

Chapter 8 / Capítulo 8

AI, metaverse and sustainability in the new
organizational design
ISBN: 978-9915-9928-8-4
DOI: 10.62486/978-9915-9928-8-4.Ch08
Pages: 49-53



© 2026 The authors. This is an open access
book chapter distributed under the terms of
the Creative Commons Attribution (CC BY)
4.0 License.

Cybersecurity, trust and digital culture

Ciberseguridad, confianza y cultura digital

Jesús Alejandro Vázquez Meza¹  

Víctor Manuel Martínez García²  

Yennifer Díaz Romero³  

Manuel Iván Tostado Ramírez⁴  

Rogelio Estrada Lizárraga⁴  

José de Jesús Reyes Machain²  

1 Universidad Autónoma de Sinaloa, Unidad Académica Preparatoria Rubén Jaramillo, Vicerrectoría, Sinaloa, México

2 Universidad Autónoma de Sinaloa, Facultad de Arquitectura y Diseño, Vicerrectoría, Sinaloa, México

3 Universidad Autónoma de Sinaloa, Facultad de Ciencias de la Educación, Vicerrectoría, Sinaloa, México

4 Universidad Autónoma de Sinaloa, Facultad de Informática, Vicerrectoría, Sinaloa, México

5 Universidad Autónoma de Sinaloa, Facultad de Informática, Vicerrectoría, Sinaloa, México

ABSTRACT

This chapter analyzes cybersecurity as an organization-wide responsibility that cannot be reduced to technical equipment or solutions. It begins with the role of processes, everyday decisions, and attitudes toward information risks. Human factors and social engineering are considered, including attempts to manipulate individuals into unsafe behavior. The discussion distinguishes awareness of security recommendations from consistent safe practices, a distinction linked to cybersecurity culture. Risks concerning data protection and the use of AI tools outside institutional oversight are examined. The chapter also addresses hybrid and distributed workplaces, where devices, providers, and locations multiply. Management frameworks discussed in the manuscript help explain why security practices require continuity, training, and evaluation. The central argument is that digital trust depends on both suitable systems and organizational habits. Security is therefore presented as a shared task involving technical specialists, managers, and users, one that must adapt to changing patterns of work and collaboration. The chapter connects the human and technical dimensions of protection without treating either as a complete solution in isolation.

Keywords: Cybersecurity; Digital culture; Social engineering; Human factors; Data protection

RESUMEN

El capítulo analiza la ciberseguridad como una responsabilidad que atraviesa a toda la organización y no se agota en equipos o soluciones técnicas. Parte del papel que desempeñan los procesos, las decisiones cotidianas y las actitudes frente a los riesgos de información. Examina el factor humano y la ingeniería social, incluidas las formas de manipulación que buscan inducir comportamientos inseguros. Distingue entre conocer recomendaciones de seguridad y practicarlas de manera consistente, una diferencia vinculada con la cultura de ciberseguridad. La revisión considera los riesgos asociados a la protección de datos y a la incorporación de herramientas de inteligencia artificial fuera de los mecanismos de control institucional. También aborda las dificultades que presentan los entornos laborales híbridos y distribuidos, donde los dispositivos, proveedores y ubicaciones se multiplican. Los marcos de gestión mencionados en el capítulo sirven para mostrar por qué las prácticas de seguridad requieren continuidad, formación y evaluación. Su argumento central es que la confianza digital depende tanto de sistemas adecuados como de hábitos organizacionales. La seguridad aparece así como una tarea compartida entre responsables técnicos, directivos y usuarios, que debe adaptarse a nuevas modalidades de trabajo y colaboración. Esta perspectiva conecta las medidas preventivas con la comprensión real de los riesgos y con las prácticas que se repiten en el trabajo cotidiano. Se subraya así la relevancia de la formación y de la responsabilidad organizacional.

Palabras clave: Ciberseguridad; Cultura digital; Ingeniería social; Factor humano; Protección de datos

8.1 LA SEGURIDAD COMO PROBLEMA ORGANIZACIONAL

Durante mucho tiempo, la ciberseguridad se trató como un asunto exclusivamente técnico, centrado en *firewalls*, antivirus y parches de *software*; si bien dicha visión no está equivocada, resulta gravemente incompleta. Da Veiga y Eloff (2010) plantean desde las primeras líneas de su trabajo, en donde establecen que el enfoque de una organización hacia la seguridad de la información debe centrarse en el comportamiento de sus empleados, esto porque el éxito o el fracaso de esa seguridad depende, en última instancia, de lo que esas personas hacen o dejan de hacer todos los días.

Con esta idea se desplaza el centro de gravedad del problema. Además de comprar la herramienta técnica correcta, se vuelve necesario entender la seguridad como una propiedad emergente de toda la organización, es decir, de sus procesos, su cultura, sus incentivos y, sobre todo, de las decisiones cotidianas y aparentemente pequeñas que toma cada persona con acceso a un sistema. Cabe destacar que una organización puede invertir fuertemente en infraestructura de seguridad de última generación y, aun así, quedar expuesta si nadie dentro de ella entiende por qué esas medidas importan o cómo evitar comprometerlas sin darse cuenta.

8.2 FACTOR HUMANO

Si la seguridad es un problema organizacional, además de técnico, el factor humano se convierte casi por definición en la variable más determinante y, al mismo tiempo, en la más difícil de controlar. En su obra ya clásica sobre ingeniería social, Mitnick y Simon (2002) documentan con detalle cómo los atacantes más efectivos rara vez necesitan vulnerar un sistema técnico complejo cuando pueden, con mucha menos dificultad, convencer a una persona de que les entregue de manera voluntaria el acceso que necesitan.

Esta observación, formulada hace más de dos décadas, sigue siendo tan vigente como entonces, y quizás más. Por su parte, Da Veiga y Eloff (2010) señalan que una cultura organizacional consciente de la seguridad reduce el riesgo de mal comportamiento de los empleados y de interacciones dañinas con los activos de información. Se trata, en este sentido, del tipo de vulnerabilidad que ningún *firewall* puede prevenir por sí solo, ya que es un problema de comportamiento humano bajo presión, curiosidad o simple desconocimiento, ajeno a la infraestructura.

El reporte anual de IBM (2025) sobre el costo de las violaciones de datos aporta la evidencia económica más reciente de esta misma idea. En dicho estudio, el error humano fue la causa directa del 26 % de las violaciones de datos analizadas, mientras que el *phishing*, la técnica de manipulación más básica de la ingeniería social, volvió a ser el vector de ataque más común, presente en el 16 % de los incidentes y con un costo promedio de 4.8 millones de dólares por incidente (IBM, 2025). El mismo informe documenta algo inquietante sobre la velocidad con la que esto está empeorando, al señalar que la inteligencia artificial generativa redujo el tiempo necesario para redactar un correo de *phishing* convincente de hasta 16 horas a apenas 5 minutos, lo que multiplicó tanto la escala como la personalización de estos ataques. Con esto se puede ver que el factor humano, lejos de perder relevancia conforme avanza la tecnología de defensa, se está convirtiendo en un blanco cada vez más fácil de explotar con la misma inteligencia artificial que las organizaciones esperaban usar para protegerse.

8.3 CULTURA DE CIBERSEGURIDAD

El concepto de “cultura de ciberseguridad” suele usarse como frase hecha, sin que su contenido quede del todo claro. Da Veiga y Eloff (2010) ofrecen una respuesta precisa, en la que la cultura de seguridad de la información se entiende como la suma de percepciones, actitudes, valores y comportamientos que una comunidad organizacional demuestra al interactuar con la tecnología; con ello se puede ver que dicha cultura no se reduce a un cúmulo de conocimientos técnicos memorizados. Su marco distingue de forma explícita entre saber qué es una buena práctica de seguridad y haberla asimilado como parte natural del propio comportamiento cotidiano.

Esta distinción, que no es meramente académica, explica por qué muchas organizaciones invierten de forma considerable en programas de capacitación técnica sobre seguridad y, aun así, siguen siendo vulnerables, puesto que el haber transmitido información no equivale a haber cambiado el comportamiento. De acuerdo con este marco, construir una cultura genuina de

ciberseguridad requiere actuar al mismo tiempo sobre tres niveles, los cuales son el técnico, el procedimental y el humano-conductual, reconociendo que ninguno de ellos produce por sí solo el resultado que sí produce su combinación sostenida en el tiempo.

El estudio de Ruiz Sevilla (2026) sobre estudiantes de informática en la Facultad de Informática Mazatlán aporta evidencia empírica directa de esta brecha entre conocimiento y comportamiento, en donde se encontró que los estudiantes de semestres avanzados identifican correctamente, en un 86 % de los casos, los vectores de ataque basados en engaño textual o en suplantación de identidad corporativa, lo que revela un dominio conceptual sólido. Sin embargo, ese mismo grupo mostró un patrón de comportamiento que el estudio describe como “exposición técnica deliberada”, el cual consiste en la desactivación consciente de *firewalls* y antivirus, justificada por la necesidad percibida de mayor libertad técnica, y en un exceso de confianza que el propio autor vincula con el efecto Dunning-Kruger, es decir, con la creencia de que la habilidad técnica propia es suficiente para “controlar” un entorno inseguro sin las protecciones estándar (Ruiz Sevilla, 2026). En otras palabras, el conocimiento teórico no elimina la conducta de riesgo y, en este caso específico, incluso la transforma en una forma distinta y más deliberada de exposición.

8.4 INGENIERÍA SOCIAL

Más de 20 años después de que Mitnick y Simon (2002) la documentaran con detalle, la ingeniería social, entendida como el conjunto de técnicas de manipulación psicológica diseñadas para inducir a una persona a comprometer la seguridad de forma voluntaria, aunque involuntariamente perjudicial, sigue siendo uno de los vectores de ataque más efectivos que existen, esto porque ataca la confianza humana en lugar de los sistemas técnicos.

El propio texto de Mitnick y Simon (2002) plantea algo que resulta incómodo, pero que es necesario reconocer, en el sentido de que el elemento humano de la seguridad es, con frecuencia, el más débil de toda la cadena, lo cual no se debe a la incompetencia de las personas, ya que los atacantes explotan de forma deliberada rasgos humanos universales, como el deseo de ser útil, el respeto a la autoridad percibida y la urgencia inducida artificialmente, mismos que ninguna capacitación técnica logra desactivar por completo. Por ello, para combatir la ingeniería social no bastan las reglas memorizadas y se requiere una cultura organizacional en donde cuestionar una solicitud sospechosa, incluso si aparenta venir de una autoridad superior, se perciba como un comportamiento correcto, sin que se interprete como insubordinación.

La inteligencia artificial generativa está reescribiendo, en tiempo real, las reglas de este juego. De acuerdo con IBM (2025), el 16 % de las violaciones de datos analizadas en su estudio ya involucró el uso de IA por parte del propio atacante, principalmente para generar correos de *phishing*, presentes en un 37 % de esos casos, y contenido falsificado mediante *deepfakes*, presente en un 35 %. Lo que antes requería horas de investigación manual sobre una víctima potencial para redactar un mensaje convincente y personalizado hoy puede automatizarse casi por completo. Si bien las técnicas de manipulación que documentaron Mitnick y Simon (2002) dependían del ingenio y la paciencia de un atacante humano, la ingeniería social asistida por IA elimina buena parte de esa fricción, lo que exige que la cultura organizacional de sospecha saludable madure a la misma velocidad que la sofisticación de estos ataques.

8.5 PROTECCIÓN DE DATOS

Con la protección de datos, todos los principios anteriores se convierten en una obligación operativa concreta. En su publicación sobre programas de concientización y capacitación en seguridad, el Instituto Nacional de Estándares y Tecnología (2003) establece que ningún programa de este tipo puede considerarse completo si se limita a explicar amenazas en abstracto, sin conectar esa información con las responsabilidades específicas que cada persona tiene sobre los datos con los que trabaja a diario.

Por su parte, la norma ISO/IEC 27001:2022 aporta el marco de gestión formal para sostener esta protección de manera sistemática. En ella se establecen los requisitos que debe cumplir todo sistema de gestión de seguridad de la información para considerarse robusto y auditable, en lugar de quedarse en un conjunto de buenas intenciones sin verificación. La combinación de ambos enfoques, el educativo y el normativo, resulta indispensable, puesto que sin capacitación las normas se cumplen de forma mecánica y sin una comprensión real, mientras que sin normas la capacitación carece de estructura y de mecanismos de verificación que confirmen si está

funcionando.

Un riesgo particular y cada vez más frecuente que ilustra bien por qué ambos enfoques deben ir juntos es el de la llamada “IA en la sombra”, es decir, el uso de herramientas de inteligencia artificial por parte de colaboradores sin autorización ni supervisión de la organización. IBM (2025) encontró que el 97 % de las violaciones de datos relacionadas con IA ocurrieron en organizaciones que carecían de controles de acceso adecuados sobre estas herramientas, y que las violaciones vinculadas a la IA en la sombra generaron, en promedio, 670 000 dólares adicionales en costos para las organizaciones con un uso más extendido de este tipo de herramientas no autorizadas. El dato revela una paradoja incómoda, la cual consiste en que, mientras más entusiasmo pone una organización en adoptar la inteligencia artificial sin gobernarla, más se expone al tipo de fuga de datos que la protección formal está diseñada para prevenir.

8.6 SEGURIDAD EN ORGANIZACIONES HÍBRIDAS Y DISTRIBUIDAS

Todo lo discutido en este capítulo se vuelve considerablemente más complejo cuando la organización deja de operar desde un perímetro físico único y controlado para hacerlo de forma híbrida y distribuida, que es el mismo tipo de organización que se discutió en capítulos anteriores de este libro. En su informe sobre el panorama global de ciberseguridad, el Foro Económico Mundial (2024) documenta una brecha creciente entre las organizaciones que logran mantenerse resilientes ante estas nuevas condiciones y las que no, a la vez que señala que la escasez de talento especializado en ciberseguridad continúa ampliándose de manera notable en paralelo a esta transición.

Cabe destacar que el mismo informe advierte que solo el 15 % de las organizaciones se muestra optimista respecto a que esta brecha de habilidades mejore significativamente en los próximos dos años (Foro Económico Mundial, 2024).

Los datos de IBM (2025) permiten ver que este entorno disperso encarece de forma directa la respuesta de una organización ante un incidente. Su estudio documenta que las violaciones de datos toman, en promedio, 254 días en detectarse y contenerse por completo, plazo que se alarga considerablemente cuando la infraestructura de la organización está distribuida entre múltiples ubicaciones, proveedores de nube y dispositivos. El caso documentado por Ruiz Sevilla (2026) en el entorno universitario ilustra esta misma dinámica a menor escala, en donde, cuando miles de dispositivos personales de estudiantes se conectan al mismo tiempo a la red institucional bajo un esquema de *Bring Your Own Device*, el perímetro de seguridad tradicional deja de existir como línea de defensa única y la organización queda dependiendo, casi por completo, de que cada persona conectada mantenga por su cuenta buenos hábitos de higiene digital. Esta observación converge con lo discutido a lo largo del capítulo, esto es, con la idea de que en una organización híbrida y distribuida la seguridad deja de resolverse únicamente en el perímetro y pasa a depender, en buena medida, del comportamiento de cada persona conectada.