AÑO 4. No. 2
ISSN:2992-7978

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN EN NORTEAMÉRICA: UN ANÁLISIS COMPARATIVO DE LA CREACIÓN Y GESTIÓN DE LOS DEPARTAMENTOS DE TI EN EMPRESAS MEDIANAS

INFORMATION TECHNOLOGY MANAGEMENT IN NORTH AMERICA: A COMPARATIVE ANALYSIS OF THE ESTABLISHMENT AND MANAGEMENT OF IT DEPARTMENTS IN MEDIUM-SIZED ENTERPRISES

David Castillo Solis[1]
Rodrigo Cadena Martinez[2]

[1] Doctorando en Informática, Universidad Americana de Europa (UNADE). Correo:themrmind@gmail.com
[2] Profesor - Investigador, Universidad Americana de Europa (UNADE). Correo: rodrigo.cadena@unade.edu.mx

RESUMEN

Los departamentos de TI, tanto en empresas públicas como privadas de tamaño medio, en los diferentes países de Norteamérica, tienen su génesis de formas muy distintas, lo que da lugar a modelos de gestión diferentes y, por ende, a formas de desarrollo que contrastan notablemente entre sí. El objetivo de este estudio es explicar el fenómeno de las diferencias actuales entre los departamentos de TI de dichos países para justificar la necesidad de un modelo local de génesis y gestión orientado a empresas medianas, tanto públicas como privadas, a partir de la comparación entre los tres países de Norteamérica en aspectos como el estado de la gobernanza, la situación geopolítica, el nivel de madurez en ciberseguridad y protección de datos, así como el análisis de la cultura organizacional y de las distintas dinámicas de trabajo regionales a partir de un análisis descriptivo cualitativo y documental, tomando solo documentos de 10 años a la fecha, de sitios en internet de los respectivos gobiernos de los países de Norteamérica y de organismos privados.

Palabras clave: CIO; Administración; IT.

ABSTRACT

IT departments in medium-sized public and private companies across North America started in very different ways, leading to different management models and, as a result, development paths that contrast quite a bit.This study aims to explain why these differences exist today among IT departments in the region and to justify the need for a local model of IT origin and management designed for medium-sized public and private organizations. The study compares the three North American countries in terms of governance, geopolitical conditions, cybersecurity and data protection maturity, as well as organizational culture and regional work dynamics, using a qualitative descriptive and documentary analysis based on documents from the past 10 years found on government websites of the North American countries and private institutions.

Keywords: IT; CIO; Administration.

AÑO 4. No. 2
ISSN:2992-7978

INTRODUCCIÓN

Los departamentos de Tecnologías de la Información en Norte América no han evolucionado en un vacío, sino como una respuesta adaptativa a las presiones de la globalización dentro de un entorno regional marcado por profundas contradicciones. Si bien en la última década se han observado avances normativos y presupuestarios significativos, la realidad operativa dista de la homogeneidad observada en el norte del continente americano.

A pesar de los esfuerzos por estandarizar procesos empresariales y mejorar la transparencia, los organismos públicos y privados de empresas medianas enfrentan obstáculos sistémicos. La narrativa predominante sugiere que el área de TI ha transitado de ser un mero soporte técnico a un motor estratégico de competitividad. “Ya no se trata solo de resolver problemas técnicos, sino de facilitar la transformación digital y mejorar la eficiencia operativa” (Lanet Systems 2025). Sin embargo, esta transición en empresas medianas en Norte America se ve obstaculizada por roles laborales difusos y una precariedad institucional que no encuentra paralelo en el rigor contractual del primer mundo, pero parece agudizarse en las empresas medianas. Debido a estas razones, es necesario buscar el origen de estas diferencias, buscar en cada una de las áreas documentadas el nivel de impacto que tiene en la problemática.

El objetivo del presente artículo de investigación documental es en primera instancia, encontrar las razones de estas diferencias contrastando la evolución normativa, social, económica, política y tecnológica en USA, Canadá y México, buscando justificar la hipótesis de la necesidad construir un modelo particular para la zona y tipo de empresa que se estudia.

ESTADO DEL ARTE Y MARCO TEÓRICO

Consideremos la siguiente tabla 1:

Tabla 1
Personal de TI estimado por empresa

Tipo de Empresa	Total Empleados	Ratio Sugerido (TI:Usuarios)	Personal de TI Estimado
Pequeña	11 - 50	1: 18	1 3 personas
Mediana	51 - 250	1: 25	3 10 personas
Grande	251 - 1,000	1: 50 - 75	10 20 personas
Corporativo	> 1,000	1: 100+	20+ personas

Nota. Tabla de elaboración propia basada en datos de BBVA (2025)

Las empresas medianas y grandes, entre 51 y 1000 empleados (BBVA, 2025) tienen una ratio de personal de TI entre 1:25 y 1:50 (NinjaOne 2026). De acuerdo con las mismas fuentes, el de las empresas medianas debería de ser de 1:50, esto es, entre 3 a 20 personas. En las empresas pequeñas y medianas, las necesidades de TI se resuelven usando solo administradores de terceros que solucionan los problemas de la empresa, no tienen personal suficiente para hacerlo localmente. Según (ChannelProNetwork 2025), estas organizaciones "dependen en gran medida de los MSP para que actúen como su departamento de TI subcontratado"

En los grandes corporativos, su tamaño les exige, por naturaleza, especializar al personal de TI. En estas empresas, la "complejidad empresarial" aumenta exponencialmente. (CIO.com 2025) y Lucid Software señalan que la fragmentación de sistemas, la ciberseguridad avanzada y la gobernanza de datos requieren roles que un generalista no puede cubrir. En este nivel, se hace indispensable contar con

especialistas en ciberseguridad (CISSP), arquitectos de la nube y analistas de datos, ya que un error en sistemas críticos puede costar millones.

En las empresas medianas el problema es distinto, no son tan pequeñas como para tercerizar todo ni tan grandes como para permitirse contratar personal altamente especializado.

METODOLOGÍA

Enfoque

La investigación adoptó una metodología estructurada utilizando un enfoque cualitativo, buscando comprender u fenómeno organizacional, como es la génesis de los departamentos de TI en empresas medianas en Norteamérica, sin buscar una generalización estadística, con un alcance descriptivo, buscando detallar de manera minuciosa de los niveles de madurez en ciberseguridad, normativas y protección de datos, perfilando las diferentes realidades operativas de los países estudiados y un diseño de investigación documental fundamentada en la consulta sistémica de sitios gubernamentales y publicaciones de organismos públicos y privados de esa región., que no superen los 10 años de antigüedad.

Población

El estudio se enfoca solo en empresas medianas, de 51 a 250 empleados de acuerdo con la clasificación de BBVA.

RESULTADOS

A continuación, se presenta la tabla 2, que sistematiza los resultados del análisis comparativo documental.

Tabla 2

Análisis comparativo documental

Categoría Temática	Estados Unidos y Canadá (Norte del continente)	México	Implicaciones para la Gestión de TI
1. Estructura organizacional y el dilema empresarial	Las grandes corporaciones cuentan con personal de TI altamente especializado (CISSP, arquitectos de nube, analistas de datos) para hacer frente a una elevada complejidad empresarial.	Las empresas medianas (51 a 1000 empleados) operan en una realidad híbrida: no son tan pequeñas para tercerizar toda su operación (a proveedores MSP), ni poseen presupuesto para contratar especialistas.	Obliga a las gerencias regionales en empresas medianas a operar bajo un modelo de supervivencia y alta exigencia funcional, asumiendo un ratio de personal de 1:25 a 1:50.
2. Gobernanza, marcos regulatorios y ciberseguridad	Poseen marcos unificados y maduros. Canadá es punta de lanza con leyes transversales como PIPEDA y percibe la ciberseguridad como un	Alta incertidumbre institucional. Las recientes reformas de simplificación orgánica (2024-2025) en México disolvieron al INAI, trasladando la vigilancia de	Los departamentos de TI americanos enfrentan un entorno de cumplimiento fragmentado y operan expuestos a riesgos elevados debido a las limitadas

	asunto de seguridad nacional mediante el CCCS.	datos al órgano desconcentrado "Transparencia para el Pueblo".	estrategias de ciberseguridad pública.
3. Dinámicas laborales y gestión del talento humano	Impera el rigor contractual y la alta especificidad. Los roles están estrictamente delimitados, lo que fomenta una especialización profunda del profesional técnico.	Aplicación laxa de la Ley Federal del Trabajo, instrumentalizando la figura del empleado "de confianza" (Art. 9) para ampliar responsabilidades y eludir el pago de horas extras.	Surge el fenómeno del "generalista forzado", donde el profesional asume tareas dispares bajo un rol genérico (ej. "Analista de Sistemas"), lo que impide la profundidad técnica necesaria para la innovación.
4. Adopción tecnológica y marcos de trabajo estándar	La Inteligencia Artificial y la computación en la nube alcanzan niveles de ubicuidad, impulsadas por inversiones sólidas y un entorno económico o fiscal estable.	Aceleración desigual y déficit de inversión en capacitación técnica e infraestructura. Los marcos de gestión estándar importados (ITIL, COBIT, CMMI) resultan insuficientes.	Implementar normativas prescriptivas (ITIL/COBIT) en pymes con roles indefinidos es análogo a "ensamblar un mueble complejo sin tener las piezas prefabricadas", evidenciando la necesidad de un modelo local y regionalizado.

DISCUSIÓN

El contexto político y la economía de la confianza

El entorno político en la región actúa frecuentemente como una barrera para la adopción tecnológica, exacerbada por la volatilidad en la inversión interna y externa. “En muchas situaciones, los desafíos de gobernanza en América Latina son más específicos y dependen de crear una perspectiva sobre realidades sociales y políticas muy desiguales, heterogéneas en cuanto a las capacidades estatales, las diferencias en los mercados y las perspectivas sobre los emprendimientos sociotécnicos” (Filgueira F. 2023).

La tendencia reciente hacia gobiernos de corte populista en diversas latitudes del continente ha generado, en ocasiones, desincentivos para el capital extranjero, resultando en una desaceleración económica natural. El riesgo país inherente a las economías emergentes sigue siendo un factor determinante que contrasta con la estabilidad de los mercados norteamericanos (CEPAL 2022)

Más allá de la macroeconomía, el concepto de confianza es central. entendida como la expectativa de que una institución actuará de manera positiva, la confianza es una métrica crítica de gobernanza (OCDE, 2022). El informe *Panorama de las administraciones públicas: América Latina y el Caribe 2020* revela un deterioro preocupante: la confianza ciudadana en los gobiernos cayó del 38% en 2007 al 34% en 2018.

En este escenario de erosión institucional, la digitalización no es solo una mejora técnica, sino una herramienta de legitimidad. No obstante, la capacidad de los departamentos de TI para liderar esta transformación depende intrínsecamente de la estabilidad del ecosistema político en el que operan.

Marcos regulatorios: Privacidad y protección de Datos

La disparidad legislativa es uno de los puntos de divergencia más notables.

El modelo canadiense:

AÑO 4. No. 2
ISSN:2992-7978

Canadá es punta de lanza en protección de datos en América. Desde 1983 se aprobó la ley de privacidad (Privacy Act), que regula cómo deben manejar la información privada los diferentes departamentos y oficinas del gobierno de ese país.

Destaca que desde 1984, la Oficina del Comisionado de Privacidad menciona que la privacidad (de los datos) no es solo un recurso humano que cuidar, sino un acto de reconocimiento y respeto a la dignidad humana.

En el año 2000, Canadá promulgó la *Personal Information Protection and Electronic Documents Act* (PIPEDA), una legislación federal orientada a regular la protección de la información personal y el uso de documentos electrónicos, sentando las bases del marco canadiense de privacidad de datos en entornos públicos y privados (Government of Canada, 2023).

A partir de 2001, las funciones de la *Office of the Privacy Commissioner of Canada* se extendieron formalmente a la industria privada, estableciéndose un periodo de implementación progresiva entre 2001 y 2004 que permitió a las organizaciones adaptar sus procesos internos a las nuevas obligaciones legales en materia de tratamiento de datos personales (Government of Canada, 2023).

En 2015 se introdujeron modificaciones sustantivas a la legislación de privacidad digital mediante reformas a PIPEDA, entre las que destacan la obligación de mantener registros de todas las brechas de seguridad, la notificación tanto a la Oficina del Comisionado de Privacidad como a los individuos afectados, así como el fortalecimiento de los requisitos de consentimiento informado, el cual exige que las personas comprendan la naturaleza, propósito y consecuencias del uso de sus datos. Asimismo, se incorporaron excepciones específicas en el ámbito laboral para facilitar la gestión de relaciones entre empleadores y empleados, se reforzaron medidas de protección contra el fraude y para menores vulnerables, y se establecieron sanciones económicas de hasta 100,000 dólares canadienses por incumplimiento (Government of Canada, 2023).

Durante 2024 se impulsaron nuevas modificaciones y lineamientos interpretativos a PIPEDA con el objetivo de endurecer los requisitos para la compartición de datos personales y reforzar los principios de responsabilidad organizacional, transparencia y control por parte de los titulares de la información, en respuesta a los desafíos derivados de la digitalización y el intercambio transfronterizo de datos (Government of Canada, 2023).

En conjunto, Canadá presenta un enfoque federal unificado en materia de protección de datos personales, considerado un referente a nivel internacional. La *Personal Information Protection and Electronic Documents Act* (PIPEDA) establece reglas claras, homogéneas y transversales para el sector público y privado, lo que contribuye a simplificar la gestión de datos y fortalecer la confianza digital en la economía canadiense (Government of Canada, 2023).

Estados Unidos y su modelo por estado.

En 1890 se publica de *"The Right to Privacy"* por Warren y Brandeis, sentando las bases legales del derecho a la intimidad.

Warren & Brandeis (1890), que se reconoce como el origen sectario de las leyes en USA, en donde cada esta promulga sus leyes.

Esta es la evolución de las leyes de privacidad en ese país.

1974: Privacy Act. Primera ley general de protección de información personal, aunque limitada únicamente a las agencias federales tras el escándalo de Watergate. (Saldaña, 2011; Sobrino García, 2020)

1996: HIPAA. Establece estándares federales para proteger la información médica sensible (PHI),(Secureframe, 2023; Sobrino García, 2020)

1998: COPPA. Ley de Protección de la Privacidad en Línea para Niños, que exige el consentimiento parental previo a la recopilación de datos de menores de 13 años. (Sobrino García, 2020)

1999: Gramm-Leach-Bliley Act (GLBA). Regula la privacidad de la información recolectada por instituciones financieras. (Sobrino García, 2020)

2001: USA Patriot Act. Aprobada tras el 11-S, permitió un aumento en la vigilancia electrónica y el acceso gubernamental a datos privados, lo que supuso un retroceso en los niveles de privacidad previos. (Saldaña, 2011)

2009: Ley HITECH. Fortaleció las protecciones de HIPAA e introdujo incentivos para el uso de registros electrónicos. (Secureframe, 2023)

2018/2020: CCPA y CPRA (California). California aprueba la legislación de privacidad más ambiciosa del país, otorgando derechos similares al RGPD europeo (acceso, eliminación y opción de no venta) a sus residentes. (Goldman, 2020; Kapitsaki et al., 2025)

2022: ADPPA (Proyecto). La American Data Privacy and Protection Act fue el intento más cercano de una ley federal integral, pero se estancó en el Congreso y no se convirtió en ley. (Termly, 2025)

El caso mexicano y la incertidumbre institucional:

En 2002, en México se promulgó **la** Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental**,** marcando el inicio formal de un marco normativo orientado a garantizar el acceso ciudadano a la información en poder del Estado (Cámara de Diputados, 2022). A diferencia de otros modelos internacionales centrados desde su origen en la privacidad individual, el desarrollo normativo mexicano en materia de datos personales surgió inicialmente como una extensión de la política de transparencia gubernamental, buscando evitar la divulgación no autorizada de información personal contenida en archivos públicos, más que como una regulación integral de la privacidad (INAI, 2023).

Con el objetivo de garantizar este derecho, se creó el Instituto Federal de Acceso a la Información Pública (IFAI)**,** encargado de regular y supervisar el cumplimiento de las disposiciones en materia de acceso a la información y protección de datos personales dentro del ámbito federal (INAI, 2023).

En 2009, una reforma constitucional al artículo 16 reconoció explícitamente la protección de datos personales como un derecho fundamental y autónomo, otorgando a los ciudadanos los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición). De manera complementaria, se reformó el artículo 73 constitucional, facultando al Congreso de la Unión para legislar de forma expresa en materia de protección de datos personales (Diario Oficial de la Federación, 2010).

Posteriormente, en 2010 se promulgó la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)**,** mediante la cual México extendió la regulación del tratamiento de datos personales al sector privado, estableciendo obligaciones específicas para empresas y entidades no gubernamentales (Diario Oficial de la Federación, 2010).

En 2011 se expidió el Reglamento de la LFPDPPP, precisando los principios, procedimientos y medidas de seguridad aplicables al tratamiento de datos personales por parte de particulares, así como los mecanismos de supervisión y sanción correspondientes (Diario Oficial de la Federación, 2010).

En 2014, como resultado de una reforma constitucional en materia de transparencia, el IFAI se transformó en **el** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)**,** adquiriendo carácter constitucional autónomo y competencia a nivel nacional para los sectores público y privado (INAI, 2023).

En 2017 se publicó **la** Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, cuyo objetivo fue estandarizar las reglas aplicables al tratamiento de datos personales en el sector público federal, estatal y municipal, consolidando un marco homogéneo de obligaciones para las autoridades (INAI, 2023).

En 2018, México fortaleció su marco normativo mediante la adopción de estándares internacionales en materia de protección de datos personales y la emisión de lineamientos específicos,

como aquellos relativos a la portabilidad de los datos, alineándose con tendencias regulatorias globales (INAI, 2023).

Durante 2024 se publicó un decreto de reforma constitucional orientado a la simplificación orgánica del Estado, mediante el cual se ordenó la extinción de diversos órganos constitucionales autónomos, incluyendo al INAI, lo que representó un cambio estructural en el modelo institucional de supervisión de la protección de datos personales (INAI, 2023).

En 2025 se formalizó la disolución del INAI y se creó el organismo Transparencia para el Pueblo como órgano desconcentrado, asignándose las funciones de vigilancia y control en materia de datos personales a la Secretaría Anticorrupción y Buen Gobierno, redefiniendo el esquema institucional de protección de datos en México (INAI, 2023).

En conjunto, la evolución del caso mexicano muestra un proceso que inicialmente siguió trayectorias similares a las de Canadá y Europa, comenzando por la regulación de la información en poder de organismos gubernamentales y ampliándose posteriormente al sector privado, aunque con una fuerte impronta de transparencia pública como eje rector de su desarrollo normativo (INAI, 2023).

Ciberseguridad: De la estrategia a la práctica

Al analizar el marco político de la ciberseguridad, la brecha se ensancha. Canadá fomenta una colaboración estrecha entre el sector público y privado a través del Canadian Centre for Cyber Security (CCCS), bajo la premisa de que la seguridad corporativa es seguridad nacional (Canadian Centre for Cyber Security, 2023). Estados Unidos, por su parte, se apoya en agencias como CISA y marcos del NIST que, aunque voluntarios, son adoptados como estándares de facto por la industria (Cybersecurity & Infrastructure Security Agency, 2023; National Institute of Standards and Technology, 2023).

En contraste, aunque México posee una Estrategia Nacional de Ciberseguridad, su implementación enfrenta retos de presupuesto y madurez. La inversión pública es limitada y las prácticas de seguridad en el sector privado son heterogéneas, exponiendo a los departamentos de TI a riesgos elevados (Gobierno de México, 2019).

El factor económico y la inversión en tecnología

A pesar de la desaceleración económica generalizada en Norteamérica, derivada de la proliferación de políticas proteccionistas y fluctuaciones arancelarias, la inversión en TI muestra resiliencia. El informe *IT Market Review 2024-2025* indica que el 64% de las empresas planea aumentar su presupuesto tecnológico. Un hallazgo cualitativo relevante es el cambio en los criterios de compra: la alineación estratégica y la calidad del soporte han desplazado al precio como factor decisivo. Esto sugiere una maduración en la percepción del valor que aporta el área de TI.

En Norteamérica, la dinámica es distinta. Estados Unidos ha sufrido una corrección severa en el capital de riesgo, con una caída del 30% en la financiación de startups en 2023 (Pitchbook, 2023). Esto ha forzado a los departamentos de TI a priorizar la eficiencia operativa sobre la innovación disruptiva ("hacer más con menos"). Canadá ha mitigado este impacto gracias a incentivos fiscales como el programa de *Investigación Científica y Desarrollo Experimental* (SR&ED), permitiendo a sus empresas mantener cierto nivel de innovación mediante la automatización.

Adopción de nuevas tecnologías: La brecha de implementación

La adopción tecnológica sigue patrones divergentes. Mientras que en Norteamérica la computación en la nube y la Inteligencia Artificial (IA) alcanzan niveles de ubicuidad, en Norteamérica el proceso es desigual.

Cloud Computing: El 80% de las empresas latinas se encuentra en fases avanzadas de adopción, impulsando inversiones de infraestructura por parte de gigantes como Amazon y Google en México y Chile (NTT DATA & MIT Technology Review, 2023; Truora, 2024).

Inteligencia Artificial: Existe una alta expectativa laboral, pero una inversión insuficiente en capacitación limita el impacto transformacional de la IA en la región (Filgueira, 2023; Fundación Everis, 2024).

Ciberseguridad: Con un mercado regional de 21,600 millones de USD en 2024, es alarmante que solo tres países (Brasil, Chile y Colombia) cuenten con estrategias nacionales robustas (Koch, 2020).

Dinámicas laborales y contractuales: La realidad del empleado "De confianza":

Quizás el contraste más agudo se encuentra en la gestión del talento humano y la definición de roles. En Estados Unidos y Canadá, la relación laboral se caracteriza por una alta especificidad. Los contratos detallan responsabilidades puntuales; desviarse de ellas implica renegociaciones o compensaciones. Esto fomenta una especialización profunda: un administrador de bases de datos raramente realizará funciones de soporte técnico o programación web (National Conference of State Legislatures, 2022; Government of Canada, 2025).

En México y gran parte de Latinoamérica, la Ley Federal del Trabajo (LFT) ofrece un marco proteccionista en teoría, pero la práctica revela una flexibilidad que a menudo raya en la informalidad funcional. La figura del "trabajador de confianza" (Artículo 9 de la LFT) es frecuentemente utilizada para eludir el pago de horas extras y ampliar indefinidamente las responsabilidades del empleado (Cámara de Diputados, 2022; AbogadoLaboral.mx, 2024; Justia México, 2025).

El fenómeno del generalista forzado. En las empresas latinas, es común que el contrato defina un "rol" genérico (ej. "Analista de Sistemas"), lo que permite a la gerencia asignar tareas dispares —desde programación hasta cableado de redes— bajo el mismo salario. Esta falta de especialización, aunque otorga flexibilidad operativa a corto plazo, impide la profundidad técnica necesaria para la innovación compleja (Infochannel, 2024; International Labour Organization, 2025).

La Insuficiencia de los Marcos de Gestión Estándar. Durante las últimas dos décadas, se ha intentado "importar" la eficiencia mediante herramientas como ITIL, COBIT o CMMI. Si bien son valiosas, estas metodologías presentan una limitación fundamental para el contexto latinoamericano: son marcos prescriptivos de operación, no de creación y por supuesto, no están pensadas para la innovación y renovación de las empresas (Axelos, s. f.; ISACA, s. f.; CMMI Institute, s. f.).

Podemos establecer una analogía: implementar ITIL en una PyME latinoamericana con roles indefinidos es como intentar ensamblar un mueble complejo sin tener las piezas prefabricadas. Estos marcos asumen una estructura organizacional madura, con procesos preexistentes y roles segregados, que rara vez existen en la región. No es lo mismo estandarizar un proceso que ya funciona, que diseñar la interrelación de procesos desde cero en un entorno de incertidumbre (CEDIA, 2023; ISO, s. f.).

CONCLUSIONES

En las empresas medianas, la estructura organizacional esta ligada a una cultura organizacional poco desarrollada debido a que pocas personas tienen que hacer muchas cosas. El departamento de TI tiene una ratio muy bajo de personal, usualmente menor a lo que se recomienda.

Las estrategias de ciberseguridad, en los tres países han evolucionado de maneras muy similares, pero en las empresas medianas no suele haber una estrategia planeada, reaccionando a los cambios de la empresa.

La protección de datos se trata diferente en cada país, debido a un génesis legislativo con un contraste enorme. Gran parte de las grandes diferencias entre la gestión en las empresas de mayor o menor tamaño, y en particular en el nivel de desarrollo económico del país del que se trate, provienen de estas diferencias.

Las dinámicas laborales, aunque en los países desarrollados de Norteamérica parecen proteger mas a los empleados, los de ti incluidos, sufren del mismo problema que en México del empleado de TI con

muchas responsabilidades, poco especializado y con delimitación de funciones difusa debido a la figura del Empleado de Confianza.

Todas estas razones evidencian la necesidad de generar un modelo particular de génesis y g gestión que tenga en cuenta estas deficiencias. Parece que las empresas conocen al nuevo valor de los departamentos de TI, pero este modelo debe buscar consolidar la función de innovación y estratégico de estos departamentos, tanto en su función como en su formación.

REFERENCIAS

AbogadoLaboral.mx. (2024, octubre 16). *Clave sobre los derechos y limitaciones de los trabajadores de confianza en México*. https://www.abogadolaboral.mx/2024/10/16/clave-sobre-los-derechos-y-limitaciones-de-los-trabajadores-de-confianza-en-mexico

Axelos. (s. f.). *ITIL® 4 framework*. https://www.axelos.com/itil-4-framework

Banco Interamericano de Desarrollo. (2021). *Digitalización en América Latina y el Caribe*. https://publications.iadb.org/publications/spanish/document/Digitalizacion-en-America-Latina-y-el-Caribe.pdf

Banco Interamericano de Desarrollo, & Organización para la Cooperación y el Desarrollo Económico. (2020). *Panorama de las administraciones públicas: América Latina y el Caribe 2020*. https://doi.org/10.18235/0002232

BBVA México. (s. f.). *¿Cuál es la clasificación de las empresas por su tamaño?* https://www.bbva.mx/educacion-financiera/empresa/pyme/cuenta-pyme-clasificacion-de-las-empresas-por-tamano.html

Biblioteca del Congreso Nacional de Chile. (2023). *Ley N.º 19.628 sobre protección de la vida privada*. https://www.bcn.cl/leychile/navegar?idNorma=143642

Cámara de Diputados. (2022). *Ley Federal del Trabajo*. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFT.pdf

Canadian Centre for Cyber Security. (2023). *About us*. https://cyber.gc.ca/en/about-us

Canadian Venture Capital and Private Equity Association. (2023). *CVCA market activity report: Q3 2023*. https://www.cvca.ca/research-publications/reports/cvca-market-activity-report-q3-2023

Canada Revenue Agency. (2023). *Scientific research and experimental development (SR&ED) tax incentive program*. https://www.canada.ca/en/revenue-agency/services/scientific-research-experimental-development-sred-tax-incentive-program.html

CEDIA. (2023). *Planeación y gestión estratégica de las tecnologías de la información*. https://cedia.edu.ec/docs/efc/GTI1.pdf

ChannelPro Network. (2025, noviembre 17). *MSP comparison guide: Should I specialize in SMBs or midmarket/enterprise clients?* https://www.channelpronetwork.com/2025/11/17/smb-clients-vs-midmarket-enterprise/

CIO. (2025, septiembre 19). *Key strategies to reduce IT complexity*. https://www.cio.com/article/4058804/reasons-that-increase-it-complexity-and-strategies-to-reduce-it.html

Comisión Económica para América Latina y el Caribe. (2022). *La inversión extranjera directa en América Latina y el Caribe 2022*. https://www.cepal.org/es/publicaciones/48366-la-inversion-extranjera-directa-america-latina-caribe-2022

CMMI Institute. (s. f.). *CMMI version 2.0*. https://cmmiinstitute.com/cmmi-v20

CMS Law. (2025). *Dismissals and termination of employment in Mexico*. https://cms.law/en/int/expert-guides/cms-expert-guide-to-dismissals/mexico

Cybersecurity and Infrastructure Security Agency. (2023). *About CISA*. https://www.cisa.gov/about-cisa

Departamento de Trabajo de los Estados Unidos. (2024, noviembre 8). *Fact sheet No. 17D: Exemption for professional employees*. https://hr.nmsu.edu/documents/Fact_Sheet_17D__Exemption_for_Professional_Employees_Under_the_Fair_Labor_Standards_Act_FLSA___U.S._Department_of_Labor.pdf

Departamento de Trabajo de los Estados Unidos. (s. f.). *Fact sheet No. 17A: Exemption for executive, administrative, professional, and outside sales employees*. https://www.dol.gov/agencies/whd/fact-sheets/17a-overtime

Diario Oficial de la Federación. (2010). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP_270117.pdf

Employment and Social Development Canada. (s. f.). *Excluded employees from hours of work provisions (IPG-049)*. https://www.canada.ca/en/employment-social-development/programs/laws-regulations/labour/interpretations-policies/excluded-employees.html

Filgueira, F. (2023). Desafíos de gobernanza de la inteligencia artificial en América Latina. *Revista del CLAD Reforma y Democracia*, (87). https://doi.org/10.69733/clad.ryd.n87.a3

Fundación Everis. (2024). *Avances y desafíos de la inteligencia artificial en Estados Unidos*. https://fundacioneveris.com/tecnologia/ia-estados-unidos

GeoVictoria. (2025). *Ley Federal del Trabajo: Obligaciones y derechos en México*. https://www.geovictoria.com/es-mx/blog/ley-federal-del-trabajo-obligaciones

Gobierno de México. (s. f.). *Centro Federal de Conciliación y Registro Laboral*. https://www.gob.mx/cfcrl

Goldman, E. (2020). *An introduction to the California Consumer Privacy Act (CCPA)*. Santa Clara University.

Government of Canada. (2023). *Personal Information Protection and Electronic Documents Act*. https://laws-lois.justice.gc.ca/eng/acts/P-8.6/

Government of Canada. (2025, abril 30). *Federal labour standards*. https://www.canada.ca/en/services/jobs/workplace/federal-labour-standards.html

Government of Canada. (2025, junio 25). *Hours of work: Federally regulated workplaces*. https://www.canada.ca/en/services/jobs/workplace/federal-labour-standards/work-hours.html

Infochannel. (2024). *1994–2024: Claves del éxito de cuatro integradores mexicanos*. https://infochannel.info/la-evolucion-en-la-industria-tic/

International Labour Organization. (2025). *Latin America and the Caribbean: Regional overview*. https://www.ilo.org/regions-and-countries/latin-america-and-caribbean

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2023). *¿Quiénes somos?* https://home.inai.org.mx/quienes-somos/

ISACA. (s. f.). *COBIT 2019*.

https://www.isaca.org/resources/cobit

ISO. (s. f.). *ISO/IEC 20000-1:2018*. https://www.iso.org/standard/70636.html

Justia México. (2025). *Ley Federal del Trabajo: Jornada de trabajo (arts. 58–68)*. https://mexico.justia.com/federales/leyes/ley-federal-del-trabajo/titulo-tercero/capitulo-ii/

Justia México. (2025). *Ley Federal del Trabajo: Trabajadores de confianza (arts. 182–186)*. https://mexico.justia.com/federales/leyes/ley-federal-del-trabajo/titulo-sexto/capitulo-ii/

Kapitsaki, G. M., Papoutsoglou, M., Treude, C., & Theophilou, I. (2025). Analyzing developer discussions on EU and US privacy legislation compliance in GitHub repositories. *arXiv*. https://arxiv.org/abs/2503.03988

KeepCoding. (2024). *Evolución de las TIC: Un recorrido histórico*. https://keepcoding.io/blog/evolucion-de-las-tic-hasta-la-actualidad/

Koch, I. (2020). *Avances en la gestión de riesgos en América Latina*. Pontificia Universidad Católica de Valparaíso.

Krolls. (2023). *Tecnología en México: Conoce la situación actual*. https://krolls.com.mx/tecnologia-en-mexico-conoce-la-situacion-actual/

Lanet Systems. (2025, abril 19). *La importancia del soporte TI en la transformación digital empresarial*. https://www.lanet.mx/soporte-ti/

Layoffs.fyi. (2023). *Tech layoffs*. https://layoffs.fyi/

Lucid Software. (s. f.). *The real impact of business complexity* https://lucid.co/blog/business-complexity

McMillan LLP. (2024). *Employment law in Canada: Federally regulated employers*. https://mcmillan.ca/wp-content/uploads/2024/04/Employment-Law-Canada-Federally-Regulated-Employers-Brochure.pdf

Milenio. (2023). *Sector público-privado de Canadá invierte en tecnología*. https://www.milenio.com/negocios/sector-publico-privado-canada-invierte-tecnologia-economia

Monkhouse Law. (2025, junio 2). *The manager exception to overtime*. https://www.monkhouselaw.com/the-manager-exception-to-overtime-toronto-employment-lawyer/

Mordor Intelligence. (2024). *Canada cybersecurity market report*. https://www.mordorintelligence.com/es/industry-reports/canada-cybersecurity-market

National Conference of State Legislatures. (2022). *At-will employment: Overview*. https://www.ncsl.org/labor-and-employment/at-will-employment-overview

National Institute of Standards and Technology. (2023). *Cybersecurity framework*. https://www.nist.gov/cybersecurity

National Labor Relations Board. (s. f.). *National Labor Relations Act*. https://www.nlrb.gov/guidance/key-reference-materials/national-labor-relations-act

NinjaOne. (2026, febrero 4). *IT staffing ratio guide*. https://www.ninjaone.com/blog/it-staffing-ratio/

NTT DATA & MIT Technology Review. (2023). *Cloud en América Latina 2023*. https://us.nttdata.com/en/engage/cloud-in-latin-america-2023

PitchBook. (2023). *PitchBook–NVCA venture monitor: Q3 2023*. https://pitchbook.com/news/reports/q3-2023-pitchbook-nvca-venture-monitor

Procuraduría Federal de la Defensa del Trabajo. (s. f.). *Horas extra u horas de trabajo extraordinario*. https://www.profedet.gob.mx/micrositio/index.php/horas-extras-u-horas-de-trabajo-extraordinario

Radio Canadá Internacional. (2024). *La inteligencia artificial en todas sus formas en Canadá*. https://ici.radio-canada.ca/rci/es/noticia/2097925/serie-la-inteligencia-artificial-en-todas-sus-formas-en-canada

Saldaña, M. N. (2011). El derecho a la privacidad en los Estados Unidos. *Revista de Derecho de la UNED*, (9), 279–311.

Secretaría del Trabajo y Previsión Social. (2021–2024). *Legitimación y revisión de contratos colectivos de trabajo*. https://reformalaboral.stps.gob.mx/sitio/rl/doc/legitimacion-de-contratos-colectivos.pdf

Secureframe. (2023). *Historia de HIPAA: Cómo el estándar ha evolucionado desde 1996*. https://secureframe.com/es/blog/history-of-hipaa

Sobrino García, I. (2020). Protección de datos y privacidad. *Revista de Derecho de la UNED*, (25), 687–713.

TechTarget. (s. f.). *What is DevOps?* https://www.techtarget.com/whatis/definition/DevOps

Termly. (2025). *American Data Privacy Protection Act (ADPPA): A first look*. https://termly.io/resources/articles/american-data-privacy-protection-act/

Truora. (2024). *¿Cuál es el impacto de la transformación digital en América Latina?* https://blog.truora.com/es/transformacion-digital-en-america-latina

U.S. Bureau of Labor Statistics. (2025, enero 28). *Union members—2024*. https://www.bls.gov/news.release/pdf/union2.pdf

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220.