

Explorando los canales de denuncia y al informante (*whistleblower*): factores que inhiben o impulsan a utilizar la herramienta digital

Exploring reporting channels and the whistleblower: factors that inhibit or encourage the use of the digital tool

Esthela Carrillo Cisneros¹ y Oswaldo Pacheco Camacho² y María Guadalupe Bustamante Ruiz³

Resumen: El objetivo en esta investigación es identificar factores que inhiben o impulsan el uso del canal digital de denuncia, mediante un instrumento adaptado de teoría unificada extendida de aceptación y uso de tecnología (UTAUT2); así como evaluar si esta herramienta contribuye a la transparencia e integridad en las organizaciones, considerando que la Ley General de Responsabilidades Administrativas vinculada a particulares establece que el proceso puede ser de manera electrónica. Con enfoque cuantitativo, alcance explicativo, correlacional, no experimental y corte transversal; se aplicaron 290 cuestionarios a conveniencia y se realizó un exhaustivo análisis a la legislación. Los resultados destacan que seguridad, anonimato y confianza fortalecen la percepción positiva del canal digital, cuya accesibilidad mejora el proceso de alertar y promueve la transparencia e integridad. Factores que inhiben denunciar son el desconocimiento, miedo a ser identificado y falta de confidencialidad, destacando necesidad de blindar, integrar tecnología y ciberseguridad al proceso; resultados bajo el alfa de Cronbach=0.838, KMO=0.90 y $r^2=0.538$.

Palabras clave: Canales de denuncia, whistleblower o informante, integridad

Abstract: The objective of this research is to identify factors that inhibit or promote the use of the digital reporting channel through an instrument adapted from the extended unified theory of acceptance and use of technology (UTAUT2), to evaluate whether this tool contributes to transparency and integrity in organizations; considering that the General Law of Administrative Responsibilities linked to individuals establishes that complaints can be made electronically. With a quantitative approach, explanatory, correlational, non-experimental and cross-sectional scope, 290 questionnaires were applied at convenience and exhaustive analysis of legislation. The results highlight that security, anonymity and trust strengthen the positive perception of the digital channel, whose accessibility improves reporting and promotes transparency and integrity. Factors that inhibit reporting are ignorance, fear of being identified and lack

1 Profesora investigadora de la Universidad Estatal de Sonora y del Doctorado en Ciencias Económico Administrativas.

2 Profesor investigador en Universidad Estatal de Sonora y doctor en Derecho Penal.

3 Profesora investigadora en la Universidad Estatal de Sonora.

of confidentiality, highlighting the need to shield, integrate technology and cybersecurity in the process; results under Cronbach's alpha = 0.838, KMO = 0.90 and $r^2 = 0.538$

Keywords: Reporting channels, whistleblower, integrity

Introducción

Como se identifica en esta investigación, en México, una de las principales carencias que existe es la protección de los ciudadanos y servidores públicos que alertan o denuncian conductas que pudieran ser constitutivas de actos de corrupción. Entre los mecanismos que se consideran más convenientes para disponer de información relevante que permita el inicio de investigaciones sólidas contra opciones de fraude y corrupción está la implementación de canales de denuncias (whistleblowing) debidamente regulados y sencillos de usar, a fin de que los informantes dispongan de las suficientes garantías para utilizarlos. Aunado a esto, dicha herramienta tecnológica debería ser asequible para las empresas de menor tamaño y con menor presupuesto, ya que, como se observará en los resultados más adelante detallados, las mipymes afirman tener mayor ocurrencia de actos de corrupción.

Alertar, denunciar, avisar, delatar o señalar incumplimientos detectados en la empresa o en la organización en la que se labora no es algo nuevo. El hecho de “soplar el silbato” (traducción literal del término anglosajón whistleblowing) lleva entre nosotros desde tiempos inmemoriales (Martínez et. al 2020, p. 15). A su vez, tal y como recuerda Del Rey, una de las primeras definiciones del whistleblowing acuñada por el abogado activista Ralph Nader, pretendió abandonar su tradicional connotación negativa (chivato) y darle un enfoque positivo con la siguiente definición: “Un acto de un hombre o una mujer que, creyendo que el interés público prevalece por sobre el interés de la organización en la que él o ella sirve, sopla el silbato públicamente cuando la organización está implicada en actividades corruptas, ilegales, fraudulentas o lesivas” (Martínez et. al 2020, p. 18).

Por ello es de relevancia identificar la proliferación de políticas del whistleblower como un tipo específico de delación (acusación o denuncia que hace alguien de un hecho censurable) que, en términos generales, hace referencia a la denuncia de hechos ilícitos cometidos por una organización pública o privada llevada a cabo por alguno de los miembros de la organización. En las últimas décadas se ha convertido en una de las herramientas de control más eficaz en manos de los Estados; el fomento de este tipo de informantes se ha convertido en contenido habitual en las políticas públicas (Martínez et al., 2020, p.30).

Esta investigación se aborda a través de una metodología cuantitativa aplicando encuesta adaptada de la teoría UTAUT2 e ítems agregados específicamente para

atender el objetivo de la investigación; asimismo, está fundamentada bajo un amplio marco normativo local, nacional e internacional, que explora la identificación de factores que inhiben o impulsan el uso del canal digital para evaluar si esta herramienta contribuye a la transparencia e integridad en las organizaciones; considerando que la Ley General de Responsabilidades Administrativas vinculada a particulares establece que las denuncias pueden ser de manera electrónica.

Marco de referencia

De acuerdo con Bueno (2022), la extensión y complejidad creciente de las organizaciones públicas y privadas exige que se obtenga información directa e inmediata sobre su funcionamiento; una de las vías hábiles para su obtención es la denuncia. El mismo autor continúa aportando que:

La denuncia actúa a modo de alarma ante un indicio racional de que se está preparando o cometiendo algún tipo de irregularidad que en ocasiones, pueden anunciar un comportamiento aislado que merece ser suprimido, en otras, evidencian síntomas de una auténtica «patología» o colapso institucional que los mecanismos formales y periódicos de auditoría no han conseguido detectar, a veces simplemente provocados por la inercia administrativa, por seguir el precedente o porque, como suele esgrimirse en la práctica administrativa «siempre se ha hecho así y nunca se había tenido problema» (p.215).

México ha avanzado en la gobernanza de esta temática. Al respecto, fue publicado en el Diario Oficial de la Federación del 19 de octubre de 2020 el acuerdo para el protocolo de protección para personas alertadoras de la corrupción, apartado cuarto para la aplicación de las medidas de protección a que hace referencia el protocolo de la Secretaría de la Función Pública por conducto de la Coordinación General de Ciudadanización y Defensa de Víctimas de la Corrupción. La Dirección General de Denuncias e Investigaciones, los órganos internos de control, las unidades de responsabilidades en las empresas productivas del Estado deberán realizar las gestiones de manera oportuna y sin dilación, a fin de evitar poner en riesgo al alertador.

Asimismo, la Ley General de Responsabilidades Administrativas establece la obligación para los servidores públicos de “Denunciar los actos u omisiones que en ejercicio de sus funciones llegare a advertir, que puedan constituir faltas administrativas” (fracción II de su artículo 49); es de relevancia enfatizar que esta ley aplica no solo a servidores públicos, sino también a particulares.

Aún se mantiene como iniciativa con proyecto de decreto expedir la Ley Federal para Protección de los Denunciantes e Informantes de Actos de Corrupción, por lo pronto, el DOF: 11/06/2020 mediante Acuerdo por el que se establecen los Lineamientos para la Promoción y Operación del Sistema de Ciudadanos Alertadores Internos y Externos de la Corrupción.

Localmente se cuenta con la Ley de Responsabilidades y Sanciones para el Estado de Sonora; el fundamento es la fracción II del artículo 50); considerando contemplar la revisión del artículo 25 de dicha ley en el capítulo de la integridad de las personas morales, entre otros. Aunado a lo anterior, el término ‘denunciante’ debe normalizarse dentro de una compañía, de forma que se asocie con la noción de “levantar la voz” en el interés de la empresa para reportar irregularidades, injusticias y riesgos (OCDE, 2018).

Es a través del artículo 25 de la Ley general de responsabilidades administrativas, donde se establece como requisito y se valorará si cuentan las organizaciones con una política de integridad; así como los siete elementos que se deben contener: manual de organización, código de conducta, sistemas de control, vigilancia y auditoría, denuncia y de capacitación en materia de integridad, políticas de recursos humanos tendientes a mitigar riesgos que afecten a la institución y mecanismos de transparencia y publicidad.

El canal digital de denuncia y su gobernanza

Bajo el contexto anterior, analizar la herramienta tecnológica de canales de denuncia en el ámbito público-privado y la figura del informante o whistleblowing traen consigo implicaciones no solo normativas hacia la protección de los informantes, sino también de escasa cultura de la denuncia y de fuertes requerimientos de tecnología e informática de blindaje al usuario potencial para que estas herramientas realmente contribuyan como barrera contra la corrupción en cualquier ámbito.

Por esto, con el objetivo de mejorar la integridad corporativa en México, en 2019, el Programa para las Naciones Unidas para el Desarrollo (PNUD) México emprendió la implementación del proyecto “Fortalecimiento de las capacidades de las mipymes para identificar y combatir riesgos de corrupción en México” para apoyar los esfuerzos del sector privado y fortalecer el cumplimiento de las normativas vigentes en materia de responsabilidades administrativas, particularmente robustecer sus prácticas de ética e integridad por medio de herramientas que faciliten la identificación, el análisis y la gestión de riesgos de corrupción en sus estrategias de negocios.

De lo anterior, se generó la “Guía para establecer el canal de denuncias” como propuesta de procedimientos que faciliten y promuevan las denuncias anónimas brindando seguridad y evitando represalias, así como otras prácticas en detrimento de las libertades y derechos fundamentales de las personas.

Dicha herramienta se propone como un mecanismo de utilidad práctica para identificar y recolectar información sobre posibles actos de corrupción que permitan mitigar estos riesgos y atender malas prácticas que socaven el valor de las mipyme. La Ley Antisoborno del Reino Unido en sus principios 2 y 3 fueron el hilo conductor en el desarrollo del proceso e instrumento.

Por su parte, la “Guía para el otorgamiento de medidas de protección a denunciantes y alertadores de corrupción en materia administrativa para funcionarios de la administración pública” (2024) clarifica procesos y procedimientos que promueven una aplicación efectiva y coherente del sistema de protección a alertadores. En su interior señala que: “Es fundamental asegurar que los canales disponibles para las alertas y denuncias sean accesibles, confiables y garanticen la confidencialidad y/o anonimato” (p.5). Es en dicho documento que se aborda esta herramienta digital como “Plataforma tecnológica de alerta, definida como la herramienta tecnológica dispuesta por la Secretaría para garantizar el anonimato en la presentación de alertas” (p.12).

A su vez y en respuesta a la regulación o de forma voluntaria de introducir o mejorar políticas y procesos internos de denuncia, las organizaciones están considerando el establecimiento de la norma ISO 37002: Sistemas de gestión de la denuncia de irregularidades, la cual se basa en principios de confianza, imparcialidad y protección en los siguientes cuatro pasos: a) recepción de las denuncias de irregularidades, b) evaluación de las denuncias de irregularidades, c) tratamiento de las denuncias de irregularidades, d) conclusión de los casos de denuncia de irregularidades. Las directrices de este documento son genéricas y están destinadas a ser aplicables a todas las organizaciones, independientemente del tipo, tamaño, naturaleza de la actividad, ya sea en los sectores público, privado o sin fines de lucro (p.1).

La creación de los canales de denuncia ha sido reconocida por la ONU en la Convención de las Naciones Unidas contra la Corrupción, resaltando que cada Estado parte debe procurar el planteamiento de medidas y sistemas para facilitar la denuncia de todo acto de corrupción a las autoridades competentes (artículo 8.4).

Adicionalmente, la Organización de Estados Americanos (OEA) en la Ley Modelo para Facilitar e Incentivar la Denuncia de Actos de Corrupción y Proteger a sus Denunciantes y Testigos (Ley Modelo de la OEA), determina en su artículo octavo que las autoridades tienen el deber de facilitar a los empleados públicos y particulares el cumplimiento de la obligación de denunciar actos de corrupción.

La transformación digital en este caso, en los órganos fiscalizadores y de auditoría del ámbito estatal requieren innovar los sistemas informáticos que faciliten el registro y seguimiento de los casos y que estos sistemas no solo permitan recibir alertas, quejas o denuncias, sino que deben ser escalables para darles trazabilidad y seguimiento a los diversos casos, ya que es en estos procesos que se implica el especial cuidado de la cadena de custodia.

Entonces, como parte de los requerimientos tecnológicos, se encuentra el recurrir a la ciberseguridad, la cual ayuda a identificar y mitigar vulnerabilidades que ponen en riesgo la identidad de los denunciantes ante el ataque de algún *malware* o intrusiones en el *software* utilizado para resguardar las denuncias y que el canal de denuncia esté

siempre disponible y no sea derribado por un ataque al servicio; por lo que la seguridad cibernética genera confianza en el usuario de esta herramienta tecnológica.

Los canales de denuncia al menos para ser efectiva como herramienta informática, debe cumplir con lo siguiente: estricto diseño bajo normativas legales y vigentes de cada país, seguridad que contemple un software actualizado y sin vulnerabilidades de seguridad, facilidad de uso, flexibilidad adaptable al tipo de organización, independencia al resto de los *softwares*, tener un responsable del sistema y su gestión, independiente y autónoma respecto al resto de departamentos de la organización, trabajar con expertos en seguridad informática, o forenses digitales para asegurar que la investigación sea completa y precisa.

A esta complejidad se suma el proceso de cadena de custodia enfocado a cómputo en la nube, ya que este proceso es fundamental para dar certeza científica y jurídica de que la evidencia ha sido gestionada de una manera adecuada y garantizar la calidad e integridad de la prueba (Vázquez, 2022).

Es entonces que el uso de la cadena de custodia implica una mayor complejidad, debido a quienes se involucran en el proceso y de quienes deberían tener acceso a las evidencias digitales, empezando por los usuarios (whistleblower), auditores y jurídicos a cargo; los administradores técnicos, proveedor de la nube (CSP); es decir, todos tienen acceso a los datos en mayor o menor medida dependiendo de su rol, por lo que se debe considerar evitar que terceros pudieran corromper la evidencia o se reciban ataques externos, lo que hace necesaria la ciberseguridad; y esto propicia que mantener la cadena de custodia sea un reto en la gobernanza de la herramienta digital o canal de denuncia.

Los canales de denuncia, en diversos países ya se han convertido en requerimiento legal. Como ejemplo, la Ley 2/2023 de protección de los informantes, de orden aplicable a todos los poderes públicos y de la ciudadanía española, fue analizada por Puebla (2023), quien resume que esta ley impone a las empresas la obligación de implementar un canal interno de información o denuncia para que, entre otras personas, sus propios trabajadores puedan comunicar delitos o infracciones que conozcan con motivo de su trabajo; asimismo, incorpora una batería de medidas dirigidas a proteger a estas personas trabajadoras informantes o denunciante frente a posibles represalias (p. 32).

Por su parte, Martínez *et. al* (2020), a través del libro *La protección del whistleblower*, expresan que la protección de la identidad y los datos personales de los denunciante son esenciales para que los sistemas de denuncias generen confianza a los usuarios y, por lo tanto, alienten su uso. Puyol y Franco (2023), en su libro titulado *Las evidencias y garantías en las investigaciones en el canal de denuncias* expresan que “La existencia de una cultura de silencio o del miedo en una organización puede obstaculizar

significativamente las investigaciones del canal de denuncias, desalentar a empleados a denunciar irregularidades; por lo que es necesario implementar soluciones (p.50).

En seguimiento a este tema derivan de la encuesta contra la corrupción en el sector privado (2022), cuyos resultados expresan que en las “razones para no denunciar” (al preguntar a los empresarios que experimentaron algún acto de corrupción) predominó la consideración de que hacerlo no sirve para nada. La segunda respuesta más común (23%), señaló miedo a posibles represalias. Asimismo, el 75% declaró no haber reportado o denunciado el acto de corrupción ante ninguna autoridad. Sólo 19% denunció.

En este contexto, en el ámbito federal, la Secretaría de la Función Pública a partir del año 2019, implementó la encuesta sobre la cultura de la denuncia, con la finalidad de conocer la percepción de la ciudadanía y de las personas servidoras públicas respecto de los mecanismos de denuncia de faltas administrativas en la administración pública federal (2022). Un porcentaje significativo de estos encuestados señaló que conocen la existencia de un mecanismo para realizar denuncias por faltas administrativas atribuibles a personas servidoras públicas (68%) y que sigue existiendo apatía o desconfianza a la hora de realizar este tipo de denuncias.

Asimismo, se les preguntó cuál sería la razón por la que no denunciarían; los encuestados contestaron, principalmente, que porque lo consideran inútil, por miedo y desconocimiento, lo que da muestra de que este tema debe analizarse desde enfoques multidisciplinarios.

Por lo anterior expuesto, el problema general que se percibe para detonar esta investigación, en el ámbito estatal es qué factores inhiben o impulsan a utilizar la herramienta digital para informar algún acto indebido o de corrupción.

Para la evaluación de la herramienta tecnológica, en este trabajo se consideró la teoría unificada extendida de aceptación y uso de la tecnología (UTAUT2) de Venkatesh *et al* (2012), a la cual se le cita en relación a uso extensivo en sistemas de información en investigaciones sobre la adopción y difusión de tecnología de exploración, cuyos investigadores abordan esta línea en búsqueda de comprender factores diversos que influyen en la aceptación y el uso individual de la tecnología de la información (TI) emergente.

Hipótesis

La propuesta de investigación se basa en el supuesto de que los controles internos destinados a detectar fraudes no han sido suficientes, por lo que es necesario impulsar procesos de gobernanza y políticas públicas que destaquen a los informantes de irregularidades, ofrecerles protección, blindaje de confidencialidad, anonimato, evitar

represalias e innovar en plataformas tecnológicas o canales de denuncia con el debido blindaje de seguridad; de tal forma que las hipótesis a evaluar son:

H1: El desconocimiento del canal digital de denuncia, el miedo a ser identificado y la percepción de falta de confidencialidad están asociados con la intención de uso, lo que inhibe la disposición de los individuos a utilizarlo.

H2: La seguridad, anonimato, confianza y accesibilidad en el canal digital de denuncia tienen relación positiva y significativa con su aceptación, uso y confianza de los usuarios para reportar irregularidades en las organizaciones, lo cual positivamente en la transparencia e integridad organizacional.

Metodología

Se utiliza el enfoque de metodología cuantitativa, con diseño explicativo, correlacional, no experimental y transeccional. El diseño del cuestionario contempla la experiencia del uso de los canales de denuncia disponibles de los ámbitos público federal y estatal, además de observar canales éticos de algunas organizaciones privadas, antes de que los encuestados contesten el instrumento.

Las dimensiones que se adaptaron de la teoría UATUT2 para evaluar elementos que influyen en la intención de usar el canal digital fueron: expectativa de desempeño [eficacia percibida de los canales éticos/de denuncia]; expectativa de esfuerzo [facilidad de uso de los canales]; condiciones facilitadoras [accesibilidad y apoyo para el uso de los canales]; motivación para usar los canales (motivación ética); hábitos en el uso del canal; anonimato y confidencialidad; ciberseguridad.

El cuestionario desagrega preguntas con escala Likert a 5 puntos. Las estadísticas descriptivas e inferenciales se realizaron en SPSS 25.0.

Población

Los participantes que contestaron la encuesta fueron grupos heterogéneos: servidores públicos del ámbito estatal, personas que trabajan en sector privado, comunidad universitaria y sociedad en general de la comunidad de Hermosillo, Sonora.

Resultados

Los datos recabados de la aplicación del cuestionario se procesaron para realizar las posteriores pruebas estadísticas. Primeramente, se midieron los constructos del instrumento, con los que se generó el siguiente resultado.

Estadísticas de fiabilidad		
Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
0.831	0.838	19

El instrumento utilizado para medir el constructo tiene buena consistencia interna (alfa de Cronbach de 0,838), con lo que se comprueba que los ítems son adecuados y representan un conjunto homogéneo que mide el mismo fenómeno. Valores entre 0.80 y 0.90 se clasifican como buena confiabilidad (George & Mallery, 2016).

Las pruebas de normalidad se procesaron a través del método de Kolmogorov Smirnov para analizar la distribución normal. Los datos obtenidos indican que son menores a dicho nivel de significancia (sig.=0), por lo tanto, se rechaza la hipótesis de normalidad, pero se confirma la robustez del resultado en muestras mayores (n=290), a través de la corrección de Lilliefors. Los estadísticos de los ítems van de 0.155 a 0.473; situación que permitirá continuar con análisis estadísticos posteriores, contemplando emplear métodos no paramétricos o realizar transformaciones en los datos si se busca cumplir con la suposición de normalidad.

Pruebas de normalidad			
	Kolmogorov-Smirnov ^a		
	Estadístico	gl	Sig.
ítems	0.155 a 0.473	290	0.000
a. Corrección de significación de Lilliefors			

En cuanto a la correlación de Spearman, se examina la relación entre dos variables, siendo la contrapartida no paramétrica de la correlación de Pearson. En este caso, una valoración de 0.601** indica una relación positiva, de moderada a fuerte, entre las percepciones de accesibilidad y utilidad del sistema digital (EFA_1) y la contribución de estos canales a la transparencia, justicia e integridad (DES_3).

Correlación de Spearman de EFA_1 y DES_3

		DES_3 Usar Canal de Denuncia Digital incrementa transparencia, justicia e integridad	
Rho de Spearman	EFA_1 Tecnología digital permite fácil acceso al CD, desde cualquier dispositivo, momento, lugar utilidad y eficacia	Coeficiente de correlación	.601**
		Sig. (bilateral)	0.000
		N	290

La fuerza de la relación, según los criterios de Dancey y Reidy (2007), con un coeficiente en el rango $0.50 \leq r_s < 0.70$ se clasifica como fuerte

Esto significa que, a medida que aumenta la percepción de que la tecnología digital facilita el acceso al canal de denuncia, también los usuarios perciben el sistema como más accesible, útil y también tienen una mayor percepción de ética, transparencia, integridad que se promueve en las organizaciones al disponer de esta herramienta con acceso al público en general.

La siguiente correlación entre las variables EFA_3 (el canal de denuncia facilita la automatización y el seguimiento) y DES_3 (usar el canal de denuncia incrementa la transparencia, justicia e integridad) resulta con ($rs=0.530^{**}$), relación positiva y fuerte, lo que sugiere que a medida que los encuestados perciben que el canal digital facilita la automatización y el seguimiento, se tiende a mejorar las funcionalidades técnicas de esta herramienta tecnológica y puede contribuir a aumentar la percepción de integridad y transparencia en el proceso de las organizaciones.

Correlación Spearman de EFA_3 y DES_3

		DES_3 Usar Canal de Denuncia Digital incrementa transparencia, justicia e integridad	
Rho de Spearman	EFA_3 El Canal de Denuncia digital facilitará automatización recepción y seguimiento, agilizará, eficientará la gestión	Coefficiente de correlación	.530**
		Sig. (bilateral)	0.000
		N	290

Por su parte, la correlación entre DES_2: reportar a través del canal de denuncia permite acciones correctivas rápidas y DES_3: usar el canal de denuncia incrementa transparencia, justicia e integridad, resulta con ($rs=0.605^{**}$) lo cual indica correlación positiva y fuerte entre ambas variables, debiéndosele considerar en estrategias para priorizar la eficiencia de seguimiento y respuesta al asunto recibido como un medio para fortalecer la percepción de integridad en la institución.

Correlación de Spearman entre DES_3 y DES_2

		DES_3 Usar Canal de Denuncia Digital incrementa transparencia, justicia e integridad	
Rho de Spearman	DES_2 Reportar a través de Canal de Denuncia permite acciones correctivas rápidas	Coefficiente de correlación	.605**
		Sig. (bilateral)	0.000
		N	290

Del análisis a las variables nominales donde se preguntaron las razones principales por las que las personas deciden no realizar una denuncia o queja, se obtuvieron los siguientes resultados según su frecuencia y relevancia: falta de información (38.6%), miedo a la falta de confidencialidad y que la tecnología los detecte (37.9%) fueron las principales barreras para denunciar (76.5%).

Esto apunta a la necesidad de mejorar la difusión de información sobre la existencia y disposición de la herramienta digital, con el debido blindaje de ciberseguridad que

debiera percibir el usuario. Entre el resto de las razones por las que las personas que contestan decidieron no realizar alguna denuncia o queja, se percibe que las irregularidades son comunes (10.7%); así como la falta de seguimiento (6.9%), cuyas respuestas expresan desconfianza a los procesos y efectividad del sistema de denuncia.

Por último, aunque en menor porcentaje, una cultura de resignación y apatía es visible en los datos, ya que los encuestados tienden a no denunciar si no son directamente afectados (4.1%); asimismo, la desconfianza institucional y temor a represalias (1.7%) sigue siendo una barrera importante que debe ser abordada con políticas claras de protección al denunciante; sin embargo, en esta población encuestada no resultó determinante el temor a represalias.

Los hallazgos anteriores son clave para diseñar estrategias de mejora en los sistemas de denuncia, con un enfoque en transparencia, accesibilidad y confianza. A continuación, se concentran los resultados aquí descritos.

Tabla 1. Razones para no reportar, denunciar o queja y sector laboral

MEIS_3 Razones para NO reportar denuncia o queja	Sector laboral										Total
	1	2	3	4	5	6	7	8	9	10	
No sé cómo, donde, ni ante quién hacerlo	33	3	5	2	1	2	24	19	15	8	112
Tengo miedo de que la tecnología para reportar, me detecte que fui yo	12	0	3	1	0	0	13	5	9	6	49
Tengo miedo de que 'otros' comuniquen lo que estoy reportando (falta de confidencialidad)	15	1	2	1	0	1	15	12	10	4	61
La falta administrativa o irregularidad cometida es muy común.	8	1	2	0	0	1	7	7	3	2	31
No le dan seguimiento, no me informan seguimiento	3	0	2	0	1	0	4	4	2	4	20
La falta administrativa o irregularidad no me representa una afectación directa.	1	0	0	0	0	0	3	2	0	0	6
Tengo miedo a correr algún riesgo y/o represalia	0	0	0	0	0	0	2	0	1	0	3
Creo que es inútil, porque nada cambia	0	0	0	0	0	0	1	0	1	0	2
No tengo tiempo	1	0	0	0	0	0	0	0	0	0	1
Simplemente NO haría nada	2	0	0	0	0	0	1	0	0	0	3
Otra	1	0	0	0	0	0	0	1	0	0	2
Total	76	5	14	4	2	4	70	50	41	24	290

1)No aplica / No estoy trabajando, 2)Sector privado / Empresas: Empresa comercial, 3)Sector privado / Empresas: Empresa de servicios, 4)Sector gobierno: Auditoría/Fiscalización, 5)Sector gobierno: Educación, 6)Sector gobierno: Salud, 7)Sector gobierno: Servicios, 8)Sector gobierno: Obra pública, 9)Sector gobierno: Seguridad, 10)Soy estudiante

Los resultados del chi cuadrado de Pearson cuyo valor obtenido de 46.322 y $p=1$ indica que no existe estadísticamente asociación significativa entre las variables (razones

para no reportar y el sector laboral), por lo que los sectores laborales de quienes contestaron no parecen influir significativamente en la decisión.

Pruebas de chi-cuadrado			
	Valor	df	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	46.322 ^a	9	1.000
Razón de verosimilitud	49.691	9	1.000
Asociación lineal por lineal	.071	1	.789
N de casos válidos	290		
a. 91 casillas (82.7%) han esperado un recuento menor que 5. El recuento mínimo esperado es .01.			

El 49.3% de los que contestaron fueron mujeres, el 50% hombres y un 7%, género no binario.

Por otra parte, el siguiente análisis explora qué acciones tomarían las personas ante una irregularidad y cómo prefieren reportarla según distintos medios disponibles de denuncia, concentrándose resultados en la tabla 2 (siguiente página).

Pruebas de chi-cuadrado			
	Valor	df	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	62.21	70	.735
Razón de verosimilitud	48.35	70	.977
Asociación lineal por lineal	.003	1	.956
N de casos válidos	290		
a. 79 casillas (89.8%) han esperado un recuento menor que 5. El recuento mínimo esperado es .01.			

El canal digital ético o sitio web es el medio más utilizado, con 205 casos (70.7%), reconocido como preferencia principal. La alternativa secundaria tiende a ser el buzón de quejas y, aunque menos utilizado que el canal digital, el buzón se asocia con acciones iniciales como buscar información o informar al superior. Es probable que sea percibido como una opción más tradicional, pero es cierto que la mayoría busca información antes de actuar. Se percibe que hay dudas o necesidad de orientación antes de denunciar.

Con baja selección de otros medios para reportar resultaron los tradicionales como reportes escritos, correos electrónicos personales o visitas a oficinas físicas de

Tabla 2. Medios para realizar denuncia y acciones a realizar

	MEIS_2 Acciones al conocer alguna irregularidad						Total
	Buscar información u orientación sobre qué hacer.	Informar a mi superior jerárquico	Alertar, denunciar, reportar en algún medio tecnológico o plataforma permanente anónimo con seguimiento	Acudir a la Contraloría Interna u oficina que corresponde	Enviar correo a la Contraloría Interna	Depositar algún reporte en el Buzón	
MEIS_4 Medio para realizar reporte de irregularidad, queja, denuncia, alerta, aviso preventivo, trato perjudicial, daño ambiental							
-Canal Digital Ético, de Denuncias o sitio web	157	19	23	4	0	0	205
-Buzón de quejas	26	10	4	0	0	1	42
-De manera verbal	11	1	1	0	0	0	14
-Por oficio o escrito	5	0	0	0	0	0	5
-Por correo electrónico personal	2	2	0	0	0	1	5
-Por correo electrónico a la Contraloría Interna	6	0	0	1	1	0	8
-Oficina de la Contraloría Interna	1	1	1	0	0	0	3
-Oficina que corresponde	5	0	2	0	0	1	8
Total	213	33	31	5	1	3	290

contraloría interna; quizás por posible percepción de informalidad o falta de seguimiento asociado a estos medios de reportar o denunciar; habría que fomentar el uso de estos para alertar y propiciar que los usuarios confíen más en estas opciones disponibles.

En cuanto a las acciones que tomarían las personas ante el conocimiento de alguna irregularidad, predomina el de primeramente consultar. En la mayoría de los casos, las personas prefieren “buscar información” antes de actuar, situación que refleja necesidad de orientación clara sobre los procesos de denuncia. El resto de las acciones resultaron ser menos comunes o limitadas, como alertar, denunciar o acudir a la contraloría interna, lo que sugiere que los usuarios podrían percibir obstáculos o carecer de confianza en estos métodos.

En todos los medios, la acción relacionada más frecuente es “buscar información u orientación sobre qué hacer”. Esto refleja una necesidad de mayor claridad, capacitación o comunicación sobre cómo proceder con el reporte; es decir, mejorar de manera integral la gobernanza del proceso. Son interesantes los datos obtenidos, ya que solo cuatro personas del total encuestadas (es decir, el 1.4%) señaló que no haría nada en caso de conocer alguna irregularidad, lo que demuestra que la mayoría tiene disposición a reportar si se les brinda un medio o canal confiable.

Por otra parte, se procesaron los datos para determinar el análisis factorial donde la prueba de KMO y Bartlett se utilizó para determinar la adecuación de los datos. Se concluye que es excelente ($KMO=0.90$). Según Kaiser (1974), valores cercanos a 1 indican una excelente adecuación de los datos para el análisis factorial. Asimismo, el resultado es estadísticamente significativo ($p<0.05$), lo que confirma suficiente relación entre las variables para realizar un análisis factorial.

Prueba de KMO y Bartlett		
Medida Kaiser-Meyer-Olkin de adecuación de muestreo		.900
Prueba de esfericidad de Bartlett	Aprox. Chi-cuadrado	1808.30
		4
	gl	136
	Sig.	.000

Por último, se realizó la regresión lineal, cuyo resumen se concentra a continuación en la tabla "Resumen del modelo".

Los resultados anteriores explican el 53.8% de la varianza en la percepción de que el canal de denuncia incrementa transparencia, justicia e integridad, incluyendo en el modelo diez predictores claves, que en conjunto tienen un efecto positivo y significativo en la variable dependiente.

Resumen del modelo ^e					
Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación	Durbin-Watson
1	.621 ^a	0.385	0.383	0.972	
2	.711 ^b	0.506	0.503	0.873	
3	.716 ^c	0.513	0.508	0.869	
4	.734 ^d	0.538	0.522	0.856	1.964
a. Predictores: (Constante), EFA_1					
b. Predictores: (Constante), EFA_1, DES_2 Reportar a través de CD permite acciones correctivas rápidas					
c. Predictores: (Constante), EFA_1, DES_2, EFA_4					
d. Predictores: (Constante), EFA_1, DES_2, EFA_4, EX_2, HD_1, AC_2, SD_2, AC_1, SD_1, AC_3					
e. Variable dependiente: DES_3					

Validez del modelo: el ajuste progresivo de r^2 , junto con la independencia de los residuos (Durbin-Watson=1.964), confirma que el modelo es robusto y adecuado para explicar la relación entre los predictores y la variable dependiente.

Las hipótesis se comprueban con resultados estadísticos, donde la regresión lineal indica que la percepción de transparencia, justicia e integridad es significativamente influenciada por los predictores evaluados, validando el impacto positivo del canal digital en los usuarios. Asimismo, con la validación del modelo UTAUT2 adaptado a las dimensiones de la herramienta digital, se confirma que los factores como expectativa de desempeño, condiciones facilitadoras y motivación ética impulsan el uso del sistema.

Conclusión

Las hipótesis planteadas comprueban, a través de análisis estadísticos, cómo los canales digitales de denuncia, cuando son accesibles, confiables y efectivos, fortalecerían la confianza de los usuarios y contribuirían a los valores organizacionales de transparencia, justicia e integridad. Estos hallazgos resaltan la importancia de diseñar sistemas tecnológicos confiables y promover su uso mediante estrategias de difusión y fortalecimiento de ciberseguridad.

Como se observó en los resultados, los principales factores que inhiben la denuncia fueron el desconocimiento del proceso, el miedo a ser identificado y la falta de confidencialidad, destacando la necesidad de blindar, integrar tecnología y ciberseguridad en la gobernanza del proceso, situación que se comprueba en este trabajo de investigación, donde persiste la desconfianza en la protección al denunciante o *whistleblower*: el que alerta, denuncia, avisa, delata o señala incumplimiento; por

lo que se requiere robustecer e incentivar el marco normativo para blindar a los denunciantes contra represalias y fomentar la cultura de integridad.

Comparando la percepción en el ámbito federal, el resultado fue contrario en cuanto al desconocimiento del proceso; es decir, un porcentaje significativo señaló que sí conocen la existencia de un mecanismo para realizar denuncias por faltas administrativas atribuibles a personas servidoras públicas. Entre las razones para no denunciar se encuentran, principalmente, que lo consideran inútil por miedo y desconocimiento, lo que demuestra que este tema debe analizarse en distintos contextos.

Limitaciones en este trabajo fueron la visita a pymes factibles de contar con algún canal ético o de denuncia, pero se avanzó en analizar algunos portales web donde disponen de dicha herramienta para el público, considerando que estas entidades enfrentan desafíos para implementar estas herramientas, ya sea por cuestiones presupuestales o por desinterés, pero también porque aún no es obligatoria en México (a nivel legal) su implementación.

Este estudio destaca la importancia de las plataformas tecnológicas de alerta y/o canales de denuncia como herramientas clave en la lucha contra la corrupción, pero subraya que la efectividad en su gobernanza depende de una combinación de factores tecnológicos, culturales, normativos y, sobre todo, reservar la identidad de los denunciantes como factor decisivo para incentivar la participación en el uso del canal digital. Con este trabajo, aunque exploratorio, se logra cumplir con el objetivo planteado mediante identificación de factores impulsores clave que contribuyan a la integridad de las organizaciones públicas y privadas.

**Proyecto de investigación financiado por la Universidad Estatal de Sonora (UES).*

Fuentes de información

- Bueno, J. M. (2022). Oportunidad legal y necesidad democrática de crear una Autoridad Administrativa Independiente de lucha contra la corrupción y protección del denunciante. *Revista de Administración Pública*, 217, 209–240. <https://doi.org/10.18042/cepc/rap.217.07>
- Dancey, C. P., & Reidy, J. (2007). *Statistics without maths for psychology* (5a ed.). Pearson Education. <https://www.pearson.com>
- Diario Oficial de la Federación. (2020, 11 de junio). *Acuerdo por el que se reforma el diverso por el que se establecen los Lineamientos para la Promoción y Operación del Sistema de Ciudadanos Alertadores Internos y Externos de la Corrupción*. https://dof.gob.mx/nota_detalle.php?codigo=5594816&fecha=11/06/2020#gsc.tab=0
- George, D., & Mallery, P. (2016). *IBM SPSS statistics 23 step by step: A simple guide and reference* (14a ed.). Routledge. <https://doi.org/10.4324/9781315545899>
- Kaiser, H. F. (1974). An index of factorial simplicity. *Psychometrika*, 39(1), 31–36. <https://doi.org/10.1007/BF02291575>
- Ley de Responsabilidades y Sanciones para el Estado de Sonora*. (2023). <https://contraloria.sonora.gob.mx/informacion-de-interes/compendio-legislativo-basico-estatal/leyes/8199-ley-de-responsabilidades-y-sanciones-para-el-estado-de-sonora/file.html>
- Ley General de Responsabilidades Administrativas*. (2023). <https://www.diputados.gob.mx/LeyesBiblio/pdf/LGRA.pdf>
- Ley Modelo para Facilitar e Incentivar la Denuncia de Actos de Corrupción y Proteger a sus Denunciantes y Testigos*. Organización de los Estados Americanos. https://www.oas.org/juridico/ley_modelo_proteccion.pdf
- Lilliefors, H. W. (1967). On the Kolmogorov-Smirnov test for normality with mean and variance unknown. *Journal of the American Statistical Association*, 62(318), 399–402. <https://doi.org/10.1080/01621459.1967.10482916>
- Martínez, D., Abril, J., Rodríguez, E., & Reyes, L. (2020). *La protección del whistleblower*. Editorial Tirant Lo Blanch.
- Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2018). *Guidelines on whistleblower protection for companies in Greece*. <http://www.oecd.org/corruption/anti-bribery/OECD-Guidelines-WhistleblowerProtection-Companies-in-Greece-ENG.pdf>
- Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2017). *Estudio de la OCDE sobre integridad en México – Adoptando una postura más firme contra la corrupción*. París: OCDE.
- Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2021). *Estudio de la OCDE sobre integridad en el estado de México: Facilitando una cultura de integridad*. París: OCDE. <https://archivos.juridicas.unam.mx/www/bjv/libros/15/7008/1.pdf>
- Programa de las Naciones Unidas para el Desarrollo (PNUD). (2020). *Herramienta 3:*

- Guía para establecer el canal de denuncias*. <https://www.undp.org/es/mexico/publicaciones/guia-para-establecer-el-canal-de-denuncias>
- Puebla, A. de la. (2023). Ley 2/2023, de protección de los informantes. Problemas aplicativos desde una perspectiva laboral. *LABOS Revista De Derecho Del Trabajo y Protección Social*, 4, 32–49. <https://doi.org/10.20318/labos.2023.7929>
- Regulatoria e Impacto Gubernamental en Empresas (ENCRIGE) 2020*. Última actualización revisada mayo 2022. https://www.inegi.org.mx/contenidos/programas/encrige/2020/doc/encrige2020_presentacion.pdf
- Transparencia Internacional. (2022). *Índice de Percepción de la Corrupción 2022*. <https://www.transparency.org/en/cpi/2022/index/mex>
- Vance Center for International Justice (Cyrus, R.) & Derechos Humanos y Litigio Estratégico Mexicano (DLM). (2024). *Guía para el otorgamiento de medidas de protección a denunciantes y alertadores de corrupción en materia administrativa*. <https://www.vancecenter.org/publication/guia medidas de proteccion/>; <https://dlmex.org/>
- Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Aceptación y uso de los consumidores de tecnología de la información: Ampliación de la teoría unificada de aceptación y uso de la tecnología. *MIS Quarterly*, 36(1), 157–178.