47

Fecha de presentación: Agosto, 2024
Fecha de aceptación: Octubre, 2024
Fecha de publicación: Noviembre, 2024

# IMPACTO

## DE CENTRALIZAR BASES DE DATOS EN ECUADOR CON CIBERSEGURIDAD BASADA EN INTELIGENCIA ARTIFICIAL

## IMPACT OF CENTRALIZING DATABASES IN ECUADOR WITH ARTIFICIAL INTELLIGENCE-BASED CYBER SECURITY

Alberto Leonel Santillán Molina[1]
E-mail: aleonelsm@hotmail.com
ORCID: https://orcid.org/0000-0001-8517-8980
[1]Centro de Estudios para la Calidad Educativa y la Investigación Científica "CECEIC", México.

Cita Sugerida (APA 7ma Edición)

Santillán Molina, A. L. (2024). Impacto de centralizar bases de datos en Ecuador con ciberseguridad basada en inteligencia artificial. ***Universidad y Sociedad, 20***(6),454-464.

RESUMEN

El Ecuador fue víctima de varios ataques informáticos, en el año 2019 se obtuvo ilegalmente información personal y financiera de diecisiete millones de ecuatorianos; en el año 2021 fue atacada la Corporación Nacional de Telecomunicaciones mediante la implantación de un virus informático denominado RansomEXXX, que secuestró información de usuarios, lo que develó la inseguridad y vulnerabilidad informática en Ecuador. En el año 2022 se formuló una Estrategia Nacional de Ciberseguridad con lineamientos específicos para la seguridad en el ciberespacio, sin embargo esta no da solución a los problemas de vulnerabilidad en las empresas públicas o privadas, generándose un problema de investigación por la falta de políticas públicas que permita la centralización de base de datos nacional, protegido por un sistema de ciberseguridad basado en inteligencia artificial, planteándose como objetivo al determinar el impacto de una política pública que garantice un sistema de ciberseguridad basado en IA, y que permita la detección de los incidentes informáticos y prevención de la vulneración de los sistemas de información. En esta investigación se utilizaron métodos como el histórico-lógico para analizar la evolución de las TIC y la ciberseguridad, el analítico-sintético para comprender el papel de las TIC en el ciberdelito, y el inductivo-deductivo para formular estrategias de prevención. Se emplearon técnicas como el análisis documental, entrevistas y grupos de discusión para recopilar datos sobre los temas tratados, y al término de esta se concluyó que una política pública en estos términos, fortalecería la ciberseguridad y fomentaría un entorno de confianza informática.

Palabras clave: Política pública, Inteligencia artificial, Ciberseguridad, Cibercrimen.

ABSTRACT

Ecuador was the victim of several computer attacks. In 2019, the personal and financial information of seventeen million Ecuadorians was illegally obtained; in 2021, the National Telecommunications Corporation was attacked through the implementation of a computer virus called RansomEXXX, which kidnapped user information, which revealed computer insecurity and vulnerability in Ecuador. In 2022, a National Cybersecurity Strategy was formulated with specific guidelines for security in cyberspace, however, it does not provide a solution to vulnerability problems in public or private companies, generating a research problem due to the lack of public policies. That allows the centralization of a national database, protected by a cybersecurity system based on artificial intelligence, setting the objective of determining the impact of a public policy that guarantees a cybersecurity system based on AI, and that allows the detection of incidents IT and prevention of breaches of information systems. In this research, methods such as the historical-logical method were used to analyze the evolution of ICT and cybersecurity, the analytical-synthetic method to understand the role of ICT in cybercrime, and the inductive-deductive method to formulate prevention strategies. Techniques such as documentary analysis, interviews and discussion groups were used to collect data on the topics discussed, and at the end of this it was concluded that a public policy in these terms would strengthen cybersecurity and promote an environment of computer trust.

Keywords: Public policy, Artificial intelligence, Cybersecurity, Cybercrime.

## INTRODUCCIÓN

Las Tecnologías de la Información y la Comunicación, presentan a la humanidad una nueva forma de vida con avances tecnológicos, que permiten a los usuarios tener mayor facilidad para el manejo de sus vidas y sus actividades cotidianas.

Esta forma de administración del control de la información, fue manejado por instituciones estatales, con el objetivo de mantener controlado el flujo de la información, lo cual facilita el desarrollo de personas, empresas, e instituciones que ven en las Tecnologías de la Información y la Comunicación, TIC, un cúmulo de oportunidades para crecer gradualmente, pero al mismo tiempo, se han "abierto puertas para actividades ilícitas por medios informáticos, así como a un amplio campo de riesgos para la vulneración de estos sistema" (Ojeda-Pérez et al., 2010)

Las Tecnologías de la Información y la Comunicación, se han convertido en un "motor eficiente de administración pública entre las empresas y el gobierno que incluyen nuevos procesos, nuevas formas de administración. Con el uso de las TIC se relacionan directamente las entidades gubernamentales con el gobierno y las empresas privadas" (Medina-Quintero et al., 2021), desarrollando también estudios e investigaciones en disciplinas jurídicas y técnicas, pero especialmente en aquellas asociadas con auditoría de sistemas o auditoría informática, con la finalidad de evitar que los sistemas automatizados de información se vuelvan inseguros.

"La seguridad informática debe asegurar los recursos que presenta un sistema automatizado de información de una institución, empresa o negocio, para que estos sean utilizados del modo que decidió el titular" (Costas, 2011), y que su acceso, así como la modificación de los datos informáticos, solo le sea permitido a quien cuentan con la autorización y estén acreditados para ello.

Tanto la seguridad de la información, como la seguridad informática, es un derecho que tiene cada individuo para el uso de los medios tecnológicos, operativizar sus actividades, y acceder a la información que se encuentran en base de datos gubernamentales o privadas, a nivel territorial, nacional o internacional y beneficiarse de ellos.

De este modo la ciberseguridad en el Siglo XXI se encuentra ante múltiples retos tales como la "detección de intrusiones, la identificación de comportamientos anómalos dentro de un sistema de información automatizado, la protección de datos personales privados, la detección de las ciberamenazas" (Ayerbe, 2020).

La inteligencia artificial es una "rama de la informática, que con el uso de algoritmos crean mecanismos que pueden mostrar comportamientos inteligentes con capacidad de razonamiento y aprendizaje como el ser humano" (Ardila et al., 2020), que sumado a la ciberseguridad y con auxilio de la IA, podrán tecnológicamente identificar, proteger, detectar y dar una respuesta, así como recuperarse ante incidentes informáticos.

En tal virtud, la ciberseguridad debe considerarse como un "bien público, el cual es un recurso que es propiedad de todos los ciudadanos" (López, 2021), es indivisible y puede ser compartido por todos los miembros de una comunidad.

Sin embargo, dado que las TIC tienen aplicación a nivel mundial, el acceso a la información y su seguridad se encuadrarían en la definición que para el efecto desarrolló Jorge García en su calidad de autor de la Teoría de los Bienes Públicos Globales, el cual define que un "bien público global se verifica cuando se encuentra provisto de beneficios para más de un grupo de países o para una parte importante de la población a nivel mundial" (García, 2004) y aún más, para aquellas generaciones venideras que se beneficiarían de este bien público.

La República del Ecuador en el año 2019, sufre un ataque informático del cual se obtiene de manera ilegal datos personales de ciudadanos nacionales, por lo que el Presidente Constitucional de aquel entonces Lic. Lenin Moreno Garcés, mediante memorando núm. 0184 del mes de septiembre de ese año, entrega a la Función Legislativa el Proyecto de Ley Orgánica de Protección de Datos Personales, el cual entra en vigencia el 26 de marzo de 2021 mediante publicación en el V Suplemento del Registro Oficial núm. 459, ordenamiento jurídico que tiene como objeto y finalidad el "garantizar el ejercicio del derecho a la protección de datos personales" (Ley Orgánica de Protección de Datos Personales, 2021), pero que dicha ley no aborda la seguridad de los sistemas informáticos como tal, teniendo en cuenta que en el ciberespacio no solo hay datos personales que proteger, sino también el dato informático en específico, debido que en su conjunto al momento de ser procesados, permiten el funcionamiento de la simbiosis tecnológica como es la inter operatividad de los sistemas informático, telemático y de telecomunicaciones.

La Corporación Nacional de Telecomunicaciones (CNT) como empresa responsable del ciberespacio en el Ecuador, en 2021 fue víctima de ciberdelincuentes mediante la implantación de un virus informático denominado RansomEXXX, el cual tenía como objetivo el secuestro de la información y con permisos de administrador,

impedir el acceso del titular a la información guardada en sus archivos, para posteriormente solicitar el rescate de esta. Esta conducta en informática se la conoce como *Ransomware*.

El dieciocho de marzo de 2004 se publicó en el Registro Oficial del Ecuador No. 337 la Ley Orgánica de Transparencia y Acceso a la Información Pública, en concordancia con lo dispuesto en la Constitución, así como en la Convención Americana de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos, donde se normativiza el "derecho de las personas de acceder a la información con las restricciones del caso" (Ley Orgánica de Transparencia y Acceso a la Información Pública, 2004).

La Constitución de la República del Ecuador en su artículo 66, numeral 19, describe el "derecho a la protección de sus datos de carácter personal de cada uno de los ciudadanos nacionales o extranjeros residentes en el país, así también la decisión de su manejo, procesamiento y archivo de la información" (Constitución de la República del Ecuador, 2008).

El 10 de agosto de 2014 en el Ecuador entra en vigencia el Código Orgánico Integral Penal (Código Orgánico Integral Penal, 2014), donde describe y sanciona los delitos informáticos, habiendo sufrido una reforma que fue insertada en dicho ordenamiento jurídico punitivo el 8 de diciembre de 2020 y publicada en el Registro Oficial núm. 345 donde se tipificaron los delitos informáticos vigentes en la República del Ecuador.

La Organización de las Naciones Unidas en el año 2013 a través de la Oficina de las Naciones Unidas contra la Droga y el Delito UNODC, determinó que el aumento de la cibercriminalidad se debía a los siguientes hechos:

a) La existencia de leyes nacionales diversas; b) Dependencia a la cooperación internacional para abordar la cibercriminalidad; c) Imposibilidad en la obtención de la evidencia digital debido a la falta de norma en las diferentes legislaturas; d) Falta en la organización para la obtención de la evidencia digital y la investigación; e) Falta de recursos en países en vías de desarrollo para la investigación del cibercrimen; y f) Prevención del ciberdelito. (Ministerio del Interior de la República del Ecuador, 2019).

En el Plan Específico de Seguridad Pública y Ciudadana 2019-2030, (Ministerio de Interior del Ecuador, 2019), con el objeto de enfrentar a los grupos organizados de poder, se plantea los siguientes objetivos: 6. Fortalecer el sistema de información con la estandarización y calidad de datos y las estadísticas encargadas de seguridad y justicia; y 7. Implementar la anticipación estratégica en las acciones públicas, para enfrentar amenazas con el crimen organizado, lavado de activos, delincuencia transnacional, terrorismo y cibercriminalidad (Ministerio del Interior de la República del Ecuador, 2019).

Con la implementación de las TIC en esta sociedad digital, a la ciudadanía se le permite acceder a equipos informáticos que "editen, produzcan, intercambien, almacenen y transmitan datos informáticos, a través de los sistemas automatizados de información" (Desongles & Moya, 2006), permitiendo así la "conexión intersubjetiva" (Aboso & Bidasolo, 2017), a nivel global que presentan un crecimiento acelerado de los entes sociales, financiero, económico, político y cultural, debido a la facilidad en la operativización de las actividades cotidianas tales como el comercio en línea o el uso de las diferentes plataformas digitales de las instituciones financieras, permitiendo así el desarrollo de los países con acceso a la tecnología, y ahondando la "brecha digital" (Organizacion de las Naciones Unidas [ONU], 2002), en aquellos territorios a los que les hace falta aquella.

Del mismo modo en que se desarrolla la sociedad de la información con los avances tecnológicos beneficiosos para la ciudadanía en general, también lo hizo la "cibercriminalidad al momento de ejecutar actividades ilícitas en territorio digital con el uso de las Tecnologías de la Información y Comunicación" (Pérez, 2021), alertando de manera clara de la entrada de un nuevo orden en el mundo delictivo como es la ciberdelincuencia.

Las medidas de seguridad más comunes a las que tienen acceso la mayoría de las personas en esta era digital son: "el registro biométrico facial, registro de patrones de voz, lector de retina, usuario y contraseña y huella dactilar", (Suarez, 2017), configurándose el delito de hackeo cuando existe vulneración de estas medidas de seguridad informática.

La "vulneración de las medidas de seguridad que están implementadas en los sistemas automatizados de información, para luego acceder a este y consumar las conductas de espionaje o sabotaje informático" (Santillán, 2023) se lo define como el delito de hackeo, o acceso no autorizado a un sistema informático, telemático o de telecomunicaciones.

La Organización de Estados Americanos define el Gobierno Electrónico como:

La entidad que controla el uso de las Tecnologías de Información y Comunicación TIC por parte de las instituciones de gobierno, para mejorar cualitativamente los servicios e información que se ofrecen a los ciudadanos;

aumentar la eficiencia y eficacia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación ciudadana (Organizacion de los Estados Americanos [OEA], 2022).

El Ecuador en el año 2022 formula una Estrategia Nacional de Ciberseguridad con lineamientos específicos para la seguridad en el ciberespacio basado en seis ejes coyunturales: "1. Gobernanza y coordinación nacional; 2. Resiliencia cibernética; 3. Prevención y combate a la ciberdelincuencia; 4. Ciberdefensa; 5. Habilidades y capacidades de ciberseguridad; y, 6. Cooperación internacional" (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022).

Una política pública es una "estrategia con la que un gobierno coordina y articula las acciones intencionales para la ejecución concreta de decisiones que giran en torno de objetivos colectivos, los cuales son de interés público, frente a situaciones socialmente relevantes" (Torres, 2013).

En esta política pública de ciberseguridad, con la finalidad de dar cumplimento al objetivo 2.3 del Pilar 2 sobre la Resiliencia Cibernética, en la que se dispone continuar desarrollando capacidades de respuesta y gestión de incidentes cibernéticos del CERT Nacional, a través del Centro de Respuesta a Incidentes Informáticos del Ecuador, EcuCERT por sus siglas identificativas, se puede llegar a determinar de los propósitos de la Agencia de Regulación y Control de las Telecomunicaciones, que al "cooperar y ser el punto de contacto con otros equipos de respuesta; así como promover la creación de equipos de respuesta a incidentes informáticos; y establecer criterios generales y específicos" (ARCOTEL, 2015), se considera que no se da solución a los problemas socialmente relevantes, tales como: 1. Que la ciberseguridad se la deja a cada institución, empresa, o negocio y al ciudadano común; 2. Los ataques y ciberamenazas continúan; 3. No hay responsabilidad del Estado de asumir la ciberseguridad como bien público y tomar decisiones para el control, prevención y detección de ciberataque o ciberamenazas.

El Estado Ecuatoriano con la finalidad de proteger la seguridad de la información e informática, debería centralizar los datos de las instituciones del sector público, así como de empresas, negocios y ciudadanía en general, y de esa manera garantizar la ciberseguridad de estos, pero sucede que cada institución maneja de forma independiente su seguridad, con estrategias diversas de acuerdo a su naturaleza y sin un conocimiento especializado, lo único que hace el Estado ecuatoriano es ser un ente de control y supervisión que solicita a sus empresas e instituciones, información referente a sus estrategias de seguridad implementadas.

En este sentido el Gobierno Nacional debería establecer un conjunto de políticas públicas que potencien el objetivo 2.3 del Pilar 2 de la Estrategia Nacional de Ciberseguridad del Ecuador, centralizando todos los datos de las empresas e instituciones públicas y privadas, y así controlar, detectar y prevenir el delito informático.

Por tanto, se puede establecer que el problema de investigación radica, en la falta de políticas públicas que permitan la centralización de base de datos nacional, protegido por un sistema de ciberseguridad basado en inteligencia artificial, y así prevenir la vulneración de los sistemas automatizados de información en el Ecuador.

Por lo expuesto, se plantea el objetivo de determinar el impacto de una política pública que garantice un sistema de ciberseguridad basado en inteligencia artificial, que permita la detección de los incidentes informáticos y la prevención de la vulneración de los sistemas de información, el fortalecimiento de la seguridad de estos tanto en las instituciones públicas como privadas.

## MATERIALES Y MÉTODOS

Se emplearon métodos del nivel teórico y empírico en el desarrollo de la investigación, entre ellos:

- Histórico-lógico que permitió establecer la trayectoria histórica de las TIC, el bien público, el gobierno electrónico, las políticas públicas, el cibercrimen y la ciberseguridad, y en base a esto, se estableció cómo funcionan las diferentes entidades públicas y privadas en cuanto a los procedimientos establecidos para garantizar la seguridad de los sistemas automatizados de información.
- El Analítico-sintético fue aplicado a las definiciones teóricas que permitió realizar el estudio sobre el empleo de las TIC en favor del ciberdelito, así como la necesidad de que el Estado se responsabilice por la ciberseguridad como bien público.
- El método inductivo deductivo se empleó para la generalización de los resultados de las entrevistas semiestructurada las que estuvieron diseñadas, desde la inducción, a través de un cuestionario que permitió expresar sus opiniones de manera abierta sobre la vulneración de los sistemas automatizados de información, la ciberseguridad, y la inteligencia artificial, y desde la deducción se formuló en acuerdo una estrategia para prevenir esta vulneración, mediante la centralización de base de datos protegido por un sistema de ciberseguridad basado en inteligencia artificial.

Las técnicas de investigación científica que se utilizaron en este instrumento fueron:

- El análisis de documentos que fueron consultados en cuanto al tema. Dentro de esta técnica se tuvo especial atención al análisis de contenidos aplicado a las diferentes fuentes documentales relacionadas con las TIC, el bien público, el Gobierno Electrónico, las políticas públicas, el cibercrimen y la ciberseguridad y la inteligencia artificial.
- La técnica de la entrevista fue de capital importancia para recabar cualitativamente datos de expertos sobre los temas relacionados con las TIC, el bien público, el Gobierno Electrónico, las políticas públicas, el cibercrimen, la ciberseguridad y la inteligencia artificial.
- Se utilizó el grupo de discusión como técnica de investigación cualitativa con el fin de obtener información sobre el objetivo de investigación a través de un diálogo colectivo con expertos referente a los temas planteados en este trabajo de investigación, tales como: políticas públicas, administración pública, ciberseguridad e inteligencia artificial.

## RESULTADOS Y DISCUSIÓN

De las entrevistas realizadas a expertos, entre ellos:

- Técnicos de seguridad informática y de la información;
- Jefes de las Direcciones, Unidades o Departamentos de TIC de las empresas públicas o privadas, entre estas a personal de Fiscalía General del Estado;
- Personas que han sido víctimas de ciberataques;
- Personal docente de instituciones del nivel medio y superior;
- Personal de Fiscalía General del Estado del Ecuador;
- Personal de la Corporación Nacional de Telecomunicaciones, empresa estatal dedicada al control, manejo y comercialización de las telecomunicaciones en la República del Ecuador;
- Entrevista a Asambleístas de la Asamblea Nacional del Ecuador, se pudo obtener la siguiente información:

En las intromisiones a los sistemas automatizados de información, generalmente se detectan una vez que ya ha sido vulnerado el mismo, en virtud de que si no existe un proceso de ***hardening*** que es el "endurecimiento de las medidas de seguridad" (Centro de innovación y soluciones empresariales y tecnológicas, 2020), o no se tienen actualizados los respectivos softwares que den resguardo a ese sistema, no se puede detectar sino hasta cuando ya se ha realizado el acceso no autorizado y la información se encuentra ya en poder del hacker.

Es necesario diferenciar entre un ataque informático de una intromisión. Un ataque informático se refiere a cualquier intento malintencionado de comprometer la seguridad de un sistema informático. Esto puede incluir intentos de acceder a información confidencial, dañar o modificar archivos importantes, interrumpir el funcionamiento normal de un sistema o utilizarlo para fines malintencionados. Los ataques informáticos pueden llevarse a cabo mediante diversas técnicas, como la ingeniería social, la explotación de vulnerabilidades del software, la suplantación de identidad o el uso de malware.

Por otro lado, la intromisión informática se refiere específicamente a la entrada no autorizada en un sistema informático con el fin de acceder a información o recursos a los que el intruso no tiene derecho. Esto puede implicar el uso de técnicas de ***hacking*** para sortear las medidas de seguridad del sistema, la explotación de vulnerabilidades o la utilización de credenciales robadas o comprometidas para acceder a este.

En lo que tiene que ver con el ataque como tal, inmediatamente después de que el "hacker ético, quien realiza intromisiones controladas y bajo la supervisión del titular de los datos" (Rodríguez Llerena, 2020) ha podido detectar que se está atacando el sistema, este puede utilizar medidas de seguridad que contrarresten el ataque o la intromisión, tales como:

a) identificar y aislar la amenaza para evitar que se propague a otros sistemas y causar daños adicionales;
b) desconectar el sistema de la red lo que puede ayudar a evitar que la amenaza se irradie a otros lugares del sistema;
c) eliminar la amenaza de los sistemas afectados es importante para evitar que siga causando daño. Esto puede implicar la eliminación de archivos infectados, la eliminación de usuarios o cuentas de usuario comprometidas, o la limpieza de los sistemas infectados con malware;
d) restaurar los sistemas afectados a un estado anterior conocido como seguro, lo que implicaría la reinstalación del software y la restauración de los archivos importantes a partir de copias de seguridad;
e) cambio de contraseñas de las cuentas afectadas para evitar que los atacantes vuelvan a obtener acceso a los sistemas y datos; y finalmente; f) investigar la intromisión informática para determinar cómo ocurrió y tomar medidas preventivas para evitar que vuelva a suceder en el futuro, para lo cual se implementarán medidas adicionales de seguridad informática, la capacitación de los usuarios o la mejora de las políticas de seguridad informática.

En cuanto a la capacitación, esta no se imparte dentro de las empresas, instituciones del sector público, debido a que no ha existido una cultura seria de ciberseguridad de los sistemas, razón por la cual ha existido muchas

denuncias en fiscalía por los incidentes informáticos, que entre 2019 a 2023, se pudo evidenciar las amenazas denunciadas en esta entidad del Estado; ni tampoco existe en la educación media y secundaria una malla curricular que garantice el proceso enseñanza-aprendizaje sobre ciberseguridad, lo que se pudo evidenciar mediante la entrevista a un director de un centro de estudios medio y superior, lo que sí hay en formación básica y media es en uso de las TIC, más no en seguridad informática.

Los mecanismos de respuesta a los incidentes informáticos que se presenten son: a) identificación de la infección; b) determinar su alcance si es en el equipo o en la red; c) mantener la continuidad del negocio; d) contener las acciones maliciosas; e) erradicar la infección y el vector de ataque; f) recuperar la normalidad de las operaciones; y, g) registrar las lecciones aprendidas.

De los mecanismos de respuesta a los incidentes informáticos que anteceden, los que se pueden aplicar con inteligencia artificial son el literal a) y el c), ya que la IA detecta anomalías en virtud de que puede analizar grandes cantidades de datos y detectar patrones o comportamientos que se desvían de lo normal, lo que puede ayudar a identificar posibles amenazas o intrusiones en una red o sistema.

Así también realiza un análisis automático de los comportamientos de usuarios los cuales pueden ser sospechosos o anómalos que podrían indicar una amenaza, identificaría vulnerabilidades que pueden ser corregidas por desarrolladores de software antes de que sean explotadas, además de que la IA también puede ser programada para bloquear el acceso de un usuario sospechoso o desconectar un dispositivo infectado de la red.

a) De las entrevistas se pudo determinar que las capacitaciones que deberían de impartirse deben ser sobre ciberseguridad básica, así como la seguridad en profundidad y el uso de los mecanismos de ciberdefensa, para que tanto los ciudadanos como las empresas, estén preparados y capacitados para enfrentar estas amenazas y protegerse de ellas, cuyos temas deberían abordar: a) la conciencia de riesgos a comprometer la seguridad informáticas y la forma de prevenirlos;
b) mejores prácticas que permitan proteger sus sistemas y redes informáticas, que incluirán el manejo de contraseñas seguras, la actualización regular de software, la identificación de correos electrónicos fraudulentos y el uso de software antivirus;
c) prevención de ataques en la que los usuarios identifiquen y respondan a las amenazas de manera más efectiva;
d) aplicación del proceso de ***hardening***, que consiste en el endurecimiento de las medidas de seguridad informática y de la información;
e) conocimiento para la aplicación de la seguridad en profundidad para que esta sea más eficiente.

Como resultado de las entrevistas se obtuvo información relevante sobre un mecanismo de ciberseguridad que las empresas con recursos suficientes lo usan en la actualidad, denominado “seguridad en profundidad” cuyos componentes de respuesta a los incidentes informáticos, son los siguientes: a) datos informáticos mediante la encriptación, ofuscación digital, ***right management***; b) aplicación técnicas de programación, tales como: política de contraseña segura, controles de acceso firewall; evaluación de seguridad; c) host: mediante controles de seguridad; estándares de endurecimiento del proceso de ***hardening***; gestión de parches de seguridad; prevenciones de intromisiones; antimalware; log de seguridad; y, escaneo de vulnerabilidades; d) en la red interna mediante auditorías de seguridad; e) perímetro del sistema mediante la aplicación de un firewall; pruebas de penetración o ***pest testing; web app, firewall***; sistema de detección y de prevención de intrusos; f) seguridad física, tales como el control de acceso físico; monitoreo; vigilancias; alarmas de seguridad perimetral; controles ambientales; g) políticas y procedimientos de concientización; política de seguridad de la información; organización de seguridad de roles y responsabilidad de seguridad; procedimiento y estándares; y programas de educación sobre ciberseguridad.

De las entrevistas realizadas se pudo llegar a establecer que uno de los principales desafíos en la implementación de niveles de seguridad informática radica en el aspecto oneroso de los costos asociados. Establecer un sistema de seguridad sólido implica una inversión significativa en términos de recursos financieros, tecnológicos y humanos. La adquisición de software especializado, hardware de última generación, capacitación del personal y la contratación de expertos en ciberseguridad implican gastos considerables para las organizaciones.

Además del aspecto económico, otro obstáculo importante es la falta de cultura en ciberseguridad. En muchos casos, las empresas y los individuos no son plenamente conscientes de los riesgos y las amenazas existentes en el ámbito digital. La falta de conciencia sobre las mejores prácticas de seguridad, como el uso de contraseñas fuertes, la actualización regular de software y la protección contra el phishing y el malware, contribuye a la vulnerabilidad de los sistemas informáticos.

Asimismo, la falta de inversión adecuada en seguridad informática puede tener consecuencias negativas. Al no destinar suficientes recursos para proteger la información, las organizaciones corren el riesgo de sufrir brechas de seguridad y filtraciones de datos. La información sensible y confidencial puede caer en manos equivocadas, lo que puede resultar en pérdidas financieras, daño a la reputación e incluso acciones legales.

Es importante destacar que la información que se maneja en los sistemas informáticos debe recibir la debida importancia y protección. Los datos personales, financieros y estratégicos deben ser resguardados de manera adecuada para garantizar la privacidad, la integridad y la disponibilidad de la información.

De las diferentes opiniones entregadas por los entrevistados se pudo llegar a determinar que efectivamente las inversiones a futuro son en ciberseguridad, debido a que todos los procesos operativos que tenga que ver con el manejo de información en las empresas, negocios e instituciones públicas serán mediante el uso de las TIC.

Se pudo verificar que todos los entrevistados, a excepción del técnico de seguridad informática que labora en la Corporación Nacional de Telecomunicaciones, han sido víctimas de hackeo en sus sistemas, sea en su trabajo o en sus cuentas del sistema financiero, así como también el acceso a sus teléfonos móviles.

Una de las funciones de la Asamblea Nacional en la República del Ecuador es: discutir, debatir y tomar decisiones sobre temas de interés nacional, para lo cual se discuten y aprueban leyes, por lo que al entrevistarse a un Asambleísta en funciones, supo explicar que esa clase de proyectos de ley sobre ciberseguridad, aún no han sido presentados en el Poder Legislativo para ser discutidos en atención a la realidad que se presente en ese momento histórico determinado, teniendo en cuenta las diferentes implicaciones sociales, culturales y políticas relativas a la seguridad de la información. Sin embargo, anota que se encuentra en vigencia la ley de Protección de Datos Personales como un avance en esta materia.

De la entrevista al Técnico de Seguridad Informática de la Corporación Nacional de Telecomunicaciones, se pudo determinar que el sistema de la CNT, fue infectado con el virus ***Ransomware*** XX 2.0, extrayéndose información sensible sobre los abonados quienes figuran como clientes de la empresa estatal de telecomunicaciones, no pudiéndose obtener más información sobre el caso, debido a la reserva legal de la investigación que lleva Fiscalía General del Estado. La hipótesis que se maneja hasta ahora sobre la intromisión a la CNT es que se realizó una ingeniería social, que no es otra cosa que el análisis de perfiles de usuarios, así como también con el uso de un ***insider hacker***, es decir de una persona que ingresó manualmente el virus al sistema lo que no permite detectarlo antes, sino cuando ya la información estaba en poder de los hacker, quienes aplicando la metodología para el hackeo esto es, buscaron el punto de entrada y allí cargaron el virus ***Ransomware*** XX 2.0.

De la información recabada sobre la centralización de datos en una sola base protegido por un sistema de ciberseguridad basado en inteligencia artificial, sería muy beneficioso por dos vectores importantes al momento de una ciberdefensa: 1. La base de datos se concentra en un solo dominio o servidor lo que permitiría abaratar costos; y 2. Sería más fácil responder a los incidentes informáticos cuando se debe defender un solo elemento, y que con el auxilio de la IA, que no solo daría la alerta para que agente de seguridad informática actúe, sino que también se le puede programar para que responda al ataque o intromisión de manera emergente y así prevenir la vulneración de los sistemas automatizados de información.

Discusión

El grupo de discusión es una técnica cualitativa de investigación científica en la cual un "grupo de personas especialistas en el tópico a tratar, se reúnen con el objetivo de discutir un tema específico" (Mena & Mendez, 2019), el cual está dirigido por un moderador, por tanto, permite estudiar y hace emerger las diferentes posiciones del grupo de pares, en un ambiente de confianza.

En atención a lo expuesto se invitó al grupo de discusión a profesionales de diferentes ramas, entre ellos, Abogados y Magister en Administración Pública; Lic. En Administración pública y Políticas Públicas, y Magísteres en Ciberdelincuencia, a quienes, para respetar su privacidad, se los identificará asignándoles un numero en específico.

Estos profesionales son invitados a un grupo de discusión a través de una reunión por el aplicativo ***Zoom*** para obtener información detallada sobre las experiencias, percepciones, opiniones y actitudes respeto al tema de discusión el cual fue: "Impacto de una política pública que centralice una base de datos en el Ecuador, protegido por un sistema de ciberseguridad basado en inteligencia artificial, con la finalidad de prevenir la vulneración de los sistemas automatizados de información, tanto en entidades públicas como privadas".

La dinámica que se articula en este grupo de discusión fue a través de una presentación sobre el problema de investigación, así como el objetivo, que generó una situación discursiva en la cual, mediante un grupo de

preguntas realizadas por el moderador que en este caso fue el investigador, cada uno de los participantes expresaba su opinión al tema planteado:

Participante 1 (Política Pública y Administración Pública).

a) Que le parece viable una propuesta de política pública sobre la centralización de base de datos protegidos por un sistema de ciberseguridad basado en inteligencia artificial, pero que, en consenso con lo sostenido con otros participantes en el grupo de discusión, se suma al hecho de que éstas deben ser fortalecidas con otras políticas públicas y asegurar el buen funcionamiento del sistema.

b) Considera que debe de ponerse en práctica esta política pública para preservar y garantizar el derecho de los ecuatorianos a la intimidad y privacidad de los datos personales.

c) Finalmente sostiene que la centralización de base de datos es viable dada la situación que se encuentra el país, y que los continuos ataques y amenazas informáticas de la cual es víctima el Ecuador, se debe a que la moneda de legal circulación en territorio ecuatoriano es el dólar americano, y esto vuelve atractivo a la cibercriminalidad, ya que no tienen que vulnerar sistemas informáticos americanos que tienen niveles de seguridad de grado militar, sino que acceden a un país como el nuestro donde la ciberseguridad no es tan fuerte.

Participante 2 (Política Pública y Administración Pública).

Sostiene que la propuesta es viable desde tres elementos básicos: a) el metodológico; b) la dimensión del Derecho constitucional y legal; y c) la viabilidad técnica.

La parte metodológica ha sido acreditada a través de los parámetros de una investigación científica profunda, que aborda los problemas socialmente relevantes en materia de ciberseguridad en Ecuador y su posible solución.

Desde la dimensión del Derecho constitucional y legal, sostiene que las políticas públicas son garantías jurisdiccionales de derechos constitucionales, los cuales deben ser cumplidos por el gobierno, sustentándose en el marco legal ecuatoriano, tal como lo ha hecho en esta propuesta al abordar, tanto la Constitución de la República del Ecuador, la Ley Orgánica de Protección de Datos, así como la Ley Orgánica para la Transformación Digital y Audiovisual, y finalmente la Estrategia Nacional de Ciberseguridad.

Concluye sosteniendo que la viabilidad técnica fue aclarada por los Maestros en ciberseguridad que participaron en este grupo de discusión, quienes de forma clara explican que es viable la centralización de base de datos protegidos por un sistema de ciberseguridad basada en inteligencia artificial, pero con dispositivos informáticos de respaldo que garanticen la protección de los sistemas, a más de otras políticas públicas adyacentes a la principal para que el sistema quede fortalecido.

Participante 3 (Política y Administración Pública).

Considera viable la centralización de base de datos, la cual debe ser fortalecida con otros sistemas de toda la infraestructura gubernamental, teniendo cuidado en el manejo de la información con las empresas privadas que se consideraría la parte débil del sistema.

Participante 4 (Ciberseguridad y políticas públicas).

a) Considera que la propuesta se ve muy viable por el rumbo crucial que está tomando el Ecuador en la protección de datos, no obstante, uno de los problemas en el conglomerado social ecuatoriano, es la falta de confianza en el gobierno de turno por la poca seriedad en la aplicación de políticas públicas que protegen los intereses ciudadanos.

b) Sostiene que con la aplicación de esta política pública el Estado ecuatoriano ganaría mucho más dinero, con la centralización de base de datos, ya que eliminaría todos los ***data center*** a nivel nacional, centralizándolos en uno solo.

c) Con la implementación de esta propuesta, se aplicarían métodos de seguridad informática mucho más seguros, además de que el personal que trabajaría en el sistema seria infalible, debido a su profesionalismo y la capacitación específica que recibirían para el manejo del sistema, convirtiéndola así en una infraestructura robusta.

d) Que el éxito en el tiempo de esta política pública radica en que debe seguirse financiando y fortaleciendo la centralización de base de datos, mediante el sistema de ciberseguridad basado en inteligencia artificial.

e) Concluye manifestando que la propuesta es viable y que esta garantizaría la seguridad de la información, ya que en la práctica se ha observado que cuando se dan los ataques a los sistemas informáticos, las empresas quedan inoperativas ya que sus sistemas al ser hackeadas y dañadas, no pueden seguir operando, es decir se vuelven inservibles.

Participante 5 (Ciberseguridad y políticas públicas).

a) Concuerda con el participante 4 en su calidad de especialista en ciberseguridad especialmente en lo concerniente al ahorro para el Estado en la centralización de base de datos, además que, con la implementación de esta, se reducen los puntos de fallos en el sistema, así como también se reduce el gasto en el procesamiento de esa información.

b) Montar un sistema de esta naturaleza es muy costoso, teniendo en cuenta que un gobierno lo miraría como un gasto y no como una inversión a largo plazo que protege los datos personales y empresariales, ya que esta necesita una inversión constante para mantener un adecuado control y monitoreo, pero al invertir el dinero en seguridad de la información a través de esta centralización, existe ahorro y más seguridad, tal como lo están haciendo otros países tales como Inglaterra y China.

c) Se debe tener en cuenta que la propuesta es viable debido que, el garantizar la protección de datos a través de la centralización de estos, resultaría mucho más económico que una pérdida de la información, ya que su recuperación es muy onerosa, además de que, al haber daño en el sistema, muchas de las veces ésta se vuelve irrecuperable.

d) La centralización de base de datos más bien generaría ingresos para el Estado por los diferentes negocios en línea que se manejarían, permitiéndole a la ciudadanía la seguridad de proyectos de inversión en línea que garantizaría el flujo de capitales.

La implementación de una política pública que se sustenta en una centralización de base de datos protegidas por un sistema de ciberseguridad basada en inteligencia artificial, marca un hito significativo en el fortalecimiento de la seguridad de la información tanto en entidades públicas como privadas.

Este enfoque proactivo no sólo busca salvaguardar los datos críticos, sino que también aborda de manera integral la prevención de las vulneraciones en los sistemas automatizados de información, marcando así un avance de capital importancia en la protección de la privacidad, la confidencialidad, integridad y disponibilidad de datos informáticos.

Partiendo del análisis de los resultados obtenidos del grupo de discusión, la centralización de bases de datos permite una gestión más eficiente de la información, al consolidar todos los datos que se encuentran dispersos en diferentes entidades, así como en los ***data center*** que el mismo estado tiene, reduce la complejidad operativa y facilita un control mucho más efectivo sobre los accesos y las actualizaciones de software.

Esta concentración de los datos en una sola base agiliza los procesos administrativos, así como también optimiza la respuesta ante las posibles amenazas y ataques cibernéticos, permitiendo así una supervisión mucho más rigurosa, asegurando de esta manera que cualquier actividad sospechosa pueda ser identificada y repelida de manera inmediata.

El sistema de ciberseguridad basada en inteligencia artificial añade un elemento adicional de sofisticación técnica en esta política pública, ya que la capacidad de aprendizaje y adaptación continua que mantiene la inteligencia artificial, mejora la capacidad de detección de aquellos patrones anómalos que se presentan en un sistema automatizado de información que va a ser atacado, identificando las posibles amenazas antes de que ésta se convierta en un problema significativo para el sistema, por lo que la rápida respuesta que de manera automática generan a los incidentes y la adaptación a través del aprendizaje que tiene la IA, así como aquellas nuevas amenazas cibernéticas, garantizan una defensa robusta contra los ataques sofisticados que evolucionan constantemente en el mundo digital.

El impacto de una política pública en estos términos, fortalecería la ciberseguridad, fomentaría un entorno de confianza que impulsa de uno de otra manera la innovación, así como el desarrollo tecnológico en empresas tanto del sector público como privado, lo que permitirá que puedan operar con mayor tranquilidad sabiendo de sobremanera que sus datos se encuentran protegidos de una manera sólida.

Por lo expuesto, una política pública que centralice una base de datos resguardada mediante un sistema de ciberseguridad impulsado por inteligencia artificial, representa un avance crucial para salvaguardar de manera completa la información en esta era tecnológica del Siglo XXI. Sus ventajas abarcan desde la optimización de procesos operativos, la fortificación de la estabilidad económica, hasta la promoción de la transparencia y la cooperación interinstitucional, lo que se traduce en la consolidación de un entorno sólido y confiable para la gestión de datos en todos los ámbitos de la sociedad.

El presente trabajo investigativo se sustenta en una investigación doctoral realizada en el Centro de Estudios para la calidad Educativa y la Investigación Científica de México, cuyo tema es: “Políticas Públicas para la detección y prevención de los delitos informáticos en la República del Ecuador”, cuyo doctorando es el autor de esta comunicación, no existiendo otra investigación, hasta donde el autor ha indagado, de iguales características en la academia que aborde multidisciplinariamente las Ciencias Políticas, el delito informático, la ciberseguridad y la inteligencia artificial.

## CONCLUSIONES

El Ecuador fue víctima de varios ataques informáticos en los años 2019 y 2021 que devela la inseguridad informática en los sistemas automatizados de información, así

como la vulnerabilidad a la que se encuentran expuestos los datos informáticos.

En el año 2022 la República del Ecuador formula una Estrategia Nacional de Ciberseguridad con lineamientos específicos para la seguridad en el ciberespacio basado en seis ejes coyunturales, la que tiene como finalidad de dar cumplimento al objetivo 2.3 del Pilar 2 sobre la Resiliencia Cibernética, en la que se dispone continuar desarrollando capacidades de respuesta y gestión de incidentes cibernéticos del CERT Nacional, a través del Centro de Respuesta a Incidentes Informáticos del Ecuador, la cual no da solución a los problemas de vulnerabilidad en las empresas o negocios públicas o privadas

Una política pública que centralice una base de datos resguardada mediante un sistema de ciberseguridad basado en inteligencia artificial, representa un avance crucial para salvaguardar de manera completa la información en esta era tecnológica del Siglo XXI.

Las ventajas de esta política pública abarcarían desde la optimización de procesos operativos, la fortificación de la estabilidad económica, hasta la promoción de la transparencia y la cooperación interinstitucional, lo que se traduce en la consolidación de un entorno sólido y confiable para la gestión de datos en todos los ámbitos de la sociedad.

El impacto de una política pública en estos términos, fortalecería la ciberseguridad, fomentaría un entorno de confianza que impulsa de uno de otra manera la innovación, así como el desarrollo tecnológico en empresas tanto del sector público como privado, lo que permitirá que puedan operar con mayor tranquilidad sabiendo de sobremanera que sus datos se encuentran protegidos de una manera sólida.

## *REFERENCIAS BIBLIOGRÁFICAS*


Aboso, G., & Bidasolo, M. (2017). ***Derecho penal cibernético: la cibercriminalidad y el Derecho Penal en la moderna sociedad de la información y la tecnología de la comunicación***. Euros Editores.

ARCOTEL. (18 de Febrero de 2015). ***Agencia de Regulación y Control de las Telecomunicaciones. Obtenido de Agencia de Regulación y Control de las Telecomunicaciones.*** https://www.ecucert.gob.ec/centro-de-respuesta-a-incidentes-informaticos-del-ecuador/#

Ardila, J., Salcedo, F., Pedraza, C., & Saavedra, M. (2020). Revisión sobre hacking ético y su relación con la inteligencia artificial. ***Reto, 8***(1), 11-21. https://revistas.sena.edu.co/index.php/RETO/article/view/3064/4118

Asamblea Nacional Constituyente del Ecuador. (2008, 20 de octubre). ***Constitución de la República del Ecuador***. Registro Oficial N. 449. https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

Asamblea Nacional del Ecuador. (2014, 10 de febrero). ***Código Orgánico Integral Penal***. Registro Oficial Suplemento N. 180. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Asamblea Nacional del Ecuador. (2021, 26 de mayo). ***Ley Orgánica de Protección de Datos Personales***. Registro Oficial Suplemento N. 459. https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Ayerbe, A. (10 de Noviembre de 2020). ***La ciberseguridad y su relación con la inteligencia artificial***. Real Instituto Elcano (ARI). https://www.realinstitutoelcano.org/analisis/la-ciberseguridad-y-su-relacion-con-la-inteligencia-artificial/

Centro de innovación y soluciones empresariales y tecnológicas. (28 de Mayo de 2020). ***Centro de innovación y soluciones empresariales y tecnológicas***. Obtenido de CISET: https://www.ciset.es/publicaciones/blog/746-hardening

Congreso Nacional del Ecuador. (2004, 18 de mayo). ***Ley Orgánica de Transparencia y Acceso a la Información Pública***. Registro Oficial N. 337. https://www.educacionsuperior.gob.ec/wp-content/uploads/downloads/2014/09/LOTAIP.pdf

Costas, J. (2011). ***Seguridad y alta disponibilidad***. Editorial RA-MA.

Desongles, J., & Moya, M. (2006). ***Conocimientos Básicos de la Informática***. Marcial Editorial MAD.

García, J. (2004). Un nuevo marco de análisis para los bienes públicos: la Teoría de los Bienes Públicos Globales. ***Estudios de economía aplicada, 22***(2), 187-212. https://www.redalyc.org/pdf/301/30122203.pdf

López, D. (2021). Las políticas públicas como garantía de los derechos fundamentales. ***Sociedad & Tecnología, 4***(S1), 44-60. https://institutojubones.edu.ec/ojs/index.php/societec/article/view/113/311

Medina-Quintero, J. M., Ábrego-Almazán, D., & Echeverría-Ríos, O. (2021). Satisfacción, facilidad de uso y confianza del ciudadano en el gobierno electrónico. ***Investigación administrativa, 50***(127), 23-41. https://www.redalyc.org/articulo.oa?id=456065109004

Mena, A., & Méndez, J. (2019). La técnica de grupo de discusión en la investigación cualitativa. Aportaciones para el análisis de los procesos de interacción. ***Revista Iberoamericana de Educación, 49***(3). 1-7. https://rieoei.org/RIE/article/view/2094

Ministerio de Interior del Ecuador. (04 de feb de 2019). *Plan Específico de Seguridad Pública y Ciudadana 2019-2030*. Ministerio de Defensa del Ecuador: https://www.defensa.gob.ec/wp-content/uploads/downloads/2019/07/plan-nacional-min-interior-web.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022). *Estrategia Nacional de Ciberseguridad del Ecuador*. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2022/10/Difusion-ENC.pdf

Ojeda-Pérez, J. E., Rincón-Rodríguez, F., Arias-Flórez, M. E., & Daza-Martínez, L. A. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos de Contabilidad, 11*(28), 41-66. http://www.scielo.org.co/pdf/cuco/v11n28/v11n28a03.pdf

Organización de las Naciones Unidas ONU. (2002). *Informe sobre Derecho Humano en Venezuela 2002*. Las Tecnologías de la Información y Comunicación al servicio del desarrollo. https://hdr.undp.org/system/files/documents/venezuela2002es.pdf

Organización de los Estados Americanos OEA. (18 de Diciembre de 2022). *Guía de Mecanismos para la Promoción de la Transparencia y la Integridad en las Américas* https://www.oas.org/es/sap/dgpe/guia_egov.asp

Pérez, J. (2021). Cibercriminalidad: hacia la nueva realidad-virtual-del derecho penal. *Revista Internacional de Doctrina y Jurisprudencia*, (26), 175-193. https://ojs.ual.es/ojs/index.php/RIDJ/article/view/7063/5890

Rodríguez Llerena, A. E. (2020). Herramientas fundamentales para el hacking ético. *Revista Cubana de Informática Médica*, *12*(1), 116-131. Epub 01 de junio de 2020. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1684-18592020000100116&lng=es&tlng=es.

Santillán, A. (2023). *Derecho informático. Un estudio comparado*. Corporación de Estudios y Publicaciones. https://biblioteca.bne.gob.ec/cgi-bin/koha/opac-ISBDdetail.pl?biblionumber=59674

Suarez, A. (2017). *Manual de delito informático en Colombia.Análisis dogmático de la Ley 1273 de 2009*. U. Externado de Colombia. https://books.google.es/books?hl=es&lr=&id=MXE-DgAAQBAJ&oi=fnd&pg=PA13&dq=Suarez,+A.+(2016).+Manual+de+delito+informe%C3%A1tico+en+Colombia.+An%C3%A1lisis+dogm%C3%A1tico+de+la+ley+1273+de+2009,.+Bogot%C3%A1:+Universidad+Externado+de+Colombia&ots=54TABGhyMW&sig=rKsL5qD6srFHvuAq5euoqli2Fng#v=onepage&q&f=false

Torres, J. (2013). *Introducción a las políticas públicas*. Bogotá. https://biblioteca.inci.gov.co/handle/inci/19106