

UNIVERSIDAD CATÓLICA DE CUENCA



Maestría en Ciberseguridad

**Informe de Investigación previo a la obtención del título de Magíster en
Ciberseguridad**

Tema: Estudio Exploratorio de la Ciberseguridad en Ecuador: Hacia la
construcción de un modelo de madurez

Autor: Ing. Fernanda Michaelle Narváez Ochoa.

Asesores: Ing. Cristhian Humberto Flores Urgilés. Mg
Ing. Juan Carlos Ortega Castro. Mg

Cuenca, 2025

Certificación de Asesores

Se certifica que:

El informe de investigación “Estudio exploratorio de la Ciberseguridad en Ecuador: Hacia la construcción de un modelo de madurez”, de autoría de la Señorita Ingeniera de Sistemas de Información: Fernanda Michaelle Narváez Ochoa, CC: 0302358601, ecuatoriana, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Ciberseguridad, cumple con la caracterización y estructura (parte protocolaria y parte expositiva) y se sujeta a la normativa pertinente exigida por el Consejo de Educación Superior, CES y la Universidad Católica de Cuenca, en consecuencia se autoriza su presentación para los trámites pertinentes.

Santa Ana de los Cuatro Ríos de Cuenca

Enero, 2025.

Ing. Diego Cordero Guzmán. PhD
Asesor Científico

Ing. Juan Carlos Ortega Castro. Mg
Asesor Metodológico

Certificación de Autoría

Certifico que:

“Estudio exploratorio de la Ciberseguridad en Ecuador: Hacia la construcción de un modelo de madurez”, es el tema del informe final de investigación de mi AUTORÍA, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Ciberseguridad, por lo que, asumo su originalidad y el uso de fuentes de terceros registrados según las normas APA vigentes.

Santa Ana de los Cuatro Ríos de Cuenca

Enero, 2025.

Ing. Fernanda Michaelle Narváez Ochoa

CC: 0302358601

Agradecimiento

Agradezco a Dios por iluminar cada paso de mi vida y brindarme salud, sabiduría y determinación para cumplir con cada una de mis metas

A mi tutor de tesis, por su invaluable guía y paciencia durante todo este proceso. Su experiencia y conocimientos han sido fundamentales para la culminación de este trabajo.

A todos los docentes de la Universidad Católica de Cuenca, quienes a través de sus enseñanzas y motivación han contribuido significativamente a mi formación profesional.

A mis padres, quienes con su sacrificio y amor me han inspirado a dar siempre lo mejor de mí; a mi hermano quien es uno de mis pilares fundamentales para salir adelante.

Finalmente, agradezco a todas las personas que directa o indirectamente, contribuyeron al desarrollo de esta investigación, con todo su apoyo me han ayudado a alcanzar mis objetivos.

Dedicatoria

A Dios, por ser mi guía y fuente de fortaleza, por iluminar mi camino y permitir que cada día esté lleno de oportunidades para aprender y crecer.

A mi familia, quienes con su amor incondicional, apoyo constante y palabras de aliento, me han dado la motivación necesaria para alcanzar este logro. A mis padres Klever y Bélgica, por enseñarme el valor del esfuerzo y la perseverancia; a mi hermano Jesús Eduardo, por brindarme siempre su confianza y estar para mí en todo momento.

A mi querido abuelo, mi ángel, quién me dejó como herencia sus más preciados valores. Su recuerdo siempre vivirá en mi corazón y me acompaña en cada paso que doy.

A todas las personas que siempre me han motivado, apoyado y creído en mí para no rendirme y luchar siempre por lo que quiero. Gracias por sus palabras y consejos. Gracias por ser parte de este logro.

Resumen

El trabajo de investigación actual examina la situación actual de la seguridad cibernética en Ecuador desde una perspectiva centrada en las Tecnologías de la Información y la Comunicación (TIC). Usando un enfoque descriptivo se ha recopilado información de diversas fuentes oficiales y académicas para evaluar aspectos clave como las políticas públicas en el campo de la tecnología y las principales amenazas existentes. Se ha determinado que Ecuador ha experimentado avances significativos en la implementación de marcos legales y estrategias nacionales para fortalecer su seguridad cibernética; un claro ejemplo de ello es la promulgación de leyes como la Ley Orgánica de Protección de Datos Personales y el establecimiento del Centro Nacional de Respuesta a Incidentes Informáticos (ECU-CERT). A pesar de ello se encontraron obstáculos importantes como la falta de conexión en áreas rurales, la escasez de profesionales especializados y el aumento de los ataques cibernéticos dirigidos a infraestructuras críticas. El análisis de la situación resaltó que áreas como energía, comunicaciones y transporte exhiben vulnerabilidades importantes, agravadas por la dependencia tecnológica y la falta de inversión en medidas de seguridad informática. Para mejorar la resiliencia digital del país se consideran fundamentales el fortalecimiento de la infraestructura tecnológica, la cooperación internacional y el desarrollo del talento humano. Este informe deja un fundamento para futuras acciones estratégicas orientadas a salvaguardar los activos críticos de Ecuador ante las amenazas del entorno digital mundial.

Palabras claves: Ciberseguridad, Infraestructuras Críticas, Amenazas Cibernéticas.

Abstract

The current research work examines the current situation of cybersecurity in Ecuador from a perspective focused on Information and Communication Technologies (ICT). A descriptive approach has collected information from various official and academic sources to evaluate key aspects such as public policies in the field of technology and the main existing threats. It has been determined that Ecuador has experienced significant progress in the implementation of legal frameworks and national strategies to strengthen its cybersecurity; A clear example of this is the enactment of laws such as the Organic Law on the Protection of Personal Data and the establishment of the National Computer Incident Response Center (ECU-CERT). Despite this, important obstacles were found such as the lack of connection in rural areas, the shortage of specialized professionals and the increase in cyber-attacks directed at critical infrastructures. The analysis of the situation highlighted that areas such as energy, communications and transportation exhibit significant vulnerabilities, aggravated by technological dependence and lack of investment in computer security measures. To improve the country's digital resilience, strengthening technological infrastructure, international cooperation and the development of human talent are considered essential. This report provides a foundation for future strategic actions aimed at saving Ecuador's critical assets in the face of threats from the global digital environment.

Keywords: Cybersecurity, Critical Infrastructures, Cyber Threats.

Índice de contenidos

Capítulo I. Introducción	11
1.1. Situación problemática.....	11
1.2. Objetivos.....	12
1.2.1. Objetivo General	12
1.2.2. Objetivos Específicos	12
1.3. Estado del arte	13
1.4. Fundamentación teórica.....	14
1.4.1. Ciberseguridad.....	14
1.4.2. Ciberseguridad en países.....	15
1.4.3. Infraestructura crítica de ciberseguridad.....	15
1.4.4. Amenazas cibernéticas.....	16
1.4.5. Políticas públicas y legislación en el ámbito de las TIC.....	16
1.4.6. Modelos de Madurez en ciberseguridad	17
Capítulo II. Diagnóstico situacional	18
2.1 Metodología	18
2.1.1. Diseño de la investigación.....	18
2.1.2. Método de investigación	18
2.1.3. Fuentes de información	18
2.1.4. Procedimientos	18
2.1.5. Alcances y Limitaciones.....	19
2.2 Análisis situacional.....	19
2.2.1. Estado Actual de la Infraestructura de TIC en Ecuador	19
2.2.1.1. Redes de Telecomunicaciones	19
2.2.1.2. Centros de Datos y Servicios en la Nube.....	20
2.2.2. Economía digital en Ecuador y su relación con la Ciberseguridad	21
2.2.3. Indicadores Clave de la Economía Digital en Ecuador	21
2.2.3.1. Penetración de Internet y Telefonía Móvil:	21
2.2.3.2. Índice de Preparación para la Red (NRI) y Gobierno Electrónico (EGDI):	21
2.2.3.3. Índices de Innovación y Desarrollo de las TIC:	23

2.2.3.4. Servicios en Línea y Comercio Electrónico:	23
2.2.4. Políticas y Estrategias de Ciberseguridad en Ecuador	24
2.2.4.1. Marco Regulatorio y Políticas Gubernamentales	24
2.2.4.2. Conexión con las Instituciones Clave:	25
2.2.5 Brechas y Amenazas de Ciberseguridad.....	26
2.2.6. Evaluación de Capacidades Nacionales	28
2.2.6.1. Colaboración Internacional	28
2.2.6.2. Capacidades Gubernamentales.....	29
2.2.6.3. Capacitación en Ciberseguridad en el Sector Público y Privado.....	29
2.3 Análisis comparativo	30
2.3.1. Penetración de internet.....	30
2.3.2. Índice de Ciberseguridad Global (GCI).....	31
2.3.3. Índice de Desarrollo de las TIC (IDI).....	32
2.3.4. Índice de Preparación para la Red (NRI)	33
2.3.5. Índice de Desarrollo del Gobierno Electrónico (EGDI)	36
Capítulo III. Resultados	37
Análisis DAFO de la Seguridad Cibernética en Ecuador.....	37
Fortalezas.....	37
Oportunidades.....	38
Debilidades.....	38
Amenazas	39
Resumen de los resultados del Análisis FODA.....	40
Conclusiones	41
Recomendaciones	42
Referencias.....	43

Índice de figuras

Ilustración 1. NRI Ecuador. Fuente: Autoría Propia	22
Ilustración 2. EGDI Ecuador 2024.....	¡Error! Marcador no definido.
Ilustración 3. Índice de Penetración de Internet 2024. Fuente: Autoría Propia.....	31
Ilustración 4. IDI 2024. Fuente: Autoría Propia.....	33
Ilustración 5. Análisis Comparativo NRI Ecuador. Fuente: Autoría Propia.	33

Capítulo I. Introducción

En el contexto de una acelerada transformación digital, las Tecnologías de la Información y la Comunicación (TIC) se han convertido en un eje fundamental para el desarrollo económico, social y cultural de las naciones.

Sin embargo, surge junto a las oportunidades que brinda esta digitalización, desafíos críticos relacionados con la seguridad informática, tales como la protección de información confidencial y la reducción de amenazas cibernéticas. En naciones en vías de desarrollo como Ecuador, el crecimiento de la economía digital y la extensión del uso de tecnologías de información y comunicación han generado avances notables en aspectos como la conectividad y los servicios en línea. A pesar de ello, estos progresos también han revelado vulnerabilidades significativas, poniendo de manifiesto la importancia de abordar holísticamente el tema de la seguridad informática. Ecuador se encuentra en un proceso de mayor digitalización que lo expone a amenazas informáticas cada vez más complejas como el ransomware o la pesca de datos personales junto a ataques dirigidos a infraestructuras clave. Estos riesgos resaltan la importancia de reforzar las políticas y estrategias nacionales en materia de seguridad informática dada la escasez de infraestructura tecnológica en áreas rurales y la falta de personal especializado en este campo.

El propósito de este informe es examinar la situación actual de la seguridad cibernética en Ecuador y señalar sus puntos fuertes y débiles junto a las áreas en las que se necesita mejorar las capacidades nacionales en esta materia. Este análisis es fundamental para crear un modelo de madurez en seguridad cibernética que se ajuste a los retos y necesidades específicas del país. Se empleará un enfoque cualitativo y se consultarán fuentes secundarias confiables para ofrecer una visión completa que ayude al diseño de políticas duraderas y efectivas en el ámbito de la ciberseguridad.

1.1. Situación problemática

Ecuador se encuentra en una etapa crucial de su evolución hacia la era digital al igual que otros países en vías de desarrollo. Implicando así una mayor conexión y actualización de servicios que ofrecerán beneficios palpables a la población; sin embargo también plantea retos importantes como la creciente amenaza de ataques cibernéticos que pone en riesgo la privacidad de los ciudadanos y la estabilidad de servicios esenciales y estructuras críticas. La falta de

conexión equitativa en las áreas rurales contribuye al mantenimiento de una brecha digital que restringe la disponibilidad de herramientas digitales seguras; al mismo tiempo que las estructuras esenciales como las redes eléctricas y los sistemas financieros carecen de medidas sólidas de seguridad. A pesar de los intentos como la Ley de Protección de Datos Personales y la Estrategia Nacional de Ciberseguridad existentes actualmente algunas deficiencias en su aplicación y una carencia de coordinación entre las instituciones que complica la respuesta unificada ante eventos adversos.

Además, la escasez de profesionales cualificados en el ámbito de la seguridad informática y la falta de programas educativos especializados agravan la vulnerabilidad del país tanto en el sector público como en el privado. El crecimiento de amenazas digitales como el ransomware y el phishing plantean un desafío para Ecuador al exponerlo a mayores riesgos y socavar la confianza en su entorno digital. Es vital fortalecer las defensas de seguridad informática para asegurar una evolución digital segura y acorde a normativas internacionales.

1.2. Objetivos

1.2.1. Objetivo General

Analizar el estado actual de la ciberseguridad en Ecuador en el ámbito de las Tecnologías de la Información y la Comunicación (TIC), evaluando la infraestructura crítica, las políticas públicas, la legislación vigente y las organizaciones públicas de ciberseguridad, como paso inicial hacia la construcción de un modelo de madurez.

1.2.2. Objetivos Específicos

- Identificar las principales características de la infraestructura crítica de ciberseguridad en Ecuador, destacando los avances y brechas existentes en términos de conectividad, protección y resiliencia tecnológica.
- Analizar las políticas públicas actualmente implementadas en Ecuador en lo que respecta a la ciberseguridad y evaluar su eficiencia y conformidad con los estándares globales.
- Analizar la función y las responsabilidades de las entidades gubernamentales de seguridad cibernética en Ecuador al detectar puntos fuertes y áreas de mejora en la administración de riesgos y la respuesta a incidentes en línea.

1.3. Estado del arte

Con el objetivo de como trabajo futuro diseñar un modelo de madurez en ciberseguridad que sea relevante y efectivo para el contexto ecuatoriano, es indispensable conocer las experiencias y los hallazgos de investigaciones previas. Este estado del arte se centrará en analizar estudios realizados por otros autores sobre ciberseguridad en Ecuador, con el propósito de identificar las mejores prácticas, los desafíos y las oportunidades para fortalecer la seguridad cibernética en el país.

Ron et al. (2019) en su artículo abordan la necesidad de establecer una línea base de ciberseguridad en Ecuador como fundamento para desarrollar una política nacional en este ámbito. El estudio identifica algunos problemas clave, como la falta de aplicación de políticas de seguridad de la información en organizaciones públicas y privada, escasa investigación académica en ciberseguridad, insuficientes campañas de capacitación, y una limitada gestión del ECU-CERT. Para abordar estos desafíos, se propone un plan de investigación que incluye la evaluación de la infraestructura de la información, el marco legal, la institucionalidad, la cooperación nacional e internacional, y la sensibilización y formación en ciberseguridad. Este documento es una referencia valiosa para comprender el estado actual de la ciberseguridad en Ecuador y las acciones necesarias para fortalecerla a través de una política nacional bien definida.

Por un lado, Gutierrez et al. (2020), en su estudio, analizan las vulnerabilidades más comunes en los portales web gubernamentales de Ecuador, utilizando herramientas como Acunetix para identificar fallos de seguridad. Además, presentan un análisis de las vulnerabilidades desde el año 2015 hasta el 2019, evidenciando que muchas de las instituciones estatales no habían implementado mecanismos de control para mitigar los ciberataques. Los hallazgos destacan la presencia de debilidades significativas que podrían ser explotadas por atacantes, poniendo en riesgo la integridad y confidencialidad de la información pública.

Por otro lado, Morán (2021) en su estudio, identifica el estado de la ciberseguridad en la gestión de empresas públicas ecuatorianas mediante una revisión sistemática de la literatura. La investigación aborda la creciente preocupación por los ataques a la seguridad informática y la necesidad de que las instituciones públicas diseñen soluciones para mejorar la seguridad

tecnológica, con el fin de prevenir pérdidas de recursos estatales y proteger información privada y sensible.

El documento destaca la importancia de implementar medidas de ciberseguridad en las empresas del sector público para salvaguardar sus activos digitales y garantizar la continuidad operativa. Además, resalta la necesidad de fortalecer las políticas de seguridad, capacitar al personal y adoptar tecnologías avanzadas para enfrentar las amenazas cibernéticas actuales. Este trabajo es una referencia valiosa para comprender los desafíos y el estado actual de la ciberseguridad en las empresas públicas de Ecuador, proporcionando una base para futuras investigaciones y la formulación de estrategias efectivas en este ámbito.

1.4. Fundamentación teórica

El marco teórico de este estudio tiene como objetivo establecer una base conceptual sólida que facilite la comprensión de los elementos fundamentales relacionados con la seguridad cibernética en su contexto global y su importancia en el ámbito de las infraestructuras críticas. En un mundo cada vez más digitalizado donde los sistemas tecnológicos son vitales para el funcionamiento de las sociedades modernas, la seguridad cibernética se ha convertido en una prioridad estratégica para las naciones. Esta parte estructura los puntos importantes para asegurar una lectura coherente y fluida, introduciendo primeramente el significado de la ciberseguridad, su progreso en el ámbito nacional, y su conexión inherente a la defensa de infraestructuras críticas. Entender estos elementos resulta de suma importancia para situar en contexto el presente estado de la ciberseguridad en Ecuador y delimitar de forma clara las áreas que necesitan ser reforzadas.

1.4.1. Ciberseguridad

Se puede definir a la ciberseguridad como el conjunto de estrategias, procesos y tecnologías que permiten proteger los sistemas informáticos, redes y dispositivos frente a accesos no autorizados y demás riesgos digitales. Su objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de la información, pilares esenciales para el funcionamiento seguro de las organizaciones y los gobiernos. En la actualidad, la ciberseguridad abarca diversos ámbitos, desde la protección de dispositivos en el hogar así como la protección de infraestructuras críticas, la defensa contra ciberamenazas avanzadas y la implementación de marcos regulatorios efectivos a nivel de gobierno. A medida que las amenazas cibernéticas se

vuelven más sofisticadas, la ciberseguridad no solo protege los activos digitales, sino que también asegura la confianza en la transformación digital y la estabilidad económica de las naciones (Stevenson, 2014).

1.4.2. Ciberseguridad en países

Como se mencionó anteriormente, la ciberseguridad, como disciplina, se extiende más allá de la protección de datos y sistemas individuales, abarcando sectores clave que son esenciales para el funcionamiento de una nación. Estos sectores, denominados infraestructuras críticas, incluyen áreas como energía, transporte, salud y telecomunicaciones, y su protección es vital para garantizar la continuidad de los servicios esenciales y la estabilidad social y económica (Urbanovics & Guajardo, 2022).

1.4.3. Infraestructura crítica de ciberseguridad

La infraestructura crítica de ciberseguridad se refiere a los sistemas y activos esenciales que sustentan el funcionamiento de servicios vitales en una sociedad, cuya interrupción podría afectar gravemente la seguridad pública, la salud o incluso la estabilidad económica. Estos sistemas incluyen tanto componentes físicos como virtuales, y su protección es fundamental para garantizar la continuidad operativa de sectores clave.

Según IBM, la infraestructura crítica abarca diversos sectores interconectados, tales como:

- Energía: Redes eléctricas, instalaciones de petróleo y gas natural.
- Transporte: Aeropuertos, puertos marítimos, ferrocarriles y sistemas de transporte público.
- Agua y saneamiento: Plantas de tratamiento de agua, embalses y sistemas de alcantarillado.
- Comunicaciones: Redes de telecomunicaciones y proveedores de servicios de Internet.
- Servicios financieros: Bancos, bolsas de valores y sistemas de pago.
- Salud: Hospitales, clínicas y cadenas de suministro médicas.
- Tecnología de la información: Centros de datos, software crítico y sistemas de ciberseguridad (IBM, 2024).

La interconexión de estas infraestructuras implica que una falla en un sector puede desencadenar efectos negativos en otros, amplificando el impacto de cualquier interrupción. Por ello, la ciberseguridad en estas infraestructuras es esencial para prevenir ataques cibernéticos que

puedan comprometer su funcionamiento. Las amenazas comunes incluyen ataques cibernéticos, desastres naturales, pandemias y vulnerabilidades en la cadena de suministro.

En el contexto de Ecuador, la protección de la infraestructura crítica de ciberseguridad es vital para asegurar la prestación continua de servicios esenciales y salvaguardar la estabilidad nacional. La creciente digitalización y dependencia de las TIC hacen imperativo fortalecer las medidas de ciberseguridad para enfrentar amenazas potenciales y garantizar la resiliencia de estos sistemas.

1.4.4. Amenazas cibernéticas

Las amenazas cibernéticas son acciones malintencionadas dirigidas a sistemas informáticos, redes o datos con el fin de causar daño, obtener acceso no autorizado o simplemente interrumpir servicios.

Estas amenazas pueden manifestarse de diversas formas, desde el simple envío de correos electrónicos fraudulentos (phishing) hasta ataques sofisticados que buscan explotar vulnerabilidades en sistemas operativos o aplicaciones. Los actores detrás de estos ataques pueden ser desde individuos con conocimientos básicos hasta grupos organizados con recursos significativos. Es fundamental destacar que el panorama de las amenazas cibernéticas evoluciona constantemente. Los atacantes desarrollan nuevas técnicas y herramientas con mayor frecuencia, lo que hace que la defensa contra estas amenazas sea un desafío en constante evolución. Además, la creciente dependencia de las tecnologías digitales en todos los aspectos de nuestra vida ha ampliado la superficie de ataque, haciendo que las organizaciones y los individuos sean cada vez más vulnerables (Laubshtein, 2023).

1.4.5. Políticas públicas y legislación en el ámbito de las TIC

Las políticas públicas y la legislación en el ámbito de las TIC constituyen el marco normativo que orienta y regula el desarrollo y uso de las tecnologías de la información y la comunicación. Estas normativas, al establecer reglas claras y promover la adopción de estándares, permiten garantizar un entorno digital seguro, equitativo y que fomente la innovación. Sin embargo, el dinámico y cambiante panorama tecnológico plantea desafíos constantes a la hora de adaptar las regulaciones existentes y desarrollar nuevas políticas que aborden los emergentes problemas de la ciberseguridad, la privacidad, la inteligencia artificial y otros temas que adoptan gran relevancia (Freitag & Berners-Lee, 2021).

1.4.6. Modelos de Madurez en ciberseguridad

Los modelos de madurez en el ámbito de la ciberseguridad, son un esquema que permiten determinar las distintas etapas de evolución de las capacidad de seguridad de una organización. Teniendo como objetivo principal, facilitar una guía estructurada para alcanzar un nivel óptimo de protección de los activos de información. Estos modelos suelen estar basados en estándares internacionales y mejores prácticas reconocidas por la industria.

Entre los modelos de madurez más relevantes, se encuentran el NIST Cybersecurity Framework; ISO/IEC 27001; CMMI; CMM. (Buzdugan & Capatana, Cyber Security Maturity Model for Critical Infrastructures, 2021)

La implementación exitosa de un modelo de madurez en ciberseguridad a nivel nacional requiere una adaptación minuciosa a las particularidades del contexto local. Es fundamental definir objetivos y acciones específicas que consideren el tamaño de la infraestructura crítica, el nivel de digitalización, la madurez tecnológica y las amenazas cibernéticas más prevalentes en el país (Buzdugan & Căpățână, The Trends in Cybersecurity Maturity Models, 2023).

Capítulo II. Diagnóstico situacional

2.1 Metodología

El presente estudio adopta un enfoque cualitativo-descriptivo, basado en el análisis documental de fuentes secundarias confiables. Permitiendo una comprensión integral de la ciberseguridad en Ecuador, al evaluar la infraestructura crítica, las políticas públicas, la legislación vigente y el rol de las organizaciones públicas.

2.1.1. Diseño de la investigación

Se emplea un diseño exploratorio y descriptivo, ya que el objetivo es caracterizar el estado actual de la ciberseguridad en Ecuador en el contexto de las Tecnologías de la Información y la Comunicación (TIC). Esto incluye la identificación de fortalezas, debilidades y brechas a partir de datos obtenidos de documentos oficiales y publicaciones académicas.

2.1.2. Método de investigación

El presente diagnóstico situacional, se desarrolla bajo el método descriptivo, con el fin de analizar y documentar las características actuales del entorno cibernético en el país. Recopilando, organizando y presentando información clave sobre políticas públicas, infraestructura crítica y amenazas cibernética, generando así una visión integral de la situación actual.

2.1.3. Fuentes de información

La recopilación de datos se basa en:

- **Documentos gubernamentales:** Informes del Ministerio de Telecomunicaciones, ECU-CERT, COCIBER y otras entidades clave.
- **Publicaciones académicas:** Estudios previos sobre ciberseguridad, infraestructura tecnológica y transformación digital en Ecuador.
- **Organismos internacionales:** Reportes de la OEA, UIT y otros relacionados con ciberseguridad en países en desarrollo.
- **Bases de datos públicas:** Estadísticas nacionales sobre conectividad, penetración de internet y vulnerabilidades.

2.1.4. Procedimientos

- **Revisión documental:** Identificación y selección de fuentes relevantes mediante criterios de actualidad, confiabilidad y pertinencia.

- **Análisis temático:** Clasificación de la información en categorías clave: infraestructura crítica, políticas públicas, legislación y organizaciones públicas.
- **Triangulación de datos:** Validación de hallazgos mediante la comparación de diferentes fuentes para garantizar la fiabilidad de los resultados.

2.1.5. Alcances y Limitaciones

Este diagnóstico se limita al análisis de información disponible públicamente, sin interacción directa con expertos ni levantamiento de datos primarios.

En cuanto a las limitaciones, la falta de datos actualizados y la posible ausencia de indicadores específicos pueden restringir el alcance de las conclusiones.

2.2 Análisis situacional

2.2.1. Estado Actual de la Infraestructura de TIC en Ecuador

La modernización tecnológica en Ecuador ha avanzado gracias al impulso del gobierno y las iniciativas privadas. Esta evolución ha facilitado la expansión de las redes de comunicación y la mejora tanto de los centros de datos como de los sistemas informáticos; creando así una base sólida para el desarrollo de las Tecnologías de la Información y Comunicación (TIC) en el país (Acosta, Velastegui, & Pérez, 2018). Sin embargo y pesar de estos avances notables, persistan desafíos relevantes existentes, particularmente en regiones rurales y alejadas, donde el acceso a la tecnología aún es limitado y desigual. A continuación se expondrán los temas que reflejan la progresión lógica de la infraestructura tecnológica en Ecuador. En primer lugar se analiza la infraestructura de las telecomunicaciones, base fundamental para el desarrollo digital. Después vienen los centros de datos y la nube, esenciales para procesar y almacenar información de forma eficiente. Finalmente los equipos informáticos del ámbito público son esenciales para potenciar la eficiencia en la gestión administrativa y asegurar la seguridad de los datos y la confianza de los ciudadanos.

2.2.1.1. Redes de Telecomunicaciones

La infraestructura de telecomunicaciones ha registrado mejoras notables, destacándose la expansión de la cobertura de fibra óptica y la implementación de tecnologías móviles avanzadas como 4G. Recientemente, se han llevado a cabo pruebas para la introducción de redes 5G, lo que refleja un compromiso con la innovación y el acceso a servicios más rápidos y eficientes (Telefónica, 2023) (Ministerio de Telecomunicaciones y de la Sociedad de la Información,

2023). A pesar de estos avances, la brecha digital sigue siendo un desafío significativo. En regiones rurales, la conectividad es limitada o, en algunos casos, inexistente, lo que genera disparidades en el acceso a los beneficios de las TIC, y consecuentemente compromete la seguridad y accesibilidad a los servicios digitales.

2.2.1.2. Centros de Datos y Servicios en la Nube

El crecimiento en la cantidad y calidad de los centros de datos es otro indicador del avance de las TIC en Ecuador. Tanto el sector público como el privado han invertido considerablemente en la construcción de centros de datos modernos que cumplen con estándares internacionales de seguridad y eficiencia (MINTEL, 2023). Estas infraestructuras han permitido una adopción más amplia de servicios en la nube, facilitando el almacenamiento y procesamiento de grandes volúmenes de información, y han fomentado la transformación digital de empresas e instituciones gubernamentales. No obstante, la protección de estos centros de datos y su resiliencia ante posibles ciberamenazas debe seguir siendo una prioridad.

2.2.1.3. Sistemas Informáticos en el Sector Público

El sector público ha sido un actor clave en la modernización de los sistemas informáticos del país. Se han implementado plataformas de gestión electrónica y servicios de e-gobierno que han mejorado notablemente la eficiencia y la transparencia en la prestación de servicios públicos. Ejemplos destacados incluyen sistemas para trámites ciudadanos, gestión de impuestos y acceso a información gubernamental. Estas iniciativas no solo han optimizado procesos internos, sino que también han reforzado la confianza ciudadana en las instituciones públicas. Sin embargo, uno de los desafíos más relevantes es que no existe un Sistema Nacional de Información integrado, aunque se ha creado el Sistema Nacional de Registro de Datos Públicos (SINARDAP), que integra la información de varios organismos que procesan información pública. Además, otros sistemas como el Sistema Nacional de Información para la Planeación (SNI), el Sistema de Información para Gobiernos Autónomos Descentralizados (SIGAD), el Sistema de Gestión Documental Quipux, y el SIGEF han sido clave en la modernización (Software Ecuatoriano, 2024). Sin embargo, la integración y protección de la información pública a través de estos sistemas sigue siendo un reto, especialmente en términos de ciberseguridad, para evitar vulnerabilidades que puedan comprometer datos sensibles.

2.2.2. Economía digital en Ecuador y su relación con la Ciberseguridad

La economía digital se ha convertido en un pilar esencial para el desarrollo socioeconómico de los países, y Ecuador no es la excepción. La rápida evolución de las Tecnologías de la Información y Comunicación (TIC) ha permitido avances significativos en áreas clave como el comercio electrónico, la inclusión digital y la innovación tecnológica (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022). Sin embargo, a medida que el país avanza en la adopción digital, también surgen retos considerables en materia de ciberseguridad, que pueden afectar el desarrollo pleno de la economía digital.

2.2.3. Indicadores Clave de la Economía Digital en Ecuador

2.2.3.1. Penetración de Internet y Telefonía Móvil:

En enero del 2024, Ecuador alcanzó una penetración de internet del 83.6%, ubicándose por encima del promedio mundial del 62% (branch, 2024). Este crecimiento se debe a la expansión de la infraestructura de telecomunicaciones, la reducción de costos de acceso y la mayor concienciación sobre los beneficios del uso de internet. No obstante, el aumento de usuarios de internet incrementa las vulnerabilidades digitales, exponiendo a los usuarios a amenazas cibernéticas como phishing, fraudes electrónicos y ataques a infraestructuras críticas.

La penetración de internet móvil supera el 96%, mientras que la banda ancha fija creció un 23% entre 2021 y 2022, reflejando un avance continuo en la conectividad nacional. Sin embargo, la falta de educación en ciberseguridad en ciertas zonas puede convertir a los usuarios en blanco fácil para ataques.

2.2.3.2. Índice de Preparación para la Red (NRI) y Gobierno Electrónico (EGDI):

Ecuador ocupa el puesto 82 de 133 países en el Índice de Preparación para la Red (2024), lo que refleja avances moderados en infraestructura digital y gobernanza. Sin embargo, la falta de políticas nacionales de ciberseguridad robustas y la insuficiente inversión en capacitación digital aún limitan el progreso completo hacia una infraestructura segura.

PENETRACIÓN DE INTERNET

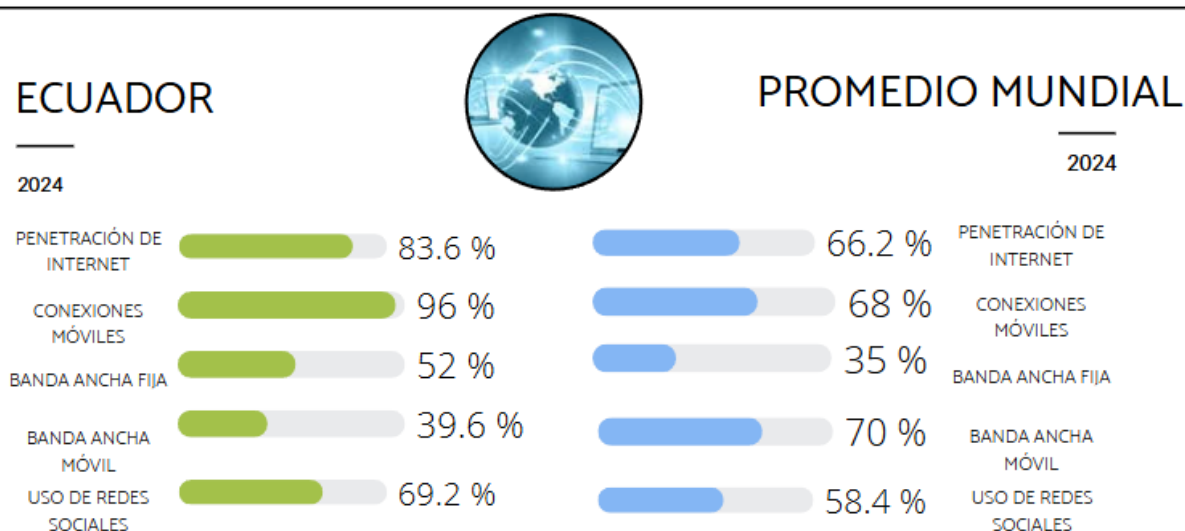


Ilustración 1. NRI Ecuador. Fuente: Autoría Propia

El Índice de Desarrollo del Gobierno Electrónico (EGDI) es una medida que evalúa el nivel de digitalización del gobierno y su capacidad para ofrecer servicios públicos a través de plataformas en línea, en este contexto Ecuador se posiciona en el puesto 67 de 193 países con una puntuación de 0.7800 (UN E-Government Knowledgebase, 2024).

Este índice se compone de tres subíndices, cada uno evaluando un aspecto clave del gobierno electrónico en Ecuador:

1. Índice de servicios en línea (0.8851): Este índice mide la disponibilidad y la calidad de los servicios públicos ofrecidos a través de plataformas digitales. Con un valor de 0.8851, Ecuador demuestra un nivel alto de accesibilidad y eficiencia en sus servicios en línea, lo que refleja el esfuerzo del gobierno por digitalizar y modernizar sus servicios públicos.
2. Índice de infraestructura de telecomunicaciones (0.6834): Este subíndice evalúa la infraestructura tecnológica que respalda la prestación de servicios en línea. Con un valor de 0.6834, Ecuador presenta una infraestructura tecnológica relativamente buena, pero aún hay áreas de mejora, especialmente en zonas rurales donde la conectividad y la calidad de los servicios podrían optimizarse para garantizar una mayor accesibilidad.

3. **Índice de capital humano (0.7715):** Este componente mide el nivel de habilidades digitales de la población y su capacidad para utilizar los servicios en línea. Con un índice de 0.7715, Ecuador muestra un nivel significativo de competencias digitales en su población, aunque hay margen para mejorar la educación y capacitación tecnológica en algunas áreas para aumentar aún más las habilidades digitales de los ciudadanos.

En resumen, los valores obtenidos en los tres subíndices reflejan un desarrollo notable en los servicios en línea, aunque aún existen desafíos en la infraestructura de telecomunicaciones, especialmente en áreas menos desarrolladas, y en el fortalecimiento de las habilidades digitales de la población.

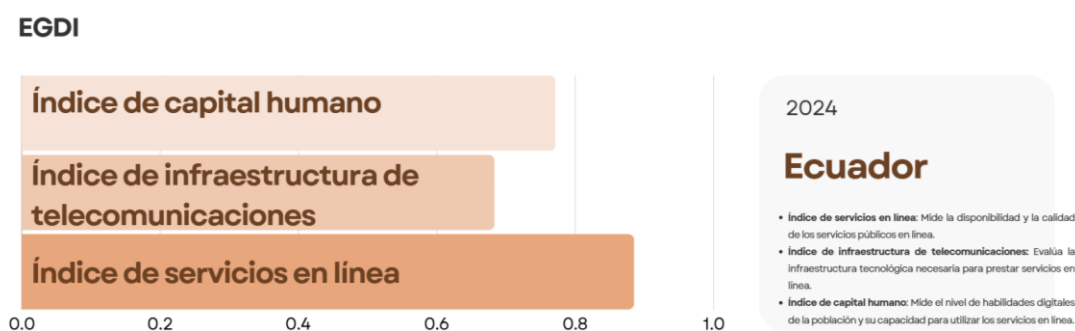


Figure 1. EGDI Ecuador 2024. Fuente: Autoría Propia

2.2.3.3. **Índices de Innovación y Desarrollo de las TIC:**

Según el Índice Global de Innovación (2022), Ecuador se encuentra en el puesto 98 de 132 países, destacándose en educación tecnológica e inversión en I+D. Sin embargo, el acceso limitado a tecnologías emergentes y las vulnerabilidades tecnológicas revelan deficiencias en las capacidades de ciberseguridad del país.

En el Índice de Desarrollo de las TIC, Ecuador ocupa el puesto 91 de 182 países, con un incremento de 0,1 puntos respecto al año anterior. Aunque ha mejorado, el país sigue por debajo de la media global en términos de acceso y calidad de las telecomunicaciones, lo que podría generar desafíos en la protección de infraestructuras críticas.

2.2.3.4. **Servicios en Línea y Comercio Electrónico:**

El Índice de Servicios en Línea (OSI) posiciona a Ecuador en el puesto 66 de 150 países, con una puntuación de 0,8118, reflejando mejoras constantes en la disponibilidad y calidad de servicios digitales.

Aunque el comercio electrónico ha crecido significativamente, enfrenta barreras como la baja alfabetización digital en ciertas regiones y la limitada confianza en las transacciones en línea. Estos desafíos están estrechamente relacionados con las vulnerabilidades de seguridad en las plataformas de pago, el fraude digital y la protección de los datos personales (Gobierno Electrónico, 2024).

2.2.4. Políticas y Estrategias de Ciberseguridad en Ecuador

El avance hacia la digitalización en Ecuador ha sido impulsado por diversas iniciativas del gobierno y el sector privado. Sin embargo, con el crecimiento de las Tecnologías de la Información y la Comunicación (TIC), también han emergido desafíos importantes en términos de ciberseguridad, lo que ha generado la necesidad de establecer políticas y estrategias robustas que protejan tanto los activos digitales como la infraestructura crítica del país.

2.2.4.1. Marco Regulatorio y Políticas Gubernamentales

Ecuador ha tomado medidas importantes para fortalecer su marco de ciberseguridad. Sin embargo, la creación y aplicación de políticas ha sido un proceso gradual, y aún existen áreas clave que requieren atención urgente. A continuación, se destacan las principales políticas y regulaciones relacionadas con la ciberseguridad en el país:

1. Agenda Digital del Ecuador (2021-2022):

- Esta agenda establece los lineamientos para la transformación digital en el país, promoviendo la expansión de la infraestructura de telecomunicaciones y la digitalización de los servicios públicos. Aunque no es un documento exclusivamente enfocado en ciberseguridad, establece los cimientos para la adopción de nuevas tecnologías y la mejora de la gobernanza digital. Sin embargo, la falta de un enfoque integral de ciberseguridad en esta agenda ha sido un reto importante en términos de protección de los datos y la infraestructura digital del país.

2. Ley Orgánica de Protección de Datos Personales (2022):

- En 2022, Ecuador aprobó la Ley Orgánica de Protección de Datos Personales, que regula el uso y manejo de los datos personales en el ámbito público y privado. Esta ley es un paso importante hacia la protección de la privacidad de los

ciudadanos, aunque su implementación aún enfrenta desafíos debido a la falta de concienciación y capacitación tanto en el sector público como en el privado. Además, la falta de infraestructuras adecuadas para el almacenamiento y la protección de estos datos en el sector público sigue siendo un reto.

3. Estrategia Nacional de Ciberseguridad:

- El Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL) ha liderado la creación de una estrategia nacional de ciberseguridad, que incluye un conjunto de medidas para proteger la infraestructura crítica del país, gestionar incidentes cibernéticos y fortalecer las capacidades nacionales en este ámbito. La estrategia aboga por una gestión integral de riesgos y el desarrollo de capacidades de respuesta y gestión de incidentes cibernéticos por parte del CERT nacional (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022). La coordinación entre el MINTEL, COCIBER y otras entidades clave como ECU-CERT es fundamental para garantizar una respuesta rápida ante ciberincidentes. No obstante, la coordinación interinstitucional aún enfrenta desafíos relacionados con la falta de recursos y la duplicación de esfuerzos.

4. Ley de Gobierno Electrónico:

- Esta ley fomenta el uso de plataformas digitales en el sector público, promoviendo la transparencia y la eficiencia en la administración pública. Sin embargo, la ciberseguridad no ha sido siempre un enfoque prioritario dentro de esta ley, lo que ha llevado a lagunas en las normativas de protección para los servicios públicos digitales. ECU-CERT, el CEDIA-CERT y otros centros de respuesta, deben jugar un papel central en asegurar que las plataformas digitales implementadas bajo esta ley estén protegidas frente a ciberataques y que las medidas de seguridad sean adecuadas.

2.2.4.2. Conexión con las Instituciones Clave:

El éxito de la implementación de estas políticas y estrategias de ciberseguridad depende en gran medida de las instituciones clave del país:

- MINTEL ha sido crucial en la formulación de políticas nacionales y en la coordinación de esfuerzos para la protección de infraestructuras críticas.
- COCIBER juega un papel destacado en la gestión de riesgos cibernéticos y la formación de capacidades en ciberseguridad.
- ECU-CERT y CEDIA-CERT son actores fundamentales en la respuesta a incidentes cibernéticos, ayudando a mitigar los impactos de los ataques cibernéticos en sectores públicos y privados.

Estas entidades deben trabajar de manera más coordinada para superar las barreras relacionadas con la falta de recursos y capacitación, y para asegurar que la ciberseguridad sea un componente integral en todas las políticas de gobernanza digital.

2.2.5 Brechas y Amenazas de Ciberseguridad

Ecuador enfrenta un panorama de ciberseguridad desafiante, marcado por significativas brechas estructurales y una creciente sofisticación de las amenazas cibernéticas. A medida que el país avanza en la digitalización de sus infraestructuras y servicios, se incrementan las vulnerabilidades, lo que subraya la necesidad urgente de fortalecer las políticas y estrategias de ciberseguridad.

Una de las principales vulnerabilidades radica en la desigualdad de acceso a la conectividad, especialmente en las áreas rurales, donde la infraestructura es insuficiente para garantizar una protección adecuada contra los ciberataques. Esta situación crea una brecha digital que no solo limita el acceso a servicios de TIC, sino que también expone a los usuarios en estas regiones a amenazas como phishing y fraudes digitales debido a la falta de alfabetización digital y educación en ciberseguridad. Además, la falta de inversión en tecnologías de seguridad digital en sectores estratégicos como la salud, la energía y el transporte deja a estos sectores vulnerables a incidentes cibernéticos que podrían afectar la infraestructura crítica del país. En particular, la infraestructura de redes aún carece de protocolos de seguridad robustos, lo que facilita la explotación de vulnerabilidades tecnológicas (Ibarra, Tapia, Tene, Toapanta, & Ormaza, 2024).

Otra brecha crítica es la falta de profesionales especializados en ciberseguridad. La escasez de programas educativos y certificaciones en ciberseguridad ha creado un déficit de talento, lo que dificulta la implementación de estrategias de defensa efectivas y la gestión de

incidentes. Las capacidades nacionales en ciberseguridad siguen siendo limitadas, lo que pone en riesgo la protección de datos y la continuidad de los servicios digitales.

Las amenazas cibernéticas también se han intensificado, con un notable incremento en ataques de ransomware que afectan tanto a instituciones públicas como privadas, cifrando datos críticos y exigiendo rescates financieros (REGISTRO OFICIAL Órgano de la República del Ecuador, 2021). Estos ataques representan una amenaza significativa para la seguridad de los datos en sectores como la salud, donde el acceso a información sensible puede ser restringido o manipulado. La protección de datos personales y la privacidad son áreas que requieren atención urgente, especialmente con la implementación de la Ley de Protección de Datos Personales.

Los ataques de phishing son otra amenaza recurrente, aprovechándose de la falta de educación digital en gran parte de la población para obtener información confidencial a través de engaños. La alfabetización digital sigue siendo insuficiente en muchos sectores, lo que hace que los ciudadanos y empleados sean más susceptibles a caer en estos tipos de fraude. Este fenómeno no solo afecta a los individuos, sino también a las instituciones que gestionan información sensible.

Adicionalmente, los ciberataques dirigidos a infraestructuras críticas, como las redes eléctricas y el sector financiero, han demostrado la vulnerabilidad de estos sistemas esenciales. Un ataque a la infraestructura energética o financiera podría tener un impacto devastador en la estabilidad económica y social del país, afectando tanto a la ciudadanía como a la economía en general.

La propagación de malware y el aumento de ataques a dispositivos móviles añaden complejidad al panorama de ciberseguridad en Ecuador. Estos ataques ponen en riesgo tanto a individuos como a organizaciones al exponerlos a riesgos de pérdida de datos, interrupciones operativas y compromisos de privacidad (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022) (ARCOTEL-EcuCERT, 2023). La creciente dependencia de dispositivos móviles en el día a día ha creado un vector de ataque adicional que necesita ser gestionado adecuadamente.

Estas brechas y amenazas subrayan la urgente necesidad de fortalecer la infraestructura de ciberseguridad del país (Córdova, 2024).. Para mitigar estos riesgos, es necesario invertir en formación especializada, mejorar las capacidades de respuesta ante incidentes y fomentar la

cooperación internacional. Las iniciativas de entidades como MINTEL, COCIBER, ECU-CERT y CEDIA-CERT son pasos en la dirección correcta, pero se requiere una acción más coordinada y un marco regulatorio más robusto que aborde las vulnerabilidades existentes y responda a las amenazas emergentes.

La creación de un centro nacional de ciberseguridad y la implementación de políticas públicas más agresivas son esenciales para garantizar un entorno digital resiliente y seguro. La educación en ciberseguridad debe ser una prioridad, no solo en el ámbito académico, sino también en el sector privado y público, para fortalecer la capacidad de los ciudadanos y las organizaciones frente a las amenazas digitales.

2.2.6. Evaluación de Capacidades Nacionales

Ecuador ha dado pasos importantes hacia el fortalecimiento de su ciberseguridad, pero aún enfrenta desafíos significativos en términos de capacidades nacionales para enfrentar las amenazas cibernéticas. A continuación, se evaluarán las principales capacidades existentes en el país, incluyendo la colaboración internacional, las capacidades gubernamentales y la capacitación en ciberseguridad en los sectores público y privado.

2.2.6.1. Colaboración Internacional

En el ámbito de la ciberseguridad, la colaboración internacional es fundamental para enfrentar amenazas transnacionales y obtener acceso a recursos y conocimientos especializados. Ecuador ha logrado establecer acuerdos de cooperación con diversos organismos internacionales, como la Organización de Estados Americanos (OEA), la Interpol y la Unión Internacional de Telecomunicaciones (UIT). Estas alianzas permiten a Ecuador participar en programas internacionales que fomentan el intercambio de información sobre ciberamenazas y mejoran la capacidad del país para responder a incidentes cibernéticos.

A través de la cooperación bilateral y multilateral, Ecuador también ha accedido a capacitación y asistencia técnica para mejorar sus capacidades en defensa cibernética, protección de infraestructuras críticas y gestión de incidentes cibernéticos. Sin embargo, para maximizar los beneficios de estas relaciones internacionales, es esencial que Ecuador continúe reforzando su infraestructura tecnológica y se mantenga actualizado sobre las mejores prácticas globales en ciberseguridad.

2.2.6.2. Capacidades Gubernamentales

El gobierno ecuatoriano ha dado pasos clave para establecer una estrategia nacional de ciberseguridad, liderada por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL). Esta estrategia incluye medidas para proteger la infraestructura crítica del país, gestionar incidentes cibernéticos y fomentar una cultura de ciberseguridad en todas las instituciones del sector público. Además, el país ha creado diversas entidades, como el COCIBER (Comité de Ciberseguridad), encargado de coordinar los esfuerzos nacionales en el ámbito de la ciberseguridad.

Sin embargo, existen desafíos relacionados con la coordinación interinstitucional y la asignación de recursos adecuados para implementar las políticas de ciberseguridad de manera efectiva. Muchas de las instituciones gubernamentales aún carecen de personal especializado en ciberseguridad, lo que limita su capacidad para gestionar incidentes de manera eficiente. Además, la falta de infraestructura adecuada en ciertas regiones del país y la falta de integración entre los sistemas de ciberseguridad a nivel nacional dificultan la implementación de medidas de seguridad uniformes.

2.2.6.3. Capacitación en Ciberseguridad en el Sector Público y Privado

Uno de los mayores desafíos que enfrenta Ecuador es la falta de profesionales capacitados en ciberseguridad. Si bien el país ha hecho esfuerzos para fomentar la educación y capacitación en este campo, la oferta educativa sigue siendo limitada, especialmente en zonas rurales y en sectores no tecnológicos. Esta falta de talento especializado repercute directamente en la capacidad de las organizaciones públicas y privadas para defenderse de los ataques cibernéticos.

A nivel público, el gobierno ha implementado algunos programas de capacitación en ciberseguridad para empleados gubernamentales, pero estos son insuficientes y no siempre se actualizan de acuerdo con las amenazas emergentes. La formación en gestión de incidentes cibernéticos y protección de datos debe ser una prioridad dentro de la administración pública.

En el sector privado, la ciberseguridad sigue siendo un área poco comprendida por muchas pequeñas y medianas empresas, que carecen de los recursos para invertir en formación especializada o en la implementación de sistemas de protección avanzados. Aunque algunas

empresas grandes han adoptado medidas de seguridad, muchas aún operan bajo estándares de seguridad desactualizados o insuficientes para enfrentar el panorama actual de amenazas.

Para mejorar esta situación, es crucial implementar programas de formación continua en ciberseguridad, tanto en el sector público como privado, y promover la colaboración con instituciones educativas para fomentar el desarrollo de nuevas generaciones de profesionales especializados en ciberseguridad.

Recomendaciones para Mejorar las Capacidades Nacionales

- Fortalecer la cooperación internacional mediante acuerdos más profundos con países y organizaciones internacionales, lo que permitiría a Ecuador acceder a recursos adicionales y mejorar su capacidad de respuesta ante amenazas cibernéticas globales.
- Invertir en la capacitación y formación especializada en ciberseguridad, con programas dirigidos tanto a funcionarios públicos como a empleados del sector privado, para garantizar que el país cuente con personal capacitado para enfrentar los desafíos de ciberseguridad.
- Fortalecer las capacidades del gobierno mediante una mayor coordinación entre instituciones y una asignación adecuada de recursos para la implementación efectiva de la Estrategia Nacional de Ciberseguridad.
- Fomentar la inversión en infraestructura de ciberseguridad, tanto en el sector público como privado, para garantizar que Ecuador esté preparado para defenderse de las amenazas cibernéticas más sofisticadas.

2.3 Análisis comparativo

En este apartado, se comparan los indicadores de ciberseguridad de Ecuador con otros países de la región y del mundo en desarrollo. Los indicadores analizados incluyen la penetración de internet, el Índice de Ciberseguridad Global (GCI), el Índice de Desarrollo de las TIC (IDI), y el Índice de Preparación para la Red (NRI). Este análisis permite identificar áreas donde Ecuador muestra fortalezas y aquellas donde se requiere mayor intervención.

2.3.1. Penetración de internet

- Ecuador: 83.6% (2024)
- Promedio mundial: 62%

- Países comparados: Colombia (86%), Perú (78%), México (74%)

Análisis:

Ecuador tiene una penetración de internet superior al promedio mundial y comparable con Colombia, pero enfrenta desafíos en la conectividad rural, donde aún hay importantes brechas digitales.

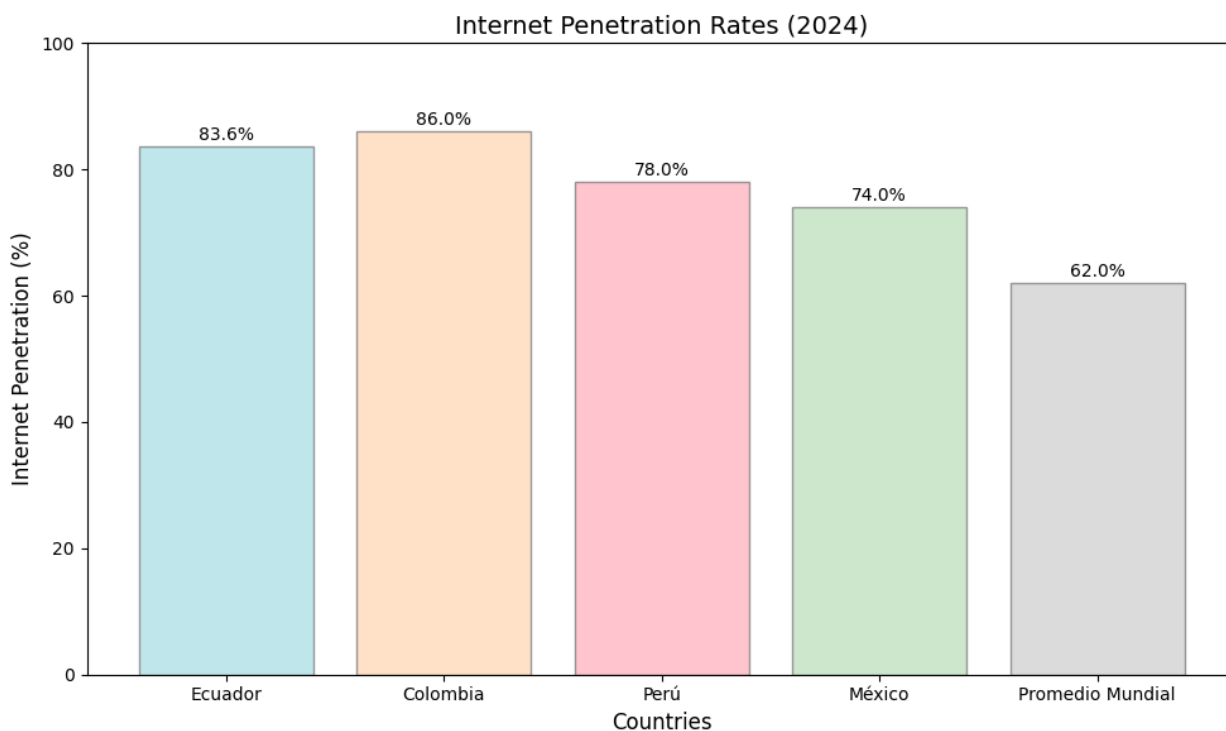
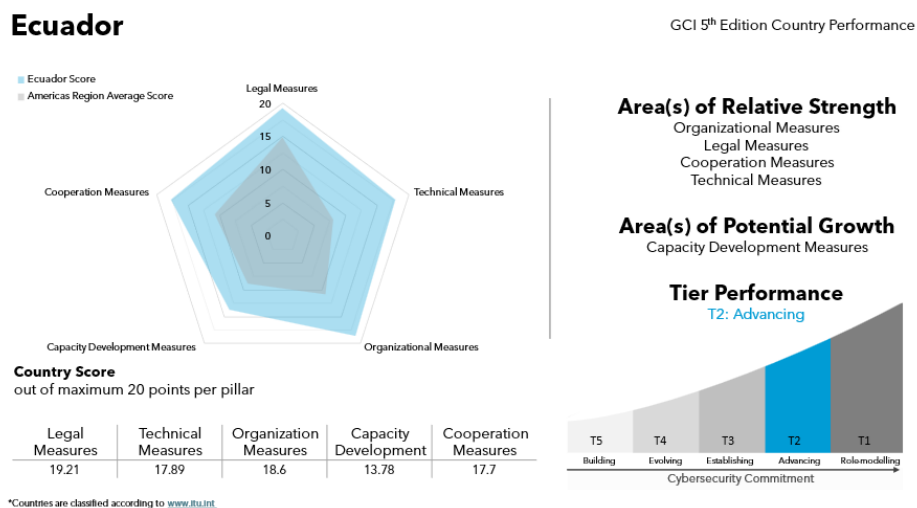


Ilustración 2. Índice de Penetración de Internet 2024. Fuente: Autoría Propia.

2.3.2. Índice de Ciberseguridad Global (GCI)

El Índice Global de Ciberseguridad (GCI), en América se clasifica en cinco niveles de desempeño en ciberseguridad: **T1 (Role-Modelling)**, **T2 (Advancing)**, **T3 (Establishing)**, **T4 (Evolving)** y **T5 (Building)**. Ecuador se encuentra en el nivel **T2 (Advancing)**, junto con Canadá, México y Uruguay, lo que refleja avances significativos en el desarrollo de medidas de ciberseguridad, aunque aún existen áreas por fortalecer, como el desarrollo de capacidades. Este nivel indica que Ecuador ha superado a varios países de la región que se encuentran en **T3 (Establishing)**, como Colombia, Chile y Costa Rica, que están en proceso de establecer compromisos sólidos. Sin embargo, Ecuador todavía no alcanza el nivel **T1 (Role-Modelling)**, donde se ubican Brasil y Estados Unidos, considerados referentes globales en ciberseguridad.

gracias a sus marcos sólidos, estrategias avanzadas y colaboración internacional efectiva (ITU, 2024).



2.3.3. Índice de Desarrollo de las TIC (IDI)

En el **Índice de Desarrollo de las TIC (IDI) 2024**, Ecuador obtuvo una puntuación de 68.8, lo que representa un crecimiento del 3% respecto al año anterior, posicionándose dentro del grupo de países de ingresos medios-altos (UMI) en la región de las Américas. Aunque muestra un avance significativo, Ecuador se encuentra por debajo de los líderes regionales como Chile (91.7) y Brasil (89.2), que destacan por su infraestructura tecnológica avanzada y mayor acceso a las TIC. Sin embargo, Ecuador supera a otros países de la región como Bolivia (69.4) y Colombia (73.2), reflejando un desarrollo moderado pero constante. Este desempeño evidencia la necesidad de fortalecer áreas clave, como la conectividad en zonas rurales y el uso significativo de las TIC, para cerrar la brecha con los países más avanzados de la región y aprovechar plenamente las oportunidades de la economía digital (ITU, 2024).

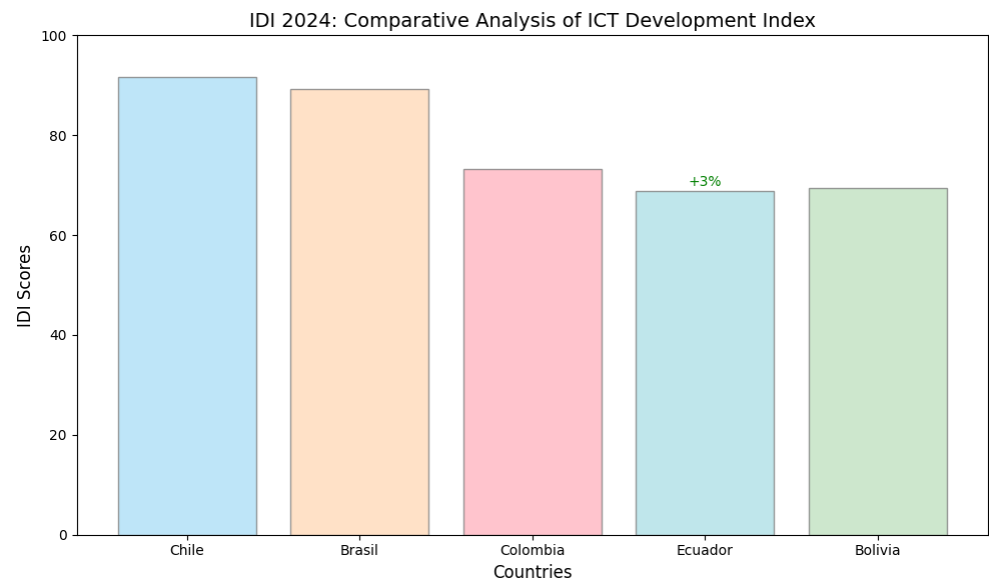


Ilustración 3. IDI 2024. Fuente: Autoría Propia

2.3.4. Índice de Preparación para la Red (NRI)

El NRI mide la preparación de los países para aprovechar las oportunidades de la economía digital, evaluando cuatro pilares: Tecnología, Personas, Gobernanza e Impacto. A continuación, se compara el desempeño de Ecuador, Colombia, Perú y Chile.

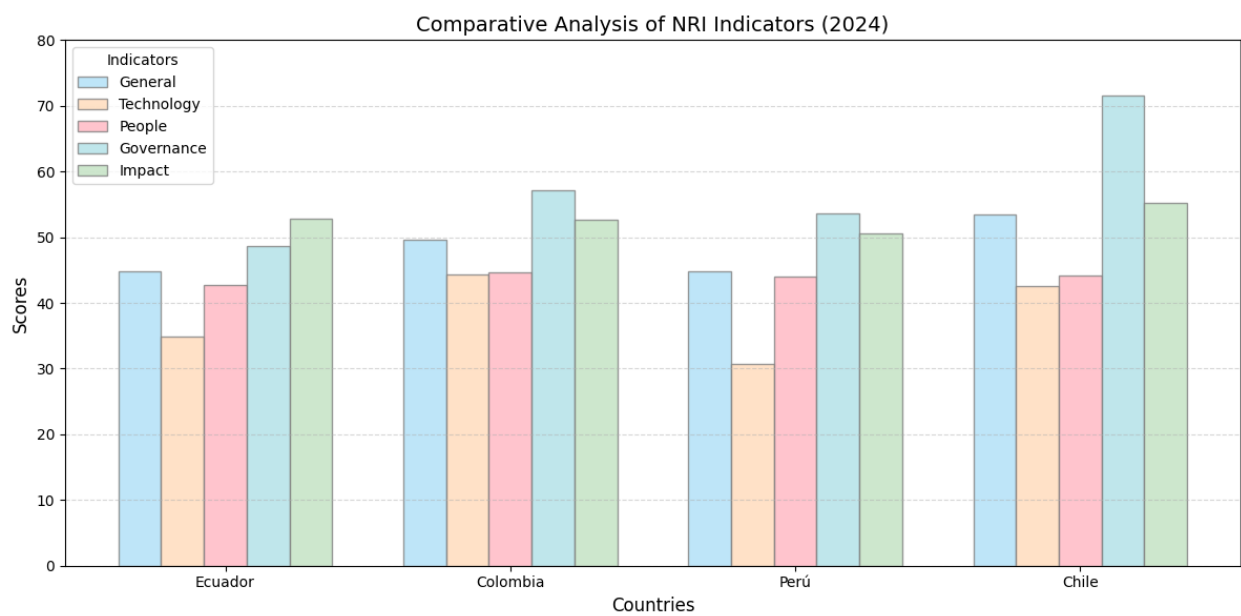


Ilustración 4. Análisis Comparativo NRI Ecuador. Fuente: Autoría Propia.

1. Puntaje y ranking general

- Ecuador: Rank 82/133, puntaje 44.76.
- Colombia: Rank 64/133, puntaje 49.64.
- Perú: Rank 83/133, puntaje 44.76 (igual a Ecuador, pero con un peor desempeño en subindicadores).
- Chile: Rank 54/133, puntaje 53.40.

Análisis:

Chile lidera claramente entre los países comparados, mostrando una mejor preparación para la economía digital, mientras que Ecuador y Perú se posicionan más abajo con el mismo puntaje general, aunque Ecuador tiene un rendimiento más equilibrado. Colombia supera a Ecuador y Perú, pero se encuentra detrás de Chile.

2. Pilar: Tecnología

- Ecuador: Puntaje 34.90 (Rank 89).
- Colombia: Puntaje 44.26 (Rank 60).
- Perú: Puntaje 30.75 (Rank 99).
- Chile: Puntaje 42.54 (Rank 69).

Análisis:

Colombia y Chile destacan en este pilar, especialmente en acceso y contenido. Ecuador supera a Perú, pero ambos tienen dificultades para avanzar en tecnologías futuras y en la disponibilidad de infraestructura digital robusta.

3. Pilar: Personas

- Ecuador: Puntaje 42.73 (Rank 63).
- Colombia: Puntaje 44.58 (Rank 52).
- Perú: Puntaje 44.07 (Rank 56).

- Chile: Puntaje 44.20 (Rank 54).

Análisis:

En este pilar, Colombia tiene una ligera ventaja, destacando en la adopción digital por parte de empresas y gobiernos. Ecuador se mantiene competitivo en comparación con Perú y Chile, pero necesita fortalecer la digitalización de su población.

4. Pilar: Gobernanza

- Ecuador: Puntaje 48.65 (Rank 92).
- Colombia: Puntaje 57.15 (Rank 74).
- Perú: Puntaje 53.61 (Rank 77).
- Chile: Puntaje 71.61 (Rank 36).

Análisis:

Chile es el líder indiscutible en gobernanza digital, reflejando altos niveles de confianza, regulación efectiva e inclusión digital. Colombia y Perú se ubican en un nivel intermedio, mientras que Ecuador muestra debilidades significativas en confianza y regulación.

5. Pilar: Impacto

- Ecuador: Puntaje 52.76 (Rank 75).
- Colombia: Puntaje 52.58 (Rank 76).
- Perú: Puntaje 50.62 (Rank 87).
- Chile: Puntaje 55.25 (Rank 61).

Análisis:

Chile nuevamente lidera en impacto, impulsado por una mejor calidad de vida digital y contribución a los ODS (Objetivos de Desarrollo Sostenible). Ecuador tiene un desempeño más fuerte en este pilar en comparación con Colombia y Perú, reflejando una contribución moderada al bienestar digital y la economía.

De esta forma, se concluye que Chile es el país mejor posicionado en los cuatro pilares del NRI, con avances significativos en gobernanza y tecnología. Colombia le sigue, destacándose en personas y tecnología. Ecuador y Perú están más rezagados, con puntajes similares, pero Ecuador tiene un desempeño más equilibrado entre los pilares. Para mejorar su competitividad, Ecuador debe priorizar inversiones en infraestructura tecnológica, mejorar la regulación en gobernanza y fomentar la adopción digital tanto en el ámbito gubernamental como empresarial (Dutta & Lanvin, 2024).

2.3.5. Índice de Desarrollo del Gobierno Electrónico (EGDI)

- Ecuador: Puesto 67/193 países (2024), puntuación: 0.78
- Países comparados:
 - Colombia: Puesto 68, puntuación 0.77
 - Chile: Puesto 31, puntuación: 0.88
 - México: Puesto 65, puntuación: 0.78

Análisis:

Ecuador ha avanzado en la oferta de servicios en línea, pero aún tiene áreas de mejora, como la integración de sistemas nacionales y la seguridad de sus plataformas digitales.

Basado en el análisis comparativo anteriormente, se puede determinar que Ecuador ha mostrado avances significativos en la penetración de internet y el desarrollo de servicios de gobierno electrónico, pero enfrenta desafíos en infraestructura tecnológica, políticas de ciberseguridad, y desarrollo de habilidades digitales. Comparado con países como Colombia y Chile, Ecuador necesita reforzar su estrategia nacional de ciberseguridad y aumentar la inversión en capacitación, innovación y sobre todo tecnología.

Capítulo III. Resultados

Análisis DAFO de la Seguridad Cibernética en Ecuador

El análisis de los hallazgos sobre la ciberseguridad en Ecuador se sintetiza en el marco FODA (Fortalezas, Oportunidades, Debilidades y Amenazas). Este análisis permite comprender el estado actual y las perspectivas futuras en el ámbito de la ciberseguridad, proporcionando una base sólida para recomendaciones estratégicas.

Fortalezas

1. Marcos legales actualizados

La promulgación de la Ley Orgánica de Protección de Datos Personales y otros instrumentos regulatorios ha establecido un marco normativo que fortalece la ciberseguridad en Ecuador. Esto brinda confianza a los usuarios sobre la protección de sus datos y fomenta la adopción de tecnologías digitales, posicionando al país en un nivel competitivo dentro de la región.

2. Presencia de instituciones relevantes

Organismos como el ECU-CERT desempeñan un papel clave en la coordinación de esfuerzos de ciberseguridad. Su capacidad para responder a incidentes cibernéticos y su labor de sensibilización representan un paso significativo hacia un ecosistema digital más seguro.

3. Avances en conectividad

La expansión de la cobertura de internet, especialmente en áreas urbanas, ha permitido un mayor acceso a servicios digitales. Esto genera oportunidades para implementar estrategias de ciberseguridad en un entorno donde cada vez más personas están conectadas.

4. Estrategias nacionales

La Estrategia Nacional de Ciberseguridad proporciona un marco para coordinar acciones entre el sector público, privado y académico. Este enfoque integrado es clave para abordar las crecientes amenazas cibernéticas.

Oportunidades

1. Interés gubernamental en la digitalización

La digitalización priorizada por el gobierno representa una oportunidad para incorporar medidas de ciberseguridad desde la planificación de nuevos proyectos tecnológicos, garantizando que sean seguros desde su diseño.

2. Acceso a cooperación internacional

Ecuador puede fortalecer su capacidad cibernética mediante alianzas con organismos como la Unión Internacional de Telecomunicaciones (ITU) y la OEA, accediendo a recursos técnicos, programas de capacitación y mejores prácticas internacionales.

3. Desarrollo de talento especializado

La creciente demanda de profesionales en ciberseguridad ofrece la oportunidad de crear programas educativos y certificaciones que contribuyan a formar especialistas en esta área crítica.

4. Adopción de tecnologías emergentes

Tecnologías como la inteligencia artificial y el blockchain pueden mejorar significativamente las capacidades de detección, prevención y respuesta ante amenazas cibernéticas, fortaleciendo sectores estratégicos.

Debilidades

1. Infraestructura tecnológica desigual

Aunque hay avances en conectividad, persisten brechas significativas en las zonas rurales, donde el acceso a tecnologías de la información es limitado. Esto dificulta la implementación de medidas de ciberseguridad homogéneas en todo el país.

2. Déficit de talento especializado

La falta de profesionales capacitados en ciberseguridad limita la capacidad del país para responder a amenazas avanzadas. Esto afecta tanto al sector público como al privado, dejando expuestos activos críticos.

3. Falta de confianza digital

Los usuarios aún perciben que las plataformas digitales, especialmente las gubernamentales, no son completamente seguras. Esto impacta negativamente en la adopción de servicios digitales y limita el avance de la economía digital.

4. Limitada inversión en ciberseguridad

Las prioridades presupuestarias no siempre consideran a la ciberseguridad como un área crítica. Esta limitación financiera reduce la capacidad para implementar tecnologías avanzadas y fortalecer la resiliencia cibernética.

Amenazas

1. Incremento de ciberataques sofisticados

Amenazas como el ransomware y los ataques dirigidos a infraestructuras críticas son cada vez más comunes, representando un desafío constante para las capacidades de defensa cibernética del país.

2. Dependencia tecnológica

Ecuador depende en gran medida de tecnologías y soluciones extranjeras, lo que podría generar vulnerabilidades si estas no se adaptan correctamente al contexto local o no se actualizan oportunamente.

3. Cambios regulatorios globales

La presión internacional para cumplir con estándares más estrictos de ciberseguridad puede ser difícil de manejar para un país con recursos limitados, lo que podría afectar su competitividad y seguridad.

4. Falta de concienciación

A nivel general, existe un bajo nivel de educación y sensibilización sobre la importancia de la ciberseguridad, tanto en las organizaciones como entre los ciudadanos. Esto amplía la superficie de ataque y aumenta la probabilidad de incidentes cibernéticos.

Resumen de los resultados del Análisis FODA

El análisis FODA realizado sobre la ciberseguridad en Ecuador permite identificar fortalezas significativas, como la implementación de marcos legales actualizados, entre ellos la Ley Orgánica de Protección de Datos Personales, y la creación de instituciones clave como el ECU-CERT. Estas iniciativas han proporcionado al país un punto de partida sólido para enfrentar los desafíos cibernéticos y coordinar estrategias nacionales. Además, la expansión de la conectividad en áreas urbanas y el creciente interés gubernamental en la digitalización han impulsado el desarrollo de un entorno tecnológico más robusto, aunque con limitaciones en su alcance.

No obstante, el diagnóstico también evidencia debilidades críticas que afectan la postura de ciberseguridad del país. Entre ellas, destacan la desigualdad en la infraestructura tecnológica, que deja a las zonas rurales en una posición de vulnerabilidad, y el déficit de talento especializado, que limita la capacidad de respuesta ante amenazas avanzadas. A esto se suma la percepción de inseguridad digital por parte de los usuarios, especialmente en plataformas gubernamentales, lo que afecta la confianza y adopción de servicios digitales. Estas brechas se ven agravadas por la insuficiente inversión en medidas de ciberseguridad, tanto en el sector público como en el privado.

Finalmente, las amenazas externas, como el incremento en la sofisticación de ciberataques y la dependencia tecnológica de soluciones extranjeras, representan riesgos significativos para el país. Sin embargo, el análisis también identifica oportunidades importantes, como la posibilidad de fortalecer la cooperación internacional, desarrollar talento especializado y adoptar tecnologías emergentes que mejoren la resiliencia cibernética. Este panorama plantea la necesidad de una estrategia integral que priorice las áreas críticas y aproveche las oportunidades para consolidar un entorno digital más seguro y resiliente en Ecuador.

Conclusiones

El presente informe de investigación permitió realizar un análisis exhaustivo sobre el estado actual de la ciberseguridad en Ecuador; resaltando los avances logrados y las limitaciones presentes en dicha materia en términos generales. El país ha mostrado avances notables en la implementación de marcos legales y organizativos como la aprobación de la Ley Orgánica de Protección de Datos Personales y el establecimiento del ECU-CERT. Estas acciones reflejan un compromiso crecientemente mayor hacia la protección de los activos digitales y la privacidad de los ciudadanos; situando a Ecuador en una posición intermedia dentro de la región.

Sin embargo persisten desafíos significativos en el ámbito de la infraestructura tecnológica actualmente en día. A pesar de que se han logrado avances en la conectividad en las áreas urbanas, todavía existen brechas significativas en las regiones rurales que hacen difícil implementar de manera consistente medidas eficientemente para proteger contra amenazas informáticas. Esto restringe el acceso seguro a herramientas digitales y agrava aún más las disparidades en la adopción de nuevas tecnologías. El país enfrentará dificultades para mejorar sus capacidades nacionales debido a la falta de personal calificado en ciberseguridad; esta carencia de talentos especializados se posicionará como uno de los principales desafíos a superar tanto en el ámbito público como privado debido al creciente demandante del sector.

Por otro lado, la situación de las amenazas digitales sigue empeorando, con un aumento constante en la intensidad de los ataques como el ransomware, el phishing y aquellos que apuntan hacia infraestructuras críticas. Esta situación destaca la importancia de adoptar estrategias más robustas para asegurar la resistencia ante eventuales incidentes. Sin embargo, también se observan oportunidades en este contexto. La colaboración global junto a organizaciones como la OEA y la UIT y la implementación de tecnologías avanzadas como la inteligencia artificial y blockchain podrían ser clave para fortalecer la seguridad informática en Ecuador de forma notablemente positiva. Estos recursos no solo aumentarán las capacidades de prevención sino también las respuestas ante situaciones adversas.

Por último, se observa que la confianza de los ciudadanos en las plataformas digitales, particularmente en aquellas gubernamentales, sigue siendo limitada, lo que afecta negativamente

la adopción de servicios digitales y la expansión de la economía digital en el país. En este sentido, es crucial implementar campañas de sensibilización y medidas que refuercen la percepción de seguridad en los sistemas.

En conclusión, aunque Ecuador ha avanzado de manera considerable en la construcción de un entorno digital más seguro, aún enfrenta retos significativos que requieren atención prioritaria. El fortalecimiento de la infraestructura tecnológica, la inversión en talento humano, la cooperación internacional y la promoción de la confianza digital son aspectos clave para que el país pueda alinearse con los estándares internacionales y consolidarse como un referente en ciberseguridad dentro de la región.

Recomendaciones

En base al análisis realizado en este informe, se plantean las siguientes recomendaciones con el fin de fortalecer la ciberseguridad en Ecuador, abordando las principales brechas y desafíos identificados:

- Fortalecer la infraestructura tecnológica en Ecuador, cerrando brechas digitales existentes, especialmente en las zonas rurales, mediante inversiones en infraestructura tecnológica que permitan el acceso equitativo a servicios digitales seguros. Incluyendo la expansión de redes de alta velocidad y la implementación de centros regionales de apoyo tecnológico.
- Crear programas nacionales de cultura en materia de ciberseguridad dirigidos a profesionales del sector público y privado, ya que esto es crucial para reducir el déficit de talento especializado.
- Promover la colaboración internacional en materia de ciberseguridad aprovechando las posibilidades de trabajar juntos con organismos internacionales como la OEA y la UIT y otros participantes globales. Estas asociaciones pueden ofrecer recursos técnicos formación especializada y asistencia en el cumplimiento de normas internacionales de ciberseguridad.
- Mejorar y reforzar las políticas y normativas relacionadas con la ciberseguridad, garantizando su aplicación efectiva. Asimismo, se deben realizar campañas de sensibilización para aumentar la confianza de los ciudadanos en los servicios digitales, destacando la importancia de la privacidad y la protección de datos.

Bibliografía

Referencias

- Acosta, M., Velastegui, A. Y., & Pérez, V. C. (2018). PERSPECTIVAS DE LA ECONOMÍA DIGITAL EN LATINOAMÉRICA: CASO ECUADOR. *Investigación y pensamiento crítico*, 29-43.
- ARCOTEL-EcuCERT. (01 de 01 de 2023). *www.ecucert.gob.ec*. Recuperado el 10 de 11 de 2024, de <https://www.ecucert.gob.ec/bibliotecadealertas/>
- branch. (05 de 07 de 2024). *branch.com.co*. Recuperado el 28 de 08 de 2024, de [branch.com.co](https://branch.com.co/marketing-digital/situacion-digital-de-ecuador-en-2024/): <https://branch.com.co/marketing-digital/situacion-digital-de-ecuador-en-2024/>
- Buzdugan, A., & Capatana, G. (2021). Cyber Security Maturity Model for Critical Infrastructures. En C. Ciurea, P. P. Cătălin Boja, & M. Doinea, *Education, Research* (págs. 225-236). Springer Nature Singapore Pte Ltd. 2022.
- Buzdugan, A., & Căpăţână, G. (2023). The Trends in Cybersecurity Maturity Models. *Education, Research and Business Technologies*, 217-228.
- Córdova, J. E. (01 de 04 de 2024). 204.199.82.243:8080. Recuperado el 28 de 10 de 2024, de 204.199.82.243:8080: <http://204.199.82.243:8080/bitstream/handle/123456789/2399/Brechas%20del%20Peritaje%20Inform%C3%A1tico%20Forense%20Impacto%20para%20Juristas%20y%20Peritos.pdf?sequence=1&isAllowed=y>
- Dutta, S., & Lanvin, B. (12 de 11 de 2024). *download.networkreadinessindex.org*. Obtenido de [download.networkreadinessindex.org](https://download.networkreadinessindex.org/reports/data/2024/nri-2024.pdf): [download.networkreadinessindex.org](https://download.networkreadinessindex.org/reports/data/2024/nri-2024.pdf): <https://download.networkreadinessindex.org/reports/data/2024/nri-2024.pdf>
- Freitag, C., & Berners-Lee, d. M. (01 de 01 de 2021). *arxiv.org*. Obtenido de [arxiv.org](https://arxiv.org/pdf/2102.02622): <https://arxiv.org/pdf/2102.02622>
- Gobierno Electrónico. (02 de 05 de 2024). *www.gobiernoelectronico.gob.ec*. Recuperado el 01 de 11 de 2024, de [www.gobiernoelectronico.gob.ec](https://www.gobiernoelectronico.gob.ec/ecuador-escala-posiciones-en-el-ranking-mundial-sobre-el-desarrollo-del-gobierno-electronico/#:~:text=El%20EGDI%20eval%C3%BAa%20tres%20par%C3%A1metros,%2C%20App's%20m%C3%B3vil%2C%20entre%20otros.&text=A%20nivel%20de%20): <https://www.gobiernoelectronico.gob.ec/ecuador-escala-posiciones-en-el-ranking-mundial-sobre-el-desarrollo-del-gobierno-electronico/#:~:text=El%20EGDI%20eval%C3%BAa%20tres%20par%C3%A1metros,%2C%20App's%20m%C3%B3vil%2C%20entre%20otros.&text=A%20nivel%20de%20>
- Ibarra, C. S., Tapia, C. A., Tene, A. M., Toapanta, R. J., & Ormaza, G. S. (2024). Análisis de los ataques de ingeniería social en Ecuador. *Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.* , 4354 - 4367.
- IBM. (01 de 05 de 2024). *www.ibm.com*. Obtenido de [www.ibm.com](https://www.ibm.com/mx-es/topics/critical-infrastructure): <https://www.ibm.com/mx-es/topics/critical-infrastructure>
- ITU. (12 de 09 de 2024). *www.itu.int*. Obtenido de [www.itu.int](https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf): https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf

ITU. (24 de 06 de 2024). *www.itu.int*. Obtenido de *www.itu.int*: https://www.itu.int/hub/publication/d-ind-ict_mdd-2023-2/

Laubshtein, Y. (2023). Protegiendo las infraestructuras de agua y saneamiento de amenazas cibernéticas: un estudio de ciberseguridad para América Latina y el Caribe, IADB: Inter-American Development Bank. United States of America.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (12 de 10 de 2022). *www.gobiernoelectronico.gob.ec*. Recuperado el 04 de 08 de 2024, de *www.gobiernoelectronico.gob.ec*: <https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2022/10/Difusion-ENC.pdf>

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (29 de 08 de 2022). *www.gobiernoelectronico.gob.ec*. Recuperado el 25 de 11 de 2024, de *www.gobiernoelectronico.gob.ec*: <https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-2022.pdf>

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (17 de 05 de 2023). *www.telecomunicaciones.gob.ec*. Recuperado el 08 de 10 de 2024, de *www.telecomunicaciones.gob.ec*: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2023/06/Poli%CC%81tica-Pu%CC%81blica-Telecomunicaciones-2023-2025-con-ANEXOS-nuevos-signed-signed-signed-signed_firmado.pdf

MINTEL. (14 de 07 de 2023). *asobanca.org.ec*. Recuperado el 02 de 07 de 2024, de *asobanca.org.ec*: <https://asobanca.org.ec/wp-content/uploads/2023/07/ACUERDO-Nro.-MINTEL-MINTEL-2023-0015-Uso-adeecuado-de-servicios-en-la-nube-en-entidades-del-sector.pdf>

Morán Maldonado, N. M. (01 de 01 de 2021). *dspace.ups.edu.ec*. Obtenido de *dspace.ups.edu.ec*: <https://dspace.ups.edu.ec/handle/123456789/20243>

Portulans Institute . (28 de 12 de 2024). *download.networkreadinessindex.org*. Recuperado el 29 de 12 de 2024, de *download.networkreadinessindex.org*: <https://download.networkreadinessindex.org/reports/countries/2024/ecuador.pdf>

REGISTRO OFICIAL Órgano de la República del Ecuador. (23 de 06 de 2021). *www.gobiernoelectronico.gob.ec*. Recuperado el 18 de 11 de 2024, de *www.gobiernoelectronico.gob.ec*: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2021/07/PP_Ciberseguridad_Ecuador.pdf

Ron, M., Rivera, O., Fuentes, W., Toulkeridis, T., & Díaz, J. (2019). Línea base de ciberseguridad, una exploración que permite delinear la estrategia nacional de ciberseguridad en Ecuador. *Tecnologías y sistemas de información*, 847-857.

Sánchez, J. G., Mendoza, M. N., & G. M. (2020). Vulnerabilidades de sitios web gubernamentales en Ecuador: Un estudio exploratorio pre-muestral. *Revista Ibérica de Sistemas e Tecnologías de Informação*, 67-78.

Software Ecuatoriano. (03 de 05 de 2024). *www.softwarepublico.gob.ec*. Recuperado el 23 de 08 de 2024, de *www.softwarepublico.gob.ec*: <https://www.softwarepublico.gob.ec/listado-de-software-publico-nacional/>

Stevenson, C. L. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 1908-1979.

Telefónica. (01 de 09 de 2023). *www.arcotel.gob.ec*. Recuperado el 10 de 10 de 2024, de *www.arcotel.gob.ec*: <https://www.arcotel.gob.ec/wp-content/uploads/2023/10/2023.10.02-Telefo%CC%81nica-Comentarios-consulta-topes-de-espectro.pdf>

UN E-Government Knowledgebase. (2024). *publicadministration.un.org*. Recuperado el 12 de 10 de 2024, de *publicadministration.un.org*: <https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/52-Ecuador>

Urbanovics, A., & Guajardo, R. (2022). Estrategias de ciberseguridad en los países latinoamericanos – un análisis comparativo. *Acta Hispanica*, (IV), 89-104.