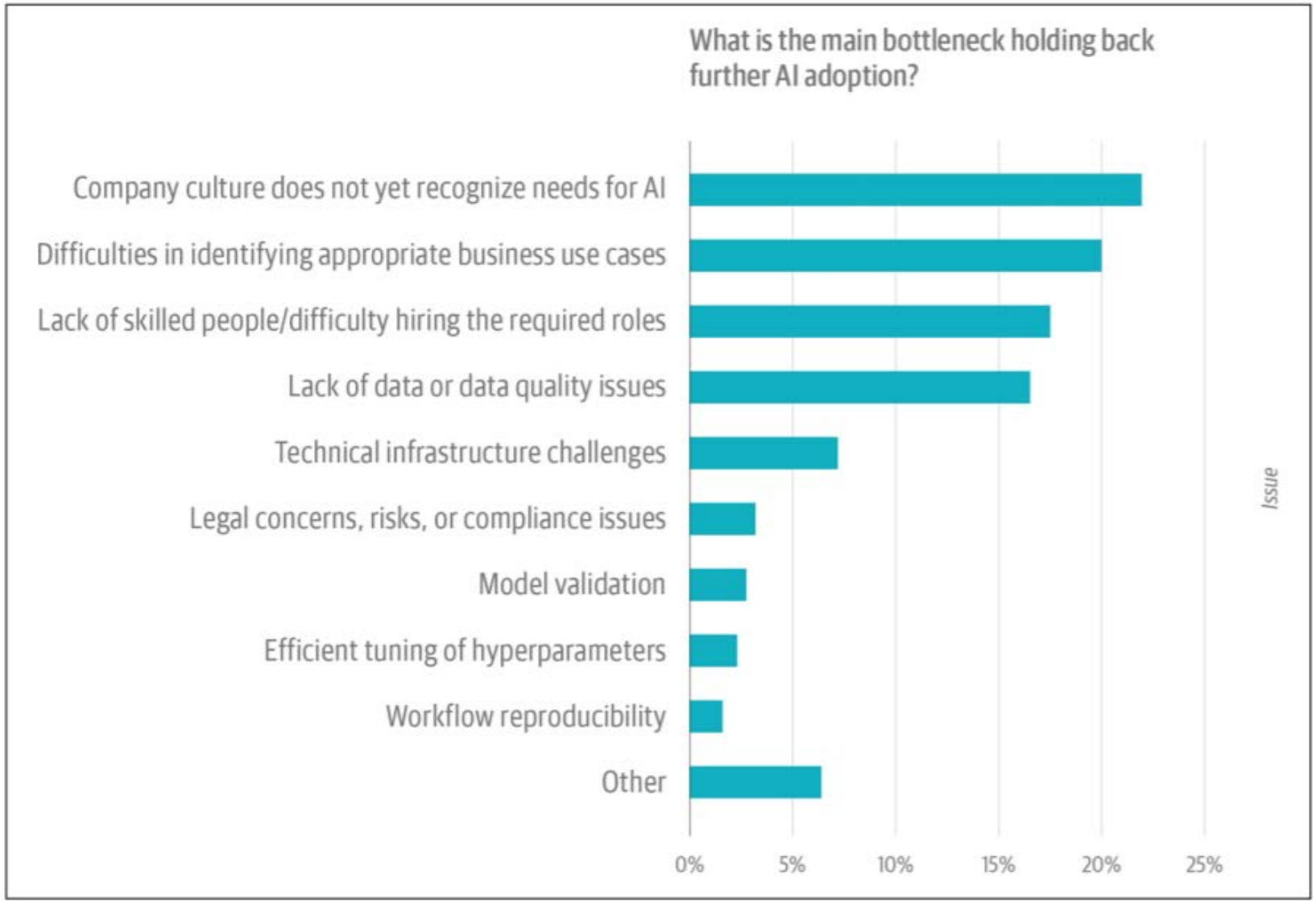
Source: Gartner

Gartner


No more
hiding in
plain
sight.

Principales vulnerabilidades del uso de IA

XI Congreso de Prevención de Lavado de activos de las Américas



Fuente: O´Reilly (2020). AI Adoption in the Enterprise.

Principales vulnerabilidades del uso de IA

XI Congreso de Prevención de Lavado de activos de las Américas

Apetito por Datos, y no cualquier dato

Principales vulnerabilidades del uso de IA

XI Congreso de Prevención de Lavado de activos de las Américas

Confiar ciegamente en la tecnología

Wrongfully Accused by an Algorithm

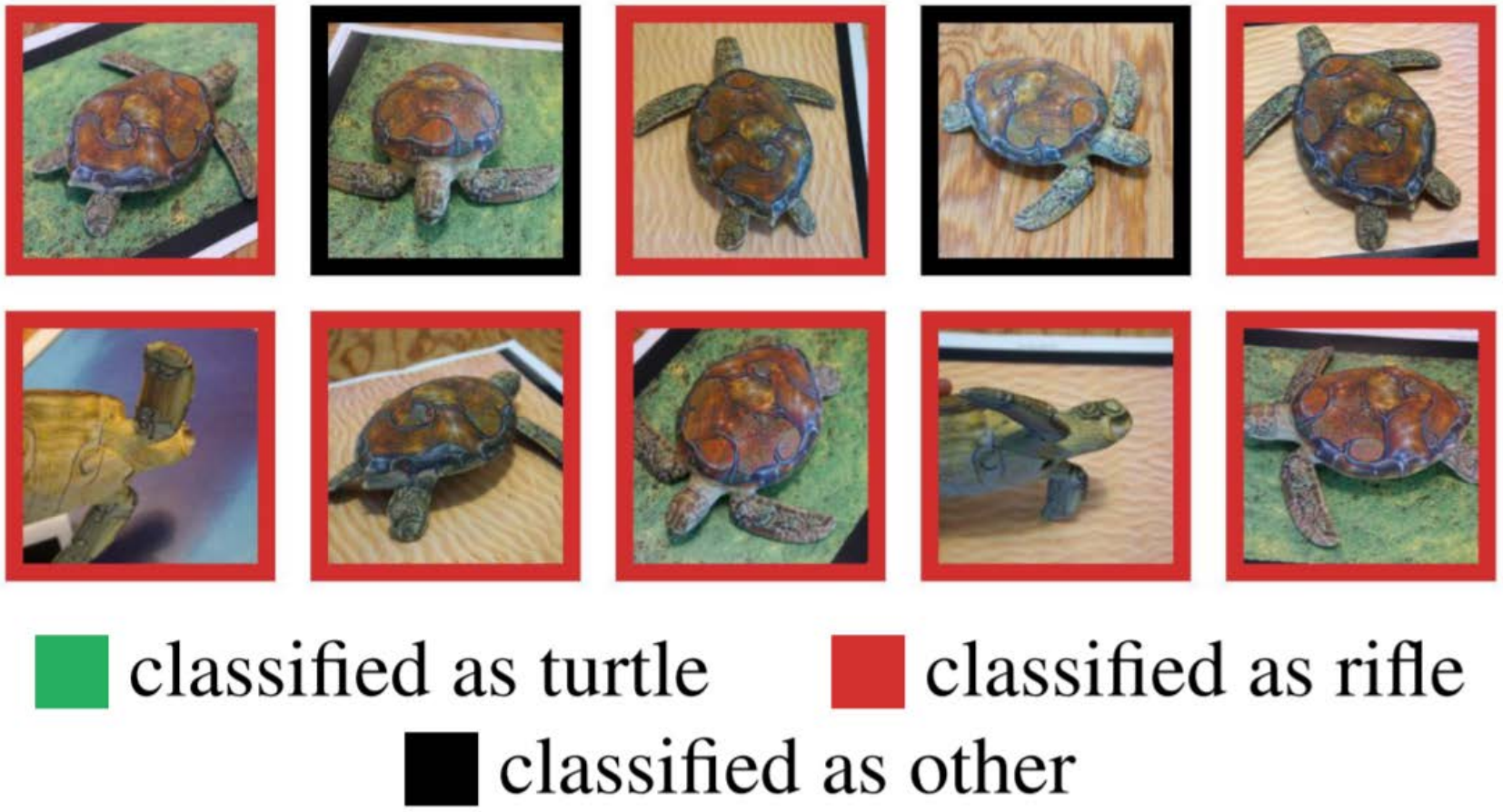
In what may be the first known case of its kind, a faulty facial recognition match led to a Michigan man's arrest for a crime he did not commit.

https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

Principales vulnerabilidades del uso de IA

XI Congreso de Prevención de Lavado de activos de las Américas

Ataques adversos



Desbloqueo de teléfonos
Acceso a edificios
Detección de objetos
Identificación de objetos riesgosos (p.e. scanner de aeropuerto)

Fuente: Anish Athalye, Logan Engstrom, Andrew Ilyas, Kevin Kwok. Synthesizing Robust Adversarial Examples.

Principales vulnerabilidades del uso de IA

XI Congreso de Prevención de Lavado de activos de las Américas

Ataques adversos

This Clothing Line Tricks AI Cameras Without Covering Your Face

JAN 20, 2023 PESALA BANDARA

Principales vulnerabilidades del uso de IA

XI Congreso de Prevención de Lavado de activos de las Américas

Profundización de sesgos

Tech BBC

IBM abandons 'biased' facial recognition tech

9 June

Migrar sesgos a sistemas de IA

"Discriminación" automática

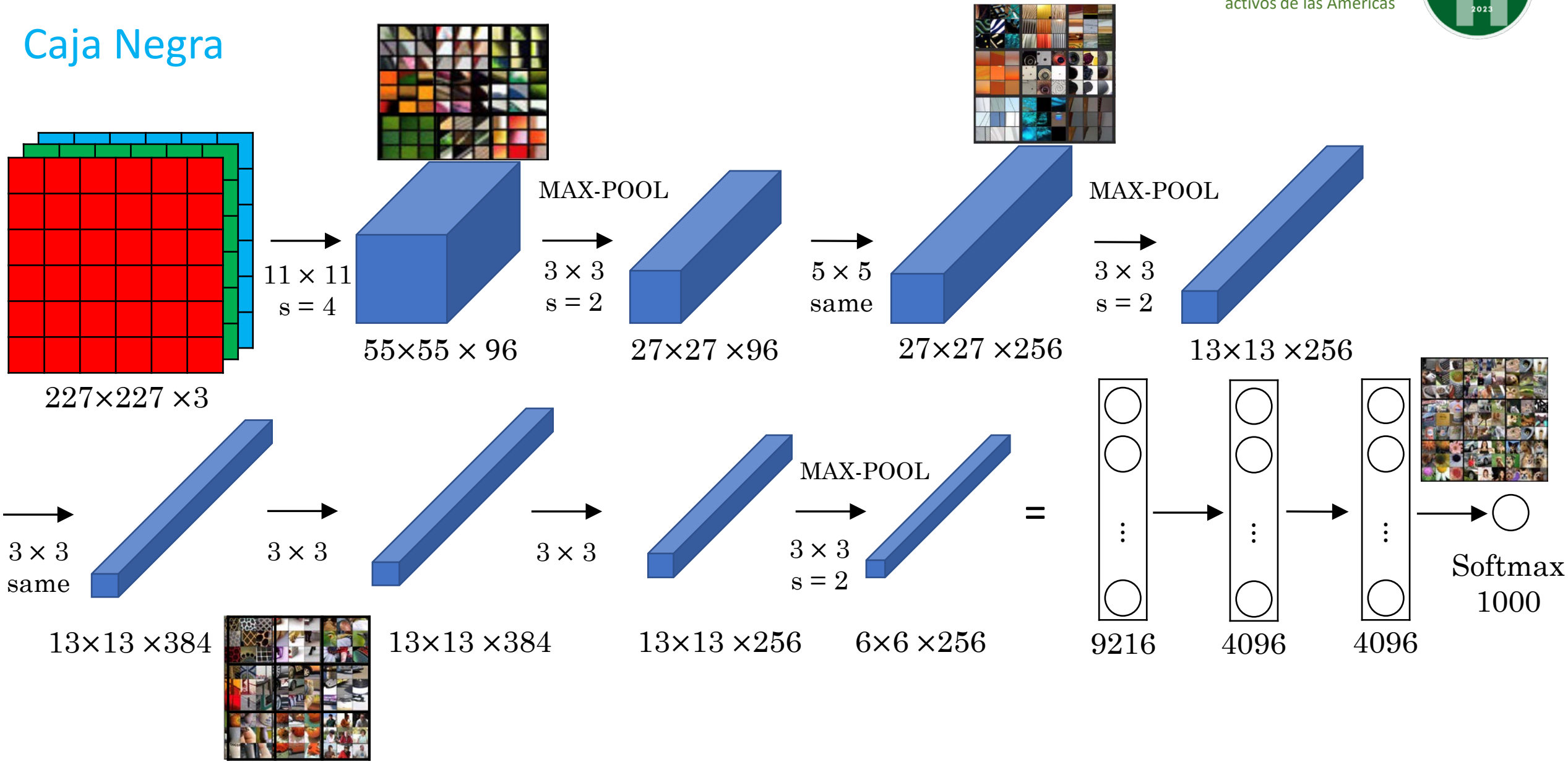
REUTERS

Amazon scraps secret AI recruiting tool that showed bias against women

Principales vulnerabilidades del uso de IA

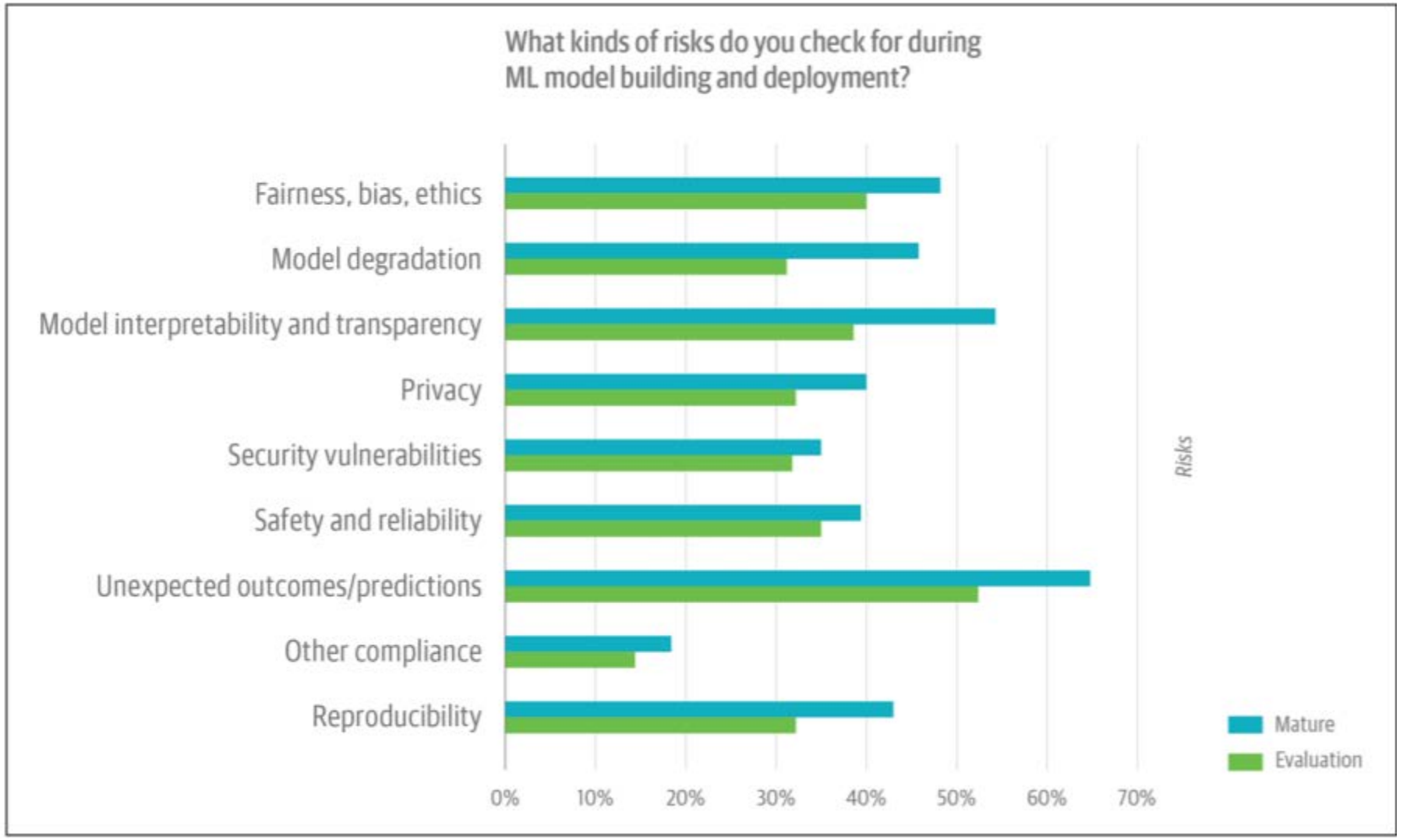
XI Congreso de Prevención de Lavado de activos de las Américas

Caja Negra



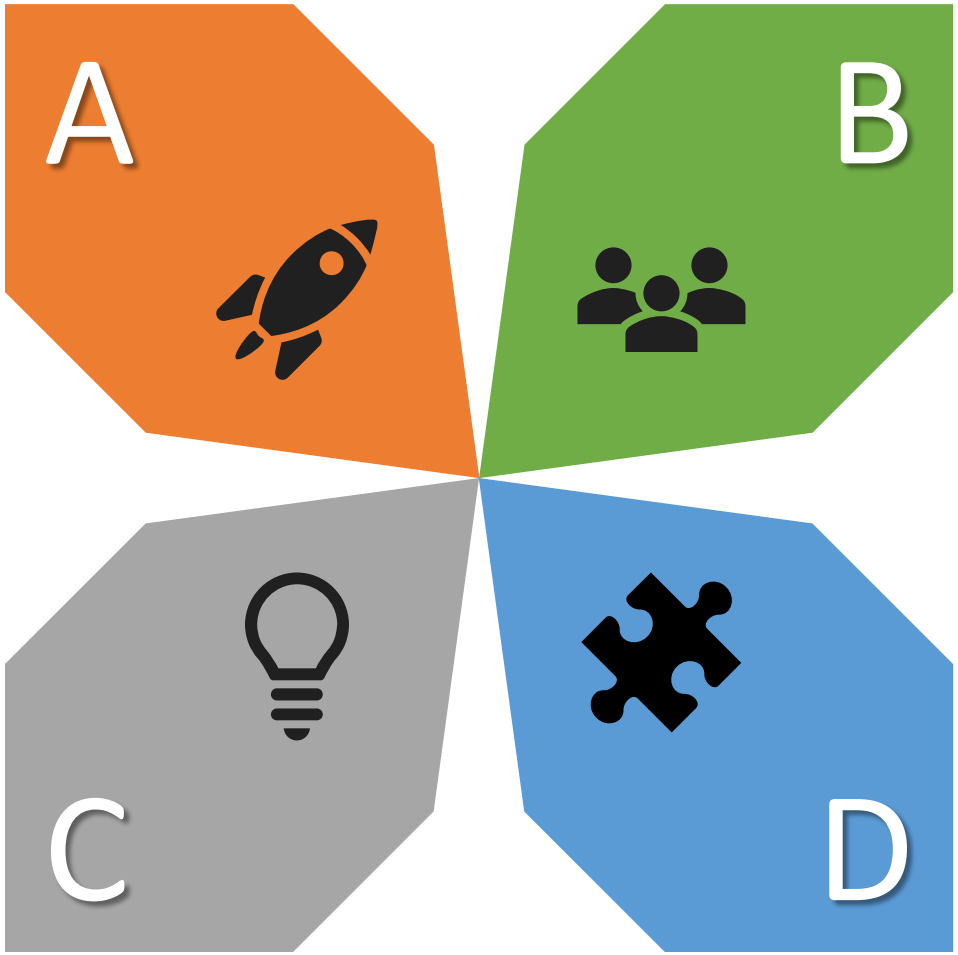
Principales vulnerabilidades del uso de IA

XI Congreso de Prevención de Lavado de activos de las Américas



Fuente: O´Reilly (2020). AI Adoption in the Enterprise.

Algunas restricciones del uso de IA y ML



Tecnológicas

Separación de ambientes (transaccional vs analítico)
Selección de la infraestructura tecnológica
Deployment
Integración de sistemas

Presupuestales

Hardware / Software
Calidad de datos
RRHH / Servicios profesionales

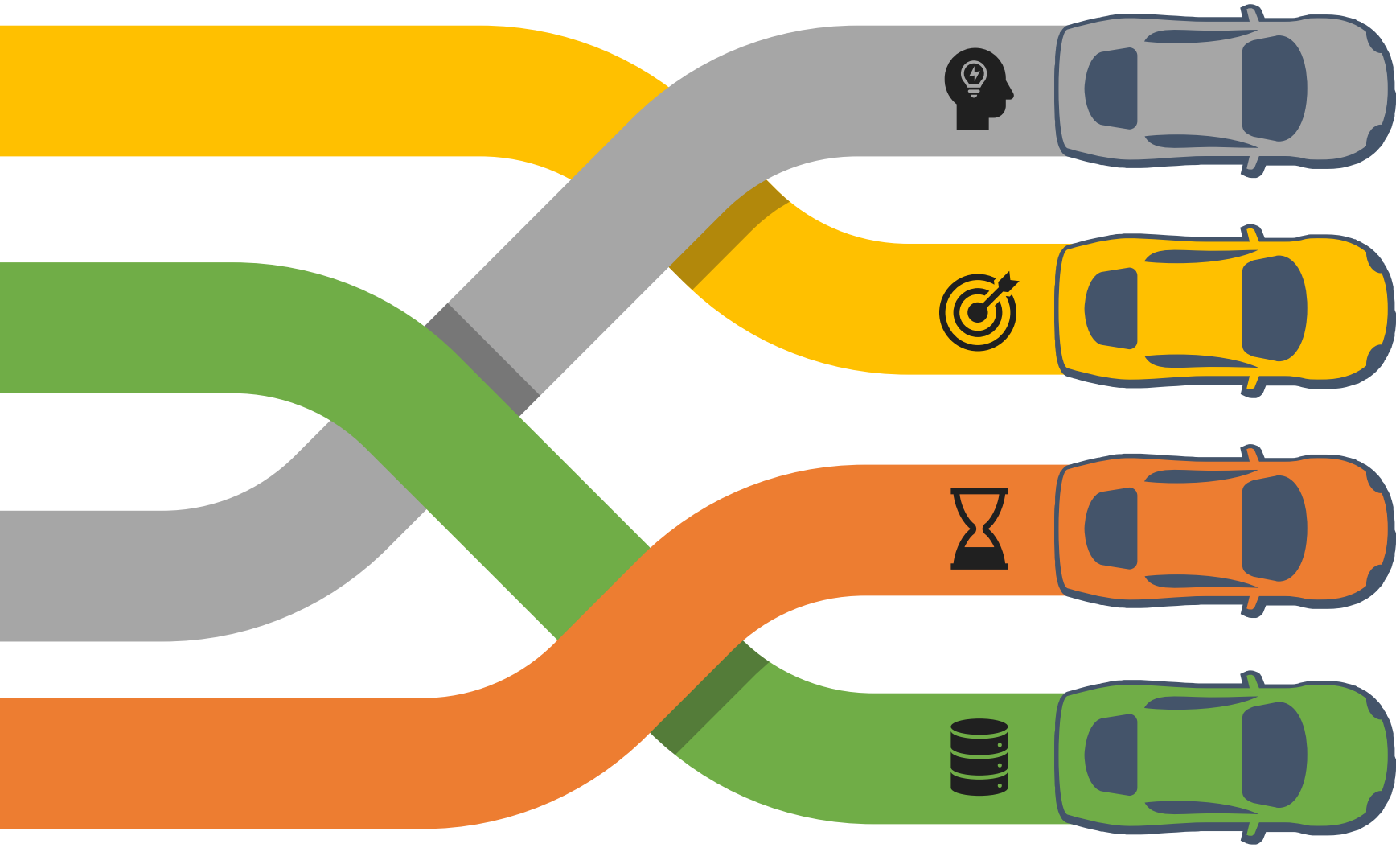
RRHH

Personal altamente capacitado
Reentrenamiento de personal
Mantenimiento de personal crítico

Eticas

Existen sesgos?

Algunas restricciones del uso de IA y ML



Restricciones

La regulación exige que algunos elementos sean realizados específicamente por humanos? **Aceptacion por el regulador**

Romper Paradigmas

Es complejo “convencer” a un regulador del potencial de uso de IA para ciertas laboras que usualmente realiza un humano, p.e. análisis de alertas?

Protección de datos personales

Viajan datos desde y hacia el modelo de IA fuera de la institución, fuera de la jurisdicción?.

Accountability

Dilusión de responsabilidades a través del modelo de IA?

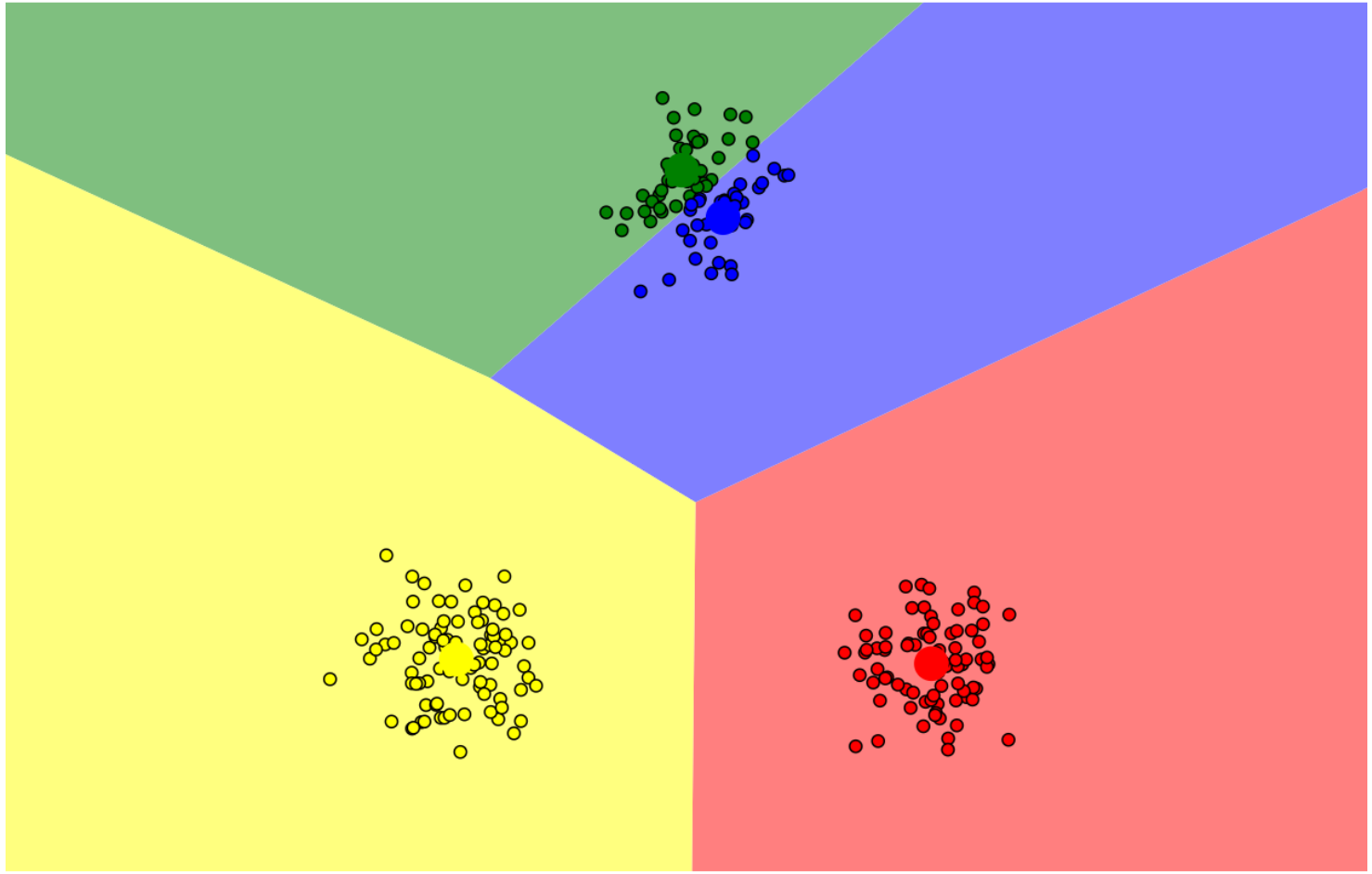
Taller: Entender en qué consiste el aprendizaje supervisado

XI Congreso de Prevención de Lavado de activos de las Américas

CPLDFT
CPLDAMERICAS.COM
2023

Aprendizaje no supervisado

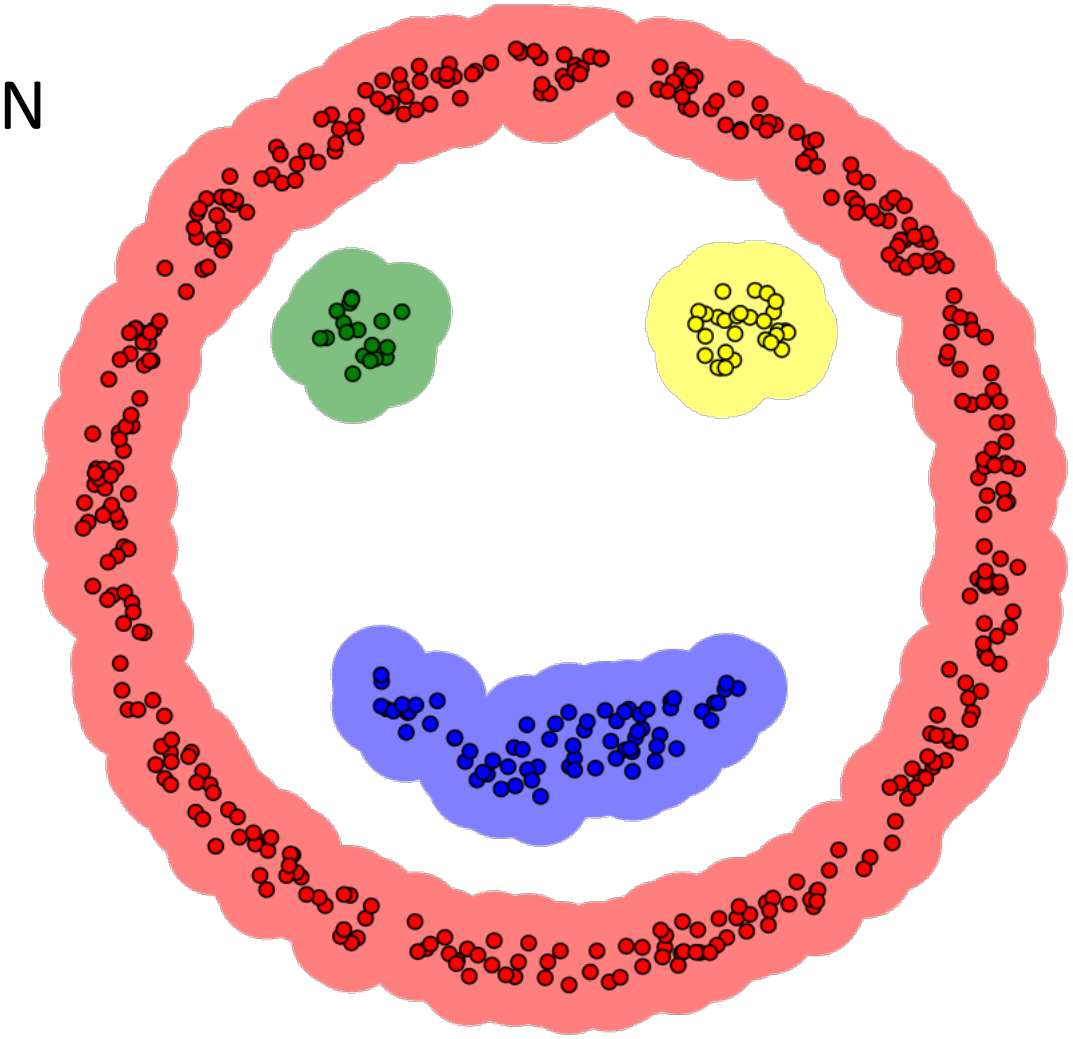
KMeans



Taller: Entender en qué consiste el aprendizaje supervisado

XI Congreso de Prevención de Lavado de activos de las Américas

- Aprendizaje no supervisado: DBSCAN



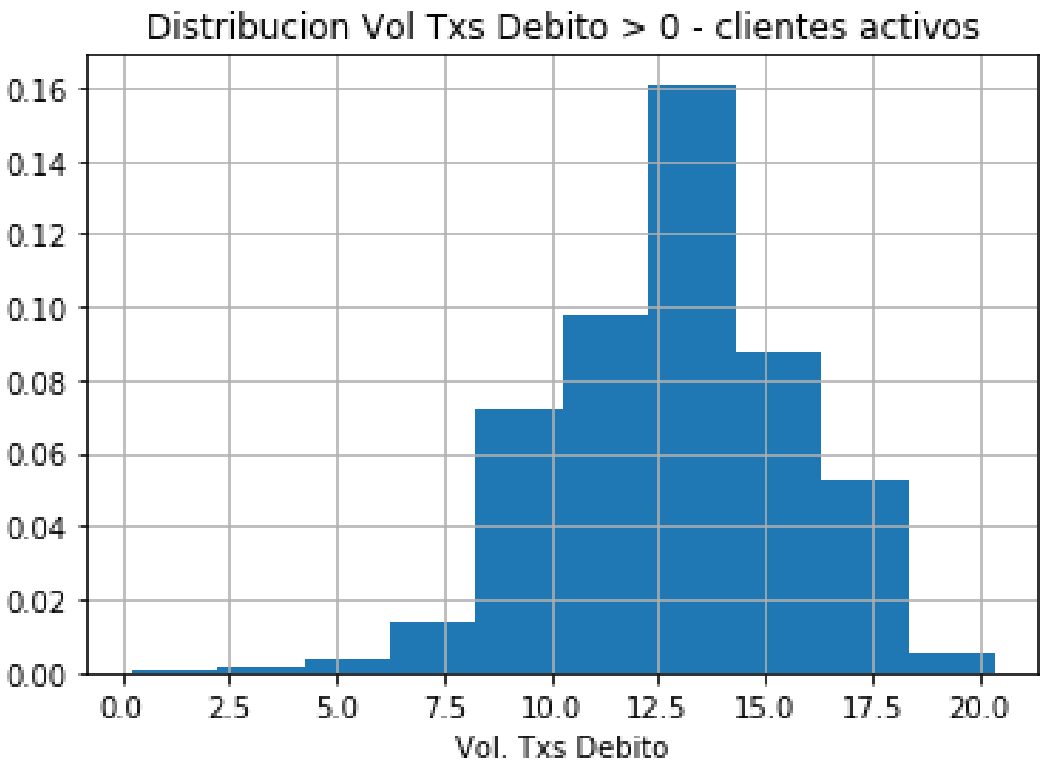
Usos de Aprendizaje Supervisado en prevención de delitos financieros y antifraude

https://www.youtube.com/watch?v=FnAuOVocE-A&ab_channel=NoticierosTelevisa

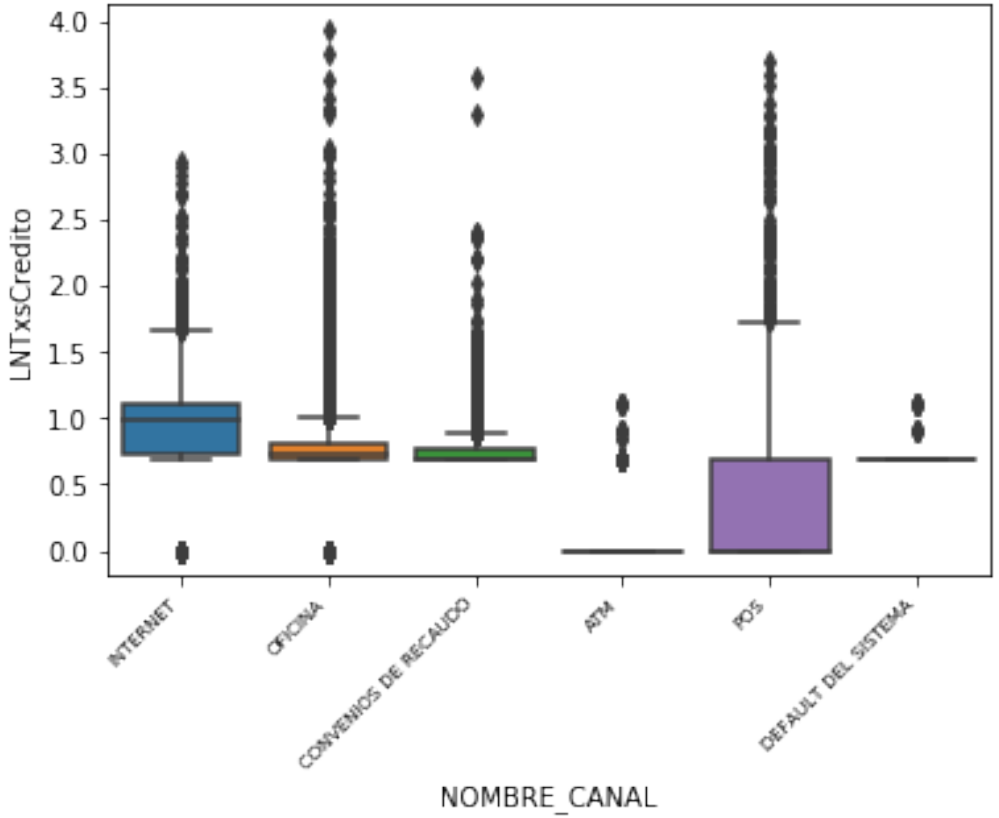
Casos de Uso en la prevención de delitos financieros

Prevención de blanqueo de capitales

Monitoreo transaccional con reglas duras



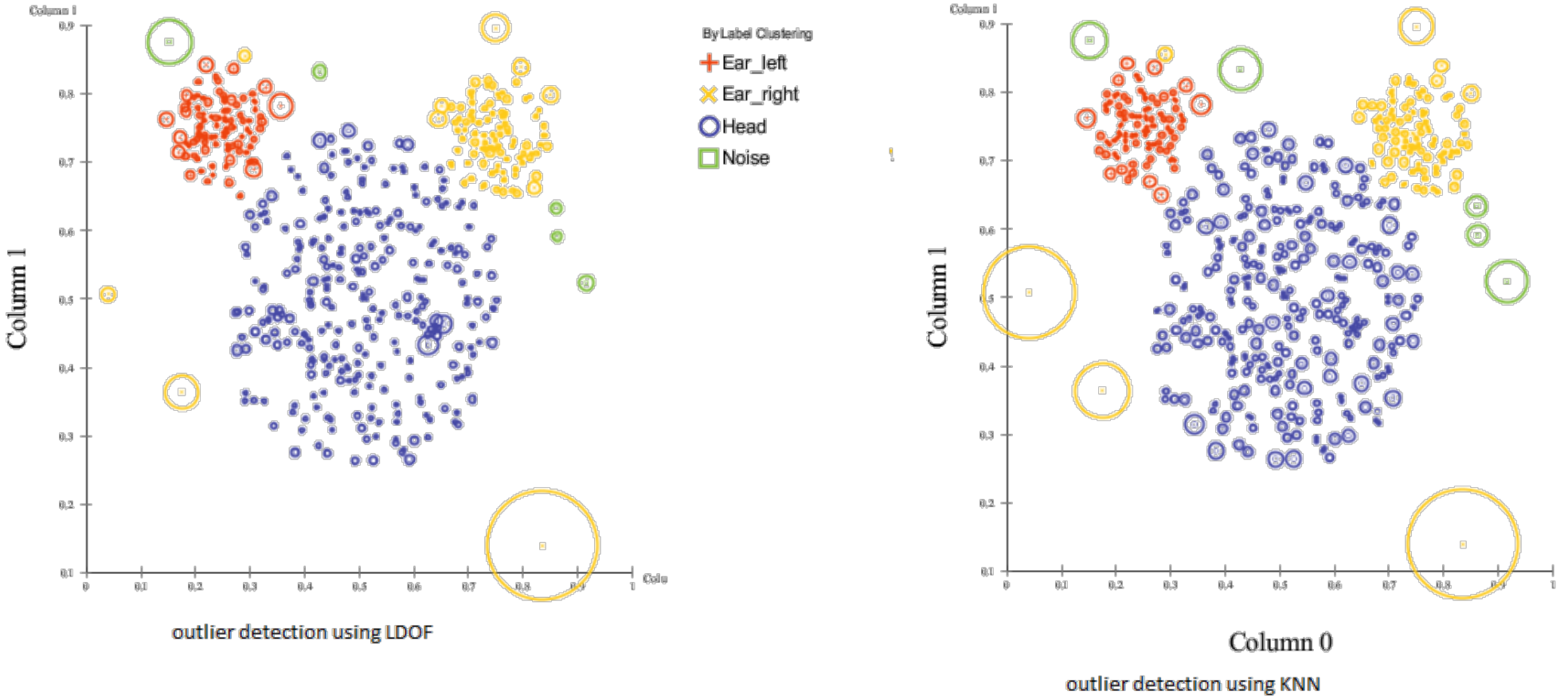
Análisis estadístico básico



Casos de Uso en la prevención de delitos financieros

Prevención de blanqueo de capitales

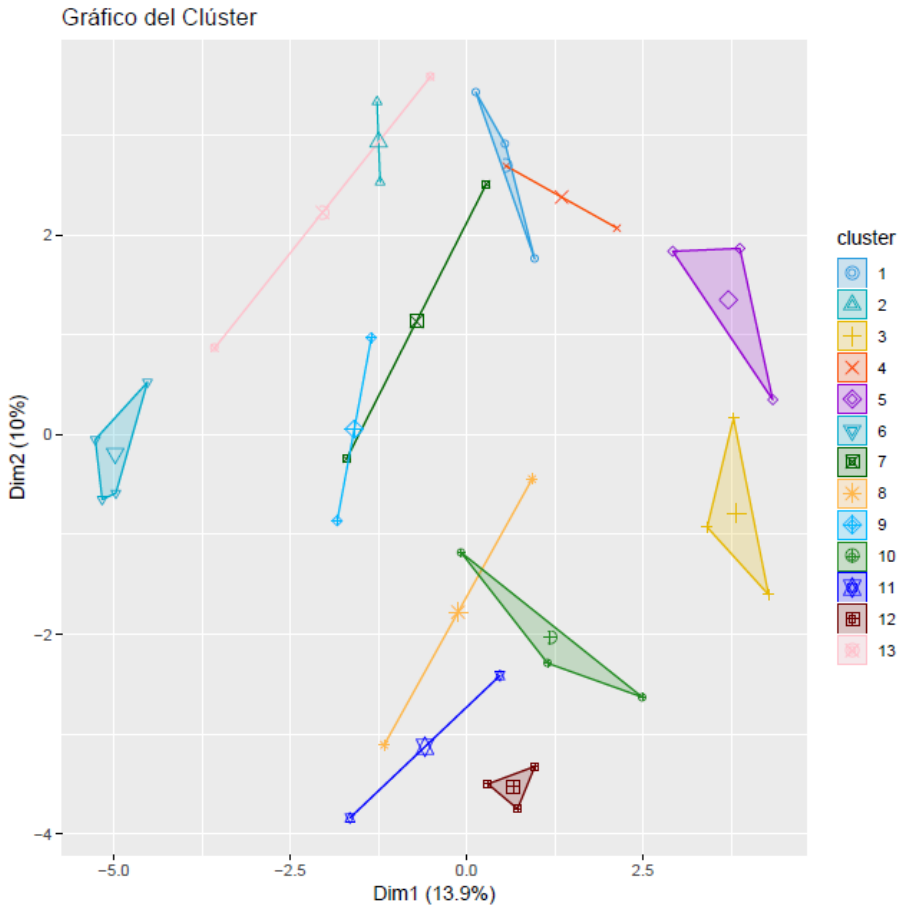
Detección de anomalías



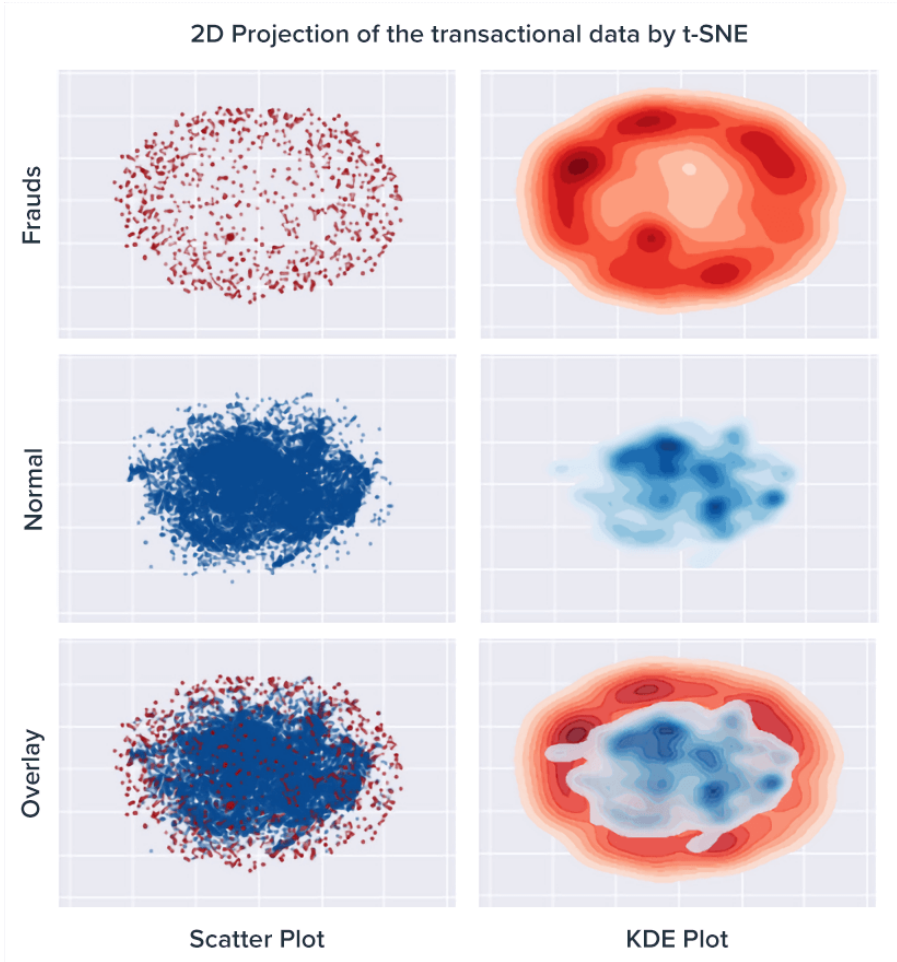
Casos de Uso en la prevención de delitos financieros

Prevención de blanqueo de capitales

Segmentación



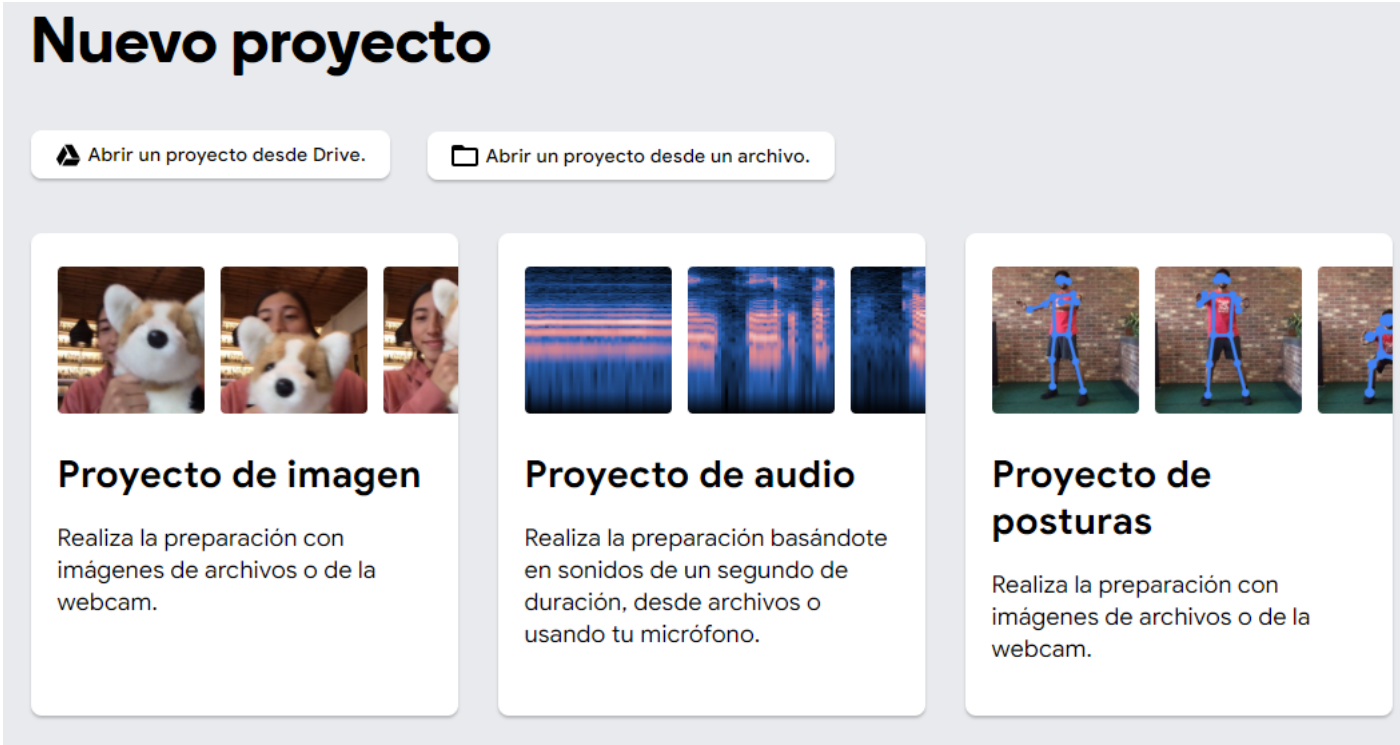
Identificación de posibles Transacciones fraudulentas



Taller: Entender cómo funciona un modelo de aprendizaje supervisado

XI Congreso de Prevención de Lavado de activos de las Américas

SCAN ME



Usos de aprendizaje supervisado en prevención de delitos financieros y antifraude

XI Congreso de
Prevención de Lavado de
activos de las Américas

Casos de Uso en la prevención de delitos financieros

Prevención de fraude

https://www.youtube.com/watch?v=wff83z_rE0Q&ab_channel=VisaEspa%C3%B1ol

Casos de Uso en la prevención de delitos financieros

Prevención de blanqueo de capitales

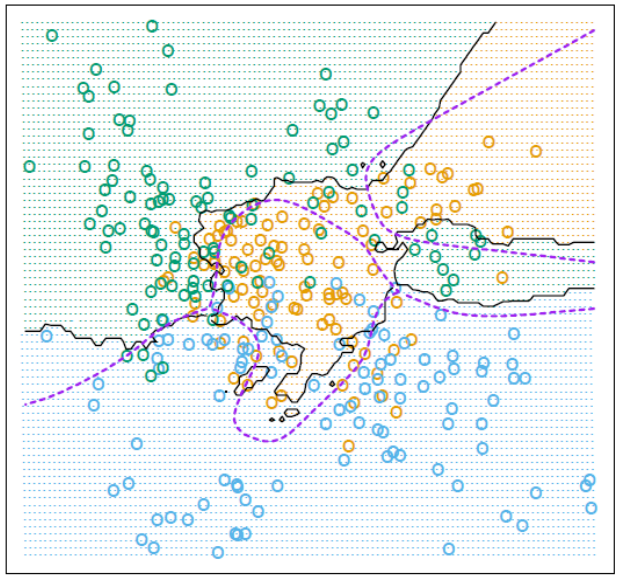
Scoring de Clientes y Niveles de Debida Diligencia

Scoring tradicional

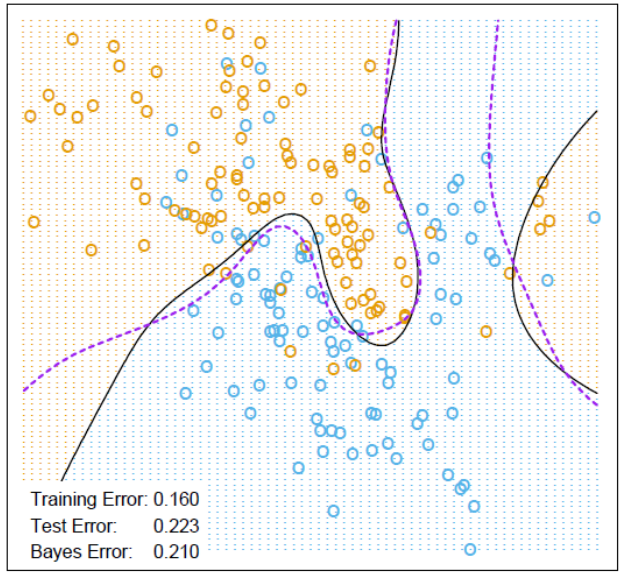
$$Calificación\ LAFT\ Clientes\ (CLAFT_{cliente}) = \beta_c R_c + \beta_p R_p + \beta_z R_z + \beta_o R_o$$

$$\beta_c + \beta_p + \beta_z + \beta_o = 1$$

K Vecinos más cercanos



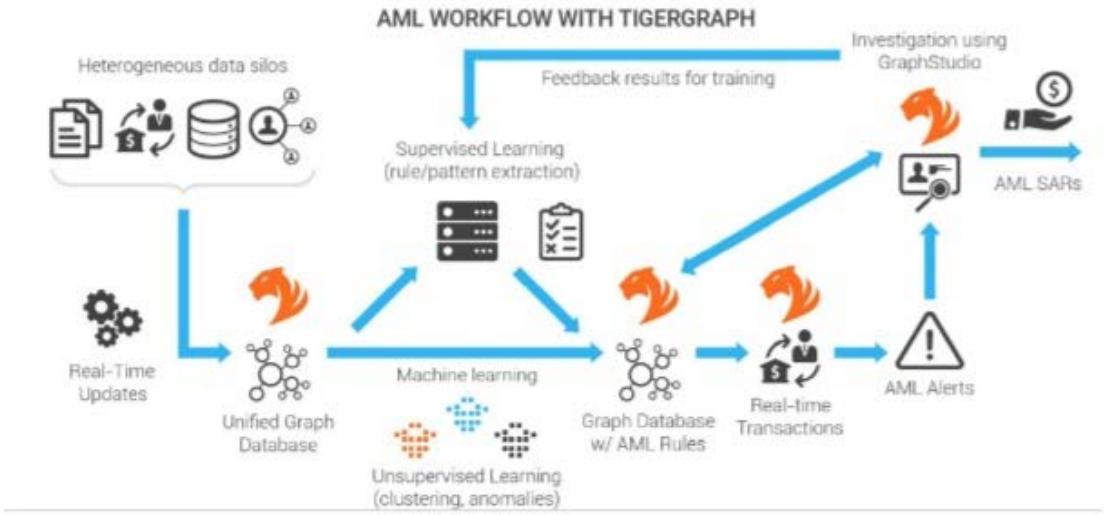
Deep Learning

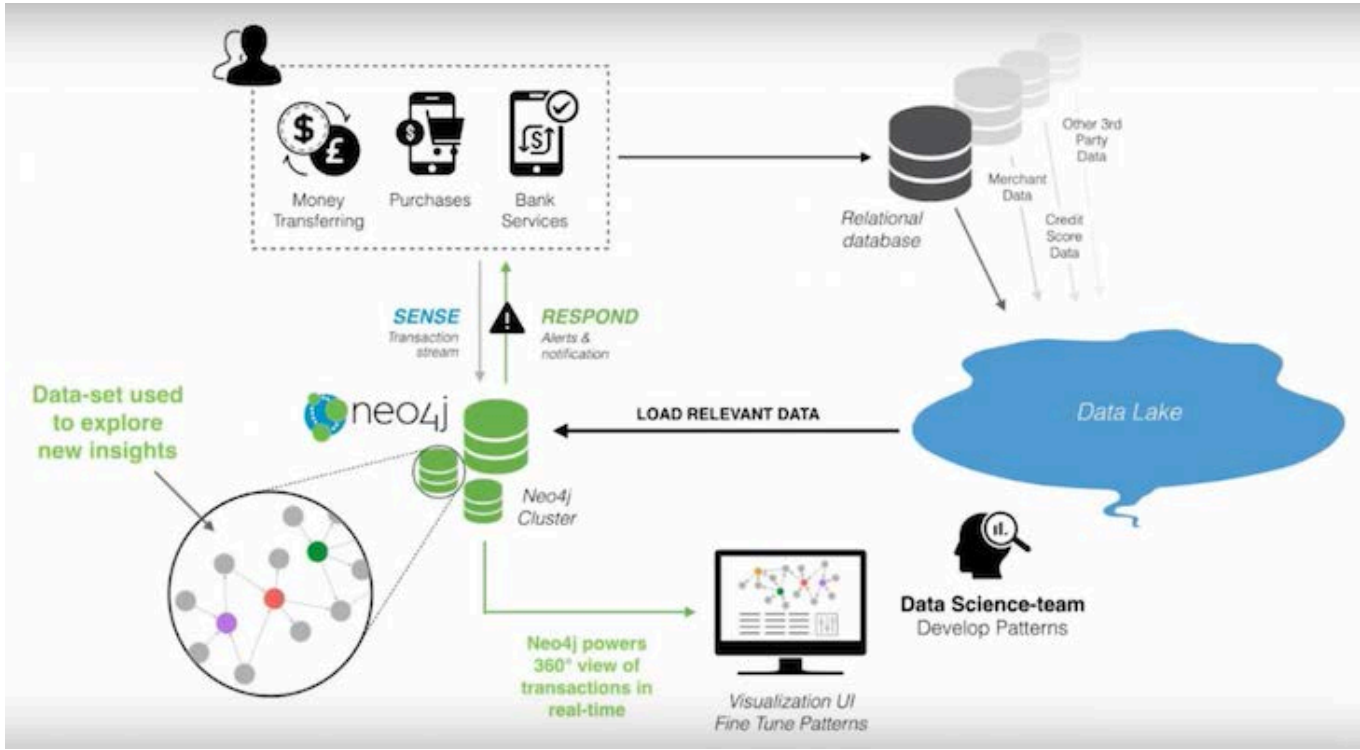


Fuente: Hastie, T; Tibshirani, R.; Friedman, J. The elements of statistical learning. Data mining, inference and prediction. Second Edition. Springer.

Casos de Uso en la prevención de delitos financieros

Graph-enhanced workflow for Anti-Money Laundering



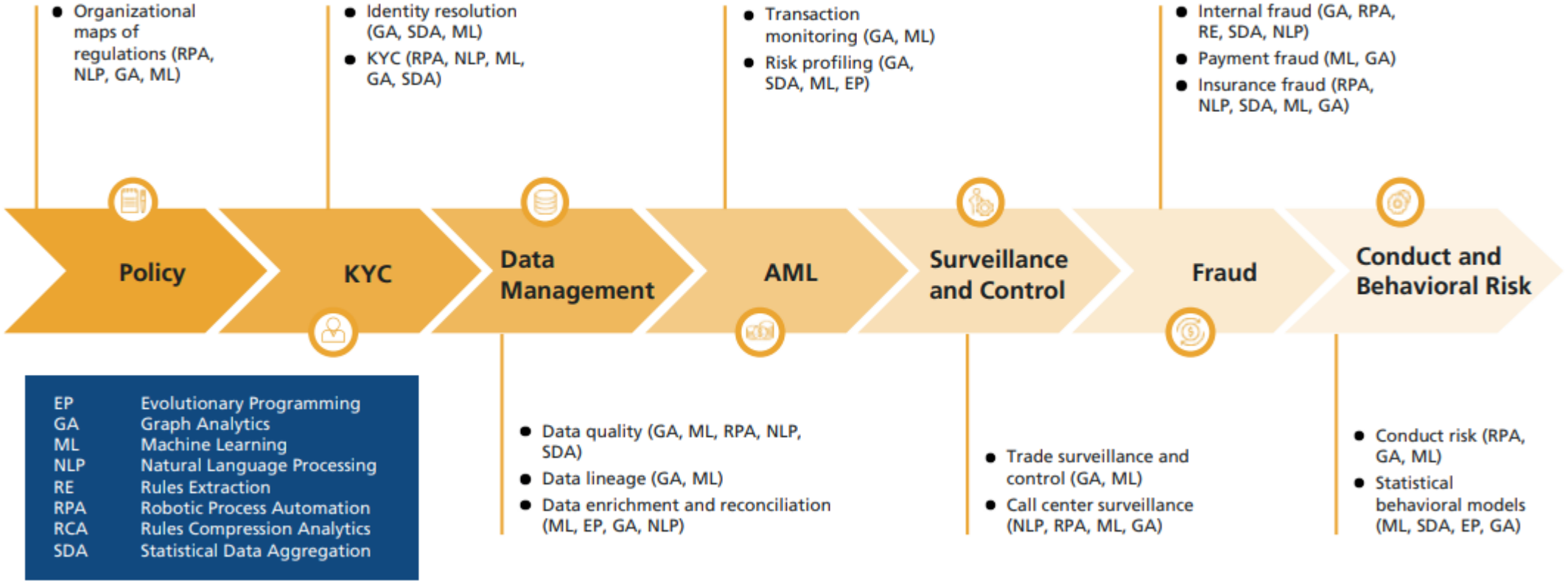


TigerGraph

Casos de Uso en la prevención de delitos financieros

Prevención de blanqueo de capitales

Figure 14: Areas where implementing AI tools could have the biggest benefit – financial crime and compliance



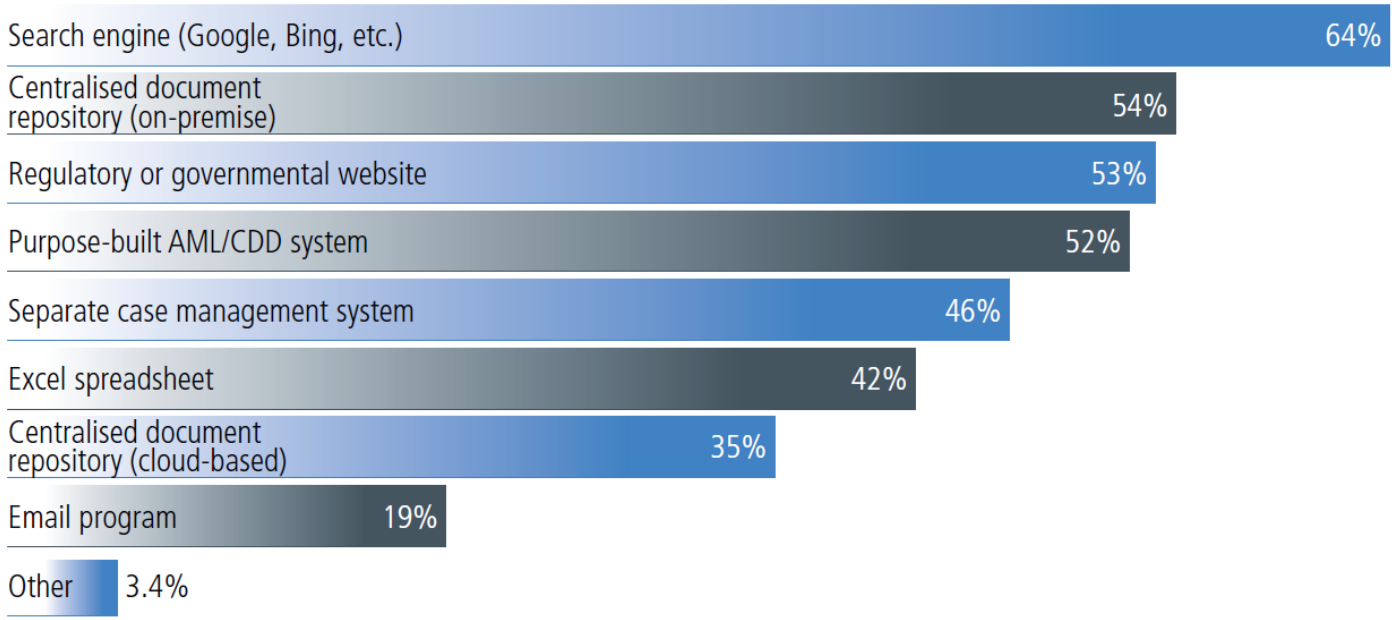
Source: Chartis Research

Prevención de blanqueo de capitales

Entity resolution e identificación de noticias adversas

Google

Figure 4 Technologies/tools used by organisations during the analysis and investigation process



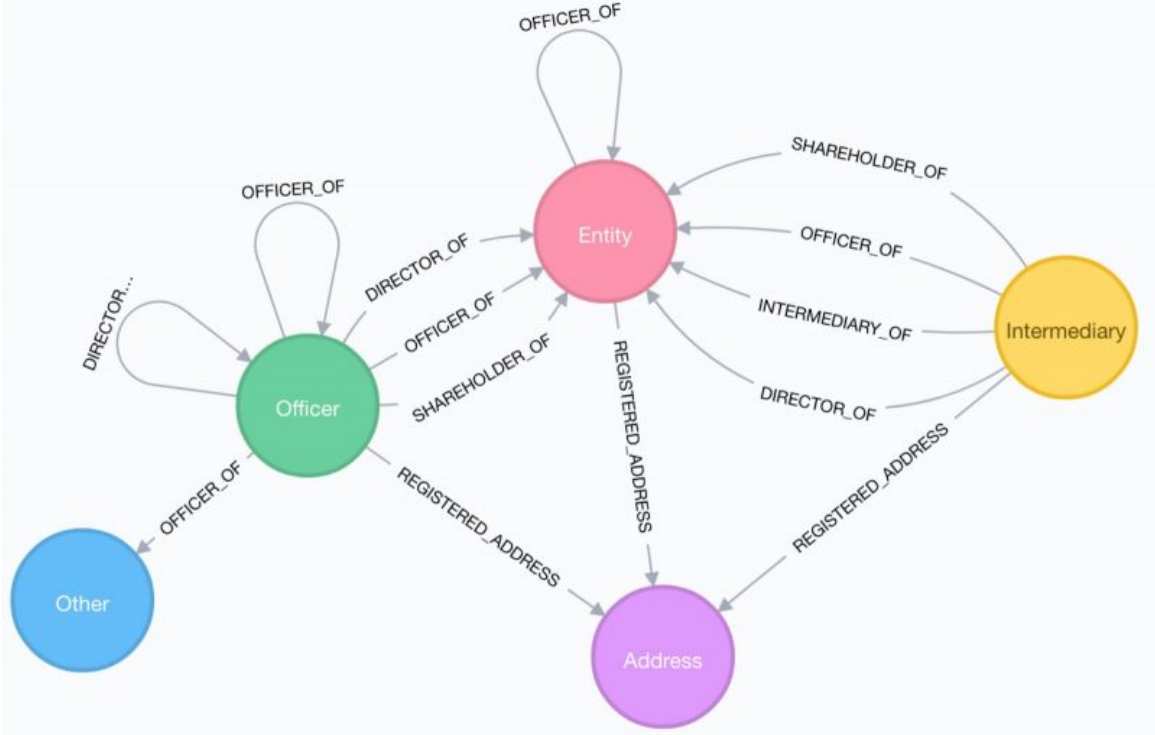
Risk.net (2019). Smarter thinking around financial crime prevention

Casos de Uso en la prevención de delitos financieros

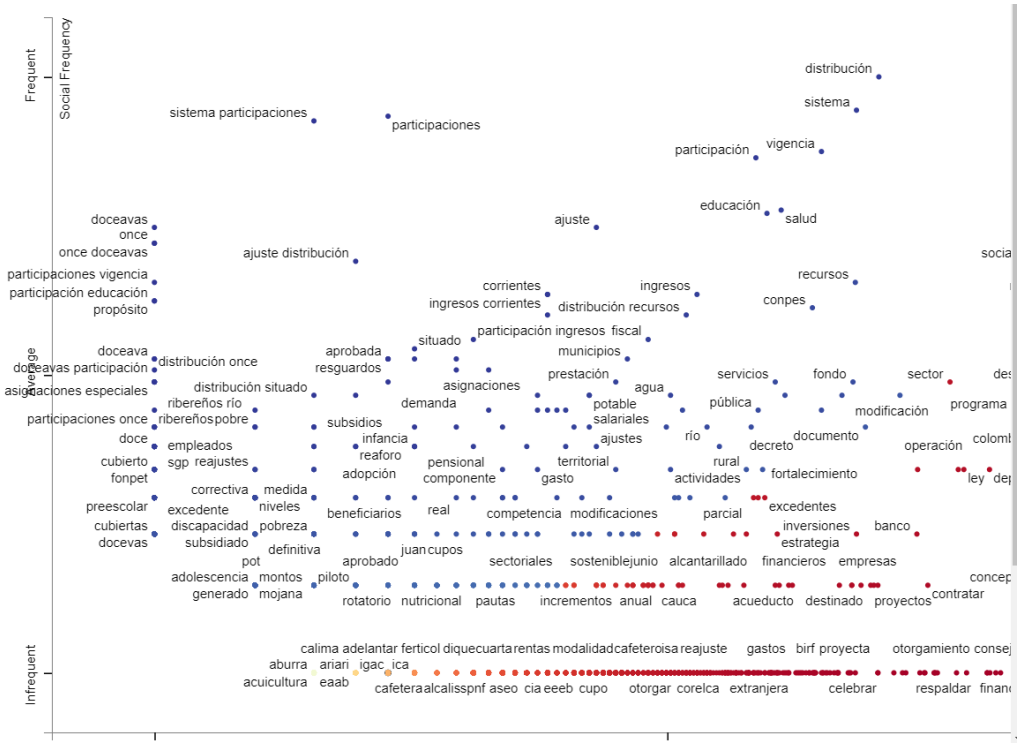
X Congreso de Prevención de Lavado de activos de las Américas

Prevención de blanqueo de capitales

Identificación de redes



PLN



Casos de Uso en la prevención de delitos financieros

X Congreso de Prevención de Lavado de activos de las Américas

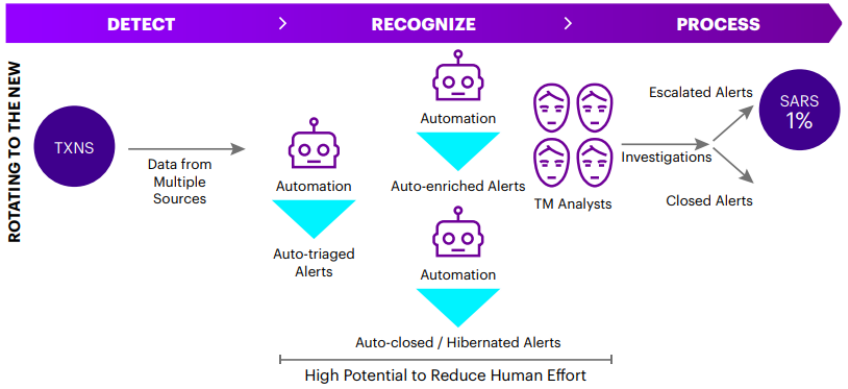
Prevención de fraude

Fraude de identidad (p.e. Identidad digital)

El ID presentado corresponde a la persona que está conectada?

Se interactúa con la persona real o es una foto?

Triage de alertas



Fuente: Acenture

Ciberseguridad

AI^2 : Training a big data machine to defend

Kalyan Veeramachaneni, CSAIL, MIT Cambridge, MA
Ignacio Arnaldo, PatternEx, San Jose, CA
Alfredo Cuesta-Infante, Vamsi Korrapati, Costas Bassias, Ke Li, PatternEx, San Jose, CA

Abstract

We present an analyst-in-the-loop security system, where analyst intuition is put together with state-of-the-art machine learning to build an end-to-end active learning system. The system has four key features: a big data behavioral analytics platform, an ensemble of outlier detection methods, a mechanism to obtain feedback from security analysts, and a supervised learning module. When these four components are run in conjunction on a daily basis and are compared to an unsupervised outlier detection method, detection rate improves by an average of 3.41×, and false positives are reduced fivefold. We validate our system with a real-world data set consisting of 3.6 billion log lines. These results show that our system is capable of learning to defend against unseen attacks.

1 Introduction

Today, information security solutions generally fall into two categories: *analyst*-driven, or *unsupervised machine learning*-driven. Analyst-driven solutions rely on rules determined by fraud and security experts, and usually lead to high rates of undetected attacks (*false negatives*), as well as delays between attack detection and implementation of preventative countermeasures. Moreover, bad actors often figure out current rules, and design newer attacks that can sidestep detection.

Using *unsupervised machine learning* to detect rare or anomalous patterns can improve detection of new attacks. However, it may also trigger more *false positive* alarms and alerts, which can themselves require substantial investigative efforts before they are dismissed. Such false alarms can cause *alarm fatigue* and *distrust*, and over time, can cause reversion to *analyst-driven* solutions, with their attendant weaknesses.

We identified three major challenges facing the information security industry, each of which could be addressed by machine learning solutions:

Lack of labeled data: Many enterprises lack labeled examples from previous attacks, undercutting the ability to use supervised learning models.

Constantly evolving attacks: Even when supervised learning models are possible, attackers constantly change their behaviors, making said models irrelevant.

Limited investigative time and budget: Relying on analysts to investigate attacks is costly and time-consuming.

A solution that properly addresses these challenges must use analysts' time effectively, detect new and evolving attacks in their early stages, reduce response times between detection and attack prevention, and have an extremely low false positive rate. We present a solution that combines analysts' experience and intuition with state-of-the-art machine learning techniques to provide an end-to-end, artificially intelligent solution. We call this system AI^2. AI^2 learns and automatically creates models that, when executed on new data, produce predictions as intelligent as those deduced by human analysts. Backed by big data infrastructure, we achieve this in close to real time.

Our contributions through this paper are as follows:

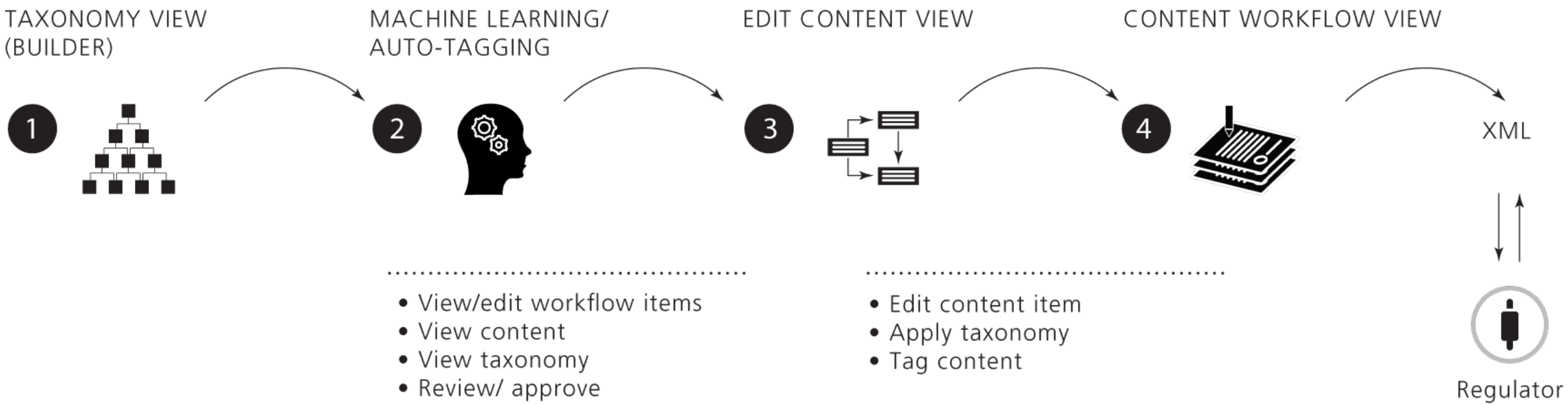
1. Developed an *Active Model Synthesis* approach, which:
   (a) computes the behaviors of different entities within a raw big data set,
   (b) presents the analyst with an *extremely* small set of events ($k <<< N$), generated by an unsupervised, machine learning-based outlier detection system,
   (c) collects analyst feedback (*labels*) about these events,
   (d) learns supervised models using the feedback,
   (e) uses these supervised models in conjunction with the unsupervised models to predict attacks, and
   (f) continuously repeats steps (a) - (e).
2. Designed multivariate methods that are capable of modeling the joint behaviors of mixed variable types (numeric and discrete ordinal). These methods include density-based, matrix decomposition-based, and replicator neural networks.
3. Demonstrated performance of the AI^2 system by monitoring a web-scale platform that generated millions of log lines per day over a period of 3 months, for a total of 3.6 billion log lines.

Summary of results: In Figure 1, we present a snapshot of our system's progress after 12 weeks of use. With 3 months' worth of data, and with awareness of attacks, we evaluate

Casos de Uso en la prevención de delitos financieros

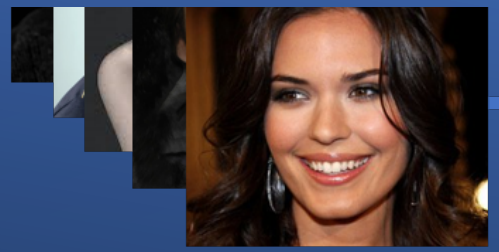
Prevención de blanqueo de capitales

RegTech

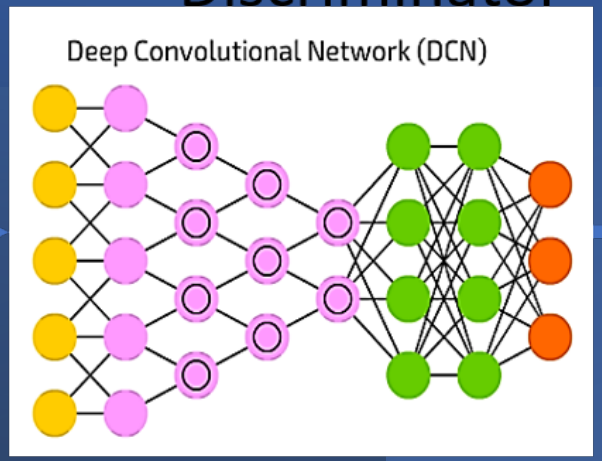


http://corlytics.com/solutions/

Modelos LLM



Discriminator

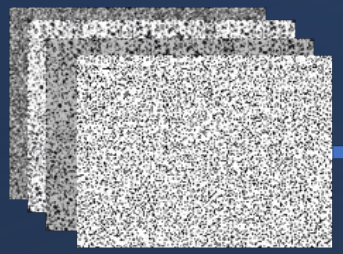


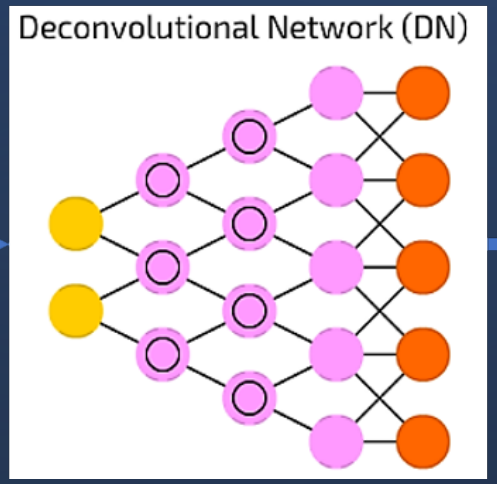
Fake

Real

Generator

Random noise





Generated faces

Taller: Uso de modelos LLM

Generación de imágenes para perfiles falsos en redes sociales

Usos antiéticos de Inteligencia Artificial

Dilemas Eticos de Uso de IA

XI Congreso de Prevención de Lavado de activos de las Américas

The New York Times

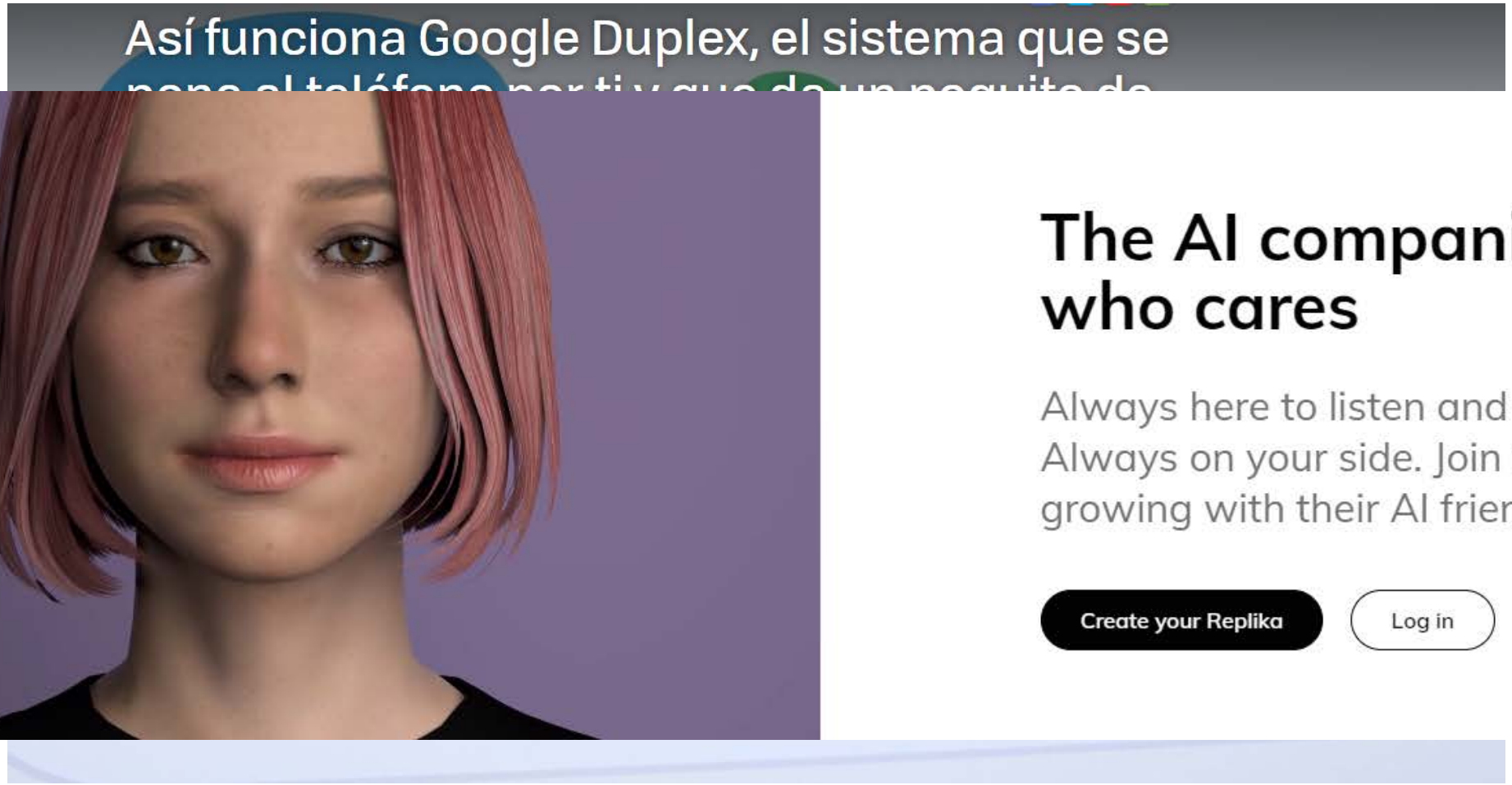
Killer Robots Aren't Regulated. Yet.

"Killing in the Age of Algorithms" is a New York Times documentary examining the future of artificial intelligence and warfare.

Dilemas Eticos de Uso de IA

XI Congreso de Prevención de Lavado de activos de las Américas

- Desconocimiento de humanos que interactúan con sistemas de IA



Autoritarismo

Dilemas Eticos de Uso de IA

TECH

Big Brother Is Watching: UK police to increase use of AI facial recognition despite inaccuracies

The UK government wants the police to use AI-based facial recognition systems more than they currently do. However, activists, AI experts and tech scholars have repeatedly warned that AI Facial Recognition doesn't work, and is prone to fail by flagging the wrong people

Mehul Reuben Das | Last Updated:September 01, 2023 12:43:50 IST

OZ ESSAY

China's new weapon of choice is your face

Article

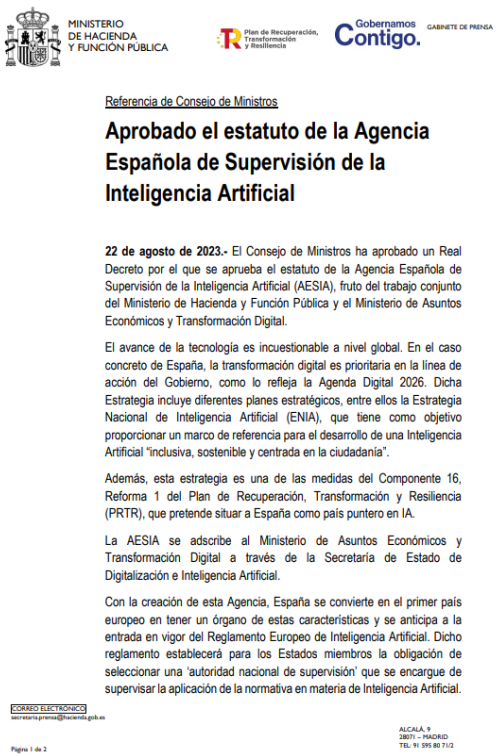
Russia: Govt. uses facial recognition technology to identify and arrest peaceful protesters

Deepfake / faceswap

Como hacer tu propio deepfake

1. Necesitas un audio de al menos 2 minutos
2. Genera la voz replicando la voz real con IA, p.e. elevenLabs
3. Toma una fotografía de la mejor resolución
4. Utiliza una plataforma de IA para “animar “ la fotografía con la voz, p.e. https://app.heygen.com/
5. Listos

Tendencia



MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

Plan de Recuperación, Transformación y Resiliencia

Gobernamos Contigo. GABINETE DE PRENSA

Referencia de Consejo de Ministros

Aprobado el estatuto de la Agencia Española de Supervisión de la Inteligencia Artificial

22 de agosto de 2023.- El Consejo de Ministros ha aprobado un Real Decreto por el que se aprueba el estatuto de la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA), fruto del trabajo conjunto del Ministerio de Hacienda y Función Pública y el Ministerio de Asuntos Económicos y Transformación Digital.

El avance de la tecnología es incuestionable a nivel global. En el caso concreto de España, la transformación digital es prioritaria en la línea de acción del Gobierno, como lo refleja la Agenda Digital 2026. Dicha Estrategia incluye diferentes planes estratégicos, entre ellos la Estrategia Nacional de Inteligencia Artificial (ENIA), que tiene como objetivo proporcionar un marco de referencia para el desarrollo de una Inteligencia Artificial "inclusiva, sostenible y centrada en la ciudadanía".

Además, esta estrategia es una de las medidas del Componente 16, Reforma 1 del Plan de Recuperación, Transformación y Resiliencia (PRTR), que pretende situar a España como país puntero en IA.

La AESIA se adscribe al Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial.

Con la creación de esta Agencia, España se convierte en el primer país europeo en tener un órgano de estas características y se anticipa a la entrada en vigor del Reglamento Europeo de Inteligencia Artificial. Dicho reglamento establecerá para los Estados miembros la obligación de seleccionar una 'autoridad nacional de supervisión' que se encargue de supervisar la aplicación de la normativa en materia de Inteligencia Artificial.

CORREO ELECTRÓNICO
secretaria.prensa@hacienda.gob.es

ALCALÁ, 9
28071 – MADRID
TEL: 91 595 80 71/2

Página 1 de 2

Gracias