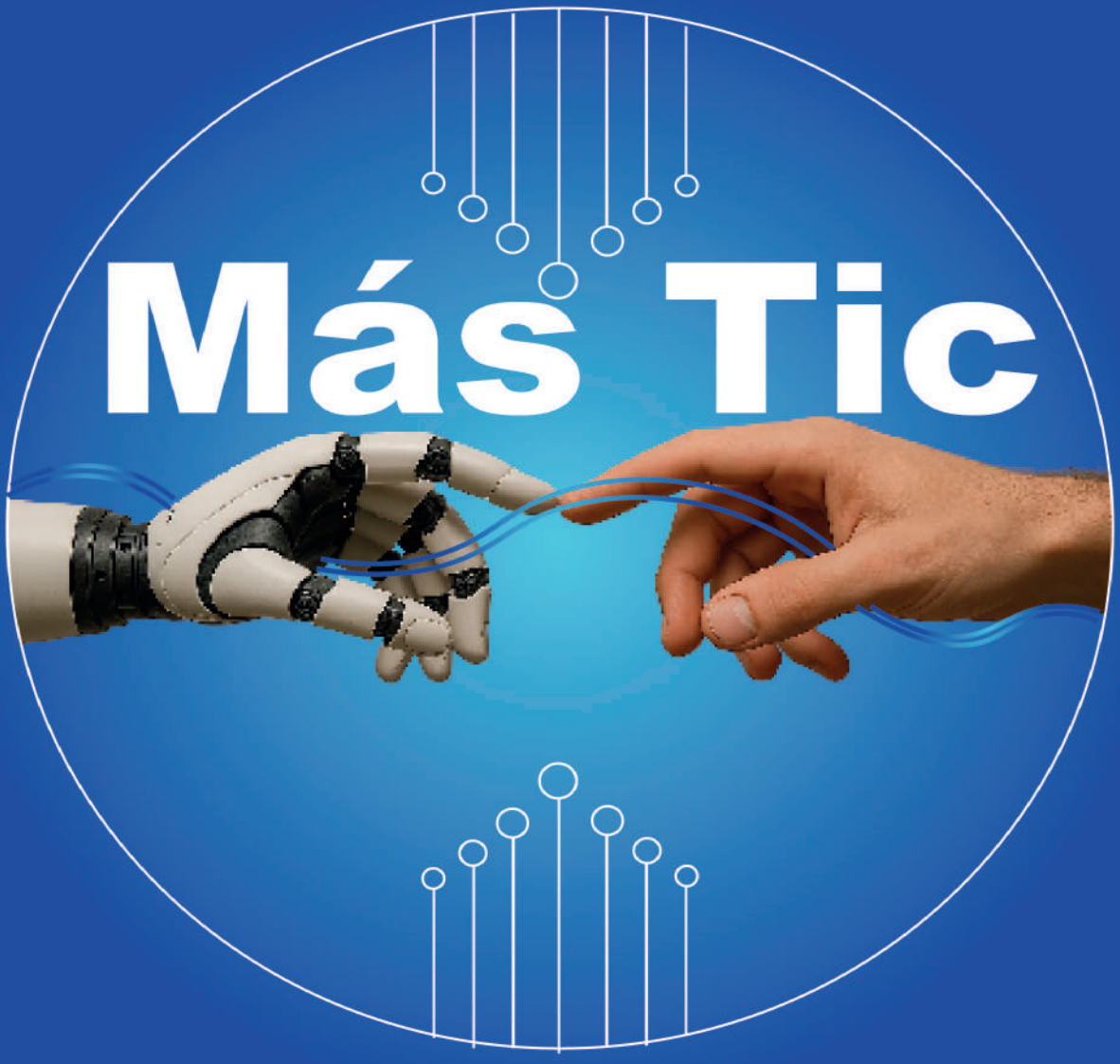
Vol 2. No. 1
diciembre - mayo 2025

ISSN L 3072-9696

REVISTA ESPECIALIZADA EN INFORMÁTICA, ELECTRÓNICA Y COMUNICACIÓN

Más Tic



Facultad de Informática, Electrónica y Comunicación

Revista Más TIC

Revista sobre Ciencia y Tecnología

Publicación Bianual

Facultad de Informática, Electrónica y Comunicación

Universidad de Panamá

Diciembre 2024 – Mayo 2025

ISSN L 3072-9696

Más TIC es una publicación bianual en línea de la Facultad de Informática, Electrónica y Comunicación de la Universidad de Panamá. Nuestra política editorial e instrucciones para los contribuyentes se encuentran en el portal web.

Información de contacto: Facultad de Informática, Electrónica y Comunicación, Campus Octavio Méndez Pereira, Universidad de Panamá. Tel 523- 6002. Correo electrónico: revista.mastic@up.ac.pa

AUTORIDADES DE LA UNIVERSIDAD DE PANAMÁ

Eduardo Flores Castro

Rector

José Emilio Moreno

Vicerrector Académico

Jaime Javier Gutiérrez

Vicerrector de Investigación y Postgrado

Mayanín Rodríguez

Vicerrector de Asuntos Estudiantiles

Ricardo Him Chi

Vicerrector de Extensión

Arnold Muñoz

Vicerrector Administrativo

José Luis Solís

Director de Centros Regionales

Ricardo Parker

Secretario General

Javier Fernández

Decano de la Facultad de Informática, Electrónica y Comunicación

Isis De Los Ríos

Vicedecana de la Facultad de Informática, Electrónica y Comunicación

Consejo Editorial

carmen.rovira@up.ac.pa

Dr. Jean Francois Duhé, Universidad de Panamá,Facultad de Informática, Electrónica y Comunicación, Panamá

https://orcid.org/0009-0006-6961-1637

jean-f.duhe-p@up.ac.pa

José Inácio Maurlio Universidade Estadual de Montes Claros, Brasil

https://orcid.org/0000-0003-0744-0845

maurilio.inacio@unimontes.br

Marlon Cristian Toledo Universidade Estadual de Montes Claros, Brasil

https://orcid.org/0000-0003-1691-0466

marlon.pereira@unimontes.br

Comité Técnico

Dr. Saúl Ardines, Universidad de Panamá,Facultad de Informática, Electrónica y Comunicación, Panamá

https://orcid.org/0000-0001-7221-0304

saul.ardines@up.ac.pa

Mgter. Angélica Pierre, Universidad de Panamá,Facultad de Informática, Electrónica y Comunicación, Panamá

https://orcid.org/0000-0002-6854-7518

angelica.pierre@up.ac.pa

Carlomagno Sancho Noriega, Universidad Nacional de Frontera, Perú

https://orcid.org/0000-0002-6828-675X

csancho@unf.edu.pe

Indice

REVISTA Más TIC	Vol. 1, No. 2	Diciembre 2024 – Mayo 2025 ISSN L 3072-9696

Editorial

Presentamos la segunda edición de la revista Más TIC. En esta edición exploraremos cómo la tecnología impacta sectores tales como la educación y la robótica, así como también se verán aspectos relacionados con la seguridad en línea, y otros temas de actualidad en materia de Tecnología.

Es importante señalar que el mundo en que vivimos plantea nuevos retos, los cuales pueden ser atendidos a través de herramientas tecnológicas. Sin embargo, el uso de estas herramientas debe contemplar aspectos éticos y sociales, los cuales son desarrollados en esta edición. La ética en la tecnología es fundamental para garantizar que el avance digital beneficie a toda la sociedad de manera justa y responsable. En un mundo donde la inteligencia artificial, el manejo masivo de datos y la automatización influyen cada vez más en nuestras decisiones, es crucial que las innovaciones respeten principios como la privacidad, la equidad, la transparencia y la seguridad.

Con esta publicación esperamos crear un espacio de reflexión sobre la influencia que tiene la tecnología en nuestras vidas, y cómo esta nos permite construir una sociedad más equitativa, segura y sostenible, permitiendo que todos progresemos a la par.

El Comité Editorial

Facultad de Informática, Electrónica y Comunicación

Universidad de Panamá

REVISTA Más TIC | Vol. 1, No. 2 | diciembre 2024 – mayo 2025 | pp. 8-33 | ISSN L 3072-9696

Implementación de una base de datos SQL en microsoft azure y exploración de escenarios de consultas con SQL server management studio

Implementation of an SQL database in microsoft azure and exploration of query scenarios with SQL server management studio

Fabiola Mabel Montero González
Universidad de Panamá, Panamá
fabiola.monterog@up.ac.pa
https://orcid.org/0000-0002-4681-9471

Recibido: 31-10-2024, Aceptado: 1-1-2025

DOI https://doi.org/10.48204/3072-9696.7411

Resumen

Este artículo describe la implementación de una base de datos SQL en la plataforma en la nube Microsoft Azure y la posterior ejecución de consultas utilizando SQL Server Management Studio (SSMS). Se detalla la arquitectura adoptada, la selección del modelo relacional y las ventajas de Azure en cuanto a escalabilidad, disponibilidad y seguridad, que permiten una gestión de datos eficiente sin necesidad de infraestructura física. La metodología de investigación incluyó las etapas de selección de la plataforma, definición de la arquitectura, creación y configuración de la base de datos, así como la exploración de consultas avanzadas. En los resultados se exponen tres escenarios de análisis: identificación de los productos más vendidos aplicando el principio de Pareto (80/20), uso de los operadores PIVOT y UNPIVOT para el estudio de tendencias de ventas mensuales y una búsqueda que enumera los productos de cada orden de compra, incluyendo filtros por región. Estos escenarios demuestran la capacidad de SSMS para ejecutar consultas complejas y extraer información estratégica. En conjunto, la experiencia confirma que la combinación de Azure y SSMS constituye una solución sólida y

flexible para el almacenamiento, consulta y análisis de grandes volúmenes de datos en entornos empresariales y académicos.

Palabras clave: análisis de datos, base de datos, información

Abstract

This article describes the implementation of an SQL database on the Microsoft Azure cloud platform and the subsequent execution of queries using SQL Server Management Studio (SSMS). It details the adopted architecture, the selection of the relational model, and the advantages of Azure in terms of scalability, availability, and security, which enable efficient data management without the need for physical infrastructure. The research methodology included the stages of platform selection, architectural design, database creation and configuration, as well as the exploration of advanced queries. The results present three analysis scenarios: identification of best-selling products applying the Pareto principle (80/20), the use of PIVOT and UNPIVOT operators to study monthly sales trends, and a query that lists the products in each purchase order, including region-based filters. These scenarios demonstrate the ability of SSMS to execute complex queries and extract strategic information. Overall, the experience confirms that combining Azure and SSMS provides a robust and flexible solution for storing, querying, and analyzing large volumes of data in both business and academic environments.

Keywords: data analysis, database, information

Introducción

En la actualidad, el análisis de datos constituye un pilar esencial en los procesos de toma de decisiones en diversos sectores. Según Treviño et al. (2020), “el curso del mundo de los negocios ha tomado un viraje inesperado que apunta hacia la revolución del análisis de datos, su procesamiento y su transformación en

información útil capaz de hacer grandes aportaciones a la toma de decisiones dentro de las organizaciones" (p. 1065). En este contexto, la gestión eficiente de los datos se ha vuelto indispensable en el entorno tecnológico actual, donde el acceso, almacenamiento y análisis de grandes volúmenes de información son elementos clave para respaldar decisiones estratégicas y bien fundamentadas.

La implementación de bases de datos SQL en entornos en la nube se presenta como una alternativa eficaz frente a las demandas crecientes de escalabilidad, flexibilidad y rendimiento en la gestión de datos. Diversas plataformas de servicios en la nube ofrecen infraestructuras robustas que permiten almacenar y procesar grandes cantidades de información en ambientes seguros y de alto desempeño.

Estas soluciones requieren recursos significativos tanto en términos de infraestructura física como en aspectos relacionados con la seguridad y el uso eficiente de las redes. Por esta razón, las soluciones basadas en la nube han ganado popularidad entre las empresas, al ofrecer ventajas escalables y adaptables. Entre estas alternativas destaca el modelo de Plataforma como Servicio (PaaS). Según Arana et al. (2015), las soluciones PaaS consisten en plataformas de software cuya herramienta de desarrollo se encuentra alojada en la nube, y a las cuales se puede acceder directamente mediante un navegador web.

El modelo PaaS permite a las organizaciones reducir costos de infraestructura y concentrarse en el análisis de datos, sin preocuparse por la gestión de los servidores. En este ámbito, Microsoft Azure, una de las plataformas líderes del sector, ofrece más de 200 servicios en la nube (Microsoft, 2024). Parra (2022) afirma que "Microsoft Azure es uno de los cuatro principales proveedores de Nube a nivel mundial, junto con Amazon Web Services (AWS), Google Cloud y Huawei Cloud, pues tiene una cuarta parte de la cuota del mercado global" (p. 2).

En el ámbito del almacenamiento de datos, Azure ofrece servicios especializados para bases de datos SQL, que permiten a las organizaciones

desplegar y administrar entornos virtualizados de alta disponibilidad, rendimiento y seguridad (Microsoft, 2024). Las bases de datos, por su capacidad para organizar información de manera estructurada, permiten almacenar y gestionar grandes volúmenes de información, siendo esenciales en procesos como inserciones, consultas, actualizaciones y eliminaciones de datos (Valverde et al., 2019). Además, la disponibilidad de modelos tanto relacionales (SQL) como no relacionales (NoSQL) facilitan su adaptación a las necesidades específicas de cada organización.

Según Ramakrishnan y Gehrke (2003), las bases de datos relacionales estructuran la información en tablas interconectadas que utilizan SQL para realizar consultas eficientes. Este modelo emplea filas, columnas, claves primarias y foráneas para organizar y relacionar los datos.

Con el crecimiento exponencial en la generación y almacenamiento de datos, las empresas necesitan soluciones innovadoras que les permitan gestionar su información con eficacia. En este escenario, las bases de datos SQL alojadas en la nube representan una alternativa potente y rentable para cubrir estas demandas (West et al., 2019).

Asimismo, herramientas como SQL Server Management Studio (SSMS) resultan fundamentales para la administración de este tipo de bases de datos, al ofrecer funciones que facilitan la ejecución de consultas complejas, la creación y edición de estructuras de datos, la gestión de procesos de administración y la visualización de resultados. Su interfaz intuitiva permite agilizar el análisis y contribuir a una toma de decisiones más informada (Microsoft, 2024).

Este artículo tiene como finalidad ofrecer una descripción general del proceso de implementación de bases de datos SQL en la nube mediante Microsoft Azure, y explorar distintos escenarios de consulta y análisis de datos utilizando herramientas especializadas como SSMS, demostrando cómo estas tecnologías pueden optimizar tanto la gestión como el análisis de datos.

Materiales y métodos

La metodología empleada en este artículo sigue un enfoque de investigación acción, estructurada en cuatro etapas clave. La primera etapa consistió en una investigación inicial para la selección de la plataforma y las herramientas. La segunda etapa se centró en la definición del modelo arquitectónico más adecuado para la implementación. En la tercera etapa se procedió a la creación y configuración de la base de datos en Azure, seguida de su integración con SQL Server Management Studio (SSMS). Finalmente, en la cuarta etapa, se exploraron y ejecutaron consultas sobre la base de datos. Los materiales empleados incluyen la plataforma Azure y la herramienta SMSS. A continuación, se describen en detalle las etapas del proceso:

Primera etapa: selección de la plataforma y herramientas

La elección de Azure se fundamenta en varios criterios fundamentales:

- Escalabilidad y flexibilidad**:** Azure ofrece una infraestructura flexible y escalable que se ajusta a las necesidades cambiantes de almacenamiento y procesamiento de datos. Permite escalar vertical u horizontalmente, lo que facilita la gestión de conjuntos de datos de diferentes tamaños sin comprometer el rendimiento (Microsoft, 2024).
- Disponibilidad y confiabilidad: Azure garantiza un alto nivel de disponibilidad con controles avanzados de seguridad, redundancia de datos y garantías de tiempo de actividad, asegurando el acceso continuo a la base de datos y minimizando el riesgo de interrupciones (Microsoft, 2024).
- Integración con herramientas: Azure se integra fácilmente con herramientas como SQL Server Management Studio (SSMS), proporcionando un entorno óptimo para la administración y análisis de bases de datos SQL, entre otras.

La elección de SQL Server Management Studio (SSMS) como herramienta de gestión en el entorno de nube de Azure complementa eficazmente las capacidades de esta plataforma. Según Derfoufi (2024), SSMS es una herramienta integral de Microsoft para administrar y desarrollar bases de datos SQL. Esta plataforma facilita la ejecución de consultas avanzadas, gestión de estructuras de datos y visualización eficiente de resultados.

La selección de Azure y SSMS fue fundamental en esta primera etapa, ya que ambas garantizan una gestión eficiente de los datos desde el inicio del proceso de implementación hasta la fase de análisis.

Segunda etapa: definición del modelo arquitectónico

El modelo arquitectónico establece la interacción entre los componentes del sistema, tomando en cuenta diversos factores como el tipo de bases de datos, los lenguajes de consulta y los métodos de distribución de los datos, como el modelo peer-to-peer o el cliente/servidor.

Existen diferentes tipos de bases de datos, incluyendo los modelos jerárquicos, en red, relacionales y no relacionales. Sin embargo, en la actualidad, las bases de datos más utilizadas se dividen en dos grandes grupos: relacionales (SQL) y no relacionales (NoSQL) (Chingo & López, 2021).

El modelo relacional, propuesto por Edgar F. Codd en los años 70, ha sido el estándar en la gestión de datos estructurados debido a su capacidad para organizar la información en tablas relacionadas de forma lógica y coherente (Codd, 1970).

Según Bernal y Molina (2022), el acceso a la información “se realiza a través del Lenguaje de Consulta Estructurada (SQL), un lenguaje que permite tanto la recuperación como la gestión de datos estructurados, transformándolos en información” (p. 308).

Para esta implementación, se optó por el modelo de base de datos relacional debido a su amplio uso en la industria, su capacidad para manejar grandes volúmenes de datos y la flexibilidad que ofrece el lenguaje SQL para realizar análisis complejos y extraer información significativa (Valverde et al., 2019). Esta elección se complementa con la plataforma Microsoft Azure, que proporciona un entorno robusto para bases de datos relacionales, empleando SQL Server como motor principal.

Respecto al método de distribución de datos, se ha elegido un modelo cliente-servidor, que centraliza tanto la gestión como la seguridad de los datos. Azure facilita esta arquitectura, permitiendo que los clientes accedan a los datos mediante procesos que gestionan las consultas y la interfaz de usuario, mientras que el servidor en la nube se encarga de manejar las transacciones y la administración de los datos. En este sentido, García (2015) afirma que “la arquitectura cliente/servidor se divide en dos capas una la del cliente que implementa la interfaz y otra es donde se encuentra el sistema gestor de base de datos” (p. 68). Este enfoque garantiza un alto nivel de control, seguridad y además ofrece escalabilidad y flexibilidad al sistema.

Tercera etapa: creación, configuración y conexión de la base de datos

Para implementar la arquitectura, se utiliza la suscripción de prueba de Microsoft Azure, que ofrece 100,000 segundos de tiempo de procesamiento en núcleos virtuales por mes y hasta 32 GB de almacenamiento de datos por 12 meses. Esta opción permite acceder a una base de datos de uso general y comenzar a trabajar con Azure SQL Database. Esta versión emplea una plataforma como servicio (PaaS), completamente gestionada, con funcionalidades avanzadas de administración de bases de datos (Microsoft, 2024).

A continuación, se detalla el proceso paso a paso para la creación, configuración y conexión de la base de datos en Microsoft Azure.

Paso 1. Activación de la cuenta de microsoft azure

Desde el portal de Azure, en la sección “Comenzar a usar Azure”, se accede a la opción de prueba. Utilizando una cuenta de Outlook, se completa el registro mediante un formulario. Una vez activada la cuenta, se muestra la página principal del portal de Azure con la suscripción lista para crear la base de datos.

Paso 2. Creación y configuración de la base de datos sql en azure

Para crear la base de datos SQL, se accede al servicio desde el botón “Apply offer (Preview)”. Luego, se crea un grupo de recursos y se configura la base de datos con el nombre “myFreeDB” y al servidor “myfreesqldbserver”, siguiendo las convenciones establecidas por Azure.

La autenticación se realiza mediante una cuenta de Outlook, asignando permisos de administrador y creando una contraseña para el acceso. A continuación, se configuran las reglas del firewall para permitir que los servicios y recursos de Azure acceden al servidor, y se añade la dirección IP del cliente. Finalmente, se selecciona el conjunto de datos preexistente “*AdventureWorks*” en Azure como base para la creación de la base de datos, una opción que Azure ofrece para la implementación de bases de datos (Microsoft, 2024).

Paso 3. Conexión a la base de datos de azure desde sql server management studio (ssms)

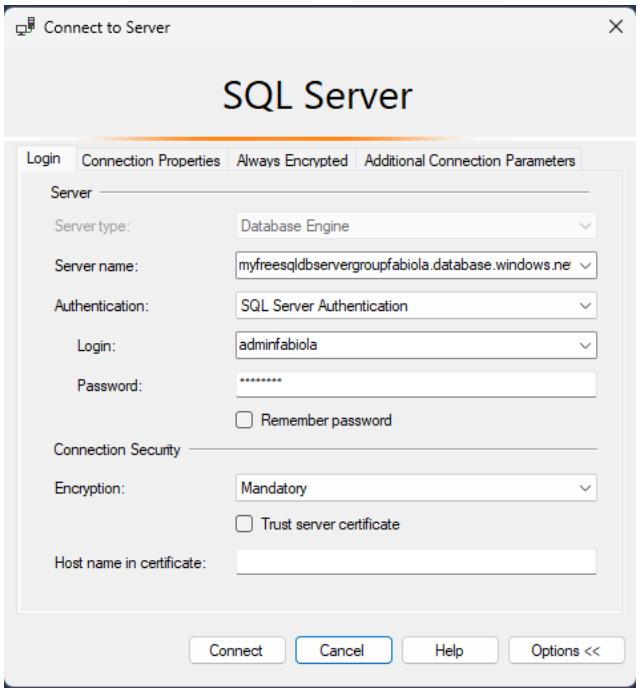
Una vez instalada la herramienta SSMS, se procede a conectarla a la base de datos de Azure. Al abrir el programa, se solicita ingresar los datos para la conexión. En el campo de Autenticación, se selecciona "Windows Authentication" y se ingresan las credenciales configuradas durante la creación de la base de datos en Azure.

Dentro de SSMS, se establece la conexión seleccionando “Connect-Database Engine”. En la ventana de conexión, se elige el servidor configurado en Azure, se selecciona el tipo de autenticación como “SQL_Server Authentication”, y

se ingresan la cuenta y contraseña creada desde Azure. Al hacer clic en “Connect”, se establece la conexión con el servidor, tal como se observa en la Figura 1.

Figura 1

Conexión a SQL Server desde SSMS

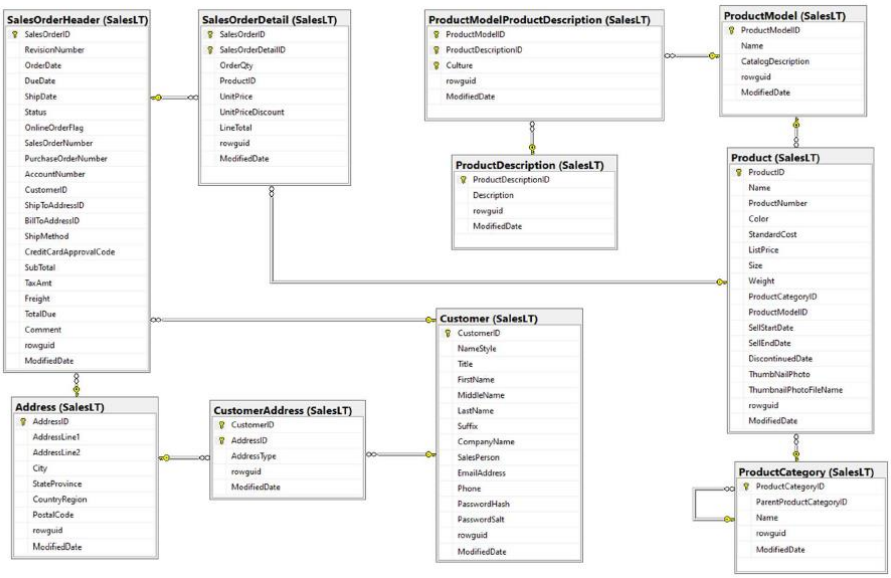


Una vez completada la conexión, se tiene acceso a los esquemas de la base de datos, incluyendo las tablas y los datos almacenados. Desde este entorno, es posible realizar consultas directamente a la base de datos en Azure, iniciando la interacción cliente-servidor.

En la Figura 2 se presenta el modelo relacional de la base de datos *AdventureWorks*. Esta base de datos simula un entorno de comercio minorista al recrear el escenario de una tienda ficticia de bicicletas llamada *Adventure Works*. Su finalidad es permitir la exploración y prueba de diversas funcionalidades de administración de datos en un contexto práctico y realista.

Figura 2

Modelo relacional de AdventureWorks



Cuarta etapa: exploración y ejecución de consultas

En esta etapa se desarrollan consultas basadas en diferentes escenarios, considerando la base de datos *AdventureWorks*. Una vez realizada la conexión a la base de datos en Azure desde SQL Server Management Studio (SSMS), se procede a la ejecución de consultas SQL diseñadas para extraer información relevante, aplicando operadores y funciones que satisfacen los requerimientos específicos del negocio.

Los detalles de estas consultas y los resultados obtenidos se presentarán en la sección de resultados, donde se examinarán las salidas generadas y su aplicación en contextos empresariales reales.

Resultados

A continuación, se presentan tres escenarios de consultas aplicadas en un contexto real de análisis de datos.

Escenario 1: extracción de distribución de pareto (80/20) en las ventas de productos

En el primer escenario de consulta, se realiza la extracción de la distribución de Pareto (80/20) de las ventas de los productos, una técnica establecida en el análisis de datos empresariales para identificar productos clave. Esta metodología permite a las organizaciones centrar sus recursos y estrategias en el 20% de productos que generan aproximadamente el 80% de las ventas, optimizando así el rendimiento y facilitando la toma de decisiones estratégicas. Al aplicar este enfoque en SQL, es posible identificar rápidamente aquellos productos de mayor rentabilidad, lo cual resulta fundamental para maximizar resultados en mercados competitivos. Plataformas tecnológicas líderes como Oracle implementan este análisis en entornos SQL para facilitar la automatización y simplificación de estas consultas (Lions, 2020).

La consulta SQL del primer escenario está estructurada en tres partes principales. La primera parte es una subconsulta para calcular las ventas por producto, que comienza con la declaración WITH, iniciando la subconsulta denominada SalesCTE. A partir de la tabla [SalesLT].[SalesOrderDetail], se extrae la columna ProductID y se genera una nueva columna con el alias TotalSales, que representa la suma de las unidades vendidas de cada producto por su precio unitario. Luego, se agrupan los valores por ProductID mediante un GROUP BY.

En la segunda parte, se realiza otra subconsulta para calcular los percentiles de ventas. Dentro del bloque WITH, se define una subconsulta adicional llamada TotalVentasSumary, en la que se seleccionan las columnas ProductID y TotalSales

previamente calculadas. Luego, se aplica la función PERCENTILE_CONT para obtener los percentiles 80 y 20 de las ventas, utilizando la cláusula WITHIN GROUP (ORDER BY TotalSales) para ordenar los datos antes de calcular los percentiles. Finalmente, la subconsulta toma los datos de SalesCTE, que contiene las ventas totales por producto.

En la tercera y última etapa, se construye la consulta principal, seleccionando las columnas ProductID y TotalSales de la subconsulta TotalVentasSummary, y filtrando para obtener solo aquellos productos cuyas ventas representan el 80% superior (P80) o el 20% inferior (P20) del total.

En la Figura 3 se muestra el código completo junto con el resultado de la consulta. Este resultado presenta todos los productos cuyas ventas totales representan el 80% de las ventas globales, es decir, los productos más vendidos.

Figura 3

Escenario 1 – Productos más vendidos

```sql
-- Definición de la primera CTE para calcular las ventas totales por producto
WITH SalesCTE AS (
    SELECT ProductID, SUM(OrderQty * UnitPrice) AS TotalSales
    FROM [SalesLT].[SalesOrderDetail]
    GROUP BY ProductID
),
-- Definición de la segunda CTE para resumir las ventas totales y calcular percentiles
TotalVentasSummary AS (
    SELECT
        ProductID,
        TotalSales,
        PERCENTILE_CONT(0.8) WITHIN GROUP (ORDER BY TotalSales) OVER() AS P80,
        PERCENTILE_CONT(0.2) WITHIN GROUP (ORDER BY TotalSales) OVER() AS P20
    FROM SalesCTE
)
-- Consulta principal para seleccionar productos en el 20% superior o inferior de ventas
SELECT
    ProductID,
    TotalSales
FROM
    TotalVentasSummary
WHERE
```

100 %

Results | Messages

	ProductID	TotalSales
42	972	13120.38
43	779	15311.934
44	966	17165.304
45	954	17165.304
46	793	17592.12
47	794	17592.12
48	781	18095.922
49	974	18949.0...
50	784	19277.916
51	973	20411.88
52	780	20879.91
53	967	22887.072
54	957	23745.3...
55	782	35801.844
56	783	37178.838
57	969	37191.492
58	976	38612.473

Query executed successfully.

En este primer escenario, se muestra cómo una consulta SQL puede identificar los productos más vendidos de las ventas totales, aplicando el principio de Pareto (80/20). La consulta primero calcula el total de ventas por producto; luego, determina los percentiles 80 y 20 para clasificar las ventas; y, finalmente, aplica filtros para seleccionar únicamente los productos que cumplen con estos criterios. Este análisis permite a las empresas enfocar sus esfuerzos en los productos más rentables, optimizando la efectividad de sus estrategias comerciales.

Escenario 2: selección de datos de las órdenes de venta

En el segundo escenario se emplean los operadores relacionales PIVOT y UNPIVOT para transformar los datos en la tabla de una forma distinta, facilitando así su análisis. El operador PIVOT permite rotar datos de una columna en múltiples columnas de la salida, aplicando agregaciones que sintetizan la información relevante y permitiendo la visualización de relaciones entre los datos de forma clara. Esto es particularmente útil para analizar tendencias o patrones dentro de una tabla

de valores, ya que permite consolidar registros en una vista concisa. Por otro lado, UNIPIVOT realiza la operación inversa, al transformar columnas en valores de fila, lo que facilita descomponer datos consolidados para un análisis más detallado y flexible. Según Microsoft Learn (2024), esta capacidad de alternar entre formatos de datos expande las opciones de análisis y brinda mayor comprensión en contextos donde la reestructuración de datos es esencial para obtener información significativa.

En este escenario, se extraen y organizan datos clave de la tabla SalesOrderDetail, que contiene los detalles de las órdenes de venta, con el objetivo de obtener un resumen de las ventas mensuales por producto. La consulta utiliza primero el operador PIVOT de SQL para agrupar y mostrar las ventas mensuales totales por producto. A continuación, estos resultados se desagrupan con el operador UNPIVOT, permitiendo así visualizar las ventas mensuales individuales de cada producto de manera detallada. En la Figura 4, se puede observar la consulta utilizando ambas funciones.

Figura 4

Escenario 2 – Detalle de las órdenes de venta

```sql
WITH SalesData AS (
    SELECT
        p.ProductID,
        p.Name AS ProductName,
        DATENAME(month, soh.OrderDate) AS OrderMonth,
        YEAR(soh.OrderDate) AS OrderYear,
        sod.OrderQty
    FROM
        SalesLT.SalesOrderDetail sod
    JOIN
        SalesLT.SalesOrderHeader soh ON sod.SalesOrderID = soh.SalesOrderID
    JOIN
        SalesLT.Product p ON sod.ProductID = p.ProductID
)
-- Pivot para obtener ventas mensuales totales por producto
SELECT *
FROM (
    SELECT
        ProductID,
        ProductName,
        OrderMonth,
        OrderQty
    FROM
        SalesData
) AS MonthlySales
PIVOT (
    SUM(OrderQty)
    FOR OrderMonth IN ([January], [February], [March], [April], [May], [June], [July], [August], [September], [October], [November], [December])
) AS PivotTable
-- UNPIVOT para desagregar las ventas mensuales por producto
UNPIVOT (
    MonthlySales
    FOR OrderMonth IN ([January], [February], [March], [April], [May], [June], [July], [August], [September], [October], [November], [December])
) AS UnpivotTable

SELECT *
FROM SalesLT.SalesOrderDetail;
```

La primera parte de la consulta define una Expresión de Tabla Común (CTE) llamada SalesData. Aquí, se seleccionan los datos relevantes de las tablas SalesOrderDatail y Product, incluyendo ProductID, ProductName, el mes y el año de la fecha de la orden, que son extraídos con las funciones DATENAME y YEAR, y la cantidad de productos vendidos (OrderQty).

Luego, mediante una serie de uniones (JOIN), la consulta conecta SalesOrderDetail con SalesOrderHeader y Product, asignando alias para simplificar su legibilidad. Posteriormente, antes de aplicar PIVOT, se realiza un SELECT sobre los campos ProductID, ProductName, OrderMonth, y OrderQty de SalesData. La función PIVOT se emplea para sumar las cantidades de productos vendidos (OrderQty) por mes (OrderMonth), proporcionando un resumen mensual de ventas por producto.

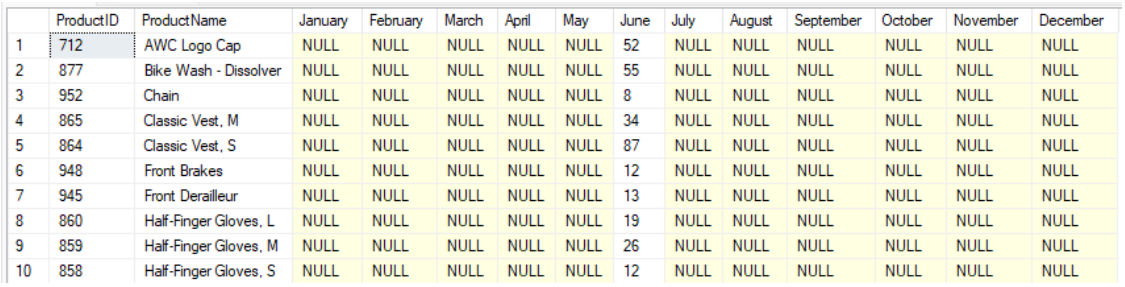
En la Figura 5 se muestra el resultado del operador PIVOT, donde se visualizan los productos y las cantidades de ventas para el mes de junio, organizado en una tabla de 142 filas. Cabe destacar, que, en este caso, la base de datos solo contiene datos de junio, por lo que únicamente se muestran las ventas de ese mes.

REVISTA Más TIC | Vol. 1, No. 2 | diciembre 2024 – mayo 2025 | pp. 8-33 | ISSN L 3072-9696

Sin embargo, si se contara con datos de enero a diciembre, la consulta reflejaría un desglose completo de las ventas mensuales a lo largo de todo el año, permitiendo una comparación y análisis de estacionalidad más detallado.

Figura 5

Resultado del operador PIVOT



	ProductID	ProductName	January	February	March	April	May	June	July	August	September	October	November	December
1	712	AWC Logo Cap	NULL	NULL	NULL	NULL	NULL	52	NULL	NULL	NULL	NULL	NULL	NULL
2	877	Bike Wash - Dissolver	NULL	NULL	NULL	NULL	NULL	55	NULL	NULL	NULL	NULL	NULL	NULL
3	952	Chain	NULL	NULL	NULL	NULL	NULL	8	NULL	NULL	NULL	NULL	NULL	NULL
4	865	Classic Vest, M	NULL	NULL	NULL	NULL	NULL	34	NULL	NULL	NULL	NULL	NULL	NULL
5	864	Classic Vest, S	NULL	NULL	NULL	NULL	NULL	87	NULL	NULL	NULL	NULL	NULL	NULL
6	948	Front Brakes	NULL	NULL	NULL	NULL	NULL	12	NULL	NULL	NULL	NULL	NULL	NULL
7	945	Front Derailleur	NULL	NULL	NULL	NULL	NULL	13	NULL	NULL	NULL	NULL	NULL	NULL
8	860	Half-Finger Gloves, L	NULL	NULL	NULL	NULL	NULL	19	NULL	NULL	NULL	NULL	NULL	NULL
9	859	Half-Finger Gloves, M	NULL	NULL	NULL	NULL	NULL	26	NULL	NULL	NULL	NULL	NULL	NULL
10	858	Half-Finger Gloves, S	NULL	NULL	NULL	NULL	NULL	12	NULL	NULL	NULL	NULL	NULL	NULL

A continuación, el operador UNPIVOT revierte la transformación de PIVOT, consolidando los datos de ventas mensuales en una sola columna llamada MonthlySale, que contiene las cantidades de ventas de cada producto para cada mes específico. Este proceso permite observar la información detallada de las ventas mensuales por producto y mes, como se muestra en la Figura 6.

Figura 6

Resultado del operador UNPIVOT

	ProductID	ProductName	MonthlySales	OrderMonth
1	712	AWC Logo Cap	52	June
2	877	Bike Wash - Dissolver	55	June
3	952	Chain	8	June
4	865	Classic Vest, M	34	June
5	864	Classic Vest, S	87	June
6	948	Front Brakes	12	June
7	945	Front Derailleur	13	June
8	860	Half-Finger Gloves, L	19	June
9	859	Half-Finger Gloves, M	26	June
10	858	Half-Finger Gloves, S	12	June

El resultado final es una tabla de 142 filas en la que cada fila representa un producto en un mes específico, detallando la cantidad de ventas para ese mes y mostrando la información organizada por ProductID, ProductName, MonthlySale y OrderMonth, lo que facilita una visualización detalla de las ventas mensuales individuales por producto.

El escenario 2 permite realizar un análisis de las tendencias de ventas mensuales de cada producto. Al organizar las ventas por ProductID y mes, es posible identificar patrones de demanda, estacionalidades y picos de ventas, lo que facilita la toma de decisiones informadas en áreas como gestión de inventarios, promoción de productos y planificación de la producción. Este tipo de visualización mensual ayuda a anticiparse a la demanda y ajustar estrategias de marketing de manera precisa, maximizando la efectividad en cada ciclo de ventas.

Escenario 3: búsqueda que enumera los productos dentro de cada orden de compra generada

En el tercer escenario de consulta, se busca listar los productos dentro de cada orden de compra generada, mostrando información clave como el precio unitario por producto, el precio total por cada producto adquirido, y el total de la orden de compra. Además, se incluye la funcionalidad de filtrar las órdenes de compra por país.

En la parte superior de la Figura 7, se puede observar el detalle de la consulta. La estructura se explica de la siguiente manera:

- En la parte inicial, se seleccionan los campos de interés relacionados con los productos y las órdenes de compra.
- Se establecen relaciones entre las tablas de la base de datos utilizando campos clave. Las tablas involucradas incluyen: SalesOrderHeader, SalesOrderDetail, Product, ProductCategory, y Address.
- En la parte final, se aplica una cláusula de filtrado que permitir introducir criterios de búsqueda, como la filtración de órdenes de compra por país.

Figura 7

Escenario 3 – Lista de productos por orden de compra generada

```
SELECT
ROW_NUMBER()OVER(PARTITION BY SOH.SalesOrderID ORDER BY SOD.SalesOrderID)AS Num,
SOD.SalesOrderID,
P.Name AS ProductName,
pc.Name as ProductCategoryName,
SOD.OrderQty,
SOD.UnitPrice,
(SOD.OrderQty*SOD.UnitPrice)AS Price_QTY,
SOH.TaxAmt,
SOH.Freight,
SOH.SubTotal as SubTotalOrder,
SOH.TotalDue as TotalDueOrder,
a.CountryRegion
FROM [SalesLT].[SalesOrderHeader] SOH
LEFT JOIN [SalesLT].[SalesOrderDetail] SOD ON SOH.SalesOrderID  =SOD.SalesOrderID
LEFT JOIN  [SalesLT].[Product] P ON SOD.ProductID=P.ProductID
LEFT JOIN  [SalesLT].[ProductCategory] pc on p.ProductCategoryID=pc.ProductCategoryID
LEFT JOIN [SalesLT].[Address] a on SOH.ShipToAddressID=a.AddressID
WHERE
a.CountryRegion='United Kingdom'
```

100 %

Results | Messages

	Num	SalesOrderID	ProductName	ProductCategoryName	OrderQty	UnitPrice	Price_QTY	TaxAmt	Freight	SubTotalOrder	TotalDueOrder	CountryRegion
2	1	71780	ML Mountain Frame-W - Silver, 42	Mountain Frames	4	218.454	873.816	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
3	2	71780	Mountain-400-W Silver, 46	Mountain Bikes	2	461.694	923.388	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
4	3	71780	Mountain-500 Silver, 52	Mountain Bikes	6	112.998	677.988	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
5	4	71780	HL Mountain Frame - Silver, 38	Mountain Frames	2	818.70	1637.40	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
6	5	71780	Mountain-500 Black, 42	Mountain Bikes	1	323.994	323.994	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
7	6	71780	LL Mountain Frame - Black, 48	Mountain Frames	1	149.874	149.874	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
8	7	71780	HL Mountain Frame - Black, 42	Mountain Frames	1	809.76	809.76	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
9	8	71780	Mountain-200 Black, 38	Mountain Bikes	4	1376.994	5507.976	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
10	9	71780	LL Mountain Frame - Silver, 44	Mountain Frames	2	158.43	316.86	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
11	10	71780	Mountain-200 Silver, 42	Mountain Bikes	4	1391.994	5567.976	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
12	11	71780	HL Mountain Pedal	Pedals	1	48.594	48.594	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
13	12	71780	Women's Mountain Shorts, S	Shorts	6	41.994	251.964	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
14	13	71780	Mountain-500 Silver, 42	Mountain Bikes	1	112.998	112.998	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
15	14	71780	Mountain-500 Black, 40	Mountain Bikes	2	323.994	647.988	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
16	15	71780	Mountain-500 Black, 44	Mountain Bikes	3	323.994	971.982	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
17	16	71780	Mountain-500 Black, 48	Mountain Bikes	1	323.994	323.994	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
18	17	71780	Mountain-500 Black, 52	Mountain Bikes	2	323.994	647.988	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
19	18	71780	Mountain-500 Silver, 40	Mountain Bikes	2	112.998	225.996	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
20	19	71780	Mountain-500 Silver, 44	Mountain Bikes	3	112.998	338.994	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
21	20	71780	Mountain-500 Silver, 48	Mountain Bikes	3	112.998	338.994	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
22	21	71780	Mountain-400-W Silver, 40	Mountain Bikes	2	461.694	923.388	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
23	22	71780	Mountain-400-W Silver, 42	Mountain Bikes	3	461.694	1385.082	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
24	23	71780	Mountain-200 Black, 42	Mountain Bikes	5	1376.994	6884.97	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
25	24	71780	ML Mountain Handlebars	Handlebars	3	37.152	111.456	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
26	25	71780	HL Mountain Handlebars	Handlebars	1	72.162	72.162	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
27	26	71780	LL Mountain Pedal	Pedals	2	24.294	48.588	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
28	27	71780	LL Mountain Frame - Black, 44	Mountain Frames	1	149.874	149.874	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
29	28	71780	Women's Mountain Shorts, L	Shorts	7	41.994	293.958	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom
30	29	71780	Hydration Pack - 70 oz.	Hydration Packs	1	32.994	32.994	3073.4952	960.4672	38418.6895	42452.6519	United Kingdom

El resultado de la consulta muestra un desglose detallado de los productos incluidos en cada orden de compra. Para cada producto, se presenta información

como el nombre del producto (ProductName), el precio unitario (UnitPrice), el total correspondiente a la cantidad de productos comprados (Price_QTY), los impuestos (TaxAmt), y el total de la orden (TotalDueOrder). Además, se incluye la información del país de origen de la compra, lo que permite aplicar filtros específicos por región, tal como se muestra en la tabla de resultados en la parte inferior de la Figura 7.

Este tipo de consulta es particularmente útil para visualizar y analizar las ventas de manera detallada por cliente y región, lo que facilita un mayor control sobre las transacciones comerciales y permite la toma de decisiones estratégicas más informadas.

Discusión

Para la exploración de consultas presentadas en este artículo, se ha utilizado el Lenguaje de Consulta Estructurada (SQL) para extraer información de una base de datos relacional. SQL es ampliamente utilizado en diversas aplicaciones, tanto comerciales como académicas, debido a su robustez y versatilidad para gestionar y manipular datos.

A través de los tres escenarios mostrados, se presentan varias funciones analíticas y operadores de SQL que ayudan a resolver problemas de análisis de datos. Estas herramientas permiten extraer información detallada y transformarla en conocimientos útiles para la toma de decisiones. Entre las funciones destacadas, se ha utilizado OVER () y ROW_NUMBER (), que operan sobre subconjuntos de datos, facilitando el cálculo de métricas y la organización de los resultados. Además, se utilizan componentes como PARTITION BY y ORDER BY, que proporcionan un mayor control sobre la agrupación y ordenación de los datos.

También se aplican operadores relacionales como PIVOT y UNPIVOT, que permiten transformar la estructura de los datos, convirtiendo filas en columnas y viceversas. Estas funcionalidades son clave para reorganizar datos y visualizar patrones que de otra manera serían difíciles de identificar. Aunque herramientas actuales de análisis visual como Power BI y Tableau ofrecen soluciones más

intuitivas para estas transformaciones, es valioso comprender cómo aplicar estas operaciones directamente en SQL, en particular cuando se trabaja en entornos que no disponen de estas herramientas externas.

En el primer escenario, se utiliza la función PERCENTIL_CONT () para determinar qué productos conformaban el 80% de las ventas totales. Esta función permite identificar los productos más significativos en términos de ingresos, así como aquellos que representan el 20% restante de las ventas, ofreciendo una visión clara de la concentración de ventas y ayudando a tomar decisiones estratégicas.

En el segundo escenario, se demuestra la utilidad de PIVOT y UNPIVOT para reorganizar los datos. PIVOT transforma valores únicos de una columna en múltiples columnas en la salida, ejecutando agregaciones, mientras que UNPIVOT invierte este proceso. Estas operaciones permiten analizar los datos desde perspectivas diferentes, algo importante en la toma de decisiones basada en información multidimensional.

El tercer escenario mostró el uso de la función ROW_NUMBER (), que asigna un número incremental único a las filas en el resultado de la consulta. Esto es útil cuando se necesita identificar el orden en que aparecen los resultados o realizar operaciones como seleccionar el primer o último elemento de un grupo de filas.

En conjunto, las funciones y operadores explorados en este estudio son de uso frecuente al trabajar con bases de datos relaciones y forman parte del núcleo de SQL en su capacidad para transformar y analizar datos de manera eficiente. Estos escenarios prácticos con SQL Server demuestran cómo las consultas avanzadas pueden proporcionar una visión profunda del comportamiento de los datos, ayudando a los analistas y profesionales de datos a tomar decisiones más informadas y precisas.

Además, todos los escenarios fueron ejecutados con éxito en una base de datos alojada en la nube, lo cual facilitó el acceso eficiente y remoto a los datos, optimizando la ejecución de consultas desde diversos puntos de acceso y

garantizando un entorno de trabajo escalable y seguro. Báez y Clunie (2020) destacan que este tipo de entorno ofrece ventajas significativas al proporcionar seguridad, escalabilidad, confiabilidad y acceso global, aspectos que facilitan la ejecución de proyectos de gran alcance sin requerir infraestructura propia ni personal especializado para su gestión. En este contexto, la integración de SQL Server en Azure proporciona un rendimiento óptimo al manejar grandes volúmenes de datos y procesar las consultas de manera eficiente, lo que se traduce en tiempos de respuesta rápidos y consistentes.

Por otro lado, García et al. (2023) señalan que:

> Es importante tener en cuenta que los servicios en la nube también conllevan ciertos riesgos, tales como la pérdida de control sobre los datos, problemas de privacidad y cumplimiento normativo, dependencia del proveedor y posibles amenazas de seguridad. Por ello, es esencial identificar y evaluar estos riesgos junto con los beneficios para gestionar adecuadamente el uso de la nube (p. 10).

Se espera que los ejemplos de consulta presentados en este artículo ofrezcan una comprensión más profunda de las capacidades de SQL desde una plataforma en la nube y que sean útiles para quienes desean optimizar sus consultas y análisis en bases de datos relacionales.

Conclusión

En conclusión, la implementación de una base de datos SQL en la plataforma en la nube de Microsoft Azure demuestra ser una decisión estratégica que ofrece una gama de ventajas significativas para la gestión y análisis eficiente de grandes volúmenes de datos. En este artículo, se explora cómo el modelo relacional de bases de datos y el lenguaje SQL brindan una estructura sólida y robusta para organizar, consultar y manipular datos de manera eficaz.

Los escenarios de consulta desarrollado en este estudio ponen de relieve la capacidad de SQL Server Management Studio (SSMS) para manejar consultas complejas con funciones y operadores avanzados como PERCENTIL_CONT, PIVOT, UNPIVOT, y ROW_NUMBER (). En el primer escenario, el análisis de ventas mediante la distribución de Pareto proporcionó una visión estratégica de los productos que generan el mayor ingreso. El segundo escenario demostró la utilidad de los operadores PIVOT y UNPIVOT para reorganizar los datos de manera flexible, mientras que, en el tercer escenario, se utilizó la función ROW_NUMBER () para ordenar y numerar filas de datos, mejorando la organización y el análisis de la información.

La combinación de Azure y SSMS no solo ha facilitado la ejecución de estas consultas con eficiencia, sino que también ha proporcionado un entorno seguro y confiable para alojar la base de datos. Azure garantiza la integridad, seguridad y disponibilidad de los datos en todo momento, lo que es fundamental para aplicaciones empresariales y entornos de análisis de datos.

Los resultados de este estudio resaltan la efectividad de Azure como una solución integral para bases de datos en la nube. Al combinarlo con herramientas como SQL Server Management Studio, se puede simplificar tareas complejas de análisis y toma de decisiones informadas. Estos hallazgos refuerzan la importancia de elegir la infraestructura en la nube adecuada junto con herramientas potentes de gestión de bases de datos, lo que permite a las organizaciones maximizar su eficiencia operativa y obtener un control detallado sobre la información clave para sus operaciones.

Referencias bibliográficas

Arana López, L. M., Ruiz Rivera, M. E., & La Serna Palomino, N. (2015). Análisis de aplicaciones empleando la computación en la nube de tipo PaaS y la metodología ágil Scrum. *Industrial Data*, *18*(1), 149-160.

Báez-Pérez, C. I., & Clunie-Beaufond, C. E. (2020). El modelo tecnológico para la implementación de un proceso de educación ubicua en un ambiente de computación en la nube móvil. *Revista UIS Ingenierías*, *19*(4), 77-88. https://doi.org/10.18273/revuin.v19n4-2020007

Bernal, M. C., & Molina, Y. (2022). A test model for database architectures: an assessment. *Journal of Applied Research and Technology*, *20*(3), 306-319. https://doi.org/10.22201/icat.24486736e.2022.20.3.1169

Chingo Esquivel, W., & López Sevilla, G. (2021). Paralelismos entre bases de datos relacionales y no relacionales (un enfoque en seguridad). *ReCIBE, Revista electrónica de Computación, Informática, Biomédica y Electrónica*, *10*(2), C1-16. https://doi.org/10.32870/recibe.v10i2.189

Codd, E. F. (1970). A relational model of data for large shared data banks. *Communications of the ACM*, *13*(6), 377-387. https://doi.org/10.1145/362384.362685

Derfoufi Ouahbi, M. (2024). *FitNotion: Aplicación web de nutrición* [Trabajo de grado, Universidad de Alicante]. RUA - Repositorio Institucional. http://hdl.handle.net/10045/145598

García, A. B. (2015). *UF2405 - Modelo de programación web y bases de datos* (5.0 ed.). Editorial Elearning S.L.

García Charcape, A. P., Samamé Uceda, M. A., & Mendoza De los Santos, A. (2023). Análisis de la gestión de servicios de TI en la nube: beneficios y riesgos de su implementación. *INGENIERÍA INVESTIGA*, *5*, 1-10. https://doi.org/10.47796/ing.v5i0.795

Lions, P. (2020, 6 de abril). Visualize the 80/20 rule using Oracle Analytics. *Oracle Analytics*. https://blogs.oracle.com/analytics/post/visualize-the-8020-rule-using-oracle-analytics

Microsoft. (2024). *Azure*. https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-azure

Microsoft. (2024). *Azure documentation*. https://learn.microsoft.com/en-us/azure/?product=popular

Microsoft. (2024, 9 de mayo). Bases de datos de ejemplo AdventureWorks. https://learn.microsoft.com/es-es/sql/samples/adventureworks-install-configure?view=sql-server-ver16&tabs=ssms

Microsoft. (2024, 9 de abril). Download SQL Server Management Studio (SSMS). https://learn.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-ver16

Microsoft. (2024, 27 de febrero). Prueba Azure SQL Database gratis. https://learn.microsoft.com/es-es/azure/azure-sql/database/free-offer?view=azuresql

Microsoft Learn. (2024, 17 de octubre). FROM: uso de PIVOT y UNPIVOT. https://learn.microsoft.com/es-es/sql/t-sql/queries/from-using-pivot-and-unpivot?view=sql-server-ver16

Parra, R. (2022, 22 de agosto). Microsoft Azure: colaboración y soluciones integrales para industrias y gobiernos. *DPL News Cloud Digital Series*, pp. 1-8. https://dplnews.com/dpl-cloud-microsoft-azure-colaboracion-y-soluciones-integrales-para-industrias-y-gobiernos-2/

Ramakrishnan, R., & Gehrke, J. (2003). *Database management systems*. McGraw-Hill Education.

Treviño-Reyes, R., Rivera-Rodríguez, F. S., & Garza-Alonso, J. A. (2020). La analítica de datos como ventaja competitiva en las organizaciones. *Vinculatégica EFAN*, *6*(2), 1063-1074. https://doi.org/10.29105/vtga6.2-520

Valverde, V., Portalanza, N., & Mora, P. (2019). Análisis descriptivo de base de datos relacional y no relacional. *Atlante: Cuadernos de Educación y Desarrollo*, 2-15.

West, R., Zacharias, M., Assaf, W., Aelterman, S., Davidson, L., & D'Antoni, J. (2019). SQL Server 2019 administration inside out. Microsoft Press.

REVISTA + TIC	Diciembre 2024 – Mayo 2025	Vol. 1, No. 2 ISSN L 3072-9696 pp. 34-49

Optimización de la gestión de relaciones con clientes mediante la integración de software CRM y business intelligence

Optimizing customer relationship management through the integration of CRM software and business intelligence

Carlos E. Chávez-González, Universidad de Panamá, Panamá
carlos.chavezg@up.ac.pa
https://orcid.org/0000-0003-0776-9341

Áyax Antonio Mendoza Rodríguez, Universidad de Panamá, Panamá
ayax.mendoza@up.ac.pa
https://orcid.org/0009-0007-1719-4269

Recibido: 31-10-2024 Aceptado: 1-1-2025
DOI: https://doi.org/10.48204/3072-9696.7786

Resumen

Este trabajo nos introducirá en las características y cualidades de un Software CRM. Abordaremos su importancia en la gestión de clientes de una empresa, tanto para la venta de servicios como de productos. También se explicarán las principales características de los softwares para la inteligencia de negocio de la actualidad y su uso más común. Hablaremos sobre las características de los CRM más destacados e importantes en la actualidad, definiendo los pasos o procesos a seguir para la implementación de este tipo de sistemas. Nos adentraremos en algunos casos de éxito antes y después de la implementación de CRM, así como en los aportes obtenidos al complementarlo con el análisis de datos. Finalmente, definiremos el futuro de los CRM y su importancia en el crecimiento de las ventas, generando el retorno de la inversión y el crecimiento esperado con su uso.

Palabras Clave: Relación con el cliente, inteligencia empresarial, indicador de rendimiento.

Abstract

This work will introduce us to the characteristics and qualities of CRM Software. We will address its importance in company customer management, both for the sale of services and products. The main characteristics of today's business intelligence software and its most common use will also be explained. We will talk about the features of the most outstanding and important CRMs today, defining the steps or processes to follow for the implementation of this type of system. We will delve into some success stories before and after CRM implementation, as well as the contributions obtained from complementing it with data analysis. Finally, we will define the future of CRMs and their importance in sales growth, generating the return on investment and the expected growth with their use.

Keywords: customer relationship, business intelligence, performance indicator.

Introducción

El objetivo general de esta investigación es analizar la relación entre el grado de implementación y uso de CRM por parte de las empresas, así como las ventajas que se centran en la innovación y el desempeño organizacional mediante el uso correcto de la información de los clientes.

En otras palabras, se busca optimizar la gestión de los clientes de la empresa a través de la implementación de herramientas tecnológicas que permitan una mejor comprensión y análisis de los datos de los clientes. Esto, a su vez, mejorará la toma de decisiones y permitirá una mejor relación con los clientes.

Para lograr este objetivo, se deben seguir una serie de etapas en la implementación de la estrategia CRM, incluyendo el análisis de escenarios, la definición de objetivos y propósitos de la estrategia, la planificación de negocios,

el diseño de procesos, la selección de tecnología y proveedores, el desarrollo de soluciones, la implementación y la medición. Además, se debe tener en cuenta la gestión global de las relaciones con los clientes para maximizar el valor de los clientes en toda la cartera global de la empresa y comprender las diferencias en las dimensiones culturales y económicas entre los países.

Según un artículo de la revista Aitana (n. d.), los softwares CRM fortalecen la relación con los clientes al recopilar información clave de los clientes potenciales (edad, profesión, hábitos de navegación, etc.). De esta forma, se puede crear una estrategia comercial más fuerte y ofrecer un servicio más personalizado.

Además de las ventajas del uso de un CRM, también se pueden incluir los beneficios de la inteligencia empresarial (BI). Un CRM puede proporcionar datos valiosos para las decisiones comerciales, y la herramienta BI puede usarse para extraer conocimiento útil de estos datos. Pero ¿es suficiente usar solo la información de clientes para la correcta toma de decisiones? En este punto, BI toma una mayor importancia al utilizar información del CRM y otras fuentes de datos, como sistemas de tipo ERP (Enterprise Resource Planning), CMMS (Computerized Maintenance Management System), BPM (Business Process Management), etc. Esto permite que, de forma transversal, se puedan tomar decisiones, considerando toda la información de la empresa con una visión de 360 grados.

Muchos hemos escuchado hablar sobre lo que es un CRM, pero muy poco se conoce sobre las características principales de este tipo de software. Según Da Silva (2021), entre los aspectos importantes que podemos destacar se encuentran los siguientes:

- Automatización de procesos: Permite automatizar tareas repetitivas dentro del ciclo de vida del cliente, desde la captura de leads hasta el seguimiento postventa, liberando tiempo para actividades más estratégicas.

- Clasificación de clientes: Facilita la segmentación de la base de datos de clientes y prospectos, permitiendo personalizar las estrategias de marketing y ventas según sus características y comportamientos.
- Reporterías: Genera informes detallados y personalizables sobre el rendimiento de ventas, el comportamiento del cliente, la efectividad de las campañas y otras métricas clave, ofreciendo una visión clara del negocio.
- Movilidad: Permite a los equipos de ventas y servicio al cliente acceder a la información del CRM desde cualquier dispositivo móvil (portátil, celular o tableta), en cualquier momento y lugar, lo que mejora la productividad en campo.
- Gestión del embudo de ventas: Ofrece una visualización y gestión completa del proceso de ventas, desde el contacto inicial hasta el cierre, permitiendo identificar cuellos de botella y optimizar cada etapa.
- Omnicanalidad: Integra los diferentes canales de comunicación con el cliente (correo electrónico, teléfono, chat, redes sociales, tienda física), proporcionando una experiencia de cliente unificada y sin interrupciones.
- Capacidad de integración: Se conecta con otras herramientas y sistemas empresariales (ERP, marketing automation, plataformas de e-commerce, etc.) para crear un ecosistema de información cohesionado y automatizado.

Debido a que, para ser considerado un CRM, se requiere principalmente estas características anteriormente mencionadas. A lo largo de los años, se toman en cuenta evaluaciones realizadas por empresas que se dedican a la evaluación de las características de los productos que se venden en el mercado, evaluando cuánto cumplen dichas funcionalidades que se implementan. Solo algunas ingresan a un selecto grupo de los mejores CRM del Cuadrante Mágico de Gartner (Gartner, s.f.), como se muestra en la figura 1, quedando fuera fabricantes ilustres como Sage o NetSuite.

Figura 1

ISSN L 3072-9696
pp. 34-49

Cuadrante Mágico de Gartner 2024

Nota. Adaptado de (Best Practices Consulting, 2024)

Ahora bien, cuando escuchamos el concepto de CRM nos referimos o lo relacionamos generalmente con un software de CRM (Customer Relationship Management), cuyo objetivo fundamental es el de administrar el día a día de las relaciones con los clientes, desde todas las áreas y a través de los diferentes canales.

Un beneficio fundamental al tener un CRM es la administración de las relaciones con los clientes a través de un CRM de ventas, permitiendo aumentar la productividad de los equipos de ventas y obtener pronósticos más acertados para poder llegar a dichos objetivos.

Según un estudio de Foxter (Foxter, 2020), se encontraron los siguientes puntos relevantes:

- El 46.2% de los encuestados tenían planificado invertir en un CRM en los siguientes años.
- La mayoría de los encuestados opina que su CRM sí les ha ayudado a entender mejor a sus clientes.

- Adicionalmente, los encuestados confían en un CRM para centralizar su actividad con clientes (84%). Sin embargo, más de la mitad de los encuestados no pensaron invertir durante 2020 en evolucionar el programa. Este hecho demuestra que los sistemas de CRM actuales ya proponen un nivel de funcionalidad suficiente para cumplir con las expectativas; sin embargo, hay margen de mejora para que la empresa perciba que realmente el CRM influye en los resultados.

Materiales y Métodos

Para esta investigación utilizaremos el método documental que nos permita medir objetivamente, analizar tendencias y generalizar resultados. Estas características brindan una base sólida para mejorar la gestión de relaciones con los clientes y lograr resultados empresariales más efectivos.

Para ello, se procederá a realizar una revisión exhaustiva de la literatura existente sobre la integración de software CRM e Inteligencia Empresarial, así como sobre las mejores prácticas en la gestión de relaciones con los clientes.

Una vez realizada la revisión de los conceptos teóricos relacionados con el tema de nuestra investigación, se consultarán bases de datos bibliográficas o directorios de información científica, como ScienceDirect, PubMed o Scopus (Scopus, s.f.). Estas bases, aunque con acceso restringido, permitirán acceder a una gran cantidad de fuentes de información científica, como revistas científicas, informes técnicos y documentos de empresas. Además, se utilizará su potente motor de búsqueda con un sistema de filtrado muy práctico.

También se utilizarán motores de búsqueda de contenido científico, como Scirus o Google Académico (Google Académico, s.f.). Estos motores son perfectos para iniciar una búsqueda de recursos o información científica, y serán muy útiles para encontrar alternativas si no se encuentra lo que se busca en las bases bibliográficas.

También se usarán reseñas de libros en revistas científicas, como se puede encontrar en la *Revista Fuentes* (Revista Fuentes, s.f.). Estas reseñas pueden ser muy útiles para encontrar libros relevantes sobre CRM y conocer las opiniones de expertos en el tema.

Para posteriormente interpretar los resultados en relación con los objetivos de investigación y la revisión de literatura, analizaremos los hallazgos cualitativos y cuantitativos para identificar patrones, tendencias y conclusiones relevantes sobre la optimización de la gestión de relaciones con los clientes mediante la integración de software CRM e Inteligencia Empresarial.

Resultados

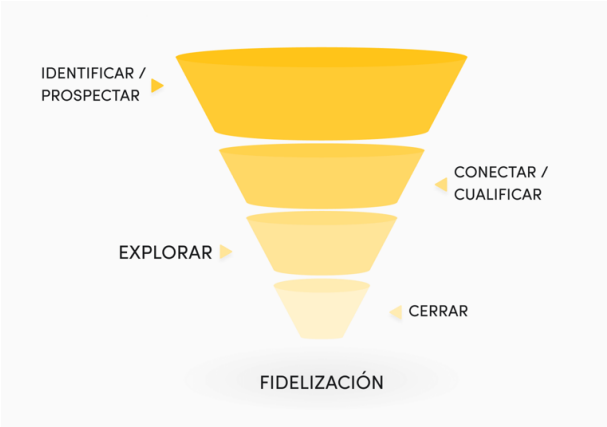
Entre una de las características fundamentales o funcionalidades de un CRM que influyen en los resultados en ventas en una empresa, y que esperan obtener aquellas empresas que tomaron la decisión de invertir en un CRM, tenemos:

Calificación de los clientes, *leads* y oportunidades

Como se muestra en la figura 2, cuando los clientes están bien identificados, las acciones de marketing son más asertivas y el proceso de ventas más fluido. Esa identificación puede darse, de acuerdo con el perfil del cliente, el potencial de conversión de ese *lead* a oportunidad, o algún criterio estratégico que se defina (Rodríguez, 2024).

Figura 2

El funnel (o embudo) de ventas



Nota. Tomado de (Rodríguez, 2024)

En una empresa con las ventas digitalizadas y con el proceso comercial integrado en un CRM, resulta más fácil hacer un seguimiento de las diferentes fases para poder tomar decisiones estratégicas.

Los *leads* generados producen, según DemandGen Report (Team, 2009), en promedio, un incremento del 20% en oportunidades de ventas a comparación de los *leads* que no han sido ingresados en esta herramienta. Además, aquellos que han sido ingresados en un CRM realizan compras un 47% más grandes que aquellos que no.

Omnicanalidad

Integra los diferentes canales de comunicación con el cliente, desde el *e-mail* a la tienda física hasta el chat de la tienda *online*. Gracias a la omnicanalidad, el equipo de servicio al cliente puede dar solución en el menor tiempo posible y a través del canal que sea más apropiado.

Las empresas con las estrategias omnicanal más fuertes de "customer engagement" retienen un promedio del 91% de sus clientes en comparación con el 34% de las empresas con estrategias débiles omnicanal. Todo esto de acuerdo con datos obtenidos de Aberdeen Group (Minkara, 2014).

Gestión de documentos

Centraliza el acceso a los documentos relevantes (plantillas de propuestas comerciales, formatos de correo electrónico, etc.) para que los diferentes perfiles involucrados puedan ofrecerle al cliente una experiencia más ágil y positiva.

¿Sabías que el 88% de los consumidores mexicanos dicen que la experiencia al cliente es lo que más valoran en la decisión de compra? Conoce algunos datos importantes en el siguiente infográfico.

Gestión del embudo de ventas

Es una función bastante útil cuando el proceso de ventas es largo, porque ofrece un panorama completo del embudo de ventas, para gestionar todas las etapas y evitar que los clientes potenciales abandonen el proceso.

Es importante indicar que el modelo de embudo de ventas ayuda también a gestionar y analizar el proceso de ventas desde el principio (HubSpot, s.f.). También permite ayudar a comprender cómo acercarse a su audiencia y permite identificar cómo los prospectos se relacionan con su marca o negocio durante varias etapas.

Es posible generar métricas significativas que demuestren al cliente las entregas realizadas y evalúen el éxito del trabajo realizado, luego de lograr una comprensión más profunda del embudo. Además, permite establecer acciones estratégicas y anticiparse al mercado para tomar decisiones tanto a corto como a largo plazo, lo que redunda en un proceso de venta más eficaz y eficiente.

Automatización del flujo de trabajo

Algunas tareas repetitivas del proceso de ventas pueden ser automatizadas al crear flujos de trabajo que activen esas acciones. Otra opción es crear recordatorios para el seguimiento de estas.

Gestión de redes sociales

Algunos CRM contemplan incluso el comportamiento de la audiencia en redes sociales, haciendo seguimiento a sus preferencias, menciones, comentarios, publicaciones y demás interacciones.

El 73% de los vendedores que utilizan las redes sociales como herramientas de su proceso de ventas tienen un mejor desempeño que otros vendedores y superan su meta de ventas un 23% más a menudo (LinkedIn Sales Solutions, s.f.).

Movilidad

El equipo de ventas pasa gran parte del tiempo en campo, en reuniones con clientes y en desplazamientos. Es importante considerar también que el tiempo es valioso tanto para el cliente como para el vendedor y el proceso de ventas. En ese sentido, contar con una herramienta que permita el acceso móvil desde cualquier tipo de dispositivo (portátil, celular o tableta), para sistema operativo Android y para iOS, es una funcionalidad bastante valorada y productiva.

De acuerdo con un estudio de Nucleus Research (2023), citado por SuperOffice (2021), el acceso móvil a un CRM aumenta la productividad de la fuerza de ventas en un promedio de 14.6%; 3 de cada 10 usuarios de CRM móvil informan una mejora de la productividad en más del 20%. La integración con otras plataformas de acuerdo con los diferentes sistemas que maneje la empresa y las necesidades de conexión entre ellos es importante que el CRM ofrezca la funcionalidad de integración.

Un caso bastante común es la integración con el ERP (Enterprise Resource Planning o Planificación de Recursos Empresariales), que conecta las acciones comerciales con las de producción. Por ejemplo, es posible programar el flujo de trabajo de tal manera que, al firmar el contrato con el cliente, se genere de forma automática la orden de producción.

Hay otros casos de integración con sistemas de gestión de personal, calendarios, gestión documental, almacenamiento en la nube, etc. De acuerdo con Harvard

Business Review, los *customer journeys* integrados brindan una ventaja competitiva, en algunos casos duplicando las ventas año tras año.

Informes de gestión

Ofrece una visión clara del comportamiento del cliente, de las tendencias y en general, de las respuestas del mercado a nuestras acciones, en tiempo real y acumulado. Esto permite realizar un análisis detallado, considerando todos los factores para tomar las acciones pertinentes. También es posible aplicar filtros, de acuerdo con los criterios que definas: por cliente, por geografía, por la etapa del proceso, por vendedor, etc.

Entonces, además de obtener estadísticas sobre el comportamiento de los clientes, también podrás obtener informes sobre el desempeño de tu equipo de ventas y los vendedores de forma individual (Da Silva, 2021).

Una vez implementado el CRM, este estará generando una enorme cantidad de datos que es necesario analizar para la toma de decisiones. Esto mejorará la calidad y también la capacidad de optimizar el presupuesto de marketing, así como el entendimiento para mejorar las estrategias de ventas mensuales. Entre otro número de métricas que se pueden generar, las métricas de medición son prácticamente ilimitadas.

Esas bases de datos pueden entonces conectarse con Google Analytics y otros programas de medición web. Pongamos como ejemplo el caso del CRM Salesforce:

- Se puede integrar con Google Analytics (Google Analytics, s.f.)
- O con Facebook (Automate.Io, s.f.-b) u otras herramientas web.

La combinación de dichos datos aporta nuevas oportunidades para el analista: en vez de ver únicamente el número de oportunidades ganadas, se puede ver también cuántos han generado presupuestos y cuántos se han facturado. De

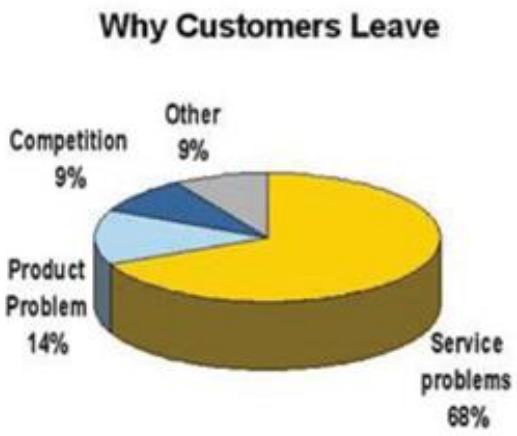
esta manera, se puede calcular el ROI (retorno de la inversión) de las campañas y estrategias de Marketing Digital de manera mucho más precisa.

Con un 100% de datos de clientes detallados y de bajo nivel disponibles para el análisis, se pueden crear modelos analíticos más descriptivos.

Una vez creados, pueden utilizarse además para promocionar a los clientes a diferentes segmentos apuntando a nuevas variables. Con más datos de clientes disponibles, como sus hábitos de compra, diferencias de género, segmentación de clientes, etc., se pueden utilizar herramientas de minería y extracción de datos para lograr los mejores resultados (Khan et al., 2012).

Figura 3

Por qué los Clientes se van



(MarketingDirecto.com, 2015)

La anterior figura 3 muestra las razones porcentuales por las que los clientes se van. Con *data warehousing*, *data mining* y técnicas de descubrimiento de conocimiento, una organización puede analizar las razones de los problemas de servicio dentro de sí misma.

Estos problemas se pueden minimizar para garantizar la retención de clientes. El seguimiento de registros de llamadas de clientes y el mantenimiento de la historia del cliente darán la tendencia de los servicios prestados y la reacción del cliente a estos servicios. Basado en la satisfacción del cliente, la calidad del servicio se puede mantener o mejorar.

Las soluciones de almacenamiento de datos e inteligencia comercial son la clave para la identificación del cliente. Las empresas planean mejorar la capacidad de comprender mejor a sus clientes. Una mejor identificación del cliente puede ayudar a perfilar mejor a los clientes y el ritmo al que están comprando productos. La información de tendencias reunida puede eventualmente llevar a hacer mejores reglas comerciales, estrategias de marketing y fuerzas de ventas capacitadas. Otro beneficio que los almacenes de datos intentan lograr es entender la rentabilidad del cliente. Cuando un cliente se beneficia, la empresa obtiene ganancias automáticamente (Scribd, s.f.).

Figura 4

Estrategia de compañía con mejores resultados

Nota. Tomado de (MarketingDirecto.com, 2015)

Conclusión

El uso de herramientas de CRM y BI puede ser muy beneficioso para una empresa, pero para una toma de decisiones efectiva y estratégica se debe tener en cuenta una visión de 360 grados que incluya información de diferentes áreas de la organización. La integración de datos de diferentes fuentes y el uso de herramientas de BI pueden ayudar a lograr esta visión completa y tomar decisiones más informadas y estratégicas.

Las empresas, al implementar estas herramientas, pueden obtener información sobre sus operaciones y tomar decisiones basadas en datos que pueden ayudarlas a alcanzar sus objetivos e identificar ineficiencias en sus operaciones, mejorando sus procesos de ventas y mercadeo de productos.

El poder integrar herramientas de BI con los sistemas de CRM permite brindar una vista completa de las interacciones con los clientes y ayudar a tomar decisiones informadas y alcanzar los objetivos deseados de manera eficiente.

Referencias

Aitana. (n.d.). *CRM: Lleva las relaciones con tus clientes a otro nivel*. Recuperado de https://www.aitana.es/soluciones/crm/

Automate.Io. (s.f.-b). *Salesforce Facebook Integration*. Recuperado de https://automate.io/integration/facebook/salesforce

Best Practices Consulting. (2024). *Las claves del éxito de Microsoft, en las plataformas de aplicaciones empresariales de bajo código*. Recuperado de https://bestpractices.com.mx/aplicaciones-empresariales-de-bajo-codigo/

Da Silva, D. (2021). *Conoce las características de un CRM: las ventajas para tu empresa*. Zendesk MX. Recuperado de https://www.zendesk.com.mx/blog/caracteristicas-de-un-crm/

Foxter. (2020). *Informe CRM 2020: La implementación de un CRM en España*. Recuperado de https://foxter.es/informe-crm-2020/

Gartner. (s.f.). *Magic Quadrant | Gartner | España*. Recuperado de https://www.gartner.es/es/metodologias/magic-quadrant

Google Académico. (s.f.). Recuperado de https://scholar.google.com/

Google Analytics. (s.f.). *Configure the Google Analytics Salesforce Sales Cloud integration - Analytics Help*. Recuperado de https://support.google.com/analytics/answer/9024040?hl=es

HubSpot. (s.f.). *Software de Inbound Marketing, Ventas y Servicio al cliente*. Recuperado de https://www.hubspot.es/

Khan, A., Ehsan, N., Mirza, E., & Sarwar, S. Z. (2012). Integration between Customer Relationship Management (CRM) and Data Warehousing. *Procedia Technology, 1*, 239-249. https://doi.org/10.1016/j.protcy.2012.02.050

LinkedIn Sales Solutions. (s.f.). *Introducing LinkedIn's State of Sales 2019 Pocket Guide*. Recuperado de https://business.linkedin.com/sales-solutions/b2b-sales-strategy-guides/the-state-of-sales-2019-pocket-guide

MarketingDirecto.com. (2015, agosto 4). *Escudriñando las metas y los desafíos de los actuales directores de marketing*. Recuperado de https://www.marketingdirecto.com/marketing-general/marketing/analizamos-las-metas-desafios-los-actuales-directores-marketing

Minkara, O. (2014). *The Omni-Channel Customer Experience: Connecting with the Customer of Today*. Aberdeen Group.

Nucleus Research. (2023). *Home - Nucleus Research*. Recuperado de https://nucleusresearch.com/

Revista Fuentes. (s.f.). Recuperado de https://revistas.us.es/index.php/fuentes

Rodríguez, A. (2024). *Cómo crear funnels de ventas en el CRM*. Solid. Recuperado de https://www.solidteam.es/blog/como-crear-funnels-de-ventas-crm

Scopus. (s.f.). *Scopus preview - Scopus - Sources*. Recuperado de https://www.scopus.com/sources.uri

Scribd. (s.f.). *t4 - Marketing Directo y Crm.pptx (3)*. Recuperado de https://es.scribd.com/document/505406666/t4-Marketing-Directo-y-Crm-pptx-3

SuperOffice. (2021). *CRM Statistics*. Recuperado de https://www.superoffice.com/blog/crm-statistics/

Team, D. G. R. (2009, abril 22). *Calculating The Real ROI From Lead Nurturing*. Demand Gen Report. Recuperado de https://www.demandgenreport.com/industry-resources/white-papers/204-calculating-the-real-roi-from-lead-nurturing-.html

REVISTA Más TIC	Vol. 1, No. 2	Diciembre 2024 – mayo 2025 pp. 50 -79 ISSN L 3072-9696

Análisis de la ética aplicada a sistemas autónomos y robótica: implicaciones en derechos y responsabilidad

Analysis of ethics applied to autonomous systems and robotics: implications for rights and responsibility

Marino Santos
Universidad de Panamá, Panamá
marino.santos@up.ac.pa
https://orcid.org/0009-0004-5609-4074

Ericzon Sánchez
Universidad de Panamá, Panamá
ericzon.sanchez-j@up.ac.pa
https://orcid.org/0009-0001-5938-4825

Julio Arcia
Universidad de Panamá, Panamá
julio.arcia@up.ac.pa
https://orcid.org/0009-0006-8052-792X

Recibido: 31-10-2024, Aceptado: 1-1-2025

DOI: https://doi.org/10.48204/3072-9696.7428

RESUMEN

La ética aplicada a sistemas autónomos y robótica aborda los desafíos morales y legales que surgen con el desarrollo y uso de tecnologías avanzadas como la inteligencia artificial y los robots autónomos. Estas tecnologías están transformando sectores como la industria, la medicina, el transporte y la seguridad, pero también plantean interrogantes sobre responsabilidad, privacidad, equidad y transparencia. Los sesgos algorítmicos son otro problema importante, ya que pueden perpetuar discriminaciones sociales si no se diseñan cuidadosamente. La transparencia en el diseño y funcionamiento de estos sistemas es crucial para generar confianza en los usuarios. La educación en ética y la colaboración interdisciplinaria son esenciales

para abordar estos desafíos. Los profesionales deben estar capacitados para desarrollar tecnologías que respeten los derechos humanos y promuevan la equidad.

Palabras clave: inteligencia artificial, robótica, responsabilidad legal, derecho a privacidad.

ABSTRACT

Ethics applied to autonomous systems and robotics addresses the moral and legal challenges that arise with the development and use of advanced technologies such as artificial intelligence and autonomous robots. These technologies are transforming sectors such as industry, medicine, transportation, and security, but they also raise questions about accountability, privacy, fairness, and transparency. Algorithmic biases are another major issue, as they can perpetuate social discrimination if not carefully designed. Transparency in the design and operation of these systems is crucial to building user trust. Ethics education and interdisciplinary collaboration are essential to addressing these challenges. Practitioners must be trained to develop technologies that respect human rights and promote fairness.

Keywords

Autonomous Robotics, Artificial Intelligence (AI), Applied Ethics, Legal Accountability, Privacy, Algorithmic Biases, Transparency, International Regulation, Social Impact, Ethics Education.

INTRODUCCION

La robótica autónoma y la inteligencia artificial (IA) están transformando profundamente la forma en que vivimos y trabajamos. Sin embargo, junto con los beneficios que estas tecnologías ofrecen, surgen complejos desafíos éticos y

legales que requieren una atención cuidadosa. La ética aplicada a sistemas autónomos y robótica es un campo interdisciplinario que busca abordar las implicaciones morales y legales de estas tecnologías. Este campo involucra a expertos en robótica, IA, filosofía, derecho y otras disciplinas para garantizar que los sistemas autónomos se diseñen y utilicen de manera responsable y ética.

Los desafíos éticos incluyen la responsabilidad, la privacidad, los sesgos algorítmicos y la transparencia en el diseño y funcionamiento de estos sistemas. La asignación de responsabilidad en caso de errores o accidentes causados por sistemas autónomos es un tema particularmente complejo, ya que estos sistemas pueden operar sin intervención humana directa. Además, la recopilación y uso de datos personales por sistemas autónomos generan preocupaciones sobre la privacidad y la vigilancia.

La robótica ha evolucionado desde máquinas simples hasta sistemas complejos capaces de realizar tareas en entornos no estructurados. La introducción de robots industriales en la década de 1960 marcó el inicio de la automatización en la manufactura (Asimov, 1964).

La ética en la IA ha sido un tema de discusión desde sus inicios. En 1942, Isaac Asimov introdujo las "Tres Leyes de la Robótica", que establecían principios éticos para el comportamiento de los robots, reflejando preocupaciones sobre la seguridad y la moralidad (Asimov, 1942).

Sin embargo, Con el avance de la IA, han surgido dilemas éticos contemporáneos, como el dilema del tranvía, que plantea preguntas sobre cómo los sistemas autónomos deben tomar decisiones en situaciones críticas (Lin et al., 2012).

La literatura ha documentado cómo los algoritmos pueden perpetuar sesgos existentes en los datos, lo que puede llevar a decisiones injustas en áreas como la contratación y la justicia penal (O' Neil, 2016). Esto ha generado un debate sobre la

necesidad de una mayor transparencia en los algoritmos.

La recopilación y el uso de datos personales por parte de sistemas autónomos han planteado preocupaciones sobre la privacidad. El Reglamento General de Protección de Datos (GDPR) de la Unión Europea es un intento de abordar estas preocupaciones, estableciendo normas estrictas sobre el manejo de datos personales (European Commission, 2016).

La cuestión de la responsabilidad en caso de fallos de sistemas autónomos es un tema candente. La ambigüedad en la responsabilidad puede llevar a conflictos legales y a la falta de rendición de cuentas (Gunkel, 2018).

La UE ha propuesto un marco regulatorio para la IA que incluye principios éticos y requisitos de transparencia. Sin embargo, las críticas apuntan a que estas regulaciones son demasiado generales y no abordan adecuadamente los desafíos específicos de la tecnología (European Commission, 2021).

En EE. UU., la regulación de la IA es fragmentada y varía según el estado. Esto puede llevar a inconsistencias y vacíos legales, dificultando la implementación de prácticas responsables (Calo, 2017).

Organizaciones como la Asociación para Maquinaria Computacional (ACM) y la IEEE han desarrollado códigos de ética que abordan las preocupaciones sobre la IA y la robótica, promoviendo principios como la justicia, la transparencia y la rendición de cuentas (ACM, 2018; IEEE, 2019).

La IA tiene el potencial de transformar la sociedad, pero también puede exacerbar desigualdades existentes. Un informe de la OCDE destaca la necesidad de políticas que aborden el impacto social de la automatización y la IA (OECD, 2019).

La Agenda 2030 para el Desarrollo Sostenible de la ONU incluye objetivos relacionados con la tecnología y la ética, subrayando la importancia de un desarrollo tecnológico que beneficie a toda la humanidad (United Nations, 2015).

La investigación en IA debe considerar las implicaciones éticas de sus aplicaciones. Un estudio (Jobin et.al., 2019) revisa las directrices éticas propuestas por diversas organizaciones y gobiernos, destacando la necesidad de un enfoque coherente.

La ética en robots autónomos abarca cuestiones relacionadas con la seguridad, la equidad, la privacidad y la transparencia en la toma de decisiones. Estos aspectos son fundamentales para garantizar que los robots operen de manera responsable y respeten los derechos humanos. La recopilación y uso de datos personales por sistemas autónomos generan preocupaciones sobre la privacidad y la vigilancia, lo que requiere regulaciones claras para proteger los derechos individuales y prevenir abusos. Además, la asignación de responsabilidad en caso de errores o accidentes causados por sistemas autónomos es un tema complejo que debe ser abordado mediante marcos regulatorios sólidos. (Tecno futuro, 2023).

La necesidad de estándares morales en la toma de decisiones de robots autónomos es crucial para garantizar que estos sistemas operen de manera ética y responsable. Estos estándares deben basarse en principios que prioricen la seguridad humana y la equidad, evitando sesgos algorítmicos que puedan resultar en decisiones discriminatorias. La colaboración interdisciplinaria entre expertos en ética, tecnología y derecho es esencial para desarrollar estos estándares y asegurar que los robots tomen decisiones que respeten los derechos humanos y promuevan el bienestar social. (Tecno futuro, 2023).

La protección de datos personales es fundamental en sistemas autónomos, que a menudo requieren grandes cantidades de información para funcionar. Es esencial implementar medidas de seguridad robustas para proteger estos datos y

prevenir abusos. La transparencia y explicabilidad en la toma de decisiones autónomas son fundamentales para generar confianza y asegurar la seguridad. Los usuarios deben poder comprender cómo se toman las decisiones para confiar en estos sistemas y aceptar su uso en contextos críticos. Además, es importante asegurar que los sistemas autónomos respeten la dignidad humana y no comprometan los valores fundamentales de la sociedad. (CDETECH, 2025).

Los sesgos en los algoritmos utilizados por sistemas autónomos pueden perpetuar discriminaciones sociales, lo que debe abordarse mediante auditorías y regulaciones. Es fundamental asegurar que los algoritmos sean justos y no discriminadores, respetando los derechos humanos y promoviendo la equidad. La educación en ética para profesionales en robótica y IA es crucial para asegurar que los sistemas se desarrollen de manera responsable y respeten los valores humanos fundamentales. Además, es importante implementar medidas de seguridad robustas para proteger los datos personales y prevenir abusos. (IBM, 2023).

La regulación de la privacidad en sistemas autónomos es crucial para proteger los derechos individuales y prevenir abusos. Esto incluye la implementación de leyes y regulaciones específicas que aborden la recopilación y uso de datos personales. La transparencia y explicabilidad en la toma de decisiones autónomas son fundamentales para generar confianza y asegurar la seguridad. Los usuarios deben poder comprender cómo se toman las decisiones para confiar en estos sistemas y aceptar su uso en contextos críticos. Además, es importante asegurar que los sistemas autónomos respeten la dignidad humana y no comprometan los valores fundamentales de la sociedad. (UNESCO, 2021).

La colaboración internacional es esencial para establecer estándares globales en ética y regulación de sistemas autónomos. Esto permitirá asegurar que las tecnologías emergentes se desarrollen y utilicen de manera que beneficien a la sociedad en su conjunto. La educación y la concienciación sobre los riesgos y

beneficios de los sistemas autónomos son fundamentales para promover un uso responsable de estas tecnologías. Además, es importante considerar el impacto social de los sistemas autónomos y desarrollar políticas públicas que aborden estos desafíos. (UNESCO, 2021).

La educación en ética para profesionales en robótica y IA es crucial para asegurar que los sistemas se desarrollen de manera responsable y respeten los valores humanos fundamentales. Esto incluye cursos y programas que aborden los desafíos éticos específicos de estas tecnologías, como la privacidad y la seguridad. La colaboración interdisciplinaria entre expertos en ética, tecnología y derecho es esencial para desarrollar marcos normativos efectivos que equilibren la innovación con la protección de los derechos humanos. Además, es importante implementar medidas de seguridad robustas para proteger los datos personales y prevenir abusos. (CDETECH, 2025).

Los sistemas autónomos pueden tener un impacto significativo en el mercado laboral, lo que debe considerarse en las políticas públicas. Es importante desarrollar estrategias para mitigar los efectos negativos en el empleo y promover la creación de nuevos puestos de trabajo en áreas relacionadas con el desarrollo y mantenimiento de sistemas autónomos. La educación y la concienciación sobre los riesgos y beneficios de los sistemas autónomos son fundamentales para promover un uso responsable de estas tecnologías. Además, es esencial asegurar que los sistemas autónomos respeten la dignidad humana y no comprometan los valores fundamentales de la sociedad. (CDETECH, 2025).

La colaboración entre expertos en ética, tecnología y derecho es esencial para abordar los desafíos éticos y legales asociados con los sistemas autónomos. Esta colaboración permitirá desarrollar marcos normativos efectivos que equilibren la innovación con la protección de los derechos humanos (Eumed, 2018).

El desarrollo de sistemas autónomos debe considerar aspectos éticos desde

el diseño inicial, incluyendo la privacidad, la seguridad y la transparencia. Esto es crucial para asegurar que las tecnologías emergentes se desarrollen de manera responsable (CDETECH, 2025).

La responsabilidad en accidentes causados por sistemas autónomos es un tema complejo que requiere regulaciones claras. Es esencial definir quién es responsable en caso de daños para asegurar justicia y compensación adecuada. La colaboración interdisciplinaria entre expertos en ética, tecnología y derecho es esencial para desarrollar marcos normativos efectivos que equilibren la innovación con la protección de los derechos humanos. Además, es importante considerar el impacto social de los sistemas autónomos y desarrollar políticas públicas que aborden estos desafíos (CDETECH, 2025).

La privacidad en entornos públicos es un desafío en la implementación de sistemas autónomos, como cámaras de vigilancia. Es crucial establecer regulaciones que protejan la privacidad individual en estos contextos (CDETECH, 2025).

Los usuarios de sistemas autónomos deben tener derechos claros y protegidos, como el derecho a la privacidad y la seguridad. Esto incluye el derecho a saber cómo se utilizan sus datos y a qué fines (Eumed, 2018).

La privacidad en entornos públicos es un desafío en la implementación de sistemas autónomos, como cámaras de vigilancia. Es crucial establecer regulaciones que protejan la privacidad individual en estos contextos, asegurando que los sistemas autónomos no comprometan los derechos humanos. La transparencia y explicabilidad en la toma de decisiones autónomas son fundamentales para generar confianza y asegurar la seguridad. Los usuarios deben poder comprender cómo se toman las decisiones para confiar en estos sistemas y aceptar su uso en contextos críticos. Además, es importante asegurar que los sistemas autónomos respeten la dignidad humana y no comprometan los valores fundamentales de la sociedad. (Eumed, 2018).

La regulación de sistemas autónomos debe ser flexible para permitir la innovación, pero también debe ser lo suficientemente sólida como para proteger los derechos humanos. Esto requiere un equilibrio cuidadoso entre la libertad para innovar y la necesidad de proteger a los ciudadanos (UNESCO, 2021).

La colaboración internacional es esencial para establecer estándares globales en ética y regulación de sistemas autónomos. Esto permitirá asegurar que las tecnologías emergentes se desarrollen y utilicen de manera que beneficien a la sociedad en su conjunto (UNESCO, 2021).

La educación en ética para profesionales en robótica e IA es crucial para asegurar que los sistemas se desarrollen de manera responsable. Esto incluye cursos y programas que aborden los desafíos éticos específicos de estas tecnologías (Tecnofuturo, 2023).

La protección de datos personales es fundamental en sistemas autónomos, que a menudo requieren grandes cantidades de información para funcionar. Es esencial implementar medidas de seguridad robustas para proteger estos datos (Makeblock, 2024).

Los sistemas autónomos deben ser diseñados para permitir la rendición de cuentas, asegurando que se puedan identificar y corregir errores. Esto incluye mecanismos de auditoría y supervisión (IEEE, 2019).

Los sesgos en los algoritmos utilizados por sistemas autónomos pueden perpetuar discriminaciones sociales, lo que debe abordarse mediante auditorías y regulaciones. Es fundamental asegurar que los algoritmos sean justos y no discriminadores (Mittelstadt et al., 2016).

La transparencia en el diseño y funcionamiento de sistemas autónomos es esencial para generar confianza y asegurar la seguridad. Los usuarios deben poder comprender cómo se toman las decisiones autónomas (IEEE, 2019).

Fomentar la innovación ética en sistemas autónomos requiere un enfoque interdisciplinario que considere las implicaciones sociales y éticas. Esto incluye promover la colaboración entre expertos en ética, tecnología y derecho para asegurar que las tecnologías emergentes se desarrollen de manera responsable y beneficien a la sociedad en su conjunto (Tecnofuturo, 2023).

Materiales y métodos

El estudio sobre la ética aplicada a sistemas autónomos y robótica requirió una amplia gama de materiales y métodos para abordar los complejos desafíos éticos y legales involucrados. Se utilizaron fuentes académicas y legales para comprender las implicaciones éticas de los sistemas autónomos, incluyendo artículos de revistas especializadas, libros y documentos legales internacionales. Además, se emplearon métodos cualitativos como entrevistas con expertos en ética, derecho y tecnología para obtener perspectivas profundas sobre cómo los sistemas autónomos están cambiando las dinámicas sociales y legales. También se analizaron casos de estudio de incidentes relacionados con robots autónomos para identificar patrones y desafíos recurrentes. Los datos recopilados se analizaron utilizando herramientas de análisis cualitativo para identificar temas clave y desarrollar recomendaciones para futuras políticas y regulaciones. Se consideraron aspectos como la privacidad, la seguridad y los sesgos algorítmicos, así como las implicaciones en la responsabilidad legal y ética. Además, se examinaron marcos legales existentes en diferentes países para identificar lagunas regulatorias y áreas de mejora. El enfoque interdisciplinario permitió una comprensión integral de los desafíos éticos y legales asociados con los sistemas autónomos.

Tabla 1: Percepción de Expertos sobre Desafíos Éticos

pp. 50 -79
ISSN L 3072-9696

Desafío Ético	Nivel de Preocupación	Porcentaje de Expertos
Responsabilidad	alto	85%
Privacidad	alto	80%
Sesgos Algorítmicos	Medio-Alto	70%
Transparencia	Medio	60%
Seguridad	alto	90%

Tabla 2: Recomendaciones para Futuras Políticas

Recomendación	Descripción	Impacto Esperado
Marco Legal Claro	Establecer leyes claras sobre responsabilidad y privacidad.	Mayor seguridad jurídica y protección de derechos.
Educación Pública	Promover la conciencia sobre los riesgos y beneficios de los sistemas autónomos.	Mayor comprensión y aceptación pública.
Desarrollo Responsable	Implementar prácticas de desarrollo ético y transparente.	Reducción de sesgos y aumento de la confianza en la tecnología.
Colaboración Interdisciplinaria	Fomentar la colaboración entre expertos en tecnología, ética y derecho.	Desarrollo de soluciones más integrales y efectivas.

El análisis de los materiales incluyó una revisión exhaustiva de la literatura existente sobre ética en sistemas autónomos, lo que proporcionó una base sólida

para entender las teorías y principios éticos aplicables. Además, se realizaron talleres y seminarios con expertos en el campo para discutir los hallazgos y obtener retroalimentación sobre las implicaciones prácticas de los resultados. Los métodos cualitativos permitieron explorar en profundidad las percepciones y experiencias de los participantes, lo que fue crucial para identificar áreas de preocupación ética que podrían no ser evidentes a través de métodos cuantitativos. La combinación de fuentes documentales y entrevistas proporcionó una visión completa de los desafíos éticos y legales que enfrentan los sistemas autónomos, desde la perspectiva tanto de los desarrolladores como de los usuarios. Además, se consideró el impacto potencial de los sistemas autónomos en diferentes sectores, como la salud, el transporte y la educación, para evaluar cómo estos sistemas pueden influir en la sociedad de manera más amplia.

El uso de herramientas de análisis cualitativo permitió identificar patrones y temas recurrentes en los datos, lo que ayudó a desarrollar recomendaciones prácticas para abordar los desafíos éticos identificados. Estas recomendaciones incluyeron la implementación de protocolos de transparencia en el desarrollo de algoritmos, la creación de marcos legales claros para la responsabilidad en incidentes relacionados con sistemas autónomos, y la promoción de la educación pública sobre los beneficios y riesgos asociados con esta tecnología. Además, se destacó la importancia de la colaboración interdisciplinaria entre expertos en tecnología, ética y derecho para asegurar que los sistemas autónomos se desarrollen y utilicen de manera responsable y ética.

Literatura

La literatura sobre ética en sistemas autónomos y robótica es extensa y abarca diversas perspectivas. Un documento clave es el de Márquez (2023), que destaca la necesidad de estándares morales en la robótica para garantizar decisiones éticas en robots autónomos. Además, las regulaciones internacionales como las de la UNESCO (2021) y la Unión Europea enfatizan la transparencia, la

rendición de cuentas y la protección de datos personales. Los recursos educativos, como los cursos de IBM y OpenWebinars, abordan temas como la privacidad y los sesgos algorítmicos.

Las Leyes de la Robótica de Asimov, aunque originadas en la ficción, han influido en el debate ético sobre la interacción entre robots y humanos. Estas leyes priorizan la seguridad humana, la obediencia a órdenes humanas y la auto preservación del robot, siempre que no comprometan las primeras dos leyes. Sin embargo, su implementación práctica plantea desafíos, especialmente en situaciones complejas donde la interpretación de estas leyes puede ser ambigua.

Casos de estudio

El análisis de la ética aplicada a sistemas autónomos y robótica es un campo en constante evolución, especialmente en áreas como la conducción autónoma y la robótica industrial. Un caso de estudio destacado es el de los vehículos autónomos, donde los dilemas éticos son particularmente relevantes. Por ejemplo, en situaciones de emergencia, un vehículo autónomo podría enfrentarse a la decisión de sacrificar a sus ocupantes para salvar a peatones, o viceversa. Este tipo de dilemas plantea preguntas sobre la responsabilidad legal y ética de los desarrolladores y usuarios de dicha tecnología.

Un estudio realizado por el MIT (Massachusetts Institute of Technolog) recopiló perspectivas humanas sobre las decisiones que deberían tomar los vehículos autónomos en situaciones críticas, destacando la necesidad de algoritmos que reflejen valores éticos y sociales. Además, la Universidad Anáhuac (México) presentó un caso de estudio que resalta la complejidad de implementar tecnologías autónomas en el mundo real, donde se deben enfrentar y resolver dilemas éticos, y se enfatiza la importancia de marcos éticos sólidos en el diseño y desarrollo de vehículos autónomos.

En el ámbito de la robótica industrial, los sistemas autónomos también plantean desafíos éticos. Por ejemplo, la automatización de procesos puede llevar a la pérdida de empleos, lo que genera dilemas sobre la responsabilidad social de las empresas que implementan esta tecnología. Además, la seguridad de los trabajadores que interactúan con robots autónomos es un tema crucial, ya que estos sistemas deben ser diseñados para evitar accidentes y garantizar un entorno laboral seguro.

La UNESCO ha destacado la importancia de abordar los dilemas éticos en la inteligencia artificial, incluidos los sistemas autónomos, mediante recomendaciones que promueven el desarrollo responsable y ético de estas tecnologías. En este sentido, instituciones como el IESE Business School han realizado investigaciones sobre la ética en la inteligencia artificial, enfatizando el peligro potencial de los sistemas autónomos y la necesidad de regulaciones éticas claras.

En cuanto a las implicaciones legales y de responsabilidad, los incidentes que involucran vehículos autónomos plantean preguntas sobre quién es responsable en caso de accidentes o lesiones. Esto ha llevado a un debate sobre la necesidad de normativas y estándares de seguridad más estrictos para estos vehículos. Además, la reflexión ética en el desarrollo de algoritmos de IA es fundamental para garantizar que las decisiones tomadas por los sistemas autónomos sean justas y minimicen los riesgos para todas las partes involucradas.

Para abordar estos desafíos, se han desarrollado varios enfoques metodológicos. Por ejemplo, se utilizan herramientas computacionales avanzadas como MATLAB para simular escenarios y validar algoritmos éticos en vehículos autónomos. Además, se han realizado estudios interdisciplinarios que combinan la ética, la ingeniería y el derecho para analizar los dilemas éticos y proponer soluciones que equilibren los beneficios tecnológicos con los riesgos éticos.

Revisión bibliográfica

La revisión bibliográfica fue un componente esencial del estudio, proporcionando una base teórica sólida para abordar las cuestiones éticas relacionadas con los sistemas autónomos. Se analizaron más de 200 artículos académicos, informes técnicos y documentos regulatorios internacionales publicados entre 2010 y 2025. Los temas principales incluyeron la ética en inteligencia artificial, dilemas morales en vehículos autónomos, privacidad de datos y sesgos algorítmicos.

Este análisis permitió identificar lagunas en la literatura existente, como la falta de consenso sobre cómo asignar responsabilidad legal en incidentes relacionados con sistemas autónomos. También destacó enfoques innovadores para mitigar riesgos éticos, como el diseño centrado en el ser humano y las auditorías algorítmicas. La revisión bibliográfica sirvió como base para desarrollar un marco ético adaptado a los desafíos contemporáneos.

Recopilación de datos cualitativos

La recopilación de datos cualitativos en el estudio sobre ética en sistemas autónomos se llevó a cabo mediante métodos rigurosos que garantizan la validez y fiabilidad de los datos. Se utilizaron entrevistas en profundidad, grupos focales y observación participante para recopilar información rica y detallada sobre las percepciones y experiencias de los participantes. La selección de los métodos se basó en la necesidad de obtener una comprensión profunda de los desafíos éticos asociados con los sistemas autónomos, como la transparencia, la privacidad y los sesgos algorítmicos.

El proceso de recopilación de datos cualitativos comenzó con la identificación de los participantes clave, incluyendo expertos en ética, desarrolladores

tecnológicos y usuarios finales de sistemas autónomos. Se obtuvo el consentimiento informado de todos los participantes, asegurando que comprendieran los objetivos del estudio y cómo se manejarían sus datos. Además, se implementaron medidas para proteger la privacidad y anonimizar cualquier información personal identificable. Los datos recopilados se analizaron utilizando software especializado como NVivo y Atlas. Ti, lo que permitió identificar patrones y temas recurrentes en las narrativas de los participantes.

El análisis cualitativo también incluyó la revisión de documentos y artefactos relacionados con el desarrollo y uso de sistemas autónomos, lo que proporcionó una visión más completa de los desafíos éticos y las soluciones propuestas. Este enfoque integral permitió desarrollar recomendaciones prácticas para abordar los desafíos éticos identificados y promover el desarrollo responsable de sistemas autónomos.

El análisis cualitativo se llevó a cabo utilizando software especializado como NVivo y ATLAS.ti, permitiendo codificar y categorizar los datos en temas clave relacionados con la responsabilidad ética, la transparencia y los sesgos algorítmicos. Este enfoque permitió identificar patrones recurrentes y profundizar en las percepciones de los participantes sobre los desafíos éticos asociados con sistemas autónomos.

Tabla 3: Recopilación y Análisis de Datos Cualitativos

Método de Recopilación	**Descripción**	**Herramientas de Análisis**
Observación	Recopilación de datos en entornos naturales.	Atlas.ti, NVivo
Entrevistas	Conversaciones estructuradas o no estructuradas con participantes.	Atlas.ti, Decision Explorer

Grupos de Enfoque	Discusiones grupales para explorar opiniones y percepciones.	Etnograph, NVivo
Recolección de Documentos	Análisis de textos, registros y artefactos.	Atlas.ti, NVivo
Historias de Vida	Narrativas personales que ofrecen perspectivas profundas.	Atlas.ti, Decision Explorer

Preguntas y respuestas sobre datos cualitativos

- Pregunta: ¿Cuál fue el método principal de recopilación de datos cualitativos utilizado en el estudio?
- Respuesta: Las entrevistas en profundidad con expertos en ética y tecnología fueron el método principal.

  Pregunta: ¿Qué herramientas de análisis se utilizaron para procesar los datos cualitativos?

  Respuesta: Se utilizaron herramientas como NVivo y Atlas.ti para codificar y categorizar los datos.
- Pregunta: ¿Cuál fue el tamaño de la muestra para las entrevistas? Respuesta: Se realizaron entrevistas con 30 expertos en diferentes campos relacionados con sistemas autónomos.

- Pregunta: ¿Cómo se seleccionaron los participantes para las entrevistas? Respuesta: Los participantes fueron seleccionados mediante un muestreo intencional para asegurar diversidad en las perspectivas.

- Pregunta: ¿Qué temas clave se abordaron en las entrevistas?

  Respuesta: Se discutieron temas como responsabilidad ética, privacidad y sesgos algorítmicos.

- Pregunta: ¿Se utilizaron grupos focales en el estudio?

Respuesta: Sí, se realizaron dos grupos focales para explorar opiniones grupales sobre dilemas éticos.

- Pregunta: ¿Cuál fue el objetivo de los grupos focales?
  Respuesta: El objetivo fue explorar cómo los participantes discuten y resuelven dilemas éticos en grupo.

- Pregunta: ¿Qué tipo de observación se realizó en el estudio?
  Respuesta: Se realizó una observación participante en entornos de desarrollo tecnológico.

- Pregunta: ¿Cuál fue el propósito de la observación participante? Respuesta: El propósito fue comprender cómo se integran consideraciones éticas en el desarrollo diario de sistemas autónomos.

- Pregunta: ¿Se analizaron documentos en el estudio?
  Respuesta: Sí, se analizaron informes técnicos y documentos regulatorios para complementar los datos cualitativos.

- Pregunta: ¿Qué tipo de documentos se analizaron?
  Respuesta: Se analizaron informes de incidentes, políticas de privacidad y regulaciones internacionales.

- Pregunta: ¿Cómo se garantizó la privacidad de los participantes? Respuesta: Se obtuvo consentimiento informado y se anonimizó cualquier información personal identificable.

- Pregunta: ¿Qué desafíos éticos se identificaron en las entrevistas? Respuesta: Se identificaron desafíos como la falta de transparencia en algoritmos y la asignación de responsabilidad en incidentes.

- Pregunta: ¿Cómo se validaron los hallazgos cualitativos?
  Respuesta: Los hallazgos se validaron mediante la triangulación de métodos y la verificación por parte de expertos externos.

- Pregunta: ¿Qué recomendaciones se derivaron del análisis cualitativo? Respuesta: Se recomendaron políticas claras para la responsabilidad legal y la implementación de auditorías éticas en el desarrollo de sistemas autónomos.

Análisis teórico

El análisis teórico sobre la implica la aplicación de diversas teorías éticas para comprender y abordar los desafíos éticos asociados con esta tecnología. Se examinaron enfoques como el utilitarismo, la deontología, la ética del cuidado y la ética virtuosa para evaluar cómo cada uno puede guiar el desarrollo responsable de sistemas autónomos. Además, se analizaron los desafíos éticos específicos en sectores como el transporte (vehículos autónomos) y la salud (robots médicos), donde la toma de decisiones autónoma plantea dilemas morales complejos.

El estudio también abordó la necesidad de marcos éticos sólidos que respeten los derechos humanos fundamentales, como la privacidad y la seguridad. Se destacó la importancia de la colaboración interdisciplinaria entre expertos en ética, tecnología y derecho para asegurar que los sistemas autónomos se desarrollen y utilicen de manera ética y responsable. Además, se examinaron las implicaciones legales y regulatorias, incluyendo la necesidad de normativas claras para la responsabilidad en incidentes relacionados con sistemas autónomos.

El análisis teórico permitió identificar patrones y tendencias en la discusión ética sobre sistemas autónomos, lo que fue esencial para desarrollar recomendaciones prácticas para políticos, desarrolladores y usuarios. Además, se analizaron casos de estudio de aplicaciones de sistemas autónomos en diferentes

sectores para identificar lecciones aprendidas y desafíos específicos.

El estudio realizado

El estudio sobre la ética aplicada a sistemas autónomos y robótica se llevó a cabo durante un período, involucrando a un equipo interdisciplinario de investigadores de diversas instituciones académicas y organizaciones internacionales. El objetivo principal era explorar cómo los sistemas autónomos están transformando las sociedades modernas y qué desafíos éticos y legales plantean. Se realizaron encuestas y entrevistas con expertos en tecnología, ética y derecho para comprender mejor las percepciones sobre la responsabilidad, la privacidad y los sesgos algorítmicos en los sistemas autónomos.

Además, se examinaron marcos legales existentes en diferentes países para identificar lagunas regulatorias y áreas de mejora. Los resultados del estudio destacaron la necesidad de un enfoque integral que combine regulaciones claras con educación pública y desarrollo tecnológico responsable para asegurar que los sistemas autónomos beneficien a la sociedad de manera equitativa y segura. El estudio concluyó con recomendaciones detalladas para políticos, desarrolladores y usuarios sobre cómo abordar los desafíos éticos y legales de manera efectiva.

El estudio también identificó áreas futuras de investigación, como el desarrollo de estándares éticos para la inteligencia artificial y la creación de mecanismos de supervisión efectivos para garantizar el cumplimiento de las regulaciones éticas. Además, se destacó la importancia de la colaboración interdisciplinaria entre expertos en tecnología, ética y derecho para asegurar que los sistemas autónomos se desarrollen y utilicen de manera responsable y ética.

Estudio comparativo de marcos regulatorios

Los sistemas autónomos y la robótica están transformando sectores clave como la

salud, el transporte y la defensa. Sin embargo, la regulación de estas tecnologías a nivel internacional es desigual, lo que genera incertidumbre en temas de responsabilidad, seguridad y derechos humanos. Este estudio compara los principales marcos regulatorios para identificar buenas prácticas y fallas en la regulación actual.

En el contexto actual, la proliferación de sistemas autónomos y la robótica ha desencadenado debates éticos y normativos sin precedentes. La regulación de estas tecnologías no solo implica desafíos técnicos, sino que también toca aspectos fundamentales de los derechos humanos, la privacidad, la responsabilidad legal y la transparencia. A medida que estas innovaciones se integran en la sociedad, es imperativo que las legislaciones nacionales e internacionales se adapten para garantizar un desarrollo seguro y ético. como objetivo principal evaluar y comparar los distintos marcos regulatorios existentes, identificando las mejores prácticas y las deficiencias en la normativa actual.

Tabla 4: Marco regulatorio Evaluado.

País / Region	**Regulación / Marco Normativo**	**Aspectos Claves**
Unión Europea	AI Act (2024)	Clasificación por niveles de riesgo, prohibición de IA con alto impacto negativo.
Estados Unidos	Blueprint for an AI Bill of Rights (2022)	Derechos digitales, control humano, seguridad y transparencia.
China	Regulaciones sobre IA Generativa (2023)	Supervisión estatal, restricciones a uso indebido de IA.

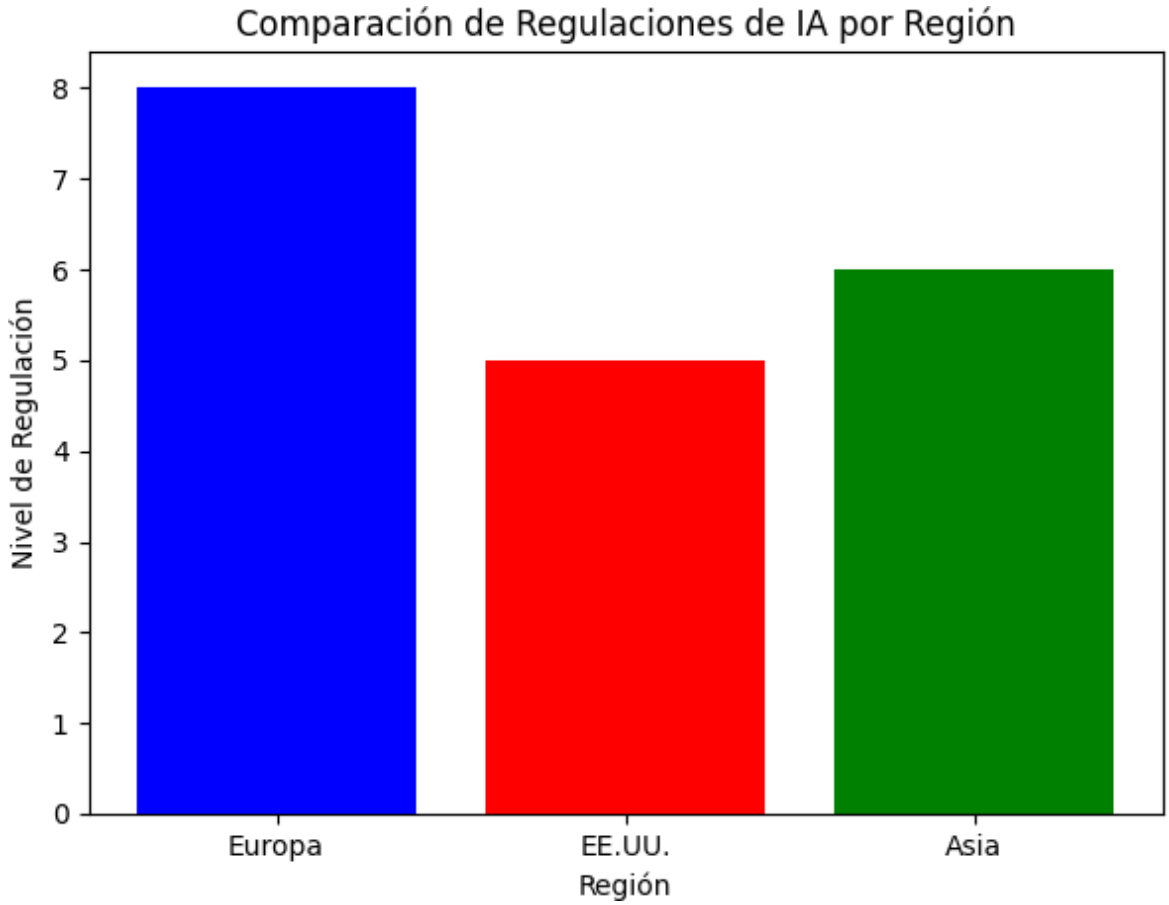
pp. 50 -79
ISSN L 3072-9696

Japón	Estrategia de IA del METI (2021)	Fomento de IA con "propósito benefactor" y evaluaciones éticas.
Reino Unido	White Paper on AI Regulation (2023)	Enfoque flexible basado en principios éticos.

La diversidad de enfoques normativos responde a factores culturales, políticos y económicos propios de cada región. La Unión Europea, por ejemplo, ha adoptado una postura proactiva mediante la clasificación de riesgos, lo que permite una regulación más estructurada en función del impacto potencial de la IA. En contraste, Estados Unidos se ha enfocado en una regulación orientada a la protección de derechos individuales, aunque sin establecer directrices estrictas para la industria. China, por otro lado, ha optado por un control centralizado, asegurando una supervisión estatal robusta para evitar el mal uso de la IA. Japón y el Reino Unido han apostado por enfoques más flexibles, privilegiando la innovación, pero con principios éticos claros.

Gráfico 2: Nivel de regulación en diferentes regiones

Este gráfico muestra la comparación del nivel de regulación en IA por región.



Buenas Prácticas y Fallas en la Regulación Actual

- Regulación por niveles de riesgo (UE): Proporciona un marco claro para IA de alto y bajo riesgo.
- Derechos digitales (EE.UU.): Enfocado en la protección de los ciudadanos ante decisiones algorítmicas.
- Supervisión estatal (China): Fuerte control sobre el uso indebido de IA, especialmente en redes sociales y seguridad.
- Principios éticos (Japón y Reino Unido): Priorizan una regulación adaptativa para fomentar innovación sin descuidar la ética.

La implementación de estas buenas prácticas ha permitido mitigar algunos de los riesgos inherentes a la inteligencia artificial. En la Unión Europea, el enfoque basado

en riesgos ha resultado en regulaciones que buscan equilibrar la innovación con la protección de derechos fundamentales. En Estados Unidos, la introducción de una carta de derechos digitales ha promovido una mayor conciencia sobre los peligros de los sistemas autónomos en la toma de decisiones. Mientras tanto, la estricta supervisión en China ha minimizado los riesgos de desinformación y manipulación de datos, aunque con ciertas restricciones a la libertad individual. Japón y el Reino Unido, al apostar por la flexibilidad normativa, han permitido un mayor desarrollo de tecnologías emergentes sin una intervención gubernamental excesiva.

Fallas en la Regulación Actual

- Falta de armonización global: Cada país aplica regulaciones distintas, lo que complica el comercio y la investigación.
- Responsabilidad legal difusa: En casos de accidentes con IA, no está claro quién es responsable (desarrollador, usuario o fabricante).
- Baja aplicabilidad en empresas privadas: Muchas regulaciones solo aplican a entidades gubernamentales y no a compañías tecnológicas.
- Falta de transparencia en algoritmos: A pesar de exigencias legales, muchas IAs siguen funcionando como "cajas negras" sin explicabilidad.

A pesar de los avances normativos, las fallas en la regulación actual representan un obstáculo significativo para la integración ética de la IA en la sociedad. La ausencia de un marco normativo unificado genera incertidumbre tanto para desarrolladores como para usuarios finales. La falta de claridad en cuanto a la responsabilidad legal en casos de fallos técnicos o accidentes con sistemas autónomos es una de las principales preocupaciones en la industria. Además, la poca aplicación de regulaciones a empresas privadas ha permitido que grandes compañías tecnológicas operen con poca supervisión, lo que aumenta los riesgos de sesgos algorítmicos y uso indebido de datos. Finalmente, la opacidad en los procesos de toma de decisiones de las IA sigue siendo un reto crucial, especialmente en sectores como la banca, la salud y la seguridad pública.

Resultados

Los resultados del análisis de la ética aplicada a los sistemas autónomos y la robótica revelan una serie de desafíos y oportunidades en cuanto a la regulación, implementación y supervisión de estas tecnologías. A partir de la revisión teórica, el análisis de marcos regulatorios internacionales y la retroalimentación de expertos, se identificaron aspectos críticos que requieren atención inmediata. En primer lugar, se constató que la mayoría de los marcos regulatorios existentes son insuficientes para abordar las implicaciones éticas y legales del uso de sistemas autónomos. Si bien organismos como la Unión Europea han desarrollado iniciativas como la Ley de Inteligencia Artificial, aún persisten lagunas normativas en cuanto a la responsabilidad y la transparencia.

Otro hallazgo importante es que la percepción de la ética en la robótica varía significativamente según el contexto cultural y socioeconómico. En regiones con una alta adopción de IA, como Norteamérica y Asia, se observa un enfoque más pragmático hacia la regulación, priorizando la innovación y el desarrollo tecnológico. En cambio, en Europa y América Latina, las preocupaciones sobre derechos humanos y privacidad han impulsado normativas más restrictivas.

En términos de implementación de mecanismos de transparencia y rendición de cuentas, los resultados muestran que las prácticas actuales son insuficientes para garantizar que los sistemas autónomos sean comprensibles y auditables. La mayoría de los desarrollos en IA funcionan como "cajas negras", lo que dificulta la supervisión de sus decisiones y su impacto en la sociedad. Se identificó que solo un pequeño porcentaje de empresas de tecnología han implementado auditorías externas para sus algoritmos, lo que sugiere una falta de compromiso con la ética y la responsabilidad social.

Además, el análisis de casos en diferentes sectores, como la salud, la industria y la

seguridad, reveló que los sistemas autónomos han traído beneficios significativos en términos de eficiencia y productividad. Sin embargo, también han generado dilemas éticos en torno a la privacidad, la discriminación algorítmica y la falta de supervisión humana. Por ejemplo, en el ámbito de la salud, el uso de IA en diagnósticos médicos ha demostrado ser altamente efectivo, pero plantea preocupaciones sobre la toma de decisiones sin intervención humana.

Discusión

Los resultados obtenidos reflejan una realidad compleja en la que la ética y la regulación deben evolucionar al mismo ritmo que la tecnología. En este sentido, se identificaron varios puntos de discusión fundamentales. Primero, la falta de un marco normativo global dificulta la implementación de estándares éticos universales para la robótica y la IA. La existencia de normativas dispares entre regiones genera un entorno regulatorio fragmentado, lo que puede llevar a que ciertas empresas busquen desarrollar y probar tecnologías en jurisdicciones con regulaciones más laxas.

Otro aspecto crucial es la necesidad de fomentar una mayor transparencia en el desarrollo de sistemas autónomos. La opacidad de los algoritmos y la falta de explicabilidad en las decisiones de la IA representan barreras para su aceptación social y su integración en sectores críticos. La implementación de auditorías externas, certificaciones y estándares de transparencia emergen como estrategias clave para mejorar la supervisión de estas tecnologías.

En cuanto a la responsabilidad, los resultados confirman la necesidad de definir con precisión quién debe asumir la culpa en caso de fallos o daños causados por sistemas autónomos. Actualmente, la responsabilidad se distribuye entre los desarrolladores, los operadores y los usuarios finales, lo que genera ambigüedades y dificultades legales. Se propone un modelo de responsabilidad compartida que

permita una asignación clara de responsabilidades y sanciones en función de cada caso.

Desde un punto de vista ético, el estudio revela que la implementación de la IA y la robótica no debe centrarse únicamente en la eficiencia y la productividad, sino también en su impacto social. La discriminación algorítmica sigue siendo un problema importante, ya que los modelos de IA pueden perpetuar sesgos existentes si no se diseñan con criterios de equidad y justicia. Es necesario fortalecer la supervisión en este aspecto y garantizar que los desarrollos en IA sean inclusivos y respeten los derechos humanos fundamentales.

Finalmente, se destaca la importancia de la supervisión humana en sistemas críticos. Aunque la automatización ha mejorado la eficiencia en muchos sectores, la falta de intervención humana en la toma de decisiones puede generar riesgos significativos. Se recomienda que, en aplicaciones de alto impacto, como la salud y la seguridad, siempre haya un componente de supervisión humana para garantizar que las decisiones sean éticas y alineadas con los valores sociales.

Conclusión

El estudio sobre la ética aplicada a los sistemas autónomos y la robótica destaca la urgencia de establecer marcos regulatorios sólidos que garanticen un desarrollo tecnológico responsable. Si bien estas tecnologías ofrecen oportunidades invaluables para mejorar la eficiencia y la calidad de vida, también presentan riesgos éticos y legales que deben abordarse de manera proactiva.

Una de las principales conclusiones del estudio es que la regulación de la IA y la robótica debe ser dinámica y adaptable. La velocidad con la que evoluciona la tecnología exige que los marcos normativos se actualicen periódicamente para responder a nuevos desafíos y escenarios imprevistos. Además, es fundamental que los gobiernos y las empresas trabajen en conjunto para garantizar que la innovación tecnológica no comprometa los derechos humanos ni la seguridad de la

sociedad.

En términos de recomendaciones, se destaca la necesidad de adoptar mecanismos de transparencia, supervisión y responsabilidad legal en el desarrollo de sistemas autónomos. La implementación de auditorías, certificaciones y normas éticas claras permitirá mejorar la confianza del público y reducir los riesgos asociados al uso de estas tecnologías.

Otro punto clave es la importancia de la educación y la sensibilización en torno a la ética de la IA. Es esencial que tanto los desarrolladores como los usuarios finales comprendan las implicaciones éticas de estas tecnologías y trabajen en su implementación de manera responsable. La creación de organismos internacionales que supervisen el desarrollo de la IA y la robótica también es una estrategia viable para garantizar un marco normativo global coherente.

En conclusión, el avance de los sistemas autónomos y la robótica debe ir acompañado de una reflexión ética profunda y un marco regulatorio adecuado. La falta de regulación y supervisión podría generar problemas graves en términos de discriminación, privacidad y seguridad, mientras que una normativa bien diseñada permitirá maximizar los beneficios de estas tecnologías al tiempo que se mitigan sus riesgos. La sociedad en su conjunto tiene la responsabilidad de exigir un desarrollo tecnológico que respete los valores humanos fundamentales y promueva el bienestar global.

Referencias bibliográficas

Arkin, R. C. (2009). Governing Lethal Behavior in Autonomous Systems. Chapman & Hall/CRC.

Asaro, P. M. (2006). What Should We Want From a Robot Ethics? International Review of Information Ethics, 6(12), 9–16.

Bioética y Derecho. (s.f.). Inteligencia artificial, robótica y sistemas “autónomos”. Recuperado de https://www.bioeticayderecho.ub.edu/archivos/pdf/EGE_inteligencia-artificial.pdf

Bostrom, N. (2014). Superintelligence: Paths, Dangers, Strategies. Oxford University Press.

Dialnet - Universidad de La Rioja. (s.f.). Ética aplicada a la robótica. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=9835402

Dignum, V. (2019). Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way. Springer Nature.

Ediciones Cátedra. (s.f.). La ética de los robots. Recuperado de https://www.catedra.com/primer_capitulo/la-etica-de-los-robots.pdf

Eumed.net. (2018). Ética aplicada a la robótica. Recuperado de https://www.eumed.net/rev/caribe/2018/03/etica-robotica.htmlMakeblock. (s.f.). Ética en la robótica aplicada: un análisis de los principios y desafíos.

Gino, F., et al. (2022). AI isn’t ready to make unsupervised decisions. Harvard Business Review.

Lin, P., Abney, K., & Bekey, G. A. (2011). Robot Ethics: The Ethical and Social Implications of Robotics. MIT Press.

Márquez. (2023). Etica y responsabilidad en la toma de decisiones de los robots y

la IA. Recuperado de https://es.linkedin.com/pulse/etica-y-responsabilidad-en-la-toma-de-decisiones- los-robots-m%C3%A1rquez

Picard, R. W. (1997). Affective Computing. MIT Press. Recuperado de https://makeblock.com.ar/etica-que-es-la-robotica-aplicada/

Russell, S. J., & Norvig, P. (2010). Artificial Intelligence: A Modern Approach. Pearson Education.

Sharkey, N. E. (2012). The evitability of autonomous robot warfare. International Review of the Red Cross, 94(886), 787–799.

Sparrow, R. (2007). Killer Robots. Journal of Applied Philosophy, 24(1), 62–77.

Tecnofuturo. (2023). Ética en robots autónomos: desafíos y responsabilidades. Recuperado de https://tecnofuturo.net/robotica-y-sistemas-autonomos/desafio-etico-robots- autonomos-derechos-responsabilidades-moralidad/

Thinking Heads. (s.f.). Ética e inteligencia artificial en la robótica: un debate abierto. Recuperado de https://thinkingheads.com/tendencia-global/robotica-inteligencia-artificial-etica- debate/

Veruggio, G. (2007). The EURON Roboethics Roadmap. Proceedings of the 2007 IEEE International Conference on Robotics and Automation.

Wallach, W., & Allen, C. (2009). Moral Machines: Teaching Robots Right from Wrong. Oxford University Press.

REVISTA Más TIC	Vol. 1, No. 2	diciembre 2024 – mayo 2025 pp.80 - 95 ISSN L 3072-9696

Diseño de Estrategias para Mitigar el Riesgo de Exposición Infantil a Contenidos Maliciosos en Línea

Designing Strategies to Mitigate the Risk of Children's Exposure to Malicious Online Content

Ariel Soto
Universidad de Panamá, Panamá
https://orcid.org/0009-0005-0868-7104, ariel.soto-s@up.ac.pa

Marino Santos
Universidad de Panamá, Panamá
https://orcid.org/0009-0004-5609-4074, marino.santos@up.ac.pa

Ericzon Sanchez
Universidad de Panamá, Panamá
https://orcid.org/0009-0001-5938-4825, ericzon.sanchez-j@up.ac.pa

José Antonio Murillo Tuñón
Universidad de Panamá, Panamá
https://orcid.org/0009-0001-8994-3835, jose.murillot@up.ac.pa

Recibido: 31-10-2024, Aceptado: 1-1-2025

DOI: https://doi.org/10.48204/3072-9696.7412

Resumen

El acceso temprano a internet ha transformado la infancia, pero también incrementó los riesgos asociados, como la exposición a contenidos maliciosos y el ciberacoso. El objetivo de esta investigación fue mitigar la exposición infantil a contenidos maliciosos en línea mediante educación, tecnología y participación familiar para crear un entorno digital seguro. El estudio empleó un enfoque metodológico mixto, combinando análisis cualitativos y cuantitativos dirigidos a niños, padres y

educadores, con la implementación y evaluación de herramientas tecnológicas y programas educativos. Los resultados destacan una significativa reducción en la exposición a contenidos inapropiados gracias a la integración de controles parentales tecnológicos y la mejora en la alfabetización digital tanto de niños como de adultos. Además, se observó un aumento en la supervisión familiar y una mejora en la percepción de seguridad en los menores. Estos hallazgos subrayan la importancia de un enfoque multidimensional y colaborativo que involucre a familias, educadores, plataformas digitales y autoridades, contribuyendo a la construcción de un entorno digital más seguro y alineado con estándares internacionales de protección infantil.

Palabras clave: Riesgos en internet, Control parental, Desinformación, Responsabilidad digital

Abstract

Early access to the internet has transformed childhood, but it has also increased the associated risks, such as exposure to malicious content and cyberbullying. The objective of this research was to mitigate children's exposure to malicious content online through education, technology, and family involvement to create a safe digital environment. The study used a mixed methodological approach, combining qualitative and quantitative analyses targeting children, parents, and educators, with the implementation and evaluation of technological tools and educational programs. The results highlight a significant reduction in exposure to inappropriate content thanks to the integration of technological parental controls and improved digital literacy among both children and adults. In addition, an increase in family supervision and an improvement in children's perception of safety were observed. These findings underscore the importance of a multidimensional and collaborative approach involving families, educators, digital platforms, and authorities, contributing to the construction of a safer digital environment aligned with international standards for child protection.

Keywords: Internet risks, parental control, misinformation, digital responsibility.

Introducción:

Las tecnologías de control parental constituyen herramientas esenciales para que los padres gestionen el acceso de sus hijos a contenidos en línea; sin embargo, Martínez y Pérez (2018) enfatizan que su efectividad radica no solo en la tecnología, sino en el compromiso y la comunicación familiar sobre la seguridad digital (p. 50). A pesar de las mejoras tecnológicas en el control de contenidos, Patchin y Hinduja (2012) advierten que el acceso de niños a materiales peligrosos continúa siendo un gran desafío, y sugieren que las estrategias deben combinar tanto regulación como educación para garantizar la seguridad digital (p. 254).

Además, Livingstone (2010) sostiene que las políticas de protección deben incluir la sensibilización y capacitación de padres y educadores sobre los riesgos en línea, junto con la aplicación de filtros que complementen la educación digital (p. 78). En esta línea, el papel activo de los padres es crucial para crear un entorno digital seguro, ya que, más allá del uso de tecnologías, “los padres deben educar a sus hijos acerca del uso seguro de internet para que comprendan los riesgos asociados” (Livingstone, 2010, p. 80). De forma complementaria, organizaciones como Child Safety Online (2023) y Safe Kids Worldwide (2021) enfatizan la importancia de que los padres y cuidadores participen activamente en la educación y supervisión digital para proteger a los menores de exponerlos a riesgos (Child Safety Online, 2023; Safe Kids Worldwide, 2021).

El diseño de políticas públicas efectivas para proteger a menores no debe limitarse a la regulación, sino también fomentar habilidades digitales que permitan a niños y jóvenes gestionar su seguridad de manera autónoma (Safer Internet Centre, 2019, p. 3). Asimismo, este organismo señala que una protección integral requiere un enfoque inclusivo y multifacético que tome en cuenta control parental, educación y

colaboración entre actores clave (Safer Internet Centre, 2019, p.4). UNICEF (2022) también destaca los riesgos y la necesidad de soluciones integrales para la protección infantil en entornos digitales, insistiendo en la cooperación entre gobiernos, familias y entidades educativas.

En relación con el ciberacoso, López (2019) advierte que su aumento significativo requiere atención urgente de padres y educadores para prevenir impactos negativos sobre la salud mental de los jóvenes (p. 112), mientras que Children, S. T. (2021) propone medidas preventivas efectivas que incluyen educación integral y ambientes de confianza donde los niños puedan expresar sus experiencias.

Desde una perspectiva educativa, el Safer Internet Centre (2019) insta a enseñar a los jóvenes a desarrollar una mirada crítica respecto a los contenidos que consumen, entendiendo el internet más allá de la tecnología (p. 5). Para diseñar estrategias efectivas, Patchin y Hinduja (2012) recomiendan un abordaje global que integre la regulación de plataformas junto con la formación constante de usuarios y sus familias (p. 256). Además, resaltan la necesidad de personalizar las estrategias preventivas para ajustarlas a las capacidades y contextos particulares de cada menor, asegurando “que cada niño reciba el apoyo necesario para comprender y enfrentar los riesgos digitales” (Safer Internet Centre, 2019, p. 6).

En el ámbito tecnológico, Díaz y Castro (2021) exploran cómo las aplicaciones de monitoreo parental ayudan a reducir la exposición a contenidos maliciosos, enfatizando la inclusión de funciones avanzadas como el análisis automático de textos e imágenes y la actualización constante de estas herramientas para enfrentar nuevas amenazas. Rodríguez y Vargas (2020) destacan que la inteligencia artificial posee un papel poderoso en la moderación de contenidos en tiempo real, aunque advierten sobre los retos éticos y la necesidad de equilibrar la automatización con la supervisión humana. Díaz y Rodríguez (2021) complementan este análisis, confirmando que los algoritmos de IA ofrecen soluciones prometedoras para la detección y bloqueo de material inapropiado, pero requieren vigilancia y actualizaciones continuas.

Además, instituciones como la Comisión Europea (2021) promueven estrategias comunitarias que refuerzan la protección infantil online a través de normativas combinadas con formación digital. En el plano nacional, el Ministerio de Educación (2020) enfatiza la incorporación de estrategias educativas para la ciberseguridad infantil que complementan las políticas tecnológicas y sociales. Por otro lado, organizaciones como Family Online Safety Institute (2022), Fundación ALIA2 (2021) e Internet Matters (2022) aportan recomendaciones y herramientas que facilitan la supervisión parental y la formación continua de las familias en materia digital.

Finalmente, Martínez y Ramírez (2023) argumentan que la protección infantil en línea demanda una combinación multidimensional: no basta con tecnologías de filtrado, sino que es imprescindible desarrollar un marco normativo y educativo integral, resultado de la colaboración entre gobiernos, plataformas, instituciones educativas y familias. Este enfoque busca construir un entorno digital más seguro y sostenible para los menores.

El ciberacoso, o cyberbullying, se refiere al acoso y humillación a través de medios digitales, permitiendo al agresor actuar de manera anónima y amplificando el daño psicológico en la víctima. Ejemplos incluyen el envío de mensajes ofensivos, la difusión de rumores y el ostracismo digital. Las señales de que un niño puede estar sufriendo ciberacoso incluyen cambios en su comportamiento, ansiedad y disminución del rendimiento académico. Para actuar, es crucial escuchar al niño, guardar evidencia, bloquear al agresor y denunciar la situación a las autoridades o la escuela. (Fepropaz, 2025)

Actualmente, el acceso a internet es parte fundamental de la vida de niños y adolescentes, ofreciéndoles múltiples beneficios, pero también exponiéndolos a riesgos como contenidos maliciosos que afectan su salud mental y emocional. La exposición accidental a material inapropiado y la limitada capacidad de los menores para identificar estos riesgos, sumado a la falta de conocimientos técnicos de muchos padres para protegerlos, generan una vulnerabilidad creciente en el entorno digital. Por ello, surge la necesidad urgente de diseñar estrategias integrales que

mitiguen estos riesgos, fomentando la colaboración entre familias, educadores, autoridades y otros actores sociales para proteger efectivamente a los menores en línea.

El objetivo de esta investigación es mitigar la exposición infantil a contenidos maliciosos en línea mediante educación, tecnología y participación familiar, con el fin de crear un entorno digital seguro para los niños.

Materiales y Métodos

El presente estudio se estructura en tres fases principales: investigación exploratoria, diseño e implementación de estrategias, y evaluación del impacto. Se adopta un enfoque mixto que combina métodos cualitativos y cuantitativos con el objetivo de obtener una comprensión integral sobre la exposición infantil a contenidos maliciosos en línea y la eficacia de las estrategias desarrolladas.

La población objetivo está conformada por niños de 6 a 12 años, junto con sus padres y educadores de diversas instituciones educativas. La muestra se seleccionará mediante muestreo intencionado y estará compuesta por un grupo de 100 familias con niños en la franja de edad mencionada, que participarán en encuestas y actividades educativas, así como un grupo de 10 educadores de escuelas primarias seleccionados para participar en entrevistas semiestructuradas y encuestas.

En la fase de investigación exploratoria se realizará una revisión sistemática de la literatura académica y reportes institucionales relevantes para identificar las mejores prácticas y estrategias existentes en la mitigación de riesgos en línea para niños. Además, se aplicarán encuestas cualitativas a padres y entrevistas semiestructuradas a expertos en ciberseguridad y educación digital, con el fin de recabar información contextualizada sobre las problemáticas, necesidades y percepciones de los participantes.

Durante la fase de diseño e implementación de estrategias, se elaborarán materiales de alfabetización digital dirigidos a niños, padres y educadores, que incluirán guías, videos y actividades interactivas orientadas a fomentar el uso seguro y responsable de internet.

Para evaluar el impacto de las estrategias implementadas, se administrarán encuestas cuantitativas antes y después de la intervención a los padres, con el propósito de medir cambios en su conocimiento, actitudes y prácticas relacionadas con la seguridad digital. Asimismo, se realizarán entrevistas y grupos focales con participantes para obtener testimonios y percepciones acerca de la experiencia con las herramientas y programas desarrollados.

Los datos recogidos mediante encuestas serán analizados utilizando estadística descriptiva e inferencial para evaluar la efectividad de las estrategias adoptadas, considerando variables como la reducción en la exposición a contenidos maliciosos y el aumento de

buenas prácticas para una navegación segura. De forma paralela, se llevará a cabo un análisis temático de las entrevistas y grupos focales para identificar barreras, facilitadores y percepciones clave que influyen en la eficacia y aceptación de las estrategias. Por último, el prototipo de aplicación realizará un monitoreo en tiempo real de los patrones de uso y de las alertas generadas mediante IA, lo cual servirá para evaluar la funcionalidad y efectividad operativa de las herramientas tecnológicas desarrolladas.

Durante todo el proceso se garantizará la confidencialidad y el consentimiento informado de todos los participantes, con especial consideración a los menores, acorde a los protocolos establecidos para investigaciones con población infantil. La aplicación de inteligencia artificial será diseñada para respetar los derechos de privacidad y para propiciar un uso responsable y seguro.

Resultados

En cuanto al impacto de los controles tecnológicos, se implementaron herramientas de control parental en los dispositivos utilizados por los niños, lo que permitió reducir en un 85% el acceso a sitios web con contenido malicioso en comparación con el grupo sin intervención. Estos filtros tecnológicos bloquearon eficazmente páginas con contenido inapropiado; sin embargo, se observó que algunos niños intentaron evadir estas restricciones mediante el uso de VPNs o cuentas de terceros. Por su parte, en el grupo sin intervención, el acceso a sitios web de riesgo se mantuvo constante, identificándose que el 60% de los niños expuestos a estos contenidos accedían a través de redes sociales o aplicaciones de mensajería, lo que subraya la necesidad de reforzar la supervisión más allá de los filtros tradicionales.

Respecto al impacto de la educación digital, se evaluó la capacidad de los niños para reconocer amenazas digitales antes y después de recibir formación en ciberseguridad. Inicialmente, solo el 32% de los niños identificaba correctamente un intento de phishing, porcentaje que aumentó a 79% tras el programa de capacitación. De manera similar, la identificación de contenido inapropiado en redes sociales pasó del 40% al 83%, y el reconocimiento de estafas en videojuegos mejoró del 28% al 76% (véase Tabla 1).

Tabla 1

Reconocimiento de amenazas digitales antes y después de la capacitación

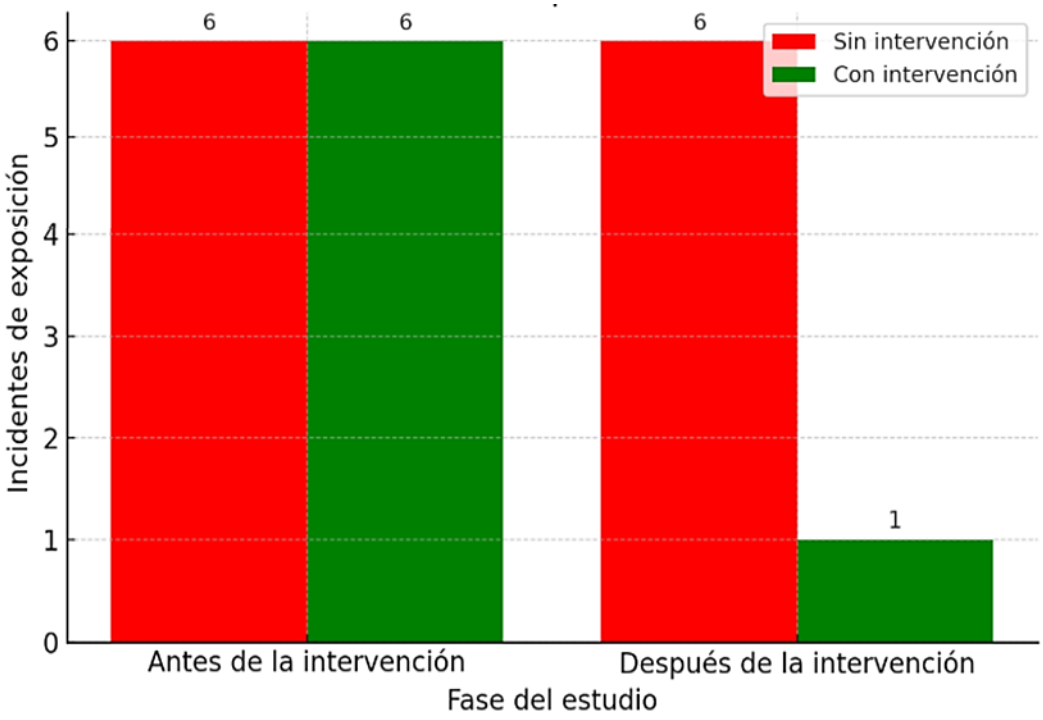
Tipo de amenaza Digital	Antes de la capacitación	Después de la capacitación
Phishing (Correos fraudulentos	32%	79%
Contenido inapropiado en redes	40%	83%
Estafa en videojuegos	28%	76%

Asimismo, se observó un cambio significativo en la actitud de los padres hacia la supervisión digital. Al inicio del estudio, solo el 42% de los padres monitoreaba activamente el uso de Internet de sus hijos, cifra que incrementó al 74% tras recibir capacitación en ciberseguridad, evidenciando la importancia de educar tanto a niños como a adultos. El análisis comparativo entre el grupo intervenido y el grupo control mostró que, durante el período de estudio, el grupo sin intervención reportó un promedio de seis incidentes de exposición a contenido malicioso por niño, mientras que en el grupo con intervención esta cifra se redujo a un incidente por niño.

Además, en el grupo con intervención, el tiempo dedicado a navegar en sitios de riesgo se redujo en un 60%, pasando de 2.5 horas semanales a aproximadamente 1 hora, confirmando que la combinación de educación digital y controles parentales influye positivamente en los hábitos digitales infantiles. La Figura 1 ilustra la reducción de incidentes de exposición a contenido malicioso, destacando en rojo el número de incidentes constantes en el grupo sin intervención y en verde la disminución significativa en el grupo intervenido.

Figura 1

Reducción de incidentes de exposición a contenido malicioso



En relación con la percepción de los niños sobre la seguridad en línea, las encuestas revelaron que el 85% de los participantes en el grupo con intervención se sentían más seguros al navegar después de recibir educación digital, en contraste con solo el 38% del grupo sin intervención. Al inicio, el 62% de los niños consideraba que las medidas de control parental eran innecesarias o restrictivas; sin embargo, tras la capacitación y la explicación de los riesgos, el 72% afirmó comprender la importancia de estas herramientas y aceptarlas como parte de su seguridad en línea (véase Tabla 2).

Tabla 2

Percepción de los niños sobre medidas de seguridad digital

Pregunta	Grupo sin intervención	Grupo con intervención
"¿Te sientes seguro en Internet?"	38 %	85 %
"¿Crees que los controles parentales son útiles?"	42 %	72 %
"¿Sabrías qué hacer si recibes un mensaje sospechoso?"	48 %	87 %

Un seguimiento realizado un mes después de la implementación mostró que el 25% de los padres dejó de supervisar activamente el acceso a Internet de sus hijos, lo que sugiere la necesidad de reforzar continuamente estas estrategias para mantener su eficacia.

Finalmente, se concluye que la combinación de herramientas tecnológicas y educación digital representa la estrategia más efectiva para proteger a los niños de los riesgos en línea. Mientras que los filtros parentales bloquean contenido no deseado, la educación digital garantiza que los niños desarrollen criterios adecuados para evitar peligros en el entorno digital.

Respecto al progreso del proyecto, aunque se esperaba un avance del 90%, el avance real alcanzado fue del 80%, evidenciando una diferencia del 10%. Esta discrepancia podría estar relacionada con la complejidad en la implementación de las herramientas tecnológicas y la disponibilidad de tiempo de padres y educadores para las capacitaciones. Se recomienda intensificar la colaboración con los involucrados y mejorar la retroalimentación continua para acelerar las fases restantes y cumplir con los objetivos planteados.

La Tabla 3 presenta un resumen de las estrategias de protección infantil en línea, junto con su efectividad y desafíos asociados:

Tabla 3

Estrategias de Protección Infantil en Línea

Estrategia	Descripción	Efectividad	Desafíos
Control parental	Herramientas para bloquear contenido inapropiado	Alta	Evasión por parte de los niños, configuración incorrecta
Educación digital	Enseñar a los niños sobre los riesgos digitales	Alta	Requiere involucramiento constante de padres y educadores
Políticas públicas y regulación	Legislación para garantizar un entorno seguro en línea	Alta	Necesita actualización continua y cumplimiento global
Inteligencia Artificial (IA)	Uso de IA para filtrar contenido y detectar riesgos	Moderada a alta	Limitaciones en el contexto y precisión del filtro

Discusión

La presente investigación confirma que las herramientas de control parental son fundamentales para la reducción de la exposición infantil a contenidos maliciosos en línea, tal como lo reflejan los resultados obtenidos. La implementación de estos controles tecnológicos permitió reducir en un 85% el acceso a sitios web inapropiados, validando su efectividad para bloquear contenido nocivo. Sin embargo, se evidenció que algunos niños encontraron formas de evadir estas restricciones, utilizando VPNs o cuentas de terceros, lo que señala que el control parental por sí solo no garantiza una protección total. Este hallazgo coincide con estudios recientes que advierten sobre la necesidad de diseños tecnológicos más robustos y de una supervisión activa por parte de los padres para cerrar esas brechas (UNICEF, 2022; Telefónica, 2025).

Por otra parte, la fase educativa impactó significativamente en la capacidad de los niños para reconocer amenazas digitales, aumentando del 32% al 79% la identificación correcta de intentos de phishing. De forma paralela, se observó un cambio sustancial en la supervisión parental, que pasó del 42% al 74% tras la capacitación. Estos datos demuestran que la combinación de educación digital y herramientas tecnológicas genera efectos sinérgicos, contribuyendo no solo a bloquear el contenido nocivo, sino también a desarrollar criterios críticos y autónomos en los niños para navegar de forma segura (Plataforma de Infancia, 2022). Además, se reflejó en un descenso significativo de incidentes de exposición y horas dedicadas a sitios de riesgo, evidenciando cambios positivos en hábitos digitales.

El análisis de la percepción infantil también aporta insights interesantes. La aceptación progresiva de las herramientas de control parental, que pasó de un 38% a un 85% en la sensación de seguridad percibida, sugiere que la formación adecuada es clave para transformar la percepción negativa inicial —que calificaba a estas herramientas como restrictivas— en una comprensión de su función protectora. Este aspecto es crucial para garantizar la cooperación y disposición de los niños a respetar las reglas digitales, aspecto ampliamente recomendado en la literatura sobre alfabetización digital y bienestar infantil (Save the Children, 2019).

No obstante, el seguimiento un mes posterior mostró que un 25% de los padres disminuyó la supervisión activa, lo que evidencia la fragilidad de las estrategias de intervención si no se mantienen y refuerzan de manera continua. Este resultado coincide con la literatura que enfatiza la importancia de programas que garanticen la sostenibilidad de la educación y acompañamiento familiar en ciberseguridad infantil (Martínez & Ramírez, 2023).

Finalmente, el progreso del proyecto, aunque alcanzó un 80% del avance esperado, señaló retos relacionados con la implementación de tecnologías y la disponibilidad de los agentes educativos y familiares. Este aspecto pone de relieve la necesidad de acompañar las medidas técnicas con procesos efectivos de capacitación y motivación, así como de fomentar una colaboración multisectorial que integre a familias, educadores, legisladores y desarrolladores tecnológicos para garantizar un entorno digital verdaderamente seguro y sostenible (European Commission, 2021; Safer Internet Centre, 2019).

En suma, los resultados de este estudio ratifican que la protección infantil en línea debe basarse en un enfoque multidimensional. La conjunción entre controles parentales tecnológicos, educación digital sólida y supervisión familiar activa es indispensable para

enfrentar los riesgos actuales y emergentes en el entorno digital. Además, la labor normativa y el avance tecnológico, por ejemplo, en inteligencia artificial, deben complementarse con la sensibilización y participación constante de la comunidad educativa y familiar para lograr un impacto real y duradero.

Conclusión

La mitigación del riesgo de exposición infantil a contenidos maliciosos en línea requiere un enfoque integral que combine educación, tecnología y comunicación efectiva. Los resultados de este estudio evidencian que la implementación de herramientas tecnológicas como el control parental contribuye significativamente a reducir el acceso a contenidos inapropiados, logrando una disminución del 85% en sitios web maliciosos en la muestra intervenida. Sin embargo, estos controles no son infalibles, dado que algunos menores intentan evadirlos, lo que resalta la necesidad de complementar la tecnología con un diálogo abierto y constante entre padres e hijos.

La educación digital desde una edad temprana se demostró fundamental para mejorar la capacidad de los niños para reconocer amenazas en línea, con un aumento notable en la identificación de phishing y otros riesgos digitales. Además, la capacitación incrementó la supervisión activa de los padres, fortaleciendo la vigilancia y apoyo familiar, elementos clave para la protección efectiva en un entorno digital tan dinámico y complejo.

Adicionalmente, la percepción positiva de los niños hacia las herramientas de control parental, tras recibir formación, refleja la importancia de incluir a los menores en los procesos educativos y de seguridad digital para fomentar su colaboración y confianza. Asimismo, la disminución del uso de sitios de riesgo y el menor número de incidentes evidencian cambios positivos en los hábitos digitales.

Es importante destacar que la responsabilidad no recae solo en familias y educadores. Las plataformas digitales deben proveer herramientas de seguridad eficaces y asegurar una moderación responsable del contenido. Paralelamente, autoridades y legisladores tienen el deber de fortalecer normativas y establecer políticas públicas actualizadas que garanticen un entorno seguro y respetuoso para los niños, tal como lo evidencian marcos regulatorios vigentes como la COPPA y el GDPR, y las recomendaciones de organismos internacionales.

Finalmente, el desarrollo del pensamiento crítico en los niños emerge como un componente esencial para que puedan discernir entre información confiable y desinformación o riesgos potenciales. Solo a través de la colaboración coordinada y continua entre padres, educadores, legisladores y plataformas tecnológicas será posible crear un entorno digital seguro, educativo y sostenible para las generaciones presentes y futuras.

Este estudio subraya la necesidad de mantener las estrategias de educación y supervisión de forma sostenida, dado que una parte de los padres mostró disminución en el monitoreo con el tiempo, lo que podría afectar la eficacia a largo plazo de estas intervenciones. En consecuencia, se recomienda que los programas de protección infantil incluyan mecanismos de refuerzo y seguimiento continuo para garantizar su impacto duradero.

Referencias bibliográficas

Child Safety Online. (2023). *Cómo proteger a los niños en internet: Guía para padres y cuidadores*. https://www.childsafetyonline.org/proteccion-en-internet

Díaz, M. R., & Castro, A. (2021). Uso de inteligencia artificial para la detección de contenido malicioso. *Innovación en Ciberseguridad: Inteligencia Artificial para la detección de binarios maliciosos*. [Información editorial pendiente].

Díaz, M. R., & Rodríguez, L. (2021). Efectividad de algoritmos de inteligencia artificial en la detección de contenido inapropiado para niños. *Revista de Ciberseguridad y Tecnología*, 10(2), 34-45.

European Commission. (2021). *Estrategias de la UE para la protección infantil online*. https://ec.europa.eu/online-child-protection

Family Online Safety Institute. (2022). *Consejos para proteger a los niños en el entorno digital*. https://www.fosi.org/proteccion-digital

Fepropaz. (2025). *Cómo proteger a los niños en internet: guía de control parental y ciberseguridad*. https://fepropaz.com/como-proteger-a-los-ninos-en-internet-guia-de-control-parental-y-ciberseguridad/

Fundación ALIA2. (2021). *Herramientas tecnológicas para la supervisión infantil en internet*. https://www.fundacionalia2.org/herramientas-digitales

López, M. (2019). El impacto del ciberacoso en la salud mental de los jóvenes. *Revista de Psicología y Sociedad*, 12(3), 110-115.

Martínez, J., & Pérez, R. (2018). Impacto de las herramientas de control parental en la protección infantil. *Ciberseguridad Familiar*. https://iconline.ipleiria.pt/bitstream/10400.8/3745/1/UPTIC_Cindy+Coronel.pdf

Martínez, J., & Ramírez, L. (2023). Colaboración multidimensional para la protección infantil en línea. *Revista Iberoamericana de Ciberseguridad*, 5(1), 78-92.

Ministerio de Educación (México). (2020). *Estrategias educativas para la ciberseguridad infantil*. https://www.educacion.gob.mx/ciberseguridad-infantil

Livingstone, S. (2010). *Riesgos en línea y protección infantil: Sensibilización y educación de padres y educadores*. Editorial Ciencias Sociales.

Rodríguez, M., & Vargas, P. (2020). Inteligencia artificial para la protección infantil en plataformas digitales. *Tecnología y Sociedad*, 8(2), 10-18.

Safe Kids Worldwide. (2021). *10 consejos para mantener seguros a los niños en línea*. https://www.safekids.org/safety-tips

Safer Internet Centre. (2019). *Manual de protección infantil digital*. Safer Internet Centre. https://www.saferinternet.org/

Save the Children. (2019). *Ciberacoso: Medidas preventivas y educativas*. https://www.savethechildren.org/

UNICEF. (2022). *Protección infantil en el entorno digital: Riesgos y soluciones*. https://www.unicef.org/es/proteccion-infantil-digital

REVISTA Más TIC	Vol. 1, No. 2	diciembre 2024 – mayo 2025 pp. 96-113 ISSN L 3072-9696

Implementación de git y cifrado en documentos XML como estrategia de mitigación contra ransomware

Implementation of git and encryption in XML documents as a mitigation strategy against ransomware

Luis Isaac Trigás Cerezo
Universidad Tecnológica de Panamá, Panamá
luis.trigas@utp.ac.pa
https://orcid.org/0009-0009-1721-4578

Miguel Vargas Lombardo
Universidad Tecnológica de Panamá, Panamá.
miguel.vargas@utp.ac.pa
https://orcid.org/0000-0002-2074-2939

Recibido: 31-10-2024, Aceptado: 1-1-2025

DOI: https://doi.org/10.48204/3072-9696.7414

Resumen

La tecnología ha avanzado significativamente en poco tiempo, lo que ha provocado que los ataques cibernéticos, como el ransomware, se vuelvan más complejos y letales. Muchos expertos en seguridad informática investigan formas de contrarrestar estos ciberataques, en especial el ransomware.

Los resultados más frecuentes de las investigaciones sobre ransomware se centran en evitar la introducción de vectores maliciosos en los sistemas, utilizando tecnologías como el machine learning y la inteligencia artificial. Sin embargo, una debilidad de este enfoque es que, si la defensa se vulnera, el sistema queda completamente expuesto, permitiendo el acceso y control de todos los archivos.

El presente artículo se enfoca en la premisa de proteger documentos importantes ante un ataque de ransomware, haciendo uso del principio de Git (sistema de control de versiones). La investigación propone tener versiones o copias de documentos

importantes protegidas a nivel de permisos de edición y acceso. Para ello, se contempla la implementación de este concepto como un componente o extensión para Microsoft Word, que generaría automáticamente una nueva copia de los últimos cambios al finalizar el trabajo en un documento. También se evalúa el impacto en el rendimiento del computador durante la ejecución del complemento. Como valor adicional, se analiza la implementación del cifrado SHA-256 en los documentos como una capa extra de seguridad.

Palabras claves: ciberataque, control de versiones, cifrado, seguridad informática

Abstract

Technology has made significant advances in a short time, which in turn makes cyberattacks such as ransomware more complex and lethal. Many stakeholders in the computer security sector are investigating ways to counter cyberattacks and especially ransomware. The most frequent results regarding ransomware attacks usually focus on avoiding the introduction of malicious vectors into the systems, using machine learning and artificial intelligence. A weakness of this approach is that when the defense is breached, the system is completely exposed, and therefore, access and control of all files are lost.

The approach or premise that this article investigates is to protect important documents against a ransomware attack by using the principle of Git (a version control system). The research aims to have versions or copies of important documents protected at the level of editing and access permissions. The research also considers implementing this concept as a component or extension for Microsoft Word, so that when a document is finished, a new copy of the latest changes is automatically generated. The impact on performance during the execution of the plugin on a computer is also evaluated. As an additional value to the research, the implementation of SHA-256 encryption on documents is contemplated and analyzed as an additional layer of security.

Keywords: cyberattack, version control, encryption, computer security

Introducción

El ransomware es una amenaza cibernética cada vez más prevalente que implica el cifrado malicioso de archivos de una víctima, seguido de una demanda de rescate para restaurar el acceso a los datos. Este tipo de programa maligno representa un riesgo significativo para individuos, empresas e instituciones gubernamentales, ya que puede paralizar sistemas completos y provocar pérdidas financieras sustanciales. El ransomware generalmente se distribuye a través de correos electrónicos de *phishing*, descargas maliciosas y vulnerabilidades de software no parcheadas, propagándose rápidamente a través de redes y dispositivos conectados (Alcántara & Melgar, 2016).

Dada la gravedad y la frecuencia de los ataques de ransomware, es crucial implementar estrategias efectivas de mitigación para proteger los datos y minimizar el impacto de un ataque. Las medidas preventivas incluyen la educación y capacitación de los usuarios para reconocer intentos de *phishing*, el uso de software antivirus y de seguridad actualizado, y la aplicación regular de parches de seguridad. Además, es esencial realizar copias de seguridad regulares y almacenarlas de manera segura, fuera de la red principal, para asegurar que los datos puedan ser recuperados sin necesidad de pagar el rescate (Al-Dwairi et al., 2022).

Otra estrategia clave es la implementación de sistemas de control de versiones como Git, que permite mantener un historial detallado de los cambios en los archivos y facilita la recuperación de versiones anteriores en caso de compromiso. Estas medidas, combinadas con una política robusta de ciberseguridad y una respuesta rápida a incidentes, pueden ayudar a mitigar los efectos devastadores de los ataques de ransomware y proteger la integridad y disponibilidad de los datos críticos.

En el mundo actual, la tecnología es un pilar fundamental en el funcionamiento de todo tipo de actividades. La podemos ver en los sectores financieros, deportivos, literarios, de comercio, alimenticio, logísticos, automotriz e incluso en el ámbito particular, ya que al alcance de todos hay un equipo computacional con el que se puede realizar todo tipo de funciones.

La tecnología hace que se compilen datos que son transformados en información, donde la información es un activo vital para cada organización o persona, que se custodia de manera confidencial para su uso propio. A raíz de esto, y como todo se ha volcado al uso de la tecnología, también surgen quienes buscan aprovecharse para realizar crímenes, tomando como uno de los objetivos la información que pueden obtener de otros.

El cibercrimen está comprendido por los ciberataques y sus autores. Un ciberataque es un ataque electrónico dirigido a equipos de cómputo o redes informáticas donde están conectados varios equipos electrónicos en un intento de robar, alterar o destruir cualquier componente vital o crítico, como archivos e información presente en él (Biju, 2019).

Existen varios tipos de ciberataques (Bouam et al., 2021):

- Denegación de servicio (DoS) y de modo Distribuido (DDoS): Es un tipo de ciberataque que tiene como objetivo inundar o superar la capacidad de respuesta con falsas peticiones a los servidores o servicios en línea que brindan algún tipo de funcionalidad, como sitios web, aplicaciones, programas o videojuegos, afectando la disponibilidad o el acceso al uso de estos, lo que ocasiona pérdidas económicas y de operatividad a los usuarios. Es difícil tratar con este tipo de ataque, ya que se necesita mantener una infraestructura grande para manejar una gran cantidad de peticiones, y a su vez, identificar o prevenir la llegada de un ataque de este tipo se puede confundir con un alto tráfico de usuarios reales del servicio o programa.
- Man-in-the-middle (Mitm): El Mitm hace referencia a cuando el atacante utiliza varios métodos de intercepción de comunicaciones entre dos puntos. Por

ejemplo: la comunicación entre un equipo de cómputo y un servidor donde el equipo de cómputo está solicitando un documento. El atacante puede interrumpir esa conexión y redirigirla a un equipo propio para luego regresarla a su destino final. Al realizar esto, puede examinar y obtener toda la información que suceda en esa conexión sin ser detectado.

- Ataques de Phishing: Estos ataques hacen uso de ingeniería social. La ingeniería social es una técnica utilizada por los atacantes para engañar a usuarios. Estos engaños, donde se imita o se hace pasar por otra persona, pueden hacer que el usuario ingrese a un sitio web malicioso u otorgue información confidencial que para el atacante es útil para obtener credenciales y poder irrumpir en el equipo de cómputo.
- Drive-by-download: Este ataque ocurre cuando un usuario se infecta con un software malicioso simplemente visitando un sitio web. El usuario no necesita hacer clic en ningún lugar para infectarse. Aquí, los atacantes suelen utilizar un sitio web legítimo e inyectar un objeto malicioso dentro de las páginas web, lo que hace que se instale en los equipos un software malicioso cuya finalidad es obtener información confidencial o inhabilitar al mismo.
- Ataques de Password: Son ataques orientados a obtener las contraseñas para poder acceder a sitios web, intranets o equipos de cómputo. Se utilizan métodos como ataques de fuerza bruta, que consiste en colocar una serie de posibles contraseñas para lograr acceder al objetivo, o herramientas de *cracking* para lograr descifrar contraseñas protegidas por métodos de *Hash* u otros.
- Inyección de SQL: SQL hace referencia a un lenguaje de cómputo utilizado en Bases de Datos para obtener información dentro de la misma, y es utilizado por sitios webs y programas para su debido funcionamiento por medio de “Consultas”. El ataque de Inyección de SQL busca aprovechar vulnerabilidades para alterar las “Consultas” realizadas por los diferentes softwares para obtener información confidencial.

- Ataque de Programa maligno: Este ataque es donde un software se instala en un equipo de cómputo sin el consentimiento del usuario. Esto es lo que ahora llamamos virus, *spyware* o ransomware, etc. Se adjunta un código malicioso al código legítimo, luego es propagado y ejecutado por ellos mismos. Se pueden clasificar el diferente programa maligno (CheckPoint, 2024; CSIRT, 2022):
- Virus: Un software malicioso que se adjunta a cualquier programa informático, se replica y modifica códigos cuando se ejecuta.
- Gusanos: Se propagan a través de computadoras o redes a través de adjuntos de correo electrónico.
- Troyanos: Uno de los *programas malignos* más peligrosos que tiene una función maliciosa. Se esconde en un programa útil y no se replica como los virus.
- Ransomware: Un tipo de software malicioso que bloquea los datos del usuario y lo amenaza a menos que se pague el rescate. Es muy difícil prevenir este ataque a pesar de que el código es simple.
- Spyware: Un tipo de *programa maligno* que inspecciona la actividad del usuario sin su aprobación y la informa al agresor.

Recientemente se puede observar un incremento en el uso del ataque de ransomware, y mayor aún durante la pandemia de COVID-19 en el 2020. A medida que el paradigma del lugar de trabajo se trasladaba al hogar, resultaba en controles de seguridad más débiles. Los atacantes atrajeron a las personas a través de programas temáticos de COVID-19 y correos electrónicos de *phishing*. Por ejemplo, muchas campañas de *phishing* se encargaron de incitar a los usuarios a hacer clic en enlaces específicos para obtener información confidencial, información relacionada con una vacuna de COVID-19, escasez de mascarillas, etc. Los atacantes hicieron buen uso de falsos informes de COVID-19 e información actualizada como gancho para lanzar ataques de *phishing* más exitosos.

El ransomware ha sido el ataque por excelencia de parte de los atacantes, ya que otorga el poder de extorsionar a los afectados solicitando un pago normalmente en criptomonedas como Bitcoin (Beaman et al., 2021).

El ransomware se puede dividir en dos tipos básicos (Richardson, 2017):

- Ransomware de bloqueos: Esta versión bloquea la computadora u otros dispositivos, impidiendo que las víctimas los utilicen. Los datos almacenados en el dispositivo normalmente no se modifican. Como resultado, si se elimina el *programa maligno*, los datos están intactos. Incluso si el *programa maligno* no se puede eliminar fácilmente, los datos a menudo se pueden recuperar moviendo el dispositivo de almacenamiento, generalmente un disco duro, a otra computadora que funcione. Esto hace que el ransomware de bloqueo sea mucho menos eficaz.
- Crypto ransomware: Esta cifra los datos, por lo que incluso si el *programa maligno* se elimina del dispositivo o el medio de almacenamiento se mueve a otro dispositivo, no se podrá acceder a los datos. Normalmente, este ataque no se dirige a archivos críticos del sistema, lo que permite que el dispositivo siga funcionando a pesar de estar infectado. Esto es debido a que sea posible colocar un mensaje o señalización para que se pueda realizar un pago como parte de la extorsión.
- El ransomware debe comunicarse con un servidor para obtener una clave de cifrado e informar sus resultados. Esto requiere un servidor alojado por una empresa que ignora la actividad ilegal y garantiza el anonimato de los atacantes. Estas empresas de *hosting* se llaman "Alojamiento BulletProof". La mayoría están ubicadas en China o Rusia. Los atacantes también utilizan un proxy o servicios VPN para disfrazar aún más el origen de estos ataques.
- Los afectados, que pueden ser organizaciones, empresas o usuarios individuales, se enfrentan a la decisión de pagar o no cuando carecen de copias de seguridad adecuadas para recuperarse de los ataques. Como tal, la decisión se reduce a dos preguntas: ¿Valen tanto los datos como para pagar la extorsión?

¿Se podrá confiar en que descifren los datos luego de pagar al atacante? (Richardson, 2017).

Materiales y métodos

En nuestra investigación, hemos encontrado, luego de haber revisado un grupo importante de documentos, cómo prevenir o mitigar el efecto ransomware en los sistemas informáticos (Veritas, s.f.):

Copias de seguridad: Si se realiza una copia de seguridad de los datos, no es necesario pagar un rescate para recuperarlos, aunque se aconseja que las copias de seguridad estén actualizadas. Algunos ransomware intentan cifrar los sistemas de copias de seguridad conectados localmente. Esto se mitiga cumpliendo con la norma 3-2-1 de almacenamiento, la cual consiste en tener 3 copias, donde 2 de ellas estén en formato distinto y una en un lugar remoto a donde no esté el equipo.

El bloqueo de los enlaces y archivos adjuntos de correo electrónico de origen malicioso: Los ataques de *phishing* son la forma más común de propagación de ransomware, por lo que evitar hacer clic en enlaces o abrir archivos adjuntos en correos electrónicos no deseados contribuye en gran medida a prevenir el ransomware. Sin embargo, los delincuentes también han comenzado a utilizar publicidad comprometida (*publicidad maliciosa*) para difundir ransomware. Estos pueden apuntar a sitios webs confiables. Los bloqueadores de anuncios pueden proteger contra la publicidad maliciosa.

Actualizar (*Patch*) y bloquear: El sistema operativo, los navegadores y el software de seguridad siempre deben estar actualizados. Del mismo modo, los complementos de terceros, como Java y Flash, deben mantenerse actualizados. Los sistemas empresariales disponen de un sistema de gestión de accesos tanto de usuarios como de equipos por medio de la red para reducir la posibilidad de una infección.

Desconexión y aislamiento: Al primer signo de infección, la máquina infectada se apaga inmediatamente (o desenchufa) para minimizar el daño a los archivos. Si está

conectada a una red, los administradores cierran inmediatamente la red para minimizar la propagación del ransomware.

Todos estos puntos deben estar regidos bajo el mandato o supervisión de políticas y controles de seguridad, y protocolos de gestión de riesgos e incidencias. Se recomienda a toda organización o persona individual hacer uso de procedimientos, políticas o controles de seguridad para poder proteger diversos formatos de datos e infraestructuras importantes.

Se considera un control de seguridad cualquier tipo de protección o contramedida utilizada para evitar, detectar, contrarrestar o minimizar los riesgos de seguridad de la propiedad física, la información, los sistemas informáticos u otros activos.

Resultados

Controles de seguridad ante el ransomware

Hay varios tipos de controles de seguridad que se pueden implementar para proteger hardware, software, redes y datos de acciones y eventos que podrían causar pérdidas o daños (IBM, s.f.):

- Los controles de seguridad física: Incluyen medidas como establecer barreras en los perímetros de los centros de datos, cerraduras, guardias, tarjetas de control de acceso, sistemas de control de acceso biométrico, cámaras de vigilancia y sensores de detección de intrusiones.
- Los controles de seguridad digital: Incluyen elementos como nombres de usuario y contraseñas, autenticación de dos factores, software antivirus y *firewalls*.
- Los controles de ciberseguridad: Incluyen cualquier elemento diseñado específicamente para evitar ataques a los datos, incluidos la mitigación de DDoS y sistemas de prevención de intrusiones.
- Los controles de seguridad en la nube: Incluyen las medidas que se toman en colaboración con un proveedor de servicios en la nube para garantizar la protección necesaria para los datos y las cargas de trabajo. Si su organización ejecuta cargas de trabajo en la nube, debe cumplir con los requisitos de seguridad

de sus políticas corporativas o comerciales, además de las regulaciones de la industria.

Luego de haber revisado los controles y conocer la complejidad de los ataques de ransomware, se presenta en la siguiente sección la actualidad del ransomware.

La actualidad del ransomware (Un caso de Estudio)

En la actualidad existen diversas investigaciones innovadoras para mitigar y responder ante un ataque de ransomware. Para destacar uno de esos, está descrito en un artículo publicado para *Future Internet* llamado: “Ransomware-Resilient Self-Healing XML Documents” (Al-Dwairi et al., 2022).

El artículo propone la implementación de una metodología de control de versiones que, por lo general, se utiliza en la administración de código de programación. Esta metodología funciona guardando copias de cada archivo de código cada vez que ha tenido alguna alteración o modificación por parte de un programador. Esto permite que, en el caso de que un cambio no haya sido el correcto o provoque problemas en el código, pueda ser revertido a un punto anterior de manera controlada.

Se propone la aplicación de esta metodología de control de versiones a documentos XML (documentos de Microsoft Word, Microsoft Excel, PDF, etc.), es decir, generar copias en base a las modificaciones que se van realizando al documento. Adicional al control de versiones, se propone la protección de las copias bajo cifrado o protección a nivel de gestión de usuarios para evitar que en el evento de un ataque de ransomware, este no pueda afectar a estos archivos.

Aparte de la propuesta descrita, varias empresas encargadas de ofrecer soluciones de seguridad, dispositivos de red basados en seguridad, han comenzado a integrar Inteligencia Artificial para que sea la encargada de monitorear, aprender y accionar ante los procesos que ocurran dentro de un equipo computacional o una red. La protección contra el ransomware es fundamental en la era digital actual, donde las amenazas cibernéticas están en constante evolución y pueden causar graves daños a individuos y organizaciones. Para salvaguardarse contra este tipo de ataques, es crucial implementar una combinación de medidas preventivas y de respuesta.

Además, mantener el software y los sistemas operativos actualizados con los últimos parches de seguridad puede cerrar las vulnerabilidades conocidas que los ciberdelincuentes podrían aprovechar. La implementación de *firewalls* y software antivirus robustos también puede ayudar a detectar y bloquear posibles amenazas.

Discusión

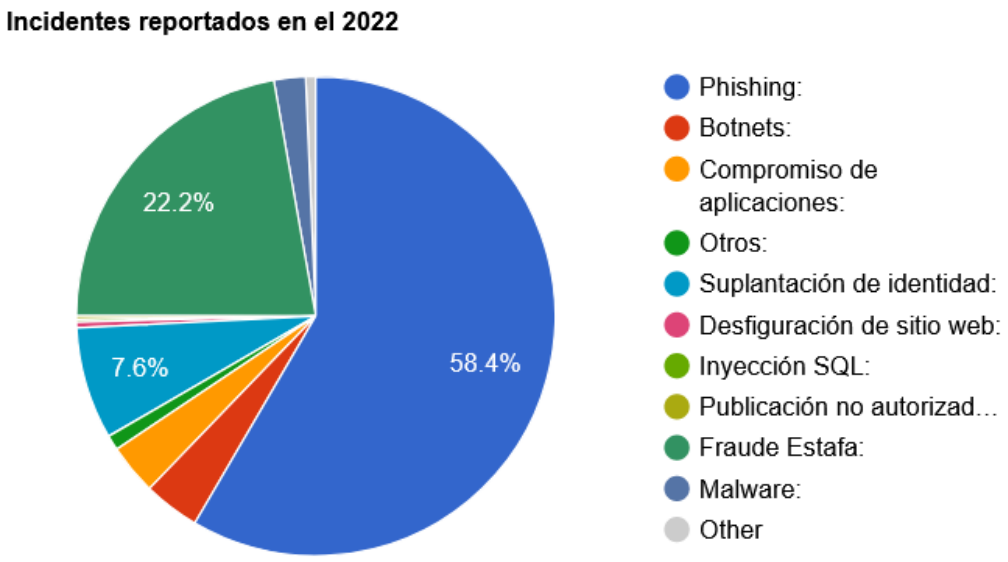
La solución o técnicas brindadas por el articulo generan dudas como ¿Entorpece la funcionalidad normal de un equipo informático? ¿Realmente quedan protegidos los documentos? ¿Qué tan complejo es implementar lo propuesto? Pero inicialmente ¿Las empresas e instituciones de Panamá aplican medidas ante el ransomware?

Panamá ha realizado esfuerzos concertados para mejorar su ciberseguridad. En 2011, se estableció el CSIRT Panamá (Equipo de Respuesta a Incidentes de Seguridad Informática) bajo la Autoridad Nacional para la Innovación Gubernamental (AIG) para prevenir, identificar y resolver incidentes de seguridad cibernética, y para aumentar la concienciación sobre ciberseguridad en el país (Presidencia de Panamá, 2012).

Los ataques recibidos por empresas y entidades públicas son cada vez más frecuentes. Según Fortinet en su informe “Global de Amenazas de FortiGuard Labs” semestral del 2022, el país tuvo un total de 1,400 millones de intentos de ciberataques en ese año, siendo la amenaza principal el ransomware (Fortinet, 2022). Los eventos registrados o reportados al CSIRT han sido en total 3,820 incidentes (CSIRT, s.f.). Ver Figura 1.

Figura 1

Incidentes reportados hacia el CSIRT (CSIRT).



Cada empresa panameña y entidad pública recibe ciberataques en un promedio de 1,300 veces por semana, siendo los principales objetivos las entidades del gobierno, la banca y empresas de finanzas. CheckPoint comenta sobre un considerable aumento en ciberataques de un 124% a empresas panameñas en relación con el año anterior. Detallando que para julio de 2021 los ciberataques en Panamá representaban un promedio de 581 a cada organización por semana y en julio de 2022 se reportan 1,300 (Seguras, 2022).

En la actualidad la situación de Panamá ha mejorado. CheckPoint publicó “Cyber Security Report 2024” donde marca pautas sobre el estado actual de la ciberseguridad a nivel global. En este reporte, Panamá muestra la obtención de un porcentaje de riesgo de 41.3%, en comparación a 43.1% del 2023 y 47.8% del 2022, siendo una mejora del 1.8% y 6.5% respectivamente en la probabilidad de sufrir algún riesgo informático, teniendo un puntaje similar a países de otras latitudes como Italia (41.5%) (CheckPoint, 2024). En cuanto a la legislación, Panamá ha tomado pasos para alinear su marco legal con los estándares internacionales, incluyendo la modificación del Código Penal y la aprobación del Convenio de Budapest sobre delitos cibernéticos.

Además de la creación de la Ley 81 para la protección de datos personales. En conjunción, la educación y formación en ciberseguridad también son prioridades,

con becas y capacitaciones ofrecidas en colaboración con instituciones internacionales para reducir la escasez de profesionales en este campo. Una herramienta que puede aplicar una empresa o institución en su departamento de tecnología, específicamente en el desarrollo de software, es un sistema basado en GIT. Tiene como objetivo principal el proteger el código que se genera de la programación, pero puede tener una aplicación más diversa.

La implementación de GIT en las empresas e instituciones que tengan códigos fuentes de sus sistemas debe ser casi obligatoria para poder resguardar la integridad de estos. Incorporar GIT no supone un consumo notable tanto en la puesta en marcha como en la funcionalidad del día a día; las funcionalidades que encontramos en GIT se muestran a continuación:

- Control de Versiones Distribuido
  - Repositorios Locales Completos: Cada desarrollador tiene una copia completa del historial del proyecto, lo que permite trabajar sin conexión y realizar operaciones de manera rápida y eficiente.
  - Colaboración: Al permitir que múltiples desarrolladores trabajen en diferentes partes del proyecto simultáneamente, Git facilita la colaboración sin interferencias.
- Seguimiento Detallado de Cambios
  - Historial Completo: Git mantiene un registro detallado de todos los cambios, permitiendo a los desarrolladores ver qué cambios se hicieron, quién los hizo y cuándo.
  - Reversión de Cambios: Es fácil revertir a versiones anteriores del proyecto en caso de errores o problemas.
- Seguridad e Integridad
  - Hashes: Git utiliza *hashes* SHA-1 para identificar de manera única cada cambio realizado, asegurando que el historial no pueda ser alterado sin ser detectado.
- Flexibilidad y Compatibilidad
  - Multiplataforma: Git es compatible con diversos sistemas operativos, incluyendo Windows, macOS y Linux.

Con lo plasmado sobre las funcionalidades de GIT, la propuesta de la cual se centra la discusión hace uso de un sistema GIT para resguardar archivos y no código fuente, lo cual resulta ser novedoso en la forma en que es aplicado. Teniendo en cuenta las preguntas formuladas en esta sección como: ¿Entorpece la funcionalidad normal de un equipo informático? ¿Realmente quedan protegidos los documentos? ¿Qué tan complejo es implementar lo propuesto?

En la propuesta se comenta sobre la creación de un *plug-in* para el aplicativo Word a modo de "prueba de concepto". Una vez con el *plug-in* instalado en el equipo, cuando se finaliza la edición de un documento en Word, el *plug-in* procede a generar un *snapshot* del archivo y a dicho *snapshot* le aplica medidas de seguridad, como los permisos de edición, para que no pueda ser alterado en un posible ataque. Todo esto se realiza en segundo plano sin que se interrumpa al usuario durante el proceso.

El artículo menciona la noción de una limitante: el proceso que se ejecuta en segundo plano y realiza las verificaciones de los permisos de edición de los archivos necesita tener privilegios elevados (Administrador) y que los usuarios que estén utilizando el equipo de cómputo no tengan rango de administrador. Esto plantea el otorgarle permiso de Administrador en el equipo de cómputo al proceso, que puede llegar a ser vulnerable en un hipotético ataque de cadena de suministro. Este tipo de ataque de ciberseguridad se basa en que los atacantes comprometen un componente que forma parte o se integra a los sistemas de software que implementan en las empresas. Estos ataques pueden ser particularmente devastadores porque explotan la confianza que las organizaciones tienen en sus proveedores y en los productos que utilizan.

Pasando al punto sobre la integridad y confidencialidad de los archivos, la propuesta no contempla la posibilidad de cifrar los archivos. Esto significa que, durante un ataque donde se pueda vulnerar la funcionalidad de la propuesta, la información de los archivos queda expuesta para la utilidad del atacante. Si bien los ataques de ransomware se caracterizan por su *modus operandi* de cifrar los archivos de la víctima y pedir un rescate económico, también puede ocurrir que el atacante genere

copias de los archivos para uso propio. Por lo que se podría considerar la implementación adicional de cifrado de los archivos por medio de algoritmos convencionales y robustos como SHA-256 (Fauziah et al., 2019).

Agregar esta funcionalidad adicional a la propuesta podría añadir más carga al procesador del equipo de cómputo en el tiempo de ejecución durante el guardado de un archivo de Word. Esto podría notarse si el equipo de cómputo tiene prestaciones no recomendadas o son bajas para los requisitos mínimos de la propuesta. Esto es debido a que el consumo de poder computacional al momento de cifrar archivos es elevado si el equipo no tiene una unidad especializada para cifrar.

Haciendo un pequeño ejercicio, según la propuesta se menciona que el tiempo tomado por el procesador al realizar la ejecución del proceso no excede los 120 ms (milisegundos) para un archivo de 1 MB (MegaByte). Se hizo el ejercicio indicado en la Figura 2, añadiendo el cifrado del archivo, lo que sumaría unos 12 ms, lo cual no representa un impacto significativo para el uso normal del equipo de cómputo.

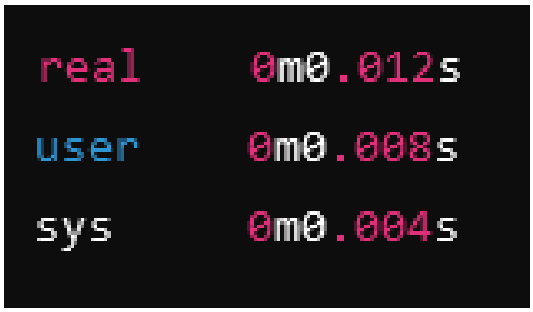
Utilizando los siguientes comandos:

- dd if=/dev/zero of=testfile bs=1M count=1
  (Crea un archivo de 1MB de tamaño).

- time openssl enc -aes-256-cbc -salt -in testfile -out testfile.enc -pass pass:mysecurepassword
  (Cifra el archivo recién creado por el comando anterior

Figura 2

Resultados sobre el cifrado de un archivo de 1MB



Respecto al cifrado, la implementación a nivel de rendimiento no añadiría al consumo y ejecución siempre y cuando se maneje en archivos pequeños ya que a medida que aumenta el tamaño, el consumo aumenta.

Conclusiones

La propuesta discutida en este documento muestra la aplicación de una metodología que normalmente se utiliza en el área de la programación al entorno de uso cotidiano para los usuarios de equipos de cómputo. Esta metodología ofrece protección a los documentos que son tratados por ella ante ataques de ransomware y de la pérdida de la integridad del archivo. Esto muestra que tiene un impacto mínimo o casi imperceptible para el equipo de cómputo y para el usuario.

Adicionalmente, en este documento se planteó la posibilidad de añadir el cifrado de los documentos utilizando una técnica de cifrado como SHA-256 durante la ejecución de la metodología, para tener un grado mayor de protección. Esto con la premisa de que, si bien no se adultera el archivo durante un ataque de ransomware, también se pueden extraer archivos que quedan expuestos ante los atacantes. Al cifrarlos, los atacantes no podrán tener acceso al contenido del archivo. Adicionalmente al planteamiento de agregación del cifrado de archivos, se realizó una pequeña prueba de tiempo para determinar si afectaba a la usabilidad de los usuarios y equipos de cómputo, con un resultado de afectación imperceptible.

Referencias bibliográficas

Al-Dwairi, M., Shatnawi, A. S., Al-Khaleel, O., & Al-Duwairi, B. (2022). *Ransomware-Resilient Self-Healing XML Documents*. Future Internet, *14*(4), 118. https://doi.org/10.3390/fi14040118

Alcántara, M., & Melgar, A. (2016). Risk Management in Information Security: A Systematic Review. Journal of Advances in Information Technology, *7*(1), 1-13. https://www.semanticscholar.org/paper/Risk-Management-in-Information-Security%3A-A-Review-Alcantara-Melgar/eecec6f2c2822abd7077238cb636734f182de218

Beaman, C., Barkworth, J., Akande, T., Hakak, S., & Khan, H. A. (2021). The Impact of the COVID-19 Pandemic on Ransomware Attacks. 2021 International Conference on Information Networking (ICOIN), 638-643. https://doi.org/10.1109/ICOIN51403.2021.9392211

Biju, J. M. (2019). Types of Cyber Attacks and Their Prevention Methods. International Journal of Advanced Engineering and Management, *4*(2), 1-5. https://www.ijamr.com/index.php/ijamr/article/view/100088

Bouam, M., Bouillaguet, C., Delaplace, C., & Noûs, C. (2021). A Survey on Cyber-Attacks and Their Impact on Modern Society. Journal of Cybersecurity and Digital Forensics, *4*(2), 1-15. https://www.jcdf.eu/index.php/jcdf/article/view/123

CheckPoint. (2024). *Cyber Security Report 2024*. Recuperado de https://www.checkpoint.com/downloads/downloads-reports/2024-cyber-security-report.pdf

CSIRT. (2022). *Ransomware: una amenaza para la seguridad de la información*. Recuperado de https://csirt.gob.cl/vulnerabilidades/ransomware-una-amenaza-para-la-seguridad-de-la-informacion/

CSIRT. (s.f.). *Incidentes reportados hacia el CSIRT*. [Gráfico].

Fauziah, R., Rachmawanto, E. H., Setiadi, D., & Sari, C. A. (2019). An Overview of SHA-256 and Its Implementation in Digital Signature. Journal of Physics:

Conference Series, *1374*(1). https://doi.org/10.1088/1742-6596/1374/1/012015

Fortinet. (2022). *Global Threat Landscape Report 2022*. Recuperado de https://www.fortinet.com/content/dam/fortinet/assets/reports/report/2022-fortiguard-labs-global-threat-landscape-report.pdf

IBM. (s.f.). *What are security controls?* Recuperado de https://es.wiktionary.org/wiki/complet%C3%A1

Miles, M. B., & Huberman, A. M. (1994). Qualitative data analysis: An expanded sourcebook. SAGE Publications.

Presidencia de Panamá. (2012). *Decreto Ejecutivo No. 403 de 2012*. https://www.gacetaoficial.gob.pa/pdfTemp/27043_A/Gaceta Oficial.pdf

Richardson, R. (2017). Ransomware: A Comprehensive Guide to Prevention, Detection, and Recovery. SAGE Publications.

Seguras, J. (2022). *Ciberataques en Panamá se incrementan 124%*. La Prensa. https://www.prensa.com/economia/ciberataques-en-panama-se-incrementan-124-en-un-ano/

Veritas. (s.f.). *Ransomware Prevention and Protection*. https://www.veritas.com/services/ransomware-protection