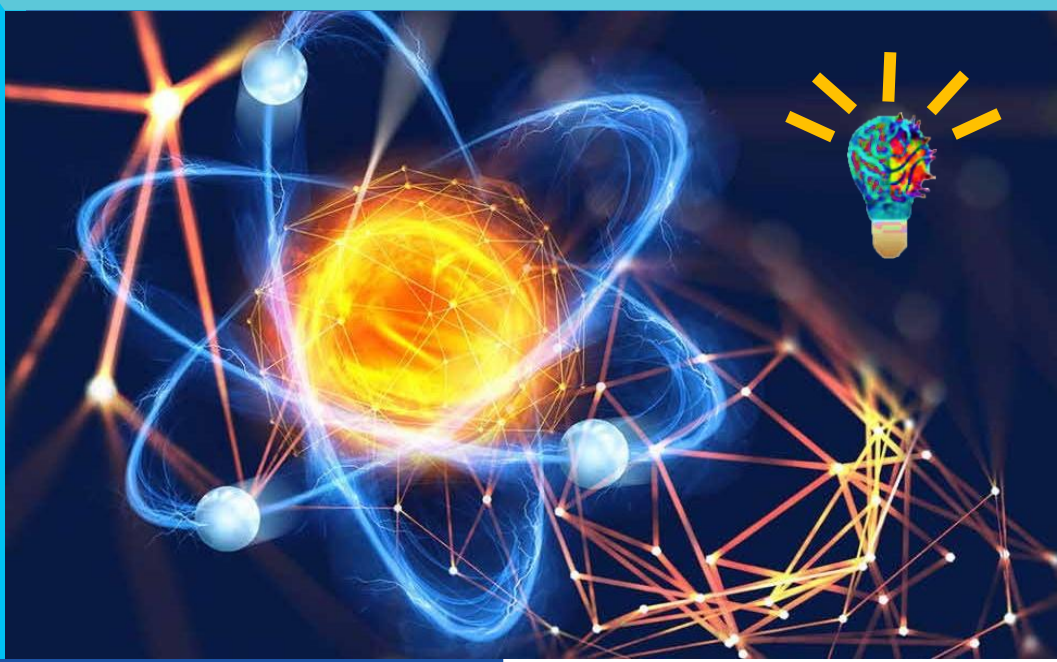
Universidad Nacional Experimental
Politécnica de la Fuerza Armada
Nacional Bolivariana

UNEFA

INGENIO

Vol. IV Nº 1

JULIO - DICIEMBRE 2023



Revista Científica Arbitrada Transdisciplinaria
Universidad Nacional Experimental Politécnica de la Fuerza Armada Bolivariana (UNEFA)

Vicerrectorado de Investigación, Desarrollo e Innovación (VIDI)
Coordinación Editorial Universitaria

E-mail:
ceuvidiunefa@gmail.com

Web
https://revistaingenio.org

Depósito Legal:
DC2017000513

UNEFA
Edif. Sede UNEFA, entre Av. La Estancia y Av. Caracas con calle Holanda, frente al Edif. BANAVEN (Cubo Negro) Municipio Baruta, estado Miranda, UNEFA-Venezuela
Teléfono: 0212-9082350

Editada por: Dr. Nelson Mata Villegas
Diagramación y montaje: Lic. Yeslibeth Díaz
Corrección de Estilo: Lic. Yeslibeth Díaz

AUTORIDADES

Rector
M/G. RICARDO NICODEMO RAMOS

Vicerrector Académico
G/D. ANDRÉS JOSUÉ YALASTASI YÉPEZ

Vicerrector Administrativo
CNEL. CRISTO NERIO MOLINA CARRILLO

Secretaria General
DRA. JASVELIN RAMONA MUJICA BENITEZ

Vicerrectorado de Investigación Desarrollo e Innovación
G/B. EDGAR MAESTRE LOBO

Vicerrector Defensa Integral
G/B. JOSÉ LUIS MONCADA MONCADA

Vicerrector de Asuntos Sociales y Participación Ciudadana
DR. MARLON JUNIOR ACUÑA LEZAMA

EQUIPO DE PRODUCCIÓN
Director:
GB. EDGAR MAESTRE LOBO
Editor:
Dr. Nelson Mata Villegas
Diseño e Imagen:
Lic. Yeslibeth Díaz
Corrección y Estilo:
Lic. Yeslibeth Díaz

COMITÉ EDITORIAL

ARBITROS DE ESTE NÚMERO
PROCESO “DOBLE CIEGO”

Los artículos publicados en la Revista Uirtus-UNEFA son arbitrados mediante el sistema doble ciego.

Roiman Valbuena Castro
Ingeniero en Electrónica
Especialista en Docencia para la Educación Superior

Anderso Andrade Rivera
Ingeniero Agrícola
Doctor en Ciencias de la Educación

Mario Sanabria
Ingeniero en Mantenimiento
MSc. en Gerencia de Mantenimiento

Nelson J. Mata Villegas
Licenciado en Administración
Doctor en Seguridad Social

CONTENIDO

NOTA EDITORIAL

Para el inicio de milenio XXI, los conocimientos científicos existentes en las Universidades; especialmente, lo atinente a los avances tecnológicos, conlleva a la asignación de significados a la cotidiana humana; los cuales mediante las redes hibridas ciberespaciales (redes de comunicación interactivas con fines comunes, sin ubicación geofísica, fragmentadas y difuminadas en diferentes partes del mundo), mezclan soluciones prácticas a subjetividades colectivas; lo cual era inaceptable en siglos pasados en donde Ciencias y Sociedad se encontraba separadas.

Asimismo, en las primeras tres décadas del siglo XXI, el sitio dedicado a la generación de conocimiento, pasa del laboratorio al campo y de éste a los espacios virtuales, como lugares de investigación, de encuentros y desencuentros, discusiones y debate sobre aspectos específicos desarrollados por diversas personas, sea cual sea su naturaleza, sin ningún tipo de contratación, ni organización jurídica legal, física, con sólo un objetivo común investigar, innovar y desarrollar la solución a determinado problema sobre determinado tema de interés común.

La disciplina científica pasa de un paradigma experimental puro a un paradigma práctico-instrumental flexible y multimodal, cuyo registros y tratamientos de las observaciones y resultados se llevan a software con posibilidad

de acceso para todos los interesados (Kerguelen, 2008).

El punto de sostén de la generación de conocimiento en la actualidad parece soportarse en un paradigma práctico-instrumental científico, siendo la clave de este, la claridad del objetivo a buscar; acceso libre, abierto y voluntario a la colaboración de aportes e identificación consensuada y compartida de los criterios de calidad exigidos para que dichos conocimientos sea admitido y legalizado por la comunidad científica “enredada”.

Luego, el método científico racional horizontal pasa a ser un proceso científico espiral dinámica de inducción–abducción-deducción-abducción-deducción-inducción, como dinamia trilógica inseparable recursiva combinada e integradora de resultados verificable y comprensión subjetividad de dichos resultados.

Los resultados obtenidos se reproducen y se discuten a medida que avanza su aplicación y se apropian de dichos resultados por aquellos que son al mismo tiempo objeto y sujetos de la investigación. El investigador se sitúa en posición de co-aprendiz y no de experto, una manifestación de la premisa aprender haciendo; se ubica en posición de escucha identificando lo desconocido para elaborar nuevos supuestos e hipótesis e incluso revisa la ya pre construida.

El novísimo milenio parece exigir complementar los tradicionales indicadores científico, tales como: veracidad, confiabilidad, sustentabilidad, validez, fiabilidad, objetividad, credibilidad, transfebilidad, confirmabilidad, autenticidad entre otros. Con nuevos criterios científicos milenarios tales como:

grado de demanda social, sea nacional, regional o mundial; nivel de satisfacción a las manifestaciones y reclamos socioculturales y sociopolítica; nivel de garantía colectiva relativa al uso de los resultados de la investigación; entre otros.

Por eso, la relevancia del pensamiento complejo mediante la interdisciplinariedad y la transdisciplinariedad en el abordaje de los procesos científicos, para atrapar las mayores propiedades comunes en la interrelación dinámica de éstas" (Hall). En este horizonte y dirección el paradigma de la complejidad, alude a "un tejido de constituyentes heterogéneos inseparablemente asociados, que presentan la paradójica relación de lo uno y lo múltiple". Dicho pensamiento, por su amplitud, flexibilidad y relación con la heterogeneidad y la convivencia de posturas contradictorias en un mismo espacio guarda una estrecha relación con el razonamiento trialéctico; ergo, permitirá a cada investigador la opción de una aproximación a la completud en las ciencias.

Los resultados de las investigaciones expuestas en esta edición del segundo semestre del 2023, se orientan a la solución de problemas demandados y requeridos por la localidad y región de ubicación; revelan el examen del entorno y sus potenciales efectos sobre disparejas áreas instrumentales de la cotidianidad humana.

Dr. Nelson Mata Villegas
Coordinador Editorial Universitaria

ARTÍCULOS

Y ENSAYOS ARBITRADOS

INGENIERÍA INVERSA EN LAS INCUBADORAS NEONATALES DEL SISTEMA DE SALUD DEL ESTADO LARA

Coautores: Dra. Ismenia María Suárez Finol
Ing. Edward Ángel Pereira Morales
Ing. Juan Emiro Mora Arcila
Institución: Universidad Nacional Experimental Politécnica de la Fuerza Armada Nacional Bolivariana (UNEFA).
Núcleo Lara
Correos: ismeniasuarezunefalara@gmail.com
edwardpereira65@gmail.com
morajuan24@gmail.com

RESUMEN

La presente investigación aplicada de tipo tecnológico, enmarcada en la línea de investigación de la UNEFA Ingeniería, Tecnología e Innovación que busca estimular y promover actividades de investigación, desarrollo e innovación tecnológica orientadas al fortalecimiento del desarrollo social del país, tuvo como propósito aplicar ingeniería inversa al módulo de control en las incubadoras neonatales desincorporadas en los centros asistenciales del sector salud del estado Lara. Se parte del basamento teórico conceptual, que en cuanto a la ingeniería inversa proviene del ámbito filosófico del razonamiento abductivo planteado por Peirce (1987) es un tipo de razonamiento que a partir de la descripción de un hecho ofrece llegar a una hipótesis que explica las posibles razones del hecho mediante premisas obtenidas, como que se construye a partir de conjeturas que se permiten diferenciar de la premisa y los postulados de la heurística según Polya (1989). En conclusión, la experiencia de aplicar ingeniería inversa al módulo de control de una incubadora neonatal desincorporada en un centro asistencial del sector salud del estado Lara, significó poder colocar en práctica la idea de que el conocimiento tecnológico se puede llevar a la praxis venciendo la dependencia técnica especializada, validando la apropiación del saber científico y la investigación desde la universidad. Se recomienda realizar la debida certificación del prototipo de la tarjeta controladora de la incubadora ante el ministerio de Salud y conformar un equipo multidisciplinario en la UNEFA para desarrollar investigación en torno a la electromedicina y áreas relacionadas con la reparación de equipos médicos e ingeniería inversa.

Palabras clave: Ingeniería inversa, incubadoras neonatales, placa Arduino.

REVERSE ENGINEERING IN THE NEONATAL INCUBATORS OF THE LARA STATE HEALTH SYSTEM

ABSTRAC

The present applied technological research, framed in the research line of UNEFA Engineering, Technology and Innovation that seeks to stimulate and promote research, development and technological innovation activities aimed at strengthening the social development of the country, had the purpose of applying reverse engineering to the control module in the neonatal incubators disincorporated in the healthcare centers of the health sector of the state of Lara. It starts from the conceptual theoretical foundation, which in terms of reverse engineering comes from the philosophical field of abductive reasoning proposed by Peirce (1987) is a type of reasoning that, based on the description of a fact, offers to arrive at a hypothesis that explains the possible reasons for the fact through premises obtained, as it is constructed from conjectures that can be differentiated from the premise and postulates of heuristics according to Polya (1989). In conclusion, the experience of applying reverse engineering to the control module of a neonatal incubator disincorporated in a health care center in the state of Lara, meant being able to put into practice the idea that technological knowledge can be put into practice, overcoming dependency. specialized technician, validating the appropriation of scientific knowledge and research from the university. It is recommended to carry out due certification of the prototype of the incubator controller card before the Ministry of Health and form a multidisciplinary team at UNEFA to develop research around electromedicine and areas related to the repair of medical equipment and reverse engineering.

Keywords: Reverse engineering, neonatal incubators, Arduino board.

INTRODUCCIÓN

La ingeniería inversa es un proceso de desmontaje, análisis y reconstrucción de un producto o sistema existente con el fin de determinar su funcionamiento interno y diseño. En otras palabras, se trata de trabajar en reversa, desde el producto

terminado hasta sus componentes, para entender cómo funciona. Este proceso puede ser utilizado en una amplia variedad de ámbitos, desde el militar, institucional hasta el empresarial y el tecnológico.

Acevedo y Puma (2007) plantean que: “El término Ingeniería Inversa tiene sus orígenes en el mundo del hardware. Una empresa desensambla un producto de la competencia para intentar comprender los secretos del diseño y de la fabricación” (p. 39). En tal caso, la ingeniería inversa tiene aplicaciones disimiles en cuanto al desarrollo de tecnologías y conocimientos para la apropiación y desarrollo de la necesaria independencia tecnológica de los pueblos.

En términos técnicos, la ingeniería inversa se divide en tres etapas: análisis, diseño y construcción. La primera etapa, el análisis, consiste en la descomposición del producto para identificar cada uno de sus componentes y clasificarlos según su función. De esta forma, la etapa de diseño implica la creación de un modelo detallado del producto o sistema basado en la información recopilada durante la etapa de análisis. Este modelo puede ser utilizado para la creación de un nuevo producto similar o mejorar el diseño del producto existente. En algunos casos, esta etapa también incluye la creación de software o código para sistemas electrónicos complejos.

La última etapa es la construcción, en la que se implementa el diseño resultante en la creación de un nuevo producto. Dependiendo del propósito final de la ingeniería inversa, el producto reconstruido puede ser idéntico al original o haber sido mejorado y modificado para cumplir con las necesidades específicas. Un ámbito importante de aplicación lo representa el

sector de la salud.

Así pues, hoy día el campo médico está altamente tecnificado y se requiere de múltiples equipos de cuyo mantenimiento y correcto uso depende la vida de los pacientes. Es por ello fundamental el mantenimiento preventivo y correctivo, como las mejoras que se pueda realizar a esos equipos, que también experimentan la obsolescencia programada. Tal como lo plantean Cabrera y otros (2020):

> En la actualidad los modelos de Gestión de Equipo Médico se han vuelto una herramienta de suma importancia para poder administrar la conservación y operación adecuada de equipos médicos en centros de atención, esto permite una mejora en la atención al paciente, mayor productividad del personal médico, además de ampliar la vida útil de la inversión realizada por las organizaciones hospitalaria públicas y privadas. (p. 53).

En correspondencia con lo anterior, la gestión de equipos médicos es una herramienta que la gerencia de los centros de salud no debe desatender, ya que, reviste una importancia vital. Tal es el caso de las incubadoras de neonatos, que son dispositivos médicos de alta complejidad y se utilizan para mantener a los recién nacidos prematuros o enfermos en un ambiente cálido y seguro, similar al que encontrarían en el útero materno. Estos equipos se controlan mediante una tarjeta que cumple tareas vitales para el correcto funcionamiento de la incubadora, como regular la temperatura, la humedad, la oxigenación, la iluminación y otros aspectos relevantes para el bienestar del neonato.

Ante la importancia de estas tarjetas controladoras, resulta fundamental contar con herramientas y técnicas que permitan

su diseño, prueba y mejora de manera eficiente y precisa. En palabras de Restrepo y otros (2007) “Cada uno de los componentes mecánicos y físicos que forman la incubadora, así como los sensores que miden las diferentes variables, deben estar sincronizados y en perfecto funcionamiento para que el microambiente del neonato no se altere” (p. 6). En este sentido, la ingeniería inversa se presenta como una alternativa relevante para obtener información detallada acerca del funcionamiento de la tarjeta, lo que permite corregir errores, mejorar su rendimiento y optimizar su diseño.

En consecuencia, en Venezuela, en los centros de salud públicos y algunos privados, ha habido una desincorporación masiva de incubadoras para neonatos por diversas causas, diferentes fallas que no podían ser arregladas porque una vez que se inicia el bloqueo económico las empresas internacionales suspendieron el servicio técnico y el envío de repuestos. De esta forma, se plantea la ingeniería inversa como una solución para rediseñar la fuente de poder y adaptar los requerimientos de la tarjeta controladora de la incubadora a la realidad venezolana. Rediseñando el sistema de control, revisando el dispositivo que censa cada parámetro de la incubadora. Tal como plantea López (2021):

> Con un bloqueo económico como el impuesto por el gobierno de los Estados Unidos y la Unión Europea ningún país a estas alturas nos vendería algún componente. El bloqueo económico afecta en todos los niveles el desenvolvimiento de los venezolanos, impidiendo el acceso a la tecnología no solo en el sector salud, sino en otras áreas, sin distinción de ninguna clase. (p. 2).

En ese orden de ideas, ante el bloqueo económico a que ha sido sometida Venezuela y el llamado a la independencia

tecnológica para superar las dificultades, reviste vital importancia un proyecto que propenda a la aplicabilidad de la ingeniería inversa para la recuperación de las incubadoras neonatales en los hospitales. Según lo reseña el mismo López (op cit): “son los fabricantes quienes imposibilitan, coaccionan y limitan desde los nombres de los componentes hasta no proporcionar los diagramas para el funcionamiento de algunos equipos, llegando hasta usar bit de bloqueo para obligar a quien tenga en uso alguno de ellos, a llamar a sus técnicos especializados”. (p. 2).

He allí la justificación de un proyecto que surge de las aulas universitarias para resolver problemas prácticos sentidos por la comunidad. En correspondencia con lo anterior, en los últimos años, la tecnología Arduino se ha vuelto cada vez más popular debido a su facilidad de uso y su capacidad para simplificar el desarrollo de proyectos electrónicos. Una de las aplicaciones más interesantes de Arduino es su uso como sustituto de la placa controladora de las incubadoras de neonatos.

Es así como, la presente investigación tuvo como propósito aplicar ingeniería inversa al módulo de control en las incubadoras neonatales desincorporadas en los centros asistenciales del sector salud del estado Lara. En consecuencia, se procedió a plantear los objetivos específicos: Identificar los materiales físicos y lógicos para el diseño del prototipo de la incubadora; definir las condiciones técnicas de diseño, los componentes físicos estructurales y los requisitos de programación que configuran el prototipo de tarjeta controladora para la incubadora neonatal; elaborar un prototipo según especificaciones técnicas de diseño y programación de la tarjeta controladora para la incubadora neonatal empleando un

Arduino.

En lo concerniente a la delimitación y alcance del estudio estuvo circunscrito a la realización de un prototipo; actividad que implicó análisis de fallas de la incubadora, adquisición de los componentes, construcción del prototipo propiamente dicho y la posterior programación de Software y pruebas de campo. Queda pendiente la debida certificación ante el ministerio de Salud.

En tal caso, la aplicabilidad de la ingeniería inversa para la recuperación de las incubadoras neonatales en los centros asistenciales del sector salud del estado Lara encuentra justificación ante la necesidad de recuperar una numerosa cantidad de equipos de incubadoras neonatales que han quedado sin servicio técnico ni repuestos ante el bloqueo económico a que está sometida Venezuela. Esta investigación parte de su basamento teórico que sustenta la investigación, su metodología utilizada, se redacta las conclusiones y recomendaciones y finalmente se reflejan las referencias bibliográficas.

REFERENCIAS TEÓRICAS

El presente estudio tiene su basamento teórico en los postulados de la heurística y el razonamiento abductivo. La heurística representa un enfoque para resolver problemas, con apoyo en la experiencia previa, el conocimiento común y las reglas pragmáticas, en lugar de seguir un conjunto de reglas rígidas. Este enfoque se utiliza con frecuencia cuando el problema es complejo o no está bien definido, ya que puede

ayudar a encontrar soluciones de manera más rápida y efectiva.

La heurística atiende a la capacidad que tiene el ser humano de valerse de la creatividad, el ingenio, el lenguaje y el pensamiento divergente para generar soluciones geniales a los problemas y enigmas que requieren ser resueltos. Esta disciplina del conocimiento, data de la antigua Grecia, sin embargo, fue el matemático George Polya (1965) quien la puso en la palestra, tras la publicación de su libro “Cómo resolverlo”, explica: “La heurística moderna trata de comprender el método que conduce a la solución de problemas, en particular las operaciones mentales típicamente útiles en este proceso. Son diversas sus fuentes de información y no se debe descuidar ninguna” (p. 102). De esta forma el autor fija la atención de la disciplina heurística en la comprensión de los métodos a seguir para resolver los problemas.

En ese sentido, la heurística se ha usado en diversas áreas, como la inteligencia artificial, la toma de decisiones, la psicología, la teoría de la computación y la ingeniería inversa. En estos campos, la heurística se utiliza para encontrar soluciones a problemas que no señalan una solución precisa, como la clasificación de objetos, la selección de patrones y la planificación de rutas.

Polya (1989) recomienda que para resolver un problema se requiere, en primer lugar, comprender el problema; en segundo lugar, concebir un plan; en tercer lugar, ejecutar el plan y finalmente examinar la solución obtenida. Durante todo el proceso, el autor propone una serie de interrogantes con las cuales el investigador o quien quiera que esté buscando la solución, interrogue la realidad estudiada.

En síntesis, la heurística se fundamenta en una serie de principios teóricos, incluyendo la filosofía empírica, la teoría de los sistemas complejos y la teoría del aprendizaje. Estos principios se utilizan para ayudar a entender cómo funcionan los sistemas complejos y cómo se pueden aplicar las reglas heurísticas para encontrar soluciones a problemas difíciles.

Por otra parte, el razonamiento abductivo es un proceso de inferencia según el cual se parte de una premisa que se considera verdadera y se buscan posibles explicaciones que justifiquen tal premisa, incluso si no se dispone de toda la información necesaria para comprobarla. En otras palabras, es un método para llegar a conclusiones provisionales a partir de observaciones o datos necesariamente incompletos. De acuerdo con Hamad (2009):

> La abducción como concepto surgió en Peirce (1901) a raíz del estudio de los planteamientos aristotélicos, como un tipo de razonamiento que además de ser lógico y tener un carácter instintivo, es también un proceso dinámico de pensamiento, en la medida en que genera hipótesis y selecciona la correcta. (p. 51)

Este tipo de razonamiento se utiliza comúnmente en la investigación científica, donde se recopilan datos empíricos para elaborar hipótesis que expliquen fenómenos observados. A medida que se van incorporando nuevos datos, estas hipótesis pueden ser modificadas o descartadas, dando lugar a nuevas explicaciones más precisas y completas. El razonamiento abductivo es un proceso de inferencia que busca explicaciones plausibles a partir de evidencias parciales, incompletas o ambiguas. Es utilizado en áreas como la ciencia, la medicina, el derecho y la inteligencia artificial, entre otras.

Finalmente, tanto el razonamiento abductivo y como la heurística son herramientas esenciales para la aplicación de ingeniería inversa, en tanto permiten resolver problemas complejos de manera más efectiva y eficiente por medio de la observación y la deducción de la información disponible. Fundamentales para identificar la estructura y el funcionamiento de sistemas complejos a partir de la observación y el análisis.

INGENIERÍA INVERSA EN INCUBADORAS NEONATALES

La ingeniería inversa tiene una amplia variedad de aplicaciones. En el ámbito empresarial, puede ser utilizada por los competidores para analizar los productos de su rival y mejorar sus propios diseños. En el ámbito militar, la ingeniería inversa se utiliza para replicar y adaptar sistemas de armamento de otros países. En el ámbito tecnológico, la ingeniería inversa es utilizada por desarrolladores de software para identificar los patrones y los códigos detrás de los programas. En expresión de Jiménez, y otros (2010):

> En el campo de la Ingeniería, la tecnología y la educación, la Ingeniería Inversa se aplica cotidianamente (a pesar de que muchas prácticas de la Ingeniería no las reconocen como tal). Por ejemplo, las empresas que se dedican al diseño de equipo original, regularmente usan algunos programas de la Ingeniería Inversa para el desarrollo de los productos. Otro ejemplo del uso de la Ingeniería inversa se puede observar en el mantenimiento industrial. En el caso de la educación, por lo general se duplican planes y programas de estudio, o bien prototipos y materiales didácticos. (p. 2).

De acuerdo con lo anterior, la ingeniería inversa es un proceso complejo de análisis, diseño y construcción que implica el

desmontaje y la reconstrucción de un producto existente. Su praxis comporta construcción de aprendizajes y fomenta el pensamiento y el accionar heurístico, al desarrollar un conocimiento previo y potenciar capacidades creativas. Aunque puede ser utilizada para una amplia variedad de aplicaciones, incluyendo el diseño y mejora de productos, puede también implicar riesgos legales y éticos cuando se utiliza para copiar productos de manera desleal. Por lo tanto, la ingeniería inversa debe ser realizada con precaución y responsabilidad para evitar consecuencias negativas para todas las partes involucradas. Al respecto, Jiménez y otros (ob. cit) expresan:

> En síntesis, se puede decir que: (1) La Ingeniería Inversa es de uso común, y no se limita solo a la reproducción de partes y componentes. (2) La Ingeniería Inversa es legítima en el sentido de que busca obtener información acerca de cosas, productos, componentes o sistemas. Las malas prácticas en el uso de dicha información se deben al hombre y no a la metodología. En este sentido, la Ingeniería Inversa no es sinónimo de piratería. (p. 2).

Lo planteado por los autores antes citados, remite a una reflexión ética en cuanto a que la ingeniería inversa es una metodología válida que implica capacidad creativa, producción de nuevas ideas y productos a partir de desarmar un objeto o sistema, estudiar su composición y generar un nuevo producto mejorado. Ahora bien, el derecho a la propiedad intelectual no debe ser una manera de institucionalizar el monopolio del conocimiento en detrimento de la sociedad. En reflexión de Ramos (2013):

> Al revisar la historia del desarrollo de los países industrializados la ingeniería inversa se puede ver como una buena práctica para imitar, apropiar y copiar la tecnología industrial ha sido una tendencia que han utilizado los países

> a lo largo de la historia del capitalismo moderno: durante el siglo XIX, Estados Unidos, Alemania, Francia y los países nórdicos desde Inglaterra; durante la segunda mitad del siglo XX los países del este asiático desde Estados Unidos, Europa y Japón; actualmente los países del este europeo, China e India. (p. 3).

Es decir, que los países industrializados han mejorado su capacidad tecnológica empleando la ingeniería inversa para imitar y apropiarse de otras tecnologías acrecentando el patrimonio intelectual, científico y tecnológico de que hoy dispone la humanidad.

Ahora bien, existen varias herramientas y técnicas que se utilizan para la ingeniería inversa, como la descompilación de software, la ingeniería inversa de hardware y la ingeniería inversa de protocolos de red. Estas técnicas pueden ayudar a comprender el funcionamiento de un sistema o dispositivo existente, lo que puede ser muy útil para mejorarlos o solucionar problemas como en el caso de las incubadoras neonatales en desuso en los hospitales y ambulatorios.

De esta forma, las incubadoras de neonatos están diseñadas para proporcionar una serie de funciones importantes, como el control de la temperatura, la humedad, la ventilación y la protección contra la luz y el ruido. También se utilizan monitores de frecuencia cardíaca, oxígeno en la sangre y temperatura para evaluar la salud del bebé. En caso de que el niño requiera atención médica adicional, la incubadora se puede equipar con dispositivos médicos adicionales como ventiladores, bombas de infusión, luces de fototerapia y monitores de presión arterial. Según Acevedo y otros (2017):

> La incubadora posee dos componentes fundamentales la cúpula, el chasis y el sistema de control de variables. La cubierta es el responsable de aislar al bebé del medio y evitar que el exterior afecte las variables controladas como la temperatura y la humedad, además de las infecciones presentes en el ambiente y el chasis contiene la fuente de poder y los sensores para la protección del neonato. (p. 108).

En ese orden de ideas, uno de los principales beneficios de la ingeniería inversa en el diseño de tarjetas controladoras de incubadoras de neonatos es que permite analizar y comprender la estructura lógica del sistema, lo que facilita la identificación de fallas, depuración de errores y solución de problemas técnicos. Asimismo, permite identificar las características de los componentes utilizados y optimizar su rendimiento y eficiencia para mejorar el desempeño de la tarjeta.

Además, la ingeniería inversa puede ser útil para realizar pruebas de funcionalidad y para la integración de nuevas funciones y mejoras al sistema. Con la información obtenida a partir de la tarjeta controladora, es posible diseñar nuevos circuitos o algoritmos que permitan mejorar el funcionamiento de la incubadora y lograr una mayor precisión en su control.

Por otra parte, la ingeniería inversa también resulta fundamental para la identificación de problemas de seguridad. En el caso de las tarjetas controladoras de las incubadoras de neonatos, la seguridad es un aspecto vital, ya que cualquier fallo en el control de la temperatura, el oxígeno o la humedad podría poner en peligro la vida del neonato. Por esta razón, es fundamental realizar pruebas rigurosas para identificar posibles vulnerabilidades en la seguridad de la tarjeta y corregirlas lo antes posible.

PERSPECTIVA METODOLÓGICA

En lo referente a la perspectiva metodológica corresponde a un enfoque ontoepistemológico que se asume desde el paradigma positivista, con basamento en una investigación aplicada, sustantiva, de tipo tecnológico, bajo el enfoque de proyecto especial. Según Esteban (2018):

> La investigación aplicada o de carácter tecnológico es otro tipo de investigación científica que conduce a la trasformación material de las sociedades en el mundo. Esta se divide en investigación sustantiva que llega a ser plasmada en prototipos, y la investigación operativa que tiene que ver con los sistemas y enlaces virtuales y físicos que han experimentado un vertiginoso desarrollo en las ciencias de la comunicación e información (p. 18)

Así pues, la investigación aplicada implica el uso de conocimientos teórico-científicos para resolver problemas prácticos en campos específicos. Otro aspecto atinente al estudio es el enfoque de proyecto especial, definido en el Manual de Trabajos de Grado, de Especializaciones y Maestrías y Tesis Doctorales de la Universidad Pedagógica Experimental Libertador (2016) como:

> Trabajos que lleven a creaciones tangibles, susceptibles de ser utilizadas como soluciones a problemas demostrados, o que respondan a necesidades e intereses de tipo cultural. Se incluyen en esta categoría los trabajos de elaboración de libros de texto y de materiales de apoyo educativo, el desarrollo de software, prototipos y de productos tecnológicos en general, así como también los de creación literaria y artística (p.55).

En este caso el estudio involucra la aplicación de la ingeniería inversa y la construcción de un prototipo de tarjeta controladora

con la finalidad de solucionar un problema práctico. El estudio estuvo enmarcado en la línea de investigación de la UNEFA Ingeniería, Tecnología e Innovación que busca estimular y promover actividades de investigación, desarrollo e innovación tecnológica orientadas al fortalecimiento del desarrollo social del país.

RESULTADOS

Una vez estudiadas las características de la incubadora neonatal que implicó medir la temperatura de la cúpula, la temperatura del neonato, la humedad, mantener al recién nacido en un ambiente ideal, se procedió a cambiar el módulo de control a través de un microcontrolador Arduino 1.

Entonces se colocaron los sensores, se programaron los set point, de peso y de temperatura, es decir la máxima y mínima temperatura que pueden tener el ambiente y el neonato; los parámetros de humedad y se procedió a programar en lenguaje C, que implica llamar librerías, realizar procedimientos y funciones que realicen el sistema de control completo, cuando pasa la temperatura, qué se debe encender para bajar la temperatura; cuando la temperatura baja, qué se debe hacer para que la temperatura suba, y que no pase de un valor extremo porque se está trabajando con vida humana, por lo que tiene que tener diversos filtros que permitan que no sobrepasen los niveles de temperatura requeridos y tener beeper o alarmas que indiquen a través de sonidos que hay una situación irregular dentro de los parámetros permitidos. En concordancia con lo anterior, Bustamante, J y Cevallos, A (2013) expresan:

> Una de las variables a controlar dentro de la incubadora es la temperatura, su regulación es esencial puesto que todos los recién nacidos son muy sensibles a los cambios de temperatura. Una disminución de la misma puede ocasionar adormecimiento de los recién nacidos, dificultad para tomar, etc. (p.9).

El sistema de control monitorea la temperatura, pero controla que no supere los niveles establecidos en la programación. Eso se hace a través del microcontrolador de la placa Arduino 1, con los sensores necesarios, sensores de temperatura, sensores de humedad, sensores de ambiente y lo que es más importante, el supervisor de la corriente eléctrica para que una vez que se interrumpa la energía de la red de alimentación, pues se alimente el equipo a través del sistema de baterías. Esto, se hace a través de un inversor de polaridad, por medio del cual se puede cambiar a corriente del banco de baterías. Según Restrepo y otros (2007):

> La fuente de poder constituye la fuente de alimentación de los componentes eléctricos de la incubadora; para ello debe convertir el voltaje de corriente alterna (Vac) que suministra la red de alimentación eléctrica (aproximadamente 110V a 60Hz) a un voltaje de corriente directa de 5V (p. 56).

Esto es muy importante, ya que, a la hora de un apagón o una situación de fluctuación de energía, aunque los hospitales están dotados de plantas eléctricas de emergencia; pero se debe prever cualquier falla y el sistema de control debe monitorear la situación y si no hay energía eléctrica debe pasar al banco de baterías. Ese es el sistema de control que se realizó. Adicionalmente, se diseñó una fuente de poder completamente adaptable al Sistema Eléctrico Nacional venezolano, que tiene sus fluctuaciones y variables, inconsistencias; muy diferente por ejemplo al sistema eléctrico chino donde el pulso o la señal es

completamente sinusoidal y no hay fluctuaciones significantes. Tal como lo plantean Restrepo y otros (ob. Cit):

> La corriente que llega de la red eléctrica sufre variaciones de voltaje en su línea de tiempo. Lo que se busca con esta fase, es pasar de voltaje de corriente alterna a voltaje de corriente continua, a través de un puente rectificador o de Grates. El rectificador elimina el componente negativo de la onda sinusoidal. (p. 56).

Las pruebas que se hicieron incluyeron programar el Arduino, además cortar el fluido de energía eléctrica buscando someter el equipo a fluctuaciones de energía para monitorear el comportamiento del sistema. Se calentó el ambiente de la cúpula de la incubadora, superior a 36 º, para que el sistema de control la bajara a través del encendido de un ventilador tipo extractor que se encendía automáticamente para bajar la temperatura y cuando la temperatura subía con una foto resistencia a través de un dimmer, se subía la temperatura.

La Humedad también se sometió a pruebas, creando o bajando la humedad de acuerdo con los parámetros establecidos. Tal como recomiendan Zamorano-Jiménez y otros (2012) la humedad o humidificación:

> Es el proceso de agregar humedad de manera artificial sobre la que se encuentra en el ambiente, el término comúnmente utilizado para la humedad proporcionada por una incubadora es humedad relativa. Existe cierta renuencia en utilizar la humedad relativa en el manejo de los RN debido a los problemas en la limpieza y la regulación de la humedad junto con el riesgo de infección (p. 45)

De lo anterior se deduce que se debe tener especial cuidado en la programación de los parámetros requeridos por los pacientes

recién nacidos y la asepsia de los componentes e insumos a emplear. Pero también, una de las ventajas de utilizar Arduino como placa controladora de una incubadora de neonatos es su versatilidad. Cualquier Arduino puede ser programado y configurado para controlar la temperatura, la humedad y la concentración de oxígeno. Además, las placas controladoras de Arduino son fáciles de conseguir en cualquier tienda de electrónica y su reparación y mantenimiento son mucho más sencillos y económicos.

CONCLUSIONES

La experiencia de aplicar ingeniería inversa al módulo de control de una incubadora neonatal desincorporada en un centro asistencial del sector salud del estado Lara, significó poder poner en práctica la idea de que el conocimiento tecnológico se puede llevar a la praxis venciendo la dependencia técnica especializada, validando la apropiación del saber científico y la investigación desde la universidad.

Al momento de identificar los materiales físicos y lógicos para el diseño del prototipo de la incubadora se decidió trabajar con un Arduino 1, la tarjeta cuya placa de microcontrolador es de código abierto basado en el microchip ATmega328P que puede ser programada en lenguaje C.

Lo expuesto, nos sumergió en ese proceso investigativo, metodológico y práctico, donde se definieron las condiciones técnicas de diseño, los componentes físicos estructurales y los requisitos de programación que configuran el prototipo de tarjeta controladora para la incubadora neonatal, considerando con

suma atención y cuidado los parámetros de humedad, temperatura, peso y ambiente, los cuales condicionan el éxito operativo de las incubadoras neonatales.

Finalmente, se elaboró un prototipo según especificaciones técnicas de diseño que cuenta con una placa Arduino, que es capaz de medir, controlar y mantener la temperatura dentro de la incubadora neonatal en un rango seguro y estable; en tanto puede regular los niveles de humedad dentro de la cúpula de la incubadora para crear un ambiente adecuado para el neonato. Los sensores de temperatura y humedad miden y monitorean constantemente las condiciones dentro de la incubadora. Este incluye actuadores como ventiladores y resistencias para ajustar la temperatura y la humedad según sea necesario.

RECOMENDACIONES

Realizar la debida certificación del prototipo de la tarjeta controladora de la incubadora ante el ministerio de Salud.

Conformar un equipo multidisciplinario en la UNEFA para desarrollar investigación en torno a la electromedicina y áreas relacionadas con la reparación de equipos médicos e ingeniería inversa.

A los gerentes hospitalarios se recomienda formar a los médicos y enfermeras en el manejo y manipulación de estos equipos que son de vital importancia para la vida de los neonatos prematuros.

REFERENCIAS BIBLIOGRÁFICAS

Acevedo, G. y otros. (2017). *Sistema e-Salud para el monitoreo de un prototipo de incubadora neonatal*. Venezuela. Universidad de los Andes. Ciencia e Ingeniería, vol. 38, núm. 2, 2017.

Acevedo, J. y Puma, E. (2007). *Ingeniería inversa aplicado a sistemas desarrollados con programación orientada a objetos para obtener la documentación*. Perú. Universidad Nacional Mayor de San Marcos.

Betancur, M. (2011). *Ingeniería Inversa Aplicada: Metodología y Aplicaciones Industriales*. Colombia, Medellín. Universidad EAFIT Escuela de Ingeniería Especialización en Diseño Mecánico.

Bustamante, J. y Cevallos, A. (2013). *Diseño e Implementación de un Prototipo de Incubadora Neonatal en Cumplimiento con la Norma UNE-EN 60601-2-19*. Ecuador. Universidad Politécnica Salesiana Sede Cuenca.

Cabrera, A. y otros. (2020). *Un modelo de minimización de costos de mantenimiento de equipo médico mediante lógica difusa*. México. Revista mexicana de economía y finanzas. versión On-line ISSN 2448-6795versión impresa ISSN 1665-5346.

Esteban, N. (2018). *Tipos de Investigación*. Perú. Universidad Santo Domingo de Guzmán.

Hamad, P. (2009). *La Abducción como punto de Partida en el Desarrollo del Pensamiento Científico en Estudiantes de Química en la Fase Experimental*. Colombia. Horizonte Pedagógico. Volumen 11. Nº 1. 2009 / págs. 49-54

Jiménez, E. y otros. (2010). *La Ingeniería Inversa como*

Metodología para Potenciar la Enseñanza de la Metrología. México. Simposio de Metrología 2010.

López, A. (2021). *Ingeniería inversa para recuperación de equipos médicos ha sido clave*. Barcelona. INCE.

Manual de Trabajos de Grado de Especialización, Maestrías y Tesis Doctorales. Universidad Pedagógica Experimental Libertador Vicerrectorado de Investigación y Postgrado, Fondo Editorial de la Universidad Pedagógica Experimental Libertador (FEDUPEL), Caracas, Venezuela. (2016).

Pólya, G. (1965). *Cómo resolverlo*. España. Editorial Trillas.

Polya, G. (1989). *Cómo plantear y resolver problemas*. España. Editorial Trillas.

Ramos, D. (2013). *Uso de la Ingeniería Inversa como metodología de enseñanza en la formación para la innovación*. Bogotá, Colombia. Escuela Colombiana de Ingeniería Julio Garavito.

Restrepo, L. y otros. (2007). *Prototipo de Incubadora Neonatal*. Bogotá. Revista Ingeniería BiomédicaPrint version ISSN 1909-9762Rev. ing. Biomed. Vol.1 No.1. Medellín Jan. /June 2007

Zamorano-Jiménez, C. y otros. (2012). *Control térmico en el recién nacido pretérmino*. México. Instituto Nacional de Perinato.

ROBOT INTELIGENTE CON FINES EDUCATIVOS PARA LA DIDÁCTICA DE LA INTELIGENCIA ARTIFICIAL

Coautores: Ing. Juan Emiro Mora Arcila
Dra. Ismenia María Suárez Finol
Institución: Universidad Nacional Experimental Politécnica de la Fuerza Armada Nacional Bolivariana (UNEFA). Núcleo Lara
Correos: morajuan24@gmail.com
ismeniasuarezunefalara@gmail.com

RESUMEN

La inteligencia artificial (IA) es una tecnología que está revolucionando la manera en que las personas interactúan y ejecutan tareas. Por ello, es importante que los estudiantes universitarios desarrollen su formación en esta área de manera práctica y heurística para poder afrontar los desafíos y oportunidades que esta realidad ofrece. Sin embargo, la falta de herramientas para una didáctica de la IA en muchas universidades puede convertirse en un problema que dificulta su enseñanza y aprendizaje. El presente estudio tuvo como propósito diseñar un robot inteligente con fines educativos para la didáctica de la inteligencia artificial. Se tomó como basamentos teóricos la teoría de la complejidad de Morín y el modelo conectivista de Siemens.Desde el punto de vista metodológico se basó en una investigación aplicada de tipo tecnológica, con la construcción de un prototipo de robot; y enmarcada en la línea de investigación de la UNEFA: Ingeniería, Tecnología e Innovación. Se llegó a la conclusión que luego de realizar las interacciones necesarias, el robot logró aprender y ampliar su base de conocimiento para tomar control sobre los valores iniciales indicados (pasos propios). Se recomienda mejorar el diseño de hardware para crear el modelo de robot con materiales apropiados.

Palabras clave: Robot inteligente, didáctica, inteligencia artificial.

INTELLIGENT ROBOT WITH PURPOSES EDUCATIONAL FOR THE DIDACTIC OF THE ARTIFICIAL INTELLIGENCE

ABSTRAC

Artificial intelligence (AI) is a technology that is revolutionizing the way people interact and perform tasks. Therefore, it is important that university students develop their training in this area in a practical and heuristic way in order to face the challenges and opportunities that this reality offers. However, the lack of tools for AI didactics in many universities can become a problem that makes teaching and learning difficult. The purpose of this study was to design an intelligent robot for educational purposes for the didactics of artificial intelligence. Morín's theory of complexity and Siemens' connectivist model were taken as theoretical foundations. From the methodological point of view, it was based on applied technological research, with the construction of a robot prototype; and framed in the research line of UNEFA Engineering, Technology and Innovation. It was concluded thatafter performing the necessary interactions, the robot was able to learn and expand its knowledge base to take control over the initial values indicated (own steps).It is recommended to improve the hardware design to create the robot model with appropriate materials.

Keywords: Intelligent robot, didactics, artificial intelligence.

INTRODUCCIÓN

La Inteligencia Artificial (IA) resulta de la combinación de algoritmos diseñados con el propósito de crear artefactos que ostenten capacidades similares a las del ser humano. Una tecnología que ha venido a revolucionar la vida del ser humano y que le plantea retos éticos, pero que desde hace unos años está presente en su vida cotidiana. La inteligencia artificial resulta de la aspiración de otorgarle capacidad de imitar la inteligencia humana a las máquinas, asunto que supone un

inquietante peligro para quienes abrigan sospechas negativas en cuanto a su uso; pero lo cierto es que no son los robots los que toman las decisiones, sino las personas a la hora de diseñarlos e integrar robots con inteligencia artificial. Tal como plantea Pardiña (2020):

> Los argumentos que se encuentran en el debate van desde la denuncia de la destrucción de puestos de trabajo, la repercusión de los intereses de los sectores más privilegiados, la falta de privacidad de los datos personales, o incluso si es posible que pueda llegar a ser más inteligente y eficiente que un ser humano. (p. 6)

De acuerdo con lo anteriormente citado, existe la creencia de que las máquinas o robot con inteligencia artificial van a ir sustituyendo poco a poco puestos de trabajo de las personas y hasta superar su inteligencia; pero lo cierto es que el uso de la robótica no debe ser excluyente, sino complementario en las acciones y vida de los seres humanos. Es decir, lo que se impone es cómo conseguir que los robots sean auxiliares de las personas en la tarea de hacer su trabajo con eficacia y eficiencia. La misma Pardiña (opcit) explica:

> Actualmente, la Inteligencia Artificial forma parte de nuestro día a día, y la mayoría de sus aplicaciones están destinadas a mejorar y facilitar nuestra vida. El ejemplo más cercano y claro es el de los teléfonos móviles. Y es que es a través de la IA que los teléfonos pueden realizar reconocimientos faciales y de voz, de escritura o de patrones, así como mejorar la calidad de las fotografías. Otros usos comunes son los motores de búsqueda o las sugerencias de contenido en diversas plataformas. (p. 5).

En tal caso, los robots con inteligencia artificial pueden tener múltiples usos y estar enfocados a realizar actividades que resulten peligrosas a las personas. Por ejemplo, en las

empresas pueden sustituir a los trabajadores en tareas de riesgo o que supongan grandes esfuerzos; también para que no se cometan errores en actividades que ameriten precisión y así contribuyan a mejorar el ambiente laboral en las empresas. Así pues, la robótica se puede considerar como una herramienta para diversas áreas de la vida social de las personas en la actualidad.

Específicamente en el área educativa la IA brinda una cantidad de alternativas para simular los comportamientos en las actividades de los seres humanos siendo esto un preludio a la educación altamente tecnificada. En consecuencia, la IA está cada vez más presente en vida diaria de la gente y en la actualidad está generando un impacto significativo en la sociedad y la economía. Por lo tanto, es importante que los estudiantes desarrollen habilidades en el campo de la IA para tener éxito en la gestión del conocimiento y para asegurar la competitividad de los países en el mercado global. En opinión de García-Peñay otros (2020):

> El nuevo modelo pedagógico conectivista plantea las nuevas habilidades necesarias en los individuos que forman parte de la sociedad del conocimiento, según Siemens (2006) son: anclarse, filtrar la información, conectarse entre sí, ser humanos juntos, evaluar el valor del conocimiento, pensamiento crítico constante, reconocimiento de patrones y tendencias, capacidades de resiliencia y adaptación. (p. 650).

Desde esa perspectiva, el aprendizaje conectivista es un enfoque o modelo de aprendizaje que se basa en la creación de redes de conocimiento y la conexión de los aprendices con los recursos y las personas que los rodean y que exige del individuo emplear de manera cuidadosa la información, además de

poseer pensamiento crítico y capacidad de resiliencia. Por ello el aprendizaje sobre inteligencia artificial también puede ayudar a los estudiantes a mejorar su pensamiento crítico, resolución de problemas y habilidades creativas. Los estudiantes pueden aprender a analizar grandes cantidades de datos y encontrar patrones para tomar decisiones informadas, lo que puede ser útil para resolver problemas en diversos campos del conocimiento, lo que amerita el desarrollo de una didáctica para la IA.

En tal sentido, en cuanto a la didáctica de la IA se refiere a la enseñanza y el aprendizaje de los conceptos y habilidades relacionados con la inteligencia artificial. Esta disciplina se enfoca en cómo enseñar a los estudiantes los fundamentos de la IA, la programación y el análisis de datos para crear aplicaciones y sistemas de inteligencia artificial. Por ejemplo, los estudiantes pueden aprender a programar y controlar robots que realizan tareas simples como mover objetos de un lugar a otro, siguiendo una línea o evitando obstáculos en su camino. También pueden aprender a diseñar y programar robots más complejos que pueden interactuar con los seres humanos, como robots de asistencia médica o de atención al cliente. Domínguez y otros (2022) señalan:

> La aplicación de la robótica ha sido mencionada por diversos investigadores como una tecnología con potencial significativo para impactar en la educación. La definición actual del campo es todavía vaga y abierta a cualquier interpretación, lo que hace posible que se la utilice sin tener en consideración el objetivo real de la Robótica Educativa. (p. 68).

Así pues, la enseñanza de la inteligencia artificial en las universidades puede preparar a los estudiantes para el futuro,

proporcionándoles las habilidades y el conocimiento requeridos para tener éxito en una sociedad cada vez más tecnológica. De allí que la necesidad de formar en parámetros de inteligencia artificial a nuevos profesionales debe verse como una respuesta ante el rápido crecimiento e importancia de la apropiación y producción de tecnología y de los diversos conceptos y disciplinas, tales como algoritmos de aprendizaje automático, redes neuronales, lógica difusa, sistemas expertos, minería de datos, y procesamiento de lenguaje natural, entre otros.

Por ello, la presente investigación tuvo como objetivo general diseñar un robot inteligente con fines educativos para la didáctica de la inteligencia artificial, a fin de poder demostrar de manera pragmática que con los conceptos de robótica e inteligencia artificial se pueden construir robots agregándoles memoria y esto hace que se conciba un nuevo concepto denominado organismo artificial, capaz de comportarse y aprender del medio dotado de capacidades de toma de decisiones para resolver problemas de cualquier índole.

En tal sentido, los objetivos específicos consistieron en sistematizar la información referente a la inteligencia artificial aplicada a un robot inteligente, posteriormente, determinar los elementos constitutivos de la robótica con el fin del desarrollo de un robot inteligente, construir el robot con servomotores al que se le dio el nombre de Kippoy finalmente validar la propuesta por la vía de expertos.

El estudio estuvo sustentado en la teoría de la complejidad y el modelo conectivista. Además, desde el punto de vista metodológico se basó en una investigación aplicada de tipo tecnológica, con la construcción de un prototipo y siguiendo la

línea de investigación de la UNEFA Ingeniería, Tecnología e Innovación, cuyo propósito consiste en desarrollar y promover conocimientos científicos y tecnológicos tendientes a la solución de problemas de la sociedad venezolana, que permitan avanzar en la independencia tecnológica, la inclusión social y el progreso de capacidades nacionales en pro del desarrollo endógeno, sustentable y humano del país. (Documento de las Líneas de Investigación UNEFA, 2012).

En cuanto a la delimitación, el estudio se circunscribe a la construcción de un prototipo de robot (llamado Kippo), construido con servomotores y sensores, tomando en cuenta los parámetros iniciales dirigidos para obtener los resultados de los procesos propios de la inteligencia artificial, enfocado en el uso de los algoritmos del aprendizaje automatizado (machine learning) y el aprendizaje profundo (deeplearning) bajo un concepto de 5 valores iniciales (pasos).

El presente estudio se justifica ante la necesidad de contar con herramientas didácticas para la enseñanza de los elementos teóricos y prácticos de las tecnologías emergentes. En ese sentido, al emplear robots para la enseñanza de la inteligencia artificial se facilita el aprendizaje a los discentes sobre la visión por computadora, redes neuronales, lógica difusa, sistemas expertos, el aprendizaje automático, y otros conceptos en un ambiente para el desarrollo de la praxis y la didáctica para la tecnología. También pueden aprender sobre la programación y el diseño de robots, lo que constituye un aprendizaje útil en una variedad de aplicaciones en el campo tecnológico, empresarial y educativo.

REFERENCIAS TEÓRICAS Y PERSPECTIVAS METODOLÓGICAS

El presente estudio tuvo como basamento la teoría de la complejidad de Morín y el modelo conectivista de Siemens. Dado que la inteligencia artificial busca crear sistemas capaces de aprender y adaptarse a su entorno a través del procesamiento de grandes cantidades de datos y el uso de algoritmos y redes neuronales, se comprende que estos sistemas inspirados en el funcionamiento del cerebro humano, constituyen también un sistema complejo y dinámico. Tal como plantea Morín (1999):

> Las unidades complejas, como el ser humano o la sociedad, son multidimensionales; el ser humano es a la vez biológico, síquico, social, afectivo, racional. La sociedad comporta dimensiones históricas, económicas, religiosas… El conocimiento pertinente debe reconocer esta multidimensionalidad e insertar allí sus informaciones… (p.16).

El autor resalta el carácter multidimensional del conocimiento actual. Morín destaca en su teoría que el mundo no puede ser comprendido de manera simple, ya que se compone de múltiples sistemas y elementos interdependientes, lo que lo convierte en una entidad compleja y dinámica. Asimismo, señala que es necesario tomar en cuenta tanto los aspectos objetivos como subjetivos de estos sistemas para poder comprenderlos de manera adecuada.

De allí que, la inteligencia artificial, a la luz del pensamiento de Morín, constituye un sistema complejo con interconexión e interdependencia de los elementos dentro de un sistema. Se busca avanzar en la comprensión de los sistemas complejos y

promover la creación de sistemas más eficientes y adaptables en el futuro. En expresión de Balladares y otros (2016):

> La complejidad, gracias al aporte de Morín, es el espacio apropiado de integración de expresiones diversas y de nuevas relaciones simbólicas el espacio propicio para reflexionar sobre el futuro de la educación a partir de la mediación de las tecnologías de la información y comunicación, las redes sociales y el internet. En este sentido, el pensamiento computacional aparece como una alternativa de estas nuevas expresiones del pensamiento. (p. 148).

De acuerdo con lo anterior, la aplicación del pensamiento complejo en la educación puede ayudar a los estudiantes a comprender la complejidad de los sistemas y a desenvolverse en un mundo versátil, diverso y globalizado, caracterizado por la incertidumbre y los descubrimientos de la era digital. El pensamiento complejo se enfoca en la comprensión de las interacciones y relaciones entre los elementos de un sistema, y ayuda a los estudiantes a cuestionar sus propias representaciones, a considerar diferentes perspectivas y a tomar decisiones informadas.

En este sentido, se fomenta el aprendizaje autónomo en el que se espera que cada persona sea capaz de crear y mantener sus propias redes de conocimiento, acceder a recursos y desarrollar habilidades para filtrar y gestionar la información. En tal caso, el aprendizaje conectivista tiene basamento en la teoría de la complejidad y se enfoca en la adaptación, el aprendizaje continuo y el desarrollo de habilidades para aprender en un entorno cambiante y complejo.

Por otra parte, el aprendizaje conectivista es un enfoque o

modelo de aprendizaje que se basa en la creación de redes de conocimiento y la conexión de los aprendices con los recursos y las personas que los rodean. Este modelo propuesto por George Siemens es uno de los más influyentes dentro del campo de la educación y la tecnología. Conocido como teoría del conectivismo, sostiene que el aprendizaje es un proceso que se produce a través de la conexión entre diferentes personas, entornos y recursos. Tal como Siemens (2004) expresa:

> El conectivismo es la integración de principios explorados por las teorías de caos, redes, complejidad y autoorganización. El aprendizaje es un proceso que ocurre al interior de ambientes difusos de elementos centrales cambiantes – que no están por completo bajo control del individuo.

De acuerdo con lo anterior, la conectividad según Siemens siempre ha sido una característica fundamental de la humanidad y, por lo tanto, el aprendizaje ha tenido lugar a lo largo de la historia gracias a la interacción entre individuos y comunidades. Sin embargo, gracias a las nuevas tecnologías de la información y la comunicación, la conectividad ha adquirido una dimensión sin precedentes en la actualidad.

Este modelo propone que el aprendizaje ya no se limita al aula o al entorno escolar, sino que puede ocurrir en cualquier lugar donde haya acceso a la información y a otras personas que puedan compartir conocimientos y experiencias. Los recursos y herramientas tecnológicas juegan un papel fundamental en la creación de redes de aprendizaje y en la posibilidad de acceder y compartir información en tiempo real. El mismo Siemens (opcit) explica:

> El conectivismo presenta un modelo de aprendizaje que

> reconoce los movimientos tectónicos en una sociedad en donde el aprendizaje ha dejado de ser una actividad interna e individual. La forma en la cual trabajan y funcionan las personas se altera cuando se usan nuevas herramientas. (p. 10).

Según el autor precitado, el aprendizaje ha dejado de ser una actividad interna e individual, porque es el resultado de la capacidad del individuo para navegar y crear conexiones dentro de una red de conocimiento. En este sentido, el papel del educador es el de un facilitador que ayuda a los estudiantes a comprender el mundo en red en el que viven, les brinda herramientas y recursos para desarrollar habilidades y les ayuda a construir conexiones significativas con otros individuos y comunidades. Tal como lo expresan Padrón y Ortega (2012):

> Las redes de aprendizaje autoorganizado proporcionan una base para el establecimiento de una forma de educación que va más allá de los modelos centrados en el currículo y los cursos, y proponen un modelo de aprendizaje continuo centrado en el estudiante y controlado por el propio usuario. En lugar del aprendizaje alojado en sistemas de gestión de contenido, el aprendizaje se incrusta en espacios conversacionales yen redes que se enriquecen con la participación y la colaboración. (p. 36)

En correspondencia con lo anterior, la conectividad de Siemens propone que el aprendizaje no es sólo un proceso individual, sino que es el resultado de la interacción entre individuos, comunidades y recursos en un entorno digital y globalizado. Este modelo ha tenido una gran influencia en la forma en que se concibe la educación en la actualidad y ha llevado a una mayor exploración de herramientas y tecnologías que permitan el aprendizaje en red y la creación de comunidades de aprendizaje en línea.

Desde el punto de vista metodológico el estudio que acá se presenta se basó en una investigación aplicada de tipo tecnológica, con la construcción de un prototipo de robot. Este tipo de investigación se centra en la aplicación sistemática de conocimientos científicos, habilidades técnicas y recursos para el desarrollo de soluciones innovadoras. Según plantea Silva (2020):

> Se puede afirmar que el desarrollo tecnológico ha representado la principal palanca de transformación en el mundo de hoy, alterando de manera significativa la forma de investigar para obtener el conocimiento. Esta alteración, deviene en la aplicación de un nuevo paradigma que se preocupa más por transformar la realidad; que por darle una explicación teórica a través de la innovación tecnológica. (p. 86).

En ese sentido, la investigación tecnológica tiene un carácter pragmático, es decir, a partir de una necesidad, carencia o un problema, se busca presentar una solución, buscando la innovación de los procesos sobre la base del basamento teórico existente del conocimiento empírico, implementando una solución tecnológica mediante un prototipo, producto o solución resultado de la investigación.

KIPPO: ROBOT INTELIGENTE Y DIDÁCTICA DE LA INTELIGENCIA ARTIFICIAL

En función de generar un aporte a la didáctica de la inteligencia artificial se elaboró el prototipo de un robot al que se le dieron instrucciones de 5 valores iniciales (pasos). De modo General, el robot desarrollado, está compuesto por una placa Arduino y 4 servomotores, uniendo de esta manera 4 áreas como lo son la

robótica, la programación, la electrónica y la Inteligencia artificial, siendo esta última una de las más importantes al momento de que un robot sea autónomo en sus decisiones. Al construir un robot los estudiantes no solo aprenden cómo funcionan los sensores y los controladores: sino que pueden aprender cómo se pueden programar para que tomen decisiones y realicen acciones en función de la información que recopilen.

Para ello, se diseñó un robot inteligente construido a partir de servomotores y una placa Arduino, que además consta de varios elementos constitutivos, a saber:

Servomotores: Son motores que se pueden controlar con precisión mediante un pulso de voltaje. Estos motores son ideales para la construcción de robots ya que permiten controlar la posición y velocidad de diferentes partes del robot.

Placa Arduino: Es una placa electrónica que se utiliza para controlar el robot. La placa Arduino es programable y se puede conectar a diferentes sensores y actuadores para permitir que el robot pueda interactuar con el entorno.

Sensores: Son dispositivos que se utilizan para medir diferentes variables del entorno, como la luz, el sonido, la temperatura, la presión, etc. Los sensores son esenciales para que el robot pueda percibir y reaccionar al entorno.

Actuadores: Son dispositivos que se utilizan para mover diferentes partes del robot. Los servomotores son actuadores que se utilizan para controlar la posición y velocidad de las articulaciones del robot.

Software: Es el conjunto de instrucciones que se utilizan para controlar el comportamiento del robot. El software se ejecuta en la placa Arduino y se puede programar en lenguajes de programación como C o C++.

Fuente de energía: Es un elemento esencial para el funcionamiento del robot. La fuente de energía puede ser una batería o un adaptador de corriente que se conecta a la placa Arduino para alimentar los servomotores y otros componentes electrónicos del robot.

El proceso de construir un robot con fines educativos implicó varias etapas, desde la planificación del diseño hasta la construcción y programación. En este sentido, se utilizó la robótica colaborativa, que pretende dar respuesta a las necesidades de la sociedad, la vida empresarial y cotidiana, convirtiendo las soluciones colaborativas en el perfecto ejemplo de convivencia entre robots y operarios compartiendo un mismo puesto de trabajo.

En este caso en particular, y a modo de prototipo inicial, se le puede dar diversidad de aplicaciones al Robot Kippo, tomando en cuenta que puede ser configurado según las necesidades que se requieran, por medio de actuadores o sensores que permitan resolver alguna necesidad en particular. La integración de estas aplicaciones es tan solo un ejemplo de la versatilidad que ofrecen para adaptarse a los casos de cada proceso productivo, mejorándolos, aumentando su productividad, reduciendo el índice de errores y en definitiva impulsando la competitividad de las empresas.

Las aplicaciones de la robótica, de la inteligencia artificial y de

la electrónica en diversos ámbitos humanos han venido reportando beneficios que pueden seguirse desarrollando.

En la educación, este prototipo puede diferenciarse de dos tipos de uso de la programación y la robótica como apoyo en la clase: por un lado, la robótica y la programación educacional, que consiste en un conjunto de elementos físicos o de programación que motivan a los estudiantes a construir, programar, razonar de manera lógica y crear nuevas interfaces o dispositivos; por otro, la programación y la robótica como elemento social, por ejemplo a modo de juego o gamificación, de forma que sistemas autónomos o semiautónomos interactúan con humanos u otros agentes físicos o software en roles como entrenador, compañero, dispositivo tangible o registro de información en donde luego de realizar las interacciones necesarias, el robot logró aprender y ampliar su base de conocimiento para tomar control sobre los valores iniciales indicados (pasos propios).

Es por esto que la inteligencia artificial (IA) está cambiando rápidamente la forma en que aprendemos y enseñamos. Los robots impulsados por IA se utilizan en la educación para brindar experiencias de aprendizaje personalizadas, automatizar tareas y crear entornos de aprendizaje atractivos e interactivos. Dentro de estos beneficios de usar robots impulsados por IA en la educación encontramos:

El aprendizaje personalizado, donde los robots impulsados por IA pueden seguir el progreso de los estudiantes y proporcionar experiencias de aprendizaje personalizadas que se adaptan a las necesidades individuales de cada estudiante. Esto puede ayudar a los estudiantes a aprender de manera más efectiva y eficiente.

Tareas automatizadas, en estos casos, los robots impulsados por IA pueden automatizar tareas que normalmente realizan los maestros, como calificar trabajos, crear planes de lecciones y realizar un seguimiento de la asistencia. Esto puede liberar el tiempo de los maestros para que puedan concentrarse en tareas más importantes, como brindar atención individualizada a los estudiantes.

Entornos de aprendizajes atractivos e interactivos, en donde los robots impulsados por IA pueden crear entornos de aprendizajes atractivos e interactivos que son más divertidos y motivadores para los estudiantes. Esto puede ayudar a los estudiantes a aprender de manera más efectiva y a retener mejor la información.

Sin embargo, también existen algunos desafíos asociados con el uso de robots impulsados por IA en la educación, como el costo, ya que los robots impulsados por IA pueden ser costosos de comprar y mantener. Esto puede ser una barrera para la educación que tienen un presupuesto ajustado.

Otra dificultad pudiera ser la aceptación, ya que algunos estudiantes pueden ser reacios a interactuar con robots impulsados por IA. Esto puede deberse al miedo a lo desconocido o a la falta de confianza en la tecnología. También se generan preocupaciones con respecto a lo ético. Por ejemplo, a algunas personas les preocupa que los robots impulsados por IA puedan usarse para discriminar a ciertos grupos de estudiantes o para recopilar datos sobre estudiantes sin su consentimiento.

Conclusiones

Se diseñó un robot inteligente con fines educativos para la didáctica de la inteligencia artificial, a fin de poder demostrar en la práctica que con los conceptos de robótica e inteligencia artificial se pueden construir robots, agregándoles memoria y esto hace que se conciba un nuevo concepto denominado organismo artificial, capaz de comportarse y aprender del medio, dotado de capacidades, de toma de decisiones para resolver problemas de cualquier índole. En este caso, se le dieron los pasos iniciales y el robot amplió su base de conocimiento y realizó otros pasos de manera autónoma.

Se sistematizó la información referente a la inteligencia artificial aplicada a un robot inteligente y en cuanto a los elementos constitutivos de la robótica con el fin del desarrollo de un robot inteligente se sintetiza en el uso de servomotores, placa Arduino, sensores, actuadores y el Software que exige lenguajes de programación como C o C++.

Recomendaciones

Al momento de diseñar un robot inteligente con fines educativos para la didáctica de la inteligencia artificial se debe mejorar el diseño de hardware para crear el modelo de robot con materiales apropiados.

Se recomienda crear laboratorios de electrónica y programación.

Dotar de los componentes requeridos para crear los robots.

REFERENCIAS BIBLIOGRÁFICAS

Balladares, A. y otros. (2016). *Del pensamiento complejo al pensamiento computacional: retos para la educación contemporánea*. Sophia, Colección de Filosofía de la Educación, núm. 21, julio-diciembre, 2016, pp. 143-159 Cuenca, Ecuador. Universidad Politécnica Salesiana.

Domínguez, L. y otros. (2022). *Diseño de prototipo de enjambre de robots como herramienta educativa de bajo costo*. Ecuador: Memorias de la Vigésima Primera Conferencia Iberoamericana en Sistemas, Cibernética e Informática (CISCI 2022).

García-Peña, V. y otros. (2020). *La inteligencia artificial en la educación*. México. Revista científica Las Ciencias. Vol. 6, núm. 3, Especial septiembre 2020, pp. 648-666.

Gutiérrez, L. (2012). *Conectivismo como teoría de aprendizaje: conceptos, ideas, y posibles limitaciones*. Revista Educación y Tecnología, N° 1, año 2012 / págs. 111-122.

Irigoyen, A. y Morales, H. (2013). *La obra de George Siemens: una alternativa para el aprendizaje en la era digital*. México. Archivos en Medicina Familiar. Vol.15 (4) 53-55.

Pardiñas, S. (2020). *Inteligencia Artificial: un estudio de su impacto en la sociedad.* España. Universidad de la Coruña.

Padrón, J. y Ortega, A. (2012). *La conectividad: Dogmatismo o nuevo referente paradigmático para el docente de vanguardia*. Universidad Pedagógica Experimental Libertador. Instituto Pedagógico de Caracas Revista de Investigación Nº 75 Vol. 36. Enero – abril 2012.

Siemens, G. (2004). *Conectivismo: Una teoría de aprendizaje*

para la era digital. Creative Commons 2.5. Traducido por Diego Leal. Bogotá, Colombia. Universidad de los Andes.

Silva, E. (2020). *Investigación Tecnológica. Concepción Metodológica en las Ciencias de la Ingeniería*. Revista RECITIUTM Revista Electrónica de Ciencia y Tecnología del Instituto Universitario de Tecnología de Maracaibo. ISSN: 2443-4426; Dep. Legal: PPI201402ZU4563 Vol. X N° X (20XX).

ANÁLISIS DE RIESGOS EN TAREAS DE MANTENIMIENTO PREVENTIVO EN LA EMPRESA P&T SERVICIOS PETROLEROS C.A.

Autor: MSc. Juan Carlos Albornoz Cañizales
Institución: Universidad Nacional Experimental Politécnica de la Fuerza Armada Nacional Bolivariana (UNEFA).
Núcleo Trujillo
Correos: ing.albornoz@gmail.com

RESUMEN

La presente Investigación tuvo como propósito analizar los riesgos en tareas de mantenimiento preventivo en la empresa P&T Servicios petroleros C.A., para lo cual se consultaron varios autores en los que destacan: Cortés (2018), Covenin 3049-93, Duffaa (2018), entre otros. Metodológicamente, fue de tipo descriptivo, siendo el diseño combinado, documental y de campo; la población fue de 24 sujetos relacionados con las tareas de mantenimiento preventivo, quedando la muestra conformada por la misma cantidad al ser la misma de fácil acceso para el estudio. Se diseñó un cuestionario tipo encuesta conformada por 59 ítems de tipo cerrado, con dos alternativas de respuesta, validado según el juicio de los expertos, para determinar la confiabilidad se utilizó el coeficiente Alpha de Cronbach que arrojo un valor de 82%. Los resultados obtenidos fueron procesados a través de herramientas de estadística descriptiva, presentados en tablas y gráficos, incluyendo las herramientas de calidad de gestión, como el diagrama causa-efecto y de paretto. En el diagrama Causa-Efecto se identificaron las causas que originan los riesgos y que se analizan para tomar medidas respectivas. Con los diagramas de Pareto se establecen los riesgos y la forma como se jerarquizan los mismos, de acuerdo a los de mayor frecuencia de ocurrencia. Finalmente, se determinó en base a los resultados que el riesgo ergonómico debe considerarse de manera primordial, para disminuir la mayoría de las causas que lo produce.

Palabras clave: Riesgos, Mantenimiento.

RISK ANALYSIS IN PREVENTIVE MAINTENANCE TASKS IN THE P&T OIL SERVICES COMPANY C.A.

ABSTRAC

The present Investigation had as intention analyze the risks in tasks of preventive maintenance in the company P&T petroleum Services C.A., for which several authors consulted in those who stand out: Polite (2018), Covenin 3049-93, Duffaa (2018), between others. Methodologically, it was of descriptive type, being the design combined, documentary and of field; the population was 24 subjects related to the tasks of preventive maintenance, staying the sample shaped by the same quantity to the being same of easy access for the study. A questionnaire designed type he polls shaped by 59 articles of closed type, with two alternatives of response, validated according to the judgment of the experts, to determine the reliability Alpha de Cronbach was in use the coefficient that I throw a value of 82 %. The obtained results were processed across tools of descriptive statistics, presented in tables and graphs, including the qualit tools of management, as the graph reason - effect and of pareto. In the graph Reason - effect identify the reasons that originate the risks and that are analyzed to take respective measurements. With Pareto's graphs the risks and the form are established since the same ones are organized into a hierarchy, in agreement to those of major frequency of occurrence. Finally, it decided on the basis of the results that the ergonomic risk must consider in a basic way, to diminish the majority of the reasons that it it produces.

Keywords: Risks, Maintenance.

INTRODUCCIÓN

El ser humano constantemente está realizando una labor y por tal motivo entra en interacción con el medio que lo rodea. En ciencias sociales y en sentido estricto, trabajo o labor diaria es la actividad humana que responde a un fin productivo, o sea, que intenta resolver problemas concretos que tiene el hombre.

Se deduce por ello, que de todas las actividades que ejerce el individuo, las más importantes son las profesionales, ya que responden a lo más perentorio como lo es: la cobertura de las necesidades. Sin embargo, el ejercicio del trabajo está inmerso en una serie de riesgos que colocan en peligro la salud del trabajador, particularmente, sino se cumplen con las medidas de seguridad pertinentes.

Es ampliamente conocido que en la actualidad ocurren accidentes de toda fuente de trabajo, pero al manejar la habilidad de prevención y la conciencia de seguridad los índices disminuirán, observando así la reducción de los riesgos. En la vida cotidiana laboral se encuentran insertos todo tipo de riesgos llevando a la empresa hacer cualquier tipo de estudios y análisis de los posibles riesgos a los que está expuesto el talento humano; para la dotarlos con equipos de protección personal.

En ese sentido, el riesgo se conoce como la probabilidad de ocurrencia de un evento no deseado, tal como un accidente de trabajo o una enfermedad profesional que pueden afectar la salud de los trabajadores con deterioro de la productividad, debido a que el accidente (Cortés, 2018) se refiere a un acontecimiento no deseado, ni planificado que interrumpe o interfiere un proceso o el desarrollo normal de una actividad, y que puede generar una lesión a una persona, daños a la propiedad, materiales y equipos; generalmente la enfermedad profesional es causada a través del contacto con un riesgo ocupacional (ruido, calor, deficiente iluminación, etc.) de un determinado proceso u ofició, donde el trabajador está obligado a laborar.

En la práctica y a nivel industrial existen dos tipos de riesgos, los operacionales (eléctricos, mecánicos, entre otros.) que están presentes en las actividades, operaciones o mantenimientos que se realizan en un momento dado, y los riesgos ocupacionales (químicos, biológicos, ergonómicos, físicos, entre otros.) que se pueden encontrar en el ambiente, donde se efectúan dichas actividades, mantenimientos u operaciones.

Partiendo de esa premisa y de la probabilidad de ocurrencia de un evento no deseado, es pertinente observar, analizar, identificar, establecer y proponer medidas que conlleven a evitar que algún trabajador padezca accidentes, lesiones o enfermedades profesionales como consecuencia de los riesgos en tareas de mantenimiento. En tal sentido, el orden, el método y los sistemas de trabajo, son elementos claves para prevenir accidentes industriales.

Dicho lo anterior y Tomando como referencia la importancia de la prevención de riesgos, como garantía para la disminución de accidentes en el trabajo y evitar las enfermedades profesionales, se realizó la presente investigación de tipo descriptiva, con diseño de campo con el objetivo de analizar los riesgos en tareas de mantenimiento preventivo en la empresa P&T Servicios Petroleros C.A. de Ciudad Ojeda Estado Zulia, utilizando como técnica para la recolección de información, la observación, entrevistas directas y el análisis de información aportada por el instrumento, para luego proponer estrategias que permitan controlar los riesgos y como consecuencia mejorar la seguridad en el área Mantenimiento.

Riesgo Laboral

Cortés (2018), afirma que la palabra riesgo ha sido utilizada en gran variedad de contextos y sentidos, y que en general puede definirse como "la probabilidad de que un evento particularmente adverso ocurra durante un período de tiempo". Frecuentemente se considera como una función de probabilidad y sus consecuencias.

En muchos contextos, el concepto de riesgo es utilizado para definir la probabilidad de que ocurra una pérdida, o la probabilidad en función del tiempo de: muerte, lesión, o enfermedad a las personas. El término riesgo también se usa cuando existe cierta incertidumbre en los resultados de un evento.

Accidente De Trabajo

Casal (2017), define el accidente como: todo evento indeseado e inesperado que ocurre rápidamente causando daños a la propiedad, a las personas y al medio ambiente. Se puede definir el accidente de trabajo como un suceso repentino que sobrevenga por causa o con ocasión del trabajo, y que produzca en el trabajador una lesión orgánica, una perturbación funcional, una invalidez o la muerte.

En cuanto a las herramientas de calidad de gestión utilizadas se mencionan las siguientes:

- Diagrama de causa-efecto.
- Diagrama de Pareto.

La empresa P&T Servicios Petroleros C.A. Actualmente aplica los métodos “Análisis preliminar de peligros”, “Estudio de riesgos y operabilidad y el índice Mond”, donde ha logrado mayor efectividad en lo referente a la identificación de riesgos.

El análisis de trabajo seguro merece especial atención, porque es un procedimiento que se emplea para examinar los métodos de trabajo, y al mismo tiempo permite descubrir los peligros y riesgos que se hayan pasado por alto en el diseño del taller, y que puedan haberse identificado después de iniciado el proceso en la fase de cada tarea de mantenimiento.

Al referirse al análisis del error Humano, este tiene incidencia sobre los accidentes durante la ejecución de las operaciones; también se incluye el método “Que pasaría si...”, que aunque es uno de los menos estructurados es de gran utilidad.

El análisis o estudio de riesgos, se puede resumir en tres (3) preguntas generales: ¿Que puede salir mal?, ¿Cuáles son los efectos y consecuencias?, ¿Con que ocurrencia sucederá?

La primera pregunta es la identificación del riesgo y es una cuestión cualitativa, que puede revelar aspectos de la empresa P&T Servicios Petroleros C.A. que requieren mayor consideración. Con respecto a las otras dos preguntas, con frecuencia se dan respuestas cualitativas, aunque actualmente se aplican técnicas cuantitativas para responder a ellos, Al obtener los resultados del análisis de riesgos, se emplearán para indicar un juicio acerca de la tolerancia de riesgos y para la toma de decisiones.

A grandes rasgos el análisis de riesgos se puede indicar, que

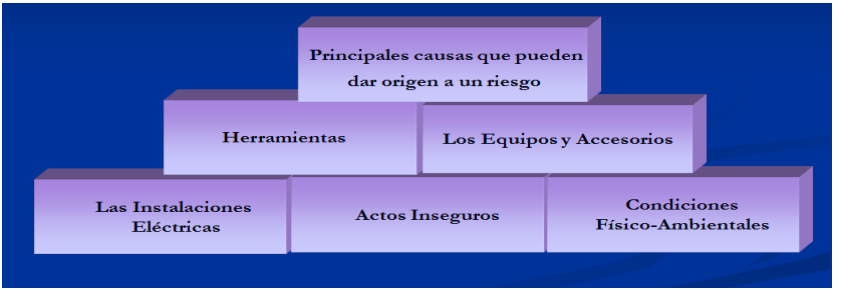
prácticamente se divide en dos etapas básicas, catalogadas como la Identificación y evaluación de riesgos.

Identificación de los riesgos: Durante esta etapa se desea conseguir los peligros presentes en la empresa P&T Servicios Petroleros C.A., donde se puede aplicar las técnicas de identificación entre las cuales se tienen las siguientes: Análisis preliminar de riesgos, que pasaría si…, evaluación técnica de seguridad industrial, estudios de riesgos y operabilidad; sin embargo por ser un taller de mantenimiento se aplica el Análisis de Seguridad, el cual surge como herramienta para la identificación y evaluación de los riesgos en el lugar de trabajo, también incluye la generación de propuestas para aumentar los niveles de Seguridad. Una característica adicional es que permite obtener una visión integral de los riesgos en el lugar de trabajo. (PDVSA, 2019).

La terminología utilizada tiende a ser variable, lo que se relaciona entre otras, a: planear, recoger información, identificar los riesgos, evaluar los Riesgos y el análisis Complementario.

Evaluación de los Riesgos: Al identificar los riesgos, se hace necesario evaluarlos, para permitir el control y la prevención de los mismos; lo cual se realiza estimando la probabilidad de ocurrencia de un evento no deseado y midiendo las consecuencias intrínsecas.

Figura N° 1



Fuente: Elaboración propia, (2020).

Según Cortes (2018) En los ambientes laborales pueden generarse los siguientes riesgos:

Riesgos Eléctricos, mecánicos, intrínsecos en actividades de mantenimiento, ergonómicos, químicos, físicos y biológicos.

Mantenimiento: Duffaa (2018), define el mantenimiento "como el aseguramiento de que una instalación, un sistema de equipos, una flotilla u otro activo fijo continúen realizando las funciones para las que fueron creados". El mismo autor especifica diferencias entre el mantenimiento preventivo o grupo de tareas planeados con anterioridad cuyo objetivo es contrarrestar causas conocidas de fallas potenciales de dichas funciones, y el mantenimiento de reparación, considerado como el reemplazo, renovación o reparación general de de los componentes de un equipo o sistema para que cumpla las funciones para lo cual fue creado.

De acuerdo a lo expresado por Duffaa, el mantenimiento por reparación puede dividirse en dos categorías: reparación planeada y reparación no planeada. "La reparación planeada

implica, en primer lugar, que todos los recursos necesarios para realizar las tareas han sido planeadas previamente y están disponibles", a diferencia de la reparación no planeada "puede tener disponible un conjunto de instrucciones normales, puede tener a la mano los trabajadores y piezas necesarias, o puede estar inserto en un programa de mantenimiento", pero bajo la base ad hoc, pero no se ajusta a los criterios de planeación y programación previa.

Tipos de Mantenimiento

Mantenimiento Operacional: Se define como la acción de mantenimiento aplicada a un equipo o sistema a fin de mantener su continuidad operacional, el mismo es ejecutado en la mayoría de los casos con el activo en servicio sin afectar su operación natural. La planificación y programación de este tipo de mantenimiento es completamente dinámica, la aplicación de los planes de mantenimiento rutinario se efectúa durante todo el año con programas diarios que dependen de las necesidades que presente un equipo sobre las condiciones particulares de operación, en este sentido el objetivo de la acción de mantenimiento es garantizar la operabilidad del equipo para las condiciones mínimas requeridas en cuanto a eficiencia, seguridad e integridad.

El mantenimiento operacional en la industria petrolera es manejado por personal de dirección de la organización con un stock de materiales para consumo constante y los recursos de equipos, herramientas y personal artesanal para la ejecución de las tareas de campo son obtenidos de empresas de servicio.

Mantenimiento Mayor: Es el mantenimiento aplicado a un equipo o instalación donde su alcance en cuanto a la cantidad de trabajos incluidos, el tiempo de ejecución, nivel de inversión o costo del mantenimiento y requerimientos de planificación y programación son de elevada magnitud, dado que la razón de este tipo de mantenimiento reside en la restitución general de las condiciones de servicio del activo, bien desde el punto de vista de diseño o para satisfacer un periodo de tiempo considerable con la mínima probabilidad de falla o interrupción del servicio y dentro de los niveles de desempeño o eficiencia requeridos.

La diferencia entre ambos tipos de mantenimiento se basa en los tiempos de ejecución, los requerimientos de inversión, la magnitud y alcance de los trabajos, ya que el mantenimiento operacional se realiza durante la operación normal de los activos, y el mantenimiento mayor se aplica con el activo fuera de servicio. Por otra parte, la frecuencia con que se aplica el mismo es sumamente alta con respecto a la frecuencia de las actividades del mantenimiento operacional, la misma oscila entre cuatro y quince años dependiendo del grado de severidad del ambiente en que está expuesto el componente, la complejidad del proceso operacional, disponibilidad corporativa de las instalaciones, estrategias de mercado, nivel tecnológico de componentes y materiales, políticas de inversiones y disponibilidad presupuestaria. (Duffaa, 2018).

Mantenimiento Preventivo: Es aquel que consiste en un grupo de tareas planificadas que se ejecutan periódicamente, con el objetivo de garantizar que los activos cumplan con las funciones requeridas durante su ciclo de vida útil dentro del contexto operacional donde su ubican, alargar sus ciclos de vida y

mejorar la eficiencia de los procesos. En la medida en que optimizamos las frecuencias de realización de las actividades de mantenimiento logramos aumentar las mejoras operacionales de los procesos.

El mantenimiento preventivo según Duffua, se define como una serie de tareas planeadas previamente, que se llevan a cabo para contrarrestar las causas conocidas de fallas potenciales de las funciones para las cuales fue creado un activo. El mismo autor plantea que este mantenimiento puede planearse y programarse con base en el tiempo, el uso o la condición del equipo.

Mantenimiento Correctivo: También denominado mantenimiento reactivo, es aquel trabajo que involucra una cantidad determinada de tareas de reparación no programadas con el objetivo de restaurar la función de un activo una vez producido un paro imprevisto. Las causas que pueden originar un paro imprevisto se deben a desperfectos no detectados durante las inspecciones predictivas, a errores operacionales, a la ausencia tareas de mantenimiento y, a requerimientos de producción que generan políticas como la de "repara cuando falle".

Mantenimiento Predictivo: Es un mantenimiento planificado y programado que se fundamenta en el análisis técnico, programas de inspección y reparación de equipos, el cual se adelanta al suceso de las fallas, es decir, es un mantenimiento que detecta las fallas potenciales con el sistema en funcionamiento.

Mantenimiento Proactivo: Es aquel que engloba un conjunto de

tareas de mantenimiento preventivo y predictivo que tienen por objeto lograr que los activos cumplan con las funciones requeridas dentro del contexto operacional donde se ubican, disminuir las acciones de mantenimiento correctivo, alargar sus ciclos de funcionamiento, obtener mejoras operacionales y aumentar la eficiencia de los procesos.

Mantenimiento por Averías: Es el conjunto de acciones necesarias para devolver a un sistema y/o equipo las condiciones normales operativas, luego de la aparición de una falla. Generalmente no se planifica ni se programa, debido a que la falla ocurre de manera imprevista.

Mantenimiento Rutinario: Está relacionado a las tareas de mantenimiento regulares o de carácter diario.

Mantenimiento Programado: Está relacionado a los trabajos recurrentes y periódicos de valor sustancial.

Metodología y Resultados

La presente se enmarca en investigación de tipo descriptiva, con un diseño combinado de campo y documental. La población y muestra considerada objeto de estudio estuvo conformada por (24) veinticuatro personas, que realizan directamente las actividades de mantenimiento preventivo, en la empresa P&T servicios petroleros. La técnica utilizada fue la encuesta, sin embargo, el investigador consideró conveniente, realizar entrevistas informales y consultas abiertas informales, al personal de experiencia en la empresa, con el fin de estimar, cuáles podrían ser las causas que originan los riesgos, al

momento de efectuar las actividades de mantenimiento, esto permitió realizar un diagrama causa-efecto, a través de una lluvia de ideas; lo cual se complementó al aplicar el cuestionario al personal respectivo. En la práctica se conformó un equipo de personas, como soporte, para la elaboración de estrategias, que permitan reducir la presencia de los riesgos encontrados como prioritarios en las diversas tareas de mantenimiento en la empresa P&T servicios petroleros.

En otro orden de ideas, se utilizó el *diagrama de pareto*, para inferir sobre los riesgos prioritarios presentes en las tareas de mantenimiento preventivo en P&T servicios petroleros. De igual forma, se jerarquizaron los riesgos, para inferir cuales son los que tienen la mayor frecuencia de ocurrencia al realizar las actividades de mantenimiento preventivo.

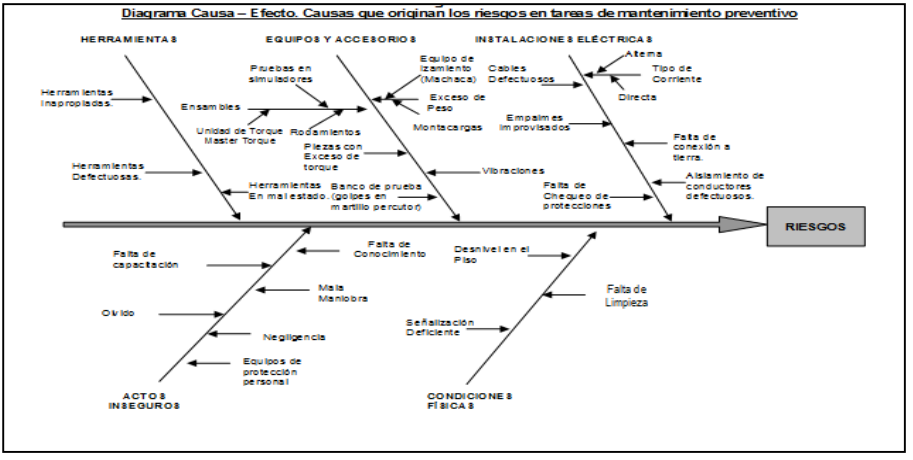
Luego de procesar toda la información recolectada, se diseñaron las estrategias, que permitirían reducir los riesgos encontrados como de mayor frecuencia de ocurrencia, para darle cumplimiento al tercer objetivo de la investigación. Así mismo el instrumento contó con 59 items de tipo cerradas, el cual fue validado a juicio de tres expertos, aplicándosele el método “Coeficiente de Cronbach” en cuanto a confiabilidad se refiere, donde se obtuvo un coeficiente de 0.82, este índice permitió demostrar que el instrumento puede ser utilizado para medir la variable Riesgos laborales en tareas de mantenimiento preventivo.

En cuanto al procesamiento de datos recolectados, por tratarse de una encuesta para recoger la investigación, el análisis se centró en una descripción de los resultados estadísticos que arrojó el instrumento, los cuales se interpretarán en función de

los parámetros teóricos que fundamenta la investigación, de acuerdo a los siguientes pasos: (a) se analizaron los ítems de acuerdo a cada uno de los indicadores, (b) se construyeron tablas por dimensión e indicadores ubicados en función de los criterios, frecuencia y porcentajes, (c) los resultados se presentaron gráficamente, (d) se realizó diagrama de pareto A y un diagrama de pareto B.

A continuación, se ilustran resultados obtenidos de la encuesta aplicada, así como también las herramientas de gestión de calidad utilizadas:

Figura N° 2.



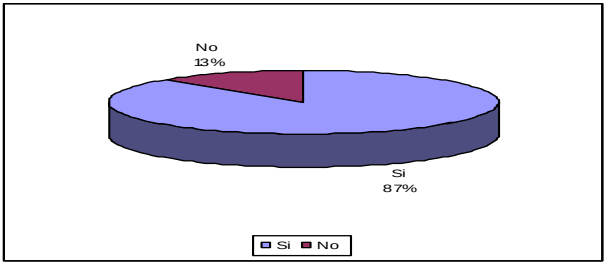
Fuente: Elaboración propia, (2021).

Indicador: Simuladores para motores de fondo.

Ítem 4: ¿Los simuladores para motores de fondo presentan fallas al realizar las pruebas posteriores al mantenimiento? Las

respuestas obtenidas las podemos visualizar en el gráfico 1, donde se evidencia que El 87% de la población en estudio señala que, si presentan fallas los simuladores para motores de fondo al realizar las pruebas posteriores al mantenimiento, mientras que un 13% manifiesta lo contrario.

Gráfico 1.

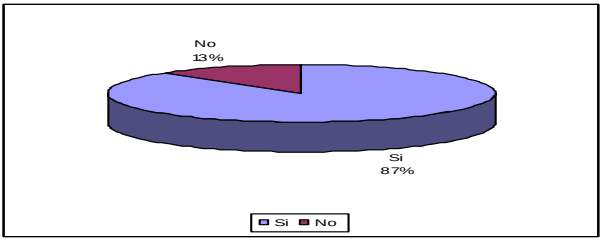


Fuente: Elaboración propia, (2021).

Sin embargo, de acuerdo con los Manuales Operativos de P&T Servicios Petroleros (2019), los motores de fondo no están exentos a fallar, solo que se debe minimizar la probabilidad de ocurrencia de fallas, realizando adecuado mantenimiento, incluso en caso de no haber utilizado la herramienta en campo.

Ítem 5: ¿Existe variación de datos en las pruebas y ensayos realizados en los simuladores para motores de fondo?

Gráfico 2.



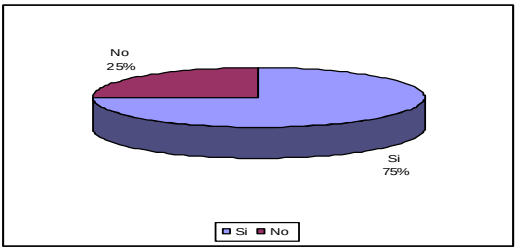
Fuente: Elaboración propia, (2021).

El 87% de la población en estudio señala que, si existe variación de datos en las pruebas y ensayos realizados en los simuladores para motores de fondo, mientras que un 13% manifiestan que no existe variación de datos. Según experiencia de equipo de trabajo de P&T Servicios Petroleros (2019), existe variación de datos en equipo simulador, cuando falla la herramienta, en la prueba de eficiencia.

Indicador: Mala Maniobra

Ítem 21: ¿Considera usted que hay malas maniobras al momento de realizar las actividades u operaciones de mantenimiento?

Gráfico 3.



Fuente: Elaboración propia, (2021).

El 75% del personal técnico de mantenimiento encuestado considera que sí hay malas maniobras al momento de realizar las actividades de mantenimiento, mientras que un 25% señala que no hay malas maniobras en las labores de mantenimiento.

A continuación, se presentan en la tabla N° 1 las causas que originan los riesgos, posteriormente en la tabla n°2, se le asignará un valor alfa numérico de orden a cada causa.

Tabla N° 1.

Causas que originan los riesgos:

CAUSA	NUMERO ASIGNADO	FRECUENCIA
Herramientas inapropiadas	A1	6
Herramientas defectuosas	A2	3
Herramientas en mal estado	A3	6
Falla en simulador	A4	21
Variación de datos	A5	21
Golpes con martillo percutor	A6	20
Uso de unidad de torque	A7	3
Herramientas con requisitos mínimos	A8	21
Limites de peso	A9	9
Derrames de aceite	A10	22
Corriente AC	A11	12
Corriente DC	A12	12
Conductores canalizados	A13	6
Instalaciones eléctricas conectadas a tierra	A15	6
Aislamiento de Conductores defectuosos	A16	9
Aislamiento Adecuado en equipos	A17	6
Chequeos periódicos	A18	12
Adecuada capacitación	A19	6
Nivel de conocimiento	A20	6
Malas maniobras	A21	18
Negligencia	A22	21
Olvido	A23	15
Equipos de protección personal	A24	6
Manipulación y transporte	A26	9
Normas en manipulación	A27	9
Desnivel en el piso	A28	18
Señalización	A29	18
Falta de limpieza	A30	24

Fuente: Elaboración propia, (2021).

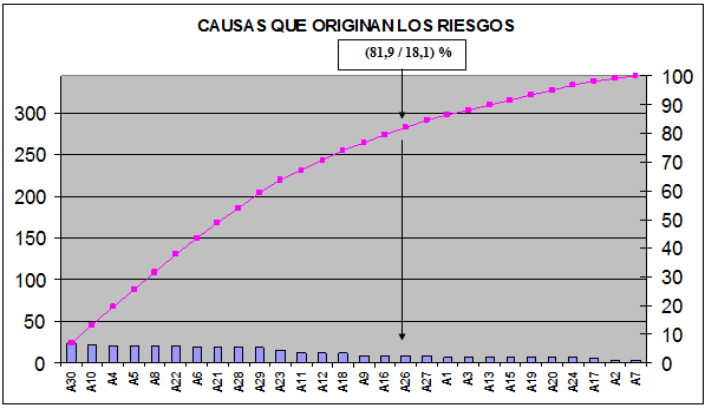
Tabla N° 2.

Causas en orden descendente con respecto a la frecuencia.

tipo de causa	frecuencia	frecuencia acumulada	%	% acumulad
A30	24	24	6,98	6,98
A10	22	46	6,4	13,38
A4	21	67	6,1	19,48
A5	21	88	6,1	25,58
A8	21	109	6,1	31,68
A22	21	130	6,1	37,78
A6	20	150	5,81	43,59
A21	18	168	5,23	48,82
A28	18	186	5,23	54,05
A29	18	204	5,23	59,28
A23	15	219	4,36	63,64
A11	12	231	3,49	67,13
A12	12	243	3,49	70,62
A18	12	255	3,49	74,11
A9	9	264	2,62	76,73
A16	9	273	2,62	79,35
A26	9	282	2,62	81,97
A27	9	291	2,62	84,59
A1	6	297	1,74	86,33
A3	6	303	1,74	88,07
A13	6	309	1,74	89,81
A15	6	315	1,74	91,55
A19	6	321	1,74	93,29
A20	6	327	1,74	95,03
A24	6	333	1,74	96,77
A17	5	338	1,45	98,22
A2	3	341	0,87	99,09
A7	3	344	0,87	100
TOTAL	344		100	

Fuente: Elaboración propia, (2021).

Gráfico 4.



Fuente: Elaboración propia, (2022).

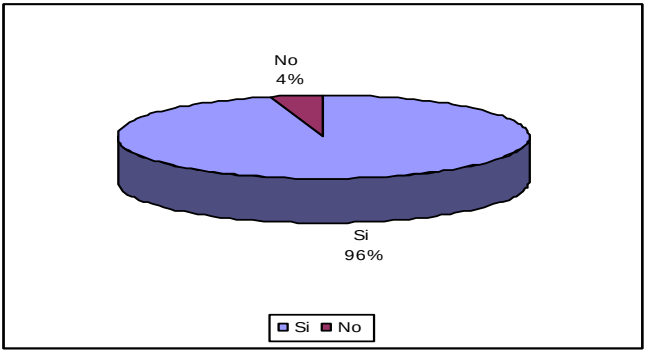
Principales Causas encontradas y jerarquizadas según el diagrama de pareto:

1.- Falta de limpieza
2.- Derrames de aceite
3.- Falla en simulador
4.- Variación de datos
5.- Herramientas con requisitos mínimos
6.- Negligencia
7.- Golpes con martillo percutor
8.- Malas maniobras
9.- Desnivel en el piso
10.- Señalización

Dimensión: Riesgos Ergonómicos

Indicador: Fatiga
Ítem 44: ¿Sus actividades habituales de mantenimiento son tan repetitivas que pueden llevarle a fatiga?

Gráfico 5.



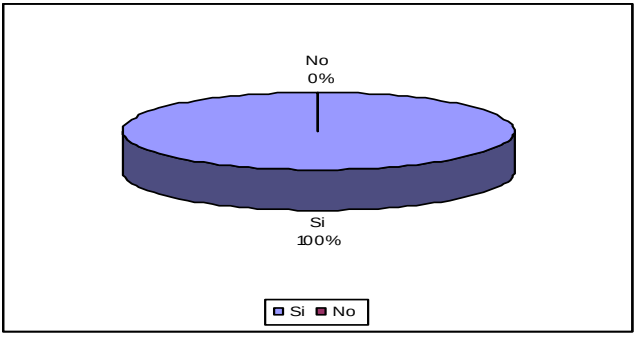
Fuente: Elaboración propia, (2022).

El 96% de los encuestados señala que sus actividades habituales de mantenimiento son tan repetitivas que si pueden llevarle a fatiga mientras el 4% señalan lo contrario. Según Albornoz (2017), La fatiga puede ser una respuesta normal e importante al esfuerzo físico, al estrés emocional, al aburrimiento o la falta de sueño. Sin embargo, también puede ser un signo no específico de un trastorno psicológico o fisiológico grave.

Indicador: Cansancio Visual

Ítem 45: ¿Considera usted que sus actividades rutinarias de mantenimiento le provocan cansancio visual?

Gráfico 6.



Fuente: Elaboración propia, (2022).

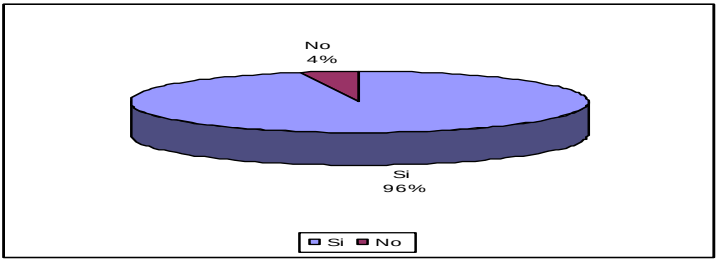
El 100% de los encuestados, es decir, la totalidad de la población objeto de estudio señalan que sus actividades rutinarias de mantenimiento si provocan cansancio visual. En este particular la Organización Mundial de la Salud (OMS) afirma respecto al cansancio visual puede traer consecuencias

a largo plazo.

Indicador: Ritmo de trabajo

Ítem 47: ¿Considera usted que realiza sus actividades de mantenimiento bajo un ritmo de trabajo acelerado?

Gráfico 7.



Fuente: Elaboración propia, (2022).

El 96% de los encuestados considera que si realizan sus actividades de mantenimiento bajo un ritmo de trabajo acelerado, mientras el 33% señalan lo contrario. Según Albornoz, F (2017), en toda actividad laboral existe una serie de elementos organizacionales como condiciones de trabajo que van a tener una influencia decisiva en la salud de los trabajadores. En ese sentido el ritmo de trabajo acelerado se cataloga como un factor de riesgo de la organización del trabajo, el cual puede traer consecuencias para la salud de los trabajadores.

A continuación, en la tabla N° 3 se presenta una breve descripción de los riesgos en base al orden del instrumento de medición, así mismo se le asigna un valor alfa numérico:

Tabla Nº 3.

Descripción de Riesgos

RIESGO	NUMERO ASIGNADO	FRECUENCIA
Riesgo de contacto directo con corriente eléctrica	B31	12
Contacto directo con partes activas	B32	12
Riesgo de contacto indirecto con corriente eléctrica	B33	18
Contacto indirecto con partes activas	B34	15
Riesgos por efecto de vibraciones	B35	16
Riesgos por efecto de elementos cortantes	B36	18
Riesgos por efecto de partes en movimiento	B37	21
Riesgo de caídas al mismo nivel	B38	15
Riesgo de caídas en diferente nivel	B39	18
Riesgo de resbalones	B40	22
Golpeado contra	B41	23
Golpeado por	B42	21
Riesgo de quedar atrapado	B43	15
Fatiga	B44	23
Cansancio visual	B45	24
Monotonía	B46	22
Ritmo de trabajo acelerado	B47	23
Temperatura ambiental	B48	11
ventilación	B49	6
Iluminación	B50	3
Radiaciones no lónicas	B51	15
Ruido	B52	17
Presencia de Humos o polvos	B53	18
Sustancias que puedan afectar la piel	B54	15
Sustancias que puedan causar daño a los ojos	B55	24
Presencia de Gases y Vapores	B56	15
Bacterias	B57	15
Virus	B58	14
Hongos	B59	15

Fuente: Elaboración propia, (2022).

En la tabla N° 4, se muestran los riesgos en tareas de mantenimiento, en orden descendente con respecto a la frecuencia:

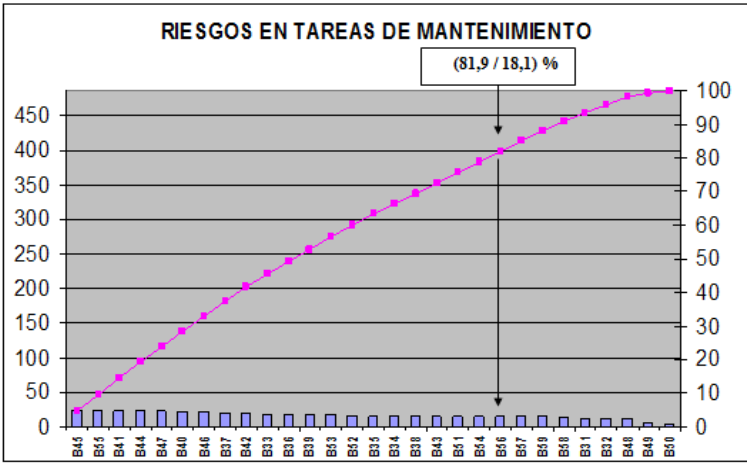
Tabla Nº 4.

Tipo de riesgo	Frecuencia	Frecuencia acumulada	%	% acumulad
B45	24	24	4,94	4,94
B55	24	48	4,94	9,88
B41	23	71	4,73	14,61
B44	23	94	4,73	19,34
B47	23	117	4,73	24,07
B40	22	139	4,53	28,06
B46	22	161	4,53	33,13
B37	21	182	4,32	37,45
B42	21	203	4,32	41,77
B33	18	221	3,7	45,47
B36	18	239	3,7	49,17
B39	18	257	3,7	52,87
B53	18	275	3,7	56,57
B52	17	292	3,5	60,07
B35	16	308	3,29	63,36
B34	15	323	3,09	66,45
B38	15	338	3,09	69,54
B43	15	353	3,09	72,63
B51	15	368	3,09	75,72
B54	15	383	3,09	78,81
B56	15	398	3,09	81,9
B57	15	413	3,09	84,99
B59	15	428	3,09	88,08
B58	14	442	2,88	90,96
B31	12	454	2,47	93,43
B32	12	466	2,47	95,9
B48	11	477	2,26	98,16
B49	6	483	1,23	99,39
B50	3	486	0,62	100
TOTAL	486		100	

Fuente: Elaboración propia, (2022).

Gráfico 8.

RIESGOS PRIORITARIOS



Fuente: Elaboración propia, (2022).

CONCLUSIONES

El presente artículo tiene la finalidad de crear conciencia y cultura en materia de seguridad al realizar laborares de mantenimiento, bien sea en una empresa o en cualquier espacio, para evitar los fallos o interrupciones violentas producto de un accidente en los flujos productivos que ocasionen daños personales debido a los comportamientos inadecuados de las máquinas y equipos que puedan alterar el buen funcionamiento de la empresa.

Así mismo, la seguridad es primordial en toda empresa, para lo cual se debe disponer de todos los implementos mínimos que ofrezcan medidas de prevención, a fin de evitar accidentes industriales o enfermedades profesionales que pongan en

peligro la integridad física de sus trabajadores. De allí el estudio permitió evidenciar que en la empresa P&T Servicios Petroleros C.A., se presentan diversos tipos de riesgos tanto intrínsecos al realizar cualquier actividad de mantenimiento, como también ergonómicos, químicos, mecánicos, eléctricos, entre otros, lo cual afectan en que el desempeño sea en forma óptima en las funciones de los operadores de mantenimiento.

En ese sentido, la jerarquización de las causas que dan origen a algún riesgo, así como también en la variedad de riesgos presentes, permiten atacar la causa raíz de forma efectiva, para reducir el riesgo, pues el mismo siempre estará presente en toda actividad. De igual forma, es importante hacer mención a los riesgos jerarquizados entre ellos están: Cansancio visual, Sustancias que puedan causar daño a los ojos, Golpeado contra, Fatiga, Ritmo de trabajo acelerado, Riesgo de resbalones, Monotonía, Riesgos por efecto de partes en movimiento, Golpeado por, Riesgo de contacto indirecto con corriente eléctrica.

Se tomaron solo diez riesgos considerados de mayor relevancia, jerarquizados en base a la mayor frecuencia de ocurrencia y los mismos pertenecen al grupo de riesgos Ergonómicos, Químicos, Intrínsecos en actividades de mantenimiento, Mecánicos y Eléctricos. Siendo los Ergonómicos los encontrados con mayor frecuencia de ocurrencia sobre todo por efectos de fatiga y monotonía en los trabajos a realizar, así como también el ritmo de trabajo acelerado al aumentar las exigencias de herramientas por empresas que requieran el servicio.

Por otra parte, las estrategias para disminuir los riesgos, son

fundamentales para la obtención de buenos resultados, entre ellas destacan la sensibilización al personal de la empresa sobre los riesgos existentes y de esta manera despertar el interés por buscar opciones de cambio a la realidad existente. Otra de importancia es la construcción de normas preventivas y las acciones de implementación como prevención en materia de riesgos. Desde esta perspectiva, se proponen una serie de estrategias que buscan prevenir situaciones de riesgos en las instalaciones de la empresa P&T Servicios Petroleros, con el propósito de contribuir en la disminución de riesgos y por consiguiente, estimular o crear conciencia, para que se asuman las medidas preventivas y exista una cultura de seguridad en el trabajo.

REFERENCIAS BIBLIOGRAFÍCAS

Abreu, J. (2018). *Ingeniería Evaluativa de la gestión de mantenimiento en las industrias manufactureras del sector privado en el estado Trujillo*. Venezuela.

Asamblea Nacional de la República Bolivariana de Venezuela. (2005). *Ley Orgánica de Prevención, Condiciones y Medio Ambiente de Trabajo*. Gaceta Oficial de la República Bolivariana de Venezuela, 38.236 julio, 2005.

Balestrini, M. (2020). *Como se elabora el proyecto de investigación.* (6ª ed.) Venezuela. BL Consultores Asociados.

Cortes, J. (2018). *Seguridad e Higiene del Trabajo*. Técnicas de

Prevención de Riesgos Laborales. Venezuela: Alfa omega.

Casal, J. (2017). *Riesgos en Instalaciones Industriales*. Colombia. Editorial Alfaomega.

Duffaa, R. (2018). *Sistemas de Mantenimiento. Planeación y Control*. México. Editorial Limusa.

Fondonorma. (2014). *Norma Venezolana 2260*. Programa de Higiene y Seguridad Ocupacional. Aspectos Generales. Caracas. FONDONORMA

Instituto Nacional de Prevención, Salud y Seguridad Laboral INPSASEL (2019). Consultado el 28 de Octubre de 2019 en: www.seguridadonline.com/modules/mastop-publish/files-474 ad09leo014.pdf

Instituto Nacional de Prevención, Salud y Seguridad Laboral INPSASEL (2019). Consultado el 30 de Octubre de 2019 en: http://www.inpsasel.gov.ve/moo_nrws/prensa-015.html

Norma Técnica. (2008). *Implementación y Evaluación de un programa de seguridad y Salud en el trabajo*. Caracas, 01/12/08. 198 y 149 Ministerio del Poder Popular Para el Trabajo y Seguridad Social. Despacho del Ministro. Nº 6227.

Petróleos de Venezuela, Sociedad Anónima (PDVSA) (2019). *Manual de seguridad, Higiene y Ambiente en la Industria*. Modulo C. Nivel Supervisorio.

P&T Servicios Petroleros C.A. (2019). *Manuales Operativos de Herramientas, Equipos Y Accesorios*.

EXPERIENCIAS EN MANEJO ETOLÓGICO DE LA BROCA DEL CAFÉ (Coffea)

Autor: Ing. Luis Enrique Matheus
Institución: Universidad Nacional Experimental Politécnica de la Fuerza Armada Nacional Bolivariana (UNEFA).
Núcleo Trujillo
Correos: lemathe58@gmail.com

RESUMEN

El control etológico de la broca del café, Hypothenemus hampei, es una herramienta útil y necesaria para el manejo, monitoreo y control de esta plaga en este cultivo. En el municipio Boconó del estado Trujillo, se utilizó un diseño de campo que combina la praxis y la teoría, como prueba evaluativa a través del uso de trampas artesanales, hechas con envases plástico reutilizables de refrescos de un litro de volumen, al cual, por uno de los costados, se le abre una ventana lateral. Como atrayente se utilizó el señuelo a base de metanol:etanol (3:1). Se colocaron 25 trampas por hectárea, bajo un diseño completamente al azar con rotación y evaluación cada 10 días. Se determinó que las trampas con botellas con una ventana lateral y usando el señuelo señalado, fueron bastante eficientes, pues al comparar la infestación en el fruto del café al inicio de la prueba, donde los niveles de daño por parte del insecto eran del ochenta por ciento (80%), tres meses después, logró reducirse dicha infestación hasta un ocho por ciento (8%). Esta metodología es más amigable con el ambiente pues se deja de utilizar plaguicidas, acción muy arraigada en agricultores de esta zona, y que viene causando gran cantidad de problemas a nuestros recursos naturales. Es importante seguir evaluando su efectividad en los diferentes pisos altitudinales presentes en el Estado Trujillo y donde se siembra cafeto y analizar sus niveles de captura.

Palabras clave: Manejo etológico, broca del café, experiencias.

RISK ANALYSIS IN PREVENTIVE EXPERIENCES IN ETOLOGICAL MANAGEMENT OF THE COFFEE BORER (Coffea)

ABSTRAC

The ethological control of the coffee borer, Hypothenemus hampei, is a useful and necessary tool for the management, monitoring and control of this pest in this crop. In the Boconó municipality of Trujillo state, a field design that combines praxis and theory was used, as an evaluative test through the use of artisanal traps, made with reusable one-liter soft drink plastic containers, to which, for one side, a side window opens. The lure based on methanol:ethanol (3:1) was used as an attractant. 25 traps per hectare were placed, under a completely random design with rotation and evaluation every 10 days. It was determined that the traps with bottles with a side window and using the indicated lure, were quite efficient, since when comparing the infestation in the coffee fruit at the beginning of the test, where the levels of damage by the insect were eighty percent. percent (80%), three months later, said infestation was reduced to eight percent (8%). This methodology is more friendly to the environment because it stops using pesticides, an action that is deeply rooted in farmers in this area, and that has been causing a great deal of problems for our natural resources. It is important to continue evaluating its effectiveness in the different altitudinal floors present in the Trujillo State and where coffee is planted and to analyze its capture levels.

Keywords: Ethological management, coffee borer, experiences.

INTRODUCCIÓN

El cafeto (Coffea arábiga), es uno de los cultivos más sembrados en nuestro país Venezuela y de manera muy particular el Estado Trujillo, existiendo en este último varios municipios que pudiéramos decir que su economía gira alrededor de la producción de este rubro.

Uno de los problemas fitosanitarios que ha venido ocasionando

grandes pérdidas en la producción de este importante rubro en nuestro estado Trujillo, es la presencia de la Broca del Café (Hypothenemus hampei). Este insecto daña el fruto del cafeto, a saber, el grano de café desde épocas tempranas de la formación del fruto hasta una avanzada edad en su desarrollo, destruyéndolo en muchas ocasiones en su totalidad.

Fue en 1995, cuando se señala la presencia de la broca del Café en Venezuela, específicamente en cafetales del estado Táchira, encontrándose luego en otras regiones del país. Durante el mes de mayo del año 2000, el Servicio Autónomo de Sanidad Agropecuaria (SASA), señaló la presencia de la broca en cafetales ubicados en el sector la Corojo, municipio Boconó, del estado Trujillo; por lo que, en dicho año, el SASA inicia un programa de control y manejo contra dicho insecto.

Considerando la gravedad de la presencia del insecto en el estado Trujillo, el Instituto Nacional de Investigaciones Agrícolas (INIA) implementa un manejo integrado de plagas (MIP) como estrategia que usa una gran variedad de métodos complementarios: físicos, mecánicos, químicos, biológicos, genéticos, legales y culturales para el control del mismo.

En este sentido, lo que buscaban era minimizar al máximo el uso de químicos, para ello, los métodos señalados anteriormente, se aplican en tres etapas: prevención, observación y aplicación. En argumentaciones de Dreistdal y Flint (1994), los métodos ecológicos aspiran reducir o eliminar el uso de pesticidas y de minimizar el impacto al medio ambiente. Se habla también de manejo ecológico de plagas (MEP) y de manejo natural de plagas (Dreistdat y Flint, 1994).

Considerando lo expuesto y con la intención de estudiar la broca del café, los investigadores del INIA iniciaron los estudios para su control, de tal manera que realizaron pruebas utilizando cepas nativas de Beauveria bassiana, con el fin de evaluar el efecto parasítico del entomopatógeno sobre la broca del café y de seleccionar una cepa adaptada a las condiciones agroclimáticas de la zona.

Uno de los métodos utilizados para el manejo de la broca con bastante éxito, fue el manejo etológico. Este consiste en el uso de trampas, elaboradas con botellas plásticas desechables de gaseosas reutilizadas y un atrayente alimenticio. Este método les permitió dar un uso útil a esos envases que se tiran a la basura, concientizar a los agricultores y transformar esa realidad de pérdidas económicas a la rentabilidad productiva.

En el manejo etológico de la broca del café se necesita un cebo como atrayente del insecto el cual se coloca dentro del envase utilizado, al cual se le ha realizado una abertura por uno de sus costados para el ingreso del insecto, y como medio para ahogar a dicho insecto se coloca un nivel de agua en el envase.

Este manejo comenzó a utilizarse en nuestro Estado Trujillo en los Municipios Boconó, Juan Vicente Campo Elías y Pampán, estando ya siendo utilizado en la totalidad de Municipios productores de café. Se recomienda el uso de Veinticinco (25) Trampas por hectárea, y un mantenimiento de parte del productor cada diez (10), días, para su limpieza y recebado.

Las finalidades de estos estudios correspondían a evaluar la eficacia de dichas metodologías que buscaban disminuir la incidencia del ataque del insecto para evitar pérdidas en la

producción, además de colocar a la mano del agricultor, herramientas que pueda utilizar al momento de determinar la presencia de dicho insecto en sus cultivos de café.

La planta de café

Es un arbusto o árbol pequeño, perennifolio, de fuste recto que puede alcanzar los 10 metros en estado silvestre. Como lo expone Monroig (1988), la planta de café es perteneciente al sub tipo de las Angiospermas, cuya clase es Dicotiledóneas de la familia Rubiaceas cuyo género es Coffea, cuyas especies pueden ser C. arábiga, C. canephora, C. liberica. (Monroig, 1988).

Su fruto es una drupa que desarrolla lentamente durante las primeras seis o siete semanas alcanzando un tamaño de 3 a 4 mm; el endospermo comienza a desarrollarse a partir de la duodécima semana, y acumulará materia sólida en el curso de varios meses, atrayendo casi la totalidad de la energía producida por la fotosíntesis. El mesocarpio forma una pulpa dulce y aromática de color rojizo que madura en unas 35 semanas desde la floración.

La mayor parte de la semilla la constituye el endospermo, que es de consistencia dura y color verdoso; el embrión se localiza dentro de la semilla a nivel de la base, de aproximadamente 4 mm de largo y una tonalidad crema que trasluce dentro de la semilla; alrededor de la semilla se encuentra la película plateada que es visible cuando se seca y luego el endocarpio o pergamino (López, 1990).

Broca del café (Hypothenemus hampei)

La broca del café Hypothenemus hampei, es el insecto plaga más importante que afecta el cultivo del café en Venezuela y en casi todos los países productores, causando pérdidas cuantiosas a los cultivadores.

Morfología

La broca vuela levantándose lentamente y casi en forma vertical hasta encontrar corrientes de aire que la arrastran a otros sitios y puede mantenerse libremente hasta una hora y media y más de tres horas en vuelos sucesivos (Baker 1984).

Los compuestos volátiles son aquellos que se evaporan fácilmente en el aire. Las sustancias volátiles proporcionan señales a los insectos sobre su existencia, para poder dirigirse a ellos. La broca es primero atraída por metabolitos secundarios que produce el cafeto en su proceso de formación del fruto y luego por el color y la forma del fruto. Las que llegan después son atraídas por los mismos factores, pero también por los volátiles liberados por la primera broca.

Hay evidencias (Giordanengo et al. 1993) que en los desechos fecales se producen sustancias que atraen otras hembras. Las hembras de la broca debido a esto tienden a agregarse al llegar a un cafetal concentrándose en ciertas ramas y árboles.

Ciclo de vida

Existen considerables diferencias en cuanto a la información sobre la duración de sus estados, pero esto obedece

fundamentalmente a diferencias en las condiciones ambientales de los diversos estudios, especialmente de temperatura.

El adulto hembra de la broca del café una vez emerge de la pupa está listo para aparearse y unos tres días después puede iniciar posturas. Su período de oviposición es de unos 20 días y coloca entre dos y tres huevos/día. El número de días que puede permanecer ovipositando se estima en 15 a 18 días aproximadamente. La incubación del huevo dura 7,6 días a una temperatura de 23°C y el estado de larva 15 días para los machos y 19 días para las hembras, la pre pupa dos días y la pupa 6,4 días a 25,8°C.

El ciclo total de huevo a emergencia de adulto se estima en 27,5 días a temperatura de 24,5°C. Sin embargo, el tiempo generacional, o sea el tiempo que tarda en iniciarse otra generación del insecto, bajo condiciones de campo se estima en 45 días a una temperatura promedia de 22°C y de unos 60 días para una temperatura de 19°C. La relación de sexos es aproximadamente de 1: 10 en favor de las hembras (Ruiz 1996).

El macho adulto de la broca no tiene sino función reproductora. Es más pequeño que la hembra, y se encuentra siempre en el interior de los frutos, además es incapaz de perforar un fruto. Debido a que los músculos de sus alas se encuentran atrofiados no puede volar. Este comportamiento explica por qué no es viable el uso de atrayentes sexuales para el manejo de este insecto (Bustillo et al. 1998).

Una vez que la hembra colonizadora inicia su oviposición, permanece en el interior del fruto del café hasta su muerte cuidando de su progenie. Bajo condiciones de la zona central

cafetera se ha determinado que, en un fruto de café, desde el momento que es susceptible al ataque de la broca hasta la época de cosecha, se pueden producir dos generaciones de la broca. Si estos frutos no se cosechan y se dejan secar en el árbol, se puede llegar a cuatro generaciones (Ruiz 1996).

Hospedero

Es el cafeto (Coffea arábiga; Rubiaceae), es el hospedador principal de la broca (Hypothenemus hampei), pero se han encontrado casos de afección en otras especies de este género. Las hembras adultas atacan los frutos del café en un período que va desde ocho semanas tras la floración hasta 32 semanas, cuando se realiza la cosecha. Prefieren los frutos maduros.

Luego que una hembra entra al fruto construye galerías y coloca unos huevos ovoides en depósitos verdes, marrones o grises en el endosperma, que sólo sólido puede ser adecuado para el desarrollo de la prole. Si la hembra ataca un fruto que tiene un endosperma líquido e inmaduro, penetra sólo hasta el mesodermo y espera varias semanas hasta que el fruto madure (Borbón, 1991).

Daños

Es muy importante conocer que el daño que ocasiona la broca al fruto de café, consiste en perforaciones a los frutos y caída de estos cuando atacan frutos jóvenes. En investigaciones realizadas por Alzate (1993), se encontró que cuando la broca ataca frutos de café de dos meses de edad, más del 50% de los frutos afectados se caen de las ramas y muchos de ellos toman un color característico de madurez; pero si el ataque ocurre

después de los tres meses de edad, la caída de frutos es menor al 23,5%. La pérdida de peso del café pergamino seco por causa de la broca fue en promedio de 18,1%, y los frutos que fueron atacados tempranamente se maduran prematuramente, lo cual repercute en un manchado del pergamino de los granos sanos (Alzate, 1993).

Control etológico

Se basa en el estudio del comportamiento de las preferencias de cada plaga en sus diferentes estados. En palabras de Romero (2004), este método en realidad constituye un enfoque que enriquece a los demás métodos al considerar las horas de desplazamiento de insectos, sus hábitos alimenticios, su preferencia por determinados colores y las condiciones que requieren para aparearse. Este método incorpora el uso de trampas entre las que destacan las de luz, calor, feromonas y alimenticias (Romero, 2004).

Contexto Metodológico

Uno de los Métodos utilizados para el manejo y control de la broca del café y con bastante éxito, es el Manejo Etológico, el cual consiste en el uso de trampas Artesanales, elaboradas con botellas plásticas desechables de gaseosas reutilizadas y un atrayente alimenticio.

A fin de eliminar o disminuir la población de brocas hembras adultas en el cultivo y después de la cosecha, y así reducir los índices de infestación a inicios de próximo ciclo, se instalan trampas para broca durante el periodo intercosecha. Este periodo dura normalmente de tres a cuatro meses después de

la cosecha y es definido por el profesional fitosanitario o Coordinador de la Campaña.

Los materiales con que se elaboran las trampas y el atrayente son muy económicos. La trampa (Imagen N° 1 y N° 2) consta de:

- Una botella desechable de plástico de tamaño variable.
- Alambre flexible para colgar la trampa de un cafeto.
- Una abertura lateral sobre la botella para permitir la entrada de la broca.
- Agua limpia en el fondo de la botella para atrapar y matar por ahogamiento a la broca.
- Un difusor o pitillo de plástico de 15 ó 20 mm de capacidad con el atrayente (mezcla de alcoholes etílico y metílico en proporciones iguales) sujetado en el interior de la botella.

Imagen N°1 y N°2.
Trampa artesanal con botellas de refresco.

Trampa artesanal con botellas de refresco: con el alambre para colgar la trampa, el envase de PET de 1 litros, la ventana para permitir la entrada de la broca, el agua en el receptáculo colector para atrapar la broca, el pitillo donde va el atrayente.

El trampeo consistió en instalar 25 trampas/ha distribuidas homogéneamente dentro del cafetal. El tiempo para la revisión tiene fluctuaciones de acuerdo a las condiciones ambientales prevalecientes. Muy importante verificar su mantenimiento, como el exista agua y atrayente suficiente en las trampas y que se encuentren limpias. Generalmente son los agricultores los responsables del mantenimiento de las trampas.

Iniciando este procedimiento, se les indica a los agricultores como se elaboran dichas trampas y como deben ser colocadas.

De igual manera se les instruye en el conteo de granos para verificar el efecto de las trampas. De esta manera continúan realizando esta práctica parta minimizar las afectaciones por broca. El trampeo ha tenido importantes resultados y es totalmente aceptado por los agricultores, ya que perciben con claridad su beneficio: pueden observar la captura y mortandad de las brocas en las trampas, la poca afectación en los frutos y pueden darse cuenta del bajo costo de elaboración y mantenimiento de las trampas.

El uso de sustancias atrayentes, como feromonas o kairomonas, no es nada nuevo en el manejo de plagas, la mezcla de metanol con etanol resulta sorprendentemente poderosa para atraer a la broca. Son dos sustancias que se producen en fábricas de productos químicos; en la naturaleza son comunes en procesos de fermentación o pudrición de

materia orgánica, como madera y frutas. Barrera, Herrera y Rojas (2006), argumentan que el alto grado de atracción, junto con el bajo costo y la fácil disponibilidad, hicieron que al paso de los años la propiedad de la mezcla fuera aprovechada para desarrollar este sistema de trampeo (Barrera, Herrera y Rojas, 2006).

En un comienzo se usó como cebo o atrayente soluciones madres realizadas con solamente los alcoholes Metanol y Etanol en proporción de Tres partes de Metanol por una parte de Etanol (3:1), pero con el tiempo se utilizó la mezcla de granos de café maduro y alcoholes, etanol y metanol, obteniendo resultados satisfactorios. En lo sucesivo, también se logró captura significativa de insectos con solamente el uso de Etanol.

Para el muestreo, se recomienda realizarlo entre los 60 y 90 días después de la floración principal, por razón de encontrarse la broca adulta en ese período en el canal de penetración del fruto, siendo más vulnerable a la acción del control.

En nuestro caso, para el conteo de los granos, se seleccionaron plantas/ha al azar, siguiendo el criterio recomendado por Decazy (1989), el cual estipula la distribución sistemática de 20 sitios de muestreo formados de cinco plantas, en un área no mayor de 3.5 ha, extrayéndose al azar 100 frutos por sitio (Decazy, 1989).

Se recolectaron granos de café de cada planta en su estado de madurez inicial y se procedió a revisar si estaban o no afectados. De esta manera se accionó al inicio de la puesta de las trampas y a los tres meses después de colocadas las mismas. Se estuvo muy pendiente del mantenimiento de las

trampas.

Resultados

Cuando se inició el establecimiento de las trampas, se tomaban 100 granos de veinte ó treinta plantas por hectárea en forma de zig-zag. Inmediatamente se llevaban al laboratorio para revisar si estaban o no afectados por dicho insecto. En la tabla 1 se muestra la cantidad de granos de café afectados al inicio de la colocación de las trampas.

Tabla 1.
Conteo de granos afectados al inicio de la prueba
Prueba de la utilización de trampas con botellas reutilizables

Prueba de la utilización de trampas con botellas reutilizables			
N° de planta	**N° de granos**	**Afectados**	**% Infestación**
1	100	87	87
2	100	81	81
3	100	75	75
4	100	80	80
5	100	77	77
Promedio			80

Fuente: Elaboración propia, 2002.

Como evidencia, se aprecia que, de los 100 granos, el promedio arrojado fue que 80 tenían perforaciones, esto se realizó cinco veces en la unidad de producción, arrojando números similares,

lo que indicaba un porcentaje de afectación del 80%.

Tres meses después de colocarse las trampas, se volvieron a contar los granos de las plantas en cuestión, y se obtuvieron buenos resultados que se evidencian en la tabla 2.

Tabla 2.

Prueba de la utilización de trampas con botellas reutilizables

N° de planta	N° de granos	Afectados	% Infestación
1	100	11	11
2	100	6	6
3	100	6	6
4	100	10	10
5	100	9	9
Promedio			8.40%

Fuente: Elaboración propia, 2002.

Se determinó que de los 100 granos observados solo ocho estaban perforados. Esta prueba se realizó cinco veces obteniéndose resultados similares. Lo que indicaba una afectación de solo el 8%.

Aunado a lo expuesto, se realizaba un conteo aproximado del insecto capturado, contando en una oportunidad hasta 2000 insectos por trampa, recordando que, en esta especie, solo tiene la capacidad de volar las hembras, por lo cual la multiplicación del insecto disminuía considerablemente.

Conclusión

La broca es una plaga muy dañina para la producción de café ya que afecta directamente al grano que es el producto final disminuyendo los rendimientos y la calidad. Cuando se tienen focos de infestación, se hace necesaria la intervención mediante la implementación de trampas artesanales para disminuir las afectaciones. Si no se presta atención a esta plaga es posible que las infestaciones se intensifiquen y que se extiendan a áreas muy grandes cuyo control resultaría muy costoso en términos económicos.

Las trampas que se utilizaron ofrecen gran ventaja al agricultor ya que se recolecta una gran cantidad de broca, evitando que se establezca en los nuevos granos y que desde allí se siga reproduciendo. Se evidencia que, con el uso de estas trampas, se puede disminuir la incidencia de las afectaciones en el grano de café hasta un 8%.

Se ha comprobado que el ataque de la broca es menor en las áreas donde se instalan apropiadamente. Pero es muy importante mantener el área de cultivo con un buen manejo, ya que lo contrario incita a condiciones que son favorables para el desarrollo de la plaga. El buen manejo se logra neutralizando la emergencia de las malezas, manteniendo buena sombra y la poda de los cafetos. La continua supervisión en el campo también es determinante para detectar oportunamente los focos de infestación y poder implementar a tiempo las trampas artesanales antes de que el ataque se extienda o se intensifique.

REFERENCIAS BIBLIOGRÁFICAS

Alzate, V. A. (1993). *Rendimiento y porcentaje de infestación del café cereza atacado por broca*. Cenicafé, Informe de labores no publicado, Chinchiná.

Barrera, J.; Herrera, J. y Rojas, J. (2006). *Atrápame si puedes: peripecias de una persecución sin tregua*. Revista Puertas Abiertas No. 37. ECOSUR. México.

Baker, P. S. 1984. *Some aspects of the behavior of the coffee berry borer in relation to its control in southern.* México (Coleoptera: Scolytidae). Folia Entomológica Mexicana.

Borbón, O. (1991). *La broca del fruto del cafeto*: programa cooperativo ICAFÉ-MAG. San José, Costa Rica. ICAFÉ.

Bustillo, A. E; Cárdenas, R.; Villalba, D.; Benavides, P.; Orozco, J. y Posada F. (1998). *Manejo integrado de la broca del café, Hypothenemus hampei (Ferrari)* en Colombia. Chinchiná, Cenicafé.

Decazy, B. (1987). *Descripción, ecología y control de las principales plagas del cafeto*. In: Memoria II Curso regional sobre manejo integrado de plagas del cafeto con énfasis en broca del fruto (Hypothenemus hampei, Ferr.) Honduras. Editado por IICA-PROMECAFÉ, HICAFÉ.

Giordanengo, P.; Brun, L. O. y Frérot, B. (1993). *Evidence for allelochemical attraction of the coffee berry borer Hypothenemus hampei, by coffee berries*. Journal Chemical Ecology 19.

López, M. (1990). *Cultivo del cafeto en México*. México. INMECAFÉ.

Monroig, M. (1988). *Prácticas modernas en el cultivo del café en Puerto Rico*. Puerto Rico. Banco Santander de Puerto Rico en colaboración con el Servicio de Extensión Agrícola.

Romero, F. (2004). *Manejo integrado de plagas: las bases, los conceptos, su mercantilización*. México. Universidad Autónoma de Chapingo, Instituto de fitosanidad.

Ruiz, R. (1996). *Efecto de la fenología del fruto del café sobre los parámetros de la tabla de vida de la broca del café; Hypothenemus hampei (Ferrari)*. Manizales, Colombia. Universidad de Caldas, Facultad de Ciencias Agropecuarias, Tesis: Ingeniero Agrónomo.

LA LUCHA CONTRA LA CIBERDELINCUENCIA: PROTEGIENDO INSTITUCIONES Y EMPRESAS CONTRA LA VULNERACIÓN DE DATOS

Autora: Dra. Yennys Alvorada Olivares
Institución: Universidad Nacional Experimental Politécnica de la Fuerza Armada Nacional Bolivariana (UNEFA).
Núcleo Aragua
Correos: yolivar965@gmail.com

RESUMEN

El artículo aborda la ciberdelincuencia como un desafío global y complejo, enfatizando la necesidad de un enfoque integral y colaborativo para su erradicación, con implicaciones que afectan a individuos, empresas, el sector gubernamental y la sociedad en su conjunto. El propósito es analizar la ciberdelincuencia como un fenómeno global desde una perspectiva holística. El enfoque teórico al centrarse en la ciberdelincuencia como un fenómeno multifacético que afecta a distintos niveles de la sociedad se fundamenta en las teorías de Naval, Fernández, Bedecarratz Scholz y Mugan, denominadas de elección racional, subcultura, etiquetamiento, rutina diaria, estrés generalizado, desorganización social, anomia. La Metodología empleada es de naturaleza documental-bibliográfica, soportada en la revisión exhaustiva de documentos y textos científicos relevantes. Los resultados indican que, si bien la tecnología ofrece numerosas facilidades y ventajas, también introduce riesgos y vulnerabilidades explotables por delincuentes cibernéticos. Se resalta la necesidad de concienciar sobre estos riesgos y promover una cultura de seguridad de la información. En conclusión, se enfatiza la necesidad de que las organizaciones adopten una cultura de seguridad para combatir los delitos informáticos. Se sugiere la incorporación de expertos en ciberseguridad y la aplicación de respaldo legal específico. Como recomendación clave, se insta a las organizaciones a incorporar profesionales capacitados en ciberseguridad y cumplir con regulaciones legales para protegerse contra las amenazas cibernéticas. La investigación aboga por acciones proactivas y medidas preventivas, subrayando la relevancia de enfrentar la ciberdelincuencia desde múltiples frentes y con un enfoque holístico.

Palabras clave: ciberdelincuencia, protección, vulneración, datos.

THE FIGHT AGAINST CYBERCRIME: PROTECTING INSTITUTIONS AND COMPANIES AGAINST DATA BREACHES

ABSTRAC

The article addresses cybercrime as a global and complex challenge, emphasizing the need for a comprehensive and collaborative approach to its eradication, with implications that affect individuals, companies, the government sector, and society as a whole. The purpose is to analyze cybercrime as a global phenomenon from a holistic perspective. The theoretical approach, focusing on cybercrime as a multifaceted phenomenon that affects different levels of society, is based on the theories of Naval, Fernández, Bedecarratz Scholz, and Mugan, called rational choice, subculture, labeling, daily routine, generalized stress, social disorganization, anomie. The Methodology used is of a documentary-bibliographic nature, supported by the exhaustive review of relevant scientific documents and texts. The results indicate that, although technology offers numerous facilities and advantages, it also introduces risks and vulnerabilities that can be exploited by cybercriminals. The need to raise awareness about these risks and promote a culture of information security is highlighted. In conclusion, the need for organizations to adopt a security culture to combat computer crimes is emphasized. The incorporation of cybersecurity experts and the application of specific legal support is suggested. As a key recommendation, organizations are urged to incorporate trained cybersecurity professionals and comply with legal regulations to protect against cyber threats. The research advocates for proactive actions and preventive measures, underlining the relevance of confronting cybercrime from multiple fronts and with a holistic approach.

Keywords: cybercrime, protection, vulnerability, data.

INTRODUCCIÓN

El problema de la ciberdelincuencia con énfasis en la vulneración de datos tenido un incremento a partir del avance tecnológico y la incorporación de elementos digitales en la vida cotidiana. Aunque estas tecnologías brindan muchas ventajas,

también pueden ser utilizadas de manera inadecuada por ciberdelincuentes para acceder y robar información confidencial de instituciones y empresas. La inexperiencia, la ingenuidad o la credulidad de los usuarios pueden hacerlos vulnerables a este tipo de delitos cibernéticos, lo que puede tener graves consecuencias para la privacidad y la seguridad de las personas y las empresas.

En el mundo de la seguridad informática, la ciberdelincuencia surge como una amenaza real para la privacidad en línea, ello porque los ciberdelincuentes aprovechan las brechas de seguridad en las tecnologías de la información y la comunicación para acceder a información valiosa y comprometer la privacidad de los usuarios. Esto incluye el robo de identidad, el fraude financiero y la vulneración de datos. Además, los ciberdelincuentes también pueden atacar a empresas y organizaciones para obtener información confidencial o para causar daños económicos y reputacionales.

En este contexto, afirma Bedecarratz Scholz (2021), es esencial que las personas y las empresas adopten medidas de seguridad adecuadas para protegerse contra la ciberdelincuencia y la vulneración de datos. Esto incluye la implementación de medidas de seguridad en los dispositivos y sistemas, así como la educación y concienciación sobre la importancia de la privacidad y la seguridad en línea. Sin embargo, a pesar de la existencia de estos tipos de delito, la ciberdelincuencia sigue siendo un problema creciente, debido a la evolución constante de la tecnología, que permite a los delincuentes cibernéticos encontrar nuevas formas de vulnerar la seguridad de las personas y empresas.

La vulneración de datos se ha convertido en una de las formas más comunes de ciberdelincuencia, en la que se accede sin autorización a información confidencial, la cual puede ser utilizada para fines ilícitos, como el robo de identidad, el spamming, entre otros. Esto muestra la importancia de tomar medidas para proteger los datos sensibles y estar alerta a posibles amenazas cibernéticas, sobre el reconocimiento que la ciberdelincuencia no solo se limita a la obtención de información y datos sensibles, sino que también incluye una amplia gama de actividades delictivas, como el phishing, el malware, el ransomware, el ciberacoso, la extorsión digital, entre otros.

Esos delitos tienen un impacto significativo en la vida de las personas y en la economía de las empresas, ya que pueden resultar en la pérdida de datos confidenciales, la interrupción de servicios y la infracción de la privacidad. Por lo demás, la ciberdelincuencia es un fenómeno en constante evolución, y los delincuentes informáticos están desarrollando nuevas técnicas para perpetrar delitos, evadir la detección y el castigo. Por lo tanto, es crucial que las empresas y las instituciones adopten medidas de seguridad efectivas y se mantengan actualizadas sobre las últimas amenazas cibernéticas, a fin de proteger sus activos, preservar la privacidad y la confidencialidad tanto de sus clientes, como de los usuarios.

Los delitos pueden ser cometidos en cualquier parte del mundo y su alcance puede ser global, lo que hace que sea muy difícil para las autoridades competentes controlar y perseguir a los responsables. Aparte, los delitos informáticos pueden ser muy sofisticados y difíciles de detectar, lo que los hace muy atractivos para los delincuentes. Reportando la Comisión Nacional de Telecomunicaciones, Conatel (2023) “La

delincuencia organizada de Venezuela encuentra en las redes sociales el lugar ideal para cometer delitos cibernéticos, que han venido aumentando desde el año 2012 en todo el territorio nacional". (p. s/n).

Pero a pesar de los esfuerzos que se vienen gestando, con soporte en la Ley Especial contra los delitos informáticos (2001), enfrentar este problema requiere una mayor colaboración internacional, mediante la capacitación de las autoridades encargadas de perseguir y combatir estos delitos, así como una mayor conciencia por parte de los usuarios, sobre las medidas de seguridad que deben implementar para protegerse. Siendo necesario una mayor inversión en tecnología para detectar y prevenir estos delitos con medidas preventivas y sistemas de seguridad efectivos en todos los niveles, con la actuación de autoridades judiciales capacitados, preparados para investigar, sancionar los delitos informáticos, con la cooperación internacional para combatir este problema global.

Con base en lo argumentado, este artículo se trazó como objetivo general analizar la lucha contra la ciberdelincuencia para la protección de las instituciones y empresas contra la vulneración de datos, considerando que no solo estas pueden afectarse, sino también los individuos y la sociedad en general. En lo metodológico el estudio es documental, sustentado en Jiménez Rodríguez y Chaparro-Tovar (2020), tratándose de una investigación que es resultado del aporte de textos, artículos y documentos legales. Empleando la técnica análisis de contenido, que según Krippendorff (2013), se enfoca en un conjunto de procedimientos sistemáticos descriptivos sobre contenidos de mensajes, con la finalidad de realizar inferencias respecto a las condiciones de producción del contenido.

CIBERDELINCUENCIA

La ciberdelincuencia es un problema que afecta a los derechos de la privacidad y la seguridad de los datos. Se puede manifestar en forma de ataques informáticos, robo de información confidencial, acceso no autorizado a cuentas en línea, entre otros. Es importante tomar medidas preventivas como utilizar contraseñas seguras, mantener el software de seguridad actualizado, ser cauteloso al hacer clic en enlaces desconocidos para protegerse contra la ciberdelincuencia y la vulneración de datos.

Además del phishing, otros delitos cibernéticos incluyen el malware, el cual puede infectar dispositivos y robar información confidencial; la suplantación de identidad, en la que un individuo se hace pasar por otra persona para cometer fraude; y el hackeo, en el que se accede sin autorización a un sistema o cuenta en línea. Es fundamental estar informado, educado sobre estos delitos y tomar medidas para proteger la información, utilizando contraseñas fuertes, sin compartir información confidencial con terceros no confiables.

De las derivaciones mencionadas, el phishing puede tener formas más avanzadas, como el uso de técnicas de engaño para hacer que los usuarios revelen información confidencial, como credenciales de inicio de sesión, números de tarjetas de crédito, información financiera y más. La ciberdelincuencia sigue evolucionando, por lo que es importante mantenerse informado y tomar medidas para proteger la información, como verificar la autenticidad de las páginas web antes de proporcionar comunicación, no hacer clic en enlaces sospechosos y mantener software de seguridad actualizado.

Teniendo presente lo planteado por Muggah (2023).

> Gran parte del problema radica en que muchas de las autoridades públicas, empresas y grupos de la sociedad civil que son víctimas de ataques no están obligadas a notificar las violaciones de la seguridad de los datos y los ciberrobos. Muchos son reacios a hacerlo, por temor a los daños a su reputación. (p. 1).

Desde esa revelación hay que tomar precauciones con los correos electrónicos que parecen ser de fuentes confiables, pero que en realidad son fraudulentos, como el cracking que puede incluir la obtención no autorizada de mensaje confidencial, con solicitud de contraseñas y datos específicos, lo que contribuye a la vulneración de la privacidad y seguridad de la información. Por otro lado, el malware o software malicioso también juega un papel importante en la ciberdelincuencia.

Ello puede incluir virus, gusanos, spyware y ransomware, que atacan los sistemas informáticos, incluyendo la distribución de malware, que es un software dañino para robar información confidencial o causar daños a los equipos informáticos. Con respecto a los ataques de ransomware, estos son una forma de ciberdelincuencia en la que los atacantes bloquean los archivos de un usuario y exigen un rescate a cambio de liberarlos. A esto se añaden los ataques de negación de servicio (DoS), que tienen como objetivo saturar un sistema para hacerlo inaccesible.

Los delitos cibernéticos representan un desafío considerable en términos de prevención y detección, dado que los perpetradores emplean técnicas avanzadas para eludir la identificación y pueden operar desde cualquier ubicación del mundo. Esta

complejidad los convierte en amenazas difíciles de anticipar. Además, el alcance de estos delitos trasciende las fronteras geográficas, afectando a cualquier individuo o entidad, ya que las legislaciones abordan esta problemática en diversas jurisdicciones a nivel mundial. Un ejemplo ilustrativo de esta compleja situación es evidente en el caso destacado por Muggah, (Óp., Cit);

> Las herramientas de nueva generación están eludiendo los programas antivirus, razón por la cual los ataques living off the land (LOtL), en los que los atacantes utilizan software y funciones legítimas para perpetrar acciones maliciosas, representaron dos tercios de todos los incidentes notificados en 2021. (p. 1)

Por esta razón, es crucial que las empresas inviertan en tecnologías y estrategias de seguridad para proteger la información sensible y evitar que sufra daños o pérdidas financieras. Precisando la prevención y protección contra estos ataques cibernéticos de un enfoque integral que incluya la educación de los usuarios, la implementación de medidas de seguridad adecuadas y la colaboración entre los gobiernos, la industria y la sociedad en general, y aun cuan afirma Muggah (ob. cit).

> La ciberdelincuencia es difícil de detener precisamente por su naturaleza distribuida. Consideremos la banda Cobalt CyberCrime que en 2018 vulneró 100 instituciones financieras en más de 40 países, cosechando unos US$ 11 millones por ataque. Aunque su líder fue capturado en Estados Unidos en 2018 y otros tres condenados en Kazajistán y Ucrania en 2021, los expertos creen que esto hará poco para mellar sus operaciones. (p. 2).

De allí el reconocer que se trata de ataques cibernéticos de alto impacto, liderado por delincuentes, para quienes la información

confidencial y financiera es un bien valioso, extremo fácil para estos crímenes, resultando en un problema global que afecta tanto a individuos como a empresas y organizaciones, aprovechándose de la sensibilidad de los sistemas y su seguimiento.

De allí que el foco del asunto no se limita solo a que las empresas y organizaciones implementen medidas de seguridad, sino que sean efectivas, sustentadas en políticas claras para proteger la información de sus clientes y empleados. Por esta razón, es fundamental que exista una regulación adecuada y una mayor conciencia sobre la importancia de proteger la información y los datos sensibles tanto en el ámbito personal como en el profesional.

La educación y conciencia sobre los peligros de la ciberdelincuencia son necesarios asumir para la prevención de estos delitos, entendiendo frente a lo argumentado que estos ciberdelitos pueden tener graves consecuencias, ya que, en muchos casos resultan difíciles de detectar y perseguir debido a la naturaleza tecnológica de los mismos. Resaltando que una cadena de delitos, de acuerdo con lo manifiesto por Fernández (2019), atenta contra la intimidad y la privacidad organizacional, como el espionaje electrónico y la invasión, donde el atacante obtiene acceso no autorizado a datas confidenciales.

La ciberdelincuencia es un problema en constante evolución y las autoridades tienen la tarea de estar al tanto de las nuevas formas en que los delincuentes están utilizando la tecnología para cometer sus crímenes. Es necesario que se adopten medidas efectivas para prevenir y combatir la ciberdelincuencia, incluyendo la educación de la población sobre cómo protegerse

de los ataques y la colaboración internacional para combatir a los delincuentes que actúan a nivel global.

Protección organizacional

Continuando con la protección organizacional contra la ciberdelincuencia, es importante destacar la importancia de la implementación de medidas de seguridad informática en las organizaciones. Esto incluye la implementación de políticas de seguridad de la información, la formación y sensibilización de los empleados sobre los riesgos cibernéticos y la adopción de tecnologías de seguridad como el cifrado de datos y la autenticación de usuarios. Además, es fundamental realizar pruebas regulares de penetración y monitoreo de actividades sospechosas en los sistemas informáticos para detectar posibles intrusiones a tiempo y tomar medidas adecuadas. De igual modo es conveniente, contar con un plan de contingencia y recuperación de datos en caso de un ataque o incidencia informática.

Además, es fundamental para las empresas/instituciones contar con políticas y medidas de seguridad que garanticen la protección de los datos y la integridad de las pruebas electrónicas. Esto incluye el uso de tecnologías de encriptación y autenticación, la implementación de controles de acceso a la información, la realización de copias de seguridad periódicas y la adopción de prácticas de seguridad informática que eviten la manipulación o alteración de los datos.

Es primordial capacitar a los empleados sobre la importancia de la protección de datos y de la integridad de las pruebas

electrónicas, y establecer procedimientos claros para la recolección, almacenamiento y presentación de estas en caso de una investigación. Acogiéndose en situaciones que ocurran en territorio venezolano a lo establecido en la Ley Especial contra los delitos informáticos (2001), artículo 1.

> La presente Ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los delitos cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta Ley.

Orientación que responsabiliza al estado de tomar las medidas pertinentes; pero no por ello quedan exentas las organizaciones para que implementen medidas de protección, prevención contra la ciberdelincuencia y la vulneración de datos. Estas medidas pueden incluir políticas y procedimientos de seguridad, encriptación de datos, monitoreo constante de la actividad en la red, entre otras. La formación y concientización de los empleados en cuestiones de seguridad cibernética también es fundamental para mantener un ambiente organizacional seguro.

Para consolidar tal cometido, las organizaciones invierten en tecnología de seguridad de última generación y actualizan constantemente sus sistemas para protegerse contra nuevas amenazas cibernéticas. La colaboración con expertos en seguridad cibernética y la contratación de servicios profesionales para la detección y respuesta a incidentes son también medidas importantes para proteger los datos de la organización y de sus clientes, las cuales deben evaluar periódicamente sus controles de seguridad y actualizarlos según sea necesario para adaptarse a los cambios en el entorno

de ciberseguridad.

La colaboración entre las organizaciones y las agencias gubernamentales es conveniente para combatir la ciberdelincuencia, ya que pueden compartir información sobre amenazas y tendencias emergentes y trabajar juntos para fortalecer la seguridad en línea. En última instancia, la protección organizacional contra la ciberdelincuencia requiere un compromiso continuo y un enfoque integrado para la seguridad de la información.

Por lo tanto, es fundamental que las organizaciones adopten medidas de protección efectivas contra la ciberdelincuencia, incluyendo la implementación de políticas y procedimientos de seguridad cibernética, la formación del personal en la identificación y prevención de ataques cibernéticos y la inversión en tecnología de seguridad cibernética de última generación. La protección de los datos confidenciales de la organización, así como de los de sus clientes y empleados, es una responsabilidad fundamental de la empresa.

Al adoptar medidas proactivas y rigurosas para proteger la información y prevenir la ciberdelincuencia, las organizaciones pueden mejorar su reputación, minimizar el riesgo de responsabilidad legal y, en última instancia, proteger su sostenibilidad a largo plazo. Esto incluye la implementación de políticas y prácticas de seguridad de la información sólida, la formación de sus empleados sobre las mejores prácticas en materia de seguridad y la adopción de tecnologías avanzadas de seguridad. Además, es necesario establecer acuerdos globales y acuerdos internacionales para asegurar que las ciberamenazas sean abordadas de manera efectiva.

Entendido de ese modo, la Ley Especial contra los delitos informáticos (2001), en el artículo 2, describe cada una de las definiciones a efectos del cumpliendo con lo previsto en el artículo 9 de la Constitución de la República Bolivariana de Venezuela, con respecto a tecnología de Información, sistema, data, (datos), información, computador, hardware, firmware, procesamiento de datos o de información, seguridad, virus, tarjeta inteligente, contraseña, mensaje de datos. Mientras que en artículo 3, se pronuncia frente a lo extraterritorial, como sigue.

> Cuando alguno de los delitos previstos en la presente Ley se cometa fuera del territorio de la República, el sujeto activo quedará sometido a sus disposiciones si dentro del territorio de la República se hubieren producido efectos del hecho punible, y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros. Artículo 4. Sanciones. Las sanciones por los delitos previstos en esta Ley serán principales y accesorias. Las sanciones principales concurrirán con las penas accesorias y ambas podrán también concurrir entre sí, de acuerdo con las circunstancias particulares del delito del cual se trate, en los términos indicados en la presente Ley.

Fundamento en aras de dar respuesta a cada una de las situaciones sobre las que deba actuar, dejando en otras instancias, a decir las organizaciones la necesaria contratación de expertos en seguridad cibernética para ayudarles a detectar, mitigar las amenazas y garantizar la protección de sus datos.

> Esto está empezando a cambiar: ley estadounidense de 2022 sobre la notificación de incidentes cibernéticos para infraestructuras críticas proporciona orientación específica de la industria para divulgaciones voluntarias, y la directiva de 2018 de la Unión Europea sobre redes y sistemas de información de seguridad, así como una serie de otras regulaciones, obligan a los servicios de pago de

telecomunicaciones, fabricantes de dispositivos médicos y proveedores de infraestructuras críticas a informar también de las brechas. Hasta que no se refuercen las normas mundiales y la notificación de las brechas sea obligatoria en la mayoría de los sectores, será imposible comprender la verdadera magnitud del desafío, y mucho menos desarrollar soluciones específicas.

Vulneración de datos

La vulneración de datos es uno de los mayores riesgos que enfrenta la ciberseguridad organizacional, ya que los delincuentes cibernéticos pueden acceder a información confidencial, financiera y de identidad de las personas y las empresas. Para protegerse contra la ciberdelincuencia, las organizaciones deben adoptar un enfoque proactivo y estratégico de seguridad de la información. Esto incluye la implementación de medidas técnicas como el cifrado de datos, la autenticación de usuarios y la detección de intrusiones, así como la formación y concientización de los empleados sobre prácticas seguras en línea y el desarrollo de un plan de respaldo y recuperación de datos.

Por ese motivo, es favorable que las empresas tomen medidas efectivas para proteger la información y los datos de sus clientes y empleados, resaltando que la protección de los datos y la privacidad son una responsabilidad compartida entre las empresas y los usuarios, con adición a la implementación de medidas de seguridad adecuadas, entre las que cuentan educar a sus empleados y clientes sobre los riesgos cibernéticos y cómo protegerse contra ellos. Las políticas y los procedimientos deben estar respaldados, de manera que, en caso de violación de la seguridad de los datos, notificar a los usuarios y a las

autoridades correspondientes de manera oportuna.

La educación y la sensibilización son esenciales para prevenir la ciberdelincuencia y la vulneración de datos en las empresas, considerando de Nadal (2018).

> El factor humano está implicado en la mayoría de los ciberataques, los ejemplos más recientes están en WannaCry y Mirai. En estos casos, todo comenzó debido a las malas decisiones y acciones de los empleados que utilizaban los equipos y los que se encargaban de gestionarlos. Desde un ingeniero que pudo crear sin darse cuenta una vulnerabilidad en el software, hasta el usuario final que hizo clic en un enlace incorrecto, tenía una contraseña débil o había descuidado la instalación de una actualización de seguridad. Así estamos poniéndoselo muy fácil a los cibercriminales. (p. 1).

En ese sentido, para ayudar a las pequeñas empresas a identificar sus debilidades de seguridad y a aprender la importancia de protegerse contra los ataques cibernéticos, a través del juego, los usuarios pueden explorar las formas en que los hackers pueden acceder a sus sistemas informáticos y aprender a tomar medidas preventivas, como cambiar contraseñas frecuentemente, actualizar software y evitar conexiones inseguras a redes Wi-Fi. Siendo el objetivo principal concientizar a los trabajadores sobre lo que pueden hacer para protegerse contra los ataques cibernéticos.

Los expertos argumentan que muchas pequeñas empresas aún no comprenden los riesgos de la ciberseguridad y están desprevenidas ante los ataques, a pesar de que sus consecuencias pueden ser perjudiciales para sus finanzas y reputación. El problema radica en la falta de comprensión sobre la importancia de la ciberseguridad, no en la falta de recursos

económicos o tecnológicos.

Demás esta insistir en que las empresas de todos los tamaños y en todos los sectores son víctimas de ataques de ciberdelincuencia, pudiendo llevarlas hasta la interrupción del negocio, al costo de los procesos legales y la reparación de los sistemas. Por esta razón, es crucial que las empresas adopten medidas de protección organizacional contra los ataques de ciberdelincuencia, que incluyan la formación de sus empleados, la implementación de software de seguridad y la planificación de un plan de respaldo ante un ataque. Al hacerlo, las empresas pueden protegerse a sí mismas y a sus clientes, asegurándose que sus datos y operaciones estén protegidos.

Ello incluye la formación y concienciación de los empleados sobre prácticas de seguridad de información, la implementación de tecnologías de seguridad avanzadas, la revisión regular de políticas y prácticas de seguridad. Soportado en el conocimiento del marco legal que proteja y regule el uso de la información y datos personales en la era digital, para asegurar que las empresas tengan responsabilidades claras y definidas en cuanto a la protección de la información y los datos sensibles. Este marco legal debe ser compatible con los acuerdos internacionales y estar en línea con los derechos humanos, para garantizar la protección adecuada de la información y los datos sensibles en el entorno digital.

Además, en el contexto de la ciberdelincuencia enfocada en la vulneración de datos, la mala gestión de información en las redes sociales puede ser perjudicial para las empresas y los individuos. Es fundamental que las personas tengan conciencia sobre la importancia de proteger sus datos personales y

conocer las medidas de seguridad necesarias para hacerlo. Las empresas, por su parte, deben implementar medidas de seguridad robustas, al tanto con las últimas amenazas y tendencias en ciberdelincuencia para proteger sus sistemas y los datos de sus clientes. Una educación consciente sobre la ciberseguridad es esencial para prevenir la ciberdelincuencia, proteger la información, los derechos de las personas y las empresas.

En consecuencia, es necesario tomar medidas para proteger la privacidad y seguridad de los datos personales en línea. Las empresas pueden implementar políticas de seguridad de la información, incluyendo la encriptación de datos sensibles y la autenticación de usuarios. Además, es significativo que los usuarios tomen medidas para proteger sus datos personales, como no compartir información confidencial en línea y utilizar contraseñas seguras. La educación y concienciación sobre los riesgos de la ciberdelincuencia y lo trascendental que significa proteger los datos para prevenir futuros ataques. Las autoridades y las empresas deben trabajar juntas para garantizar una mayor seguridad en línea y perseguir a los delincuentes cibernéticos.

Para combatir la ciberdelincuencia enfocada en la vulneración de datos en las empresas, es necesario actualizar constantemente la estructura de investigación criminal y adoptar tecnologías avanzadas. Las redes sociales son un medio importante para la perpetración de delitos, como la extorsión, por lo que deben ser monitoreadas y reguladas, sensibilizando a los usuarios y clientes de las organizaciones sobre cualquier descuido, que pueda abrir un flanco para que penetren los ciberdelincuentes.

Las medidas y su implementación deben tener presente la educación y concientización sobre seguridad cibernética para todos los empleados, y la cooperación con las autoridades encargadas de hacer cumplir la ley para investigar y perseguir los delitos informáticos. Además, es importante que las empresas estén al tanto de las últimas tendencias y técnicas utilizadas por los ciberdelincuentes para poder adaptarse y protegerse de futuras amenazas.

Estos problemas relacionados con la ciberseguridad se ven empeorados por la falta de expertos en la materia, malos hábitos en cuanto a la información y la falta de acuerdos internacionales sobre cómo regular las amenazas cibernéticas. Los ciberdelincuentes obtienen ganancias no solo a través del chantaje de correos electrónicos mediante el uso de ransomware, sino también vendiendo ilegalmente información personal, como datos de tarjetas de crédito, acceso a cuentas financieras, información de suscripciones, números de seguro social y nombres de usuario y contraseñas.

Los perpetradores de la ciberdelincuencia pueden ser desde agencias gubernamentales hasta jóvenes hackers. Es difícil abordar adecuadamente el problema y encontrar soluciones específicas hasta que no se fortalezcan las regulaciones internacionales y la notificación de brechas de seguridad, sea obligatoria en la mayoría de los sectores. Enfrentar este panorama implica apoyarse en medidas de seguridad cibernética sólidas y actualizadas, tales como la encriptación de datos, la autenticación de usuarios y el monitoreo constante de las actividades en línea.

Conclusión

Aunque las tecnologías de la información y la comunicación han revolucionado la forma en que nos comunicamos y realizamos transacciones, también han creado nuevos desafíos en términos de privacidad y seguridad. Estar al tanto de estos riesgos, tomar medidas para protegernos contra la ciberdelincuencia y la vulneración de datos es primordial, teniendo presente que el problema es que los delincuentes cibernéticos están utilizando cada vez más técnicas sofisticadas para acceder y robar información confidencial de instituciones y empresas.

Esto puede incluir información personal, financiera y comercial, con graves consecuencias para la privacidad y la seguridad de los individuos, así como para la reputación y la solvencia de las empresas.

La ciberdelincuencia contra la vulneración de datos es un problema serio que requiere la atención de todos los actores, incluyendo individuos, empresas y organizaciones, así como la implementación de medidas preventivas y la educación sobre los riesgos asociados con la información en línea, pues su comportamiento es continuo y requiere la participación de todos los niveles de la organización, desde la dirección hasta los empleados para garantizar el resguardo y la integridad de las operaciones.

REFERENCIAS BIBLIOGRÁFICAS

Bedecarratz Scholz, F. (2021). *Cibercriminalidad y la inoperancia de la Ley de Delitos Informáticos*. En https://www.elmostrador.cl/noticias/opinion/cartas/2021/07/11/cibercriminalidad-y-la-inoperancia-de-la-ley-de-delitos-informaticos/

Comisión Nacional de Telecomunicaciones (Conatel). (2023). *El fraude y las redes sociales en Venezuela.* Ministerio del poder popular para la comunicación e información. En: http://www.conatel.gob.ve/el-fraude-y-las-redes-sociales-en-venezuela/

Fernández, C. (2019). *La experticia forense como herramienta de la investigación criminal para el combate de los delitos generados en las redes sociales*. Trabajo de grado para optar al título de especialista en investigación criminalista. Universidad Militar Bolivariana de Venezuela.

Jiménez Rodríguez, S. & Chaparro Tovar, R. (2020). *Aprehensión para la construcción del Trabajo de Investigación*. Caracas, Venezuela. Editorial Grupo para la Investigación, Formación y Edición Transdisciplinar (Fundación GIFET Editores). ISBN: 978-980-7938-00-6.

República Bolivariana de Venezuela. *Ley Especial contra los delitos informáticos*. Gaceta Oficial Nº 37.313. 30 de octubre de 2001.

Krippendorff, K. (2013). *Análisis de Contenido. Una introducción a la metodología*. Londres. Sage Publications, Inc.

Muggah, R. (2023). *Por qué necesitamos normas mundiales contra la ciberdelincuencia*. Reunión Anual del Foro económico Mundial. En. https://es.weforum.org/agenda/2023/01/por-que-necesitamos-normas-mundiales-contra-la-ciberdelincuencia/4 4 ene 2023.

Nadal, V. (2018). *Los malos hábitos de los empleados son una amenaza para la ciberseguridad*. Reunión Anual del Foro económico Mundial https://es.weforum.org/agenda/2018/01/los-malos-habitos-de-los-empleados-son-una-amenaza-para-la-ciberseguridad/ 25 ene 2018.