Conciencia Digital

ISSN: **2600-5859**
Vol. 6 No. 4.1, pp. 133 – 146, octubre 2023

www.concienciadigital.org

Revelando las vulnerabilidades ocultas del sistema ERP de una institución educativa: un encuentro con el peligro

Revealing the hidden vulnerabilities of an educational institution's ERP system: facing risk

[1] Darío Xavier González Miranda https://orcid.org/0009-0007-7375-3678
Estudiante de la Universidad Católica de Cuenca, Maestría en Ciberseguridad, Cuenca, Ecuador.
dxgonzalezm49@est.ucacue.edu.ec

[2] Jorge Fernando Illescas Peña https://orcid.org/0000-0001-9316-1118
Docente de la Universidad Católica de Cuenca, Maestría en Ciberseguridad, Cuenca, Ecuador.
fernan.illescas@hotmail.com

[3] Sang Gunn Yoo https://orcid.org/0000-0003-1376-3843
Escuela Politécnica Nacional, Universidad Católica de Cuenca, Maestría en Ciberseguridad, Cuenca, Ecuador.
sang.yoo@epn.edu.ec

Artículo de Investigación Científica y Tecnológica
Enviado: 11/08/2023
Revisado: 05/09/2023
Aceptado: 01/10/2023
Publicado:30/10/2023
DOI: https://doi.org/10.33262/concienciadigital.v6i4.1.2726

Cítese: González Miranda , D. X., Illescas Peña, J. F., & Yoo, S. G. (2023). Revelando las vulnerabilidades ocultas del sistema ERP de una institución educativa: un encuentro con el peligro. *ConcienciaDigita*l, 6(4.1), 133-146. https://doi.org/10.33262/concienciadigital.v6i4.1.2726

CONCIENCIA DIGITAL, *e*s una revista multidisciplinar, t**rimestral,** que se publicará en soporte electrónico tiene como **misión** contribuir a la formación de profesionales competentes con visión humanística y crítica que sean capaces de exponer sus resultados investigativos y científicos en la misma medida que se promueva mediante su intervención cambios positivos en la sociedad. https://concienciadigital.org
La revista es editada por la Editorial Ciencia Digital (Editorial de prestigio registrada en la Cámara Ecuatoriana de Libro con No de Afiliación 663) www.celibro.org.ec

Esta revista está protegida bajo una licencia Creative Commons Attribution Non Commercial No Derivatives 4.0 International. Copia de la licencia: http://creativecommons.org/licenses/by-nc-nd/4.0/

Conciencia Digital

ISSN: **2600-5859**
Vol. 6 No. 4.1, pp. 133 – 146, octubre 2023

www.concienciadigital.org

Palabras claves:
Seguridad web**;** ciberseguridad; análisis de vulnerabilidades; amenazas; sistemas ERP.

Resumen

Introducción: La utilización inapropiada de las herramientas de las tecnologías de la información y comunicación acarrea graves consecuencias, como el robo de información, la suplantación de identidad y la comisión de ciberdelitos, entre otros. Uno de los principales motivos de preocupación radica en el empleo que se les da a estas herramientas en el ámbito educativo. El uso incorrecto de las aplicaciones web puede acarrear considerables pérdidas para las empresas, como la deterioración de su reputación, la merma de su cuota de mercado o la falta de competitividad. **Objetivo:** Realizar un análisis de vulnerabilidades para identificar exposiciones a amenazas a las que pueda estar abierto el sistema ERP de una Institución de Educación Superior. **Metodología:** Se llevó a cabo un exhaustivo análisis de las vulnerabilidades relacionadas con la plataforma web ERP utilizando herramientas útiles alojadas en Kali Linux. Estas vulnerabilidades se evaluaron en función de su grado de criticidad, considerando su posible impacto en la confidencialidad, integridad y disponibilidad (CID), utilizando una topología de análisis no autenticado **Resultados**: Se presentan un total de 36 vulnerabilidades identificadas, excluyendo aquellas de tipo "log". Además, se realiza un análisis exhaustivo de la estructura de la configuración de seguridad de la página web. **Conclusión:** La enumeración exhaustiva de las vulnerabilidades y deficiencias en la configuración proporciona una base sólida para mejorar la seguridad del sistema ERP. Esta información permite tomar medidas correctivas y aplicar las medidas de protección adecuadas para mitigar los riesgos identificados, además estas medidas serian mucho más efectivas con un análisis de topología autenticado. **Área de estudio general:** Tecnologías de la Información. **Área de estudio específica:** Ciberseguridad.

Keywords:
Web security; cybersecurity; vulnerability analysis; threats; ERP systems.

Abstract

Introduction: The inappropriate use of information and communication technology tools leads to serious consequences, such as information theft, identity theft, and the commission of cybercrimes, among others. One of the main concerns lies in the use of these tools in the educational field. The improper use of web applications can result in significant losses for companies, such as reputation damage, loss of market share, or lack of competitiveness. **Objective:** Conduct a vulnerability analysis to

ISSN: **2600-5859**
Vol. 6 No. 4.1, pp. 133 – 146, octubre 2023

identify threats and exposures that the ERP system of a Higher Education Institution may be susceptible to. **Methodology:** A comprehensive vulnerability analysis was carried out concerning the ERP web platform using useful tools hosted on Kali Linux. These vulnerabilities were evaluated based on their degree of criticality, considering their potential impact on confidentiality, integrity, and availability (CIA), using an unauthenticated analysis topology. **Results:** A total of 36 identified vulnerabilities are presented, excluding "log" type vulnerabilities. Additionally, a thorough analysis of the web page's security configuration structure is conducted. **Conclusion:** The comprehensive enumeration of vulnerabilities and deficiencies in the configuration provides a solid foundation for enhancing the security of the ERP system. This information enables the implementation of corrective measures and the application of appropriate protective measures to mitigate the identified risks, these measures would be even more effective with an authenticated topology analysis.

Introducción

Un ERP es un tipo de software empresarial que se utiliza para gestionar y optimizar los procesos y recursos de una empresa. Un ERP integra todas las funciones y procesos de la empresa en una sola plataforma, lo que permite una mayor eficiencia y una mejor toma de decisiones.

Debido a la importancia y a consecuencia de la pandemia por COVID-19 las instituciones de educación se vieron en la necesidad de crear o mejorar procesos automatizados para el desarrollo de sus actividades, en este contexto los sistemas ERP toman más relevancia al automatizar los procesos (Jiménez, 2022).

Un ERP desempeña un papel crucial en la industria de la educación al ayudar a gestionar eficientemente los procesos administrativos y académicos. En este contexto, un ERP educativo puede abarcar funciones como la administración de estudiantes, el seguimiento de la asistencia, la gestión de calificaciones, la programación de cursos y la gestión del personal docente (Noroña, 2019).

El informe publicado por el "Proyecto Abierto de Seguridad en Aplicaciones Web" OWASP (2021), señala que "A medida que el software se convierte en algo crítico, complejo e interconectado, la dificultad de lograr seguridad en las aplicaciones aumenta exponencialmente El ritmo vertiginoso de los procesos de desarrollo de software actuales, incrementa aún más el riesgo de no descubrir vulnerabilidades de forma rápida y precisa.". Un mal uso de los aplicativos webs puede conllevar a grandes pérdidas para las empresas, del mismo modo para los usuarios.

En este contexto es importante identificar el uso desarrollado de las tecnologías de la información y comunicación (TIC) como potenciador para lograr transformar la economía y aumentar la productividad (Inzunza, 2018).

La seguridad de la información describe actividades relativas a la protección de la información y los activos de la infraestructura de la información contra riesgos de pérdida, uso inadecuado, revelación o daño. En este contexto Hidayatulloh, Saptadiaji (2021), señala la importancia de constar con un sistema universitario que trate de evitar el top 10 del informe publicado por OWASP en 2017.

Rudho Sampurna (2022), indica lo siguiente: "Las pruebas de seguridad web tienen como objetivo encontrar vulnerabilidades de seguridad en las aplicaciones web y sus configuraciones. El objetivo principal es la capa de aplicación (es decir, lo que se ejecuta en el protocolo HTTP)".

La presente investigación se lleva a cabo en la infraestructura que puede estar detrás de la IP pública de un ERP de una institución de educación superior utilizando para ello herramientas para el análisis de vulnerabilidades alojadas dentro del sistema Kali Linux mediante un análisis de topología no autenticado, adicional se realiza comprobaciones de seguridad en la página web del mismo sistema.

Metodología

Entre las actividades desarrolladas en esta investigación se procedió a realizar una identificación de metodologías, técnicas y herramientas adecuadas para realizar el análisis de vulnerabilidades. De las ultimas se utilizaron aquellas que sean de libre uso en el

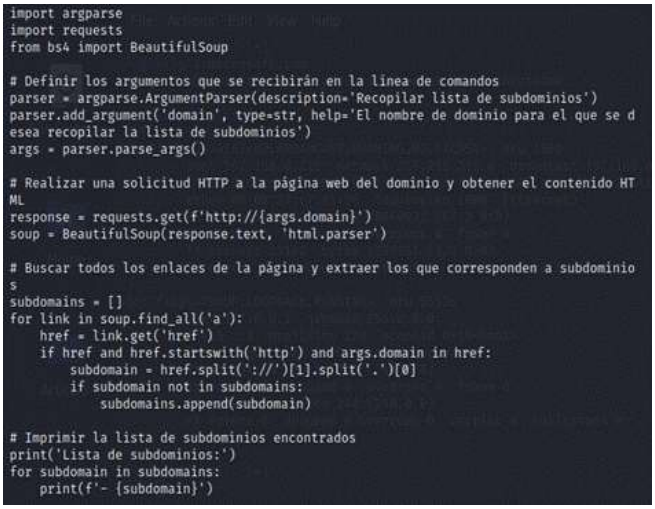
mercado, mediante el criterio de selección empírico, debido a los conocimientos adquiridos durante el desarrollo de un programa de maestría.

Para la realización de esta investigación se utilizó una metodología que se acopla al análisis de vulnerabilidades en plataformas web, según los criterios del mismo se establece las fases por las cuales está contemplado el desarrollo. Bajo este contexto Gupta & Seghal (2020), proponen una metodología para el análisis de vulnerabilidades en plataformas web, definido de la siguiente manera:

Recopilación de información: Recopilación de información relevante al sistema, direcciones IP, software utilizado, y subdominios asociados al sistema ERP.

Figura 1

Script en Bash que lista subdominios



```
import argparse
import requests
from bs4 import BeautifulSoup

# Definir los argumentos que se recibirán en la línea de comandos
parser = argparse.ArgumentParser(description='Recopilar lista de subdominios')
parser.add_argument('domain', type=str, help='El nombre de dominio para el que se d
esea recopilar la lista de subdominios')
args = parser.parse_args()

# Realizar una solicitud HTTP a la página web del dominio y obtener el contenido HT
ML
response = requests.get(f'http://{args.domain}')
soup = BeautifulSoup(response.text, 'html.parser')

# Buscar todos los enlaces de la página y extraer los que corresponden a subdominio
s
subdomains = []
for link in soup.find_all('a'):
    href = link.get('href')
    if href and href.startswith('http') and args.domain in href:
        subdomain = href.split('://')[1].split('.')[0]
        if subdomain not in subdomains:
            subdomains.append(subdomain)

# Imprimir la lista de subdominios encontrados
print('Lista de subdominios:')
for subdomain in subdomains:
    print(f'- {subdomain}')
```

Fuente: Bash (2018).

Escaneo de vulnerabilidades: utilizando herramientas de escaneo alojada en el sistema operativo KALI (2022), como OpenVAS (2019), para identificar posibles vulnerabilidades en el sistema o aplicación. Esto incluye escaneo de puertos, identificación de servicios y aplicaciones, entre otros.

Análisis manual: En esta fase se realizaron pruebas manuales para identificar vulnerabilidades que no pueden ser identificadas por herramientas de escaneo

automatizado. Las pruebas se sujetaron al informe publicado por OWASP (2021), para el análisis de la configuración de la seguridad de la página web del ERP.

Evaluación de vulnerabilidades: Se evaluó la criticidad de las vulnerabilidades identificadas y se priorizan según su impacto potencial en la seguridad del sistema.

Para la evaluación de vulnerabilidades se utilizó las valoraciones de NIST (2020). A continuación, se detalla su explicación en la tabla 1.

Tabla 1

Descripción de las métricas utilizadas

Métrica	Descripción	Valor
Acceso al Vector (AV)	Nivel de acceso necesario para explotar la vulnerabilidad	N: Acceso por red A: Acceso por red adyacente L: Acceso local P: Acceso físico
Complejidad de Ataque (AC)	Complejidad del ataque requerido para explotar la vulnerabilidad	L: Baja H: Alta
Privilegios Requeridos (PR)	Nivel de privilegios necesarios para explotar la vulnerabilidad	N: Ninguno L: Bajos H: Altos
Interacción del Usuario (UI)	Requerimiento de interacción del usuario para explotar la vulnerabilidad	N: No requerida R: Requerida
Alcance (S)	Alcance de la vulnerabilidad: si afecta únicamente al componente objetivo o también puede afectar a otros componentes.	U: Componente C: Adyacente
Confidencialidad (C)	Impacto potencial en la confidencialidad de los datos si la vulnerabilidad es explotada	N: Ninguno L: Bajo H: Alto
Integridad (I)	Impacto potencial en la integridad de los datos si la vulnerabilidad es explotada	N: Ninguno L: Bajo

ISSN: **2600-5859**
Vol. 6 No. 4.1, pp. 133 – 146, octubre 2023

		H: Alto
Disponibilidad (A)	Impacto potencial en la disponibilidad del sistema o recurso si la vulnerabilidad es explotada	N: Ninguno L: Bajo H: Alto

Fuente: NIST (2020), FIRST (2023) y MITRE (2022).

Los resultados presentados posteriormente se describen de la siguiente manera:

Para la triada CID

- C del 1 al 3
- I del 1 al 3
- D del 1 al 3

Para los valores del Impacto se lo calculó utilizando (VC+VI+VD)/3 donde V es el valor asignado, además se representa de la siguiente manera:

- Prescindible = Desde 1, hasta 1.5,
- Importante = Desde 1.6 hasta 2.5,
- Grave = Desde 2.6 hasta 3.

Remediación de vulnerabilidades: En esta fase se implementan medidas de mitigación para las vulnerabilidades identificadas según su criticidad.

Resultados

Se presentan los resultados obtenidos siguiendo la metodología aplicada:

Recopilación de información

La figura 2 muestra un listado de los subdominios asociados al ERP, además, se censuran el resto de subdominios encontrados en virtud de mantener la privacidad de los datos.

Conciencia Digital
ISSN: **2600-5859**
Vol. 6 No. 4.1, pp. 133 – 146, octubre 2023
www.concienciadigital.org

Figura 2

Lista de subdominios

La figura 3 a continuación describe el total de vulnerabilidades encontradas en el sistema ERP.

Figura 3

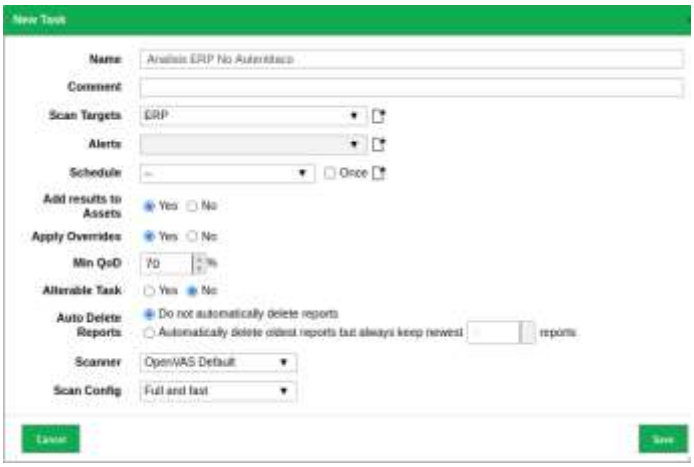
Obtención de dirección IP

Análisis de vulnerabilidades

La figura 4 a continuación presenta la configuración que se utilizó para el análisis en OpenVAS.

Figura 4

Configuración de análisis OpenVAS



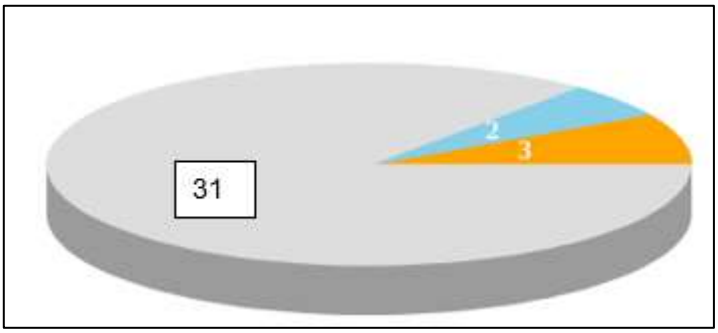
Nota: Análisis basado en la IP encontrada

Conciencia Digital
ISSN: **2600-5859**
Vol. 6 No. 4.1, pp. 133 – 146, octubre 2023
www.concienciadigital.org

La figura 5 a continuación describe el total de vulnerabilidades encontradas en el sistema ERP.

Figura 5

Vulnerabilidades encontradas en el ERP



Nota: Análisis basado en la IP encontrada con los resultados del análisis de OpenVAS.

Se presentan las vulnerabilidades divididas en categorías:

- 31 vulnerabilidades de tipo log
- 2 vulnerabilidades de tipo bajo
- 3 vulnerabilidad de tipo medio

Evaluación de vulnerabilidades

La tabla 2 a continuación describe las vulnerabilidades que se tomaron en cuenta para ser analizadas:

Tabla 2

Listado de vulnerabilidades analizadas

Código	Vulnerabilidad	CVSS	C	I	D	Severidad	Impacto
V-01	Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	CVSS Base Vector CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N	3	1	1	Media	Importante
V-02	Telnet Unencrypted Cleartext Login	CVSS Base Vector AV:A/AC:L/Au:N/C:P/I:P/A:N	2	2	1	Media	Importante

Conciencia Digital
ISSN: **2600-5859**
Vol. 6 No. 4.1, pp. 133 – 146, octubre 2023
www.concienciadigital.org

V-03	Weak Encryption Algorithm(s) Supported (SSH)	CVSS Base Vector AV:N/AC:M/Au:N/C:P/I:N/ A:N	2	1	1	Media	Prescindible
V-04	Weak MAC Algorithm(s) Supported (SSH)	CVSS Base Vector AV:N/AC:M/Au:N/C:P/I:N/ A:N	2	1	1	Baja	Prescindible
V-05	ICMP Timestamp Reply Information Disclosure	CVSS Base Vector AV:L/AC:L/Au:N/C:P/I:N/ A:N	2	1	1	Baja	Prescindible

Nota: Se descartan las vulnerabilidades de tipo “log”.

Análisis manual

En la figura 6 se muestra el resultado de un escaneo realizado con Nmap.

Figura 6

Análisis de NMAP

Nota: Recopilación de datos por el autor usando Nmap y Kali.

En la tabla 3 a continuación se presenta el resultado del análisis de vulnerabilidades y configuración encontrados en la página web del ERP.

Conciencia Digital
ISSN: **2600-5859**
Vol. 6 No. 4.1, pp. 133 – 146, octubre 2023
www.concienciadigital.org

Tabla 3

Descripción del banner de servicio

Banner	Descripción
HTTP/1.1 302 Found	El servidor ha redirigido temporalmente la solicitud del cliente a una nueva URL o recurso.
Location: https://:8015/	El servidor ha redirigido temporalmente la solicitud del cliente a una nueva URL o recurso.
Connection: close	Indica que el servidor cerrará la conexión después de enviar la respuesta.
X-Frame-Options: SAMEORIGIN	Configuración que controla si el sitio web puede ser incrustado en un marco o iframe (Iframe: Elemento HTML que permite mostrar contenido de otro documento dentro de una página web), en otro sitio.
X-XSS-Protection: 1; mode=block	Configuración que activa el filtro de protección contra ataques de scripting entre sitios (XSS (Cross-Site Scripting) es una vulnerabilidad web que permite la inyección de código malicioso en un sitio).
X-Content-Type-Options: nosniff	Configuración que previene que el navegador intente adivinar el tipo de contenido del archivo.
Content-Security-Policy: frame-ancestors 'self'	Configuración que controla qué sitios web pueden incrustar el sitio web en un marco o iframe.
Server: nginx/1.20.1	Indica el software del servidor web

Remediación de vulnerabilidades

En esta fase se brindó una lista de remediaciones que se pueden tomar en consideración en las vulnerabilidades analizadas según su criticidad.

Tabla 4

Lista de remediaciones

Código	Impacto	Tipo de Remediación	Descripción
V-01	Importante	Mitigación	Deshabilitar los algoritmos KEX.
V-02	Importante	Mitigación	Remplazar Telnet con SSH, que admita conexiones cifradas.
V-03	Prescindible	Mitigación	Deshabilitar los algoritmos de cifrado débiles.
V-04	Prescindible	Mitigación	Deshabilite los algoritmos MAC débiles.
V-05	Prescindible	Mitigación	Filtre las solicitudes de marca de tiempo ICMTP (13) y las respuestas de marca de tiempo ICMTP salientes
Nginx 1.20.1	Importante	Actualización	Mantener en constante actualización.

ISSN: **2600-5859**
Vol. 6 No. 4.1, pp. 133 – 146, octubre 2023

Conclusiones

La metodología utilizada tiene sentido altamente práctico, además, sirve como guía para realizar un análisis minucioso del contenido tanto de la página web como de la estructura del ERP.

Si se proporciona un acceso vía SSH se puede ejecutar un análisis de tipo autenticado el cual proveerá un listado de vulnerabilidades asociadas a la configuración de los servidores del ERP, y de esta manera las remediaciones que se pueden proveer serian de mayor fiabilidad.

El análisis planteado se ejecuta detrás de la infraestructura que puede estar tras la IP encontrada (Dominio Público) por lo que los resultados solo están asociados a la página web del ERP en estudio.

Conflicto de intereses

No existe conflicto de intereses entre los autores.

Referencias Bibliográficas

Brash, R., & Ganesh, N. (2018). *Bash Cookbook: Leverage Bash scripting to automate daily tasks and improve productivity*. Packt Publishing. https://public.ebookcentral.proquest.com/choice/publicfullrecord.aspx?p=5485025.

FIRST, Inc. (2023). *Common Vulnerability Scoring System v3.1: Specification Document*. Common Vulnerability Scoring System v3.1: Specification Document

g0tmi1k. (2022, septiembre 9). *KALI*. KALI: https://www.kali.org/docs/introduction/what-is-kali-linux/

Greenbone. (2019). *OpenVAS*. Retrieved Mayo 9, 2023, from https://www.greenbone.net/en/community-edition/

Gupta, B., & Seghal, M. (2020). A methodology for vulnerability assessment of information systems. In *In Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution* (pp. 107-125). IGI Global.

Hidayatulloh, S., & Saptadiaji, D. (2021). Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP). *Jurnal Algoritma, 19*(1), 77-86. Retrieved Noviembre 18, 2022, from https://jurnal.itg.ac.id/index.php/index/article/view/827

Inzunza, P. C. (2018). Amenazas y oportunidades de la economía digital en el mercado laboral de México. *Revista Facultad de Ciencias Económicas, XXVI*(2), 45-60. https://doi.org/https://doi.org/10.18359/rfce.2926

Jiménez, E. (2022, septiembre 5). *EasyChair*. EasyChair: https://wwwww.easychair.org/publications/preprint_download/HlGGl

MITRE Corporation. (2022, julio 22). *Common Vulnerabilities and Exposures (CVE)*. https://cve.mitre.org/index.html

NIST. (2020). *Nist*. https://www.nist.gov/

Noroña, J. C. (2019). Impacto de herramienta Open Source Odoo Erp en la Educación Superior. Caso Instituto Tecnológico Superior Guayaquil. *Universidad y Sociedad, II*(4). http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202019000400200

OWASP. (2021). *wiki.owasp.org*. https://wiki.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Rudho, M. (2022). Implementasi Hydra, FFUF Dan WFUZZ Dalam Brute Force DVWA. *Journal of Network and Computer, 1*(2), 25-33. https://jurnal.netplg.com/index.php/jnca/article/view/12

Conciencia Digital

ISSN: **2600-5859**
Vol. 6 No. 4.1, pp. 133 – 146, octubre 2023

www.concienciadigital.org

El artículo que se publica es de exclusiva responsabilidad de los autores y no necesariamente reflejan el pensamiento de la **Revista Conciencia Digital.**

Ciencia Digital Editorial

El artículo queda en propiedad de la revista y, por tanto, su publicación parcial y/o total en otro medio tiene que ser autorizado por el director de la **Revista Conciencia Digital.**

latindex catálogo

Conciencia Digital

Indexaciones