

CAPÍTULO

05

**TRANSFORMACIÓN DIGITAL:
TRABAJO REMOTO,
COMPETENCIAS DIGITALES,
CIBERSEGURIDAD Y ÉTICA**

En el capítulo anterior se presentaron los fundamentos teóricos que articulan la transformación digital con el clima y la cultura organizacional; además, se analizaron sus principales dimensiones: modelos de trabajo en la postpandemia, sistemas de información para la gestión del talento humano, analítica organizacional basada en datos, competencias digitales, y los desafíos en materia de ciberseguridad y ética. El presente capítulo profundiza en cada una de estas, incorporando evidencia empírica reciente, marcos de referencia internacionales y datos estadísticos que permiten comprender la magnitud y complejidad de estos fenómenos en el entorno organizacional contemporáneo.

La intención de este capítulo no es reiterar lo ya expuesto, sino ampliar el análisis desde perspectivas complementarias que enriquecen la comprensión del fenómeno. Así, se abordan las tensiones emergentes entre la flexibilidad del trabajo remoto y la cohesión organizacional; los dilemas éticos derivados del uso de inteligencia artificial en la gestión del talento; la necesidad de marcos sistemáticos para el desarrollo de competencias digitales; y las implicaciones estratégicas de la ciberseguridad como dimensión cultural de las organizaciones. Todo ello se inscribe en el marco de las instituciones de educación superior, donde estas dinámicas adquieren un matiz particular dada la doble misión de formar profesionales competentes y gestionar eficientemente sus propios procesos internos (Trenerry et al., 2021; Koska et al., 2025).

5.1 Transformación digital

El análisis de la transformación digital que se presenta en este capítulo no es una revisión bibliográfica desvinculada del caso estudiado. Se ancla, por el contrario, en evidencia institucional específica de la Universidad del Valle y en los hallazgos empíricos de las Líneas 1 y 2 de esta investigación. Los datos cuantitativos del cuestionario de clima organizacional muestran que la dimensión Recursos Institucionales obtuvo uno de los puntajes más bajos del perfil (media = 4.2/7), y las entrevistas semiestructuradas revelan que las principales fuentes de tensión reportadas por el personal administrativo durante la pandemia estuvieron asociadas a desigualdades en el acceso tecnológico, a la implementación apresurada del teletrabajo y a la ausencia de acompañamiento en el desarrollo de competencias digitales.

A su vez, los perfiles formativos identificados en el Capítulo IV (Tabla 10) muestran que docentes con orientación crítico-reflexiva tienden a adoptar las herramientas digitales de manera más selectiva y contextualizada; caso contrario aquellos alineados con el paradigma gerencial-corporativo, quienes las incorporan con mayor énfasis en la eficiencia y la productividad medible. La revisión de literatura internacional que sigue en este capítulo se lee, por tanto, en diálogo permanente con esta realidad institucional concreta.

Cinco años después del inicio de la pandemia por COVID-19, el trabajo remoto e híbrido ha dejado de ser una solución de emergencia para convertirse en un componente estructural de la organización del trabajo. Según datos de WFH Research, más de uno de cada cuatro días laborales pagados en Estados Unidos se realizaron desde el hogar durante 2024, una proporción que contrasta drásticamente con la relación de uno de cada catorce que existía antes de la pandemia (Barrero et al., 2023). Esta transformación no ha sido homogénea: mientras que los roles basados en conocimiento muestran tasas elevadas de teletrabajo, los trabajadores de primera línea y los sectores industriales continúan requiriendo presencialidad.

La evidencia reciente indica que el trabajo híbrido continúa siendo la modalidad predominante entre los empleos con potencial de trabajo remoto. Gallup (2025) informa que, en Estados Unidos, el 52 % de los trabajadores con empleos compatibles con esta modalidad laboran bajo esquemas híbridos, el 26 % de forma totalmente remota y el 22 % exclusivamente de manera presencial. Asimismo, el informe *State of Hybrid Work 2025* de Owl Labs (2025) señala que las organizaciones mantienen una tendencia hacia modelos flexibles, aunque persisten tensiones derivadas de las políticas de retorno a la oficina y de las expectativas de flexibilidad de los trabajadores.

Uno de los debates centrales en torno al trabajo remoto e híbrido ha sido su impacto sobre la productividad. Una revisión sistemática de literatura publicada en *SN Business & Economics*, que analizó estudios realizados entre 2020 y 2024 en pequeñas y medianas empresas de diversos contextos globales, concluyó que los modelos flexibles de trabajo generalmente mejoran la productividad al incrementar la satisfacción de los empleados, reducir tiempos de desplazamiento y favorecer el equilibrio entre la vida laboral y personal. El modelo híbrido resultó ser el más efectivo, al combinar la autonomía del trabajo remoto con las ventajas colaborativas de la interacción presencial (Maity & Lee, 2025).

No obstante, estos beneficios no están exentos de riesgos psicosociales. La investigación también documenta que la flexibilidad puede generar aislamiento social, difuminación de los límites entre el trabajo y la vida personal, y fatiga digital (Aprilina & Martdianty, 2023). En este sentido, Lathabhan y Mehendale (2025) demostraron que prácticas como el *mindfulness* organizacional facilitan la transición hacia modelos híbridos al reducir los niveles de estrés asociados con la adaptación. Este hallazgo es relevante para las instituciones de educación superior, donde la sobrecarga tecnológica y la multiplicidad de roles docente, investigación, extensión, gestión administrativa hacen a sus miembros particularmente vulnerables a la fatiga digital.

Los datos globales sobre la consolidación del trabajo híbrido adquieren mayor relevancia analítica cuando se examinan sus efectos diferenciados sobre las distintas dimensiones del clima organizacional. No todas las facetas del clima responden de la misma manera a la flexibilización de los modelos de trabajo: algunas se fortalecen, como la autonomía, la productividad en tareas individuales, la inclusión geográfica; otras, por el contrario, se ven presionadas, como la cohesión informal, la comunicación no verbal, la equidad en el acceso a oportunidades de desarrollo.

La Tabla 12 sistematiza dichos efectos contrastando, para cada dimensión clave, los beneficios documentados en la literatura y los desafíos emergentes que deben ser gestionados activamente. Esta sistematización es relevante para la Universidad del Valle en la medida en que los hallazgos del cuestionario de clima, especialmente los relativos a Trabajo en Equipo y Recursos Institucionales, se leen con mayor profundidad a la luz de estos efectos.

Tabla 12
Efectos del Trabajo Híbrido sobre Dimensiones Clave del Clima Organizacional

Dimensión	Efectos Positivos	Desafíos Emergentes
Autonomía y flexibilidad	Mayor control sobre horarios; mejora del equilibrio vida-trabajo; reducción de tiempos de desplazamiento	Difuminación de límites laborales-personales; riesgo de sobrecarga horaria; dificultad para desconectarse
Cohesión y pertenencia	Reunión intencional fortalece encuentros presenciales; equipos más deliberados en su comunicación	Reducción de interacciones informales; aislamiento social; dificultad de integración de nuevos miembros
Productividad	Mayor concentración en tareas individuales; ahorro de 72 minutos diarios en promedio por eliminación del desplazamiento	Fatiga por reuniones virtuales; dificultad para trabajo colaborativo espontáneo
Comunicación	Documentación más sistemática; inclusión de participantes geográficamente dispersos	Pérdida de comunicación no verbal; aumento de malentendidos; saturación de canales digitales
Equidad e inclusión	Acceso a oportunidades independiente de la ubicación geográfica; mayor diversidad en contratación	Sesgo de proximidad; trabajadores remotos perciben menor visibilidad; brecha digital socioeconómica

Nota. *Elaboración propia con base en Trenerry et al. (2021), Palumbo (2021), Han et al. (2025) y datos de Gallup (2025).*

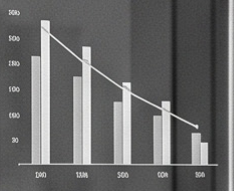
Un fenómeno emergente que merece atención particular es el denominado sesgo de proximidad (proximity bias), el cual se refiere a la tendencia de los líderes organizacionales a favorecer, consciente o inconscientemente, a los colaboradores que trabajan de manera presencial, otorgándoles mayores oportunidades de desarrollo, asignaciones estratégicas, promociones y reconocimiento (Owl Labs, 2025). Este sesgo es problemático en modelos híbridos donde coexisten trabajadores presenciales y remotos, generando lo que algunos autores han llamado una “fuerza laboral de dos niveles” con grados dispares de visibilidad, inclusión y acceso a oportunidades (Williamson et al., 2024).

Para las instituciones de educación superior, el sesgo de proximidad tiene implicaciones concretas. Docentes que trabajan en modalidad remota o híbrida podrían verse excluidos de decisiones académicas importantes, de comités de investigación o de redes informales que facilitan la colaboración científica. De igual manera, el personal administrativo que labora desde casa podría experimentar menor sentido de pertenencia institucional y menores posibilidades de ascenso. La gestión explícita de este sesgo, mediante políticas de evaluación basadas en resultados y no en presencialidad, se convierte en una necesidad estratégica para preservar la equidad organizacional.



PEOPLE ANALYTICS | HRIS OVERVIEW

ATTRITION FORECAST (85% PREDICTIVE)



RETENTION MODEL



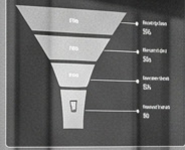
BUCKET PERFORMANCE

- 1. Identifying
- 2. Research
- 3. Analysis
- 4. Implementation
- 5. Monitoring

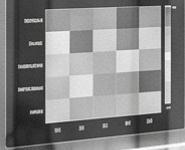
ORGANIZATIONAL HEALTH



TALENT ACQUISITION FUNNEL



EMPLOYEE ENGAGEMENT HEATMAP



5.2 Sistema de información en la gestión del talento humano

La analítica de personas (people analytics) ha experimentado una evolución significativa en los últimos años. Ha pasado de modelos descriptivos, enfocados en reportar indicadores históricos, como la tasa de rotación o el ausentismo, a modelos predictivos y prescriptivos capaces de anticipar fenómenos organizacionales y recomendar cursos de acción basados en datos (Bersin, 2024). Esta evolución ha sido impulsada por la convergencia de tres factores: la disponibilidad de grandes volúmenes de datos organizacionales, el avance de las técnicas de aprendizaje automático y la integración de la inteligencia artificial generativa en las plataformas de gestión del talento humano (Benuyenah, 2024).

En la encuesta SQ Magazine de 2025, el 50% de los profesionales de recursos humanos encuestados identificó la analítica de personas como el área donde la inteligencia artificial tendrá el mayor impacto, seguida por la adquisición de talento (37%) y el aprendizaje y desarrollo (35%). Asimismo, el 28% de las empresas estadounidenses ya utiliza tableros de desempeño impulsados por inteligencia artificial para alinear métricas individuales con los objetivos estratégicos organizacionales (SQ Magazine, 2025). Estos datos reflejan una tendencia clara hacia la centralización de la toma de decisiones sobre talento humano en sistemas algorítmicos, lo cual plantea tanto oportunidades como riesgos que deben ser cuidadosamente gestionados.

A pesar del entusiasmo en torno a la analítica de personas, la evidencia sugiere que la mayoría de las organizaciones se encuentran aún en etapas iniciales de madurez. Bersin (2024) señala que, tras miles de millones de dólares invertidos en plataformas de gestión del capital humano, menos del 10% de las empresas logra correlacionar efectivamente los datos de personas con indicadores de negocio. Esta brecha entre la promesa tecnológica y la realidad operativa constituye uno de los desafíos centrales del campo.

La analítica de personas no es un fenómeno homogéneo: las organizaciones se encuentran en estadios muy diferentes de desarrollo de esta capacidad; a su vez, la brecha entre las que están en etapas iniciales y las que operan en niveles avanzados tiene implicaciones directas sobre la calidad de las decisiones de gestión del talento. Comprender en qué nivel se sitúa una institución es el primer paso para diseñar una hoja de ruta de maduración realista y contextualizada.

La Tabla 13 presenta el modelo de cuatro niveles propuesto por Bersin (2024): desde el análisis descriptivo con reportes básicos de indicadores históricos hasta el análisis prescriptivo con recomendaciones automatizadas basadas en inteligencia artificial, indicando para cada nivel el enfoque, un ejemplo concreto de aplicación y la adopción estimada entre las organizaciones a nivel global. Estos datos muestran que la gran mayoría de las instituciones, incluidas las universidades latinoamericanas, se encuentran aún en los niveles descriptivo y diagnóstico, lo que define tanto las posibilidades como los límites razonables de la transformación digital en gestión del talento en el corto plazo.

Tabla 13
Niveles de Madurez en People Analytics

Nivel	Enfoque	Ejemplo	Adopción Estimada
1. Descriptivo	Reportes retrospectivos de indicadores básicos	Tasa de rotación trimestral; ausentismo por área	~60% de organizaciones
2. Diagnóstico	Análisis causal de fenómenos identificados	Correlación entre satisfacción y desempeño por equipo	~25% de organizaciones
3. Predictivo	Modelos estadísticos de anticipación	Probabilidad de renuncia de colaboradores de alto potencial	~10% de organizaciones
4. Prescriptivo	Recomendaciones automatizadas de acción	Asignación óptima de talento a proyectos según competencias	<5% de organizaciones

Nota. *Elaboración propia con base en Bersin (2024), Ghafoori et al. (2024) y SQ Magazine (2025).*

Uno de los riesgos más críticos asociados con la analítica de personas impulsada por inteligencia artificial es la perpetuación y amplificación de sesgos discriminatorios. Dubey y Vachher (2025) examinan cómo los prejuicios incorporados en los datos de entrenamiento, el diseño de los algoritmos y los procesos de toma de decisiones pueden reforzar la discriminación sistémica en contextos de gestión del talento humano. El caso paradigmático que ilustra este riesgo es el de Amazon, cuyo algoritmo de selección de personal fue descartado en 2018 tras comprobarse la discriminación sistemática hacia las candidatas mujeres; esto, gracias al entrenamiento del modelo con datos históricos que reflejaban patrones de contratación predominantemente masculinos (Dastin, 2018).

La demanda Mobley contra Workday, Inc., donde el demandante alegó que las herramientas de selección basadas en inteligencia artificial de la empresa discriminaban a candidatos por raza, edad y discapacidad, estableció un precedente legal relevante cuando en 2024 un juez federal en California denegó la moción de desestimación de Workday, subrayando la necesidad de que las empresas garanticen la transparencia y responsabilidad de sus sistemas de inteligencia artificial (Mobley v. Workday, Inc., 2024). Este tipo de litigios evidencia la evolución de los marcos regulatorios hacia una mayor exigencia de rendición de cuentas a las organizaciones que utilizan algoritmos para adoptar decisiones con efectos sobre las personas.

En el ámbito regulatorio, la Unión Europea lidera con el Reglamento de Inteligencia Artificial (EU AI Act), vigente desde agosto de 2024, que clasifica los sistemas de inteligencia artificial por niveles de riesgo e impone requisitos estrictos a los sistemas de alto riesgo, incluyendo evaluaciones de conformidad, registros y sanciones significativas por incumplimiento. En Estados Unidos, estados como Colorado, California y Nueva York han promulgado legislación específica sobre transparencia y mitigación de sesgos en sistemas de inteligencia artificial aplicados a decisiones laborales (ISACA, 2025). Para las organizaciones latinoamericanas, donde los marcos regulatorios sobre inteligencia artificial se encuentran en fase de construcción, estos desarrollos normativos internacionales ofrecen referentes valiosos para el diseño de políticas institucionales proactivas.

Marler y Boudreau (2017) advirtieron sobre la necesidad de equilibrar la eficiencia analítica con el respeto a los derechos de los colaboradores. Van den Heuvel y Bondarouk (2024) proponen un enfoque de tres etapas para operacionalizar la ética en la analítica de personas: identificación de principios éticos, implementación mediante estándares y educación, y validación en aplicaciones concretas. Este aspecto resulta útil para instituciones de educación superior, donde la sensibilidad ética constituye un valor fundacional que debe reflejarse coherentemente en sus propias prácticas de gestión.

Los principios fundamentales que deben orientar una analítica de personas ética incluyen la transparencia sobre los datos recopilados y su uso, la proporcionalidad en la recolección de información, la minimización del almacenamiento de datos al mínimo indispensable, la anonimización de análisis agregados para proteger la identidad individual, la participación de los colaboradores en el diseño de las métricas que evalúan su desempeño, y la existencia de mecanismos de revisión humana para decisiones críticas generadas por algoritmos (Lu & Xiong, 2025; Ghafoori et al., 2024; Avtalion et al., 2025).

5.3 Competencias Digitales y Cultura Organizacional

El desarrollo de competencias digitales ha alcanzado un punto inflexivo en el contexto organizacional contemporáneo. Según datos del Centro Común de Investigación de la Comisión Europea, en el período 2024-2025 el 92% de los trabajadores de la Unión Europea reportó necesitar habilidades digitales para desempeñar sus funciones laborales; al igual que, el 30% utilizó sistemas de inteligencia artificial en su trabajo cotidiano (Cosgrove & Cachia, 2025). Sin embargo, a pesar de esta demanda creciente, solo el 56% de los adultos en la Unión Europea alcanzaba un nivel de habilidades digitales superior al básico en 2023, evidenciando una brecha significativa entre las exigencias del entorno y las capacidades reales de la fuerza laboral.

El Marco Europeo de Competencias Digitales para Ciudadanos (DigComp), desarrollado por el Centro Común de Investigación de la Comisión Europea, constituye el referente internacional más consolidado para comprender, evaluar y desarrollar competencias digitales. En su versión más reciente (DigComp 3.0), el marco identifica cinco áreas de competencia fundamentales: alfabetización informacional y de datos; comunicación y colaboración; creación de contenido digital; seguridad y resolución de problemas. Cada área comprende competencias específicas que se despliegan en ocho niveles de dominio, desde el básico hasta el altamente especializado (Vuorikari et al., 2022; Cosgrove & Cachia, 2025).

La construcción de competencias digitales en el ámbito organizacional no puede reducirse a la capacitación técnica instrumental. Como señalan Carvalho et al. (2025) y Cyfert et al. (2025), la efectividad de los programas de desarrollo de competencias digitales depende, en esencia, de la cultura organizacional

en la que se insertan. Las organizaciones que conciben el error como parte del proceso de aprendizaje, valoran la experimentación y destinan tiempo formal para la formación, obtienen mejores resultados en sus procesos de transformación digital.

Una estrategia integral para el fortalecimiento de competencias digitales en instituciones de educación superior debería contemplar al menos cuatro componentes articulados: primero, un diagnóstico inicial de las competencias existentes, utilizando instrumentos validados, como la Escala de Competencias Digitales basada en DigComp (DCS); segundo, programas de formación escalonados que reconozcan la diversidad de trayectorias y puntos de partida; tercero, comunidades de práctica y tutorías entre pares que faciliten el aprendizaje situado; cuarto, mecanismos de evaluación continua que permitan monitorear el progreso y ajustar las intervenciones (Adam & Siladjaja, 2025; Espina-Romero et al., 2024).

Es fundamental que estas estrategias se aborden desde una perspectiva de equidad. La brecha digital no es un fenómeno puramente generacional, como frecuentemente se asume; la evidencia muestra que el dominio efectivo de herramientas digitales en contextos profesionales depende más de las oportunidades reales de formación y acompañamiento que de la edad (Nadkarni & Prüggl, 2020; Trenerry et al., 2021). En contextos regionales, como el Valle del Cauca, las desigualdades socioeconómicas en el acceso a conectividad y dispositivos tecnológicos añaden una capa adicional de complejidad; a partir de ello, las instituciones deben considerar en el diseño de sus estrategias de desarrollo de competencias digitales.

5.4 Ciberseguridad, ética y confianza

La ciberseguridad ha dejado de ser un asunto exclusivamente técnico para convertirse en una dimensión estratégica que permea la totalidad de la organización. El panorama de amenazas cibernéticas en 2025 presenta una complejidad sin precedentes, donde el costo global del cibercrimen se estima en 10,5 billones de dólares anuales, el costo promedio de una brecha de datos alcanza los 4,44 millones de dólares y los ataques de ransomware representan el 44% de las brechas de seguridad documentadas (Khalil, 2025). En este contexto, los ataques de ingeniería social constituyen la principal tipología de amenaza, con un 44% de los profesionales de ciberseguridad encuestados por ISACA, reportándola como el tipo de ataque más frecuente contra sus organizaciones, seguido por la explotación de vulnerabilidades (37%) y el malware (26%) (ISACA, 2025).

La evidencia reciente refuerza y amplía un hallazgo ya documentado en el capítulo anterior: la mayoría de las brechas de seguridad tienen su origen en el comportamiento humano. Los datos de 2025 añaden la dimensión agravante de la inteligencia artificial en este panorama. Según el informe de Fortinet (2025) sobre concienciación en seguridad, casi nueve de cada diez organizaciones reconocen que el uso de inteligencia artificial por parte de los atacantes ha incrementado la conciencia sobre la importancia de la capacitación en seguridad. Esta conciencia no se traduce automáticamente en preparación: un aproximado del 40% de los líderes considera que sus empleados disponen de las aptitudes para identificar, evitar y reportar amenazas cibernéticas basadas en inteligencia artificial.

Las amenazas impulsadas por inteligencia artificial que más preocupan a los líderes de seguridad incluyen el phishing generativo (51%), las falsificaciones de voz mediante inteligencia artificial o vishing (43%), los ataques mediante manipulación de indicaciones (prompt hacking, 45%) y las falsificaciones profundas o deepfakes (41%) (VikingCloud, 2025). Estos datos son especialmente relevantes para las instituciones de educación superior, que manejan grandes volúmenes de información sensible, como registros académicos, datos de investigación, información financiera, datos personales de miles de estu-

diantes y colaboradores; al tiempo que operan con recursos de ciberseguridad limitados en comparación con el sector corporativo.

Un factor que agrava la vulnerabilidad organizacional es la escasez crítica de profesionales en ciberseguridad a nivel global. Según el estudio ISC2 Cybersecurity Workforce Study de 2025, existe un déficit de aproximadamente 4,8 millones de profesionales de ciberseguridad en el mundo, cifra que creció un 19% en un solo año. Esta brecha no se reduce a formas cuantitativas: dos de cada tres organizaciones reportan brechas de habilidades entre moderadas y críticas en sus equipos de seguridad; por lo tanto, incluso las organizaciones que cuentan con personal de ciberseguridad enfrentan limitaciones significativas en las capacidades disponibles (ISC2, 2025).

Un dato revelador del estudio de ISACA (2025) es que la adaptabilidad ha emergido como la cualificación más valorada en profesionales de ciberseguridad (61%), por encima incluso de la experiencia previa en el campo (60%). Además, las habilidades blandas: pensamiento crítico (57%), comunicación (56%) y resolución de problemas (47%), constituyen la principal brecha de competencias percibida (59%). Estos hallazgos sugieren que la ciberseguridad organizacional requiere un perfil profesional, idóneo para combinar conocimiento técnico con capacidades humanas de análisis, comunicación y adaptación al cambio; un perfil que las instituciones de educación superior están en posición privilegiada de formar.

La ciberseguridad no es un problema técnico que pueda concentrarse en los equipos de tecnología: es una dimensión estratégica de la cultura organizacional que involucra a todos los actores institucionales. Las instituciones de educación superior son objetivos atractivos para los ciberataques, dada la combinación de datos sensibles que gestionan: información académica, registros financieros, datos personales de comunidades numerosas y diversas; además de la diversidad de sus usuarios, en la cual incluye una alta rotación de estudiantes con diferentes niveles de conciencia sobre seguridad digital.

La Tabla 14 sistematiza las principales amenazas cibernéticas identificadas en los informes de seguridad más recientes (Fortinet, 2025; VikingCloud, 2025; ISACA, 2025), describiendo para cada una su naturaleza, su impacto específico en instituciones de educación superior y las fuentes que la documentan, con el fin de ofrecer un panorama actualizado que oriente las decisiones de gobernanza digital de las universidades colombianas y latinoamericanas.

Tabla 14
Principales Amenazas Cibernéticas y su Relevancia para Instituciones de Educación Superior (2025)

Amenaza	Descripción	Impacto en IES	Fuente
Phishing generativo con IA	Correos fraudulentos personalizados generados por IA de alta sofisticación	Suplantación de identidad docente; acceso no autorizado a sistemas académicos	Fortinet, 2025; VikingCloud, 2025
Ransomware	Secuestro de datos con exigencia de pago; ataque a respaldos	Bloqueo de registros académicos; interrupción de operaciones administrativas	Deepstrike, 2025; ISACA, 2025
Deepfakes y vishing	Falsificaciones de voz e imagen para suplantación de identidad	Fraude en comunicaciones institucionales; manipulación de procesos académicos	VikingCloud, 2025
Vulneración de datos personales	Acceso no autorizado a información sensible de colaboradores y estudiantes	Daño reputacional; responsabilidad legal; pérdida de confianza institucional	PWC, 2025; ISC2, 2025
Ingeniería social	Manipulación psicológica para obtener acceso a sistemas o información	Vulnerabilidad por alta rotación de usuarios (estudiantes); diversidad de perfiles	ISACA, 2025; Fortinet, 2025

Nota. Elaboración propia con base en los informes referenciados. IES = Instituciones de Educación Superior.

La ética digital trasciende el mero cumplimiento normativo para constituirse en un pilar de la confianza institucional. Como se analizó en el capítulo precedente, la confianza se construye lentamente, pero puede erosionarse con rapidez ante incidentes de seguridad mal gestionados, usos inapropiados de información personal o decisiones automatizadas percibidas como injustas (Avtalion et al., 2025; Lu & Xiong, 2025). Este apartado añade, a la discusión anterior, el análisis de los marcos emergentes de gobernanza de la inteligencia artificial y sus implicaciones específicas para las organizaciones.

El mercado global de gobernanza de la inteligencia artificial fue valorado en aproximadamente 227,6 millones de dólares en 2024 y se proyecta que crezca a una tasa compuesta anual del 35,7% entre 2025 y 2030, alcanzando cerca de 1.420 millones de dólares (Aura Intelligence, 2025). Tal crecimiento exponencial refleja la urgencia con la que las organizaciones están adoptando herramientas de detección de sesgos, documentación automatizada de cumplimiento y mecanismos de auditoría basados en blockchain para garantizar la transparencia de sus sistemas de inteligencia artificial.

Para las instituciones de educación superior, la gobernanza de la inteligencia artificial presenta desafíos específicos. Estas instituciones no solo deben gestionar éticamente sus propios sistemas plataformas

de evaluación, sistemas de gestión del aprendizaje, herramientas de analítica académica; además, tienen la responsabilidad social de formar profesionales capaces de diseñar, implementar y auditar sistemas de inteligencia artificial éticos. En el ámbito de la investigación académica, el uso creciente de inteligencia artificial generativa plantea interrogantes sobre la integridad académica, la autoría intelectual y la validez de los hallazgos científicos que deben ser abordados mediante políticas institucionales claras (ISACA, 2025).

La construcción de confianza digital requiere un enfoque sistémico que articule políticas institucionales, prácticas de gestión y valores organizacionales compartidos. La Encuesta Global de Confianza Digital de PWC (2025) revela que las organizaciones capaces de construir reputaciones sólidas en materia de ciberseguridad y manejo ético de información generan ventajas competitivas determinantes en términos de confianza de usuarios, atracción de talento y legitimidad institucional.

Un elemento central para la construcción de esta confianza es lo que Fortinet (2025) denomina cultura de seguridad, cuyo interés alude a la internalización de las prácticas de seguridad como un componente natural del comportamiento organizacional, más allá del cumplimiento de protocolos formales. Los datos respaldan la efectividad de este enfoque: el 67% de las organizaciones que implementan programas de concienciación y capacitación en seguridad reportan reducciones moderadas o significativas en intrusiones, incidentes y brechas (Fortinet, 2025). Sin embargo, el informe también advierte que más de una cuarta parte de las organizaciones identifica el riesgo interno como razón para implementar programas de capacitación, lo cual representa un incremento notable respecto a años anteriores y refleja la complejidad del desafío.

5.5 La Transformación Digital como Proyecto Cultural

El análisis desarrollado a lo largo de este capítulo refuerza y profundiza una tesis central del capítulo anterior: la transformación digital es, ante todo, un

proyecto cultural. Las cinco dimensiones examinadas (trabajo remoto e híbrido, analítica de personas, competencias digitales, ciberseguridad y ética digital) convergen en un punto común: su éxito o fracaso depende menos de la sofisticación tecnológica disponible y más de la capacidad organizacional para gestionar los cambios culturales, relacionales y éticos que la digitalización implica (Deep, 2023; Grover et al., 2022; Cyfert et al., 2025).

Las instituciones de educación superior se encuentran en una posición condicionada y, al mismo tiempo, privilegiada frente a estos desafíos. Por un lado, enfrentan las mismas presiones de digitalización que cualquier organización contemporánea, con la complejidad adicional de gestionar comunidades diversas, como docentes, personal administrativo, estudiantes con necesidades, capacidades y expectativas heterogéneas. Por otro lado, su misión formativa les otorga una responsabilidad única: no solo deben digitalizarse de manera competente, sino hacerlo de un modo que sirva como modelo de práctica ética, inclusiva y sostenible para las generaciones de profesionales en formación (Isensee et al., 2020; Butt et al., 2024; Cardoso et al., 2025).

En este sentido, la pregunta que orienta la reflexión final no se circunscribe a cómo digitalizar más rápido o con mayor eficiencia, por el contrario, su proposición es ética y política: cómo digitalizar de maneras que fortalezcan la humanización del trabajo, la democracia organizacional, la equidad en el acceso a oportunidades y el bienestar colectivo de la comunidad institucional (Orlikowski, 2000; Grover et al., 2022). La transformación digital, concebida como un proceso socialmente construido y culturalmente mediado, requiere liderazgo visionario, participación genuina de los actores organizacionales, inversión sostenida en el desarrollo de capacidades humanas, así como una reflexividad crítica constante sobre los efectos organizacionales y sociales de las tecnologías que se adoptan (Cyfert et al., 2025; Adam & Siladjaja, 2025).