Publicación en Línea (Semestral) UPEL-Maracay (Venezuela)
DL: PPL201102AR3941
ISSN: 2244-7962
Edición Especial 2024. Vol. 21, N° 4
Revista Multidisciplinaria Dialógica
Investigación y Acción Tutorial. Tendencias y Redimensionamientos

Universidad Pedagógica Experimental Libertador
Vicerrectorado de Investigación y Postgrado
Instituto Pedagógico "Rafael Alberto Escobar Lara"
Subdirección de Investigación y Postgrado

CIBERSEGURIDAD, PRODUCCIÓN INTELECTUAL Y FORMACIÓN TUTORIAL: NAVEGANDO LOS DESAFÍOS DE LA ERA DIGITAL

Autor: Hedellwis Covy Barreto
covita.investigación@gmail.com
https://orcid.org/0000-0002-2772-1890
Universidad Nacional Experimental de la Seguridad
Maracay, Aragua - Venezuela

PP. 72-83

Barreto, E. C. (2024). Ciberseguridad, producción intelectual y formación tutorial: navegando los desafíos de la era digital. *Dialógica, Revista Multidisciplinaria. 21*(4), 72-83.

Publicación en Línea (Semestral) UPEL-Maracay (Venezuela)
DL: PPL201102AR3941
ISSN: 2244-7962
Edición Especial 2024. Vol. 21, N° 4
Revista Multidisciplinaria Dialógica
Investigación y Acción Tutorial. Tendencias y Redimensionamientos

CIBERSEGURIDAD, PRODUCCIÓN INTELECTUAL Y FORMACIÓN TUTORIAL: NAVEGANDO LOS DESAFÍOS DE LA ERA DIGITAL

Autor: Hedellwis Covy Barreto
covita.investigación@gmail.com
https://orcid.org/0000-0002-2772-1890
Universidad Nacional Experimental de la Seguridad
Maracay, Aragua - Venezuela

Recibido: Junio 2024 **Aceptado:** Noviembre 2024

Resumen

La ciberseguridad, la producción intelectual y la formación tutorial son aspectos importantes que se avizoran en la era digital, y abordar los desafíos que surgen desde ella es crucial para proteger la información y las ideas que se despliegan en la relación tutor – tesista. Este artículo tiene como objetivo exponer la incidencia de la ciberseguridad para los navegadores digitales desde la formación tutorial, incidiendo en la generación de conocimiento. Metodológicamente, se trata de un ensayo sustentado en la revisión documental y en la hermenéutica. Se hizo evidente que la seguridad de la información académica y científica es crucial para investigadores y docentes. Se deduce que, la protección de la propiedad intelectual resguarda años de trabajo, investigaciones y descubrimientos, evitando plagios, robos o alteraciones no autorizadas; y se convierte en una herramienta esencial para respaldar y salvaguardar el pensamiento propio, permitiendo la organización, clasificación y protección de documentos digitales de valor académico.

Palabras clave: Ciberseguridad, era digital, formación tutorial, producción intelectual.

CYBERSECURITY, INTELLECTUAL PRODUCTION AND TUTORIAL TRAINING: NAVIGATING THE CHALLENGES OF THE DIGITAL ERA

Abstract

Cybersecurity, intellectual production and tutorial training are important aspects that are emerging in the digital age, and addressing the challenges that arise from it is crucial to protect the information and ideas that are deployed in the tutor - thesis student relationship. This article aims to expose the impact of cybersecurity for digital browsers from tutorial training, influencing the generation of knowledge. Methodologically, it is an essay based on documentary review and hermeneutics. It became evident that the

Barreto, E. C. (2024). Ciberseguridad, producción intelectual y formación tutorial: navegando los desafíos de la era digital. *Dialógica, Revista Multidisciplinaria. 21*(4), 72-83.

security of academic and scientific information is crucial for researchers and teachers. It follows that the protection of intellectual property protects years of work, research and discoveries, avoiding plagiarism, theft or unauthorized alterations; and becomes an essential tool to support and safeguard one's own thinking, allowing the organization, classification and protection of digital documents of academic value.
Key words: Cybersecurity, digital age, intellectual production, tutorial formation.

Introducción

El presente artículo expone de manera superficial el mundo de la Ciberseguridad, la producción intelectual y la formación tutorial en el mundo donde diferentes seres humanos están interconectados en todo momento. Es internet, la mayor plataforma intercontinental que ha brindado sus lazos de unión con fines académicos investigativos, pacíficos y bélicos. Aquí, tanto la *Irenología* - entendida como el estudios de la paz o para la paz, o estudios de la paz y los conflictos - como la *Polemología* - estudio objetivo y científico de las guerras como fenómeno social - , convergen dada su naturaleza dentro de una sociedad que muchas veces parece sentir gusto o atracción hacia el conflicto y la pasiones conductuales delictivas y que se apoya en los recursos digitales y tecnológicos para difundir, infundir y perpetuar estas conductas destructivas; pero frente a las cuales también se lucha.

Y es precisamente en este escenario donde surgen nuevos *modus operandi* según la circunstancias y oportunidades que la misma víctima le ofrezca a victimario. Es en este terreno de la *Infocracia* - llamado así por Byung Chul Han- donde surgen elementos descollantes o fenómenos como la Ciberdelincuencia, o la apropiación indebida de información relevante para quienes transitan la internet. La Ciberseguridad sale a paliar con sus métodos innovadores con el fin de evitar, atajar o controlar todo aquello que pueda afectar a la producción intelectual. El investigador tesista recorre los caminos de la ciberseguridad apoyado en la inteligencia artificial. Es reconocer que abordar el internet para la investigación se necesita mucha cautela y bioética.

Barreto, E. C. (2024). Ciberseguridad, producción intelectual y formación tutorial: navegando los desafíos de la era digital. *Dialógica, Revista Multidisciplinaria. 21*(4), 72-83.

Algunas Precisiones sobre Ciberseguridad

Al hablar de Ciberseguridad someramente, la humanidad descubre la electrónica, enrumbándose descollantemente en lo que hoy se conoce como Internet. Esta herramienta que inicia con la intranet, se desprende de manera alarmante en la sociedad global, permitiendo que hoy sea un mundo paralelo al tangible. Internet desmonta el paradigma tradicionalista tangible y manual que, desde la llegada de los humanos a la tierra, dominan todas sus actividades. No obstante, aun cuando muchos procesos son llevados de manera manual, un conglomerado muy sustancial ha sido tomado por el mundo virtual. Desde entonces todo ha cambiado, es una revolución ingente qué transformó la cotidianidad del ser en todas sus formas de vida. Pudiera decir que es una revolución similar a la industrial, pero en mayores proporciones y dimensiones.

De esta manera nace la Ciberseguridad, cuyo fin consiste en defenderse de ataques virtuales gestionados por ciberdelincuentes, qué buscando fisuras en la red, más utilizando la ingeniería social, permean las páginas intentando apoderarse de información alojada por los navegadores digitales. Se puede decir que según la IBM (2023) establece:

> La ciberseguridad se refiere a cualquier tecnología, medida o práctica para prevenir ciberataques o mitigar su impacto. La ciberseguridad tiene como objetivo proteger los sistemas, las aplicaciones, los dispositivos informáticos, los datos confidenciales y los activos financieros de personas y organizaciones contra virus informáticos simples y molestos, ataques de ransomware sofisticados y costosos, y todo lo demás. (p. s/n)

Como se menciona en la cita, la ciberseguridad, es un organismo ciberpolicía, qué vigila las 24 horas del día todos los sistemas informáticos utilizados por las industrias, empresas, organismos institucionales, universidades, redes sociales, y navegadores. Con ello, se permite bloquear y perseguir a sujetos cuyo fin es dañar la construcción de información alojada en internet. En todo momento, al navegar en la web, se está a la expectativa o acecho, de quienes andan en el anonimato con la firme intención de ingresar a cualquier sitio y así, obtener beneficios de sus prácticas subrepticias y aviesas.

Ciberseguridad en Contextos Investigativos

En el proceso investigativo se desarrollan encuentros llenos de significado donde la formación tutorial establece un vínculo de armonía entre sus involucrados. Es necesario el establecimiento de una relación de confianza y respeto mutuo entre el tutor y el tesista. En esta etapa, se definen todas las herramientas que se despliegan a través del transitar por las expectativas y responsabilidades de cada parte, así como la metodología de trabajo acordada por el hegemón de la realidad quien marca el proceso de investigación.

En este punto, se puede afirmar que este revolucionario escenario como lo es internet, se perfila como una herramienta de trabajo que coadyuva a agilizar los procesos investigativos. Sin embargo, toda esta bondad trajo consigo delitos a cuestas, permitiendo que sujetos perniciosos, actuaran dentro de la red de manera necrófila, buscando siempre el lucro o causar daños a sus contrarios.

Las tendencias en Tecnologías de la Información (TI) de los últimos tiempos apuntan hacia el incremento en la computación en la nube, redes complejas, el trabajo remoto, los programas *bring your own device* (BYOD) y los dispositivos y sensores interconectados, lo que ha dado lugar a enormes ventajas académicas y empresariales influyendo en el desarrollo humano. Esto hace aún más riesgoso y peligroso ser víctima de delitos digitales gracias a la ciberdelincuencia informática en el mundo actual; y los espacios académicos y de investigación no están exentos de ello, por lo que debe imperar el conocimiento de herramientas de protección y resguardo digital de la información.

Además de lo anterior, hoy día, el investigador tesista recorre los caminos de la ciberseguridad apoyado en la inteligencia artificial. Esta vía de enriquecimiento con los autores concomitantes es innegable transitarla. Solo que es el investigador tesista quien toma la decisión de pensar lo encontrado en inteligencia artificial con ideas ajenas inspiradoras, o las hacemos ideas propias a través de la investigación deliberada. Esto implica reconocer que abordar internet para la investigación se necesita mucha cautela y habilidades que no comprometan la información tomada de la red. La existencia de aglomerantes datos, hace que se decante para poder tomar los más fiable y seguro.

Barreto, E. C. (2024). Ciberseguridad, producción intelectual y formación tutorial: navegando los desafíos de la era digital. *Dialógica, Revista Multidisciplinaria. 21*(4), 72-83.

Es importante destacar que los avances tecnológicos, han surgido de forma intempestiva, sin embargo, en esta etapa del internet de las cosas, se ha observado con preocupación el surgimiento de personas que usan y abusan de la información en los medios establecidos como mecanismos de interconectividad que se muestran vulnerables ante las redes. Como se viene dilucidando, los avances tecnológicos dispuestos al mundo global y dispuestos a al acceso en todos los niveles sociales, hacen que sea fácil adquirir herramientas de software cuyos propósitos pueden ser usados para perjudicar a quienes deciden incorporar sus producciones intelectuales dentro de la internet, en especial aquellas de gran valor.

Como parte de la producción intelectual está el *derecho de autor*. Es el derecho que se concede a todos aquellos quienes crean obras artísticas, musicales y de investigación para que se beneficien de su producción. Esto incluye la creación de obras literarias, musicales, cinematográficas, artísticas y científicas, así como la autoría de libros, artículos, ensayos y otros textos. Se puede considerar que la producción intelectual implica la libertad de crear y expresarse sin restricciones.

En concordancia con lo que se viene analizando, es fundamental tener en cuenta que para lidiar con el problema de los ciberataques y ciberamenazas, es pertinente considerar el empleo de un gran grupo de expertos en al Ciberseguridad, ello permitirá la reducción de estos individuos cuyas intenciones están plasmadas y orientadas a plagar los sistemas con malware maliciosos con el objeto de contaminar, dañar y poner en riesgo a los sistemas operativos de cualquier ente que desee usar los servicios de la internet. En este sentido, es imprescindible que los guardianes formados en Ciberseguridad, aseguren recurrentemente los sistemas, con la finalidad de blindar toda la infraestructura que opera en internet.

En este punto, es fundamental y necesario departir sobre los tipos de Ciberseguridad, al respecto establecer planes estratégicos sobre el tema en cuestión, que sean sólidos y que coadyuven en la protección de todas las capas de dominio más sustanciales de la infraestructura de la Tecnología e Información (TI) de las ciberamenazas

y ciberataques por parte de la ciberdelincuencia, al respecto se muestran varios tipos de Ciberseguridad.

Necesidad de Formar en Ciberseguridad Desde la Academia y la Investigación. Responsabilidad y Corresponsabilidad

La seguridad de la infraestructura protege los sistemas informáticos, así como programas, redes, data y otros recursos digitales de los que depende una comunidad virtual. Como se viene mencionando, este tipo de seguridad, protege los sistemas de uso en la redes de uso común y la más propensa a ser vulnerada por los grupos de Ciberdelincuentes que están usando la ingeniería social con la finalidad de penetrar con sus malware, o con el uso de mensajes falsos que invitan al usuario a revelar sus claves y así poder penetrar en el sistema y apropiarse de manera ilegal de sus bienes, producto de la inconsciencia de algunos empleados o personas particulares que no se han tomado en serio los delitos informáticos.

La seguridad de la red evita el acceso no autorizado a los recursos operados en la internet, detecta y detiene los ciberataques y las violaciones de seguridad de la red en curso, al mismo tiempo que garantiza que los usuarios autorizados tengan acceso seguro a los recursos de red que necesitan, cuando los necesitan. En lo antes expuesto, se observa una clara visión de que, a los participantes de un programa, aquellos quienes laboran en una empresa, instituciones gubernamentales del Estado, que manejan información de suma importancia, deben ser educados en el campo de la Ciberseguridad, y a estos mismos individuos participantes, se les debe hacer seguimiento de forma continua de sus viajes por la web, dentro y fuera de los lugares de labores.

Como ya se ha mencionado, los Ciberdelincuentes, están siempre al acecho de cualquier detalle, realizando ingeniaría social, en las redes, en los centros de confluencia social, como centros comerciales, en café, automarcados, en las universidades, en fin, en todos esos lugares de confluencia social. Es por eso, que se debe tener precaución en estos apartados de confluencia social ya que existen personas que están atentos a claves bancarias, entre otras, con el fin de obtener información y acceder a esos centros de

poder donde la información tiene mucho valor monetario o en el peor de los casos, inocular un malware que dañe los sistemas y así, solicitar recompensa para su restauración nuevamente.

Con respecto al tema de la nube, se puede decir que es parte de esos medios que se usan como archivos de documentos, imágenes, trabajos escritos, proyectos, etc., que son usados con el fin de evitar cargar o portar información en discos duros, pendrive, entre otros dispositivos. En este sentido la protección de los servicios y activos alojados en la nube opera según el modelo de responsabilidad compartida.

Los responsables de la información cuando se trata de la nube, son los desarrolladores del sistema, en ellos recae el mayor peso de la seguridad de toda la información que sube a esos archivos, por supuesto que quienes usan los archivos, deben estar conscientes de su responsabilidad con las claves de acceso a esos archivos, usar como norma que nunca se deben compartir esa información con nadie, de manera que toda esa información, es de uso personal. Por supuesto que allí, está la clave del éxito, la cual consiste en mantener la seguridad en los sistemas y bien resguardada la información de forma secreta.

Nadie en la red de internet está seguro, son muchos los riesgos que pueden surgir en ese mundo que el filósofo Byung Chul Han llama Infocracia, es decir, quien no esté debidamente protegido por los medios establecidos que dicta esta nueva sociedad informática, esta peligrosamente expuesto a ser estafado por los cibercriminales o piratas informáticos, al respecto se describen algunas amenazas usadas como medios para causar pérdidas a las víctimas de la internet.

Amenazas Latentes y Ciberataques. Implicaciones en la Academia y la Propiedad Intelectual

En primer lugar, podemos mencionar al *malware*, que según Carrasco et. al. (2013) se define como un software malicioso o programa maligno, como sería su traducción al inglés, que es cualquier programa malintencionado o código maligno, que ejecuta

Barreto, E. C. (2024). Ciberseguridad, producción intelectual y formación tutorial: navegando los desafíos de la era digital. *Dialógica, Revista Multidisciplinaria. 21*(4), 72-83.

acciones dañinas en un sistema informático de manera intencionada. Ellos pueden permear cualquier dispositivo y obtener información valiosa la cual usan con destinos necrófilos. Se puede decir que este tipo virus es pernicioso, y está diseñado con el propósito de perjudicar los sistemas operativos a los cuales se les infesta, de forma tal que los sistemas dejan de funcionar de forma correcta y terminan en manos de los cibercriminales, quienes más adelantes optan por exigir recompensas a los dueños de la infraestructura dañada.

Por otro lado, el *ransomware,* señalan Pedraza Moreno y Rojas Henao (2018) que se encarga de encriptar información que finalmente termina en extorción a la víctima. Este tipo de virus, es encriptado por los cibercriminales, con la finalidad de exigir recompensas. Es una modalidad de secuestro de los sistemas, con el objeto de demandar una recompensa a las víctimas propietarias de los sistemas informáticos que han sido inoculados con este tipo de virus maligno. En ocasiones sobrepasa los niveles cognitivos de quienes hacen el papel de protectores de los equipos de software dejando la red desprotegida.

Otro de las formas de estafar a las personas en internet, es usando *phishing*, y al respecto Carmona (2019) afirma que se trata de un término informático que hace mención a una serie de técnicas que buscan engañar a una víctima valiéndose de su confianza al hacerse pasar por una persona, empresa o servicio de conocido. Los delincuentes informáticos, emplean medios subrepticios donde solicitan datos de sus víctimas para estafarlas. Toda esta artimaña empieza solo haciendo *click* en cualquier ventana que ofrece de manera perniciosa un regalo que al perecer se ha ganado la víctima.

En ese orden de ideas, esas formas de aprovecharse de producción intelectual desarrollada por los navegadores digitales han causado altibajos en el momento de alojar contenido en internet. Es de hacer notar que se hacen visibles los *hackers*, quienes distantes de los delincuentes informáticos, buscan blindar la red de quienes la mantiene al acecho. De esta manera, la Real Academia Española (RAE) afirma que los *hackers* son “personas con grandes habilidades en el manejo de computadoras que investigan un

sistema informático para avisar de los fallos y desarrollar técnicas de mejora." (De la Iglesia, 2024).

Estos personajes los cuales hay que conceptualizar, por su naturaleza, conducta y prácticas en la modalidad de la Ciberseguridad y más aún en la producción intelectual, navegan en un mundo creado con la finalidad de agilizar los procesos humanos en una nueva era prevista de tecnología, vanguardia e innovación, disponible a la humanidad, para su disfrute y mejor calidad de vida. Por lo tanto, pueden ser grandes aliados en el momento de brindar seguridad a la producción intelectual generada a través de la relación tutor – tesista, quienes aportan al caldo cultivo del conocimiento.

Dentro de la formación tutorial los investigadores tienen el pleno consentimiento en desarrollar sus ideas propias, a través de sus producciones intelectuales, siempre y cuando no violen los derechos del pensamiento ajeno. Esta libertad es esencial para el progreso científico, artístico y cultural, porque permite a los investigadores explorar nuevas ideas y dar soluciones prosperas para la humanidad.

La protección de la propiedad intelectual es necesaria para fomentar la creatividad, los prototipos y la innovación. Esto estimula una competencia sana entre quienes se dedican a generar investigaciones para divulgarlas en universidades y en el propio internet. Actualmente muchos investigadores, universidades y entidades de divulgación científica son cada vez más vulnerables a la amenaza del cibercrimen. Esta información valiosa es dirigida hacia otros espacios donde buscan para obtener beneficios económicos.

La ciberseguridad debe ofrecer un blindaje a la producción intelectual para las investigaciones y producciones que se desarrollan en la red. Esta tiene el potencial de guardar y fortificar la innovación y la creatividad derivada de la relación tutor – tesista. Por tanto, se identifica a la ciberseguridad como el conjunto de medidas técnicas organizativas y legales que se utilizan para proteger la propiedad intelectual la cual se vincula a la relación tutor – tesista inspirada en la formación tutorial y asegurar que lo escrito por tesistas tengan su sello original.

A Modo de Cierre

A manera de resumen se considera la formación tutorial como el proceso que requiere una relación de confianza y respeto mutuo entre tutor - tesista. En el transitar de la investigación, es necesario des-educar y cuestionar nuestros pensamientos, siempre tomando lo necesario de las ideas ajenas para fortalecer las ideas propias a través de la investigación y sistemas de creencias. La relación tutor - tesista debe ser biofilia investigativa encaminada hacia la propiedad intelectual. Aquí se incluye el derecho de autor, patentes, marcas y otros que inciten a la propiedad elaborada por el ser humano. La protección de la propiedad intelectual es necesaria para fomentar la creatividad, los prototipos y la innovación. Aquí la ciberseguridad debe ofrecer un blindaje a la producción intelectual para las investigaciones y producciones que se desarrollan en la red. El conocimiento de los potenciales ataques y vulnerabilidades desde el mundo digital deben ser conocidas por los tutores e investigadores para tener mecanismos de control, respaldo y seguridad que vayan en atención al cuidado de su productividad académica.

Referencias

Carmona, A. (2019). *Desmontando a Lupin: La prevención de la estafa informática, desde y para el usuario*. Colegio Profesional de la Criminología de la Comunidad de Madrid. España.

Carrasco de la Fuente, R., Gumil Erena, S. y Vizcaíno González, A. (2013). *Sistema de ofuscación de malware para la evasión de NIDS*. https://docta.ucm.es/entities/publication/26e737ef-f2c7-4f5e-b1f0-16d634aef936

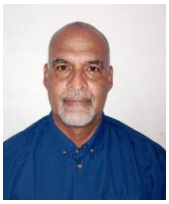
De la Iglesia, E. D. (2024, 8 julio). *Tipos de hackers*. https://www.campusciberseguridad.com/blog/item/133-tipos-de-hackers#:~:text=Seg%C3%BAn%20la%20RAE%20un%20Hacker,fama%20respecto%20a%20los%20Hackers.

Ibm. (2024, 11 octubre). *Ciberseguridad*. ibm.https://www.ibm.com/es-es/topics/cybersecurity

Piratería digital. (s. f.). https://www.interpol.int/es/Delitos/Productos-ilegales/Compre-de-forma-segura/Pirateria-digital.

Pedraza Moreno, V. M. y Rojas Henao, N. (2018). *Ransomware en Android*. https://repository.usta.edu.co/handle/11634/22002

Síntesis Curricular



Hedellwis Covy Barreto

Doctorado en Seguridad Ciudadana y Maestría en Educación, mención Investigación Educativa. Como profesor de Matemática, ha impartido conocimientos en diversas áreas. Es docente asesor-investigador a dedicación exclusiva en la UNES. Jefe Regional (e) de Creación Intelectual.