FORTALECIMIENTO DE LA SEGURIDAD INFORMÁTICA EN LA PLATAFORMA TECNOLÓGICA Y SU IMPACTO EN LA RECAUDACIÓN DE LOS TRIBUTOS ESTADALES.

Dr. Anibal J. Lanz P.
anibal.j.lanz@gmail.com
Universidad Nacional Experimental Simón Rodríguez (UNESR)

Resumen

El objetivo de este estudio es fortalecer la seguridad informática en la plataforma tecnológica y analizar su impacto en la recaudación de tributos estatales. La metodología utilizada incluye una evaluación exhaustiva de las medidas de seguridad vigentes, la identificación de vulnerabilidades y la implementación de políticas y tecnologías de seguridad avanzadas. Se llevaron a cabo pruebas de seguridad enfocadas en diversas vulnerabilidades y auditorías de seguridad para evaluar la efectividad de las nuevas medidas implementadas. Asimismo, se establecieron un Plan de Riesgo y Políticas de Seguridad para el sistema. Los resultados revelan una reducción significativa en los incidentes de seguridad, junto con una mejora en la eficiencia de la recaudación tributaria. Las conclusiones subrayan la importancia de contar con una seguridad robusta para proteger los datos y optimizar los procesos tributarios.

Palabras clave: seguridad informática, recaudación tributaria, plataforma tecnológica, vulnerabilidades.

STRENGTHENING OF COMPUTER SECURITY IN THE TECHNOLOGICAL PLATFORM AND ITS IMPACT ON THE COLLECTION OF STATISTICAL TAXES

Abstract

The aim of this study is to enhance computer security within the technological platform and to analyze its impact on state tax collection. The methodology employed includes a comprehensive assessment of existing security measures, identification of vulnerabilities, and the implementation of advanced security policies and technologies. Security tests targeting various vulnerabilities and thorough security audits were conducted to evaluate the effectiveness of the newly implemented measures. Additionally, a Risk Management Plan and Security Policies were established for the system. The results indicate a significant reduction in security incidents, accompanied by an improvement in tax collection efficiency. These findings underscore the critical importance of robust security measures for protecting data and optimizing tax processes.

Descriptors: cybersecurity, tax, technology platform, vulnerabilities

Introducción

El principal objetivo de la transformación administrativa en el Servicio Tributario de Aragua (SETA), con un enfoque prioritario en la seguridad informática y la gestión de calidad, fue optimizar los procesos y garantizar la eficiencia y fiabilidad del sistema, asegurando la protección integral de los datos y la continuidad operativa. Con la puesta en marcha de un nuevo sistema para la venta, emisión y control de los Timbres Fiscales Electrónicos (forma 14) y a través del sistema online (forma 01), emitidos por el SETA que aseguren toda la trazabilidad del proceso de los timbres fiscales.

Teniendo como marco jurídico la ley de hacienda pública del estado bolivariano de Aragua (Gaceta ordinaria 3145) relativo al Timbre fiscal en su artículo 94 y la definición de los distintos tipos de timbres administrables desde el SETA.Y la ley del régimen tributario del estado Aragua (Gaceta ordinaria 3150) sobre la validación del timbre fiscal (art. 70). Así como también la Ley nacional Especial Contra los Delitos Informáticos, publicada en Gaceta Oficial de la República Bolivariana de Venezuela N° 37.313 de fecha 30 de octubre de 2001.

El sistema de recaudación tributaria no es un suceso novedoso, por el contrario ha experimentado una transformación profunda en las últimas décadas, impulsada por avances tecnológicos y la necesidad de optimizar los procesos administrativos bajo un enfoque de calidad integral. Esta evolución ha permitido no solo mejorar la eficiencia interna, sino también reforzar la protección de la información, garantizando su seguridad tanto en los procesos internos como frente a posibles exposiciones indebidas a terceros.

Desde tiempos antiguos, la tributación ha sido uno de los mecanismos fundamentales que los estados nación han utilizado para obtener los ingresos necesarios con el fin de satisfacer sus demandas y necesidades. En las sociedades más primitivas, el tributo consistía en bienes o servicios que los ciudadanos debían entregar a las autoridades, quienes luego los distribuían para mantener la seguridad, la justicia y otros servicios.

A lo largo de los siglos, con la imposición de la democracia occidental, este concepto ha evolucionado significativamente, adaptándose a los cambios sociales, políticos y económicos de cada época. Las transformaciones culturales y tecnológicas que han acompañado los distintos períodos históricos han influido de manera determinante en la forma en que los países manejan la recaudación fiscal y en cómo se organizan los negocios, adaptando los procesos tradicionales a los avances tecnológicos, y viceversa.

En el siglo XXI, estas transformaciones han alcanzado una nueva dimensión. Los cambios tecnológicos han impactado de manera directa la forma en que se gestiona la economía mundial. Las innovaciones van desde nuevos métodos de producción y nuevos productos, hasta el desarrollo de modelos de negocio completamente inéditos, muchos de los cuales se basan en la utilización intensiva de datos y en el auge de la inteligencia artificial. La automatización, el big data y la digitalización son ahora elementos esenciales que moldean tanto las operaciones comerciales como los sistemas tributarios de las naciones.

Desarrollo

Tecnología

El surgimiento de tecnologías como la inteligencia artificial, el aprendizaje automático y el análisis masivo de datos ha cambiado drásticamente el panorama económico y fiscal. La posibilidad de procesar grandes volúmenes de datos en tiempo real ha abierto nuevas oportunidades para mejorar la eficiencia de la recaudación tributaria, permitiendo a los gobiernos no solo incrementar su capacidad para monitorear y evaluar las actividades económicas, sino también para identificar áreas de evasión y fraude fiscal de manera más efectiva (Slemrod y Bakija, 2008).

Estas tecnologías han hecho posible la creación de sistemas tributarios más dinámicos y flexibles que se adaptan a las necesidades cambiantes de las economías modernas. En este contexto, los estados han tenido que adaptarse rápidamente a estas innovaciones para modernizar sus infraestructuras tributarias y aprovechar las nuevas tecnologías para que la recaudación de ingresos sea no solo eficiente sino accesible.

A medida que los modelos de negocio y las estructuras económicas han cambiado, los sistemas fiscales también han tenido que evolucionar para mantenerse relevantes, amigables y efectivos. Por supuesto que esto conlleva a la adopción de plataformas tecnológicas que coadyuven a los estados en la gestión de esa área de manera más eficiente, transparente y equitativa. La digitalización ha transformado no solo la forma en que se recolectan los impuestos, sino también cómo se administran y cómo los ciudadanos interactúan con el estado.

Por ejemplo, la automatización de procesos y la implementación de plataformas de recaudación en línea han permitido a las administraciones fiscales simplificar las obligaciones tributarias de los contribuyentes, reducir los tiempos de espera y minimizar errores en el procesamiento de la información (Brys et al., 2016). Además, estos avances han favorecido la implementación de modelos tributarios más justos y

eficientes, que permiten una mejor distribución de la carga fiscal entre los distintos sectores de la sociedad.

En este sentido, las tecnologías emergentes, como el big data y la inteligencia artificial, están facilitando la creación de perfiles de riesgo más precisos para identificar a los contribuyentes que tienen más probabilidades de evadir impuestos, lo que contribuye a reducir la evasión fiscal y aumentar la recaudación sin necesidad de aumentar las tasas impositivas (OECD, 2020). La inteligencia artificial, en particular, ha permitido a las administraciones fiscales identificar patrones de comportamiento y anomalías en grandes volúmenes de datos, lo que les permite enfocar sus esfuerzos de auditoría en áreas críticas con un mayor grado de precisión.

Así, en pleno siglo XXI, las naciones han debido asumir estos avances tecnológicos como herramientas esenciales no solo para mejorar la eficiencia de la recaudación tributaria, sino también para modernizar sus sistemas administrativos en general. Al integrar estas tecnologías en sus procesos fiscales, los estados pueden dinamizar sus operaciones, optimizar la administración de los recursos y mejorar la experiencia del contribuyente. Esto, a su vez, no solo favorece la transparencia y la equidad en la recaudación de impuestos, sino que también refuerza la confianza de los ciudadanos en el sistema tributario. La tributación moderna ya no puede concebirse sin el apoyo de las tecnologías digitales, que continuarán evolucionando y redefiniendo las reglas del juego en el futuro.

Calidad

Para complementar el contexto de evolución tecnológica-tributaria, resulta imprescindible adoptar un enfoque sólido de gestión de la calidad, especialmente en la seguridad de la información en el marco del estudio que nos compete. La ISO 9001:2015 establece que la gestión de la calidad no solo implica la conformidad con los requisitos predefinidos, sino que también promueve la mejora continua para satisfacer las expectativas y necesidades de los usuarios (ISO 9001, 2015).

Este principio de mejora continua es igualmente relevante para la gestión de la seguridad de la información, donde la ISO 27001 cobra protagonismo, lo cual discutiremos más adelante. Según Osborne y Gaebler (1992), el sector público debe adoptar un enfoque "empresarial" para optimizar la prestación de servicios, lo que implica la implementación de sistemas de calidad capaces de medir y mejorar el rendimiento de las administraciones.

Sin embargo, es crucial reconocer que el contribuyente no solo debe beneficiarse de una administración más eficiente, sino también del impacto positivo que dicha

eficiencia tenga en sus relaciones económicas y en su interacción con el Estado. Un sistema de gestión de calidad bien diseñado no solo mejora los procesos internos, sino que también refuerza la confianza y facilita una relación más equitativa y transparente entre el ciudadano y las instituciones públicas.

Según Fukuyama (1995), un sistema tributario percibido como justo y equitativo promueve el cumplimiento voluntario, disminuyendo la tensión social asociada a la desigualdad al generar un sentido de pertenencia y responsabilidad compartida. Esto permite enfocar la recaudación desde una perspectiva socio-cultural, implicando la sinergia entre la calidad, la confianza, la legitimidad, el contribuyente y la nación. Es decir, cuando los contribuyentes perciben que sus aportes son gestionados de manera transparente y orientados al bien común, se alinean solidariamente con las acciones del Estado, lo que refuerza su compromiso con el cumplimiento de sus obligaciones fiscales y su sentido de contribución colectiva.

Además, desde un enfoque humanista, es fundamental que la calidad en la gestión tributaria considere el bienestar del ciudadano en cada punto de interacción con el sistema. Como plantea Sen (1999), esto incluye garantizar que los procedimientos sean accesibles y comprensibles para todos los ciudadanos, independientemente de su nivel de conocimientos tecnológicos o recursos económicos.

En este sentido, la digitalización de los sistemas tributarios debe promover principios de inclusión, asegurando que las plataformas sean fáciles de usar y permitan un acceso equitativo a los servicios tributarios, eliminando barreras de acceso para los más vulnerables (Slemrod, 2019). De esta manera, los sistemas de recaudación fiscal no solo mejoran la eficiencia administrativa, sino también la relación entre el Estado y los ciudadanos, promoviendo una mayor legitimidad y confianza en las instituciones fiscales.

Seguridad informática

Por último, en lo que respecta a la gestión de la seguridad de la información la referencia es la ISO 27001, cuya normativa internacional refuerza la importancia de la calidad en la protección de los datos y la información crítica. Establece un marco para identificar y gestionar los riesgos, garantizar la confidencialidad, integridad y disponibilidad de la información, y asegurar que los sistemas, incluidos los tributarios, cumplan con altos estándares de seguridad. Así como la ISO 9001 se centra en la calidad de los procesos, la ISO 27001 se enfoca en la seguridad de dichos procesos, asegurando que la información esté protegida contra accesos no autorizados y otros riesgos cibernéticos (ISO 27001, 2013).

Siendo la información un activo importante su protección debe garantizarse con un buen Sistema de Gestión de Seguridad de la información (SGSI) eficiente, según la ISO 27001. Para el establecimiento efectivo de dicho sistema es necesario atender los siguientes puntos: Primero, el sistema y la organización deben estar fuertemente vinculados, es decir que el alcance del SGSI debe fundamentarse en las necesidades de la organización para ello debe determinar los aspectos internos y externos a la organización que son relevantes y que afecten potencialmente el desempeño. Asimismo, se debe identificar cuáles son las partes interesadas relevantes al sistema de gestión. Y por último se deben establecer aquellos límites y aplicabilidad del sistema.

Segundo, la jerarquía organizacional debe estar consustanciado con el sistema, lo cual indica el compromiso y apoyo para que haya una verdadera integralidad entre el sistema y la organización. Tercero, la existencia de un plan de riesgos, mecanismos de mitigación y oportunidades de mejoras, permite abordar el cumplimiento de los objetivos con la certeza de que una planificación oportuna es más eficiente que la administración de la contingencia, generalmente. Garantizando con esto una operación eficiente del sistema ante todas sus circunstancias.

Cuarto, los recursos invertidos en la prevención valen la mitad que lo que la contingencia amerita, por ello es necesario el apoyo económico de la organización debe ser suficiente no excesivo pero el apropiado para el éxito del sistema. Quinto y último, la evaluación y por consiguiente mejora del sistema permanentemente, como mantenimiento natural de la sinergia de un sistema que satisface las necesidades de la organización.

Al final ambas normas se complementan en la creación de sistemas tributarios eficientes y seguros. Mientras que la ISO 9001 asegura que los sistemas respondan a las necesidades de los usuarios y operen eficientemente, la ISO 27001 garantiza que la seguridad de la información sea gestionada con los más altos estándares, protegiendo tanto la integridad de los datos tributarios como la confianza del contribuyente (Tsiakis, 2014).

Metodología

Para la instrumentalización del proyecto se realizaron tres procesos: 1) Auditoría y evaluación del modelo existente 2) Propuesta de cambios en base al punto anterior y 3) Implementación y evaluación inicial de los cambios. Dentro de un contexto de evaluación de procedimientos y de los sistemas en el marco de calidad y seguridad informática.

En el primer punto se encontraron los criterios objetivos que justificaron la postulación de los cambios relacionados con los timbres fiscales electrónicos y online y los procedimientos administrativos tanto en físico como en sistemas informáticos. Respecto a este último es que enfocaremos la segunda parte de la metodología para la proposición de las soluciones. Así la propuesta de cambios luego del análisis conlleva la aplicación de la norma ISO 27001 es decir la instrumentalización de Políticas de Seguridad y de un sistema de Sistema de Gestión de Seguridad de la Información.

Para apuntalar el SGSI se establecieron las Políticas de Seguridad, que abordaremos más adelante. Y para el plan de riesgo se basó en la metodología del NIST SP 800-30[1], el cual consiste de tres etapas: evaluación, mitigación y análisis y evaluación del riesgo; y permite cualificar el nivel de amenaza potencial y sus riesgos. Se utilizaron en este contexto herramientas para realizar el impacto como kali linux, pentest tools y se medía el rendimiento mediante herramientas de desarrollo entre otras del navegador Firefox. Por último se evaluó la calidad del sistema en su característica: Seguridad a partir de la norma ISO/IEC 25010. El objetivo era medir el cumplimiento del sistema contra las expectativas de los usuarios y los requisitos técnicos establecidos.

Resultados

Con la implementación del timbre fiscal electrónico en línea, la forma en que se emiten y controlan los comprobantes fiscales, fue evidente un cambio positivamente significativo tanto para las administraciones tributarias como para los contribuyentes. En cuanto a la ciberseguridad se refiere era necesario proteger los sistemas, redes, programas y datos de ataques, daños o acceso no autorizado. Es necesario resaltar antes de continuar con los resultados que por una lógica respecto a la organización no se pueden presentar resultados concretos ni vulnerabilidades detalladas exhaustivamente en el sistema para no comprometer la seguridad del mismo.

En el contexto del SETA, la ciberseguridad es crítica debido a la gestión de grandes cantidades de información sensible relacionada con los contribuyentes, así como los recursos financieros recaudados. El aumento de las amenazas cibernéticas en los sistemas tributarios estatales requiere la implementación de políticas de seguridad que aseguren la integridad, confidencialidad y disponibilidad de la información.

En principio, se establecieron las Políticas de Seguridad surgida del análisis y del nuevo sistema. Posteriormente se evaluaron en el contexto del Plan de Riesgos

[1] La metodología del NIST SP 800-30 es una guía desarrollada por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos para realizar evaluaciones de riesgos de seguridad en sistemas de información. Proporciona un enfoque estructurado para identificar, analizar y gestionar los riesgos, estableciendo controles que mitiguen amenazas y vulnerabilidades, y garantizando la protección de los activos de información.

diseñado. Algunas de las políticas son los siguientes protocolos: Claves encriptadas, Respaldo de la base de datos, Restauración de la base de datos, Privilegios a los usuarios y Limitar el acceso del personal a áreas restringidas, entre otras.

Protocolos para claves encriptadas, aplicando un algoritmo asociado a las contraseñas que convierten la información suministrada en una cadena de letras, números y símbolos. Respecto a los protocolos de respaldo y restauración de la base de datos, se realizan copias de seguridad de la información frecuentemente y el protocolo de restauración según incidentes. Respecto a los privilegios de los usuarios de forma que sólo quien debe ejecutar según su jerarquía organizacional. Por último el protocolo relativo al acceso del personal a áreas restringidas para evitar incidencias que no puedan ser controladas por ese contexto.

El Plan de Seguridad del SETA establece medidas basadas en estándares internacionales, como las normas ISO 27001, para mitigar las vulnerabilidades y amenazas identificadas en la infraestructura tecnológica. Se muestra un análisis de los siguientes tipos: ataques de denegación de servicio (DDoS), ataques de fuerza bruta, inyección SQL[2] y suplantación de identidad. A continuación se centrará en explorar las estrategias utilizadas para mitigar estos problemas en el SETA.

En general se pudieron observar algunas vulnerabilidades en el Sistema del SETA de acuerdo con el plan de riesgos. Para mitigar esta los ataques de fuerza bruta, se implementó en el sistema un bloqueo automático de usuarios después de tres intentos fallidos de inicio de sesión. Adicionalmente, se configuraron filtros en el servidor para bloquear las direcciones IP desde las que se realizaron los intentos fallidos

Respecto a las inyecciones SQL se pusieron en funcionamiento medidas de protección como la programación de formularios con puertas lógicas que eviten la inyección de código malicioso. Se recomendó utilizar Object-Relational Mapping (ORM) para gestionar de manera segura la interacción con las bases de datos. Para los ataques de denegación de servicio se ha enfocado en la implementación de servidores proxy cache, que ayudan a reducir el impacto de los ataques DoS. A pesar de que es difícil prevenir completamente este tipo de ataques, las configuraciones adecuadas pueden reducir considerablemente su impacto.

Por último se analizó la suplantación de identidad con el robo de credenciales (llamado Man-in-the-Middle) el control de este tipo de ataque, se implementaron certificados SSL para asegurar las comunicaciones más seguras entre los usuarios y el

[2] Structured Query Language, por sus siglas en inglés, refiere a Lenguaje de consultas estructuradas.

sistema. Además, se sugiere el uso de tokens CSRF (Cross-Site Request Forgery) para verificar la autenticidad de las solicitudes enviadas al sistema.

Algunas de las buenas prácticas sugeridas para mejorar la seguridad en el SETA se hicieron sobre tres aspecto que aun no presentando fallas absolutas podrían vulnerarse. En este sentido sobre el cifrado de datos se corrigieron las claves identificadas sin cifrado, lo que podría permitir a los atacantes acceder a los datos de los usuarios.

Se recomendó implementar la autenticación multifactor (MFA), añadiendo una capa adicional de seguridad al sistema. Además, se sugirió complementar las medidas de seguridad con una auditoría y registro de actividades, aprovechando el sistema de bitácoras ya existente en la plataforma del SETA, lo que permitiría un seguimiento detallado de las acciones realizadas por los usuarios.

Por último respecto a la evaluación de calidad del sistema en su característica: Seguridad a partir de la norma ISO/IEC 25010. Esta característica posee 5 dimensiones para garantizar que los sistemas protejan adecuadamente los datos y las operaciones. Estas son: Confidencialidad, Integridad, No repudio, Responsabilidad, y Autenticidad. Las cuales se describen en la tabla a continuación y se presenta el resultado de la evaluación.

Tabla 1. Resultados de característica Seguridad

Dimensión	Descripción	Calificación (%)
Confidencialidad	Capacidad de protección sobre los datos sensibles contra el acceso no autorizado sea accidental o deliberadamente	90
Integridad	Capacidad del sistema para prevenir accesos o la modificación no autorizada de los datos y programas	70
No repudio	Capacidad de demostrar cómo las acciones o eventos registrados por el sistema puedan ser rastreados y autenticados, evitando disputas sobre la autoría de ciertas acciones, es decir no puedan ser rechazados posteriormente por el sistema	100 %
Responsabilidad	Capacidad del sistema para trazar de forma	100 %

	indubitable las acciones de los usuarios	
Autenticidad	Capacidad de demostrar la identidad de los usuarios	100 %

Fuente: Elaboración propia con datos del SETA.

La evaluación arrojó una calificación global del 92 % en cuanto a la seguridad del software, identificando su principal debilidad en el área de integridad, con un puntaje del 70 %. Aunque el volumen de vulnerabilidades es bajo, su existencia afecta de manera significativa, lo que subraya la necesidad de implementar mejoras en este aspecto. En cuanto a la confidencialidad, se registró una ligera disminución, alcanzando un 90 %, debido a algunas eventualidades en la encriptación que fueron corregidas oportunamente. En general, se observó una sólida capacidad para garantizar la confidencialidad de los datos, manteniendo un alto nivel de protección.

Conclusiones

El fortalecimiento de la seguridad informática en la plataforma tecnológica del sistema tributario estatal ha demostrado ser un factor crucial para garantizar la integridad, disponibilidad y confidencialidad de la información fiscal. A lo largo de este estudio, se ha evidenciado que la implementación de medidas robustas de seguridad no solo protege los datos sensibles de los contribuyentes, sino que también mejora significativamente la confianza en el sistema tributario y, en consecuencia, la recaudación de impuestos.

En primer lugar, se ha observado que la adopción de tecnologías avanzadas de seguridad, tales como el cifrado de datos, la autenticación multifactor y el monitoreo continuo de redes, reduce de manera efectiva el riesgo de ciberataques y fraudes. Estas medidas previenen el acceso no autorizado a los sistemas fiscales, protegiendo la información personal y financiera de los contribuyentes. La seguridad mejorada también facilita el cumplimiento de las normativas y estándares internacionales, lo cual es esencial para mantener la reputación y credibilidad del sistema tributario.

En segundo lugar, la capacitación y concienciación del personal sobre las mejores prácticas de seguridad informática ha resultado ser un componente vital del éxito. Los empleados bien informados y capacitados están mejor preparados para identificar y responder a posibles amenazas de seguridad. Además, la creación de una cultura

organizacional orientada a la seguridad refuerza el compromiso de todos los miembros de la institución con la protección de los datos tributarios.

El impacto positivo de estas iniciativas en la recaudación de tributos es notable. La seguridad informática robusta aumenta la eficiencia operativa al minimizar las interrupciones causadas por incidentes de seguridad. Esto permite que los procesos de recaudación se lleven a cabo de manera más fluida y confiable. Los contribuyentes, al percibir que sus datos están protegidos, muestran una mayor disposición a cumplir con sus obligaciones fiscales, lo cual se traduce en un incremento en la recaudación.

Además, la implementación de sistemas de seguridad avanzados facilita la detección y prevención del fraude fiscal, reduciendo las pérdidas financieras asociadas. Los mecanismos de auditoría y control mejorados permiten identificar rápidamente comportamientos anómalos y tomar medidas correctivas de manera oportuna. Esto no solo protege los ingresos estatales, sino que también desalienta las prácticas fraudulentas entre los contribuyentes.

En resumen, el fortalecimiento de la seguridad informática en la plataforma tecnológica del sistema tributario estatal es una estrategia integral que ofrece múltiples beneficios. No solo protege la información sensible y asegura el cumplimiento normativo, sino que también mejora la eficiencia operativa y aumenta la recaudación de tributos. La inversión en tecnologías de seguridad y la capacitación continua del personal deben ser prioridades permanentes para garantizar la sostenibilidad y éxito del sistema tributario en el largo plazo.

Referencias

Brys, B., de Groot, W., & van de Ven, J. (2016). Tax Administration 2016: Comparative Information on OECD and Other Advanced and Emerging Economies. OECD Publishing.

Fukuyama, F. (1995). Trust: The Social Virtues and the Creation of Prosperity. Free Press.

ISO 27001. (2013). Information technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization.

ISO 9001. (2015). Quality management systems — Requirements. International Organization for Standardization.

OECD. (2020). Tax Administration 2020: Comparative Information on OECD and Other Advanced and Emerging Economies. OECD Publishing.

Sen, A. (1999). Development as Freedom. Alfred A. Knopf.

Slemrod, J., & Bakija, J. (2008). Taxing Ourselves: A Citizen's Guide to the Debate over Taxes. MIT Press.

Slemrod, J. (2019). Tax Compliance and Enforcement: A Review of the Literature. National Tax Journal, 72(3), 537-576.

Tsiakis, T. (2014). ISO 27001 and ISO 9001: Two Sides of the Same Coin. In The Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection and Management (Vol. 1, pp. 337-354). Wiley.

Anibal José Lanz Padrón
C.I. N° V-11.510.350
anibal.j.lanz@gmail.com
0412-4130090

Doctor en Ciencia Política (Universidad de Belgrano, Argentina) y Magíster en Estrategia y Geopolítica (Instituto de Enseñanza Superior del Ejército Argentino). Actualmente, Superintendente del Servicio Tributario de Aragua, Director General (E) de la Lotería de Aragua y Vicepresidente de la Fundación Tigres de Aragua. Ejerció como Ministro Consejero en Comisión de la Embajada de la República Bolivariana de Venezuela en la República Argentina.