IV Conferencia Científica Internacional
Universidad de las Ciencias Informáticas

Temática: Privacidad y seguridad en Internet, Tratamiento de ciberdelitos y amenazas, aspectos éticos y legales de la ciberseguridad

Enfoque transcultural de la ciberseguridad. Desafíos para el balance regional en América Latina

Cross-cultural approach to cybersecurity. Challenges for the regional balance in Latin America

Raynel Batista Tellez [1*]

[1] Universidad de las Ciencias Informáticas. 19370. rainer@uci.cu

[*] Autor para correspondencia: rainer@uci.cu

Resumen

Este reporte describe los desafíos potenciales para la ciberseguridad en América Latina a partir del uso malicioso de la inteligencia artificial (MUAI por sus siglas en inglés). Las tecnologías basadas en inteligencia artificial interaccionan con las creencias de las personas y le permiten a cualquier individuo, grupo, organización o estado-nación, influir en la conciencia pública como un nuevo tipo de arma en el sistema global. Los resultados de la investigación muestran cómo el comportamiento humano, la autoconfianza y la privacidad son afectadas por la cultura en relación con otras variables psicológicas, demográficas y tecnológicas. Se introduce un enfoque transcultural de la ciberseguridad centrado en las personas, que combina los controles técnicos y el riesgo humano en las organizaciones, y sostiene la idea de que la cultura representa un mecanismo de influencia social que a su vez esboza la distribución del poder desde la noción de la seguridad como fenómeno socio-cultural. Por lo que, el papel crítico de la cultura en la transformación digital permite entender cómo las tecnologías impulsadas por la IA se utilizan como armas geopolíticas para influir en la estabilidad política regional en América Latina y explica por qué el comportamiento humano puede representar el mayor desafío para la ciberseguridad, más allá de las implicaciones éticas de la privacidad de la información y las defensas técnicas de infraestructuras y redes de datos. El enfoque propuesto contribuye a la concepción e implementación de estrategias locales para la ciberseguridad como marcos de referencia para la integración de actores sociales del Estado, organizaciones y ciudadanía en la protección y resiliencia de activos en las redes de información.

Palabras clave: Cultura, Inteligencia Artificial, Ciberseguridad, Geopolítica

Abstract
This report describes the potential challenges to cyber security in Latin America from the malicious use of artificial intelligence (MUAI). Artificial intelligence-based technologies interact with people's beliefs and allow any individual, group, organisation or nation-state to influence public consciousness as a new type of weapon in the global system. The research results show how human behaviour, self-confidence and privacy are affected by culture in relation to other psychological, demographic and technological variables. It introduces a cross-cultural, people-centred approach to cybersecurity that combines technical controls and human risk in organisations, and supports the idea that culture represents a mechanism of social influence that in turn outlines the distribution of power from the notion of security as a socio-cultural phenomenon. Thus, the critical role of culture in digital transformation allows us to understand how AI-driven technologies are used as geopolitical weapons to influence regional political stability in Latin America and explains why human behaviour may represent the greatest challenge to cybersecurity, beyond the ethical implications of information privacy and the technical defences of data infrastructures and networks. The proposed approach contributes to the conception and implementation of local strategies for cybersecurity as frameworks for the integration of social actors from the state, organisations and citizens in the protection and resilience of assets in information networks.

Keywords: *Culture, Artificial Intelligence, Cybersecurity, Geopolitics*

Introducción

Las capacidades de la inteligencia artificial y el aprendizaje por computadoras están creciendo a un ritmo sin precedentes. El surgimiento del paradigma del Big Data ha sido resultado de siglos de desarrollo y esbozado la gran atención hacia las ciencias sociales computacionales. La inteligencia artificial está presente en muchos aspectos de la vida social. El volumen de datos continua en crecimiento y se duplica cada tres años. La revolución de los datos está empujando la conocida sociedad de la información hacia una nueva era cognitiva (WE ARE SOCIAL INC., 2020). El desarrollo de la inteligencia artificial y el aprendizaje por computadoras estimula la transición hacia un nuevo orden tecnológico en un mundo cada día más conducido por los datos. La época de la analítica ha llegado con beneficios y también con desafíos. Este tipo de tecnologías con incuestionables beneficios sociales, tienen la misma capacidad de transformar las relaciones de poder entre los Estados y desafiar el equilibrio global. Los análisis predictivos basados en la inteligencia artificial y las armas de pronósticos son nuevas tecnologías para influir en la conciencia pública, lo cual transforma a la inteligencia artificial y la geopolítica en dos campos mutuamente complementarios.

El uso malicioso de la inteligencia artificial (MUAI por sus siglas en inglés) incrementa los desafíos de la seguridad psicológica internacional (IPS por sus siglas en inglés). El MUAI adquiere mayor importancia en la desestabilización

psicológica de precisión para sistemas políticos, así como, en el sistema de las relaciones internacionales. (BAZARKINA AND PASHENTSEV, 2019). Las conocidas tecnologías disruptivas están creando un nuevo orden mundial y las instituciones democráticas están siendo testigos de una nueva forma de gobernanza.

Los desafíos relacionados con la inteligencia artificial han sido ampliamente alertados por expertos y líderes en diversos espacios globales, debates académicos y reportes gubernamentales (MARTÍ, 2017). Sin embargo, los desafíos más recientes del MUAI apuntan hacia la estabilidad política (BRUNDAGE AND AVIN ET AL, 2018) y los medios de comunicación han incluso notado esta prioridad (PURKAYASTHA, 2020). Varias instituciones regionales en América Latina reclamas acciones al respecto en pleno auge pandémico de la COVID_19 y señalan los riesgos crecientes para las economías y el equilibrio en la región (CEPAL, 2020) a partir de reportes de seguridad para el área (ESET, 2018). Las tecnologías basadas en la inteligencia artificial se están transformando en un nuevo tipo de armas que amenaza al sistema global. Por lo que, las implicaciones éticas de la inteligencia artificial han atraído la atención de la industria, la academia y la personas (HAGERTY AND RUBINOV, 2019).

En el orden de comprender las relaciones conceptuales entre las prácticas éticas y la inteligencia artificial, la investigación aporta una contribución clave: comprender el alcance de la influencia cultural. La cultura se ha entendido mayormente como un dominio social que relaciona las prácticas, los discursos y las expresiones materiales, que, con el tiempo, significan el valor de una vida desarrollada en común (JAMES ET AL., 2015): el modo de vida de un grupo de personas, sus comportamientos, patrones, creencias, valores y símbolos mutuamente aceptados. Por tanto, si la cultura es esencial para la creación de un sentido de pertenencia e identidad para cada ser humano (CANCIALOSI, 2018), entonces la percepción y comprensión de la inteligencia artificial es filtrada por los contextos sociales y culturales locales. El rol estratégico de la cultura en la transformación tecnológica permite asimismo comprender el uso de tecnologías basadas en la inteligencia artificial como armas geopolíticas que apuntan con precisión hacia la cultura de los pueblos para influir en la estabilidad política de la región (COMBI, 2016). La automatización cognitiva y la robótica están moldeando las creencias de las personas, interfiriendo en la construcción del conocimiento y manipulando modelos culturales. Si las culturas locales conducen el desarrollo tecnológico y las tecnologías invaden la vida de la gente afectando su cultura y modo de vida, entonces la cultura y la tecnología se vuelven un círculo de influencias auto-sustentado.

Por lo que, la comprensión del enfoque cultural del MUAI permitiría la formulación de estrategias a gran escala para proteger la soberanía de América Latina y reforzar su rol en el equilibrio global.

Materiales y métodos o Metodología computacional

El estudio estuvo basado en el análisis sistémico del rol que desempeñan la inteligencia artificial y la cultura en la esfera de la seguridad digital, a partir del análisis de escenarios simulados del MUAI en el balance regional y la estabilidad política. Varias fuentes fueron analizadas en grupos de publicaciones entre cinco y diez años, respectivamente. El empleo de analogías históricas permitió comprender la aplicabilidad del enfoque cultural al análisis de tecnologías conducidas por la inteligencia artificial. Los siguientes escenarios ilustran el rango de posibles usos de la inteligencia artificial con fines maliciosos y el papel que mayormente estas tecnologías podrían desempeñar en diversos contextos de la seguridad digital, sin pretender cubrir la totalidad del espectro fenomenológico de este objeto de estudio.

Los datos como un recurso

El avance creciente de las tecnologías digitales ha transformado muchas actividades económicas y sociales. El Big Data y la innovación conducida por datos están creando significativas oportunidades de negocio que aportan grandes riquezas en poco tiempo.

Las compañías líderes usan las capacidades que brindan estas tecnologías no solo para perfeccionar sus núcleos operacionales sino para crear nuevos modelos de negocios que incorporan el análisis de los datos como un uso estratégico. Los efectos de las redes sociales en las plataformas digitales están elevando la competitividad en algunos mercados (EUROMONITOR INTERNATIONAL, 2019).

La siguiente generación de herramientas podría incluso producir cambios más notables en el futuro. Las capacidades del aprendizaje profundo y asistido por computadoras han tenido variadas aplicaciones en casi todos los sectores de la economía. La era de las decisiones conducidas por datos han dibujado un mundo orientado por datos. Por lo que, el auge del Big Data está conduciendo a una transición que define nuevas reglas en el ámbito social.

El mundo ha cambiado dramáticamente en el 2020 a partir de la propagación de la pandemia COVID_19. Estos cambios que afectan prácticamente cada aspecto de la vida de la gente muestran con claridad el comportamiento digital a nivel global, especialmente cuando miles de millones de personas han dependido del uso de sus dispositivos móviles para rediseñar sus vidas y trabajar bajo regímenes de confinamiento. Por lo que, el confinamiento ha tenido un profundo impacto en los hábitos digitales de los seres humanos (WE ARE SOCIAL INC., 2020).

El informe de Economía Digital de la Conferencia de las Naciones Unidas para el Comercio y el Desarrollo (UNCTAD) ha revelado el crecimiento del comercio electrónico y el uso de medios sociales en la región

latinoamericana previo al periodo pandémico (UNCTAD, 2019) a partir del auge de la conectividad móvil (véase Anexo 1), lo cual distingue al mercado latinoamericano de telecomunicaciones y publicidad para móviles (GSMA ASSOCIATION, 2019). Por lo que se presume que el reporte de conectividad digital y publicidad relativo al 2020 reflejará un crecimiento abrumadoramente significativo, refuerza la urgencia de los principales desafíos que enfrenta la región en este escenario:

- La automatización de prácticas de publicidad e ingeniería social: la información personal de los usuarios en plataformas de redes sociales es empleada para generar sitios maliciosos para la atención al cliente, mensajería, enlaces y otros artefactos para cosechar y recolectar datos a partir del uso de bots conversacionales que simulan una persona real.
- Usuarios robots o personas falsas: Algunas formas de robots como los drones o los bots conversacionales imitan comportamientos humanos y cosechan datos masivos sin los límites que una persona real pueda tener, empleando técnicas de lenguaje natural y de cognición automatizada.

Los datos como arma geopolítica

El avance del Big Data incrementa provoca otras vulnerabilidades. El informe sobre seguridad digital en América Latina describe el incremento de los ciberataques en la región (ESET, 2018), alertando que tres de cada cinco empresas registradas habían recibido un ciberataque en 2018 (véase Anexo 2). Los países más comprometidos son Perú, México, Argentina, Brasil y Colombia. La industria de ciberseguridad en la región se cotizaba a mil millones de dólares en 2019 y proyectaba perspectivas de inversión hacia los 12 mil millones de dólares en los siguientes cinco años (véase Anexo 3) (KONKEL, 2019). Por lo que, los mercados seguirán orientando las opciones para enfrentar los desafíos del MUAI.

Sin embargo, el ámbito político sigue siendo el foco principal. Las pasadas elecciones generales en México, Colombia y Brasil reflejan el impacto de estrategias de desinformación en políticas de cambio de régimen (RADU, 2019). El auge de noticias falsas, ciberataques y la manipulación en redes sociales de las políticas y economías nacionales representan una amenaza al balance regional (DAVOS WORLD ECONOMY FORUM, 2020).

La política global está siendo conducida por una nueva maquinaria automatizada de propaganda capaz de manipular emocionalmente la opinión pública mediante el empleo intensivo de la inteligencia artificial (véase Anexo 4). La vigilancia electrónica a gran escala para perfilar el comportamiento humano crea un marco de actuación para la psicología computacional. En la medida que América Latina crece tanto económicamente como tecnológicamente, crece también el cibercrimen mientras las políticas de protección de datos sigan rezagadas (BOJALIL, 2019). Varios países como Argentina, Brasil, Chile, Colombia, Cuba, México y Perú tienen iniciativas legislativas en curso sin que alguno tenga todavía en 2020 un marco regulatorio consistente.

La UNCTAD ha anunciado que al menos 107 países en el mundo poseen algún tipo de regulación para la protección de los datos. Sin embargo, ninguna de estas iniciativas se compara con las garantías que ofrece el Maco General Regulatorio de la Unión Europea para la Protección de los Datos (GRDP por sus siglas en inglés) en vigor desde 2016 (UNCTAD, 2019). Por su parte, otra agencia de las Naciones Unidas, UNESCO, ha anunciado sus intenciones de establecer bases éticas para el desarrollo de la inteligencia artificial (UNESCO, 2019).

Por lo que los principales desafíos del MUAI en este escenario tienden a ser:

- La automatización del hacking: la inteligencia artificial se emplea para mejorar la precisión en la selección y priorización de objetivos, evadir la detección y responder a cambios de comportamiento en el objetivo. Autómatas han sido capaces de explotar vulnerabilidades en los sistemas durante mucho tiempo, pero las sofisticadas herramientas de hacking basadas en inteligencia artificial poseen un mejor desempeño, a tal punto que se comparan históricamente con hackers humanos.
- Reportes de noticias falsas basados en tecnología profunda: el uso de tecnología profunda para recrear videos con personas que no son reales permite la circulación de videos con líderes políticos haciendo comentarios inapropiados que nunca fueron hechos. Aunque el video quede desmentido, consigue afectar la base de seguidores del objetivo político marcado.
- Campañas automatizadas de desinformación: las personas son marcadas y segmentadas por distritos electorales para recibir mensajes personalizados que influyan en su intención de voto durante una convocatoria de elecciones.

Competencia cultural y distribución del poder

Los datos están evolucionando y convirtiendo las sociedades multiculturales en un mundo altamente conectado. Por lo que, la competencia cultural es claramente un objetivo primario para las organizaciones que tienen alcance regional o global (véase Anexo 5). La competencia cultural es entendida como un conjunto de comportamientos, políticas y actitudes que conforman un sistema que permite a grupos multiculturales trabajar profesionalmente. La competencia multicultural ha sido declarada como una de las diez mejores habilidades para la fuerza de trabajo del futuro. Los hallazgos científicos han demostrado durante mucho tiempo que la diversidad de pensamiento eleva la creatividad y la innovación tanto en equipos como en corporaciones (SINCLAIR, 1993) a partir de varios niveles de interacción:

- "Cultura del conocimiento" significa que las personas conocen sobre las características culturales, historia, valores, creencias y comportamientos de otro grupo étnico o cultural.
- "Creencia cultural" es la etapa posterior a la comprensión de otros grupos culturales y sus actitudes distintivas.
- "Sensibilidad cultural" es conocer la diferencia entre las culturas, pero no asignar valores a las diferencias (nada es mejor ni peor). En este punto pueden coexistir ideas o creencias que contradicen el multiculturalismo (conflictos internos, intra o inter personales u organizacionales). Aunque los conflictos sean difíciles de manejar, se pueden neutralizar mientras las personas logren concentrarse en alcanzas metas comunes.
- "Competencia cultural" incluye las anteriores etapas y agrega la efectividad operacional, pues una organización es culturalmente competente si posee la capacidad de incluir diferentes prácticas, actitudes y políticas para trabajar en un ambiente multicultural para producir mejores recursos.

Lo que la competencia cultural aporta al sistema de relaciones internacionales y distribución del poder, es la capacidad de promover la cooperación entre actores para crear un sentido de pertenencia e identidad. El concepto de poder es central a las relaciones internacionales. El poder es la producción, de y a través de las relaciones sociales, de efectos que modelan las capacidades de actores para determinar sus circunstancias y

objetivos (BARNETT AND DUVALL, 2005). El fracaso para crear conceptualizaciones alternativas del poder limita la habilidad de las relaciones internacionales para comprender cómo los recursos globales son generados y cómo los actores son empoderados para determinar sus objetivos (JORDÁN AND MARCO, 2018).

Por lo que, si la tecnología y la cultura representan un círculo de influencias, entonces la competencia multicultural podría hacer lo mismo con la distribución del poder. En ese sentido, los desafíos más notables del MUAI sería:

- Manipulación de la información disponible: algoritmos para la curación de contenidos en las plataformas de redes sociales son empleados masivamente para orientar a los usuarios hacia contenidos que puedan influir en su comportamiento y provocar desempeños específicos.
- Campañas automatizadas de influencia: el análisis de redes sociales basado en inteligencia artificial para identificar usuarios influyentes puede ser enfocado para elevar la efectividad y precisión de la desinformación.

Resultados y discusión

La Antropología posee instrumentos para el análisis de los cambios culturales y la comprensión de los efectos creados por los procesos de globalización y las tecnologías digitales en diversas sociedades. Las sociedades están cada día más mediadas a través de sistemas automatizados que desempeñan un rol determinante en procesos electorales, protestas sociales e incluso en política exterior. El rol de la tecnología en una sociedad es ya indisoluble de las relaciones sociales y los cambios socio-culturales, económicos y políticos. Las tecnologías digitales modifican el espacio, tiempo, relaciones y tipos de comunicación que aun coexisten en otros campos del conocimiento inherentes a la cultura.

El ciberespacio es un nuevo ámbito del conocimiento y la cibercultura se emplea para significar el conjunto de técnicas materiales e intelectuales, prácticas, actitudes, formas de pensamiento y valores que son expresados y desarrollados en el ciberespacio a través de los datos.

Los datos se han convertido en el recurso más valioso a nivel mundial. La escala y variedad de aplicaciones del Big Data es considerable, y lo seguirá siendo mientras continúe la expansión de la digitalización como la base fundacional de la siguiente sociedad moderna de la información.

América Latina es el cuarto mercado de telefonía móvil más grande del mundo y más de la mitad de su población emplea internet. Fortinet es una de las compañías líderes en la región que provee servicios de protección de internet. En Perú cubre prácticamente el 60% de los dispositivos, seguido de Brasil, Colombia, Chile, México, Venezuela y Argentina. Las compañías de Israel son también los mayores proveedores de protección de internet en la región. Verint y Elbit son también proveedores líderes en servicios de ciberseguridad: ¿un nuevo tipo de colonización?

En este escenario, Latinoamérica tiene un reto: pocos países tienen una estrategia nacional de ciberseguridad y están expuestos a los ciberataques, las compañías que ofrecen servicios de protección de internet son mayormente de Israel y de EE.UU., las cuales también fuerzan para ganar el mercado de 5G ante el avance de compañías de China en la región.

El espionaje electrónico es otra de las estrategias que involucre la intervención en las políticas internas de los Estados. Pero existen otras estrategias más indirectas que tienen un profundo impacto en escenarios políticos, como la ciberseguridad en procesos electorales. Varias de las campañas electorales en la región durante el periodo 2015-2019 han sido vinculadas a escándalos por el uso no autorizado de información personal de los usuarios en redes sociales para diseminar mensajes con precisión en Whatsapp para influir en intenciones de voto.

El riesgo potencial de que estas prácticas continúen repitiéndose, conectado al teatro de operaciones psicológicas que distingue la manipulación de la opinión pública, ha alarmado a analistas, líderes políticos e incluso a la seguridad mundial. Sin embargo, otros ven el problema como una oportunidad para expandir servicios y mercados, que ciertamente, son considerables, mientras la dinámica de las telecomunicaciones siga marcada por el auge de tecnologías emergentes como la 5G.

La articulación de la ciberseguridad con un enfoque militar evidencia que el perfil de las compañías dedicadas a proveer servicios de protección tiene por lo general una conexión con la venta de armas y servicios de inteligencia. En el caso de las compañías israelitas NSO, Elbit Systems Ltd. o Israel Aerospaces Industries, entre otras, reflejan la penetración del Estado de Israel en la región a través de este tipo de negocios, con significativas consecuencias para las soberanías nacionales, al comprometerse el acceso a información sensible. Por otro lado, la militarización de las redes sociales, con el desarrollo de armas electrónicas para neutralizar ciberataques, en el marco de la carrera armamentista, señalan la ciberseguridad como parte de la guerra híbrida.

Mientras, el caso de Venezuela muestra cómo los ciberataques al sistema eléctrico representan la puesta en práctica de un nuevo tipo de arma. El control de la energía eléctrica, los sistemas hidráulicos, los datos electorales, son solo algunos de los elementos más vulnerables en el mundo donde la tecnología confluye aspectos de la vida pública y

privada. Por lo que, la urgencia de que la ciberseguridad sea un bien público abre el debate para definir sus objetivos y alcance.

Los países con mayores oportunidades para ganar la carrera de la inteligencia artificial son aquellos que posean una extensa fuerza de trabajo para desarrollar proyectos propios. Los recursos humanos representan el núcleo del desarrollo de la inteligencia artificial y serán los que podrán limitar y modelar el alcance de la inteligencia artificial en el futuro. Sin embargo, ¿quién dictará los límites?, ¿qué rol jugará la inteligencia artificial en la creación de nuevos modelos de crecimiento si los países dependen de modelos económicos basados en el pasado?, ¿quiénes o qué permitirá el control de los algoritmos que ya poseen el control en las sociedades?

La inteligencia artificial segura requiere de la inteligencia cultural, cambios en los códigos culturales, comportamientos y campos del conocimiento. La investigación sigue abierta a una variedad de direcciones para modelar otros escenarios, entre los que resalta para futuros trabajos los nuevos modelos de inteligencia artificial para el desarrollo basados en el talento para estrategias de ciberseguridad.

.

Referencias

- BARNETT, M. AND DUVALL, R. (2005) 'POWER IN INTERNATIONAL POLITICS', INTERNATIONAL ORGANIZATION. CAMBRIDGE UNIVERSITY PRESS, 59(1), PP. 39–75. DOI: 10.1017/S0020818305050010.
- BAZARKINA, D. Y. AND PASHENTSEV, E. N. (2019) 'ARTIFICIAL INTELLIGENCE AND NEW THREATS TO INTERNATIONAL PSYCHOLOGICAL SECURITY', RUSSIA IN GLOBAL AFFAIRS. FOREIGN POLICY RESEARCH FOUNDATION, 17(1), PP. 147–170. DOI: 10.31278/1810-6374-2019-17-1-147-170.
- BOJALIL, P. (2019) DESPUNTAN LAS REFORMAS EN MATERIA DE PROTECCIÓN DE DATOS EN AMÉRICA LATINA - ABIERTO AL PÚBLICO, BID. AVAILABLE AT: HTTPS://BLOGS.IADB.ORG/CONOCIMIENTO-ABIERTO/ES/PROTECCION-DE-DATOS-GDPR-AMERICA-LATINA/ (ACCESSED: 21 MAY 2020).
- BRUNDAGE AND AVIN ET AL (2018) THE MALICIOUS USE OF ARTIFICIAL INTELLIGENCE: FORECASTING, PREVENTION, AND MITIGATION. AVAILABLE AT: HTTPS://MALICIOUSAIREPORT.COM/ (ACCESSED: 20 MAY 2020).

- CANCIALOSI, C. (2018) THE CRITICAL ROLE OF CULTURE IN TECHNOLOGY TRANSFORMATION, FORBES. AVAILABLE AT: HTTPS://WWW.FORBES.COM/SITES/CHRISCANCIALOSI/2018/11/06/THE-CRITICAL-ROLE-OF-CULTURE-IN-TECHNOLOGY-TRANSFORMATION/#7A4810963807 (ACCESSED: 21 MAY 2020).
- CEPAL (2020) COVID-19 THE SOCIAL CHALLENGE IN TIMES OF COVID-19. AVAILABLE AT: HTTPS://WWW.WELIVESECURITY.COM/WP-CONTENT/UPLOADS/2018/06/ESET_SECURITY_REPORT_LATAM2018.PDF.
- COMBI, M. (2016) 'CULTURES AND TECHNOLOGY: AN ANALYSIS OF SOME OF THE CHANGES IN PROGRESS-DIGITAL, GLOBAL AND LOCAL CULTURE', IN CULTURAL HERITAGE IN A CHANGING WORLD. SPRINGER INTERNATIONAL PUBLISHING, PP. 3–15. DOI: 10.1007/978-3-319-29544-2_1.
- DAVOS WORLD ECONOMY FORUM (2020) THE GLOBAL RISKS REPORT 2020 INSIGHT REPORT 15TH EDITION.
- ESET (2018) SECURITY REPORT. AVAILABLE AT: HTTPS://WWW.WELIVESECURITY.COM/WP-CONTENT/UPLOADS/2018/06/ESET_SECURITY_REPORT_LATAM2018.PDF (ACCESSED: 20 MAY 2020).
- EUROMONITOR INTERNATIONAL (2019) DIGITAL LANDSCAPE IN LATIN AMERICA | MARKET RESEARCH REPORT | EUROMONITOR. AVAILABLE AT: HTTPS://WWW.EUROMONITOR.COM/DIGITAL-LANDSCAPE-IN-LATIN-AMERICA/REPORT (ACCESSED: 20 MAY 2020).
- GSMA ASSOCIATION (2019) LATIN AMERICA´S EVOLVING DIGITAL LANDSCAPE. LONDON. AVAILABLE AT: WWW.GSMAINTELLIGENCE.COM (ACCESSED: 20 MAY 2020).
- HAGERTY, A. AND RUBINOV, I. (2019) GLOBAL AI ETHICS: A REVIEW OF THE SOCIAL IMPACTS AND ETHICAL IMPLICATIONS OF ARTIFICIAL INTELLIGENCE. AVAILABLE

AT: HTTPS://ARXIV.ORG/FTP/ARXIV/PAPERS/1907/1907.07892.PDF (ACCESSED: 21 MAY 2020).

- IFTF (2011) IFTF: FUTURE WORK SKILLS 2020, IFTF. AVAILABLE AT: HTTP://WWW.IFTF.ORG/FUTUREWORKSKILLS/ (ACCESSED: 21 MAY 2020).
- JAMES, P. ET AL. (2015) URBAN SUSTAINABILITY IN THEORY AND PRACTICE CIRCLES OF SUSTAINABILITY CHAPTER 8. MEASURING COMMUNITY SUSTAINABILITY: THE SOCIAL LIFE QUESTIONNAIRE.
- JORDÁN, J. AND MARCO, D. (2018) 'UN MODELO DE ANÁLISIS GEOPOLÍTICO PARA EL ESTUDIO DE LAS RELACIONES INTERNACIONALES', IEEE.ES, 04, PP. 1–44. AVAILABLE AT: HTTP://WWW.IEEE.ES/GALERIAS/FICHERO/DOCS_MARCO/2018/DIEEEM04-2018_GEOPOLITICA_RRII_JAVIERJORDAN.PDF.
- KONKEL, F. (2019) REPORT: 2020 IS THE YEAR DATA GETS WEAPONIZED - NEXTGOV, NEXTGOV. AVAILABLE AT: HTTPS://WWW.NEXTGOV.COM/CYBERSECURITY/2019/10/REPORT-2020-YEAR-DATA-GETS-WEAPONIZED/160984/ (ACCESSED: 21 MAY 2020).
- MARTÍ, A. (2017) LO NUEVO DE ELON MUSK Y FUTURE OF LIFE SON 23 PRINCIPIOS PARA UN DESARROLLO SEGURO DE LA INTELIGENCIA ARTIFICIAL, XATAKA. AVAILABLE AT: HTTPS://WWW.XATAKA.COM/ROBOTICA-E-IA/LO-NUEVO-DE-ELON-MUSK-Y-LOS-DE-FUTURE-OF-LIFE-SON-23-PRINCIPIOS-PARA-EL-DESARROLLO-DE-INTELIGENCIA-ARTIFICIAL (ACCESSED: 20 MAY 2020).
- PURKAYASTHA, K. (2020) 'CHALLENGES FROM MALICIOUS USE OF AI', DAILY OBSERVER, 18 MAY. AVAILABLE AT: HTTPS://WWW.OBSERVERBD.COM/NEWS.PHP?ID=257035 (ACCESSED: 20 MAY 2020).
- RADU, S. (2019) MEXICO, COLOMBIA AND BRAZIL FACED HEAVY AMOUNTS OF DISINFORMATION IN 2018 ELECTIONS | BEST COUNTRIES | US NEWS. AVAILABLE AT: HTTPS://WWW.USNEWS.COM/NEWS/BEST-COUNTRIES/ARTICLES/2019-08-02/MEXICO-

COLOMBIA-AND-BRAZIL-FACED-HEAVY-AMOUNTS-OF-DISINFORMATION-IN-2018-ELECTIONS (ACCESSED: 21 MAY 2020).

- SINCLAIR, A. (1993) 'APPROACHES TO ORGANISATIONAL CULTURE AND ETHICS', JOURNAL OF BUSINESS ETHICS. KLUWER ACADEMIC PUBLISHERS, 12(1), PP. 63–73. DOI: 10.1007/BF01845788.
- UNCTAD (2019) DIGITAL ECONOMY REPORT 2019. AVAILABLE AT: HTTPS://UNCTAD.ORG/EN/PUBLICATIONSLIBRARY/DER2019_EN.PDF (ACCESSED: 20 MAY 2020).
- UNESCO (2019) ESTUDIO PRELIMINAR SOBRE LOS ASPECTOS TÉCNICOS Y JURÍDICOS RELATIVOS A LA CONVENIENCIA DE DISPONER DE UN INSTRUMENTO NORMATIVO SOBRE LA ÉTICA DE LA INTELIGENCIA ARTIFICIAL - UNESCO DIGITAL LIBRARY. AVAILABLE AT: HTTPS://UNESDOC.UNESCO.ORG/ARK:/48223/PF0000367422_SPA (ACCESSED: 20 MAY 2020).
- WE ARE SOCIAL INC. (2020) DIGITAL AROUND THE WORLD IN APRIL 2020 - WE ARE SOCIAL. AVAILABLE AT: HTTPS://WEARESOCIAL.COM/BLOG/2020/04/DIGITAL-AROUND-THE-WORLD-IN-APRIL-2020 (ACCESSED: 20 MAY 2020).

Anexos

Anexo 1

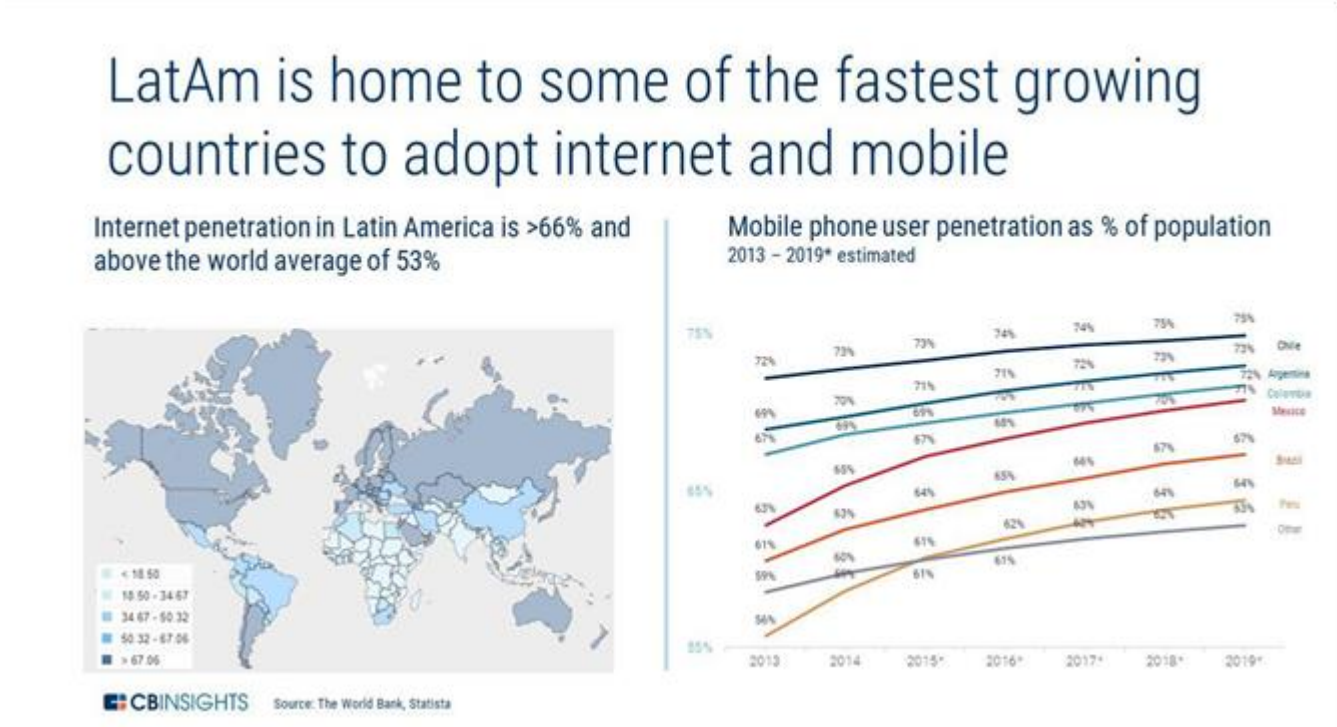
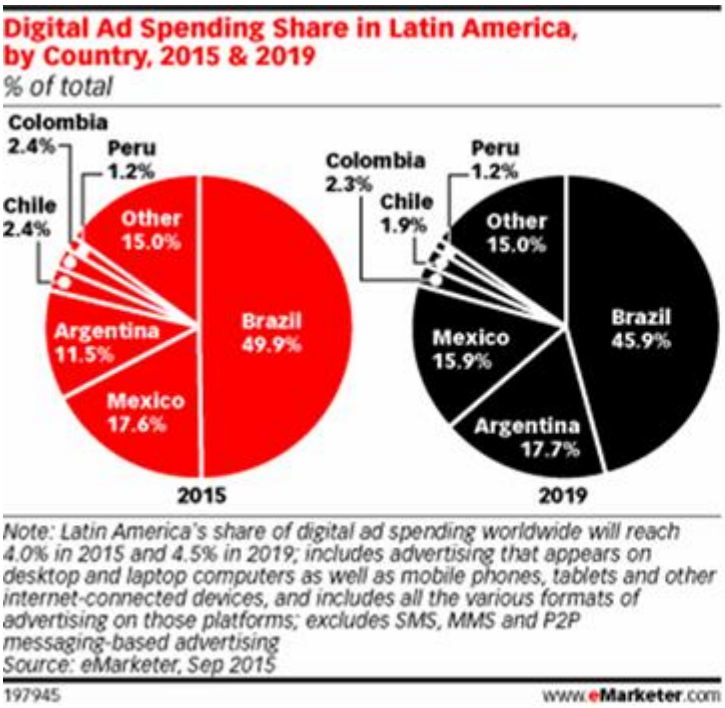
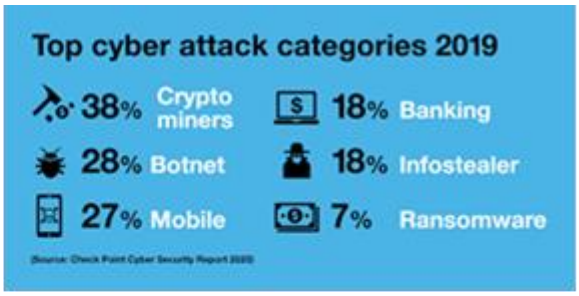


Figura 1. Comportamiento de la adopción de internet en América Latina (2013-2019), (Euromonitor, 2019)

Anexo 2





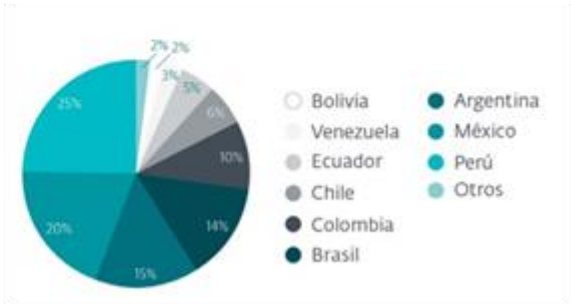


Figura 2. Gasto en publicidad digital en América Latina (2015-2019) y Ciberataques (2019), (Davos World Economy Forum, 2019).

Anexo 3

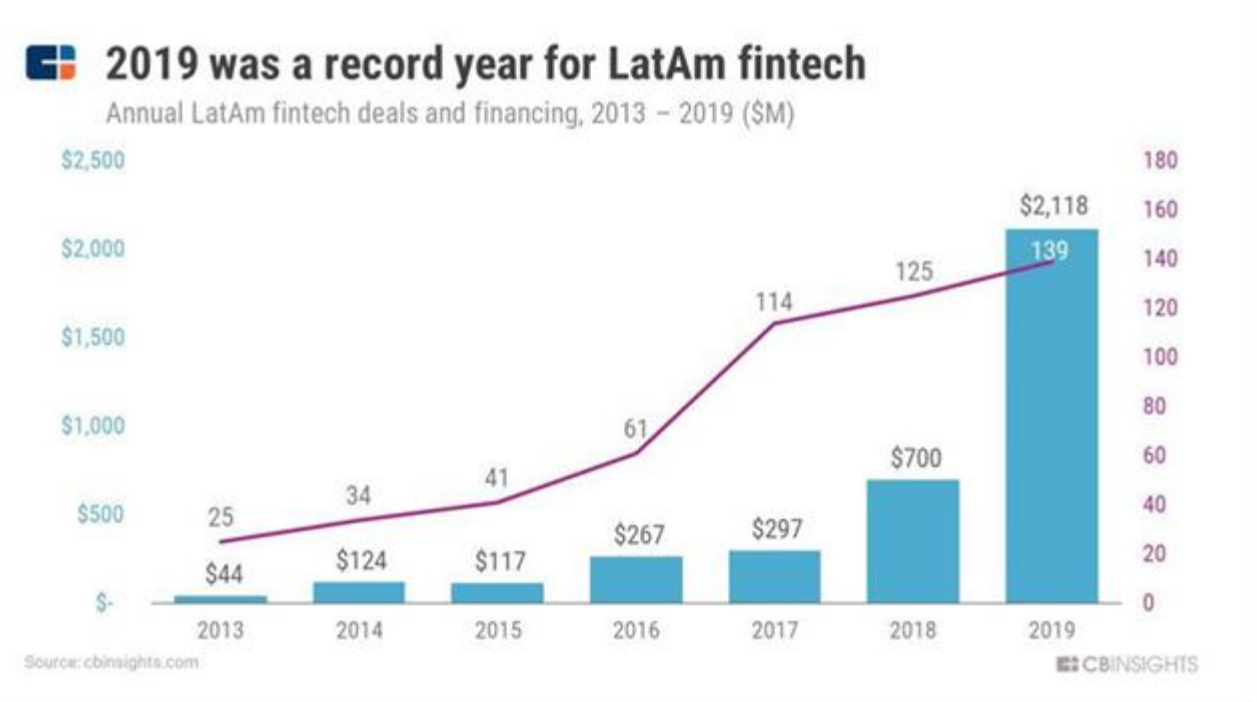


Figura 3. Digital Economy Report 2019 (UNCTAD, 2019).

Anexo 4

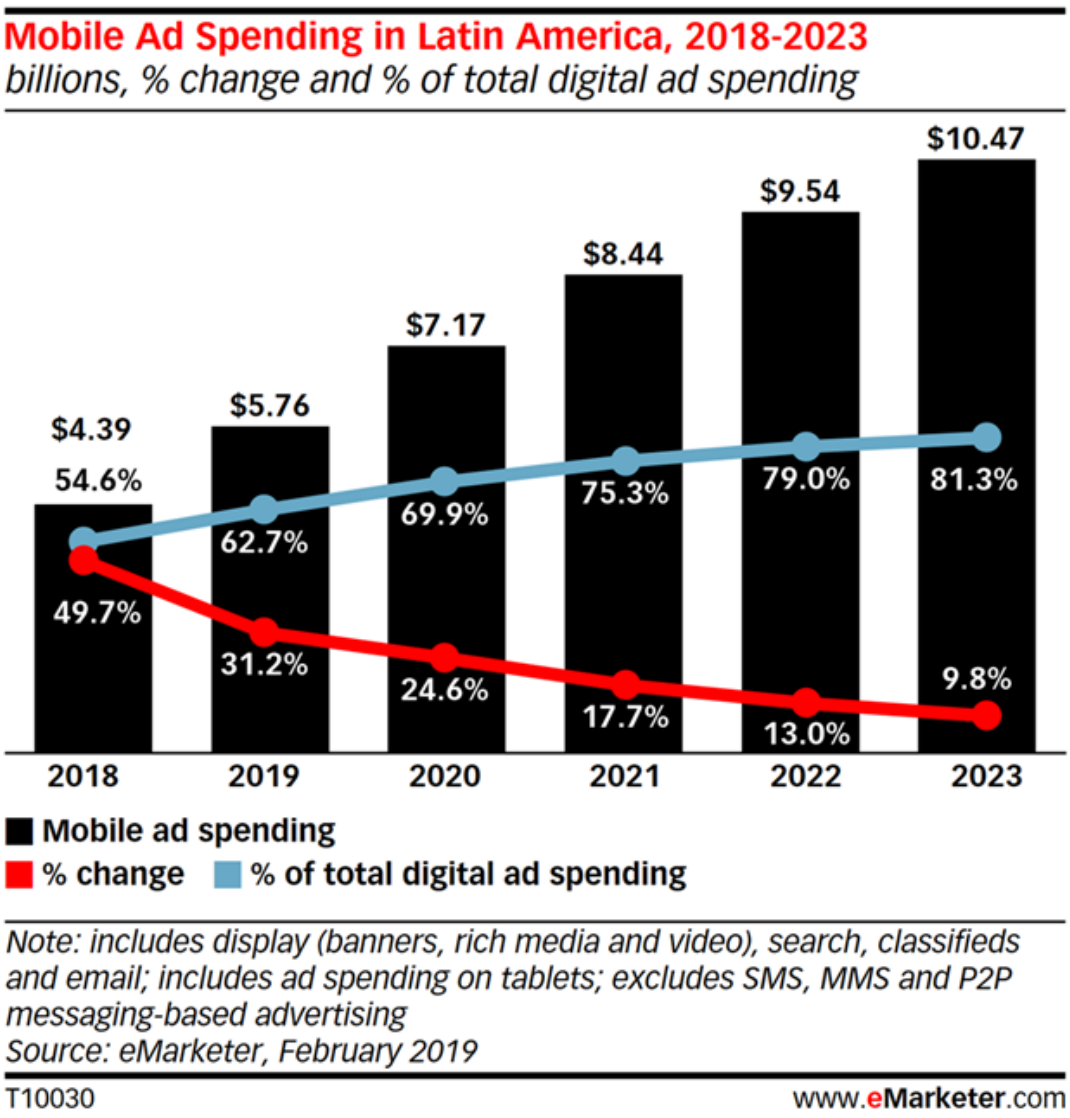


Figura 4. Tendencia del gasto en publicidad digital móvil en América Latina (2018-2023), Digital Economy Report 2019 (UNCTAD, 2019).

Anexo 5

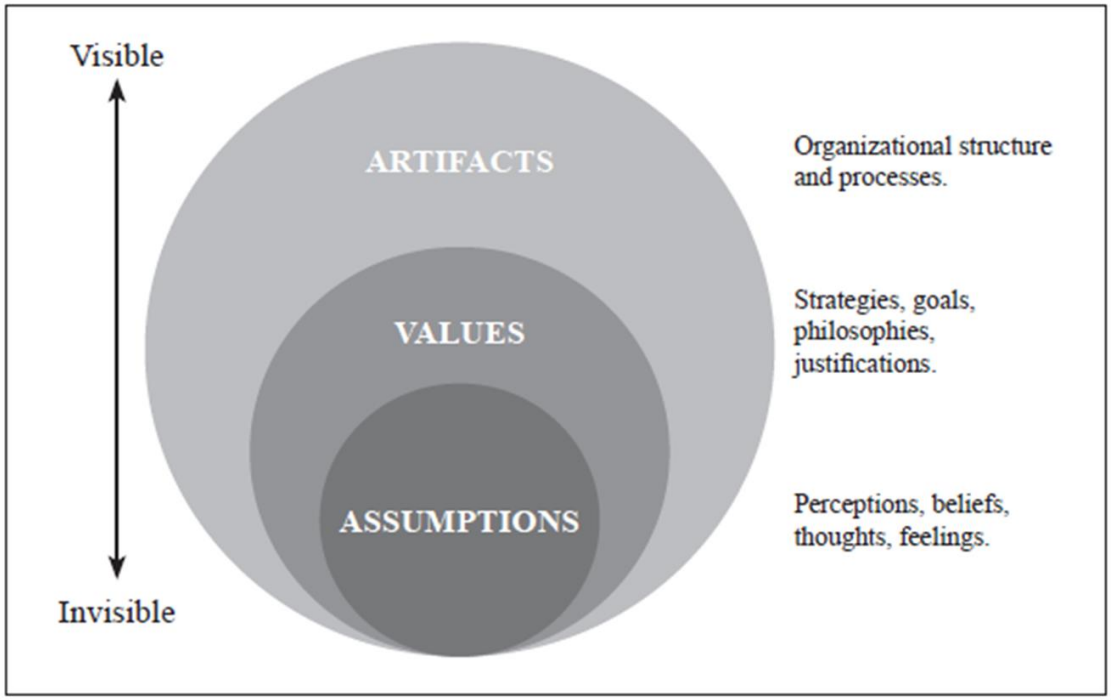


Figura 5. Modelo de cultura organizacional, (Sinclair, 1993).