Ética y Responsabilidad Social en la Implementación de TIC

▷ Mauro Alonso Gonzalez Figueroa — *T00067622*

Resumen

Este ensayo explora los dilemas éticos y las consideraciones de responsabilidad social asociadas con la implementación y el uso de tecnologías de la información en las empresas. Se examina la importancia de adoptar prácticas transparentes y responsables en la gestión de datos personales, así como el impacto de las TIC en la sostenibilidad social y ambiental. Además, se destaca la relevancia de la ciberseguridad en la protección de la información empresarial y cómo esta se integra en la responsabilidad social empresarial (RSE). Finalmente, se analizan los riesgos cibernéticos comunes y las estrategias para mitigarlos, subrayando la necesidad de una aproximación ética y responsable en el uso de TIC

Palabras claves: *Ética, Responsabilidad Social Empresarial (RSE), Tecnologías de la información (TIC), Ciberseguridad, Privacidad de datos, sostenibilidad, Riesgos cibernéticos*

Abstract

This essay explores the ethical dilemmas and social responsibility considerations associated with the implementation and use of information technology in companies. It examines the importance of adopting transparent and responsible practices in managing personal data, as well as the impact of ICT on social and environmental sustainability. Additionally, it highlights the relevance of cybersecurity in protecting business information and how it integrates into corporate social responsibility (CSR). Finally, it analyzes common cyber risks and strategies to mitigate them, emphasizing the need for an ethical and responsible approach to ICT usage.

Keywords: *Ethics, Corporate Social Responsibility (CSR), Information Technology (ICT), Cybersecurity, Data Privacy, Sustainability, Cyber Risks*

Introducción

En la era digital, las Tecnologías de la Información y Comunicación (TIC) han transformado profundamente el panorama empresarial, ofreciendo oportunidades sin precedentes para la innovación, eficiencia y expansión global. Sin embargo, esta rápida adopción de las TIC también ha traído consigo una serie de dilemas éticos y consideraciones de responsabilidad social que las empresas deben enfrentar. La implementación y uso de tecnologías

avanzadas no solo afectan la operativa interna y la competitividad de las organizaciones, sino que también tienen un impacto significativo en la privacidad de los datos, la equidad en el acceso a la información y la sostenibilidad ambiental.

La ética en el uso de TIC se refiere a la adopción de prácticas que respeten la privacidad y la seguridad de la información personal de los individuos, evitando el uso indebido de datos y asegurando la transparencia en las operaciones digitales. Por otro lado, la responsabilidad social empresarial (RSE) implica que las empresas no solo se enfoquen en la maximización de beneficios, sino que también tomen en cuenta su impacto en la sociedad y el medio ambiente, actuando de manera que promuevan el bienestar común y la sostenibilidad.

Este ensayo explora cómo las empresas pueden integrar la ética y la responsabilidad social en la implementación de TIC, abordando los desafíos y oportunidades que surgen. Se analizarán aspectos clave como la gestión responsable de datos, la importancia de la ciberseguridad, y las estrategias para mitigar los riesgos cibernéticos. Al adoptar un enfoque ético y responsable, las empresas no solo cumplen con sus obligaciones legales y morales, sino que también fortalecen su reputación y contribuyen a un entorno digital más seguro y equitativo.

Seguridad de los datos

En la era digital actual, la protección de datos se ha convertido en un aspecto fundamental para las empresas que dependen de su presencia en la web para generar ingresos. La confianza del usuario es un factor crítico en este contexto; los consumidores no solo buscan productos que cumplan con sus expectativas, sino que también desean asegurar que sus datos personales estén protegidos.

A menudo, las empresas invierten grandes sumas de dinero en soluciones de seguridad que,

aunque pueden ser costosas, prometen una alta protección contra posibles vulnerabilidades. Esta inversión en tecnología no solo asegura el funcionamiento eficaz de los productos, sino que también fomenta la confianza del cliente. Sin embargo, la cuestión ética aquí radica en el nivel de responsabilidad que las empresas tienen al implementar y mantener estas soluciones tecnológicas.

Un caso relevante para ilustrar este tema es el de CrowdStrike, una empresa estadounidense especializada en ciberseguridad que ofrece protección a nivel del Kernel del sistema operativo. El Kernel es una parte crítica del sistema operativo, y cualquier error en su seguridad puede resultar en consecuencias desastrosas. CrowdStrike se ha ganado una sólida reputación por su capacidad para ofrecer una seguridad robusta y confiable.

Sin embargo, el caso de CrowdStrike también pone de relieve las complejidades de la confianza en la ciberseguridad. A pesar de sus altos estándares de protección, la empresa ha enfrentado incidentes de seguridad que han puesto a prueba la integridad de sus soluciones. Uno de los incidentes destacados *(el cual afecto alrededor de* $8{,}5M$ *de sistemas alrededor del mundo)* implicó una vulnerabilidad que, a pesar de ser detectada y mitigada, reveló cómo una brecha en la seguridad puede afectar la confianza depositada en una empresa de ciberseguridad.

Este evento subraya una importante dimensión ética: la responsabilidad de las empresas no termina en la implementación de tecnologías de seguridad. También tienen un deber continuo de garantizar que sus soluciones sean efectivas y que sus prácticas de seguridad se mantengan actualizadas para proteger los datos de los usuarios. Las empresas que utilizan servicios de ciberseguridad, como aquellas que confían en CrowdStrike, también comparten una responsabilidad social en la protección de sus propios datos y en la implementación de medidas adicionales para garantizar la seguridad.

A pesar de una falla en las soluciones de CrowdStrike, las empresas compradoras deben

asumir su parte en la responsabilidad social. Esto incluye la implementación de prácticas de seguridad adecuadas, la capacitación de su personal en ciberseguridad y la adopción de medidas preventivas para proteger los datos de los usuarios. La colaboración entre proveedores de servicios de seguridad y sus clientes es esencial para mitigar los riesgos y mantener la confianza en la tecnología.

Riesgos en la implementación de nuevas TIC

La implementación de nuevas Tecnologías de la Información y Comunicación (TIC) presenta varios riesgos significativos que pueden afectar la seguridad de la información y la operativa de las empresas. Estos riesgos incluyen una variedad de amenazas cibernéticas, así como desafíos asociados con la transición a nuevas tecnologías.

Entre las amenazas más comunes en la red se encuentran ransomware, phishing, malware y spyware. El ransomware cifra los datos de una víctima y exige un rescate para su liberación, mientras que el phishing engaña a los usuarios para obtener información confidencial mediante correos electrónicos fraudulentos. El malware puede dañar o robar datos, y el spyware puede espiar y recopilar información sin el consentimiento del usuario.

La transición hacia nuevas TIC también conlleva desafíos adicionales. Integrar nuevas tecnologías puede requerir una reestructuración de los sistemas existentes y una actualización de los procesos operativos. Es crucial gestionar estos riesgos de manera efectiva mediante la realización de auditorías de seguridad, la implementación de medidas de protección adecuadas y la capacitación continua del personal.

Las empresas deben tener un plan de respuesta a incidentes para manejar cualquier brecha de seguridad y minimizar el impacto de los ataques. Implementar políticas de seguridad rigurosas y mantenerse al día con las mejores prácticas de ciberseguridad es esencial para

protegerse durante el proceso de transición, del mismo modo, garantizando la seguridad de sus usuarios y previniendo al máximo cualquier inconveniente durante el proceso.

Bibliografía

McGrath, A., & Jonker, A. (2023, diciembre). ¿Qué es la responsabilidad social empresarial (RSE)? https://www.ibm.com/es-es/topics/corporate-social-responsibility

Einagrafic. (2022, noviembre). Protección de datos en empresas: ciberseguridad y privacidad. https://einatec.com/blog/proteccion-de-datos-en-empresas/

CrowdStrike. (2024, agosto). Falcon Content Update Translated Resource Hub — CrowdStrike. https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/translated-resources/

Soto, J. A. (2020, julio). ¿Qué es el Kernel y para qué sirve? https://www.geeknetic.es/Kernel/que-es-y-para-que-sirve

2024 CrowdStrike incident. (2024, agosto). https://en.wikipedia.org/wiki/2024_CrowdStrike_incident

Formosa, P., Wilson, M., & Richards, D. (2021). A principlist framework for cybersecurity ethics. *Computers and Security*, *109*, 102382. https://doi.org/https://doi.org/10.1016/j.cose.2021.102382

Okorie, G., Udeh, C., Adaga, E., DaraOjimba, O., & Oriekhoe, O. (2024). ETHICAL CONSIDERATIONS IN DATA COLLECTION AND ANALYSIS: A REVIEW: INVESTIGATING ETHICAL PRACTICES AND CHALLENGES IN MODERN DATA COLLECTION AND ANALYSIS. *International Journal of Applied Research in Social Sciences*, *6*, 1-22. https://doi.org/10.51594/ijarss.v6i1.688

van der Merwe, J., & Al Achkar, Z. (2022). Data responsibility, corporate social responsibility, and corporate digital responsibility. *Data and Policy*, *4*, e12. https://doi.org/10.1017/dap.2022.2

FBI, CISA, ACSC & NCSC-UK. (2022, febrero). 2021 Trends Show Increased Globalized Threat of Ransomware [Co-Authored by: TLP:WHITE]. %5Curl%7Bhttps://www.cisa.gov/sites/default/files/publications/AA22-040A_2021_Trends_Show_Increased_Globalized_Threat_of_Ransomware_508.pdf%7D

Howley, C. (2023, abril). Gartner Identifies the Top Cybersecurity Trends for 2023. %5Curl%7Bhttps://www.gartner.com/en/newsroom/press-releases/04-12-2023-gartner-identifies-the-top-cybersecurity-trends-for-2023%7D