EDI

DICIEMBRE DE 2024 - EDICIÓN NRO 41

ELDERECHOINFORMATICO.COM

EL PERSONAJE DEL AÑO

Revista Digital Distribución gratuita

SOMOS LA RED

VAMOS DEJANDO HUELLA

ELDERECHOINFORMATICO.COM

EDITORIAL

Se tardó, pero algún día iba a salir esta edición, casi 2 años desde la última, sucedieron demasiadas cosas como para que siga pasando el tiempo, y entonces llegó, este año 2024 ha sido testigo de gigantescos avances en lo tecnológico y en el derecho informático, por poner una analogía, podría decir que han surgido nuevos cauces donde veremos el rio correr.

Crece la complejidad de las amenazas en internet, el desarrollo continuo de las tecnologías que rompen lo conocido y con ello la necesidad de reformar los paradigmas conocidos planteando un desafío para la sociedad, juristas y expertos en seguridad.

Delitos informáticos, que van desde el ransomware hasta el phishing, han requerido un análisis de estrategias en materia de ciberseguridad. Las entidades e instituciones deben invertir en herramientas tecnológicas modernas y una pedagogía implacable. El Internet de las cosas y la inteligencia artificial son omnipresentes en la actualidad.

A pesar de las contras, el futuro es más brillante y preocupante que nunca. El uso de la inteligencia artificial será cada vez más relevante a la hora de detectar delitos informáticos así como para mejorar la aplicación de la justicia. La capacidad de la IA para analizar grandes cantidades de datos, identificar patrones y pronosticar comportamientos ilícitos con precisión es una ventaja significativa en la batalla contra los infractores.

Ha sido un año de aprendizaje y desarrollo. Creo que las nuevas herramientas, abrirá puertas y permitirá enfrentar los desafíos. El camino hacia un internet seguro y justo es largo, pero con esfuerzo podemos crear un entorno en el que las herramientas digitales sean eficaces para defender una sociedad más justa y por ende una justicia acorde a ella.

DICCIONARIO
DE DERECHO INFORMÁTICO

GLOSARIO DE TÉRMINOS DE DERECHO DIGITAL
Y MATERIAS AFINES

Conseguilo en: https://www.hammurabi.com.ar/productos/zamora-diccionario-de-derecho-informatico/

1ª EDICIÓN

hammurabi
JOSE LUIS DEPALMA EDITOR

Edición n° 41

INDICE

sumate a la campaña de elderechoinformatico.com

#atentodigital

"Nunca compartas información bancaria por teléfono o internet."

NO IMPORTA QUIENES DIGAN QUE SON:

- NO DES CÓDIGOS
- NO DESCARGUES SOFTWARE
- NO HAGAS CLICK EN ENLACES

MARÍA EUGENIA
SAMANIEGO VINTIMILLA

PROTECCIÓN DE DATOS PERSONALES SENSIBLES: FALTA DE CLASIFICACIÓN POR PARTE DE LA JUSTICIA ECUATORIANA RESPECTO A DATOS PERSONALES SENSIBLES DE SALUD

Maestría en Derecho con orientación en Dirección de Empresas - Universidad de Palermo, Argentina (2009-2011) - Universidad del Azuay (2000-2006) Abogada con más de 15 años de experiencia en la gestión de proyectos judiciales, administración de sistemas informáticos y asesoría legal. Especializada en la mejora de plataformas electrónicas y gestión de sistemas informáticos para administración de justicia. Sólida experiencia en la elaboración de normativa y reformas legales, con enfoque en la mejora continua de los procesos en la administración de justicia en el Ecuador

En el 2018 un trabajador fue despedido intempestivamente, ante este hecho, demandó a su empleador a través de una acción de protección por la vulneración al derecho a la prohibición de discriminación basado en las categorías del estado de salud y por portar VIH. En Ecuador las acciones constitucionales se conocen en dos instancias, en las cuales, un juez y posteriormente un tribunal, establecieron que el trabajador tenía la obligación de revelar al empleador la información personal referente a la condición de portador del VIH, al no hacerlo, el despido se consideró eficaz, por lo que negaron la acción de protección.

Posteriormente, el trabajador presenta una acción extraordinaria de protección ante la Corte Constitucional, la cual fue aceptada y se ordenó reparación para el trabajador por parte del empleador, adicionalmente, se reconoció la vulneración del debido proceso y el derecho del trabajador a mantener su privacidad respecto a su salud.

Lo que vamos a entrar a analizar en este caso es respecto a la protección de los datos personales sensibles del accionante que va mucho más allá de las resoluciones de la justicia. En este sentido, tanto el Consejo de la Judicatura como la Corte Constitucional del Ecuador tienen el deber jurídico de realizar un tratamiento adecuado a los datos personales de quienes formen

parte de sus procesos en cuanto a administración de justicia se refiere.

Para el cumplimiento de este deber, el Pleno de la Corte Constitucional a través de la resolución 009-CCE-PLE-2021, expidió el "Protocolo de la Información Confidencial de la Corte Constitucional", mismo que recoge procedimientos administrativos que empiezan desde el ingreso de las causas hasta su culminación con la resolución de los jueces y las juezas del organismo. En tal virtud, cuando la jueza sustanciadora emitió la providencia en que avocó conocimiento del caso objeto de este análisis, estableció, en una nota al pie de página respecto a las iniciales del accionante, lo siguiente: *"En atención al artículo 66 de la Constitución, así como del Protocolo de la Información Confidencial de la Corte Constitucional, se dispone mantener en reserva los nombres y datos del accionante"*. Si bien lo establecido es correcto, quizá la importancia que se le dio al asunto fue menor.

Es fácilmente identificable el nombre de la persona que presenta la acción y los hechos pormenorizados en la ficha de este caso en la que constan todos los documentos que conforman el expediente constitucional. Inclusive, se expone el número de caso de la justicia ordinaria en el que se originó este tema, en el cual también se pueden verificar la identidad del accionante y los hechos del caso.

La sentencia se dictó en este año, 2024, no obstante, en ningún momento se estableció en la sentencia ni en el auto de reparación, la clasificación de la información de este caso, tanto por la justicia ordinaria en donde se originó, como en el Corte Constitucional, por lo tanto, la identidad y los hechos del caso son actualmente públicos[1].

Análisis de la Falta de Clasificación en Casos de Discriminación Laboral:

La protección de los datos personales es un derecho fundamental reconocido por la Constitución de la República del Ecuador y por la legislación internacional, especialmente en el marco de la protección de la privacidad y la no discriminación. Sin embargo, cuando se trata de personas que viven con el Virus de

[1] En este artículo no se ha podido citar los números de proceso tanto en la Corte Constitucional como en el Consejo de la Judicatura, puesto que la información sensible del accionante sigue siendo pública.

Inmunodeficiencia Humana (VIH), la relevancia de este derecho se intensifica, dado el estigma social y las consecuencias discriminatorias que aún enfrentan en distintos ámbitos, incluido el laboral.

En este contexto, el caso de una persona que presentó una demanda por discriminación laboral contra su empleador debido a su condición de portador de VIH, y en el que la identidad del demandante no fue adecuadamente clasificada en el proceso judicial, ilustra una serie de fallos preocupantes en cuanto al respeto de la privacidad y los derechos humanos en la justicia ecuatoriana. Esta omisión no solo pone en evidencia la falta de sensibilización y protección en torno a las personas con VIH, sino que también expone las vulnerabilidades en el tratamiento de datos sensibles dentro del sistema judicial.

La misma Corte Constitucional garantizó en parte la privacidad del accionante, no obstante, si no se hace un esfuerzo conjunto por parte de todo el personal y si no se realizan resoluciones claras para su ejecución obligatoria y correcta, el resultado es que el actor, a pesar de habérsele reconocido su vulneración, sigue su caso siendo expuesto en las páginas web de quienes administraron justicia y declararon vulnerable y sensible su información de salud, lo cual podría generar varias situaciones de discriminación para el accionante.

Por otro lado, el Consejo de la Judicatura, mediante Resolución 043-2024 expidió el Reglamento para el tratamiento de datos personales, en cuyo artículo 6 establece el siguiente procedimiento:

Los legitimados para requerir la modificación, rectificación u ocultamiento de datos personales dentro de procesos judiciales, podrán solicitar el respectivo tratamiento de los mismos a la o el juzgador o al tribunal a cargo de las causas donde estos se encuentren visibles y públicos. Para ello, deberán formular su requerimiento debidamente fundamentado por escrito, a la o el juzgador o tribunal, dentro de los respectivos procesos judiciales. Para este efecto, tendrán disponible la Oficina de Gestión Judicial Electrónica o las ventanillas físicas de las respectivas dependencias judiciales.

Cabe resaltar que, dentro de los fundamentos que se establecen para la emisión de este reglamento, se cita tanto la Constitución como la Ley de Protección de Datos Personales. En eso sentido, se cita al artículo 11, numerales 2 y 3 de la Constitución de la República del Ecuador, que determinan que todas las personas son iguales y gozarán de los mismos derechos, deberes y oportunidades establecidos en la norma constitucional y en los instrumentos internacionales de derechos humanos, los cuales son de directa e inmediata aplicación, prohibiendo de tal manera toda forma de discriminación.

En todo caso, el Reglamento referido y expedido por el Consejo de la Judicatura, se excluye de la responsabilidad de dar el tratamiento adecuado a los datos personales, diluyendo las responsabilidades entre los legitimados en los procesos y los jueces. A diferencia de la Corte Constitucional que en su protocolo regula un procedimiento que depende de la secretaría general y los jueces del organismo.

No obstante, todo esto resulta ser insuficiente, si los funcionarios a cargo de estos procedimientos no están capacitados en el cuidado de la información y la protección de datos personales.

El Derecho a la Privacidad y la Protección de Datos Personales

La Constitución de Ecuador garantiza el derecho a la intimidad personal y familiar, así como la protección de los datos personales[2] (art. 66, inciso 19). Además, el país es parte de varios tratados internacionales[3], que establecen la obligación de respetar y proteger la vida privada y los datos personales de los individuos. Esto incluye, en particular, la protección de información relacionada con la salud, que es considerada como un dato sensible que debe ser manejado con extremo cuidado.

En el caso de las personas con VIH, esta protección es aún más crucial debido al historial de estigmatización social que enfrentan. El VIH no solo es un desafío médico, sino también un factor de discriminación que puede tener consecuencias devastadoras en la vida personal, social y laboral de

[2] Art. 66, numeral 19 de la Constitución del República del Ecuador

[3] Convención Americana sobre Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos

quienes lo padecen. Por ello, la divulgación no autorizada de su estado serológico puede constituir una violación a sus derechos humanos y un acto de discriminación.

El hecho de que una persona con VIH haya decidido demandar a su empleador por discriminación es una acción valiente para visibilizar y confrontar esta problemática. Sin embargo, el proceso judicial debe garantizar que la identidad del demandante, así como su estado serológico, no se divulgue sin su consentimiento. La falta de una clasificación adecuada de esta información dentro del proceso judicial no solo afecta el principio de confidencialidad, sino que también compromete el derecho a la no discriminación.

La Falta de Clasificación de la Identidad en el Proceso Judicial

En el caso mencionado, la justicia ecuatoriana no clasificó de manera adecuada la identidad de la persona que presentó la demanda, lo que pudo haber resultado en la exposición de su estado de salud en el curso del proceso judicial. Este tipo de descuido no solo constituye una vulneración al derecho de privacidad, sino que también pone en riesgo la seguridad y el bienestar del demandante, quien podría enfrentar consecuencias graves por la divulgación de información confidencial sobre su salud.

A pesar de que en el caso de la Corte Constitucional no figura el nombre del accionante, al realizar una búsqueda en internet con el nombre del demandante, el primer resultado de la búsqueda es un documento del caso llevado a la Corte Constitucional, lo que nos puede conducir fácilmente a los hechos de la demanda y la situación sensible de salud del accionante. Esto quiere decir que el dato no fue eliminado, sino oculto, pero para buscadores como Google, esa información no pasa desapercibida.

Actualmente, en la selección de personal, se utiliza mucho este tipo de búsquedas, así como en redes sociales, con el fin de tener un antecedente de la persona que se requiere contratar, en este caso particular, quizá sin saberlo, esta persona puede estar siendo reiteradamente discriminada.

La legislación ecuatoriana establece la obligación de clasificar

correctamente la información sensible, como lo es el estado serológico de una persona con VIH. Sin embargo, la falta de cumplimiento de estas normas dentro del sistema judicial demuestra que aún existen deficiencias en la protección de datos sensibles en el ámbito judicial. Es fundamental que las autoridades judiciales sean capacitadas y sensibilizadas sobre la importancia de tratar con respeto y responsabilidad los datos relacionados con la salud de los involucrados en un proceso judicial.

Consecuencias de la Falta de Protección de Datos

Las consecuencias de una violación en la protección de los datos personales de una persona con VIH pueden ser severas. En primer lugar, la divulgación no autorizada de esta información puede acarrear discriminación adicional y daños psicológicos, ya que el individuo podría ser estigmatizado en su comunidad o en su entorno laboral. Además, la falta de privacidad podría generar un clima de desconfianza en el sistema judicial, lo que desincentiva a otras personas con VIH a presentar demandas similares por miedo a que sus derechos sean vulnerados.

Por otro lado, la falta de clasificación adecuada de datos personales en los procesos judiciales podría tener repercusiones legales para el Estado y sus instituciones, ya que violaría derechos fundamentales garantizados en la Constitución y los tratados internacionales ratificados por Ecuador.

Conclusión

Como este ejemplo, existen varios en la justicia ecuatoriana, manejando con total discrecionalidad y cuidados superficiales la clasificación o eliminación de datos personales sensibles, e incluso, revirtiendo la responsabilidad a la ciudadanía para que, soliciten, de manera fundamentada, el ocultamiento de sus datos personales.

Es importante que se tomen medidas, proceso y ajustes técnicos por parte de las instituciones encargadas de procesos de justicia, para que, además de que se respete la reserva legal de ciertos casos, se garantice la publicidad de aquellos en los que no se vulneren datos personales sensibles que puedan desencadenar procesos de discriminación o de peligro.

En este caso en particular, la omisión en la clasificación adecuada de la identidad de una persona que demanda por discriminación laboral en razón de su estado de salud, pone en evidencia la necesidad urgente de mejorar los protocolos de manejo de datos personales en el ámbito judicial. Es esencial que se implementen reformas y capacitaciones para garantizar que los derechos de la protección de datos personales sensibles sean plenamente respetados, no solo en el plano legal, sino también en la práctica cotidiana de los procedimientos judiciales.

Finalmente, al implementarse recientemente la Superintendencia del Protección de Datos Personales en el Ecuador, se espera que de seguimiento al cumplimiento de sus regulaciones. Actualmente las instituciones públicas tienen plazo hasta el 31 de diciembre de 2024 para nombrar su Delegado de Protección de Datos, por lo tanto, estaremos atentos como desempeñan sus funciones aquellos que sean nombrados en las instituciones llamadas a administrar los sistemas de justicia.

REFERENCIAS

- *Constitución de la República del Ecuador (2008).*
- *Ley Orgánica de Protección de Datos Personales, publicada en el Registro Oficial Suplemento No. 459 de 26 de mayo de 2021.*
- *Reglamento General a la Ley Orgánica de Protección de Datos publicado en el Registro Oficial, Tercer Suplemento No. 435 de 13 de noviembre de 2023.*
- *Resolución 043-2024 del Pleno del Consejo de la Judicatura en la que se expidió el Reglamento para el tratamiento de datos personales dentro de procesos judiciales, publicado en el Registro Oficial Suplemento No. 517 de 13 de marzo de 2024.*
- *Resolución 009-CCE-PLE-2021 del Pleno de la Corte Constitucional del Ecuador, en el que se expide el Protocolo de la Información Confidencial de la Corte Constitucional, publicado en el Registro Oficial Suplemento No. 246 de 3 de diciembre de 2021.*

JOSÉ LEONETT

APLICANDO EL PRINCIPIO DE INTERCAMBIO EN EL USO ADECUADO DE GUANTES EN INFORMÁTICA FORENSE

En el mundo del cómputo forense se presenta un desafío constante: la necesidad de mantener a toda costa la integridad de la evidencia digital. En este contexto es esencial recordar que nuestros principios y acciones no deben regirse por preferencias personales ni influencias culturales. Más bien debemos abrazar un enfoque objetivo y fundamentado en estándares y procedimientos científicos reconocidos, como en nuestro caso la normativa RFC 327 y la misma ISO 2703 7:2012. Exploremos cómo este principio ético y técnico (de intercambio) es fundamental en nuestro trabajo, enfocado en el análisis de datos digitales y la recopilación de evidencia.

Los guantes son un componente esencial de nuestro Equipo de Protección Personal (EPI) cuando nos enfrentamos a riesgos de exposición a sustancias biológicas o químicas. Hay varios tipos de guantes utilizados en estas situaciones.

- **Guantes de Látex:** Reconocidos por su flexibilidad y comodidad, son adecuados para protegernos contra riesgos biológicos como bacterias y virus, aunque no resisten bien a productos químicos fuertes.

- **Guantes de Nitrilo:** Son excepcionales cuando trabajamos con productos químicos, ya que son altamente resistentes a una amplia gama de sustancias químicas, incluyendo solventes y ácidos. También nos protegen contra riesgos biológicos y son ideales para quienes tienen alergias al látex.

- **Guantes de vinilo:** Económicos, pero no ofrecen la misma resistencia química que los de nitrilo. Son adecuados para riesgos biológicos más leves, pero no son la mejor elección con sustancias químicas fuertes.

Un aspecto que a menudo se pasa por alto es el nivel de pH. Los guantes de nitrilo resisten una amplia variedad de pH, desde ácidos hasta bases, generalmente en un rango de pH de 2 a 14. Esto los hace adecuados para trabajar con sustancias químicas que varían en acidez o alcalinidad.

El sudor con su contenido de agua y pH ligeramente ácido, puede afectar la integridad de los guantes de protección. Cuando los guantes de látex entran en contacto con el sudor, tienden a degradarse más rápido, lo que podría comprometer la barrera de protección en el manejo de evidencias.

Por otro lado los guantes de nitrilo, gracias a su resistencia química y capacidad para mantener su integridad en un rango de pH más amplio, se mantienen efectivos incluso cuando el sudor está presente. Esto es crucial en nuestras investigaciones, ya que garantiza que no haya compromisos en la protección de evidencias digitales debido al sudor, manteniendo así la integridad y confiabilidad de nuestras pruebas.

Nuestra elección y uso de guantes de nitrilo demuestra nuestro

compromiso con las mejores prácticas para buscar la justicia y la verdad en cada caso que manejamos. Esto se alinea estrechamente con las pautas cruciales establecidas en RFC 3227 (Sección 2.4), diseñadas para garantizar que la evidencia electrónica cumpla con los requisitos legales antes de su presentación ante el tribunal. En cada etapa de nuestro trabajo forense, cumplimos rigurosamente estos principios para evitar cualquier contaminación de la evidencia y garantizar una evaluación segura y confiable de la evidencia que presentamos.

"La informática forense requiere un enfoque reflexivo y concienzudo, sabiendo tanto lo que se debe hacer como lo que no se debe hacer".

JOSE R. LEONETT

- Gerente de CiberSeguridad en INFO Y MAS Guatemala.
- Miembro e instructor en el International Association Of Crime Analysts – IACA.
- Fundador del Grupo de Analistas Criminales de IACA en Guatemala, así como delegado de IACA para Guatemala.
- Corresponsal de la Red Iberoamericana El Derecho Informático EDI y de la Red Latinoamérica de Informática Forense REDLIF - Capitulo Guatemala.
- Founder & ExCeo del Observatorio Guatemalteco de Delitos Informáticos -OGDI.

CONVERSATORIOS DE
LA RED

CHARLANDO CON LOS QUE SABEN

ELDERECHOINFORMATICO.COM

YOUTUBE.COM/USER/ELDERECHOINFORMATICO

MARIA JOSE MOTTA

CIBEREXPLOTACIÓN SEXUAL INFANTIL: UN DESAFÍO JURÍDICO EN LA ERA DE LA INTELIGENCIA ARTIFICIAL.

Abogada especialista en cibercrimen y evidencia digital. UBA.

Diplomada en litigación penal. UCES.

Diplomada en IA. CEUPE.

Introducción

El desarrollo acelerado de la inteligencia artificial (IA) ha planteado desafíos sin precedentes en la creación de material de abuso sexual infantil (MASI). Esta nueva forma de explotación digital no solo implica la generación de contenido que simula la participación de menores en actos sexuales, sino que también presenta dificultades profundas para el sistema jurídico, que debe adaptarse a realidades tecnológicas jamás imaginadas. Este artículo se propone analizar cómo la IA intensifica la problemática del MASI, evaluar el vacío legal en la legislación argentina y presentar propuestas de reforma que fortalezcan la respuesta del Estado frente a este fenómeno.

Ampliación de la Problemática a través de la IA.

La capacidad de la IA para producir imágenes y videos hiperrealistas ha transformado el panorama del MASI. Los algoritmos, especialmente a través de técnicas como el deep learning y las redes generativas adversarias (GANs), permiten la creación de contenidos sin la necesidad de víctimas reales, lo que complica la identificación legal y el enjuiciamiento de los responsables. Este material, a menudo indistinguible del contenido real, plantea preguntas difíciles sobre la naturaleza del daño y la responsabilidad.

Además, la capacidad de distribución rápida a través de plataformas digitales potencia la proliferación del MASI, convirtiéndolo en un desafío global que trasciende fronteras. Esta facilidad de difusión también se traduce en un riesgo de normalización de la explotación sexual infantil, donde la exposición repetida a este tipo de contenido puede desensibilizar a los individuos y erosionar las barreras éticas y legales en torno al abuso infantil.

El Marco Legal Actual y sus Limitaciones.

El artículo 128 del Código Penal Argentino, que sanciona la producción y distribución de material pornográfico infantil, no contempla expresamente la creación de contenido mediante IA. Esto genera una vulnerabilidad en el sistema legal, permitiendo que aquellos que utilizan tecnología avanzada para generar MASI escapen a la sanción penal. En este contexto, es fundamental adoptar una interpretación extensiva de este artículo para incorporar el término "ciberexplotación sexual infantil", que abarque tanto el contenido generado por IA como el material tradicionalmente considerado como MASI. Dicha inclusión debería reflejar una visión moderna del abuso sexual infantil, que reconozca no solo a las víctimas directas, sino también el impacto de la generación de contenido que puede contribuir a la normalización de la explotación.

Propuestas de Reforma para una Respuesta Efectiva.

1. Inclusión Expresa de Contenido Generado por IA en el Código Penal: La legislación debe ser actualizada para especificar que el uso de IA para crear MASI es punible. Esto implica no solo sancionar a quienes producen contenido abusivo, sino también a aquellos que distribuyen o poseen dicho material. La extensión de la responsabilidad penal a incluir imágenes generadas digitalmente es esencial para cerrar las lagunas legales existentes.

2. Responsabilidad Proactiva de las Plataformas Digitales: Las plataformas tecnológicas deben ser obligadas a implementar sistemas robustos de detección y eliminación de contenido

ilegal. Esta responsabilidad incluye formación y recursos para garantizar que puedan identificar y actuar frente a contenido que sexualice a menores. Las legislaciones comparadas muestran que el establecimiento de penalidades para estas plataformas puede ser efectivo para fomentar la diligencia necesaria.

3. Aumento de Penas y Agravantes: Proponer un aumento en las penas por delitos relacionados con MASI generado por IA. Especialmente donde se utilizan imágenes de menores reales manipuladas digitalmente, las sanciones deben ser severas, reflejando la gravedad del daño causado. La consideración de factores agravantes es crucial para disuadir la producción y distribución de este tipo de contenido.

4. Desarrollo de Normas que Reconozcan la Violencia Simbólica: Establecer un marco jurídico que contemple el uso de imágenes manipuladas digitalmente como una forma de violencia simbólica, reconociendo así el daño que puede infligir sobre los menores cuyos rostros son utilizados. Esto contribuiría a una protección más amplia y efectiva de los derechos de los niños en el contexto digital.

Responsabilidad Penal y Civil en el Uso de IA.

La determinación de responsabilidad en el contexto del MASI generado por IA es compleja. La responsabilidad penal por la creación y distribución de este material debe extenderse a todos los actores involucrados, desde los desarrolladores de la tecnología hasta los usuarios finales. Esto incluye no solo a quienes crean el material, sino también a quienes lo comparten o lo poseen sin consideración de su origen. Las reformas legales deben contemplar la dificultad inherente de probar la intención detrás de la creación de contenido, por lo que es esencial que el marco legal prevea explícitamente la responsabilidad compartida.

A nivel civil, es crucial establecer mecanismos de reparación para aquellos cuyas imágenes han sido utilizadas sin autorización. Esto debería incluir la posibilidad de que tutores legales de menores que hayan sido manipulados digitalmente puedan demandar por daños y perjuicios. La violencia simbólica que representa la manipulación de imágenes de niños

debe ser reconocida legalmente, y se deben permitir acciones en contra de quienes utilizan estas imágenes para producir contenido ilegal. responsabilidad civil por los daños generados.

Además de la responsabilidad penal, el uso de IA para crear material abusivo también puede generar responsabilidad civil, especialmente en aquellos casos en que se utilicen imágenes de menores reales que son manipuladas digitalmente. Aunque el contenido final puede no representar a una víctima real, el uso no autorizado de la imagen de un menor, modificado o no, constituye una violación a su derecho a la imagen y a la dignidad, que pueden ser reparados mediante la vía civil. En este sentido, los padres o tutores de los menores afectados podrían entablar demandas por daños y perjuicios en virtud del artículo 1770 del Código Civil y Comercial de la Nación, que establece la responsabilidad civil por el daño causado por la utilización de la imagen o el nombre de una persona sin su consentimiento. Asimismo, la Ley de Protección Integral de los Derechos de los Niños, Niñas y Adolescentes (Ley 26.061) refuerza el principio de que los menores tienen derecho a su integridad física, psíquica y moral, lo que abre la puerta a la reparación civil en casos de manipulación de su imagen. Además de la reparación directa a las víctimas indirectas, es posible que las plataformas tecnológicas, en calidad de intermediarios, sean consideradas responsables civilmente si no cumplen con su deber de eliminar rápidamente el contenido ilegal. Si bien estas plataformas podrían alegar que no son responsables por el contenido generado por terceros, el principio de culpa invigilando; puede extender su responsabilidad a los casos en que no implementen medidas adecuadas para impedir la difusión de contenido ilícito. Esto sería especialmente relevante si las plataformas no cumplen con los estándares mínimos de diligencia debida en la detección y eliminación de contenido abusivo.

La Necesidad de Colaboración Internacional.

Dado que el MASI generado por IA a menudo trasciende fronteras nacionales, es imperativo fomentar la cooperación internacional en la lucha

contra esta problemática. La legislación argentina debe alinearse con convenios internacionales que exigen la protección de los derechos de los niños frente a la explotación y el abuso. Esto incluye la ratificación y aplicación de tratados como el Protocolo Facultativo de la Convención sobre los Derechos del Niño.

Además, es vital establecer redes de cooperación entre jurisdicciones para la detección y enjuiciamiento de delitos relacionados con MASI. Las autoridades deben colaborar con organizaciones internacionales y agencias de aplicación de la ley para compartir inteligencia y recursos, promoviendo una respuesta globalizada y efectiva contra el uso ilícito de la IA en la explotación infantil.

Reflexiones Finales.

La capacidad de la inteligencia artificial para generar contenido altamente realista presenta un desafío significativo para el marco legal argentino. Las reformas sugieren la necesidad de un enfoque integral que no solo aborde la producción y distribución de MASI, sino que también considere el impacto en las víctimas indirectas, la necesidad de una rápida eliminación del contenido ilegal y la protección de la dignidad de los menores.

La creación de un entorno legal que contemple las realidades de la IA es esencial para garantizar que los responsables sean llevados ante la justicia y que se protejan eficientemente los derechos de los niños en un mundo digital cada vez más complejo. Debemos actuar con urgencia para actualizar nuestra legislación y nuestras prácticas, asegurando que la inteligencia artificial no se convierta en una herramienta para la perpetuación del abuso infantil, sino más bien en un aliado en la lucha por la justicia y la protección de los más vulnerables.

Bibliografía.

1. Anderson, M. (2022). La inteligencia artificial en la jurisprudencia moderna. Oxford University Press.

2. Brown, T. J. y Hall, S. (2021). El impacto de la inteligencia artificial en el sistema penal. Revista de Tecnología y Derecho, 12(1), 45-62.

3. Fernández, P. (2020). La protección de los derechos infantiles en el entorno digital. Revista de Protección de Menores, 27(2), 159-180.

4. Martínez, J. y Ramos, P. (2021). El papel de las tecnologías avanzadas en la explotación infantil. Informe Anual de Derechos Humanos. Naciones Unidas.

5. Protocolo Facultativo de la Convención sobre los Derechos del Niño, ratificado por Argentina.

WILLIAM LIMA ROCHA

DESAFÍOS ÉTICOS Y REGULATORIOS DE LA INTELIGENCIA ARTIFICIAL: REGULACIÓN DE LA IA EN BRASIL.

Abogado y profesor especializado en Protección de Datos, Derecho del Consumo, Derecho Empresarial y Derecho Digital. Asesor de la Presidencia y Delegado de Protección de Datos (DPO) de la Junta Comercial del Estado de Río de Janeiro (JUCERJA), Socio de Terra Rocha Advogados. Estudiante de Doctorado en Ciencias Jurídicas de la Universidad Católica Argentina (UCA), estudiante de Maestría en Ciencias de la Información del Instituto Brasileño de Información en Ciencia y Tecnología (IBICT) y de la Universidad Federal de Río de Janeiro (UFRJ), Maestría en Derecho Empresarial Económico en la UCA, MBA en Derecho del Consumo y Competencia por la Fundação Getúlio Vargas (FGV/RJ)

Introducción

La Inteligencia Artificial (IA) es un campo de la ciencia de la computación que se dedica a la creación de sistemas y máquinas capaces de realizar tareas que normalmente exigirían inteligencia humana. En español, se traduce como Inteligencia Artificial, manteniendo la misma sigla IA.

¿Qué es Inteligencia Artificial?

La IA busca simular capacidades cognitivas humanas en máquinas, como:

- **Aprendizaje (Aprendizaje):** La capacidad de adquirir conocimiento a partir de datos y experiencias, mejorando el desempeño a lo largo del tiempo. El *machine learning* (aprendizaje automático) y el *deep learning* (aprendizaje profundo) son subcampos importantes de la IA que se concentran en este aspecto.
- **Razonamiento (raciocinio):** La habilidad de procesar información, resolver problemas, tomar decisiones y sacar conclusiones lógicas.
- **Percepción (Percepción):** La capacidad de interpretar información sensorial del ambiente, como visión (visión computacional), audición (procesamiento de audio) y lenguaje (procesamiento de lenguaje natural).
- **Comprensión del lenguaje natural (Comprenso da linguagem natural):** La capacidad de entender y

procesar el lenguaje humano, permitiendo la interacción entre humanos y computadoras por medio de lenguaje hablado o escrito.

Tipos de IA:

En español, así como en portugués, se suele clasificar la IA en:

- **IA débil o estrecha (IA fraca ou estreita):** Enfocada en realizar tareas específicas, como jugar ajedrez, reconocer imágenes o traducir idiomas. La mayoría de las aplicaciones de IA actuales se encuadran en esta categoría.
- **IA fuerte o general (IA forte ou geral):** Un tipo hipotético de IA con capacidades cognitivas humanas a nivel general, capaz de realizar cualquier tarea intelectual que un ser humano puede hacer.
- **Aprendizaje automático o *Machine Learning* (Aprendizaje de máquina):** Un subcampo de la IA que se concentra en el desarrollo de algoritmos que permiten a las computadoras aprender con datos, sin ser explícitamente programadas para cada tarea.
- **Aprendizaje profundo o *Deep Learning* (Aprendizaje profundo):** Una técnica de aprendizaje automático que usa redes neuronales artificiales con múltiples capas para extraer características complejas de grandes conjuntos de datos.

1. Desafíos Éticos y Regulatorios de la Inteligencia Artificial

Los desafíos éticos y regulatorios de la Inteligencia Artificial (IA) son un tema de gran importancia a nivel global, y Brasil no es la excepción. A medida que la IA se integra cada vez más en diversos aspectos de la sociedad, desde la economía hasta la salud y la seguridad pública, surgen preguntas sobre cómo garantizar su uso ético y responsable, así como la necesidad de establecer marcos regulatorios adecuados.

1.1 Desafíos Éticos:

- Privacidad y protección de datos: Los sistemas de IA a menudo requieren grandes cantidades de datos personales para funcionar, lo que plantea preocupaciones sobre la privacidad y el uso indebido de esta información. Es crucial garantizar que se cumplan las

normativas de protección de datos, como la Ley General de Protección de Datos (LGPD) de Brasil.

- Discriminación algorítmica: Los algoritmos de IA pueden perpetuar y amplificar los sesgos existentes en los datos, lo que lleva a decisiones discriminatorias en áreas como la contratación, la concesión de préstamos o la justicia penal. Es fundamental desarrollar sistemas de IA justos y equitativos.
- Transparencia y explicabilidad: En muchos casos, el funcionamiento interno de los algoritmos de IA es opaco, lo que dificulta la comprensión de cómo se toman las decisiones. Esto plantea desafíos en términos de responsabilidad y rendición de cuentas. Se busca una mayor transparencia y explicabilidad en los sistemas de IA.
- Impacto en el empleo: La automatización impulsada por la IA puede tener un impacto significativo en el mercado laboral,[1] con la posible pérdida de empleos en ciertos sectores. Es necesario abordar este desafío mediante políticas de reconversión laboral y la creación de nuevas oportunidades de empleo.
- Uso ético en aplicaciones sensibles: El uso de la IA en áreas como la vigilancia, el armamento autónomo o la medicina plantea dilemas éticos complejos que requieren una cuidadosa consideración.

1.2 Autores y Figuras Importantes en la IA (con énfasis en su relevancia para el contexto hispanohablante cuando aplicable):

Es importante notar que la IA es un campo global, y muchos de los autores y figuras más influyentes son reconocidos internacionalmente. Sin embargo, algunos nombres y conceptos tienen particular relevancia en el contexto hispanohablante:

- **Alan Turing:** Matemático británico considerado el padre de la computación y de la IA. Su test de Turing, propuesto en 1950, aún es una referencia para evaluar la capacidad de una máquina de exhibir

comportamiento inteligente equivalente al de un humano.

- **John McCarthy:** Científico de la computación americano que acuñó el término "Inteligencia Artificial" en 1956 y organizó la Conferencia de Dartmouth, considerada el marco inicial de la IA como campo de estudio.
- **Marvin Minsky:** Científico de la computación americano, cofundador del Laboratorio de IA del MIT. Sus investigaciones se concentraron en representación del conocimiento, robótica y aprendizaje automático.
- **Nils Nilsson:** Científico de la computación americano, conocido por su trabajo en búsqueda heurística, planificación automática y robótica.
- **Arthur Samuel:** Pionero en aprendizaje automático, desarrolló un programa de juego de damas que aprendía con la experiencia.
- **Yann LeCun, Yoshua Bengio y Geoffrey Hinton:** Considerados los "padrinos" del aprendizaje profundo (*deep learning*). Sus investigaciones revolucionaron el campo e impulsaron el desarrollo de aplicaciones como reconocimiento de imagen y procesamiento de lenguaje natural.
- **Ramón López de Mántaras:** Científico de la computación español, reconocido por sus contribuciones en inteligencia artificial, especialmente en razonamiento basado en casos y aprendizaje automático. Él es una figura importante en el desarrollo de la IA en España y en el mundo hispanohablante.

Además de estos nombres, muchos otros investigadores, ingenieros y pensadores contribuyeron y continúan contribuyendo al avance de la IA. Es un campo dinámico con constante evolución.

1.3 Aplicaciones de la IA:

Las aplicaciones de la IA son vastas y abarcan diversas áreas, como:

- **Asistentes virtuales (Asistentes virtuales):** Siri, Alexa, Google Asistente.
- **Reconocimiento facial (Reconhecimento facial):** Utilizado en seguridad e identificación.

- **Diagnóstico médico (Diagnóstico médico):** Auxilia en la detección de enfermedades.
- **Coches autónomos (Carros autónomos):** Vehículos que conducen sin intervención humana.
- **Traducción automática (Tradujo automática):** Google Traductor, DeepL.
- **Sistemas de recomendación (Sistemas de recomendación):** Utilizados por plataformas de *streaming* y comercio electrónico.

En resumen, la IA es un campo en expansión con gran potencial para transformar diversos aspectos de nuestras vidas. Comprender sus conceptos básicos y las figuras que moldearon su desarrollo es fundamental para acompañar los avances tecnológicos y participar del debate sobre sus implicaciones éticas y sociales.

2. Regulación de la IA en Brasil

Brasil está avanzando en la regulación de la IA, con el objetivo de establecer principios, normas y directrices para su desarrollo e impacto en la sociedad. Algunos puntos clave son:

- Estrategia Nacional de Inteligencia Artificial: Esta estrategia, creada en 2021, busca orientar el uso ético y seguro de la IA en el país, fomentando la investigación, el desarrollo y la innovación en este campo.
- Marco legal existente: Si bien Brasil aún no cuenta con una ley específica que regule la IA, existen leyes que abordan aspectos relacionados, como la LGPD, que protege los datos personales, y el Código de Defensa del Consumidor, que regula las relaciones de consumo.
- Proyectos de ley en curso: Se están discutiendo proyectos de ley que buscan establecer un marco regulatorio más completo para la IA, abordando temas como la responsabilidad civil por daños causados por sistemas de IA, la transparencia algorítmica y el uso de la IA en el sector público.
- Desafíos regulatorios: Uno de los principales desafíos es encontrar un equilibrio entre la promoción de la innovación y la

protección de los derechos de los ciudadanos. Es necesario crear un marco regulatorio que fomente el desarrollo de la IA sin sofocar la innovación, al mismo tiempo que se garantizan los derechos fundamentales y se previenen los riesgos éticos.

La regulación de la IA en Brasil se encuentra en una etapa de desarrollo. Si bien existen avances importantes, como la Estrategia Nacional de Inteligencia Artificial y la LGPD, aún es necesario un marco legal más específico que aborde los desafíos éticos y regulatorios planteados por esta tecnología. Es fundamental que este marco se construya con la participación de diversos actores, incluyendo el gobierno, la academia, la sociedad civil y el sector privado, para garantizar un desarrollo de la IA que sea ético, responsable y beneficioso para la sociedad en su conjunto.

La regulación de la Inteligencia Artificial (IA) en Brasil es un tema en desarrollo, con discusiones y proyectos de ley en curso. El principal objetivo es crear un marco legal que oriente el desarrollo y el uso de la IA en el país, buscando equilibrar innovación con ética y seguridad.

2.1 Situación actual:

- **Proyecto de Ley nº 2.338/2023:** Este es el principal proyecto en discusión, buscando crear el Marco Legal de la Inteligencia Artificial en Brasil. Fue aprobado por el Senado Federal en 2024 y ahora sigue para revisión en la Cámara de Diputados en 2025.
- **Base en la regulación por riesgo:** El proyecto se basa en la clasificación de los sistemas de IA por niveles de riesgo, con diferentes niveles de exigencia y control para cada categoría.
- **Énfasis en transparencia y derechos humanos:** La propuesta busca garantizar la transparencia en el uso de la IA y la protección de los derechos humanos, especialmente de grupos vulnerables, al mismo tiempo que promueve la innovación y el desarrollo tecnológico.

2.2 Desafíos y perspectivas:

- **Equilibrio entre innovación y regulación:** Uno de los principales desafíos es crear una regulación que no impida el

avance de la IA en Brasil, pero que también asegure el uso ético y responsable de la tecnología.

- **Seguimiento de la evolución tecnológica:** La rápida evolución de la IA exige una regulación flexible y adaptable, capaz de acompañar los cambios y nuevas aplicaciones de la tecnología.
- **Debate con la sociedad:** Es fundamental que la construcción del marco legal se realice con amplia participación de la sociedad, incluyendo especialistas, empresas, academia y representantes de la sociedad civil.

2.3 Importancia de la regulación:

- **Seguridad jurídica:** La regulación de la IA traerá más seguridad jurídica para empresas y usuarios, estableciendo reglas claras para el desarrollo y el uso de la tecnología.
- **Desarrollo ético:** La regulación busca garantizar que la IA sea utilizada de forma ética, respetando los derechos humanos y evitando discriminación y otros problemas sociales.
- **Competitividad internacional:** Un marco legal bien estructurado puede impulsar el desarrollo de la IA en Brasil, haciendo al país más competitivo en el escenario internacional.

La regulación de la IA en Brasil está en curso, con el objetivo de crear un ambiente seguro y ético para el desarrollo y el uso de la tecnología. El Proyecto de Ley nº 2.338/2023 es un paso importante en este sentido, y el debate sobre el tema debe continuar en los próximos años.

El texto del PL impone en el art. 62 Los desarrolladores de IA que utilizan contenidos protegidos en el desarrollo de sus sistemas tienen el deber de informar qué contenidos se utilizaron. Esto debe hacerse mediante la publicación de un resumen en un sitio web de fácil acceso.

El arte. 63 permite el uso automatizado de contenido protegido en procesos de extracción de textos y datos con fines de investigación y desarrollo de sistemas de IA por parte de organizaciones, instituciones científicas y de investigación, museos, archivos

públicos, bibliotecas e instituciones educativas.

Es importante acompañar los desarrollos de la tramitación del proyecto de ley y las discusiones sobre el tema para entender mejor el futuro de la regulación de la IA en Brasil.

El avance del proyecto de ley sobre Inteligencia Artificial en Brasil se encuentra en una fase importante de tramitación, con avances significativos, pero aún sin conclusión. Para entender el estado actual, es crucial enfocarse en el **Proyecto de Ley nº 2.338/2023**, que busca establecer el marco legal para el uso de la IA en el país.

2.4 Situación actual del PL 2.338/2023:

- **Aprobado en el Senado:** El proyecto fue aprobado por el Senado Federal en votación simbólica. Esto representa un paso importante, ya que demuestra el consenso inicial sobre la necesidad de regulación de la IA.
- **En tramitación en la Cámara de Diputados:** Actualmente, el PL 2.338/2023 está en análisis en la Cámara de Diputados. Allí, pasará por diferentes comisiones temáticas, donde será debatido, podrá recibir enmiendas (modificaciones) y, posteriormente, será votado por el plenario de la Cámara.
- **Análisis de la ANPD:** La Autoridad Nacional de Protección de Datos (ANPD) publicó un análisis preliminar del proyecto, ofreciendo contribuciones importantes, principalmente en lo que respecta a la protección de datos personales en el contexto de la IA. Esto demuestra la preocupación por alinear la regulación de la IA con la Ley General de Protección de Datos Personales (LGPD).

Puntos importantes sobre el proyecto:

- **Regulación basada en riesgo:** El proyecto propone un enfoque de regulación basada en riesgo, es decir, los sistemas de IA serán clasificados de acuerdo con el nivel de riesgo que representan para los derechos de los ciudadanos. Los sistemas de alto riesgo estarán sujetos a exigencias más rigurosas.
- **Principios y directrices:** El PL establece principios como transparencia, explicabilidad, responsabilidad, seguridad, no

discriminación y privacidad como rectores para el desarrollo y uso de la IA.

- **Derechos de los usuarios:** El proyecto busca garantizar derechos a los usuarios en relación con decisiones automatizadas por IA, como el derecho a la información, a la contestación y a la revisión humana.
- **Creación de una autoridad reguladora:** La propuesta prevé la creación de un órgano o entidad responsable de regular y fiscalizar el sector de IA en Brasil.

Próximos pasos:

El PL 2.338/2023 aún necesita pasar por las etapas de tramitación en la Cámara de Diputados, incluyendo:

- **Análisis en comisiones:** Discusión y votación en diferentes comisiones temáticas.
- **Votación en el plenario de la Cámara:** Votación final por los diputados.
- **Posible sanción presidencial:** En caso de ser aprobado en la Cámara, el proyecto sigue para sanción (aprobación) del Presidente de la República, quien puede sancionar (aprobar), vetar (rechazar) total o parcialmente el proyecto.

El proyecto está en curso, con un importante avance en el Senado y ahora en fase crucial en la Cámara de Diputados. La expectativa es que Brasil avance en la construcción de un marco legal para la IA, buscando equilibrar la innovación con la protección de derechos y la mitigación de riesgos.

Las tendencias en la regulación de la Inteligencia Artificial (IA) son un tema crucial en el panorama tecnológico actual. La IA se está volviendo cada vez más presente en diversas áreas de nuestras vidas, desde asistentes virtuales hasta diagnósticos médicos y coches autónomos. Con esta creciente adopción, surge la necesidad de establecer directrices y regulaciones para garantizar el uso ético, seguro y responsable de la tecnología.

Es importante acompañar las discusiones y los desarrollos en el área de regulación de la IA, pues este campo está en constante evolución. La regulación de la IA es fundamental para garantizar que la tecnología se utilice de forma beneficiosa para la sociedad, al mismo tiempo que se mitigan los riesgos y desafíos.

En resumen, las principales tendencias en la regulación de la IA son:

- Enfoque basado en riesgo
- Transparencia y explicabilidad
- Protección de datos y privacidad
- Responsabilidad y rendición de cuentas
- Colaboración internacional
- Foco en derechos humanos y ética
- Regulación sectorial
- Bancos de pruebas regulatorios

Conclusión

La regulación de la Inteligencia Artificial en Brasil se encuentra en un momento crucial. El Proyecto de Ley nº 2.338/2023 representa un avance significativo, buscando equilibrar el fomento a la innovación con la protección de los derechos de los ciudadanos y la mitigación de riesgos. Aprobado en el Senado y ahora en tramitación en la Cámara de Diputados, el proyecto aún necesita pasar por diversas etapas antes de convertirse en ley. El debate público, la participación de expertos y el seguimiento atento de la sociedad son fundamentales para garantizar que el marco legal de la IA en Brasil sea robusto, eficaz y alineado con los valores democráticos.

Al acompañar estas tendencias, podemos garantizar que la IA sea desarrollada y utilizada de forma ética, segura y responsable, trayendo beneficios para la sociedad como un todo.

1. Obras Clásicas y Fundamentales:

- **Russell, S. J., & Norvig, P. (2021). *Inteligencia artificial*. (4a ed.). Pearson Education Limited.** Esta es considerada la "biblia" de la IA, abarcando desde los conceptos básicos hasta los temas más avanzados. Es una lectura esencial para cualquier persona que quiera una comprensión profunda del área.
- **Turing, A. M. (1950). Computing machinery and intelligence. *Mind*, *59*(236), 433-460.** En este artículo seminal, Turing propone el famoso "Test de Turing" como un criterio para determinar si una máquina puede "pensar". Es un hito histórico en la IA.

2. Libros y Artículos con Enfoque en Aspectos Específicos:

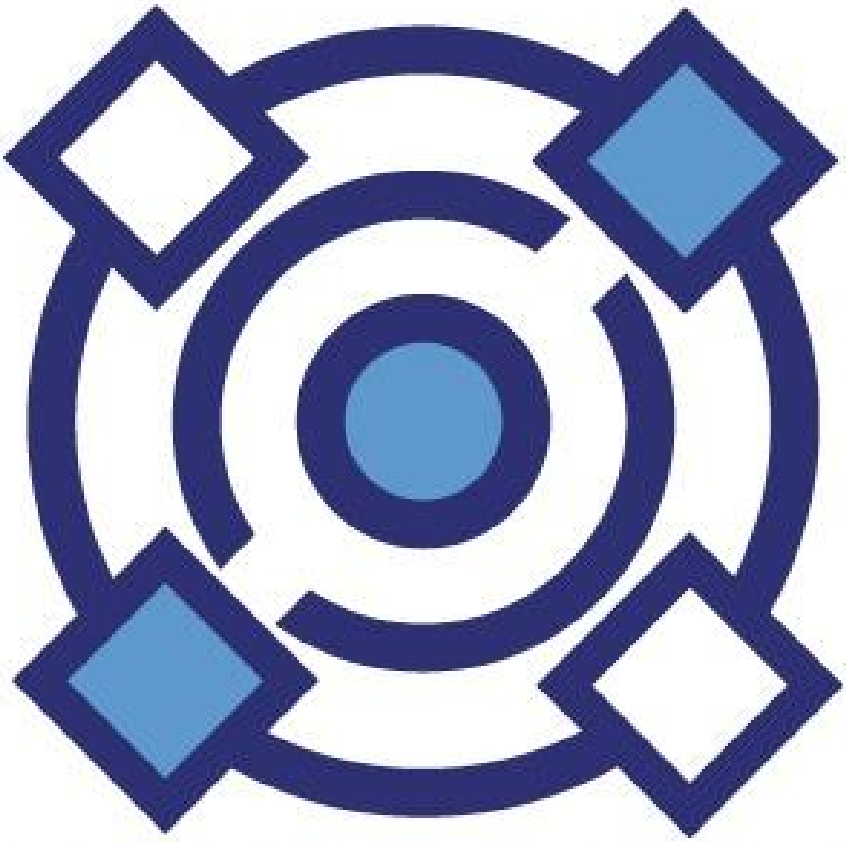
- **Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep***

***learning*. MIT press.** Este libro ofrece una introducción exhaustiva al aprendizaje profundo, una subárea de la IA que ha impulsado muchos avances recientes.

- **Mitchell, T. M. (1997). *Machine learning*. McGraw-Hill.** Una introducción clásica al aprendizaje automático, con enfoque en algoritmos y técnicas fundamentales.
- **Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science*, *349*(6245), 255-260.** Un artículo que ofrece una visión general de las tendencias y perspectivas del aprendizaje automático.

3. Aspectos Éticos y Sociales de la IA:

- **Bostrom, N. (2014). *Superinteligencia: Caminos, peligros, estrategias*. Oxford University Press.** Un análisis profundo de los riesgos e impactos potenciales de la superinteligencia artificial. (Note: A tradução literal seria "Superinteligencia: Caminhos, perigos, estratégias", mas é importante buscar se existe uma tradução oficial em espanhol para manter a uniformidade se houver.)
- **O'Neil, C. (2016). *Armas de destrucción matemática: Cómo el big data aumenta la desigualdad y amenaza la democracia*. Crown.** Un libro que explora cómo los algoritmos y modelos matemáticos pueden perpetuar y amplificar las desigualdades sociales. (Note: Novamente, verificar se existe tradução oficial para "Weapons of math destruction" para garantir a melhor versão em espanhol.)
- **Crawford, K. (2021). *Atlas de la IA: Poder, política y los costos planetarios de la inteligencia artificial*. Yale University Press.** Un análisis crítico del impacto de la IA en la sociedad, el medio ambiente y las relaciones de poder. (Note: Verificar se há uma tradução oficial para "Atlas of AI".)



LAW&DATA
PROTECTION®

KARLA ALAS MANAGING
(PARTNER KAPADUSTUDIO)

EL SALVADOR CIBER DEFENDIENDO LOS DERECHOS DIGITALES Y LA SEGURIDAD INFORMÁTICA.

El pasado mes de noviembre de 2024, fueron aprobadas por la Asamblea Legislativa de El Salvador con 57 votos, dos leyes que estaban haciendo falta y me refiero a la Ley de Ciberseguridad y la ley de Datos Personales marcando un hecho histórico, ya que desde el año 2020 y antes inclusive, la regulación y sobre todo el hecho de estandarización y transformación que ha tenido el país, en lo que es intangibles digitales, modernización del Estado, uso de cripto monedas como moneda de curso legal, el crecimiento exponencial que los mercados digitales y la manufactura de activos digitales, así como la habilitación de nuevos escenarios jurídicos para la legalización de la tecnología, y sus derivados, han hecho que muchas personas vean al Pulgarcito de América, como un espacio propicio para nuevos mercados y donde creemos que puede favorecer a la economía.

La Ley De Datos Personales reconoce por primera vez en la historia de El Salvador, nuevos derechos que solamente se conocían o se escuchaban cómo estaban surgiendo en otros países y que si bien, se han reconocido en jurisprudencia, o también, en algunas leyes secundarias, sin la profundidad o ligeramente, como se definen los criterios de la mayoría de los países, donde si existe una ley de privacidad de datos y protección de la data personal, pero también se les esta dando un valor asociado, al gran derecho universal de la información, al derecho de la integridad que como personas tenemos, el derecho a la imagen y al honor, y cómo estos

derechos interactúan entre sí, de tal suerte que no solo El Salvador, si no el mundo entero ha dado importancia al tema, y reconociendo la prioridad de lo que son los derechos digitales, pero principalmente sobre como los datos personales se recogen, cuál es el tratamiento que debe ejecutarse, cómo debe ser legalmente su almacenamiento, cómo debe ser la conservación de la información, y con muchísima importancia, la extrema necesidad de contar con la autorización, que las personas brinden de sus datos personales y las acciones legales a ser ejercidas contra aquellos que utilicen la información de forma indebida.

Por su parte, la Ley de Ciberseguridad no se queda atrás, ahora contará con el mecanismo legal y la institucionalidad, que definirá líneas de acción, y políticas de protección para estructurar, regular, auditar y fiscalizar las medidas de ciberseguridad en poder de las instituciones estatales que son en primera medida, los organismos obligados a cumplir y velar por lo establecido en la ley.

Y es a partir de esta ley que se han definido los principios con los cuales estructurar, regular y coordinar las acciones de ciberseguridad y así prevenir las actividades relacionadas a la ciberdelincuencia.

De ahí que existe a razón, respecto de cómo estas dos leyes, que regulan dos necesidades urgentes para la seguridad de la información y la ciberseguridad per se, y cómo debía contemplar diferentes aspectos, y regular aquellos vacíos que se habían dejado en otras leyes y que sin una claridad, orientación y normativas que atendieran estos aspectos como prioridad, podríamos con ello, empezar a definir las mejores estrategias y ámbito de protección para caminar en un ambiente ciber seguro, pero también, porque es a partir de esto que podemos empezar a concebir como El Salvador comienza a blindar y definir caminos hacia una ciberdefensa propiamente pura.

Con lo anterior, El Salvador se va a posicionar no solamente como un país cuyo interés es proteger la seguridad de sus ciudadanos en lo que corresponde a datos personales, si no en un campo más amplio, como lo son entornos ciberseguros y donde la exposición de la información sobre todo la que maneja el Estado se

encuentre debidamente protegida y que viene a ser una ayuda en una conjunción de nuevas leyes que han surgido y que no tenían la estructura legal para la protección de la data, tanto la estatal como la de las personas.

Ya en diferentes cuerpos normativos había una pre existencia del reconocimiento y la necesidad de proteger la data, pero también han existido ya criterios y aplicación de norma técnica internacional, así como buenas practicas que se han implementado en las empresas, pero cabe la pregunta, y en materia de datos que es lo que se debe prever y no improvisar?

Si bien las necesidades de proteger son urgentes, debe existir desde ya, los criterios y estándares internacionales para poder manejar los mismos o por lo menos los mas cercanos criterios en el tratamiento que se le dé a la información.

De ahí que por ejemplo necesitamos no solo el reglamento que estará surgiendo para la aplicación de las leyes. Necesitamos por ejemplo muchas manos, ya que la protección de la información tanto de la data personal, como la que se maneja en el Estado o en si en el ámbito privado requieren ser protegidos desde muchas aristas.

Hoy surge con la Ley de Ciberseguridad crear al ente regulador, a ser ejercido por la Agencia de Ciberseguridad del Estado, quien tendrá la obligación garantizar la seguridad informática de los ciudadanos, con diferentes y variadas funciones entre ellas:

- Elaborar la política de ciberseguridad y seguridad de la información de la Nación que contiene los lineamientos y planes de acción.
- Emitir normas protocolos lineamientos estándares y criterios técnicos tanto generales como específicos basados en buenas prácticas y marcos de referencia internacional en materia de ciberseguridad
- Implementar programas de acción para responder ante amenazas o incidentes de seguridad que involucran a los sujetos obligados.
- Requerir a las entidades obligadas donde estas se hayan

visto afectadas en sus sistemas informáticos equipos o infraestructuras por un incidente de ciberseguridad y ejecutará las acciones que sean necesarias para el cumplimiento de sus fines.

Surge a partir de este momento la atribución de crear un registro Nacional de amenazas e incidentes, así como calificar mediante resolución fundamentada a los operadores de infraestructuras críticas y someterlo a ratificación del Presidente de la República.

Pero además la misma ley de datos regulará como mecanismo de protección la necesidad de que las empresas deben contar con Delegado de Protección de Datos, generar políticas, avisos de privacidad y los procesos para notificar las vulnerabilidades a datos de las personas.

De ahí que ha surgido dudas a quienes le va a aplicar la ley. Y aunque la Ley de Ciberseguridad solo limita a que los entes obligados son todos los órganos de gobierno, sus dependencias y las instituciones oficiales autónomos las municipales, pero será obligada cualquier entidad u organismo, independientemente de su forma naturaleza o situación jurídica mediante las cuales se administran recursos públicos, bienes del estado o ejecuten actos de administración pública en general y que posean incidencia en la infraestructura crítica del Estado, incluyendo a todos los servidores públicos dentro o fuera del territorio de la República y las personas que elaboran en entidades ya mencionadas.

Importante esta aclaración porque pareciera que lo privado queda totalmente ajeno a esto, sin embargo, es ilógico pensar de esta forma. Y por ello no podemos decir que esta ley no impacta, pues nadie está exento de un incidente informático hoy día, y menos podemos alegar ignorancia de ley, y lo que sí es factible, es que una brecha de seguridad puede llegar por cualquier frente, ya sea desde una broma, una curiosidad, o con premeditación, alevosía y ventaja.

El camino ya quedo definido en el trazo legal, pero en el recorrido es determinante asfaltar, poner alertas de seguridad, activación de botones de

pánico y actuación. Necesitamos protocolos para como saber actuar y con que debemos actuar en lo mínimo.

Los ciber ataques están a la orden del día, pero no quiere decir que no es algo que no se pueda prever, medir riesgos, actuar y como dice el slogan de aquella famosa marca de whisky, debemos pensar, que, con ciberseguridad y data protegida, sin duda podremos continuar caminando o como es conocido en ambientes ciber seguros, podremos decir "keep walking".

El Salvador se transforma y hacia allá vamos!

LA AUTORA: Abogada de El Salvador • Voluntaria en Legal Hacker El Salvador, • Voluntaria en Womy (Women in Cibersecurity) Colombia • Miembro de ISOC El Salvador • Ex becaria de la Escuela del Sur de Gobernanza en Internet años 2019, 2020, 2021. • Ex Becaria Bootcamp Ciberseguridad impartido por OEA e INCIBE (INSTITUTO DE CIBERSEGURIDAD EN ESPAÑA) y UNIVERSIDAD LEON, ESPAÑA, Julio 2022 • Participo con entidades en El Salvador en el estudio y difusión sobre derecho y nuevas tecnologías. • Autora del libro Glosario de Nuevas Tecnologías vinculadas al derecho. • Blog: Un punto y una Arroba. • Experiencia en derecho tecnológico en sus ramas: Protección de Datos Personales, Delitos Informáticos, E-commerce, Teletrabajo, Habeas Data, Propiedad Intelectual Digital, Piratería Digital y Contratación de creaciones digitales. • Derecho administrativo, penal, mercantil y propiedad intelectual. Aduanera con énfasis en acciones relacionadas con Piratería. • Consultora en materia de e-commerce transfronterizo con USAID • Docente en Iseade-Fepade para Postgrado en Nuevas Tecnologías y Derecho Digital y en la Universidad Don Bosco de El Salvador • Maestría en Seguridad Informática. • Miembro de Aspi Asociación Salvadoreña de la Propiedad Intelectual. • Pionera en el combate de la piratería marcaria tanto física como digital. • Redactora en la mesa redactora de la Ley de Delitos Informáticos . • Nominada como Abogada del Año en la revista Derecho y Negocios en el 2020, 2021 y 2022 como experta en derecho y tecnología.

NOS ACOMPAÑAN SIEMPRE

EMMANUEL CARBALLO

EL SENTIDO DE JUSTICIA EN LA TECNOLOGÍA.

Estudiante de derecho

Project manager

Analista de sistemas

Una pregunta frecuente que suelen hacerme muchas veces cuando comento, luego de, en muchos casos, conocerme y conocer mi larga trayectoria en el mundo de la informática, es acerca de cuál es el sentido de estudiar una carrera como Derecho que, para ellos, es ajena al rubro tecnológico. Veo en sus rostros cual ceja levantada y la otra fruncida la incertidumbre que les provoca encontrarse ante dos caminos que parecen ser muy diferentes, caminos separados uno de otro. Es lógico, lo comprendo en quiénes quizás no están familiarizado con ninguna de ellas, pero me ha sorprendido, en algunos casos, en cuyas personas abordan el mundo de las TIC y que, sin saberlo, han aplicado la ética y los valores morales, pilares fundamentales del derecho, las soluciones que se han requerido en cada caso ya sea con motivos personales o profesionales.

Sin mayor uso del tiempo del lector voy a exponer brevemente en mi caso particular, que años después me llevó a pensar el porqué de elegir ambas carreras en mi vida. Es anecdótico, pero viajo unos años atrás cuando me doy cuenta que la razón por la cual me formé en el rubro de la informática fue un hecho de injusticia vivido. Era un adolescente curioso y con una computadora nueva (básica, muy básica), en la cual, en esos tiempos con contábamos con Internet y para un estudiante de secundaria lo mejor que uno podía tener era el “Encarta” una enciclopedia digital que venía en formato de cd o dvd y eran varios para completar la instalación. Producto de la instalación de ese software fue que se creó un perfil de usuario en la pantalla de Bienvenida, la clásica ventanita con

una foto estándar la cual debía hacerse un click para iniciar el escritorio.

Algo que previo a la instalación no tenía mi pc. Al intentar eliminarlo, solo por el simple hecho de evitar ese click, acudí a borrar el acceso a ese perfil, con lo cual, en la PC familiar, nadie podía ingresar luego. Víctima de mi inocencia decidí salvarme de culpa aludiendo no saber que podía estar sucediendo. Fue entonces que mis padres decidieron llamar al técnico y fue ahí donde se cometió el aberrante acto de formatear la pc acusando a un virus de haber infectado el sistema operativo. Sentido de Injusticia. Era una práctica habitual de los técnicos en esa época. No los culpo, de hecho, creo que la pasaban bien, dado que éste se quedó almorzando con la familia mientras hacía toda la reinstalación del Windows XP que por aquellos años duraban al menos 2 horas. La conclusión es que esto fue lo que me impulsó adentrarme al mundo de la informática y a tomar los primeros cursos de reparación de PC, que en principio fue para evitar recurrir a estos tipos actos, como así también a corregir aquellos problemas que yo mismo pudiera generar, prometiendo a mi mismo evitar estas prácticas fraudulentas.

Es en este punto en el cual vemos a esos dos caminos cruzarse. En el vínculo que necesariamente necesita la tecnología para evitar sucumbir ante manos equivocadas. Es una utopía, claro está dado que la historia está marcada por hechos que dieron lugar a atrocidades cometidas por nuestras propias decisiones en las cuáles prevaleció el hecho de demostrar poder ante otros que priorizar la vida y la dignidad humana. En dónde se discute lo ético con sentido subjetivo y no objetivo, porque era ético hacer lo que se hizo para culminar un conflicto bélico, pero no carecía de ética moral si afectaba los derechos fundamentales del hombre. En el fondo todos sabemos que en caso en dónde faltó ese sentido común que nos caracteriza como seres vivientes pensantes y dominantes del mundo persiste una sensación de injusticia. Entonces, es en esta simple y última palabra, donde entra a debatirse la dignidad del hombre, la Injusticia. Es decir, que a los actos realizados en virtud de los cuales se vieran perjudicadas las vidas humanas de alguna manera, se consideran injustos.

Lo justo entonces es evitar que este tipo de actos sean cometidos nuevamente, y es ahí dónde prima la razón del Derecho, la razón de la Justicia.

Es cuando se establecen reglas y leyes, normas y penas para quienes atenten contra lo establecido. Es ahí donde ambos caminos conectan en un punto para converger en la misma línea recta de avance y de la cual, en principio, no deberían separarse jamás una de otra. De manera metafórica podría pensarse al Derecho, como las señalizaciones del recorrido tecnológico pensándolo como una carretera, mostrando cómo debe ser conducido ese camino. Lo que está bien y lo que está prohibido. Cumpliendo ese rol de agente de tránsito pero que, a su vez, paradójicamente, también debe ir mutando a medida que la tecnología avanza. Es un trayecto de crecimiento mutuo, pero que para el Derecho se torna un poco más complejo, dado que, por lo que marcan los antecedentes, va un paso atrás y buscando adaptarse a los cambios que va experimentando el mundo tecnológico, pero que no puede perderle pisada, dado que es ahí cuando no está presente, que donde se vulneran derechos, leyes y normas.

Es un trabajo arduo y minucioso el cual deben afrontar los juristas más capacitados para hacer valer el sentido de la palabra Justicia ante hechos que parecen atentar contra los derechos de otros. Son esas lagunas del derecho, esos grises donde se discute por ejemplo que en un sitio web se permita que usuarios compartan todo tipo de información o archivos multimedia y alegando que en realidad sólo provee servidores para almacenamiento y que no infringe delito alguno. Entrando en este terreno, se comienzan a plantear muchos interrogantes acerca de las responsabilidades de los actores de los cuáles quisiera plantear algunos como por ejemplo ¿es más responsable un adulto de permitir que su hijo/a menor de edad a que suba todo tipo de contenido a una red social sin controlar lo que sucede o es de la persona que utiliza esa información para hacer un daño? ¿Hay sólo un culpable? Estos cuestionamientos pueden debatirse largamente, pero claro está que hay leyes que protegen nuestra información personal y que poseen las penas necesarias respectivas de cada

caso. La cuestión del asunto es que hoy en día es más evidente, en mundo globalizado y comunicado enteramente gracias al internet y su crecimiento, a la aparición de las redes sociales y los servicios de mensajerías. Y ahora con el boom de la inteligencia artificial insertada en cada aplicación de nuestra vida cotidiana y cuyo uso en muchos casos parece convertirse en algo habitual. Tan habitual que pueda llega a confundir desde la imagen o voz de una persona a otra hasta incluso como el simple hecho de poner en duda si este artículo fue realmente redactado por mis dedos o bien el resultado de un texto originado o mejorado por la IA.

Esto puede resultar extraño pero actualmente es un problema que a mi parecer van a enfrentar a muchos profesionales y que obligará a utilizar herramientas que permitan detectar la utilización de ésta tecnología. No sólo por el simple hecho de ser utilizada para tomar un atajo, sino que influyen en la mismísima capacidad de las personas a utilizar el camino del razonamiento, de su estimulación para explotar todo el potencial humano y creatividad para poder resolver problemas futuros.

Mas allá de esto, no todo es negativo. La IA llegó para quedarse, el mundo debe adaptarse a esta nueva herramienta ha mostrado ser muy útil y optimizar muchas actividades permitiendo un uso mas efectivo de nuestro tiempo. Pero claro está que todo debe tener un límite, debe estar reglado y las empresas, por ejemplo, deben saber proteger su patrimonio, su información y sus recursos teniendo en cuenta que la esta tecnología avanza y sigue sorprendiendo con los avances que se muestran a medida que pasa el tiempo.

Allí dónde emerge el Derecho, es ahí donde vuelven y deberán a aparecer nuevas señalizaciones en la carretera por el cuál transita la tecnología con el fin de abogar cuando esta exceda el limite permitido y no se vuelva un riesgo para la humanidad. Es este el fin de la Justicia aplicado a la informática, el de proteger nuestros derechos regulando los vicios que la misma pueda tener, debatiendo, discutiendo y gestionando los alcances de la misma para poder proyectar nuevas reglamentaciones fundadas en nuestro mayor precepto que es el respeto ante la dignidad humana.

JORGE AMADO YUNES

EL STRESS DEL MUNDO LEGAL EN DICIEMBRE.

Abogado – Mediador
Escritor de la Editorial en LinkedIn
El Impacto de la Neurociencia en la Gestión de Conflictos.

A pocos días de la feria judicial de enero, el ritmo en el mundo legal se intensifica. Hay vencimientos que atender, acuerdos por cerrar y demandas que presentar. Todo debe hacerse antes del viernes 29 de diciembre, como si luego se acabara el mundo.

Revisando investigaciones sobre el estrés en el ámbito jurídico, me encontré con un trabajo de Debra S. Austin, JD, PhD, cuyas ideas considero no solo brillantes, sino también oportunas para este contexto.

Austin explica cómo el estrés afecta la capacidad de aprender y resolver problemas. Ella recuerda una clase sobre manejo de la ira, donde se mencionó que al enojarnos “perdemos 30 puntos de coeficiente intelectual”. Aunque esta afirmación resultó ser una metáfora, la idea subyacente es clara: las emociones intensas, como el estrés y la ira, afectan nuestro desempeño cognitivo y emocional.

En el ámbito legal, operamos bajo un umbral de excitabilidad elevado, es decir, un estado constante de alerta que puede impactar negativamente en nuestra capacidad de tomar decisiones. El estrés prolongado no solo desgasta emocionalmente, sino que también puede alterar la función neuronal, afectando habilidades clave como la concentración y la memoria.

El peso de las demandas y el descanso

El estrés acumulado no solo afecta nuestra mente, sino también nuestra calidad de vida. Mi padre tenía un ejemplo que ilustra esta carga: imaginemos que viajamos en un ascensor con un portafolio. Podemos cargarlo todo el tiempo o soltarlo en el suelo y viajar más livianos. Este acto de soltar representa el descanso genuino y el poder de la meditación es un recurso que mi padre siempre destacó para aliviar el estrés.

Nunca vamos a poder conformar al otro. Nunca. Si al cóctel de la demanda social sobrecarga le agregamos la carga abrumadora de trabajo, los dilemas familiares y la necesidad de estar "disponibles", será un cóctel super devastador en tiempos cómo estos.

Sin embargo, ¿cuánto descansamos realmente? Andrew Huberman, un referente en neurociencia, enfatiza la importancia de una buena higiene del sueño: establecer horarios regulares, evitar dispositivos antes de dormir y, algo que practico, agradecer al final del día.

Les comparto un ejemplo personal: hace algunas semanas, mientras respondía correos durante un feriado, sentí un bloqueo mental. Decidí descansar y, tras una siesta de dos horas (y un sueño en el que apareció Messi), me desperté y logré tener la hora más productiva de mi semana.

El desafío del equilibrio emocional

En el mundo jurídico, la presión de cumplir con las expectativas de los clientes es constante. Sumemos a esto la sobrecarga de casos y la complejidad emocional que enfrentamos al abordar conflictos sensibles. La multitarea, tan común en nuestro ámbito, no solo reduce la eficiencia, sino que también genera un agotamiento cognitivo que afecta nuestra capacidad de respuesta.

El psicólogo **José Antonio Cousiño**, dice algo interesante "…les pagamos para que nos defiendan. Los abogados son guerreros. La sociedad empuja al mundo jurídico a un umbral de exitación alto. El modo litigante es parte de la estructura de cognitiva del mundo jurídico…"

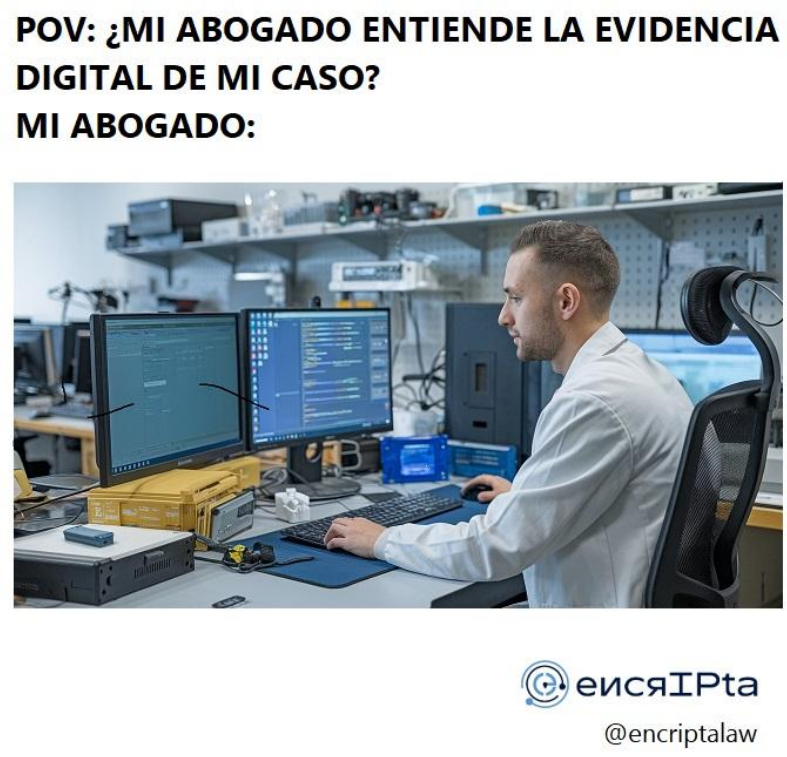
Por eso, cuidar nuestro "termómetro emocional" es fundamental. Como en una guitarra, la tensión adecuada permite sonar afinados, pero el exceso puede romper la cuerda. Encontrar el equilibrio entre un estrés que nos impulsa y uno que nos debilita es clave, especialmente en este frenético mes de diciembre.

El valor del descanso consciente

Una de las lecciones más valiosas que he aprendido es que el descanso no es un lujo, sino una necesidad. Decir "no" cuando es necesario y desconectar genuinamente puede ser la clave para mantener nuestra salud emocional y profesional.

Como mi padre decía: al final, se trata de decidir si queremos cargar con el portafolio todo el tiempo o dejarlo en el suelo del ascensor.

Podes leer mas en mi editorial de los domingos en LinkedIn.




9:15
#ATENTODIGITAL
NO IMPORTA QUIENES DIGAN QUE SON:
• NO HAGAS CLICK EN ENLACES
BANCO ESTAFA
Ahora
¡Buenos Días!
verifique su identidad haciendo click en el siguiente enlace ...
Una iniciativa conjunta de organizaciones que piensan en la gente

BELÉN MORETTI

LOS RIESGOS DE LA INTELIGENCIA ARTIFICIAL: DESAFÍOS LEGALES Y LA NECESIDAD DE UN MARCO REGULATORIO EN ARGENTINA

Abogada, egresada de la Universidad de Buenos Aires, y profesora de ciencias jurídicas. Escritora y diplomada en Ciberseguridad y Tecnologías Aplicadas. Su trabajo se enfoca en el cruce entre el derecho y las nuevas tecnologías, con un especial interés en la protección de derechos de las infancias en los entornos digitales

Los Riesgos de la Inteligencia Artificial: Desafíos Legales y la Necesidad de un Marco Regulatorio en Argentina La inteligencia artificial (IA) ha llegado para quedarse, y su impacto en la vida de los adolescentes es innegable.

Sin embargo, surge una pregunta crucial: ¿estamos realmente preparados para enfrentar los riesgos que esta tecnología plantea a nuestros jóvenes? La respuesta podría definir no solo su futuro, sino también el de nuestra sociedad.

Los adolescentes son nativos digitales, inmersos en un mundo donde la tecnología parece dominar cada aspecto de su vida. Pero esta familiaridad no los protege de los peligros. El ciberacoso se ha convertido en una sombra que acecha a muchos, amplificado por la rapidez con que la información se propaga.

La presión constante por encajar y ser aceptados, exacerbada por la exposición a imágenes ideales y vidas perfectas en redes sociales, puede provocar ansiedad, depresión y una autoimagen distorsionada. La falta de educación en el uso responsable de la tecnología no solo agrava estos problemas; les roba la oportunidad de desarrollarse de manera saludable. Los niños y adolescentes son especialmente vulnerables a la influencia de la IA.

La exposición a contenido violento o manipulativo puede dejar

cicatrices emocionales que perduran toda la vida. Los algoritmos, al personalizar su experiencia digital, pueden crear burbujas de información que limitan su perspectiva y fomentan el aislamiento. Cada día, los niños interactúan con desconocidos en línea sin la protección adecuada.

El grooming y el abuso son realidades aterradoras que no podemos permitir. En este mundo donde los datos son el nuevo oro. Sin una educación clara, pueden convertirse en víctimas de manipulaciones y violaciones de su privacidad. Esta falta de transparencia no solo pone en riesgo sus derechos, sino que también socava su confianza en el mundo digital. La exposición constante a sistemas automatizados afecta profundamente la identidad de nuestros jóvenes.

Las "burbujas de filtro" limitan su acceso a una variedad de ideas, comprometiendo su capacidad de desarrollar un pensamiento crítico. En un mundo que demanda creatividad e innovación. Ante estos desafíos, la pregunta que surge es: ¿qué papel deben desempeñar los abogados y los legisladores en la creación de un marco regulatorio adecuado? Es urgente que Argentina desarrolle políticas claras que no solo protejan a los adolescentes, sino que también responsabilicen a las plataformas que utilizan IA.

Elderechoinformatico

Youtube.com/@elderechoinformatico

JOSÉ LUIS
CHÁVEZ SÁNCHEZ

PROPUESTA PARA LA PROTECCIÓN DE OBRAS ARTÍSTICAS CREADAS CON INTELIGENCIA ARTIFICIAL EN EL DERECHO MEXICANO.

Técnico Académico Asociado.
Unidad Jurídica de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación

INTRODUCCIÓN

"Hasta hace no muchos años, la cuestión de la titularidad de los derechos de autor con relación a las obras creadas por ordenador no planteaba problema alguno, porque el programa informático constituía un instrumento de ayuda al desarrollo creativo del ser humano" (Lacruz Mantecón, 2022), sin embargo, en los últimos años, "la inteligencia artificial (IA) se está implantando cada vez más en campos que antes eran del dominio exclusivo del cerebro humano, como la creatividad y el ingenio" (Paolo Lanteri, 2020), herramientas que por sí mismas, han creado obras que destacan por su calidad, algunos ejemplos son: las pinturas "*El retrato de Edmond Belamy"* y "*The Next Rembrandt"*, composiciones musicales la "obra que completó *la Sinfonía inconclusa de Schubert"* o "*Aiva"*, la novela "*Konpyuta ga shosetsu wo kaku hi"*, el comic "*Zarya of the Dawn*", por mencionar algunas; este tipo de obras están generando dudas y retos para el derecho, por esta razón, "…surge la necesidad de resolver si las obras creadas por IA son objeto de protección, puesto que existen sistemas, máquinas o software capaces de producir obras con poca o ninguna intervención humana." (Niño Hernández et al., 2023), es decir, se plantean preguntas como: ¿Pueden ser considerados como autores los sistemas con IA?, ¿Las obras generadas totalmente con IA pueden ser protegidas por el derecho?

A continuación, para tratar de responder lo señalado con anterioridad,

y acotando el tema respecto a México, es necesario analizar de manera general el marco normativo aplicable a la creación de obras artísticas, con el propósito de establecer los requisitos legales que deben cubrir las obras para ser reconocidas y protegidas por la ley, definir los derechos que se les conceden a los creadores de éstas y señalar, si es posible, bajo la norma vigente, que las obras generadas con herramientas de IA son o no susceptibles de protección legal.

MARCO NORMATIVO MEXICANO

De acuerdo con lo establecido por la Organización Mundial de la Propiedad Intelectual (OMPI), las creaciones del ser humano son protegidas legalmente a través de la propiedad intelectual, la OMPI señala: "…la propiedad intelectual (PI) se relaciona con las creaciones de la mente, como las invenciones, las obras literarias y artísticas, y los símbolos, nombres e imágenes utilizados en el comercio".

En México, el artículo 28, párrafo décimo de la Constitución Política de los Estados Unidos Mexicanos, señala: "*Tampoco constituyen monopolios los privilegios que por determinado tiempo se concedan a los autores y artistas para la producción de sus obras y los que para el uso exclusivo de sus inventos, se otorguen a los inventores y perfeccionadores de alguna mejora*."

De acuerdo con lo señalado en el párrafo anterior, se desprenden las dos materias que protegen las creaciones del ser humano, por una parte las referidas a los inventos, y por la otra parte las obras artísticas. Las primeras, las creaciones, se protegen a través del marco legal correspondiente a la Propiedad Industrial, mientras que las segundas es por medio del Derecho de Autor.

En México, la ley que establece el marco normativo para la protección de las obras artísticas, es la Ley Federal Del Derecho De Autor, (LFDA) de conformidad con lo establecido en sus artículo 1º, el cual señala: "*la presente Ley, reglamentaria del artículo 28 constitucional, tiene por objeto la salvaguarda y promoción del acervo cultural de la Nación; protección de los derechos de los autores, de los artistas intérpretes o ejecutantes, así como de los editores, de los productores y de los organismos de radiodifusión, en*

relación con sus obras literarias o artísticas en todas sus manifestaciones, sus interpretaciones o ejecuciones, sus ediciones, sus fonogramas o videogramas, sus emisiones, así como de los otros derechos de propiedad intelectual"; y en concordancia con lo señalado en el artículo 11 de la misma, indica: "*El derecho de autor es el reconocimiento que hace el Estado en favor de todo creador de obras literarias y artísticas previstas en el artículo 13 de esta Ley, en virtud del cual otorga su protección para que el autor goce de prerrogativas y privilegios exclusivos de carácter personal y patrimonial. Los primeros integran el llamado derecho moral y los segundos, el patrimonial."*

En continuidad a lo indicado en el párrafo precedente, las obras que son reconocidas por la LFDA están comprendidas en las ramas previstas en el artículo 13: Literaria; Musical; Dramática; Danza; Pictórica o de dibujo; Escultórica y de carácter plástico; Caricatura e historieta; Arquitectónica; Cinematográfica; Obras audiovisuales; Programas de radio y televisión; Programas de cómputo; Fotográfica; y, obras de arte y de compilación; por lo que cualquier obra que se ubique en estas ramas, es protegido por la LFDA, asimismo, el párrafo final señala del artículo en mención indica que *"… las demás obras que por analogía puedan considerarse obras literarias o artísticas se incluirán en la rama que les sea más afín a su naturaleza".*

DERECHOS MORALES Y PATRIMONIALES

Una vez definidas las obras que son susceptibles de ser protegidas por el marco normativo mexicano, es importante abordar qué privilegios y prerrogativas adquieren los creadores, retomando lo indicado en el artículo 11, lo cual establece: "*en virtud del cual otorga su protección para que el autor goce de prerrogativas y privilegios exclusivos de carácter personal y patrimonial. Los primeros integran el llamado derecho moral y los segundos, el patrimonial*." De la lectura de este texto normativo, se desprenden dos tipos de derechos:

A) Derechos Morales: Que consisten en el reconocimiento que se les da a los autores creadores sobre las obras artísticas que generan, de tal

forma que se garantiza ese vínculo entre estos y sus obras.

B) Derechos Patrimoniales: Estos se refieren a las prerrogativas que permiten realizar la explotación comercial de una obra, ya sea mediante su publicación, reproducción, transmisión y/o edición, entro otros actos.

Para poder determinar si los sistemas que utilizan IA y las obras que generan son susceptibles de tener las prerrogativas contenidas en los derechos morales y patrimoniales, es importante definir que es la IA y como es que se utiliza para elaborar una obra artística.

Para efectos de definir que es la IA, se utilizará la contenida en el Libro Blanco sobre Inteligencia Artificial, de la Comisión Europea, y en el cual señala: "L*a IA es una combinación de tecnologías que agrupa datos, algoritmos y capacidad informática"*. (Comisión Europea, 2020)

Por "Sistema de IA" se abocará la definición comprendida en el Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial), el cual indica en su artículo 3, inciso 1, lo siguiente: "*sistema de IA: un sistema basado en una máquina diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras el despliegue y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar información de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos o virtuales"*.

Los sistemas tienen diferentes tipo de autonomía, por lo tanto se debe diferenciar de "los productos generados con la asistencia de la IA, en los que una persona interviene o da instrucciones de manera determinante" (Paolo Lanteri, 2020) , por esta razón dependiendo la participación humana existen dos maneras en que interviene la IA: "1). La IA es una herramienta que ayuda en el proceso creativo y 2) la IA crea de manera autónoma e independiente obras algorítmicas " (Niño Hernández et al., 2023) , en el

primer caso, los sistemas de IA son la herramienta más utilizada por los seres humanos para crear obras artísticas, mientras que en el segundo supuesto, el ser humano desarrolla un sistema y suministra los algoritmos programados, suministra datos, y es el sistema de IA que genera las obras de manera automatizada.

Una vez señalados los diferentes usos de los sistemas de IA en las generación de obras artísticas y/o literarias, es necesario acotar los requisitos legales que deben de cumplir los autores para ejercer los derechos morales y patrimoniales que les concede el marco normativo mexicano, y con ello analizaré si con base en dicho análisis, determinar si un sistema de IA puede ser susceptible de ser protegido por dicha norma; los requisitos señalados en la ley son dos: el que sea atribuible a un autor y que sea original.

Por lo concerniente al requisito de que la obra sea atribuible al autor, la LFDA indica es en su artículo 12 a quien se le considera autor, para ello señala lo siguiente: "…*es la persona física que ha creado una obra literaria y artística"*.

De acuerdo con lo anterior, los sistemas de IA que generan obras de manera autónoma no poseen una personalidad jurídica, de tal forma que dichos sistemas no son considerados como sujetos de derechos de autor por el marco normativo mexicano, y considerando que es un requisito legal que la obra sea creada por un ser humano, esto implica que la IA no puede ser reconocida como autor. Es por esto, que "…una abrumadora mayoría defienden apasionadamente la idea de que, para que una obra reciba protección por derecho de autor, es necesaria la participación humana… los argumentos jurídicos son sólidos y se comparten de forma generalizada" (Paolo Lanteri, 2020) . Esta es la razón por la cual la ley no otorga la protección a las obras creadas con sistemas de IA que se actualizan a este supuesto, "…resulta obligatorio que… una obra sea una creación humana, de lo contrario dicha obra no sería admitida o registrada" (Ávila Vallecillo, 2021).

Sin duda, no se debe reconocer a "…la IA como sujeto de derechos, pero pese a ello, es factible atribuirle los derechos o la protección a la persona o conjunto de personas que gestionen los arreglos necesarios para

la creación de las obras algorítmicas, sin ignorar que, materialmente, quien genera tal producto es la IA" (Niño Hernández et al., 2023) , o bien por las personas que hubiesen encomendado la producción del sistema utilizando IA, ya sea con la colaboración remunerada de otras, o bien esta fuera realizada como consecuencia de una relación laboral.

Propuesta de regulación

Una vez determinado que las obras generadas con IA no son sujetas de protección por el derecho de autor en México, considero que la norma debe ser modificada, tal como en su momento histórico la incorporación de la imprenta lo ameritó, estamos en un momento similar, disruptivo y coyuntural, la calidad de las obras inicialmente señaladas, es incuestionable e innegable.

Desde mi punto de vista, el derecho de autor debería protegerlas para garantizar la inversión realizada en los sistemas de IA, y continuar incentivando la innovación tecnológica. La propuesta la realizo, considerando que la norma otorgue una protección en aquellas que sí cumplen con la característica de originalidad, sobre todo por las implicaciones requeridas para su explotación comercial, es decir, las prerrogativas relacionadas con los derechos patrimoniales, para ello es necesario considerar que "…las personas o instituciones jurídicas pueden ser titulares de derechos con relación a una obra, pudiendo gozar solamente de los derechos patrimoniales inherentes, es decir, el derecho de transformación, reproducción, distribución y comunicación pública" (Ávila Vallecillo, 2021) , esto con el propósito de proteger el patrimonio de los empresarios, o de quienes comisionen o encarguen la creación de obras artísticas.

Para sustentar la propuesta de proteger las obras generadas por sistemas de IA que sean obras originales, es importante mencionar que la LFDA señala que "…*las obras protegidas son aquellas de creación original susceptibles de ser divulgadas o reproducidas en cualquier forma o medio"* (Art. 3), de tal forma que el marco normativo mexicano, en cuanto a los derechos de autor, *no protege las ideas por sí mismas* (Art. 14 frac. I), por lo que las obras son protegidas,

"…*desde el momento en que hayan sido fijadas en un soporte material, independientemente del mérito, destino o modo de expresión",* esto implica que "…la originalidad está relacionada con la forma de expresión y no con la idea de base" (OMPI, s/f), y para cumplir con la originalidad, "solo es necesario que la obra sea distinta de las que existían con anterioridad, que no sea una copia o imitación de otra" (Delia Lipszyc, 2017).

Adicionalmente, además de cumplir con el requisito de originalidad, sugiero que de manera obligatoria, cubran con los siguientes puntos:

- Respetar en su caso los derechos morales de las obras consultadas, para ello es fundamental transparentar las fuentes de los datos utilizados.
- Que el sistema de IA por el que se generan las obras, haya sido registrado ante el INDAUTOR.
- Que los sistemas de IA cuenten con información que permita que terceros puedan realizar auditorías en sus algoritmos, para verificar qué y cómo se están analizando los datos para generar las obras, con el propósito de identificar si éstas cuentan con un estilo novedoso y particular, así como constatar que no se está copiando información para generar obras derivadas.

La propiedad intelectual, a través del derecho de autor enfrenta un gran reto, pues conforme continue el avance, desarrollo y perfeccionamiento de la IA, habrá más obras generadas por estas herramientas. Es importante que más allá de plantear respuestas conservadoras que impliquen la negación de proteger este tipo de obras, o de continuar parchando la norma, se transformen y se actualicen los preceptos regulatorios para generar un marco propicio para que la norma evolucione, y no sea un obstáculo en el desarrollo creativo mediante el avance de la innovación tecnológica.

Bibliografía

Ávila Vallecillo, J. A. (2021). Inteligencia artificial: Discusiones e implicaciones actuales en materia de Derechos de Autor. *Revista de la Facultad de Derecho de México*, *71*(281–1), 55. https://doi.org/10.22201/fder.24488933e.2021.281-1.80288

Comisión Europea. (2020). *Libro Blanco Sobre La Inteligencia Artificial*. Recuperado de https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_es.pdf

Delia Lipszyc. (2017). *Derecho de autor y derechos conexos* (Cerlalc, Ed.). Colombia.

Lacruz Mantecón, M. L. . (2022). Inteligencia artificial y derecho de autor. *Revista de Derecho Civil*, *IX*, 381–387. Recuperado de https://nreg.es/ojs/index.php/RDC

Niño Hernández, F. P., Antonio, M., Vargas, B., Duarte, L. R., Patricia, F., & Hernández, N. (2023, octubre). El desafío que representan las obras creadas por inteligencia artificial al derecho de autor en Colombia. *Revista de Internet, Derecho y Política*. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=9087347

OMPI. (s/f). ¿Cómo obtener protección por derecho de autor? Recuperado el 3 de octubre de 2024, de https://www.wipo.int/copyright/es/protection.html#:~:text=La%20protecci%C3%B3n%20por%20derecho%20de%20autor%20se%20obtiene%20sin%20necesidad,ni%20cualquier%20otro%20requisito%20formal.

'aolo Lanteri. (2020). LA PROBLEMÁTICA DE LA INTELIGENCIA ARTIFICIAL Y EL DERECHO DE AUTOR LLAMA A LA PUERTA DE LA OMPI. *Cuadernos Jurídicos*. Recuperado de https://documentos-ia.s3.amazonaws.com/15+ANIVERSARIO/31+La+problema%CC%81tica+de+la+IA+y+el+derecho+de+autor+llama+a+la+puerta+de+la+OMPI+-+LANTERI+2.pdf#:~:text=Paolo%20Lanteri%20|%20La%20problem%C3%A1tica%20de%20la%20IA%20y%20el

ey Federal del Derecho de Autor, última reforma de la Ley publicada en el Diario Oficial de la Federación el 01de julio del año 2020.

MILAGROS CHANTIRI YEDRO

LAUDOS ARBITRALES EN LA BLOCKCHAIN: A PROPÓSITO DE KLEROS

Abogada graduada en la Universidad Nacional del Litoral, estudiante de las Ingenierías en Informática y en Inteligencia Artificial. Secretaria de la Comisión de Derecho Informático del CASF.

Introducción:

El futuro se edifica sobre las bases del pasado y se moldea con el enfoque del presente. Resulta paradójico observar como nuestros antecedentes históricos, que a primera vista parecen lejanos y desconectados de la modernidad, conservan una influencia determinante en los pilares de nuestra sociedad actual.

Ante un horizonte vasto y multifacético, moldeado por el flujo constante de innovaciones tecnológicas, se evidencia que dicho avance no es lineal ni aislado, sino un camino a recorrer que se encuentra iluminado por los aprendizajes del pasado.

Así, remontándonos a los saberes de filósofos antiguos y, parafraseando a Platón, podemos obtener la siguiente noción: *"(…) La ley es la razón de la ciudad, así como la razón es el gobierno del hombre. La causa inmediata de la ley es el juicio del legislador, pero la remota y última es la divinidad. La autoridad, sometida a la ley, educa al ciudadano para que sea virtuoso y obtenga la felicidad, que es también la finalidad última de la ley (…)"*[4].

La concepción de la felicidad como finalidad última de la Ley es un ideal profundamente inspirador, aunque más cercano a un anhelo que a una realidad tangible. En mi experiencia dentro del ámbito jurídico, incluso bajo el marco de un Estado de

[4] Martínez Colín, J. (1996). La Ley según Platón [Tesis doctoral, Universidad de Navarra]. Universidad de Navarra.

Derecho, rara vez he presenciado que la resolución de un caso genere alegría en sentido pleno, ni siquiera en las victorias obtenidas para mis clientes. Por el contrario, los resultados suelen brindar una sensación de alivio o tranquilidad, al poner término a un proceso judicial prolongado, engorroso y cargado de estrés. Este fenómeno refleja la naturaleza pragmática del derecho, que, en lugar de perseguir la felicidad en sí misma, se orienta hacia la restauración del equilibrio y la resolución de conflictos. Y, como suele decir una sabia persona -mi madre-, lo que es conforme a derecho no siempre es justo. En ocasiones, debemos aceptar esa realidad y convivir con ella. Sin embargo, hay momentos en que estos dos conceptos convergen y, es entonces, cuando experimentamos la satisfacción de haber contribuido positivamente al mundo, desde nuestra labor jurídica.

Ahora bien, para que el ideal platónico de una Ley orientada a la búsqueda de la felicidad trascienda la utopía, como lo fue la República de Marco Aurelio antes de la caída del Imperio Romano y con el propósito de armonizar los conceptos de justicia y conformidad con el derecho, propongo explorar juntos un sistema alternativo de resolución de conflictos.

Frente a un nuevo paradigma social:

El ser homo como especie tiene una larga trayectoria que se remonta a 2.5 millones de años atrás. Desde nuestra propia experiencia lo vemos como un largo periodo, que en realidad no tiene comparación, con el resto de los animales que habitan la Tierra. En ese entonces surgió el primer género de homo; el Australopithecus, de éste derivaron otras especies como los neandertales, el homo erectus, el homo soloensis, entre otros. Luego, hace su primera aparición el homo sapiens hace sólo 200.000 años atrás. Tal como lo explica el historiador Yuval Noah Harari en su libro “De Animales a Dioses”[5], el homo sapiens no era una especie dominante, es más, los primeros encuentros entre los sapiens y los neandertales culminaron en una victoria por parte de estos últimos. Entonces, ¿qué fue lo que provocó que saltaran a la cima de la cadena

[5] Harari, Y. N. (2014). Sapiens. De animales a dioses: Breve historia de la humanidad (J. Bernstein, Trad.). Debate. (Trabajo original publicado en 2011).

alimenticia? Definitivamente no fue el lenguaje, ya que la mayoría de las especies tienen uno propio. Fue la capacidad de transmitir información sobre cosas que no existen lo que nos impulsó a la cima del mundo. Las creencias, mitos, religiones fueron las fuerzas que reunieron ejércitos. El creer en valores supremos como la justicia, la igualdad y la libertad, han forjado lo que somos ahora.

La explicación anterior tiene como objetivo mostrarles que tras largos siglos de evolución de la sociedad, hemos podido encontrar una forma de coexistir, utilizando máximas de convivencia que garanticen la supervivencia del ser humano. Guiándonos por el concepto de Derecho de las teorías de Weber, podemos decir que dichas normas tienen un fin específico, el cual es regular las relaciones sociales.

El sistema jurídico ha sido objeto de discusión en varios momentos de la historia como: en la Antigua Grecia, intentando dar respuesta al concepto de justicia; con el surgimiento del Derecho Romano; también fue visto desde un punto de vista teleológico con el derecho canónico y, posteriormente, con subsiguientes hitos en la historia como lo fueron la revolución Francesa y su respectiva Declaración de los Derechos del Hombre y del Ciudadano.

Todos estos momentos culminantes de la humanidad contribuyeron con el concepto del Debido Proceso, como hoy lo conocemos que encuentra recepción en el art. 18 de nuestra Carta Magna. Este principio que sustenta toda la estructura procedimental del sistema jurídico, corre constante peligro debido a las continuas fluctuaciones de valores morales y éticos, a los cambios sociales que inciden y modifican el Derecho.

Actualmente, frente al surgimiento y crecimiento desmedido de las Tecnologías de la Información y la Comunicación, nos encontramos frente a una sociedad que necesita de nuevas formas de acceder a la justicia, no siendo considerada ésta como un sistema, sino como una abstracción de la equidad que impulsa a los individuos a vivir honestamente.

Según Zygmunt Bauman[6], nos encontramos viviendo una sociedad

[6] Bauman, Z. (2005). Vida líquida. Paidós.

líquida, afectada por el consumo, la tecnología y sobre todo la globalización. Si bien, dicho autor, haciendo honor a su profesión se encargaba de estudiar los comportamientos sociales y cómo -a su parecer- las relaciones afectivas comienzan a perder solidez, considero que, el carácter sólido de los vínculos sociales no se ha modificado, sino, que lo que realmente ha cambiado, es la plataforma por la cual se realizan. Este sociólogo ha manifestado en repetidas ocasiones que la preocupación de nuestra vida, tanto social como individual, se centra en cómo prevenir que las cosas queden fijas.

Relacionando esta noción a la búsqueda de un método para solucionar conflictos que trascienden fronteras nos encontramos con sistema de arbitraje reversionado, que requirió de adaptaciones para hacer frente a la necesidad del homo digital.

Conceptualización de arbitraje:

Para obtener una breve noción sobre laudos arbitrales, debemos comenzar con el trabajo de conceptualización de arbitraje, trayendo a colación la definición brindada por el respetado doctrinario, Julio Cesar Rivera que dice: *"(…) es un método adversarial de resolución de conflictos, alternativo a los tribunales estatales, al cual las partes se someten voluntariamente, defiriendo la solución a un tercero que no forma parte de ningún poder u órgano del Estado; cuya decisión es en principio final y obligatoria, lo que no excluye cierto control del Estado por vía de recursos irrenunciables y que para su ejecución (…) requiere la intervención de tribunales estatales. (…) Es un método de resolución de conflictos, pues obviamente las partes persiguen solucionar una controversia, cualquiera sea su naturaleza (…)"*[7].

Sin perjuicio de lo expuesto, resulta de mi preferencia reemplazar la noción de "sumisión voluntaria de las partes" por una "expresión de la voluntad conjunta que decide apartarse de los métodos convencionales de resolución de controversias y cuya manifestación expresa desemboca en el Laudo Arbitral dispuesto por un tercero imparcial".

Ahora bien, siendo el conflicto el inevitable destino en el que pueden desembocar las relaciones sociales

[7] Rivera, J. C. (2007). Arbitraje comercial internacional y doméstico. Abeledo Perrot.

entre diversos individuos, el arbitraje constituye no una noción nueva, más bien es antigua, y lo que ahora conocemos como tal, resulta una reversión de un sistema que existe desde tiempos remotos, pero que ha sido adaptado a las necesidades contemporáneas del homo digital.

No son los homo sapiens, María la panadera y Óliver el consumidor que alega haber sido intoxicado por los budines que le compró a aquella, quienes necesitan de un nuevo sistema que los ayude a dirimir su conflicto de consumo doméstico, porque el ordenamiento nacional les ha brindado las herramientas legales para hacerlo. Ahora, en cambio, son los homo digitales, pertenecientes a la comunidad global sin fronteras, Paula la ingeniera informática de Austria que le ha diseñado a Julio una tienda virtual para vender sus pinturas, quien no se encuentra satisfecho con el trabajo realizado.

Para ello surgen plataformas como la de Kleros que utiliza el blockchain y el crowdsourcing para resolver conflictos de homos digitales que por necesidad han convergido su voluntad, la cual, queda expresada de manera manifiesta en un laudo arbitral dispuesto por un tercero imparcial.

Conociendo a Kleros[8] y su sistema de justicia descentralizada:

Kleros es un sistema de resolución de disputas basado en blockchain que actúa como un arbitraje descentralizado. Está diseñado para resolver conflictos que surgen principalmente en transacciones en línea, contratos inteligentes y acuerdos digitales.

La clave de Kleros está en su capacidad de utilizar:

1.- Blockchain (cadena de bloques)[9]:

Kleros utiliza Ethereum como blockchain subyacente para registrar y garantizar la inmutabilidad de la información. Dicha indemnidad se logra gracias a la tecnología de registro distribuido que almacena datos en

[8] Kleros. (n.d.). Blockchain y el nacimiento de la justicia descentralizada. De https://blog.kleros.io/blockchain-y-el-nacimiento-de-la-justicia-descentralizada/

[9] Lo expuesto en relación a la blockchain resulta a los fines de que se tenga una guía general sobre cómo funciona ésta, pero no constituye una definición exacta, sino una mera aproximación ya que no poseo las autorizaciones de Ethereum, ni la preparación técnica para definir y conceptualizar su trabajo con precisión.

bloques conectados en una secuencia lineal y cronológica.

Cada uno de dichos bloques contiene a) datos, es decir, la información que se quiere registrar; b) el hash del bloque actual (un código unidireccional generado criptográficamente que identifica el bloque); c) el hash del bloque anterior (un enlace al bloque precedente que asegura la continuidad de la cadena) y; d) una marca de tiempo que indica el momento exacto en el que el bloque fue añadido a la cadena.

A lo expuesto le sigue el proceso de creación del bloque, compuesto por acciones como la validación de los datos, la minería, la adición del bloque y la distribución descentralizada.[10]

La inmutabilidad se garantiza gracias al hash, ya que cualquier cambio, por pequeño que sea, generaría un código completamente diferente, alertando a toda la red de que el bloque fue modificado.

Por lo tanto, la confianza que anteriormente era depositada en los intermediarios, ahora fue reemplazada por la blockchain y por su estructura basada en hashes criptográficos, su dependencia en bloques, el consenso distribuido y sus mecanismos de seguridad.

2.- Crowdsourcing:

El empoderamiento ciudadano en la resolución de conflictos constituye un pilar fundamental en los sistemas democráticos modernos. En este contexto, el modelo implementado por Kleros se destaca al permitir la participación de personas comunes como jurados en la resolución de disputas. Dicho modelo se estructura en dos etapas principales: la auto-postulación de los potenciales jurados y su posterior selección mediante un sorteo.

Dicha auto-postulación se lleva a cabo mediante el depósito de un token denominado Pinakion (PNK), el cual debe ser adquirido por el aspirante

[10] Validación de datos: Los nodos de la red (computadoras que participan en el sistema) verifican que los datos de una transacción sean correctos y cumplen las reglas predefinidas.
Minería o concenso: Un mecanismo de consenso, como Prueba de Trabajo (PoW) o Prueba de Participación (PoS), asegura que todos los nodos acuerden qué datos se agregarán al blockchain.
Adición del bloque: Una vez validado, el bloque se añade a la cadena de forma cronológica y queda disponible para todos los nodos de la red.
Distribución descentralizada: La cadena de bloques no está almacenada en un único lugar; cada nodo de la red tiene una copia completa del blockchain. Esto refuerza la seguridad y la integridad del sistema.

de manera onerosa. Este token representa un porcentaje de probabilidad de ser seleccionado como jurado, es decir, a mayor cantidad de PNK depositados, mayor es la probabilidad de ser elegido.

Una vez que los jurados emiten un veredicto definitivo, los PNK depositados son descongelados y redistribuidos en función de la coherencia de las decisiones emitidas por cada participante. De esta manera, el desempeño individual tiene un impacto directo en las ganancias obtenidas, lo que incentiva a los jurados a analizar detenidamente los casos, prepararse y votar con conciencia y responsabilidad.

Este modelo encuentra sus raíces en los antecedentes históricos del jurado, tanto en la antigua Grecia como en el Derecho Romano. Su implementación en Kleros refuerza el carácter democrático del sistema, al garantizar que las decisiones no sean tomadas por una única persona, sino por un colectivo. Esto asegura una mayor imparcialidad y transparencia en los laudos arbitrales, contribuyendo a la publicidad y legitimidad de los mismos.

La relevancia de los jurados trasciende el ámbito de las plataformas digitales. En el marco del Estado de Derecho, la participación ciudadana en la administración de justicia es un principio esencial. Así lo establece la forma republicana y federal de nuestro gobierno consagrado por nuestra Constitución Nacional de 1853, que ha inspirado la adopción del juicio por jurados en diversas provincias de la Argentina. Este mecanismo fortalece la democracia al involucrar a la ciudadanía en procesos decisorios de gran trascendencia, promoviendo una justicia más equitativa, participativa y transparente.

3.- Contratos inteligentes

En el núcleo de Kleros se encuentran los contratos inteligentes, que gestionan las interacciones entre las partes. Éstos consisten en un código programado que se ejecuta automáticamente cuando se cumplen ciertas condiciones previamente definidas.

Dichos contratos fueron diseñados para custodiar los fondos mientras se resuelve la disputa, establecer las reglas del arbitraje -como plazos para la presentación de las

pruebas y la selección de los jurados- e implementar la resolución final, transfiriendo los activos según el laudo emitido.

Es así como estos contratos contienen las reglas del proceso de arbitraje, mantienen los bienes inmateriales en custodia mientras se resuelve la respectiva disputa y ejecutan automáticamente la resolución una vez que los jurados deciden.

Siendo Kleros un sistema voluntario, para ser utilizado, el acuerdo entre las partes debe tener una cláusula que así lo indique.

4.- Tratamiento de la evidencia y la Prueba Electrónica:

El contrato en formato digital y las fuentes de pruebas pertinentes son enviados a Kleros utilizando seguridad criptográfica. De su valoración -al igual que en un proceso ordinario- dependerá la decisión sobre la disputa en cuestión. Por lo que la prueba continúa siendo lo que genera convicción ya no en un juez natural sino en tribunal arbitral.

Ventajas de la utilización de Kleros:

Los aspectos que inciden en la elección de esta plataforma descentralizada de resolución de conflictos pueden ser: a) la independencia de intermediarios; b) el bajo costo en comparación al inicio de un proceso ordinario, la distancia geográfica existente entre las partes que complejiza la elección de un fuero estatal competente; c) la celeridad del proceso; y d) su ejecución automática.

A. La independencia de intermediarios

Resulta menester mencionar que los orígenes de la tecnología blockchain remontan al White Paper de Bitcoin de Satoshi Nakamoto, cuyo fundamento radica en la falta de confianza que han generado los intermediarios de diversas transacciones financieras, en sumatoria, al costo del abono de dichas intermediaciones, lo que en el proceso judicial se puede asemejar a las erogaciones causídicas.

En este aspecto, Satoshi manifestaba *“ (…) lo que se necesita es un sistema de pagos electrónicos basado en pruebas criptográficas en vez de confianza, permitiéndole a dos partes interesadas en realizar*

transacciones directamente sin la necesidad de un tercero confiable (…)".

Por lo tanto, se puede afirmar que uno de los fundamentos del surgimiento de la blockchain es brindar certeza y transparencia en operaciones donde antes reinaba la desconfianza.

Gracias a la utilización de la ya mencionada cadena de bloques, Kleros puede garantizar la misma fiabilidad a sus usuarios, que justamente han recurrido a su sistema por una carencia de confianza entre ellos mismos.

B. La distancia geográfica existente entre las partes

Al encontrarnos sumergidos en una Aldea Global como consecuencia inmediata en del proceso de globalización que viene suscitándose hace décadas, podemos apreciar un cambio significativo en las relaciones contractuales que antes se daban entre partes de una proximidad territorial razonable, ahora en contraposición, se celebran acuerdos comerciales entre individuos de diversas partes del mundo.

A su vez, como efecto inmediato de lo expuesto, la solución a las controversias que surgen de dichos vínculos de carácter contractual se han visto dilatadas por continuas remisiones de los foros de los ordenamientos jurídicos involucrados, debido a la obsolescencia en la que han caído la mayoría de las normas de Derecho Internacional Privado de los Estados.

En este aspecto, el arbitraje internacional y, en particular, sistemas descentralizados como el de Kleros resultan un gran alivio para los ciudadanos, ya que ahora tienen la posibilidad de dirimir sus controversias de una manera más eficaz, con mayor celeridad y a un menor costo.

C. La celeridad del Proceso

La rapidez del proceso de resolución de conflictos de la mencionada plataforma deviene de la eliminación de intermediarios innecesarios, de la falta de burocracia estatal y la automatización de sus operaciones por el uso de tecnología blockchain.

D. Su ejecución Automática

La ejecución automática de los contratos en Kleros tiene como eje la utilización de los ya mencionados contratos inteligentes desplegados en

la blockchain de Ethereum. Estos contratos actúan como programas autoejecutables que gestionan, de manera autónoma, los términos y las condiciones predefinidos por las partes en conflicto.

A continuación veremos un ejemplo concreto para observar cómo funciona su ejecución:

a. Inicio del contrato

Configuración inicial: Antes de cualquier disputa, las partes (por ejemplo, un comprador y un vendedor) acuerdan utilizar Kleros como mecanismo de resolución de conflictos. El contrato inteligente se configura con las condiciones pactadas y, opcionalmente, recibe un depósito de fondos como garantía de cumplimiento.

Depósito en custodia: Si la transacción incluye activos (por ejemplo, divisas o criptomonedas), estos se transfieren al contrato inteligente, que actúa como una cuenta de custodia.

b. Fase de disputa

Presentación del conflicto: Si surge una disputa, cualquiera de las partes puede activar el proceso en Kleros. El contrato inteligente identifica esta acción y establece el inicio de los plazos correspondientes.

Selección de jurados: Utilizando algoritmos criptográficos, el contrato selecciona jurados de entre los participantes que poseen tokens PNK (Pinakion). Esto se realiza de manera descentralizada y verificable, garantizando imparcialidad.

Presentación de pruebas: Las partes cargan sus pruebas en la plataforma y el contrato inteligente coordina el flujo de información hacia los jurados para su evaluación.

c. Emisión del fallo

Votación de los jurados: los jurados emiten su decisión revisando las pruebas presentadas. El contrato inteligente registra los votos y calcula la decisión mayoritaria.

Validación del fallo: el contrato verifica que todos los pasos procesales se hayan cumplido correctamente, lo que asegura la legitimidad del resultado.

d. Ejecución del laudo:

Liberación de fondos o activos: una vez que los jurados han emitido su decisión, el contrato inteligente ejecuta automáticamente el fallo. Verbigracia:

si el jurado decide a favor del comprador, los fondos retenidos en custodia se devuelven a éste, en cambio, si el veredicto favorece al vendedor, los activos se transfieren a este último.

Recompensa a los jurados: los jurados que votaron conforme a la mayoría reciben una recompensa en tokens (PNK), incentivando su participación y comportamiento honestos.

Del proceso detallado anteriormente, se pueden evidenciar cuatro características esenciales: **1) Su inmutabilidad:** los contratos inteligentes están registrados en la blockchain de Ethereum, lo que asegura que no pueden ser alterados una vez desplegados. Esto refuerza la confianza en el sistema y garantiza que las condiciones acordadas inicialmente sean respetadas. **2) Su transparencia:** todas las interacciones, desde la presentación de pruebas hasta la emisión del fallo, son públicas y verificables en la blockchain, lo que elimina cualquier posibilidad de manipulación o favoritismo. **3) La descentralización**: al operar en una red distribuida, la ejecución no depende de una autoridad central, lo cual, reduce la posibilidad de demoras o interferencias externas. Y **4) la programación condicional:** los contratos han sido diseñados bajo principios de programación condicional ("si ocurre X, entonces ejecutar Y"[11]). Esto elimina la necesidad de intervención humana para ejecutar las decisiones.

Dichas características otorgan celeridad al proceso, ya que como hemos visto, las resoluciones se ejecutan inmediatamente luego de la emisión del fallo sin demoras burocráticas. Asimismo, se garantiza la seguridad de los fondos y la ejecución de las decisiones lo que brinda eficiencia.

Desventajas de la utilización de Kleros:

Debido a que este sistema en cuestión es una solución emergente y no se encuentra ampliamente implementada en todos los sectores, podemos encontrar aspectos negativos como: a) jurados inexpertos que no se encuentren aptos para decidir sobre disputas técnicas y complejas; b) la

[11] Lo expuesto, conforma una explicación extremadamente simplificada de lo que es la programación condicional.

dependencia del correcto funcionamiento de Ethereum; c) la ausencia de herramientas legales para equiparar relaciones contractuales de naturaleza desigual, donde una de las partes se encuentra en una situación de evidenciada vulnerabilidad, como es el caso de las relaciones de consumo.

De todo lo expuesto, resulta claro que sistemas como el de Kleros han venido para quedarse, debido a que ocupan el vacío que el Sistema Judicial convencional ha fallado en llenar.

No obstante, el surgimiento de sistemas alternativos de resolución de conflictos puede ser un aspecto positivo para el Sistema Judicial, ya que colabora con su descongestión y brinda la posibilidad de que los recursos finitos del Poder Judicial sean destinados a aquellos casos que por su materia y determinadas características sean de exclusivo tratamiento bajo la órbita de los ordenamientos nacionales y mediante los procesos civiles, penales o laborales correspondientes.

Es así, como dejando de ver a plataformas como la de Kleros como abominaciones que deben ser erradicadas, y más, como instrumentos que de ser perfeccionados pueden contribuir a la búsqueda de una justicia integral, podemos realmente colaborar con la felicidad de los ciudadanos del mundo como fin último de la Ley para que dicha concepción platónica deje de ser una utopía para convertirse en una realidad.

Pero, para ello, debemos pulir las imperfecciones que contienen estos sistemas en surgimiento, impulsando como ciudadanos a nuestros líderes diplomáticos y representantes para constituir bases universales que sirvan como guía y que regulen la existencia de estas plataformas dentro en el ordenamiento jurídico de cada Estado.

Bibliografía:

- Harari, Y. N. (2014). Sapiens. De animales a dioses: Breve historia de la humanidad (J. Bernstein, Trad.). Debate. (Trabajo original publicado en 2011).
- Martínez Colín, J. (1996). La Ley según Platón [Tesis doctoral, Universidad de Navarra]. Universidad de Navarra.

- Bauman, Z. (2005). Vida líquida. Paidós.
- Rivera, J. C. (2007). Arbitraje comercial internacional y doméstico. LexisNexis.
- Kleros. (n.d.). Blockchain y el nacimiento de la justicia descentralizada. De https://blog.kleros.io/blockchain-y-el-nacimiento-de-la-justicia-descentralizada/.
- Bielli, G. E., Branciforte, F., & Ordoñez, C. J. (Directores). (n.d.). Blockchain y derecho. Thomson Reuters La Ley.

ENRIQUE DUTRA

PROTEGIENDO PROCESOS DE NEGOCIO ¿EXISTE EL PLAN B?

Introducción

Niklas Luhmann (1979) nos comenta que la confianza es un mecanismo de reducción de la complejidad, destacando la relación entre la noción de confianza y las nociones de riesgo y expectativa. En el uso de la tecnología, hay ciertos riesgos que son implícitos y otros no son tenidos en cuenta por que hay una idea de que ciertas amenazas no van a impactar a ciertas industrias o procesos. La famosa frase de que a "*nosotros esto no nos va a pasar*", genera que los procesos de negocio que contengan tecnología como soporte no cuenten con las protecciones adecuadas.

Hoy en día la mayoría de las organizaciones no protegen sus procesos de negocio en cuanto a continuidad y calidad de servicio y/o producto. Vamos a observar cierto nivel de cuidado en los procesos de algunas organizaciones que tienen encima la vara de "cumplimiento" (compliance), y ese requerimiento en muchas ocasiones, no protege al ciento por ciento el proceso, si no, es más bien, una medida precautoria ante un incidente y que el que solicita el nivel deseado de cumplimiento le dé la razón o lo apruebe.

Por otro lado, la tecnología está cada vez más inmersa en los procesos de las organizaciones y la filosofía del "**plug and play**" de los '90 cada vez más radicalizado. Post pandemia, tanto los usuarios finales como las organizaciones, han comenzado a usar más la tecnología (nube, IA, automatización de procesos, etc), empujado por cuestiones de contexto, pero en ese proceso de sumar cada vez más recursos tecnológicos, muy pocas

veces se preguntan:"…*y si falla, ¿qué hacemos?*...".

Una confianza explicita en el uso de la tecnología y no evaluar los riesgos provoca lo que viene sucediendo en las organizaciones en los últimos años.

Procesos de negocio

Los procesos de negocio son el conjunto de actividades o tareas estructuradas con el objetivo de producir un servicio o producto específico para un cliente o mercado en particular. Estas actividades pueden ser internas o externas dentro de una organización y son esenciales para la generación de valor y la eficiencia operativa.

Aunque la Real Academia Española (RAE) no proporciona una definición específica para "*procesos de negocio*", podemos definir "proceso" como un conjunto de fases sucesivas de un fenómeno natural o de una operación artificial. Aplicado al contexto de los negocios, se refiere a las series de actividades o tareas que se realizan de manera consecutiva para lograr un objetivo determinado. Un proceso de negocio, por lo tanto, puede definirse como una secuencia de actividades, tareas o acciones organizadas con el propósito de alcanzar un objetivo específico dentro del ámbito comercial o empresarial. Estos procesos son fundamentales para la eficacia y la eficiencia de una organización, y su adecuada gestión es crucial para el éxito y la sostenibilidad en el mercado.

Vamos a tocar sobre todo el punto que mencionamos en el párrafo anterior, donde decimos "*adecuada gestión*", no siempre se cumple y cada vez menos en términos tecnológicos si hablamos de aspectos de Ciberseguridad.

Protegiendo Procesos de Negocio – Plan B

En el contexto de los procesos de negocio, un Plan B o contingencia se refiere a un conjunto de medidas alternativas diseñadas para garantizar la continuidad operativa en caso de que el plan principal falle. Estos planes son esenciales para mitigar riesgos y minimizar el impacto de eventos inesperados que podrían interrumpir las operaciones normales de una organización. Si queremos analizar algunos componentes básicos,

podemos decir que posee los siguientes componentes:

1. Análisis de Riesgos: Es fundamental identificar los posibles riesgos que podrían afectar los procesos de negocio. Esto incluye evaluar tanto las amenazas internas como externas, así como el impacto potencial de cada riesgo.
2. Priorización de Procesos Críticos de Negocio: No todos los procesos de negocio tienen el mismo nivel de importancia. Es vital priorizar aquellos procesos que son críticos para la operación y la supervivencia de la organización. Esto permite enfocar los recursos y esfuerzos en las áreas que más lo necesitan.
3. Identificación de Recursos Alternativos: Un buen Plan B debe identificar recursos alternativos que puedan ser utilizados en caso de una contingencia. Esto incluye personal, tecnología, infraestructura y proveedores que puedan ser movilizados rápidamente.

Un Plan B no es efectivo si no se prueba regularmente. Realizar simulacros y pruebas periódicas ayuda a identificar posibles fallas y áreas de mejora, asegurando que el plan sea viable y eficaz cuando sea necesario.

En resumen, un Plan B o contingencia para procesos de negocio es una herramienta crucial para la gestión de riesgos. Al identificar y prepararse para posibles interrupciones, las organizaciones pueden asegurar la continuidad de sus operaciones y mantener la calidad del servicio o producto ofrecido a sus clientes. Un enfoque proactivo y bien planificado en la contingencia no solo protege los intereses de la organización, sino que también fortalece la confianza de los clientes y otros stakeholders en su capacidad para enfrentar desafíos imprevistos.

Amenazas a los Procesos de Negocio

Para asegurar la continuidad y el éxito de las operaciones comerciales, es fundamental identificar y mitigar las amenazas que pueden afectar los procesos de negocio. Estas amenazas pueden ser diversas y provienen de múltiples fuentes, pero vamos a hacer

foco en dos que son dolores para las organizaciones:

1) Errores Humanos: Los errores humanos son una de las causas más comunes de interrupciones en los procesos de negocio. Estos pueden incluir desde descuidos en la ejecución de tareas hasta malas decisiones estratégicas. La capacitación adecuada y la implementación de protocolos rigurosos pueden ayudar a mitigar estos riesgos. Si hablamos de Ciberseguridad, escuchamos o leemos de manera cada vez más frecuente que una organización fue víctima de un ciberataque y que todo empezó por que alguien abrió un correo electrónico (phishing) y realizó acciones que si lo pensaba fríamente no lo haría. La confianza desmedida de los usuarios, la poca capacitación sobre las amenazas en ciberseguridad, el crecimiento de la IA, provoca que el 90% de las organizaciones afectadas en sus procesos, fuera por un error de una persona que provoca sin querer un incidente.
2) Fallas Técnicas - vulnerabilidades: Las fallas en la tecnología y los sistemas de información pueden causar interrupciones significativas. Esto incluye desde fallas en el hardware hasta problemas de software. Es crucial contar con sistemas de respaldo y planes de recuperación ante desastres para minimizar el impacto de estas fallas. La ausencia de mantenimiento puede provocar el surgimiento de vulnerabilidades que obviamente serán explotadas tarde o temprano por los ciberdelincuentes. Hoy no contar con una robustez en los recursos tecnológicos que participan en los procesos de negocio, pueden provocar un "jaque mate" a la organización.

¿A dónde vamos?

Si nos viene acompañando hasta aquí en la lectura de esta nota, observará que hemos hablado de procesos de negocio, plan de continuidad y amenazas (tratando de

no profundizar en todas ellas que podríamos escribir un libro). Ahora bien, a donde queremos llegar con todo esto: **las organizaciones no están preparadas para responder ante ciertas situaciones**.

Si hablamos de fallas técnicas, que mejor ejemplo de lo que paso con CROWSTRIKE en el 2024, en donde la ausencia de un control de desarrollo y despliegue de la solución FALCON (antimalware) paralizó los procesos de negocios de muchas organizaciones generando pérdidas millonarias. No fue un ciberataque, simplemente alguien no valido o controló una solución que estaba por ser desplegada a millones de ordenadores en el mundo. Como consecuencia, millones de usuarios se enojaron con Microsoft porque sus sistemas operativos no dejaban de mostrar pantallas azules y la corrección era netamente manual. Ahora bien, si yo llevo mi auto a una estación de servicio y el operador del surtidor pone un combustible que no es aceptado por mi vehículo, debo hacerle un juicio ¿al que me vendió el mismo?, ¿al fabricante?, ¿al que me expendió el combustible?, ¿a la petrolera?. Es el debate hoy en día de este caso, y simplemente el responsable es: "*la organización que no cuidó de sus procesos de negocio*". La organización afectada fue la que eligió la tecnología, desplegó la misma, pero no analizó si la misma fallaba como iba a soportar sus operaciones y productos. Entendamos, que esto afectó a aeropuertos, hospitales, bancos, y toda organización pública o privada que tenia un Ms Windows y la solución de Crowdstrike instalada en sus equipos.

El fallo además de tener un impacto por la cantidad de ordenadores afectados, era por el proceso de normalización, no podía desplegarse un proceso automatizado para que lo resolviera, se dependía de personas, recursos humanos que intervinieran y mitigaran el problema.

Que confianza nos puede dar , por ejemplo una aerolínea área, si ante un incidente de este tipo, podemos decir que es controlado por que no fue un ciberataque que genera más incertidumbre, nos pone en una pizarra el estado delos vuelos y nos da el ticket de embarque escritos a mano en un papel símil servilleta descartable.

Si bien el caso mencionado tenemos un claro ejemplo de error

humano, también tenemos casos de vulnerabilidades que son explotadas por ciberdelincuentes y afectan la operación de miles de organizaciones día a día. Hoy el ciberdelito es una actividad muy rentable y el año 2025 vamos a ver una escalada muy importante del mismo, sobre todo por el auge de plataformas de IA que dan cada vez más soporte a actividades maliciosas, como también, las organizaciones que descuidan sus datos y aspectos de ciberseguridad con tal de hacer usufructo en alguna plataforma de IA y tener algún beneficio, sin medir los riesgos de subir datos de la organización (todos quieren hacer algo con IA para mostrar que están en la ola).

¿Hacemos una torta?

En base a todo lo mencionado anteriormente, vamos a aseverar que las organizaciones, en muchos casos, carecen de un plan de contingencia, ya sea por un fallo de software o por un ciberataque.

Ahora la pregunta que le hago al lector, es ¿*un problema tecnológico*? O ¿*un problema de procesos*?, La respuesta es clara: *es netamente un problema de procesos*. Algo que no se incorpora a los procesos de negocio, activos tecnológicos que se suman y no se los protege ante cualquier tipo de fallo. Vamos a ver cierto nivel de madurez, en organizaciones que tiene que cumplir con regulaciones (por ejemplo Bancos, Hospitales, etc) o por cumplimientos exigidos por un asociado sin la cobertura total, más bien algo armado para tener y pasar la exigencia.

En el ámbito tecnológico, un "Playbook" es un conjunto de instrucciones detalladas que guían a los equipos a través de procesos específicos para manejar situaciones comunes o críticas. Estos documentos son esenciales para garantizar la consistencia, la eficiencia y la eficacia en la respuesta a eventos que pueden afectar negativamente a la organización.

Si queremos dar un ejemplo de ello, podemos tomar una caja con el preparado para hacer una torta en nuestro hogar. En la parte trasera de la misma vamos a tener los ingredientes (ahora en más vamos a llamarlos REQUERIMIENTOS) y el paso a paso de cómo hacer la rica torta un fin de semana (lo llamaremos PLAYBOOK).

¿Por qué a los ingredientes le llamamos REQUERIMIENTOS? Porque

sin ellos no podremos hacer la misma y deberemos improvisar. Por ejemplo, si nos cortan el gas para hacer la misma en el horno, podemos usar un horno eléctrico. Pero si no tenemos agua, no la podremos hacer.

Playbooks

En estos dos últimos años hemos trabajado en esta estrategia, y uno de los puntos fuertes de la metodología de trabajo, es analizar los ingredientes, es decir los REQUERIMIENTOS. Al hacerlo, observamos que las necesidades de los procesos de negocio están muy lejos a lo que provee el área de tecnología y en el caso de un incidente, los procesos de negocio se verían fuertemente afectados.

Los playbooks son vitales en tecnologías de la información (TI) porque:

1. Proporcionan respuestas rápidas y estandarizadas ante incidentes.
2. Mejoran la formación y la capacitación del personal.
3. Reducen riesgos y minimizan el impacto de fallos y ciberataques.
4. Fomentan la mejora continua mediante la revisión y actualización de procesos.

Entonces, definimos a los Playbooks como un conjunto de procedimientos detallados y predefinidos que guían a los equipos de respuesta a incidentes en la detección, investigación y mitigación de amenazas.

¿Por qué implementar Playbooks?

- Cualquier organización puede tener sus procesos de negocio afectado en base a lo que comentamos en párrafos anteriores.
- Es necesario contar con un esquema ordenado de procesos de recuperación.
- Permite hacer revisión de muchos puntos de protección de datos.
- Involucrar a distintos actores dentro de la organización. Se debe entender que el proceso de recuperación no depende solo de IT.
- Por cumplimiento de requerimientos normativos.

Requerimientos para armar un Playbook exitoso.

Para llevar a cabo un playbook exitoso, debemos tener todos los ingredientes o al menos definiciones de como trabajar ante ciertas situaciones.

Vamos a mencionar los más importantes.

1) Requerimiento 1: Personas

Su plan de respuesta debe identificar, con anticipación, a todas las personas y equipos que deberán participar en un evento. Los roles recomendados incluyen los siguientes:

- ✓ Líder de equipo
- ✓ Alta gerencia
- ✓ Representante legal
- ✓ Personal de TI
- ✓ Personal de seguridad de TI
- ✓ Experto en la materia de ransomware
- ✓ Mesa de ayuda
- ✓ Personal de Respuesta a incidentes
- ✓ Relaciones públicas (para comunicaciones internas y externas)
- ✓ Consultores externos, según sea necesario.
- ✓ Cumplimiento de la ley, según sea necesario.
- ✓ Persona de contacto del seguro de ciberseguridad, si está involucrada.

En organizaciones más pequeñas, muchas de estas funciones podrían estar representadas por una persona o ser desempeñadas por recursos externos. El objetivo es identificar todos los roles y las personas necesarias, con anticipación, e informarles sobre el plan de respuesta, sus objetivos y cómo deben planificar para reservar tiempo para revisarlo, aprobarlo y practicarlo. Estos roles deben estar asignados formalmente.

2) Requerimiento 2 : Plan de comunicaciones

No sorprende que muchos de los peores resultados se describan como consecuencia de malas comunicaciones. Por lo tanto, planifique con anticipación. El primer objetivo de comunicación que debe decidirse es cómo todos accederán al plan de respuesta de si es necesario.

Suponga que todos los dispositivos del entorno están comprometidos o fuera de servicio. ¿El plan de respuesta está impreso y almacenado físicamente en el hogar de cada participante? Si es así, ¿puede asegurarse de que cada participante obtenga copias actualizadas cada vez que se actualice? ¿Está almacenado en otro sitio de almacenamiento en línea que no está conectado al entorno principal de la organización al que se puede garantizar que todos los participantes puedan acceder si el

dispositivo de la organización que normalmente usan no funciona? ¿Todos tienen claro el rol?

Es importante que la organización tenga un protocolo claro y definido para comunicarse con las partes interesadas en caso de un ataque. Esto incluye los clientes, socios, proveedores y otras partes involucradas en la operación de la organización.

Puntos a tener en cuenta

1) En caso de coordinar sesiones con las partes, que plataforma de comunicación van a usar. (Ms Team, Google Meet, Zoom, WhatsApp, etc).
2) Si la organización suspende el acceso a Internet hasta tanto se resuelva como habilitarlo, como van a usar la plataforma escogida.
3) Dentro del plan se debe contemplar una sesión de kick-off involucrando a las partes indicando aspectos del plan de comunicación, frecuencia, responsable, tipo de comunicación, etc.
4) Con que frecuencia se van a comunicar las partes.
5) Se debe tener en cuenta como involucrar a las partes interesadas de la manera más rápida y eficiente. Debe quedar formalizado el proceso.
6) Se sugiere simulacros para verificar funcionamiento.

3) Requerimiento 3: Plan de relaciones públicas

Un evento que afecte el proceso de negocio tendrá un impacto significativo en las operaciones. Deberá comunicarse con los empleados, clientes, otras partes interesadas, reguladores y, potencialmente, con el "público" a través de contactos directos y canales de medios. Deberá decidir qué comunicar a quién y cuándo. Involucre a un equipo de relaciones públicas (RP) en su plan con anticipación y obtenga su opinión sobre cómo manejar las comunicaciones para cada audiencia. Deben simular algunas plantillas aproximadas para cada tipo de audiencia. El asesor legal, por supuesto, necesita revisar todas las comunicaciones (idealmente de antemano como ejemplos simulados) y

trabajar de la mano con relaciones públicas.

Deben planificar cómo comunicarse si todos los sistemas normales están caídos. Rutinariamente se ve a las víctimas de ciberataque tardar días en reconocer públicamente que ha sucedido algo. Una gran parte de esto es que todos sus sistemas y métodos de comunicación normales están caídos, y no planearon con anticipación que eso sucediera. A menudo, la única pista para el mundo exterior de que algo anda mal es la falta de comunicación de la víctima con nadie. Nadie de la organización víctima responde a los correos electrónicos. A veces, incluso los sistemas telefónicos están caídos.

4) Requerimiento 4: Copia de seguridad confiable

Aunque una copia de seguridad por sí sola generalmente no mitigará todo el daño causado, una copia de seguridad confiable, exhaustiva, probada, fuera de línea y actualizada debe ser un requisito fundamental. Desafortunadamente, muchas más organizaciones creen que tienen buenas copias de seguridad de las que realmente tienen buenas copias de seguridad. Su organización necesita confirmar que tiene una buena copia de seguridad. Tiene que ser integral. En resumen, la organización debe tener políticas claras sobre la frecuencia de las copias de seguridad, la ubicación del almacenamiento de las copias de seguridad, y el proceso de recuperación de datos para garantizar el éxito del playbook.

Puntos a tener en cuenta

1) Backup aislado con una red bastión.
2) Pruebas de restauración para medir los tiempos y verificar que estén acordes a lo que necesita el negocio.
3) Contar con versionados seguros.
4) Contar con un procedimiento de revisión de integridad de los datos restaurados.
5) Tener definido el orden de restauración de la información necesaria para restaurar los procesos de negocio. Este es un punto crítico, ya que es un cuello de botella.

5) Requerimiento 5: Pago de rescate

Una de las decisiones más importantes que cualquier organización puede tomar con anticipación es si pagar o no el rescate. Nadie quiere pagar una demanda de extorsión, aunque muchas organizaciones, con razón, ven más barato y rápido pagar el rescate. Algunas organizaciones se niegan éticamente a pagar un rescate. Otros están reglamentaria o legalmente prohibidos de pagar un rescate. No hay garantía de que el pago de un rescate resulte en la recuperación de datos, y mucho menos en la recuperación total. Muchas veces debe analizarse el contexto y la situación, pero es fundamental entender el pensamiento de la Dirección o Gerencia General. Hemos visto procesos de recuperación demorados por la ausencia de tomas de decisiones que luego se convirtieron en multas.

6) Requerimiento 6: Plan de seguro de ciberseguridad

¿Obtendrá su organización un seguro de ciberseguridad o no? Durante años, el porcentaje de organizaciones que obtuvieron un seguro de ciberseguridad fue en aumento. Hubo grandes beneficios tanto para la compañía víctima como para la industria de seguros por hacerlo. Lamentablemente, el terrible "éxito" del ransomware ha llevado a un aumento drástico en las primas, deducibles más altos, menos cobertura y menos opciones. El seguro de ciberseguridad puede no ser el beneficio financiero que alguna vez fue. Aun así, se recomienda que todas las organizaciones consideren un seguro de ciberseguridad y decidan con anticipación si desean comprarlo.

7) Requerimiento 7: Declarar brecha de seguridad

Este punto contempla lo que se necesita para declarar una violación de datos oficiales. Hay leyes y reglamentos que tienen requisitos obligatorios si ocurre una violación de datos oficiales. La mayoría de las organizaciones no quieren declarar que se ha producido una violación de datos oficiales si no es requerido legalmente. En estos días, el porcentaje abrumador de ransomware extrae datos, y eso claramente aumenta las probabilidades de que ocurra un evento de violación de datos. Como se mencionó anteriormente, no todas las filtraciones de datos cumplen con la definición legal de lo que debe

informarse como una violación de datos oficiales.

Es posible que los datos robados no hayan sido un tipo de datos cubierto y definido que cumpla con una definición de violación de datos (por ejemplo, PII, PHI, etc.) o no estén cubiertos por un contrato que requiera protección. También existe la posibilidad de que lo robado no fuera tan grave. Decida con anticipación qué factores harán que su organización declare oficialmente que ha ocurrido una violación de datos.

Si se detecta/declara una filtración de datos, ¿cuál es el tiempo máximo que puede transcurrir antes de que la organización víctima deba denunciarlo y a quién se debe denunciar? Una vez más, la alta gerencia y el departamento legal deben tomar esta decisión.

8) Requerimiento 8: Personal Internos y Consultores Externos.

¿A quién involucrará en un evento de ciberseguridad? ¿Lo manejará utilizando todo el personal interno o involucrará recursos externos? Si utiliza recursos externos, ¿quiénes serán? Si tiene un seguro de ciberseguridad, ¿está obligado a usar los recursos que dictan o solo se recomiendan los recursos de recuperación? ¿Usará un solo recurso o usará diferentes grupos para diferentes tecnologías y servicios involucrados? La recomendación es asegurarse de que quien sea que involucre tenga experiencia comprobada en responder con éxito a eventos de ciberseguridad. Elija un coordinador de respuesta de ciberseguridad con anticipación y permítale tener las personas necesarias para minimizar el daño, teniendo en cuenta las restricciones presupuestarias, por supuesto. No desea responder al ciberataque por su cuenta o utilizar un grupo externo sin experiencia. Quiere un líder probado que haya estado allí y haya hecho eso. Trate de establecer acuerdos de servicios (SLA) para contar con los recursos externos en tiempo y forma.

9) Requerimiento 9: Actualizaciones plataforma.

Las actualizaciones de software y los parches de seguridad son fundamentales para mantener el sistema seguro y reducir las vulnerabilidades que los atacantes podrían explotar. Además, se debe

contar con el antivirus actualizado (versión y firmas) en todos los servidores y estaciones de trabajo de la infraestructura de la organización.

10) Requerimiento 10: Checklist

Siempre es bueno tener una lista de verificación resumida disponible para usar, que cubra todos los puntos clave que cualquier participante pueda consultar rápidamente. Aquí hay un ejemplo de lista de verificación rápida:

- ✓ Confirme el motivo de la caída de los procesos de negocio.
- ✓ ¿El evento de ciberataque requiere una respuesta completa al incidente y la activación del plan de respuesta? Si es por un fallo de software y los proceso están caídos, continúe:
    - Active el plan de respuesta de adecuado ejecutando Playbook.
    - Notifique a la Gerencia General y a otros participantes.
    - Establezca comunicaciones alternativas según lo planeado (si es necesario)
    - Desconecte los dispositivos potencialmente involucrados de la red, incluidas las conexiones inalámbricas
    - Minimice la propagación y el daño iniciales
    - Inicie un plan de comunicaciones de relaciones públicas
    - Determine la versión/familia del ransomware e investigue el comportamiento esperado (si es posible).
    - Determine el alcance de la explotación del ciberataque y analice los daños
        - Ubicaciones, dispositivos, datos y sistemas involucrados, qué está encriptado, ex filtración de datos y credenciales, etc.
    - Póngase en contacto con la compañía de seguros de seguridad cibernética, si está involucrada.
    - Póngase en contacto con el contacto de recuperación de respuesta.
    - Busque puertas traseras y otros programas maliciosos.
    - Determine el alcance del daño inicial y las consecuencias conocidas.
    - Tenga reuniones de respuesta inicial. Decida si se debe pagar el rescate (debe estar definido previamente); si es así, inicie las

negociaciones. Inicie la recuperación.

- Hacer una copia de seguridad de los archivos cifrados para la recuperación de errores/posible descifrado futuro (opcional).
- Determinar el vector de infección de la causa raíz inicial y mitigar
- Priorizar la recuperación del sistema en función de la evaluación/necesidades del impacto comercial (BIA)
- Decidir si el descifrado es posible y deseado, si es así, comenzar
- Decidir si la restauración de la copia de seguridad es necesario, si es así, comience la recuperación o reconstrucción del sistema
- Si se pagó el rescate y se recibió la clave de descifrado, pruebe en un sistema de prueba aislado
    - Si la prueba tiene éxito y se desea descifrar usando la clave de descifrado de ransomware, pague el rescate, obtenga el resto de las claves y continúe.
- Elimine las puertas traseras y otros programas maliciosos.
- Restaure los sistemas a un estado limpio conocido o de mayor confianza.
- Cambie todas las credenciales de inicio de sesión posiblemente robadas. recuperación/restauración/reconstrucción
- Recuperar completamente el entorno
- Realizar un análisis post-mortem (lo que se hizo bien, lo que se hizo mal, lo que debe cambiarse)
- Intentar prevenir el próximo ataque
- Reunión de lecciones aprendidas

11) Requerimiento 11: Evaluación y mejora continua

La organización debería realizar regularmente una evaluación de la efectividad del playbook y hacer mejoras y ajustes según sea necesario para asegurar que esté actualizado y sea efectivo. Para medir la efectividad del playbook deben realizar simulacros acotados y sobre escenarios productivos.

<u>Puntos a tener en cuenta</u>

1) Tiempos de respuestas.
2) Compromiso con los involucrados.
3) Tiempos de restauración.
4) Comportamiento de las personas.
5) Eficacia en la comunicación.
6) Eficiencia de las herramientas de reunión.
7) Acciones que corregir.

12) Requerimiento 12: Aspectos Legales

La organización debe verificar aspectos de cumplimiento formal y legal, para entender cómo actuar ante clientes, proveedores, asociados y otros en el caso de un incidente de ciberseguridad.

A continuación, se presentan algunos aspectos legales que deberían abordarse en un playbook:

1) Cumplimiento de las leyes de privacidad: Como la organización recopila, procesa o almacena información personal, es importante cumplir con las leyes de privacidad y protección de datos aplicables. En caso de un ataque de ransomware que involucre la información personal de los clientes, la organización debe informar a las autoridades y a los afectados según lo exija la ley. En caso de irrupción y robo de datos de personas (PII), se debe verificar los requerimientos legales como la Ley 25326 (Ley Protección de Datos Personales de la República Argentina) para este caso.
2) Acuerdos de nivel de servicio (SLA): En caso de que el ataque de ransomware interrumpa los servicios que la organización proporciona a sus clientes, es posible que se violen los acuerdos de nivel de servicio (SLA). La organización debería tener en cuenta estas posibles violaciones y estar preparada para abordarlas en caso de que ocurran. Si debe mantener software o proteger procesos de negocios y hay recursos humanos propios o terceros, debe contar con SLA.

3) Responsabilidad contractual: Si la organización tiene contratos con terceros, es posible que estos contratos establezcan ciertas responsabilidades legales en caso de un ataque de ransomware o fallos tecnicos. La organización debería revisar los contratos relevantes y tener en cuenta estas posibles responsabilidades.

4) Posibles demandas: En caso de un ciberataque, la organización puede enfrentar posibles demandas de los clientes, proveedores u otras partes afectadas. La organización debería tener un plan para abordar estas posibles demandas, incluyendo la contratación de asesoría legal. Un punto que permite proteger a la organización es haciendo la denuncia penal correspondiente, para ello se requiere:

    a. Análisis forense de lo sucedido. Realizar un análisis forense con un Perito Informático y generación de documento con respaldo de un Escribano Publico. Respaldar la información, realizar tres copias suscriptas por el escribano.

    b. Presentación en la Justicia: realizar la denuncia correspondiente, adjuntando el informe forense. La idea no es intentar capturar al ciberdelincuente, si no proteger los procesos de negocio ante demandas, indicando que la organización no está siendo operativa por un ciberataque

Cocinemos un PlayBook

Teniendo los ingredientes, ya podemos armar nuestro proceso de trabajo para recuperar nuestros procesos de negocio. En este punto básicamente es reunir los ingredientes y armar un proceso detallado, y definir el trabajo en equipo para recuperar la operación de los procesos de negocio.

Los pasos para el desarrollo del mismo se basan en los siguientes puntos:

1) **Detección y evaluación:** cunado un proceso de negocio es afectado, se debe evaluar el motivo, impacto y recursos necesarios para volver a la operación normal. Uno de los puntos más destacados, es que se necesita algún tipo de monitoreo continuo, para que el usuario interno o externo no sea el que emita la alerta y cuando esto ocurra la respuesta de la organización sea que ya se está trabajado en la normalización.
2) **Evaluación impacto:** en base a esto se analizará las acciones de IT y de toda la organización, en base a lo planificado. No se deben tomar medidas apresuradas y debe trabajarse con el Comité de Crisis (si existiera) o los referentes o los distintos Gerentes de los procesos involucrados. El impacto determinará las acciones a realizar.
3) **Recolección de evidencia:** es importante entender que paso y como. Esto permite restablecer la operación de una manera diferente y comunicar interna y externamente de manera asertiva.
4) **Mitigación:** Implementar las medidas de mitigación adecuadas e ir comunicando el proceso para mantener a los usuarios de servicios y/o productos con el nivel de confianza deseado.
5) **Restauración de la operación:** el proceso de restauración de la operación debe ser ordenado y al finalizar se debe controlar la integridad de los datos y servicios. No lanzar a producción sin una previa verificación para no interrumpir nuevamente el proceso de negocio para una posterior corrección.
6) **Evaluacion post incidente:** es sumamente importante entender que paso y que acciones son las necesarias para que no vuelva ocurrir. Identifique las áreas de mejora y

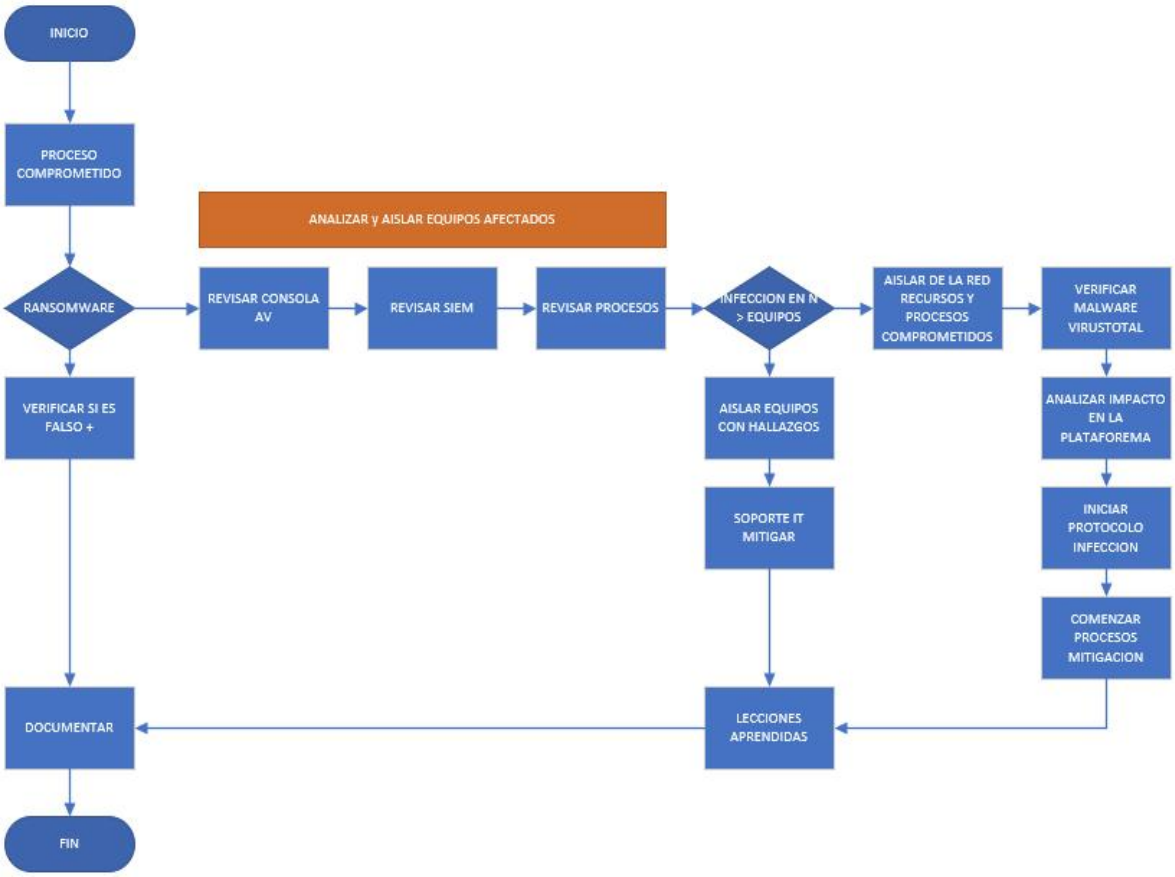
aspectos a tener en cuenta en los procesos de negocio.

Una mejor manera de cocinar es contar con un proceso tipo diagrama de flujo donde podamos explayar luego las acciones de cada ítem, como se muestra en el dibujo a continuación:

¿Cómo sabemos si es exitoso el proceso confecciona:

Una vez que contemos con todos los requerimientos y el esquema definido de Playbook, hay que probarlo, es la única manera de saber si lo que se ha confeccionado es lo que requiere la organización. Para hacerlo, se debe sumar a todas las áreas y gerencias que se requiera para llevar a la practica el Playbook.

Probar un Playbook es crucial para garantizar que todas las estrategias y procedimientos establecidos en el documento funcionen como se espera en situaciones reales. Al realizar pruebas, se pueden identificar posibles fallos o áreas de mejora que no son evidentes en la teoría. Además, permite que todos los involucrados en el proceso se familiaricen con sus roles y responsabilidades, lo que facilita una respuesta más eficaz y coordinada en



caso de un incidente real.

Las pruebas también proporcionan una oportunidad para evaluar la efectividad de la comunicación interna y externa, asegurando que la información correcta se transmita de manera oportuna. Asimismo, ayudan a verificar que los recursos y herramientas necesarios estén disponibles y en buen estado de funcionamiento.

En resumen, las pruebas del Playbook permiten ajustar y optimizar el plan, garantizando que sea robusto, práctico y alineado con las necesidades de la organización. Sin estas pruebas, un Playbook podría ser ineficaz y dejar a la organización vulnerable en momentos críticos.

Conclusiones

Hemos analizado que los procesos de negocio que poseen recursos tecnológicos como soporte son susceptibles a interrupciones, más allá del tipo de fallo que tenga la tecnología (obviamente que un ciberataque es algo más preocupante). Hoy cualquier tipo de organización puede tener una interrupción, por lo cual, es sumamente necesario contar con un PLAN B ante contingencias. Hemos comentado que ese PLAN B puede ser un esquema de PLAYBOOK, que obviamente requiere un trabajo previo, pero en el análisis de los requerimientos podemos encontrar cosas a corregir y que no están alineadas a los procesos de negocio, como también cuestiones de toma de decisiones que pueden quedar definidas.

Ante un incidente, la organización va a estar mejor preparada ante un incidente y la postura ante la sociedad es mejor, porque va a mostrar un nivel de madurez diferente, que estar poniendo en un pizarrón improvisado el estado de los servicios. No encarar un proceso de revisión y no tener en cuenta procesos de recuperación de PROCESOS DE NEGOCIO, se limitará a cuestiones técnicas y que dependerá de los recursos y la buena voluntad de su personal, mientras sus procesos están afectados.

Hoy se debe trabajar en procesos, la tecnología es la mejor herramienta, el crecimiento y las nuevas novedades que vienen como sunami a intervenir en las

organizaciones, permitirán que estén mejor posicionadas ante una situación.

Su organización está dispuesta a cocinar un bizcochuelo?

El autor

- Analista de Sistemas.
- Auditor Lider ISO 27001 by BSI.
- Perito Forense.
- Socio Gerente PuntoNet Soluciones.
- Reconocido como MVP por 19 años por Microsoft.
- Premiado 2018 CYBERSECURITY PROFESSIONAL AWARDS LATAM.
- Vicepresidente de CIIECCA.
- Docente Univ. Blas Pascal en MBA.

Puntonet tech

ROMINA FLORENCIA CABRERA

DERECHO PROCESAL Y NUEVAS TECNOLOGÍAS, REDISEÑANDO EL SISTEMA EDUCATIVO

Abogada. Dos Órdenes al Mérito, Naciones Unidas de las Letras. DHC por el Claustro Doctoral Internacional México . Maestra Destacada Interamericana Bia 2021,2022, Facultad Interamericana de Litigación. Maestra Internacional Destacada por la UNLP (IRI), UBA y el Ianca, 2023. Directora de la Dirección Internacional de Seguridad Informática de procedimientos policiales y ASCASEPP .

El Proceso está protegido en el sistema interamericano de los Derechos Humanos. Cualquier menoscabo o violación del mismo supone el no acatamiento a las normas supranacionales que conforman la comunidad internacional. El estado que vulnere dichas normativas, y que ha suscripto debidamente los Instrumentos Internacionales de Derechos Humanos, queda sujeto a las sanciones pertinentes dispuestas por los mecanismos del Derecho Internacional Público. Las tecnologías de la Información y la Comunicación, además de la llamada Inteligencia Artificial, han transformado el esquema clásico de acción, Jurisdicción y Proceso, evolucionando los conceptos de prueba y Garantías Procesales, como también del la Justicia electrónica.

Es una oportunidad para avanzar, y sobre todo, para integrar y trabajar interdisciplinariamente, el Derecho Procesal y las Nuevas Tecnologías, de una manera seria, eficiente y eficaz. La introducción de las Nuevas Tecnologías al Proceso Clásico, que pasó de la oralidad a la escritura, y ahora al expediente digital y a la firma digital, como a las audiencias por videoconferencia, constituye un avance maravilloso, si los agentes judiciales actúan como un sistema equilibrado, donde todos los elementos

interoperables, se integren, en beneficio de resultados concretos, eficientes y eficaces, buscando la solución más justa en el caso presentado.

Se pretende lograr en los educandos, pensamiento crítico; respeto a las garantías Procesales y Derechos Humanos, y la relación de los abogados con el mundo tecnológico. Incorporando las llamadas Tecnologías de la Información y la Comunicación, el juez tendrá más tiempo de analizar los casos que se plantean en su fuero y fundamentar sus fallos, utilizando estas herramientas comunicacionales queproporcionan inmediatez en lainformación y aceleramiento en el proceso. Con la debida capacitación de todos los integrantes del mismo, y un software oficial especializado y eficaz, una plataforma de desarrollo eficiente, la adecuada administración de licencias y una base de datos con seguridad en los mismos. Las políticas de publicidad, confidencialidad y privacidad de la información son fundamentales para preservar los principios constitucionales, expresados en las Declaraciones, Derechos y Garantías de nuestra Carta Magna, y de los Tratados Internacionales incorporados en el Artículo 75, inciso 22, con jerarquía constitucional

Los Educandos deberán incorporar estas nuevas herramientas, para profundizar sus conocimientos, y sobre todo, para poder desarrollarse en este nuevo campo laboral que transformará toda la actividad realizada hasta el presente. Pero sobre todo, sin perder el humanismo, y sobre todo, el sentido ético en el tratamiento de estos temas tan innovativos e importantes.

La inteligencia artificial causara y está causando impacto en el terreno legal , prediciendo sentencias y analizando causas a gran escala de velocidad y cantidad, pero esta automatización deberá estar acompañada de pensamiento holístico, critico y de apostar a trabajo en equipo e interdisciplinario.

En el esquema de corte clásico acción, jurisdicción y proceso, los abogados tienen nuevas posibilidades de maximizar sus recursos tanto técnicos como humanos, si los saben utilizar con expertis e interoperabilidad

GILBERTO PÉREZ

CALL VERIFY SECURE PROTOCOL (CVSP) PROTOCOLO DE AUTENTICACIÓN ACÚSTICA

Resumen Ejecutivo

El ***Call Verify Secure Protocol (CVSP)*** es un protocolo de autenticación acústica en tiempo real pensado y diseñado para garantizar la seguridad de las comunicaciones telefónicas. En respuesta a la creciente necesidad de trazabilidad y autenticación confiable en llamadas, especialmente en contextos como call centers, comercios y servicios financieros, CVSP ofrece un método que verifica la identidad del dispositivo en los primeros segundos de una llamada, sin necesidad de almacenar audio. Mediante el uso de parámetros acústicos y la identificación del IMEI del dispositivo, CVSP actúa como un "certificado acústico" que refuerza la confianza en las llamadas telefónicas. Este protocolo funciona de manera similar a SSL/TLS, proporcionando autenticación segura a las telecomunicaciones y constituyendo una herramienta potente para prevenir fraudes y respaldar investigaciones criminales, adaptándose a las necesidades específicas de la validación acústica en tiempo real.

Contexto

La autenticación de llamadas es un desafío creciente en el ámbito de la ciberseguridad. A medida que los delitos telefónicos y fraudes evolucionan, se necesitan métodos robustos para validar la identidad de los participantes en una llamada. En el contexto actual, donde el fraude telefónico es cada vez más frecuente, los consumidores y las empresas enfrentan riesgos significativos. CVSP surge como propuesta de solución que utiliza parámetros de voz en lugar de audio completo para autenticar al

usuario en tiempo real. Al permitir la autenticación continua y la verificación visual a través de un candado en la pantalla del receptor, CVSP aborda la demanda de una mayor seguridad en las telecomunicaciones, apoyando tanto a empresas privadas como a instituciones gubernamentales.

La idea del Call Verify Secure Protocol (CVSP) surge ante la creciente vulnerabilidad en la autenticación de identidad en llamadas, agravada por la posibilidad de clonar voces con inteligencia artificial. Tras un laboratorio experimental, se evidenció que al entrenar un sistema
de Inteligencia Artificial (IA) tipo Private Branch Exchange (PBX) con voces de instituciones conocidas y datos filtrados de usuarios, era posible realizar ataques de vishing extremadamente efectivos. Estos ataques aprovechan la falta de mecanismos de validación para suplantar voces con alta precisión, engañando a los usuarios mediante un asistente virtual que aparenta legitimidad. CVSP nace, por tanto, como una propuesta para autenticar en tiempo real la identidad en llamadas, minimizando el riesgo de suplantación al verificar la autenticidad acústica de la voz en cada comunicación.

Call Verify Secure Protocol (CVSP) es el nombre propuesto para el protocolo de autenticación acústica, este debe capturar parámetros de voz en tiempo real, generando un certificado que confirma la legitimidad o no del emisor, visible para el usuario con un candado abierto o cerrado según corresponda en la barra superior del dispositivo junto al nombre del proveedor del sistema de telefonía.

Entre sus casos de uso, CVSP permitirá detectar intentos de bots de replicar voces humanas en llamadas, asegurando la integridad de los procesos de verificación en centros de atención y canales de soporte. Al analizar parámetros acústicos específicos y compararlos con las muestras acústicas base, el protocolo puede identificar variaciones que sugieren manipulación o suplantación. Además, en situaciones de riesgo, este sistema facilita la trazabilidad de las llamadas, permitiendo que las agencias de seguridad identifiquen y bloqueen actividades automatizadas maliciosas, contribuyendo a la protección de usuarios y empresas.

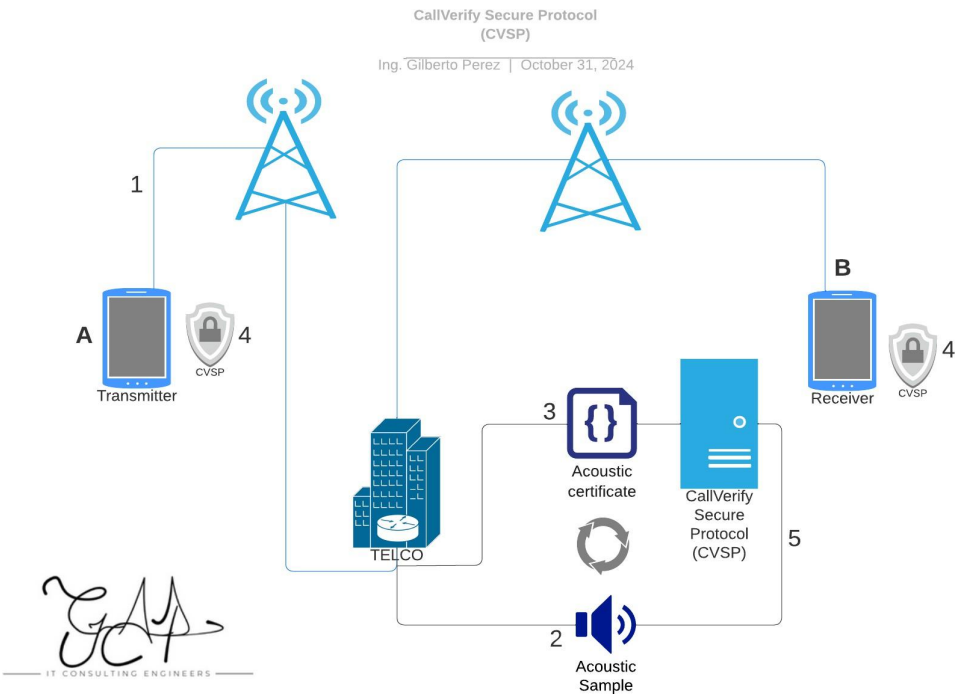
Al implementar un marco robusto de autenticación en tiempo

real, CVSP no solo mejora la seguridad de las comunicaciones, sino que también optimiza la experiencia del usuario, reduciendo falsos positivos y garantizando que solo se validen interacciones legítimas. En un entorno donde la ciberdelincuencia evoluciona constantemente, la capacidad de CVSP para adaptarse y responder a estas amenazas emergentes es fundamental para salvaguardar la confianza en los sistemas de comunicación digital.

La propuesta de protocolo CVSP prioriza la privacidad al evitar el almacenamiento de grabaciones de voz completa. En lugar de ello, extrae y transforma parámetros acústicos específicos en texto, que luego se envían al servidor de autenticación como certificados. Estos parámetros no contienen información de la voz en sí, sino características que, cuando se comparan con la muestra base registrada, verifican la autenticidad sin exponer datos sensibles del usuario.

Además, el proceso de aprendizaje adaptativo de CVSP permite actualizar la muestra base sin comprometer la privacidad del usuario ni almacenar datos identificables de forma directa. Este enfoque garantiza una alta seguridad y privacidad al cumplir con estándares de protección de datos, mitigando riesgos de exposición en el caso de intrusiones o intentos de acceso no autorizados al servidor.

Secuencia Operativa y



Arquitectura de Autenticación en Tiempo Real

Cada llamada pasaría por un análisis continuo de parámetros de voz, que son transformados en certificados enviados a ambos dispositivos participantes. A través de un sistema de notificaciones auditivas y visuales accesibles, CVSP garantizaria una comunicación confiable y privada, abordando tanto la seguridad como la inclusión del usuario en la experiencia.

1. Inicio de la Comunicación: Cuando el usuario A inicia la llamada a B, el dispositivo conecta con su celda, que transmite la solicitud a la red de telecomunicaciones (telco). Esta autenticación preliminar permite que la llamada avance hacia la celda receptora de B, estableciendo la conexión segura.

2. Captura de Muestras Acústicas: Al comenzar la llamada, la telco extrae parámetros acústicos de ambos usuarios. Estos se convierten en texto y se comparan con muestras base de cada dispositivo, verificando autenticidad sin almacenar la voz completa.

3. Generación del Certificado: Al confirmarse la autenticidad, se emite un certificado de seguridad compartido con los dispositivos de A y B.

4. Notificación Inclusiva y Visual: En los primeros 10 a 15 segundos, un tono personalizado (distinguible para no videntes) notifica la validación exitosa. Además, un candado abierto o cerrado según corresponda, aparece junto al nombre de la empresa proveedora del servicio en la barra superior del dispositivo, indicando si la llamada es segura o no.

5. Autenticación Continúa: Este proceso de verificación se realiza periódicamente en cada llamada, ofreciendo un monitoreo constante para ambas partes.

Muestra Acústica Base: Modelo Dinámico de Autenticación Adaptativo

La muestra acústica base en el CVSP, es un modelo de referencia compuesto por parámetros específicos que representan las características de la voz del usuario, sin incluir grabaciones completas. Estos parámetros incluyen aspectos como frecuencia, tono, cadencia, timbre y fluctuaciones en el sonido de la voz, que capturan los elementos

individuales de cada locutor sin almacenar el audio en sí.

La creación de esta muestra base comienza con las primeras interacciones, estableciendo un perfil inicial. Con cada nueva llamada, el sistema utiliza aprendizaje automático para ajustar y enriquecer la muestra, refinando los parámetros en función de factores como el entorno acústico, la claridad de la señal y el tono de voz. Este proceso adaptativo permite que la muestra base evolucione, manteniendo su precisión y fiabilidad independientemente de los cambios en el entorno de cada llamada.

A medida que el usuario continúa comunicándose, el sistema reconoce patrones y reajusta la muestra acústica base, minimizando errores y mejorando la autenticación.

Este modelo garantiza autenticidad en tiempo real al estudiar cada entorno acústico y adaptarse a las variaciones que ocurren naturalmente en la voz, aumentando así la eficacia del CVSP en la protección de las comunicaciones.

Registro Acústico Verificable: Análisis de Parámetros Acústicos

El registro acústico verificable (RAV), es una toma de muestra de audio diseñada para su validación, que contiene parámetros acústicos específicos que permiten comprobar su autenticidad. Este registro se compara con una muestra acústica base para determinar su veracidad.

El RAV se compone de varios parámetros que se extraen de un archivo de audio utilizando la solución de software desarrollada y otras técnicas de análisis de señales. Los parámetros incluyen:

●Energía: Mide la energía total del audio, lo que indica la intensidad de la señal.

●Duración Promedio de Silencio: Promedio del tiempo en que no hay actividad sonora.

●Entropía Espectral Promedio: Indica la complejidad y variabilidad del espectro de la señal.

●Tono (Pitch): Frecuencia fundamental de la señal, importante para identificar la voz.

●Formantes (F1, F2, F3, F4): Frecuencias resonantes que caracterizan el timbre de la voz.

●Intensidad: Mide la energía promedio de la señal RMS (Root Mean Square).

●Variabilidad de Frecuencia: Mide la dispersión de las frecuencias en la señal.

●Prosodia: Captura la variabilidad de la frecuencia a lo largo del tiempo.

●Jitter y Shimmer: Indicadores de la variabilidad en el periodo y amplitud, respectivamente.

●Voceo y Soplo: Miden características específicas de la voz.

●Timbre: Refleja la calidad tonal de la señal.

●MFCCs: Representan la envolvente del espectro de la señal y son útiles para caracterizar la calidad de la voz.

Laboratorio

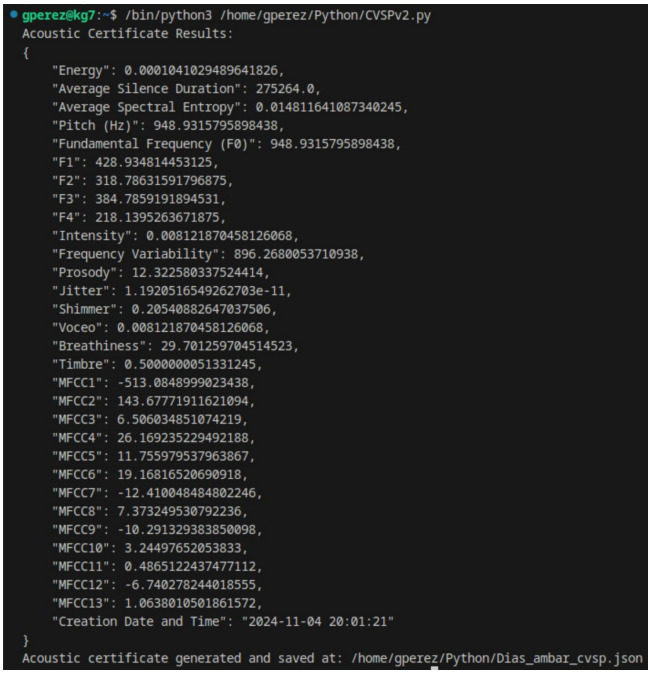
En pruebas técnicas de laboratorio, pudimos observar que esta estructura permite capturar la esencia de la voz del usuario en solo 1.1 KB, proporcionando una

representación acústica suficiente para la autenticación sin almacenar la grabación completa de la voz.

La estructura de CVSP permite una transmisión de datos rápida y eficiente, ideal para sistemas que requieren autenticación en tiempo real. Comparado con un archivo de audio típico, que tenía un tamaño de 550.6 KB en formato .WAV con 5 segundos de grabación, la compresión de información se logró a 1.1 KB

que para RAV representa una optimización significativa, logrando una reducción de aproximadamente el 99.8%.

Esta ligereza en el peso facilita la integración del protocolo en dispositivos y redes con recursos limitados, mientras que la reducción de



datos minimiza los riesgos de privacidad al evitar el almacenamiento de la voz completa. Además, el peso reducido garantiza la escalabilidad permitiendo una implementación a gran escala sin sobrecargar las redes o comprometer la velocidad de respuesta en las verificaciones de identidad.

Los parámetros acústicos capturados, como energía, duración promedio de silencio, entropía espectral promedio, tono, formantes (F1, F2, F3, F4), intensidad, variabilidad de frecuencia, prosodia, jitter, shimmer, voceo, soplo, timbre y MFCCs, contribuyen a que de alguna manera podamos alcanzar una identificación precisa y confiable, mejorando la eficacia del sistema de autenticación sin sacrificar la seguridad o la calidad de la señal.

Nota: Las pruebas de laboratorio realizadas hasta la fecha Septiembre 2024, están aún en su fase experimental y deben considerarse como referencias preliminares de viabilidad en la captura de parámetros. Se requieren más pruebas exhaustivas para establecer la validez y efectividad del protocolo en escenarios reales de autenticación.

Conclusión

Este white paper ha delineado los fundamentos y avances del Call Verify Secure Protocol (CVSP), una nueva propuesta para la validación acústica en tiempo real, que busca optimizar la autenticación en entornos de comunicación contemporáneos. A lo largo de mi investigación, estoy desarrollando modelos preliminares para demostrar la viabilidad técnica y la eficiencia del protocolo, evidenciando su capacidad de validación y para reducir significativamente el volumen de datos necesarios para la autenticación sin comprometer la integridad de la información.

La fase actual de investigación y desarrollo representa un momento crucial en la evolución del CVSP. Es imperativo contar con la colaboración de diversos sectores, incluyendo expertos académicos, profesionales de la industria y entidades gubernamentales, para enriquecer y validar mi enfoque. La integración de múltiples perspectivas y conocimientos especializados no solo fortalecerá la robustez del protocolo, sino que también permitirá su adaptación a las exigencias y desafíos específicos de cada contexto.

Al avanzar hacia las pruebas de concepto, el compromiso colectivo de

estos actores es esencial para asegurar que el CVSP se convierta en un estándar de referencia en autenticación acústica. Mi objetivo es establecer un marco sólido que garantice la privacidad y seguridad de las comunicaciones, alineándose con las mejores prácticas en ciberseguridad.

La implementación efectiva del CVSP no solo promete elevar los niveles de confianza en las interacciones digitales, sino que también contribuirá a la evolución de las tecnologías de autenticación en un mundo cada vez más interconectado.

Estoy entusiasmado por las posibilidades que este protocolo ofrece y esperamos colaborar con todos los interesados en su desarrollo y despliegue.

Referencias

La presente investigación se basa en una revisión exhaustiva de literatura científica y tecnológica en áreas clave como biometría, acústica forense, encriptación de datos y protocolos de autenticación para comunicaciones digitales. Este trabajo también incorpora aportes derivados de consultas en portales especializados, análisis de artículos académicos y conversaciones con expertos en diversas disciplinas.

A continuación, se presentan algunas de las fuentes bibliográficas relevantes:

●Vilches Lagos, N. (2002). Guía Práctica Utilización de Praat en la Evaluación Clínica de la Voz. Documento de trabajo n°48, CIES, Universidad San Sebastián. ISBN: 97156-3-X.

●Dirección Nacional Cuerpo Técnico de Investigación, Fiscalía General de la Nación. Acústica Forense. ISBN: 97156-3-X, 2002.

●López Troccoli, K. Presentación INACIF Instituto Nacional de Ciencias Forenses de Guatemala.

●Hernández Villorria, R. (2003). Análisis Acústico Computarizado de la Voz. Presentación.

●Dierks, T., & Rescorla, E. (2008). The Transport Layer Security (TLS) Protocol Version

1.2. RFC 5246, Internet Engineering Task Force (IETF). https://datatracker.ietf.org/doc/html/rfc5246

●Rescorla, E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446, Internet Engineering Task Force (IETF). https://datatracker.ietf.org/doc/html/rfc8446

●Boersma, P., & Weenink, D. Praat: Doing Phonetics by Computer (Version 6.1.40). Software de análisis de la voz y fonética. https://www.fon.hum.uva.nl/praat/

Derechos de Uso y Contribuciones

Este White Paper se presenta bajo un esquema de acceso abierto, con el propósito de fomentar el intercambio de conocimiento y la colaboración interdisciplinaria. Como propuesta en desarrollo, está abierto a mejoras, aportes y revisiones por parte de la comunidad académica, profesional y del sector interesado. Al compartir este proyecto, se invita a expertos y entidades interesadas a contribuir en su perfeccionamiento y a explorar nuevas aplicaciones. El contenido de este documento se ofrece bajo una licencia de atribución estándar, permitiendo su uso, modificación y redistribución, siempre que se respeten los créditos y se mantenga el espíritu de colaboración continua.

El autor: Gilberto Pérez es un experto en Tecnología, consultor y conferenciante internacional con más de 15 años de experiencia en el sector privado, especializado en la dirección, gestión e integración de proyectos de TI. También especializado en la creación y gestión de políticas y procedimientos de gestión de la seguridad, certificado por las principales marcas de tecnología.

Autor del libro, Inteligencia Artificial: Explorando los Límites de la Tecnología.

Es Ingeniero en Sistema y Computación con Maestría en Ciberseguridad, Experto en Informática Forense y Ciberderecho, Autopsy Digital Forensics

Certified, también cuenta con un MBA y una maestría en Gestión de Proyectos.

CEO y Fundador de Solteda Consultores, Co-fundador de Realtime Technologies, Co-fundador de la Comunidad Linux Dominicana, Docente de las cátedras de Arquitectura y Diseño de seguridad y Seguridad Informática, además de Gestión de Riesgos TI y Auditoría Informática, en varias Universidades y Centros de estudios de educación superior.


EDI
ELDERECHOINFORMATICO.COM
ESTAMOS
DONDE QUERÉS VOS
• SOMOS, LA RED •

EDI

Vamos...

ELDERECHOINFORMATICO.COM