

Edición
15

ISSN: 2953-769X

CIBERCONTABILIDAD



REVISTA SEMESTRAL



Universidad San Marcos
Revista Académica Institucional



ACADEMIA

En esta sección podrás encontrar artículos académicos y artículos científicos de la comunidad universitaria en general, los cuales son originales, y describe resultados experimentales, nuevos conocimientos o experiencias basadas en hechos conocidos de sus autores.



EL FACTOR HUMANO EN LA CIBER CONTABILIDAD: NIVEL DE CONOCIMIENTO Y APLICACIÓN DE MEDIDAS DE CIBERSEGURIDAD EN ESTUDIANTES DE ADMINISTRACIÓN DE EMPRESAS Y CONTADURÍA PÚBLICA

Carlos Bejarano Chacón, cbejarano@usam.ac.cr
Universidad San Marcos, San José, Costa Rica
Código ORCID: <https://orcid.org/0009-0002-4289-720X>

Recibido: 06 de febrero de 2026

Aceptado: 29 de mayo 2026

DOI: <https://doi.org/10.64183/3sxq8f88>

Resumen. Las personas pueden hacer la diferencia en el desempeño de las organizaciones, de manera especial cuando se relaciona con la alfabetización de una temática en específico. En el caso de este artículo se aborda desde el enfoque digital y tecnológico que los profesionales en administración y contaduría deben de tener no solamente para un adecuado desempeño, si no principalmente para prevenir los riesgos que generan en la actualidad el cibercrimen. Aunque la tecnología ha avanzado mucho en temas de ciberseguridad, quizás siguen siendo los usuarios, es decir; las personas el punto más vulnerable, ya que por medio de tretas y artimañas amparadas en el uso de tecnologías pueden quedar expuestos o ser fácilmente inducidos al error. Por esto nace la inquietud de estudiar el nivel de conocimiento y aplicación de medidas de ciberseguridad en estudiantes de administración y contaduría de la Universidad San Marcos, en San José de Costa Rica. Definir el grado de conocimiento de estas medidas facilitaría la inclusión de contenidos, charlas y capacitaciones para los estudiantes y así fortalecer estos conocimientos que resultan esenciales en los ecosistemas de trabajo. Conocer de los elementos técnicos de administración y contaduría puede ser tan importante como la alfabetización digital para el procesamiento de las tareas profesionales en los puestos de trabajo, por esto se analiza dicha temática.

Palabras clave. Ciberseguridad, Cibercontabilidad, Factor humano, Alfabetización digital, Gestión de riesgos.

THE HUMAN FACTOR IN CYBER ACCOUNTING: KNOWLEDGE LEVEL AND APPLICATION OF CYBERSECURITY MEASURES AMONG BUSINESS ADMINISTRATION AND ACCOUNTING STUDENTS

Carlos Bejarano Chacón, cbejarano@usam.ac.cr

Received: February 06, 2026

Accepted: May 29, 2026

Abstract. Individuals can make a significant difference in organizational performance, especially when it comes to literacy in a specific area. This article addresses the digital and technological perspective that professionals in administration and accounting should possess, not only for adequate performance but, more importantly, to prevent the risks posed by cybercrime. Although technology has advanced considerably in cybersecurity, users—individuals—perhaps remain the most vulnerable point, as they can be exposed or easily misled through tricks and schemes using technology. This is why the study aims to assess the level of knowledge and application of cybersecurity measures among administration and accounting students at San Marcos University in San José, Costa Rica. Defining their level of understanding of these measures would facilitate the inclusion of content, talks, and training for students, thereby strengthening this essential knowledge in today's work environments. Understanding the technical elements of administration and accounting can be as important as digital literacy for processing professional tasks in the workplace; therefore, this topic is analyzed.

Keywords. Cybersecurity, Cyber accounting, Human factor, Digital literacy, Risk management.

1. INTRODUCCIÓN

La ciberseguridad es mucho más que una tendencia; es un conjunto de prácticas que todo usuario debe implementar para su seguridad y la protección de la organización de la que forma parte (Chinchilla Morales, 2021).

En la actualidad, la mayoría de puestos de trabajo desarrollan sus funciones soportadas en las tecnologías, lo que eventualmente potencia los riesgos informáticos. El secuestro de datos, los ataques a servidores y el *phishing* están a la orden del día, pudiendo afectar cualquier sector económico.

Por esta razón nace la curiosidad de indagar el nivel de conocimiento y aplicación de medidas de ciberseguridad en estudiantes de administración y contaduría de la Universidad San Marcos en abril de 2026.

Es vital que los futuros profesionales sean conscientes de los peligros en el ciberespacio. No porque sus carreras sean del ámbito informático, sino porque sus profesiones dependen de las tecnologías para desarrollarse.

Las plataformas de facturación, los sistemas contables, los ERP y los CRM son herramientas cotidianas para las empresas y profesionales independientes. El contexto actual es propicio para esta temática, ya que los avances tecnológicos son más rápidos

y profundos que nunca, al igual que las implicaciones de un fallo de seguridad (Zaragoza Velázquez & Vera Muñoz, 2015).

Una revolución tecnológica se gestó a inicios de los años 90 con la “democratización” de las computadoras y la aparición de la internet. Esto propició un profundo desarrollo, primero en el campo laboral y luego en el educativo. Con los avances aparecieron nuevas amenazas, como los virus informáticos que contaminaban archivos locales (Salas, 2015).

Antes del final de esa década, la internet transformó el ecosistema empresarial. Las máquinas de escribir fueron desplazadas por computadores, los documentos físicos mutaron a digitales y el fax acortó distancias. En los siguientes diez años, la fibra óptica permitió un intercambio de datos masivo, estable y rápido.

Antes del año 2010, las redes sociales y las conexiones virtuales evidenciaron la transformación de los negocios. El correo electrónico sustituyó al fax; enviar cotizaciones, certificaciones o informes tomaba apenas segundos.

Pero frente a tanta modernidad llegaron riesgos mayores. Los virus locales ahora tenían la capacidad de esparcirse por el ciberespacio, entrando a las redes corporativas y contaminando cientos de terminales en minutos (Chinchilla Morales, 2021).

Hoy, el ecosistema organizacional depende de la tecnología. Esta dejó de ser un complemento para convertirse en la plataforma que sustenta toda la operación. La caída de un servidor puede paralizar a una filial entera, sea por un fallo técnico o por el ataque de cibercriminales.

Se podría pensar que un ciberataque es siempre obra de un grupo criminal altamente sofisticado. Sin embargo, la realidad muestra que muchas brechas ocurren por el descuido de un usuario que abre un correo malicioso, infectando a toda la organización (Lockton, s.f.).

La revolución actual exige una educación continua. Los profesionales deben mantener actualizada su alfabetización digital, lo que ineludiblemente incluye los conocimientos en ciberseguridad dentro de su campo de acción. Esta es la temática central que se explora en este documento.

La tecnología como soporte de las operaciones organizacionales

Es importante reconocer que el papel y el bolígrafo también representaron tecnología en su momento. Facilitaron tareas humanas, propiciaron innovación y desarrollo. Hoy los vemos con normalidad, y lo mismo sucede con la internet; se da por hecho como un recurso siempre presente (Salas, 2015).

Durante los años 80, se intensificó el

desarrollo de los computadores de escritorio. Las empresas encontraron en ellos la manera de agilizar tareas, dar soporte a procesos y archivar memorias documentales de forma práctica y segura.

La comunicación interna también mejoró drásticamente. Muchas funciones organizacionales fueron soportadas por la tecnología, evolucionando hasta la actual automatización, la cual libera tiempo para labores más analíticas (Zaragoza Velázquez & Vera Muñoz, 2015).

Sin embargo, como señala Lockton (s.f.), el sector contable y financiero maneja información altamente confidencial (declaraciones de impuestos, inversiones, estrategias). Esta digitalización de la contabilidad atrae a los delincuentes, convirtiendo a la tecnología de soporte en un blanco crítico que requiere protección constante.

La alfabetización digital de los profesionales en ciencias económicas

Los avances tecnológicos son el motor de la era digital, pero la alfabetización de los profesionales en ciencias económicas es vital para darle sentido y seguridad a este ecosistema. El nivel de preparación tecnológica de los administradores marca la diferencia en el éxito y resguardo de las operaciones corporativas.

Los profesionales de hoy no son solo usuarios; son tomadores de decisiones. Aunque la tecnología avanza, requiere de la inteligencia y el criterio humano para su programación, desarrollo y ejecución segura (Suarez Kimura & Escobar, 2016).

Existe el mito de que las nuevas generaciones, por ser “nativas digitales”, gestionan de forma segura las plataformas. Sin embargo, estudios demuestran que el conocimiento técnico no siempre equivale a un comportamiento seguro en la red (Sanchez-Garcia et al., 2024). Es vital que los centros de estudio tomen decisiones basadas en datos para fortalecer estas competencias.

La alfabetización digital no es solo usar un ERP o un software contable. Implica conocer sus vulnerabilidades, diseñar planes de contingencia y aplicar la gestión de riesgos (Suarez Kimura & Escobar, 2016). A su vez, las organizaciones deben trazar rutas de capacitación continua para que su personal integre la ciberseguridad en el giro de negocio.

2. MATERIALES Y MÉTODOS

El presente estudio posee un enfoque cuantitativo, con un diseño no experimental y de alcance descriptivo. Se buscó comprender la realidad de la ciberseguridad desde la perspectiva del usuario administrativo y contable.

Población y muestra: La recolección de datos se llevó a cabo durante abril de 2026. La muestra consistió en 65 estudiantes activos de carreras afines a las ciencias económicas (Administración, Contaduría y otras) de la Universidad San Marcos, en distintos niveles de avance de su carrera.

Instrumento de recolección: Se diseñó un cuestionario estructurado digital dividido en cuatro secciones estratégicas: 1) Perfil demográfico y académico, 2) Experiencia laboral y exposición tecnológica, 3) Nivel de conocimiento sobre ciberseguridad y 4) Aplicación de medidas prácticas.

Análisis de datos: Las respuestas fueron tabuladas en una matriz de cálculo (Excel). Se realizó un análisis de frecuencias y cruce de variables para contrastar el conocimiento auto percibido de los estudiantes frente a las medidas de seguridad que realmente aplican y la capacitación formal recibida.

3. RESULTADOS DE INVESTIGACIÓN

Tras el análisis de los datos recolectados, se identificaron hallazgos reveladores respecto a la interacción de los futuros profesionales con la tecnología y su preparación ante los ciber riesgos.

En primer lugar, existe una alta exposición tecnológica. Una gran parte de los

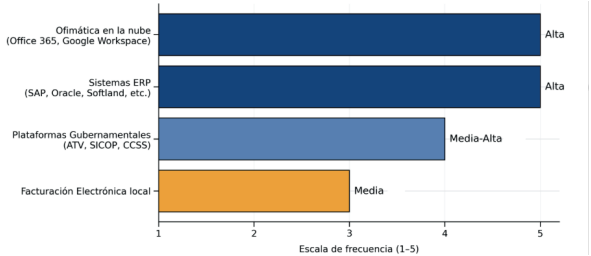
encuestados que laboran actualmente utilizan a diario herramientas conectadas a la red. Las plataformas más utilizadas son las Herramientas de Ofimática en la nube (como Office 365 y Google Workspace), seguidas de cerca por los sistemas ERP y las Plataformas Gubernamentales (ATV, SICOP).

Tabla 1. *Herramientas tecnológicas más utilizadas en el entorno laboral/práctico*

Tipo de Plataforma	Frecuencia de uso por los encuestados
Ofimática en la nube (Office 365, Google Workspace)	Alta
Sistemas ERP (SAP, Oracle, Softland, etc.)	Alta
Plataformas Gubernamentales (ATV, SICOP, CCSS)	Media - Alta
Facturación Electrónica local	Media

Fuente: Elaboración propia. (2026, con base en el sondeo)

Figura 1. *Frecuencia de uso de las encuestados de las plataformas*



Fuente: Elaboración propia. (2026, con base en el sondeo)

En cuanto al nivel de conocimiento, la mayoría de los estudiantes califica su saber en

ciberseguridad en un nivel intermedio (3 en una escala del 1 al 5). Reconocen masivamente términos como *Phishing* y *Malware*, pero muestran menor familiaridad con conceptos como *Ransomware* o Ataques *DDoS*.

La brecha formativa:

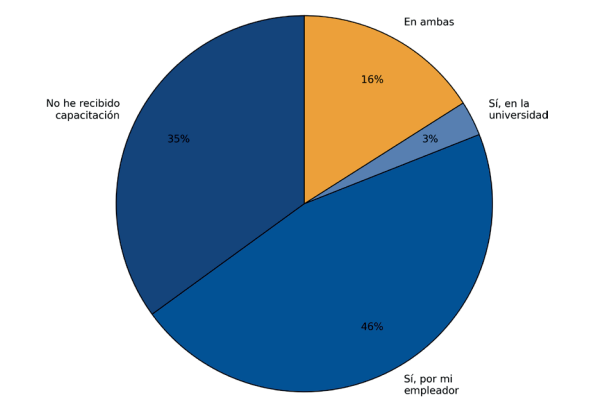
El hallazgo más contundente radica en la fuente de capacitación. Al consultarles si han recibido instrucción formal en ciberseguridad en el último año, se evidenció una desconexión académica.

Tabla 2. *Origen de la capacitación en ciberseguridad*

Origen de la capacitación	Porcentaje / Frecuencia
No he recibido capacitación	35%
Sí, por mi empleador	46%
Sí, en la universidad	3%
En ambas	16%

Fuente: Elaboración propia. (2026, con base en el sondeo).

Figura 2. *Origen de la capacitación en Ciberseguridad*



Fuente: Elaboración propia. (2026, con base en el sondeo)

Finalmente, en cuanto a prácticas aplicadas, la mayoría indica utilizar “Autenticación de dos pasos (2FA)” y “Verificar detenidamente los remitentes de correos”. Sin embargo, frente a la pregunta abierta sobre cuál es el mayor reto para mantener segura la información, la inmensa mayoría de las respuestas convergieron en una misma premisa: *El factor humano y la falta de concientización*.

Figura 3. *Prácticas aplicadas: el factor humano y la falta de concientización*



Fuente: Elaboración propia. (2026)

4. DISCUSIÓN (O ANÁLISIS DE LOS RESULTADOS)

Los resultados obtenidos validan contundentemente la premisa de Lockton (s.f.) y Chinchilla Morales (2021): la tecnología facilita los negocios, pero es la vulnerabilidad humana la que abre las puertas al cibercrimen.

Resulta sumamente llamativo que, aunque los estudiantes están expuestos a diario a plataformas críticas como sistemas ERP o los portales del Ministerio de Hacienda (ATV), un porcentaje muy bajo recibe educación formal sobre higiene digital dentro de su formación universitaria. Los datos demuestran que las universidades están delegando esta

responsabilidad a los empleadores (las empresas).

Esto genera una falsa sensación de seguridad. El estudiante sabe qué es un correo de *Phishing* a nivel teórico, pero como advierten Suarez Kimura y Escobar (2016), la falta de una política integral y de una cultura transversal de gestión de riesgos hace que, en la práctica, sigan siendo el eslabón más débil.

Los propios encuestados, en las preguntas abiertas, indicaron frases como: “*El mayor reto es el factor humano*”, “*Un solo clic equivocado puede comprometer todo*”, y “*Descuidos con las contraseñas*”. Esto demuestra que el futuro gestor contable y administrativo tiene plena conciencia de que no se trata de una falla del software (del antivirus o el *firewall*), sino de una falla en la cultura organizacional.

5. CONCLUSIONES

El ser humano como principal vulnerabilidad: Queda demostrado, por la misma percepción de los estudiantes, que el factor humano, la ignorancia y el descuido son los principales retos de seguridad en las empresas, superando a las deficiencias técnicas de los sistemas informáticos.

Brecha en la educación universitaria: Existe un vacío en la malla curricular. Los futuros contadores y administradores están siendo

entrenados en el uso operativo de sistemas (contabilidad, finanzas, planillas), pero la formación en ciberseguridad se está dejando casi exclusivamente en manos de las empresas contratantes.

Necesidad de alfabetización digital integral: Ser un «nativo digital» no garantiza tener buenas prácticas de seguridad. Es imperativo que la ciberseguridad se enseñe como un eje transversal en las ciencias económicas, fomentando políticas de «Confianza Cero» (Zero Trust) en el manejo de la información confidencial.

El administrador como “Firewall humano”: Las empresas proveedoras de software seguirán mejorando sus sistemas, pero si el usuario final no desarrolla una mentalidad preventiva, los ataques como el secuestro de datos seguirán en aumento. El contador del siglo XXI debe actuar como la primera línea de defensa digital de su organización.

6. AGRADECIMIENTOS

Se extiende un profundo agradecimiento a la Universidad San Marcos, a sus docentes y especialmente a los estudiantes de las carreras de Administración y Contaduría que, con su valiosa participación en el sondeo, hicieron posible la recopilación de datos que sustentan esta investigación.

7. CITAS Y REFERENCIAS BIBLIOGRÁFICAS

- Chinchilla Morales, J. (2021). *La Ciberseguridad*. Universidad San Marcos.
- Lockton. (s.f.). *Ataques Cibernéticos en el Sector Contable*. Lockton México. Recuperado de lockton.com.mx
- Salas C., H. (2015). *Incidencia de las nuevas TICs en la contabilidad*. INFOCONT.
- Sanchez-Garcia, I. D., Rea-Guaman, A. M., San Feliu, T., & Calvo-Manzano, J. A. (2024). Auditoría de riesgos de ciberseguridad: Revisión de Literatura, propuesta y aplicación. *RISTI - Revista Ibérica de Sistemas e Tecnologías de Informação*, (53), 69–87. <https://doi.org/10.17013/risti.53.69-87>
- Suarez Kimura, E. B., & Escobar, D. S. (2016). *Gestión de la ciberseguridad en sistemas contables digitalizados*. Centro de Modelos Contables. Universidad de Buenos Aires (UBA).
- Zaragoza Velázquez, P. G., & Vera Muñoz, M. A. M. (2015). Uso de la tecnología en función del área contable y fiscal. *Horizontes de la Contaduría*, (3), 1-13.