Universidad Nacional de Loja

Facultad de la Energía, las Industrias y los Recursos Naturales no Renovables

Maestría en Telecomunicaciones

Análisis comparativo de los diferentes tipos de ataques informáticos perpetrados en sectores estratégicos en el ecuador y su repercusión económico-social en el último lustro.

Trabajo de Titulación previa a la obtención del título de Magíster en Telecomunicaciones

AUTOR:

Ing. Alexis Vicente Pardo Sánchez

DIRECTOR:

Ing. John Jossimar Tucker Yepez, Mg. Sc.

LOJA – ECUADOR

2023

Certificación

Loja, 12 de mayo del 2023

Ing. John Jossimar Tucker Yepez Mg. Sc.
DIRECTOR DE TRABAJO DE TITULACIÓN

CERTIFICO:

Que he revisado y orientado todo proceso de la elaboración del Trabajo de Titulación denominado: **Análisis comparativo de los diferentes tipos de ataques informáticos perpetrados en Sectores Estratégicos en el Ecuador y su repercusión económico-social en el último lustro.,** previo a la obtención del título **de Magíster en Telecomunicaciones,** de autoría del estudiante **Alexis Vicente Pardo Sánchez**, con **cédula de identidad Nº 1104115439**, una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja para el efecto, autorizo la presentación para la respectiva sustentación y defensa.

Firmado electrónicamente por:
JOHN JOSSIMAR TUCKER YEPEZ

Ing. John Jossimar Tucker Yepez Mg. Sc.
DIRECTOR DE TRABAJO DE TITULACIÓN

Autoría

Yo, Alexis Vicente Pardo Sánchez, declaro ser autor del Trabajo de Titulación y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos y acciones legales, por el contenido del mismo. Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación del Trabajo de Titulación en el Repositorio Digital Institucional – Biblioteca Virtual.

Firma:

Firmado electrónicamente por:
ALEXIS VICENTE
PARDO SANCHEZ

Cédula de Identidad: 1104115439

Fecha: 15 de mayo del 2023

Correo electrónico: alexis.pardo@unl.edu.ec

Teléfono: 0986601752

Carta de autorización por parte del autor, para consulta, reproducción parcial o total y/o publicación electrónica de texto completo, del Trabajo de Titulación.

Yo, **Alexis Vicente Pardo Sánchez**, declaro ser autor del Trabajo de Titulación denominado: **Análisis Comparativo de los diferentes tipos de ataques informáticos perpetrados en Sectores Estratégicos en el Ecuador y su repercusión económico-social en el último lustro.**, como requisito para optar el título de **Magíster Telecomunicaciones**, autorizo al sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del Trabajo de Titulación que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los quince días del mes de mayo de dos mil veintitrés.

Firma:

Firmado electrónicamente por:
ALEXIS VICENTE
PARDO SANCHEZ

Cédula: 1104115439
Dirección: Barrio Nueva Granada, Loja
Correo Electrónico: alexis.pardo@unl.edu.ec
Teléfono: 0986601752

DATOS COMPLEMENTARIOS:
DIRECTOR DE TRABAJO DE TITULACIÓN: Ing. Jhon Jossimar Tucker Yepez Mg. Sc.

Dedicatoria

El presente trabajo de investigación lo dedico a mis padres Janeth Sánchez y Vicente Pardo quienes con su arduo esfuerzo y sacrificio me han apoyado en este sendero de estudio y me han apoyado innumerables veces a seguir adelante con mis metas, sueños y anhelos, sin su apoyo incondicional nunca lo hubiera logrado.

Este trabajo también va dedicado mi hermano José Luis quien me ha acompañado y apoyado con sus valiosas palabras y consejos para seguir avanzando con mis estudios y seguir mejorando cada día. De igual manera, va dirigido a mis abuelitos Héctor y Zoraida los cuales me supieron brindar su apoyo y cobijo cuando más lo necesitaba, siempre les estaré agradecido.

Mi dedicatoria también va dirigida a mis amigos y compañeros con los que he compartido gratos momentos en todos estos años de estudio y quienes me supieron brindar su apoyo incondicional para cumplir mis objetivos.

Alexis Vicente Pardo Sánchez

Agradecimiento

Agradezco profundamente mis padres quienes me han apoyado incondicionalmente en cada aspecto de mi vida y siempre han creído en mí y en lo que puedo lograr. Gracias a su ejemplo de perseverancia y esfuerzo he podido darme fuerzas para seguir adelante y triunfar en cada meta que me proyecte; estoy eternamente agradecido por su valiosa ayuda.

Al Ing. John Tucker por su asesoría y ayuda en este sendero del conocimiento, quien supo guiarme hasta lograr cumplir con este trabajo de investigación que representa un nuevo peldaño en mi camino como profesional

También agradezco a mi Universidad por permitirme desarrollar aún más mis conocimientos en la rama que me apasiona y me motiva a convertir en un gran profesional. De igual manera, le doy gracias a cada uno de mis profesores de la Maestría en Telecomunicaciones, quienes me han inculcado sus saberes y experiencias para lograr formarme como un futuro profesional de la patria.

Alexis Vicente Pardo Sánchez

Índice de Contenidos

Índice de Tablas:

Índice de Figuras:

Índice de Anexos:

1. Título

Análisis comparativo de los diferentes tipos de ataques informáticos perpetrados en sectores estratégicos en el Ecuador y su repercusión económico-social en el último lustro.

2. Resumen

En este proyecto de investigación se indago sobre los principales ataques cibernéticos que han sido registrados en el país y como han afectado en diferente medida a la economía y crecimiento del Ecuador. En este estudio se pudo evidenciar que tipos de ataques se han lanzado, cuáles han sido los más frecuentes, su principio de funcionamiento y cuál es su propósito para atacar a los sectores estratégicos del país.

De igual manera, en el estudio se evidencia como estos ataques también han afectado el ámbito social, debido al pánico que estos causan en la población, con el fin de generar conflictos internos dentro de la sociedad. Entre algunos de los objetivos de estos ataques, es el de desestabilizar gobiernos por medio de la conmoción social que se genera a partir de información fraudulenta.

Finalmente, en la investigación se determinó cual ha sido el impacto económico-social causado por estos ataques a los sectores estratégicos, los cuales son los pilares que sostienen la economía del país, al ser los campos que más capital aportan para el crecimiento del Ecuador.

Palabras Clave: Ciberataques, Sectores Estratégicos, Económico-Social.

2.1. Abstract

In this research project, we inquired about the Main Cyber Attacks that have been occurring in the country and how they have affected: to different extents, the economy, and the growth of Ecuador. In this study, it was possible to show what types of attacks have been performed, which have been the most frequent, their principle of operation, and which is their purpose when attacking the national strategic sectors of the country.

Likewise, the study shows how these attacks have also affected the social sphere due to the panic they cause in the population, generating internal disturbances within society. Among some of the objectives of these attacks is to destabilize governments through the social commotion generated by fraudulent information.

Finally, the researchers determined the investigation, which has been the economic and social impact caused by these attacks on strategic sectors, which are the pillars that support the country's economy, being the fields that provide more capital for the growth of Ecuador.

Keywords: Cyber-attacks, Strategic Sectors, Economic-Social.

3. Introducción

Uno de los grandes problemas que se vive actualmente en la era digital es la capacidad de mantener protegida la información de agentes externos, ya sea de un equipo personal, el de alguna compañía o de cualquier entidad de diversa índole. Con la llegada del Internet que conecta a diversos equipos dentro de una misma red (una red global), ha permitido que distintos usuarios, empresas y entidades puedan compartir, colaborar y almacenar información alrededor del mundo. Sin embargo, aprovechando esta facilidad que ofrece el Internet, otro tipo de usuarios que se los denomina atacantes, tienen como principal objetivo buscar tener acceso a tal información (que en la mayoría de los casos es confidencial) mediante ciberataques para exigir una compensación económica para evitar filtrar tales datos.

Para un país, este tipo de incidentes se ha convertido en un trabajo diario debido a la gran cantidad de ciberataques que se reciben en las diversas plataformas digitales con las que cuenta la nación. No obstante, estar protegido contra este tipo de amenazas supone un importante pilar sobre la seguridad del país, puesto que asegura su soberanía y protege los recursos del mismo.

Del mismo modo, en el Ecuador se han podido detectar alrededor 10 mil ataques informáticos que han efectuados y que se han podido detectar en las diferentes instituciones del país, esto según registros obtenidos de la fiscalía general del Estado.

Debido a esto, el objetivo del presente trabajo de investigación es investigar los principales ataques cibernéticos realizados a los diferentes sectores estratégicos del Ecuador en los últimos 5 años, puesto que son los ataques que más impacto han causado al país y han repercutido de una forma sin precedentes al ámbito socio-económico de la nación.

Objetivos

Objetivo general

- Investigar los principales ataques cibernéticos realizados a los diferentes sectores estratégicos del Ecuador en los últimos 5 años.

Objetivos específicos

- Identificar los tipos de ataques informáticos que se han realizado a las infraestructuras críticas del país, su funcionamiento y los efectos causados en el ámbito económico-social.

- Comparar los diferentes ataques cibernéticos encontrados y evaluar el nivel de daño que pueden causar a los sectores estratégicos con el nivel de seguridad actual.

4. Marco Teórico

En este capítulo se describe de manera resumida que son los ataques informáticos, cuál es su principio de funcionamiento, que tipos de ataques se han lanzado en el Ecuador y cuál es su propósito. De igual manera se aborda todo lo concerniente a los sectores estratégicos del país y cuál es su influencia en la economía y los demás sectores del Ecuador.

4.1. Ataques Cibernéticos

Un ataque cibernetico es cualquier intento de acceder a un sistema informatico (vulnerar o penetrar) con fines maliciosos, de tal manera que su principal objetivo es obtener datos o información confidencial (privada) de algun individuo, organización o empresa. Por tanto, la persona u organización que realiza el ataque, tiene como finalidad perpetrar el sistema de seguridad de las plataformas digitales a traves de una red (ya sea local o el Internet) para robar datos que pueden ser valiosos para otro usuario o empresa.

La mayoría de los ataques informáticos que se realizan en todo el mundo se hacen a través de Internet, esto debido a que los atacantes pueden mantener un estatus de anonimato para impedir que se puedan rastrear e identificar. Esto sumado a que el Internet al ser la red que conecta a todos los equipos del mundo, con las herramientas adecuadas se podría vulnerar cualquier equipo que desee.

Existen diversos tipos de ataques informaticos que se suelen emplear para poder penetrar la seguridad de la mayoría de sistemas. Sin embargo, estos pueden agruparse con base a patrones similares en su modo de operación. En la Fig.1. se puede observar la clasificación de los ataques según la RFC (Request for Comments) de la ITU X.800 (Unión Internacional de Telecomunicaciones, 1991).

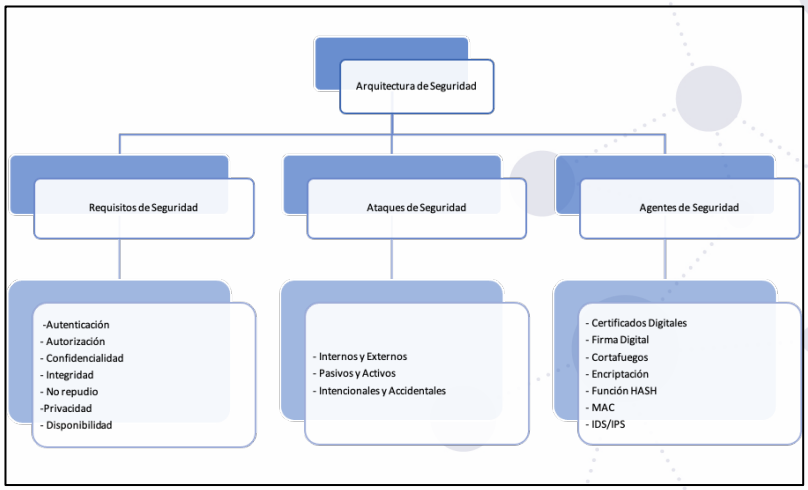


Fig. 1: Arquitectura de Seguridad en base a la recomendación X.800.
Fuente: Arquitectura de Seguridad de la Interconexión de Sistemas Abiertos para las aplicaciones del CCITT.

4.1.1. Clasificación de los Ataques Cibernéticos

4.1.1.1. Internos y Externos

Este nivel de clasificación toma como base la procedencia de los ataques hacia un individuo o una empresa, es decir, si es de origen interno, externo o ambos.

Ataques Internos

Los ataques internos generalmente se producen debido a que de manera autorizada un individuo tiene a acceso a la red, sea a un servidor o físicamente a la red de la organización. Por tanto, en el caso de un ataque interno debido a la acción humana, puede deberse a un descontento de algún empleado o exempleado de la empresa que busca perjudicarla (Mouna et al., 2014).

Ataques Externos

Este tipo de ataques se producen de manera ajena a la empresa, por tanto, el individuo o la organización que realiza el ataque no tiene acceso autorizado a los sistemas informáticos de la empresa (Mouna et al., 2014).

Los ataques externos pueden producirse por acción humana o de forma accidental debido a eventualidades dentro del sistema. En el caso de un ataque externo intencional se tiene la situación de algún espía de alguna otra empresa o institución que busca, con fines maliciosos, obtener información o causar daños a la empresa rival.

En el caso de ataques externos de forma accidental, entre los más comunes, se tienen: Roedores que destruyen el cableado, Cortocircuitos, Fenómenos Climatológicos, Personal de limpieza que desconecta el cableado de forma accidental etc.

4.1.1.2. Pasivos y Activos

Esta clasificación está basada en el modus operandi de los ataques realizados.

Pasivos

Este tipo de ataque se caracterizan por intentar obtener acceso a la red sin que existan efectos residuales, es decir, que el ataque evita dejar rastros sobre mientras esta interactuando con la red víctima. Debido a esto, la mayoría de estos ataques suelen usarse para espiar información a través de sniffers que filtran el tráfico que se está generando en la red, capturando los paquetes de forma clandestina (Shafiullah et al., 2008).

Activos

Al contrario de los ataques pasivos, estos ataques se destacan por intentar vulnerar el sistema de seguridad de la empresa, modificando o alterando la estructura o la forma en la que opera su sistema con el fin de sabotear su integridad (Mouna et al., 2014). Estos ataques se pueden clasificar en los siguientes 4 tipos (IBM, 2021):

- Intentos de acceso al sistema
- Usurpación
- Ataques de Denegación de Servicios
- Ataques Criptográficos

Entre los más comunes de estos tipos de ataques se tiene:

- **Ransomware**

Con el ransomware, el sistema de la víctima se mantiene como rehén hasta que accede a pagar un rescate al atacante. Una vez efectuado el pago, el atacante proporciona instrucciones para que la víctima recupere el control de su ordenador. El nombre "ransomware" es apropiado porque el malware exige un rescate a la víctima (Kaspersky, 2022).

En un ataque de ransomware, el objetivo descarga el ransomware, ya sea desde un sitio web o desde un archivo adjunto a un correo electrónico. El malware está escrito para explotar vulnerabilidades que no han sido resueltas ni por el fabricante del sistema ni por el equipo informático. A continuación, el ransomware cifra la estación de trabajo del objetivo. En ocasiones, el ransomware puede utilizarse para atacar a varias partes, denegando el acceso a varios ordenadores o a un servidor central esencial para las operaciones de la empresa.

La afectación de varios ordenadores se consigue a menudo no iniciando la cautivación de los sistemas hasta días o incluso semanas después de la penetración inicial del malware. El malware puede enviar archivos AUTORUN que van de un sistema a otro a través de la red interna o de unidades de bus serie universal (USB) que se conectan a varios ordenadores. Entonces, cuando el atacante inicia el cifrado, éste funciona en todos los sistemas infectados simultáneamente (Fortinet, 2023).

En algunos casos, los autores del ransomware diseñan el código para evadir el software antivirus tradicional. Por lo tanto, es importante que los usuarios estén atentos a los sitios que visitan y a los enlaces en los que hacen clic. También puede prevenir muchos ataques de ransomware utilizando un cortafuegos de nueva generación (NGFW) que pueda realizar inspecciones profundas de paquetes de datos utilizando inteligencia artificial (IA) que busque las características del ransomware.

- **Phishing**

Un ataque de phishing se produce cuando un actor malicioso envía correos electrónicos que parecen proceder de fuentes fiables y legítimas en un intento de hacerse con información sensible del objetivo. Los ataques de phishing combinan ingeniería social y tecnología y se denominan así porque el atacante está, en efecto, "pescando" el acceso a un área prohibida utilizando el "cebo" de un remitente aparentemente de confianza (Fortinet, 2023).

Para ejecutar el ataque, el malhechor puede enviar un enlace que le lleve a un sitio web que le engañe para que descargue programas maliciosos, como virus, o facilite al atacante su información privada. En muchos casos, el objetivo puede no darse cuenta de que ha sido comprometido, lo que permite al atacante ir a por otros en la misma organización sin que nadie sospeche de la actividad maliciosa.

- **Denegación de Servicios (DoS) y Denegación de Servicios Distribuida (DDoS)**

Un ataque de denegación de servicio (DoS) está diseñado para saturar los recursos de un sistema hasta el punto de que sea incapaz de responder a peticiones legítimas de servicio. Un ataque de denegación de servicio distribuido (DDoS) es similar en el sentido de que también busca agotar los recursos de un sistema. Un ataque DDoS es iniciado por una gran cantidad de máquinas host infectadas con malware y controladas por el atacante. Se denominan ataques de "denegación de servicio"

porque el sitio víctima es incapaz de prestar servicio a quienes desean acceder a él (Oficina de Seguridad del Internauta, 2018).

Con un ataque DoS, el sitio objetivo se ve inundado de peticiones ilegítimas. Como el sitio tiene que responder a cada solicitud, todas las respuestas consumen sus recursos. Esto hace que sea imposible para el sitio servir a los usuarios como lo hace normalmente y a menudo resulta en un cierre completo del sitio.

Los ataques DoS y DDoS son diferentes de otros tipos de ciberataques que permiten al hacker obtener acceso a un sistema o aumentar el que ya tiene. Con este tipo de ataques, el atacante se beneficia directamente de sus esfuerzos. En cambio, con los ataques de red DoS y DDoS, el objetivo es simplemente interrumpir la eficacia del servicio del objetivo. Si el atacante es contratado por un competidor comercial, puede beneficiarse económicamente de sus esfuerzos (IBM, 2021).

Un ataque DoS también puede utilizarse para crear vulnerabilidad para otro tipo de ataque. Con un ataque DoS o DDoS exitoso, el sistema a menudo tiene que quedar fuera de línea, lo que puede dejarlo vulnerable a otros tipos de ataques. Una forma común de prevenir los ataques DoS es utilizar un cortafuegos que detecte si las peticiones enviadas a su sitio son legítimas. Las solicitudes falsas pueden entonces descartarse, permitiendo que el tráfico normal fluya sin interrupción. Un ejemplo de un gran ataque de este tipo en Internet se produjo en febrero de 2020 a Amazon Web Services (AWS) (Ridaura, 2021).

Según la página web del Gobierno del Ecuador, los ataques mas frecuentes que se han realizado a plataformas digitales del Ecuador son: Suplantación de Identidad, Correo no Deseado (Phishing), Software Malicioso (Ransomware), Denegación de Servicios y Fuga de información (Amenaza Interna o MITM) (Revisar Anexo 1)(Gobierno Electrónico de Ecuador, 2019).

4.1.1.3. Intencionales y Accidentales

Esta clasificación parte del hecho que los ataques son realizados por acción humana.

Intencionales

Estos ataques son el resultado de una acción intencional de un individuo u organización hacia otros con fines perjudiciales para la víctima. Este tipo de accionares se consideran como delitos informáticos, entre los cuales se tiene: Espionaje, Robo de Identidad, Pornografía Infantil y delitos relacionados con robo de credenciales financieras (tarjetas de crédito/debido, cuentas de banco, etc.).

Accidentales

Son ataques producidos de forma no intencional o sin conocimiento. Dentro de este tipo de amenazas se encuentran: La corrupción de software de forma accidental como haber borrado algún archivo, necesario para el adecuado funcionamiento del sistema; Desconexión de cablería de forma no intencional; Manipulación de los equipos sin conocimiento; entre otras.

4.2. Sectores Estratégicos

Los sectores estratégicos son aquellos que, debido a su importancia o transcendencia para el país, ya sea por el aporte crucial o influencia que realizan a la economía nacional, social, política, o ambiental; representan un factor clave que se debe desarrollar y velar por su crecimiento y seguridad. Por tal motivo, el estado es el único que puede decidir sobre su accionar y tomar control sobre estos.

Según la Constitución de la República del Ecuador, los sectores estratégicos se definen como: “Aquellos que por su trascendencia y magnitud tienen decisiva influencia económica, social, política o ambiental, y deberán orientarse al pleno desarrollo de los derechos y al interés social.” (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2008).

De igual manera en el Ecuador, se consideran sectores estratégicos la energía en todas sus formas, las telecomunicaciones, los recursos naturales no renovables, el transporte y la refinación de hidrocarburos, la biodiversidad y el patrimonio genético, el espectro radioeléctrico, el agua, y los demás que determine la ley.

Fig. 2: *Sectores Estrategicos del Ecuador.*
Fuente: *Ministerio de Coordinación de Sectores Estrategicos.*

4.2.1. Sector Eléctrico y Energía Renovable (Bioenergía)

Según define el Banco Central del Ecuador, el sector eléctrico es básicamente, la cadena de producción de este subsector económico incluye las empresas de generación eléctrica (hidro o termoeléctricas) que corresponde a la producción misma de la energía, la transmisión o traslado de los flujos a través del Sistema Nacional Interconectado -SNI- y, la distribución a usuarios finales, servicio prestado por las diferentes empresas, mayoritariamente de accionariado estatal, que son propiedad del Estado ecuatoriano por intermedio del Fondo de Solidaridad. Adicionalmente y para completar la configuración del sector, constan los autogeneradores y grandes consumidores (Banco Central del Ecuador, 2005).

En cuanto a la normativa y regulación, el CONELEC, funge de brazo ejecutor de la "política eléctrica", el CENACE es el administrador del Mercado Eléctrico Mayorista - MEM- y la Ley de Régimen del Sector Eléctrico -LRSE- constituye el entorno jurídico general bajo el cual se desempeñan las actividades inherentes a esta actividad económica (Banco Central del Ecuador, 2005).

En este contexto, las actividades del mercado eléctrico se desenvuelven bajo un esquema competitivo en la etapa de generación; monopolio natural en la transmisión; y, mercado regulado en la distribución (Banco Central del Ecuador, 2005).

4.2.2. Sector de Telecomunicaciones

Como lo señala la Unión Internacional de Telecomunicaciones (UIT), "la interacción de la demanda y la oferta ha determinado que las telecomunicaciones constituyan uno de los sectores de mayor crecimiento en la economía mundial y uno de los componentes más importantes de la actividad social, cultural y política" (QUEZADA & PALADINES, 2009).

El crecimiento se ve impulsado por la penetración de las telecomunicaciones y la tecnología de la información en todos los aspectos del ser humano, en todos los sectores de la actividad económica y social, en la administración pública, en la provisión de servicios públicos y en la gestión de infraestructuras públicas, en la enseñanza y la expresión cultural, en la gestión del entorno y en las emergencias, sean naturales o provocadas por el hombre. Pero también, el crecimiento se ve impulsado por la rápida evolución tecnológica que mejora constantemente la eficacia de los productos, sistemas y servicios existentes y crea las bases para un flujo continuo de innovaciones en cada uno de estos sectores (es muy notable la convergencia de las tecnologías de las telecomunicaciones, la información y la radiodifusión) (Dirección General de Estudios, 2004).

4.2.3. Sector Industrias Básicas

El desarrollo de la industria básica es fundamental para dar soporte a la producción manufacturera. En términos generales se considera industria básica aquella que tiene como fuente de materias primas recursos naturales, y cuyos productos constituyen a su vez insumos para otros procesos de producción industrial (Cámara de Industrias de Guayaquil, 2012).

Una economía que cuenta con una industria relativamente consolidada, está sustentada por producciones de bienes obtenidos de la minería metálica (hierro, acero, cobre, aluminio, etc.) y no metálica (cemento, vidrio, cerámica); del petróleo (petroquímica, GLP) y de recursos forestales (pulpa y papel); entre las más importantes (Cámara de Industrias de Guayaquil, 2012).

4.2.4. Sector Minería

El Gobierno Nacional decidió apoyar el desarrollo de la industria minera y atraer capitales hacia este sector considerando que el Ecuador es un país con potencial minero, que tiene reservas de oro, plata y cobre, además de una variada oferta de productos mineros. Bajo este fundamento se creó el Ministerio de Minería del Ecuador, mediante Decreto Ejecutivo 578 de 13 de febrero de 2015. Esta Secretaría de Estado es el ente rector y ejecutor de la política minera del área geológico-minera de conformidad con los principios de sostenibilidad, precaución, prevención y eficiencia; además, es parte de sector estratégico del país (Banco Central del Ecuador, 2015).

La Ley de Minería establece que: “La explotación de los recursos naturales y el ejercicio de los derechos mineros se ceñirán al Plan Nacional de Desarrollo, a los principios del desarrollo sustentable y sostenible, de la protección y conservación del medio ambiente y de la participación y responsabilidad social, debiendo respetar

el patrimonio natural y cultural de las zonas explotadas. Su exploración y explotación racional se realizará en función de los intereses nacionales, por personas naturales o jurídicas, empresas públicas, mixtas o privadas, nacionales o extranjeras, otorgándoles derechos mineros, de conformidad con esta ley." (Banco Central del Ecuador, 2015).

La misma Ley clasifica a la minería en el país en cuatro clases: la artesanal o de de subsistencia, la pequeña minería, la mediana minería y la minería a gran escala. Clasificación que se da de acuerdo a los niveles de producción diarios que puede tener una mina. También determina que el Estado ejecuta sus actividades mineras por intermedio de la Empresa Nacional Minera y podrá constituir compañías de economía mixta (Banco Central del Ecuador, 2015).

4.2.5. Sector Hidrocarburífero o Petrolero

El sector hidrocarburos se considera al conjunto de actividades económicas relacionadas con la exploración, producción, transporte, refinación o procesamiento y comercialización de todo compuesto orgánico, gaseoso, líquido o sólido, que consiste principalmente de carbono e hidrógeno.

El petróleo, es un recurso energético, financiero y materia prima, perecedero, de propiedad pública nacional. Para el Ecuador, es un bien crucial que da la oportunidad única para impulsar el verdadero desarrollo, no solo petrolero, sino de otros sectores productivos: industria química, industria básica, agroindustria, mecáni- ca, eléctrica, electrónica, turística y otras que posibiliten el aprovechamiento óptimo de los recursos existentes en el país. Es decir, un instrumento para cimentar el desarrollo integral, cuyos efectos sean la generación de riqueza, empleo y bienestar de la población actual y futura (AenorEcuador, 2019).

4.2.6. Recursos Hídricos

En la Constitución de la República, específicamente en los artículos 12, 313 y 318 se consagra el principio de que el agua es patrimonio nacional estratégico, de uso público, dominio inalienable, imprescriptible e inembargable del Estado y constituye un elemento vital para la naturaleza y para la existencia de los seres humanos, reservando para el Estado el derecho de administrar, regular, controlar y gestionar los sectores estratégicos, de conformidad con los principios de sostenibilidad ambiental, precaución, prevención y eficiencia (Asamblea Nacional del Ecuador, 2014).

Además, en el artículo 318 se prohíbe toda forma de privatización del agua y determina que la gestión del agua será exclusivamente pública o comunitaria y que

el servicio de saneamiento, el abastecimiento de agua potable y el riego serán prestados únicamente por personas jurídicas estatales o comunitarias; prescribe además, que el Estado a través de la Autoridad Unica del Agua, será responsable directa de la planificación y gestión de los recursos hídricos que se destinarán a consumo humano y riego que garantice la soberanía alimentaria, caudal ecológico y actividades productivas, en este orden de prelación y que se requerirá autorización estatal para el aprovechamiento del agua con fines productivos por parte de los sectores público, privado y de la economía popular y solidaria, de acuerdo con la Ley (Asamblea Nacional del Ecuador, 2014).

4.3. Factores Socioeconómicos

Los factores socioeconómicos son un índice que permite determinar el grado de crecimiento y desarrollo que tiene un país. Tal crecimiento se ve influenciado por dos aspectos importantes, el aspecto económico y el aspecto social.

En el aspecto económico se contemplan todas las variables que aportan o no (ingreso o gasto respectivamente) al crecimiento de la renta real per cápita del país (Martín, 2011). Mientras que, en el aspecto social se consideran todos los parámetros que contribuyen o no al desarrollo de la población. Según el Banco Mundial, para social se requiere "Poner en primer lugar a las personas" en los procesos de desarrollo (MARTÍN, 2019).

En ambos aspectos se consideran ciertas variables que permiten identificar su evolución a lo largo del tiempo; entre algunas de estas se tienen (Fortes & Rueda, 2011):

Económico:

- PIB per Cápita
- Moneda
- Inflación
- Inversión
- Presión Fiscal
- Gasto Público
- Tasa de Desempleo, etc.

Social:

- Índice de Desarrollo Humano
- Pobreza
- Gasto Público en Educación
- Tasa de Alfabetización
- Gasto Público en Sanidad
- Tasa de Crecimiento Demográfico

- Gasto en I+D, etc.

En el Ecuador estos factores también se toman como referencia y sirven como indicadores que permiten identificar el nivel de la calidad de vida de la población y, por ende, del país. Según estudios de la INEC, se valoran 6 variables o "dimensiones" para determinar el "Índice de nivel Socioeconómico" en las poblaciones del Ecuador, estas son (INEC, 2010):

- Características de la vivienda
- Nivel de Educación
- Actividad Económica del hogar
- Posesión de bienes
- Acceso a tecnología
- Hábitos de consumo

Por medio de estas variables, se puede obtener valoraciones sobre el nivel de crecimiento del Ecuador y como ha sido su evolución durante el período de evaluación. No obstante, se debe destacar en esta evaluación solo contemplan variables microeconómicas, que conforman una parte del análisis socio-económico global del país.

En una evaluación de factores socioeconómicos a nivel macro, que, en su mayoría, son los que más aportan económicamente al país, se abarcan sectores como (ASOBANCA, 2021):

- Agricultura
- Explotación de Minas y canteras
- Industrias Manufactureras
- Construcción
- Comercio (Al por mayor y menor)
- Transporte y Almacenamiento
- Actividades Financieras y de Seguros
- Actividades Profesionales
- Enseñanza, entre otras.

Analizando a detalle los sectores que más aportan al desarrollo socioeconómico del país, se puede destacar que en su mayoría pertenecen a los sectores estratégicos e industrias críticas que se tiene en el Ecuador. Esto se debe, a que en los sectores estratégicos es en donde más existe inversión debido a la rentabilidad que estos tienen, por tanto, el retorno de la inversión generalmente suele ser mayor al invertido.

5. Metodología

5.1. Repercusión de los ataques informáticos

El propósito de los ataques cibernéticos es intentar vulnerar cualquier sistema digital mediante el uso de herramientas informáticas que aprovechan aperturas en la seguridad del sistema para lograr acceder a los datos confidenciales de algún individuo u organización.

En el capítulo anterior se examinó los diferentes tipos de ataques a los que están expuestos los sistemas de seguridad de las distintas empresas, los cuales en su mayoría buscan infiltrarse en el tráfico interno, para obtener información o afectar al sistema directamente.

En adición, también se pudo constatar que el principal objetivo de los distintos ataques era conseguir información para exigir, mediante algún tipo de extorsión o chantaje, una compensación económica para no revelar los datos confidenciales de la empresa. De esta manera, el atacante puede utilizar la información de alto valor, como garantía para conseguir lo que demande.

Según la Dirección Nacional de Ciberseguridad de los Estados Unidos, se documenta que "dentro de los daños sufridos por un ataque informático, los ciberdelincuentes extorsionan a las empresas con compensaciones económicas que oscilan entre 0,7% a 5% de sus ingresos anuales". Además, también se menciona que los daños que pueden ocasionarse por la filtración de los datos confidenciales pueden ser 7 veces mayor al exigido en el chantaje por el atacante (Vecchia, 2022).

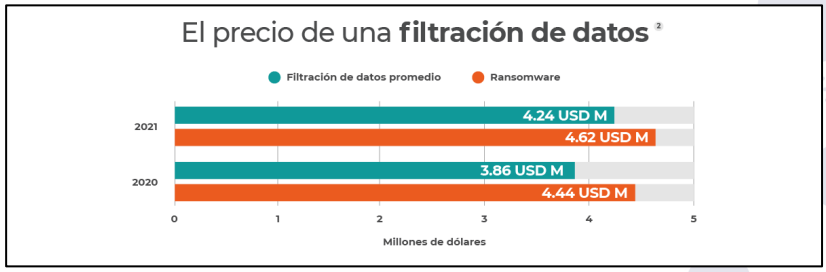


Fig. 3: Comparativa entre el valor a pagar por la filtración de datos.
Fuente: LUMU.

Así mismo, con base al Reporte de Seguridad de la compañía ESET, que examina el estado de ciberseguridad de las empresas en latinoamérica, se ha determinado que la mayor preocupación de las empresas es la infección por códigos maliciosos, puesto que se han reportado incidentes relacionados a malware que roban información confidencial (ESET, 2022).

Este tipo de amenazas cada día están en crecimiento debido a su efectividad, siendo el robo de información uno de los principales objetivos de los hackers o de otras compañías e incluso de gobiernos, con el fin de perjudicar a sus víctimas. Además del robo de

información, existe otro riesgo documentado que está muy presente dentro de las instalaciones de la empresa, el cual es el acceso indebido a los sistemas. Referirse a la Fig 4.

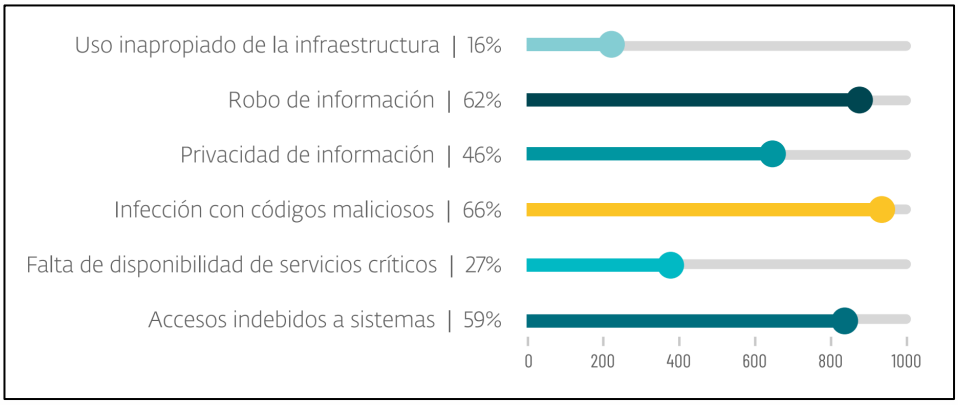


Fig. 4: Principales preocupaciones de las empresas de America Latina en terminos de seguridad.
Fuente: Reporte de Seguridad de ESET (ESR).

Del mismo modo, dentro de un ataque también pueden verse involucrados otro tipo de factores como el social o el psicológico, debido a que un ataque también puede utilizarse para causar pánico en la sociedad o para difundir información fraudulenta que la sociedad puede interpretarla como verdadera, causando conmoción en una población. De esta manera se puede lograr desequilibrar o desestabilizar la organización de un grupo de individuos e incluso a una nación.

Por tanto, también puede presentarse la situación en donde los atacantes busquen vulnerar el sistema de seguridad de la empresa no solo para obtener una compensación monetaria, si no para causar o difundir pánico dentro de la empresa o en el caso de que la empresa preste algún servicio, infundir pánico en sus usuarios.

De igual manera, situaciones en donde el objetivo principal es provocar pánico social mediante este tipo de ataques también pueden trasladarse a un país. Por ejemplo: En 2007 en Estonia se suscitó un ataque de este tipo, debido a un conflicto de ideologías se optó por retirar la estatua de una figura ilustre para el régimen comunista, por lo que como respuesta por tal acción contra el gobierno estonio, se lanzaron diversos tipos de ciberataques, como DoS, DDoS, Defacement, etc; este último permite reemplazar imágenes en sitios web, por lo que, los atacantes rusos intercambiaron imágenes de los sitios web gubernamentales estonios causando conmoción social en los habitantes, que resulto en una crisis interna (Schmidt, 2014).

Con base a la situación anterior, se puede inferir que otro propósito de un atacante es buscar infundir miedo o desesperación dentro de un grupo de individuos por medio del apoderamiento de plataformas digitales o denegando servicios; esto con el fin de causar conmoción social para hacer más vulnerable a la población para poderla manipular, de esta manera el atacante puede aprovechar tal estado de conmoción para extorsionar a sus

víctimas y obtener algo a cambio (Dinero, Información Personal, Datos Confidenciales, etc.).

Debido a esto, la mayoría de los ataques cibernéticos se centran en la ingeniería social, la cual se enfoca en emplear técnicas psicológicas para manipular el comportamiento humano, animando a las víctimas a actuar en contra de sus intereses o de los intereses de su organización (Avast, 2023).

Por tal motivo estos ataques son los más utilizados cuando se requiere obtener información confidencial sin levantar sospechas, puesto que, aprovechando el elemento humano de una organización, un atacante puede obtener acceso a su sistema sin la necesidad de lanzar ataques directos, puesto que la misma víctima es la que proporciona las credenciales de acceso al atacante.

Si se traslada tal situación en la que un atacante obtiene acceso a las plataformas digitales más importantes de un país como Bancos, Industrias, Registro Civil, Sistemas de Salud, Refinerías, etc.; sería un escenario desastroso puesto que el atacante tendría acceso a infraestructuras que sostienen la economía de una nación y la estructura de toda la sociedad.

No obstante, a pesar de que los ataques de ingeniería social como: Phishing, Spear Phishing, Vishing, Smishing, Whaling, Baiting, etc.; son altamente efectivos para traspasar los sistemas de seguridad de una empresa y obtener información confidencial, la realidad es que son solo son una parte del proceso de recopilación u obtención de información que usan los atacantes; y este se puede ver evidenciado en el reporte de ESET, en donde se documenta que algunos de los incidentes más comunes que se suscitan en una empresa son: Rasomware, Spyware, y Troyanos.

Actualmente muchas empresas e incluso gobiernos, han empezado a realizar transacciones mediante criptodivisas, las cuales a pesar de las diversas ventajas que ofrecen, son susceptibles a ser interceptadas. Adicionalmente por medio de malware, que es introducido en los equipos de las empresas o gobiernos, el atacante tiene cientos de posibilidades para acceder y bloquear las cuentas bancarias y electrónicas para hacerse con todo la información y el capital disponible.

Por tanto, con base a todo lo analizado anteriormente, el éxito de este tipo de ataques, en cualquier nivel, puede conllevar a perdidas sustanciales más allá de las económicas, porque pueden repercutir en todos los sectores de un país, desestabilizando la economía de la nación y provocando pánico social en su población.

5.2. Repercusión de los ataques informáticos en latinoamérica

La llegada a Internet ha permitido la creación de nuevas herramientas que han contribuido con el crecimiento de diversos sectores como Educación, Salud, Industrial, Telecomunicaciones, Comercial, etc.; que son la fuente principal de ingresos de muchos países en el mundo; y latinoamérica no es la excepción. El aporte económico y social debido al empleo de tales herramientas se puede ver reflejado en el incremento de la economía del país (Aumento del comercio en línea, Trámites Burocráticos Agilizados, Manejo de herramientas físicas de forma remota, etc.) y en el impacto social que están han tenido (Redes Sociales, Noticias en Vivo, Acceso a Información en tiempo real, etc.).

Además, con la creciente tendencia actual de disponer de más de dos dispositivos electrónicos como Teléfonos Inteligentes, Tabletas o Computadoras por persona; y el interés en la inversión de los gobiernos del mundo para aumentar penetración de ancho de banda en cada uno de los países debido a la creciente demanda de acceso a Internet; ha permitido que pueda conectarse a esta red global para hacer uso de sus herramientas y aplicaciones. Por el mismo motivo, los ataques cibernéticos también han aumentado exponencialmente, más aún en el período de pandemia que se vivió en el mundo.

Siendo el Internet la actual herramienta predilecta para el crecimiento, y desarrollo tecnológico, social y económico de casi todas las naciones del mundo, es lógico que cada nación intente migrar la mayoría de sus funciones a plataformas digitales para que estas estén disponibles en todo momento y para todo público.

No obstante, del mismo modo en que tanto los usuarios, las empresas y los gobiernos tienen acceso a Internet y son capaces de emplear tales herramientas para brindar o solicitar algún producto o servicio; los atacantes también pueden emplear herramientas para lanzar ataques a través de Internet hacia los diversos portales web que existen en Internet.

Con base al reporte de seguridad de la compañía ESET, se documenta que en latinoamérica, el mayor país con detecciones de ataques informáticos realizados es Perú con un 18%, seguido por México con el 17 %, Colombia con 12 %, Argentina con 11% y Ecuador con 9%. En este mismo reporte, se menciona que la mayor preocupación que se tiene es la infección por códigos maliciosos (Malware) y el robo por información (ESET, 2022).

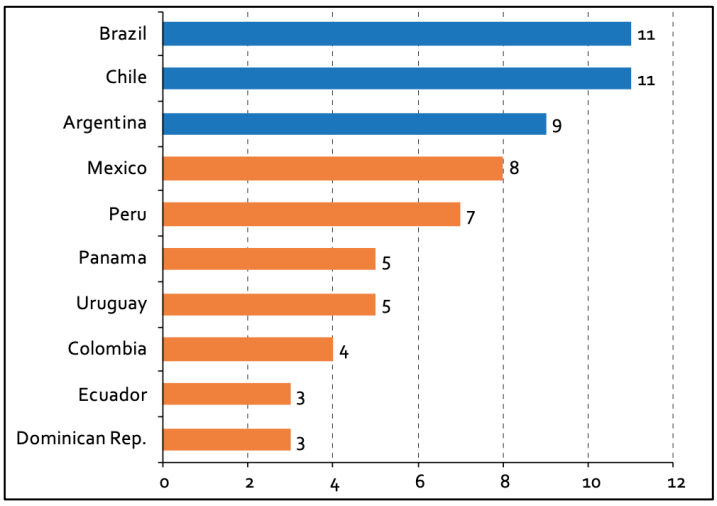


Fig. 5: Número de incidentes causados por ciberataques en latinoamerica.
Fuente: Encuesta realizada por la ECLAC.

El motivo del aumento en los ataques que se han realizado en latinoamérica, no solo se debe al incremento en el número de dispositivos que se conectan a Internet, sino que también guardan relación con la inversión en ciberseguridad, conciencia colectiva, y falta de protagonismo de las empresas públicas y privadas en materia de protección informática.

Según la IEEE, existen 3 razones principales por las que América Latina sufre más ciberataques que otras regiones del mundo: La primera es la falta de organismos de seguridad o de protección informática, las cuales puedan hacer frente a los diversos ataques que se realicen. La segunda razón es la falta de conocimiento por parte de la población y la falta de interés en los gobiernos por informar a la ciudadanía sobre los peligros latentes que existen en Internet sin las debidas medidas de protección. La última razón hace alusión a la carencia de centros de intercambio de información entre las empresas públicas y privadas de un país, esta falta de confianza entre instituciones de distinta índole ha impedido establecer un sistema solido de protección de datos (IEEE Innovation at Work, 2020).

Analizando a profundidad la primera razón, el papel que juega el gobierno en materia de inversión en la seguridad informática de una nación es esencial, debido a la importancia que tienen los datos hoy en día y el peligro que representa que un atacante obtenga tal información, más aún siendo información confidencial.

Este fue el caso de Costa Rica que fue atacada por el Grupo Conti (Banda de Hacker asociada a Wizard Spider) mediante un ransomware en abril del 2022. El ataque comenzó por el Ministerio de Hacienda del país y termino afectando 30 ministerios del país a través de una serie de ataques interconectados. El resultado de este ataque fue la paralización durante meses de parte de la infraestructura digital de Costa Rica, al mismo tiempo que fueron afectados los sistemas de Salud Pública y el Sistema de Pagos a funcionarios públicos. El grupo exigía una compensación económica inicial de 10

millones de dólares, sin embargo, el gobierno costarricense se negó a pagar tal suma, por lo que la paralización de tales servicios durante los dos meses, ocasionaron perdidas valoradas en 30 millones por día (AS/COA, 2022; INTERPOL, 2023).

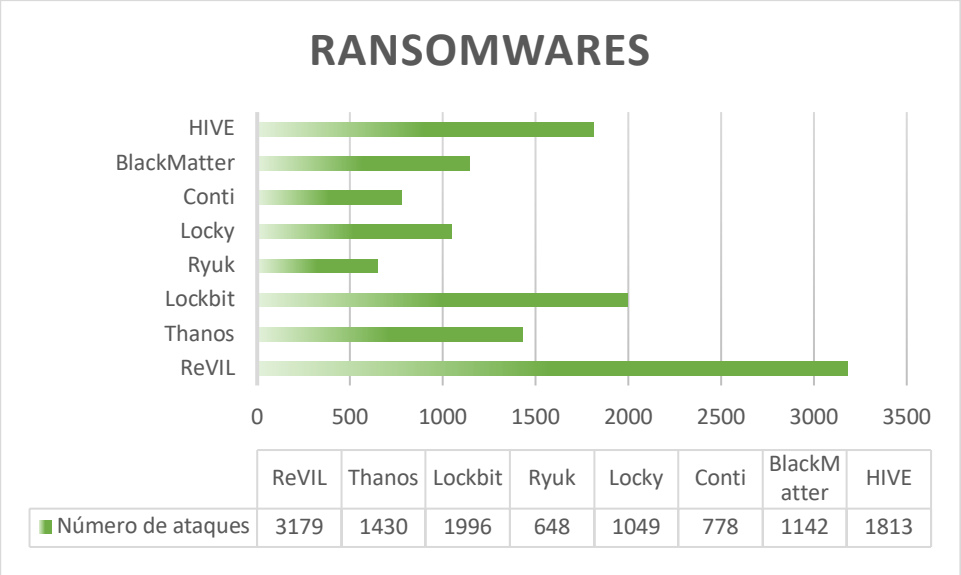
Desde el mismo modo sucedió en Argentina, en donde la empresa proveedora de servicios de Internet "Telecom Argentina" sufrió un importante ataque en el cual al menos de 18.000 equipos fueron infectados con un ransomware. En este ataque se exigía una compensación económica de 7,5 millones de dólares para permitir que se pueda acceder a la base de datos y a las VPN internas (Asif, 2020).

De forma similar en enero del 2022, el senado de Puerto Rico también se vio involucrado en un incidente del tipo ransomware, en el cual se cortó el servicio telefónico y de Internet, ocasionando que su sitio web estuviera fuera de servicio y no se pueda acceder a la base de datos del organismo. Además, en un ataque similar en el 2020, se intentó hurtar 4 millones de dólares mediante una estafa dirigida a las agencias gubernamentales del país, provocando que se congelen 2.9 millones de dólares (Juan Manuel Harán, 2022).

En adición, un caso que causo bastante revuelo fue el de Colonial Pipeline en EE.UU. que se suscitó en mayo del 2021, en donde, mediante un ransomware se comprometió el sistema de oleoductos más grande del país, provocando que se tenga que declarar estado de emergencia a nivel nacional. Tal ataque no solo afecto el sistema de transporte de combustible a toda la costa oeste, y desato una conmoción social en toda la región e incluso en el país; si no que, a ojos del mundo, el ataque mostro lo vulnerable que era el sistema de seguridad del principal oleoducto de Estados Unidos y lo fácil que fue acceder a este para controlarlo. En otras palabras, el ataque arruino el prestigio y la imagen corporativa que se tenía sobre la empresa y sobre la seguridad informática nacional en uno de los principales sectores estratégicos como son los hidrocarburos (Kerner, 2022).

Con base a los datos obtenidos de la compañía Fortinet, en donde se menciona que: En años recientes la cantidad de ciberataques a países latinoamericanos ha ido en aumento, siendo México el país más afectado con un total de 85.000 millones de intentos de ataques, seguido de Brasil con 31.500 millones, Colombia con 6.300 millones y Perú con 5.200 millones. En total, América Latina y el Caribe han recibido alrededor de 137.000 millones de intentos de ciberataques (Fortinet, 2022).

Además, en este mismo estudio se explica que la mayor amenaza en cuestión de ciberataques son los ransomware, los cuales, en palabras de Alexandre Bonetti, director de Ingeniería de Fortinet Brasil, afirma que: "Están afectando a empresas de diversos sectores, gobiernos e incluso economías enteras, con nuevas variantes que surgen constantemente de la mano de diversos grupos cibercriminales internacionales. Esto se debe a la rentabilidad y atención que este tipo de ataque trae a los criminales, volviéndolos más peligrosos y causando grandes pérdidas financieras y de imagen a sus víctimas" (Fortinet, 2022).



	ReVIL	Thanos	Lockbit	Ryuk	Locky	Conti	BlackMatter	HIVE
Número de ataques	3179	1430	1996	648	1049	778	1142	1813

Fig. 6: Principales ransomware empleados.
Fuente: BNAmericas

Por tanto, del comentario anterior se pueden destacar dos hechos importantes sobre como repercuten los ataques cibernéticos en las empresas: El primero es la compensación económica que los atacantes exigen como chantaje por haber tenido éxito en su intento de vulnerar el sistema de seguridad y obtener acceso a los datos; y el segundo es como el éxito de estos ataques perjudica a la imagen corporativa de una empresa o del país; puesto que expone lo vulnerable que es, la falta de seguridad que existe, el poco interés por mejorar la protección, etc.

A día de hoy los ransomware son la herramienta por elección de los atacantes que hasta se tiene desarrollado un modelo de negocio bien establecido con base en estos, este modus operandi se conoce como "Ransomware-as-a-Service" (RaaS). Según la compañía Fortinet: "Los actores de las amenazas emplean servicios independientes para negociar el rescate de los datos, ayudar a las víctimas a realizar los pagos y arbitrar disputas entre grupos de ciberdelincuentes." (Fortinet, 2022).

5.3. Repercusión de los ataques informáticos en el Ecuador

Como se analizó en el apartado anterior, los ataques informáticos pueden repercutir en muchos de los aspectos de las empresas y de los países, siendo los más afectados: el económico y el social. En los países de latinoamérica en donde el sector de seguridad informática recién está tomando impulso y su nivel de protección aún es bajo (debido a diversos factores que han impedido su desarrollo), ha ocasionado que tales países sean un blanco fácil para los diferentes grupos de hacktivistas que emplean herramientas como Phishing, Spyware, Ransomware (Revisar Fig 6.) para vulnerar sus sistemas, acceder a los datos confidenciales, y con base a esto obtener alguna compensación, ya sea económica o de otra índole.

Al igual que sus países vecinos, el Ecuador también se ha visto involucrado en este tipo de ciberataques, los cuales han tenido un gran impacto dentro de la economía y la ideología. Como se mencionó en el estudio realizado por la IEEE, en latinoamérica se comparten ciertos criterios acerca de la importancia de la seguridad informática y la protección de información digital, puesto que la poca inversión que existe en el campo de la ciberseguridad, combinado con la falta de interés por parte de los distintos gobiernos, ha provocado que tales países se encuentren vulnerables ante este tipo de amenazas; en donde el Ecuador también se incluye dentro de este grupo.

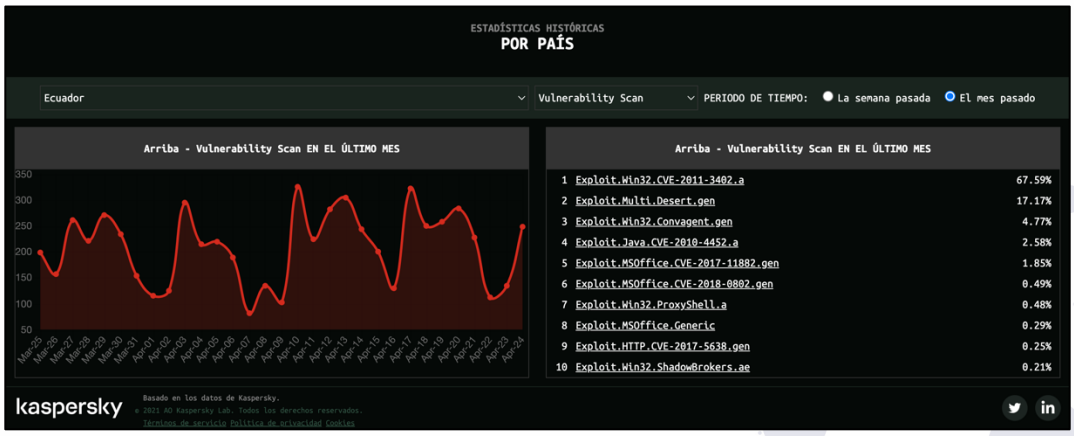


Fig. 7: Vulnerabilidades detectadas en el Ecuador en el periodo Marzo – Abril 2023.
Fuente: Cybermap Kasperky.

No obstante, se debe resaltar el hecho que países como Colombia, México, Perú y Ecuador cuentan con grupos especializados en el campo de la ciberseguridad. Generalmente tales grupos forman parte de alguna rama de las fuerzas armadas de cada país, y su función primordial es la protección informática nacional.

En el Ecuador esta organización se denomina Comando de Ciberdefensa y constituye una sólida barrera contra ciberataques que se realizan de forma interna como externa hacia las infraestructuras críticas y sectores estratégicos de la nación (COCIBER, 2018;

Guerrero & Carlos, 2021). Sin embargo, la falta de inversión por parte del gobierno; y la falta de difusión acerca de la institución y de sus intereses; ha ocasionado que este grupo sea relegado tanto por la ciudadanía como por las demás instituciones. Por tal motivo, tanto empresas privadas como públicas se ven obligadas a invertir de forma independiente en la protección de sus datos y de sus equipos, ya sea mediante el mejoramiento de su infraestructura o por medio de talento humano que se encargue del monitoreo, detección y respuesta frente a los ataques.

Fig. 8: Cibearataques que se detectan en el Ecuador diariamente.
Fuente: Cybermap Kasperky.

En el Ecuador, los sectores estratégicos del país se encuentran bajo el dominio del estado, por lo que el gobierno de turno es el que se encarga de administrar y regular como se emplean los principales recursos en bien de la ciudadanía. Debido a esto, considerando que tales sectores cuentan con plataformas digitales utilizadas para su administración y control, deben tener un nivel de seguridad lo suficientemente robusto para evitar ataques que puedan comprometer su integridad.

Sectores como el financiero, salud pública, hidrocarburos, telecomunicaciones, electricidad, etc.; son fundamentales en el día a día de la ciudadanía y de la estructura del país, por lo que, su protección es esencial para todo el Ecuador. Sin embargo, a pesar de la importancia que supone su protección y el peligro que existe si se llega a vulnerar cualquier de estos sectores, el nivel de seguridad que se tiene en tales infraestructuras no ha sido lo suficientemente robusta para impedir que los atacantes logren acceder a los sistemas de tales sectores estratégicos.

Fundamentando la investigación en los delitos informáticos registrados por la Fiscalía General del estado en el último lustro, se han podido detectar alrededor 10 mil ataques informáticos que han efectuados y que se han podido detectar en las diferentes instituciones del país; esto sin considerar los años 2022 y 2023, puesto que actualmente no se cuentan con registros de ciberataques detectados en estos años (Salazar Méndez et al., 2021). Revisar Tabla 1 y Anexo 2.

Tabla 1: Estadística de delitos ciberneticos registrados

ART. COIP	TIPO PENAL /ARTICULO	2019	2020	2021	Total
188	Aprovechamiento ilícito de servicios públicos	194	99	72	365
190	Apropiación fraudulenta por medios electrónicos	1.744	2.280	3.962	7.986
193	Reemplazo de identificación de terminales móviles		3		3
211	Supresión, alteración o suposición de la identidad y estado civil	54	23	28	105
229	Revelación ilegal de base de datos	34	30	23	87
230	Interceptación ilegal de datos	86	73	35	194
231	Transferencia electrónica de activo patrimonial	50	76	170	296
232	Ataque a la integridad de sistemas informáticos	111	95	86	292
233	Delitos contra la información pública reservada legalmente.	5	5	4	14
234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	242	295	274	811
366	Terrorismo	65	13	17	95
TOTAL GENERAL POR AÑO					10248

Dentro de este tipo de ataques reportados se pueden destacar los ataques de: Apropiación fraudulenta por medios electrónicos y el Acceso no consentido a los sistemas informáticos o de telecomunicaciones; como los más recurrentes a los diferentes sectores estratégicos del país, tales como: instituciones financieras como Bancos y Cooperativas, Empresas de Telecomunicaciones, Sistema de Salud, e inclusive tales ataques han logrado infiltrarse en plataformas gubernamentales, tanto locales (Municipios) como nacionales.

Entre los casos mayormente sobresalientes que ha provocado un impacto social sin precedentes en el Ecuador, ha sido el ataque realizado al Ministerio de Salud Pública en 2023(247 News Agency, 2023; El Universo, 2023; Usuarios Digitales, 2023). El ataque consistió en la filtración de información de la base de datos del ministerio, en la cual se revelaban datos de las personas a las que se les aplico las dosis de vacunas contra el COVID-19. En la filtración se exponen cerca de mil a setenta mil archivos que exponen información sobre:

- Año, mes, día y hora de vacunación
- Punto de la vacunación, su código, distrito, provincia y cantón del mismo.

- Nombres del vacunado, número de cédula, sexo, fecha de nacimiento, nacionalidad, identificación étnica.
- Números telefónicos, correo electrónico.
- Nombre de la vacuna, lote aplicado, cédula del vacunador, antecedentes del COVID.
- Grupo de riesgo, además de en caso de vacunarse en el exterior, el país y fecha.

De igual manera, otro caso de ciberataque que conmociono a la ciudadanía fue el realizado en contra de la Corporación Nacional de Telecomunicaciones CNT, el ISP (Internet Service Provider) más grande del país. Este ataque afecto los procesos de atención del cliente y los call centers. Dentro de la investigación realizada por los peritos de CNT se menciona que el ransomware de la famila RANSOMEXX, no ha comprometido los datos de los usuarios ni de ninguna otra índole(Corral Rosales, 2022; Heimdal Security., 2022).

16-07-21

LA CORPORACIÓN NACIONAL DE TELECOMUNICACIONES EP A LA OPINIÓN PÚBLICA

CNT EP presentó denuncia ante la Fiscalía

El día de hoy, 16 de julio del 2021, la Corporación Nacional de Telecomunicaciones, CNT EP, presentó una denuncia ante la Fiscalía General del Estado por el delito de "ataque a los sistemas informáticos" para que se realice la investigación previa y se determinen responsables.

Este ataque afectó los procesos de atención en nuestros Centros Integrados de Servicio y Contact Center; al respecto indicamos a nuestros usuarios que sus servicios no serán suspendidos por falta de pago.

Debemos informar a nuestros clientes, masivos y corporativos, que sus datos se encuentran debidamente resguardados. También informamos que los servicios como llamadas, internet y televisión, operan con normalidad.

Desde CNT EP contamos con un equipo técnico del más alto nivel profesional, gracias al cual hemos logrado contener la propagación del ataque, implementando las soluciones informáticas necesarias y tomando las debidas medidas de protección.

Trabajaremos de la mano con las autoridades pertinentes para dar con los autores de este delito y estaremos vigilantes, a fin de que los culpables reciban la sanción correspondiente por la alteración del normal funcionamiento de este sector estratégico del Ecuador.

Pedimos a la ciudadanía que por favor se remitan a canales oficiales para resolver y aclarar todas sus dudas.

Cnt

Fig. 9: Anuncio Público acerca del ataque realizado a CNT en 2021.
Fuente: CNT.

Sin embargo, a pesar que este intento de ataque no tuvo mayor repercusión en los sistemas de CNT, la importancia recae en que, siendo el principal centro de datos del país y el principal ISP, tanto usuarios como otras empresas a las cuales ofrecía su servicio, también podían haber sido afectados por los daños colaterales. En organizaciones similares en donde este ataque ha tenido éxito, se ha exigido 11 millones de dólares para evitar difundir la información robada.

En una entrevista realizada a Vadim Avdeev, experto en ciberseguridad, que ha colaborado en conjunto con la inteligencia ecuatoriana para determinar cuáles han sido los factores que contribuyeron al éxito del ataque a CNT; menciona que CNT tiene bastantes falencias no solo en cuestión de sus equipos, que están altamente expuestos a muchos ataques, si no que se debe a la falta de interés de la empresa por mejorar estos aspectos. Sin embargo, tales recomendaciones dadas por el experto, no han sido consideradas por parte de CNT (La Posta, 2022).

Así mismo, otro suceso importante que sucedió a un sector estratégico del país, fue el ataque al Banco Pichincha (el banco más grande del país) en 2021, en donde los cajeros y la aplicación móvil (Banca Web) fueron inhabilitados. Según reportes del sitio web Bleeping Computer, el ataque fue producido por un ransomware que utiliza la herramienta Cobal Strike. A pesar que el ataque como tal no tuvo éxito en penetrar el sistema de seguridad del banco, si causo una fuerte conmoción social entre los usuarios puesto que no podían acceder a sus fondos (Abrams, 2021; Centro de Respuestas a Incidentes de Seguridad Informática, 2021; Superintendencia de Bancos, 2021; WeLiveSecurity, 2021). No obstante, se especula que un usuario llamado Hotarus Corp. Supuestamente pidió un rescate de 30 millones de dólares en Bitcoin para no filtrar tal información (Freedom House, 2022).

De igual forma, en un caso similar ocurrido en las infraestructuras del Banco del Austro en 2016, se menciona que tal ataque costo alrededor de 12 millones de dólares, por lo que, como referencia se puede inferir que el éxito de tal ataque en las inmediaciones del Banco Pichincha tendría un valor similar e inclusive mayor (Sainz, 2019).

Por otro lado, se debe hacer mención que en el país han existido sucesos políticos que han desencadenado ataques cibernéticos y que ha repercutido gravemente en la economía del Ecuador. Tal es el caso de Julian Asange, fundador de Wikileaks, al cual se le había otorgado asilo político en la embajada de Ecuador en Reino Unido.

Según diversos estudios, desde que se concedió el asilo político a Julian Assange, los ataques cibernéticos a instituciones públicas y privadas del Ecuador habían aumentado abismalmente. Además, según declaraciones del excanciller de la Asamblea Nacional José Valencia: Mantener el asilo le costaba al país alrededor de 20 millones de dólares para cubrir aspectos de seguridad, alimentación y medicina. Sin embargo, lo más relevante sobre este caso es que en 2019, cuando el acuerdo de asilo se retiró, el Ecuador recibió más 40 millones de ciberataques a los sitios web del Banco Central, la Presidencia, la Cancillería, el Consejo de la Judicatura, el Ministerio del Interior, el SRI, la Corte Constitucional del Ecuador, gobiernos autónomos, entre otros (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2019).

En consecuencia de estos ataques el Ministerio de Defensa activó un protocolo de seguridad con el propósito de fortalecer la ciberseguridad del país, aunque no se ha dado a conocer los resultados de la aplicación de protocolo ni como era su funcionamiento. El caso Assange ha mostrado a las autoridades que el país no estaba preparado para contener los ciberataques, aunque si existe una tenue legislación, las entidades no están debidamente coordinadas siendo esta una debilidad al momento de aplicar políticas de seguridad. Ecuador también recibió ofertas de ayuda de países como Israel para fortalecer su seguridad informática y el de sus sitios web (Chang, 2020).

Por tanto, dentro de lo que constituye el marco legal en materia de ciberdelitos, la mayoría de los países latinoamericanos aún cuentan con leyes bastante superficiales acerca de cómo se deberían procesar cierto de tipo de delitos y que casos se deberían englobar dentro de las distintas categorías de crímenes informáticos que existen. Esto

sin contar con la ausencia de un plan de seguridad nacional en materia de ciberdelitos y las diferentes políticas de seguridad que se deberían implementar para mitigar tales ataques.

No obstante, con el incremento de ataques informáticos que suceden cada día y con las secuelas de ataques anteriores (los cuales tuvieron su auge durante el periodo de pandemia), han permito que los diferentes gobiernos logren establecer leyes y normativas que regulen y sancionen este tipo de accionares. Además, que este tipo de sucesos han alertado a las diferentes instituciones del país sobre la importancia de establecer políticas que permitan la protección de sus datos y de sus usuarios.

En el Ecuador, en el año 2002 se estableció la Ley de Comercio Electrónico, en la cual se tipifican delitos informáticos referidos a: mensajes de datos, firma electrónica, servicios de certificación, contratación electrónica y telemática, prestación de servicios electrónicos, a través de redes de información, comercio electrónico y la protección a los usuarios de estos sistemas (Salazar Méndez et al., 2021). Revisar Tabla 2 y Anexo 3 donde se detallan los delitos y su sanción.

Tabla 2: Delitos informaticos contemplados en el Codigo Organico Integral Penal del Ecuador

ART. COIP	TIPO PENAL /ARTICULO	Pena Privativa
188	Aprovechamiento ilícito de servicios públicos	6 meses a 2 años
190	Apropiación fraudulenta por medios electrónicos	1 a 3 años
193	Reemplazo de identificación de terminales móviles	1 a 3 años
211	Supresión, alteración o suposición de la identidad y estado civil	1 a 3 años
229	Revelación ilegal de base de datos	1 a 3 años
230	Interceptación ilegal de datos	3 a 5 años
231	Transferencia electrónica de activo patrimonial	3 a 5 años
232	Ataque a la integridad de sistemas informáticos	3 a 5 años
233	Delitos contra la información pública reservada legalmente.	5 a 7 años
234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	3 a 5 años
366	Terrorismo	10 a 13 años

Además, dentro de lo que corresponde a un plan de seguridad de información nacional y políticas de seguridad de la información recientemente el Ecuador ha elaborado la "Estrategia Nacional de Ciberseguridad del Ecuador" que abarca estas funciones (Ministerio de Telecomunicaciones y de la sociedad de la información, 2023). Este plan se fundamenta en 6 pilares fundamentales que son:

1. Gobernanza y coordinación nacional
2. Resiliencia cibernética
3. Prevención y combate a la ciberdelincuencia
4. Ciberdefensa
5. Habilidades y capacidades de ciberseguridad
6. Cooperación internacional

Estos 6 pilares son la base para proteger la soberanía del estado, la protección de las instituciones y la ciudadanía, y para y garantizar que las acciones e iniciativas en materia de ciberseguridad sean holísticas, coherentes y estén en concordancia con los valores

fundamentales compartidos (Ministerio de Telecomunicaciones y de la sociedad de la información, 2023).

A pesar de contar con esta estrategia nacional de ciberseguridad, la cual se debe tomar como guía en todas las instituciones públicas y privadas, y ser difundida en la ciudadanía para fortalecer la seguridad informática en todos los campos; la realidad es que tal estrategia es poco conocida debido a la falta de divulgación por parte del gobierno y las entidades responsables; además sumado al hecho que su elaboración es reciente, tal guía ha sido poco considerada dentro de la sociedad.

6. Resultados

Con base a la información recopilada en la metodología se pudieron obtener tres criterios importes que se deben considerar para determinar cómo han repercutido los ataques informáticos en los sectores estratégicos del Ecuador: El primero es el capital que se pierde a causa de la extorsión y que consecuencias genera tal perdida, el segundo criterio hace alusión al impacto social que produce un ataque y que prejuicios puede ocasionar en una sociedad, y el tercer punto se enfoca en como el Ecuador se prepara frente a este tipo de amenazas y que herramientas tiene para mitigar tales ataques.

Teniendo en cuenta lo explorado en la Tabla 1, se puede apreciar que los delitos informáticos más recurrentes que se registraron en el Ecuador son: Apropiación fraudulenta por medios electrónicos y el Acceso no consentido a los sistemas informáticos o de telecomunicaciones. De esta estadística obtenida se puede determinar que más allá de la incidencia en este tipo de ataques, es que el objetivo principal recae en el apoderamiento de los datos por medio de la infiltración a equipos informáticos, ya sea de las empresas o de los usuarios, lo cual puede emplearse con muchos fines malintencionados.

Partiendo de este apartado se puede determinar que el mayor bien actualmente son los datos de cualquier individuo, organización o sociedad. Esto no solo se debe al valor que tiene tal información por su confidencialidad, sino porque su adquisición por parte de agentes externos de forma no autorizada podría significar que se le puede poner un precio, a cambio de su rescate o para seguir manteniendo su confidencialidad.

Por tanto, analizando a fondo el ataque realizado a CNT, se puede deducir que, siendo el principal proveedor de servicios del país, el mayor centro de datos del Ecuador y una de las pocas instituciones que cuenta con acceso a fibra óptica transoceánica que conecta al Ecuador con el resto del mundo, en caso de que sus infraestructuras se vean comprometidas, los atacantes podrían obtener datos personales de los cientos de miles de usuarios del ISP e información confidencial relacionada a la empresa y sus aliados estratégicos; apoderamiento de los servicios ofrecidos por la empresa, control sobre los servidores que maneja CNT, entre otros.

Este escenario puede ocasionar que los servicios de comunicación como líneas telefónicas e Internet se deshabiliten, causando pánico en la sociedad debido a la falta de comunicación, e inclusive tales medios se podrían emplear para generar campañas de extorsión hacia los usuarios mediante el chantaje de datos o la filtración de información confidencial de las empresas. Además, el apoderamiento de medios de comunicación puede desencadenar una crisis interna en el país, al controlar lo que se puede o no transmitir.

Considerando la investigación realizada por la Dirección Nacional de Ciberseguridad de los Estados Unidos en donde se menciona que los ciberdelincuentes extorsionan a las

empresas con compensaciones económicas que oscilan entre 0,7% a 5% de sus ingresos anuales y sumado a que, en 2022, CNT reporto ingresos de 470,5 millones de dólares (65% menos de lo esperado); se puede inferir que en caso de éxito en un ataque de extorsión, se podría exigir una compensación económica de alrededor de 23,7 millones de dólares.

Además, como se mencionó en la investigación, CNT brinda servicios de hosting a otras empresas y entidades importantes del país, por lo que, se pueden comprometer otros servicios como transporte, finanzas, comercio, agricultura, etc.; aumento aún más el chantaje económico exigido por los atacantes. En otras palabras, el éxito de un ataque cibernético a las diversas infraestructuras de CNT representaría que el sector estratégico de telecomunicaciones se vería comprometido causando grandes pérdidas económicas para el Ecuador y desencadenando una crisis social interna debido a la falta de comunicación y apoderamiento de los medios.

Agregando otro factor de suma importancia, es que si un atacante logra obtener el acceso a la fibra transoceánica podría desencadenar uno de los mayores ciberataques en la región, pudiendo desembocar en el mayor ciber-terrorismo del país, de América Latina y de Estados Unidos.

De esta manera, no solo la reputación de la empresa se ve afectada, si no que los daños colaterales podrían afectar directa o indirectamente a la estructura socio-económica del país y del mundo, permitiendo que atacantes logren acceder a todos los recursos de otras empresas que se encuentran alojados en las instalaciones de CNT y que su vulneración pondría es riego el estado del Ecuador y otras naciones.

Del mismo modo, el ataque que sufrió el Ministerio de Salud Pública también refleja en como el sector de la salud también puede verse implicado en un caso de ciber-terrorismo y extorsión. La filtración de los datos de la ciudadanía que recibió la dosis de la vacuna contra el COVID-19 expone lo relativamente fácil que es para un grupo de atacantes obtener información confidencial sobre los habitantes de un país. Tal filtración podría representar miles de escenarios maliciosos como por ejemplo la Suplantación de identidad con los datos obtenidos, Extorsiones mediante los números de teléfono, Transferencias bancarias no autorizadas desde las cuentas de los usuarios, entre otros delitos.

Además, según José Ruales, Ministro de Salud del Ecuador, menciona que el presupuesto para 2023 para el Ministerio de Salud Pública será de 3.570 millones de dólares, por lo que en caso de que un atacante intente extorsionar económicamente para evitar filtrar la información obtenida, podrían conseguir una suma cercana a 178 millones de dólares; en la cual tal cantidad está prevista para la contratación de más personal para los hospitales de Duran, Bahía y Pedernales. Por tanto, si un ataque de esta magnitud llega a tener éxito, podría causar perdidas de fuentes de empleo, e inclusive recorte en el presupuesto y en el personal de varios hospitales del país (Edición Médica, 2022).

En consecuencia, tal realidad demuestra como los diversos ciberataques que se han lanzado en el Ecuador han repercutido en la economía nacional, haciendo que las perdidas monetarias asciendan a miles de millones de dólares en distintas entidades públicas y privadas. Inclusive, si se considera que un atacante pudiera apoderarse de alguna plataforma de algún sector estratégico, podría provocar el colapso de la economía del país puesto que tales sectores aportan directamente al crecimiento del PIB. Además, tal acontecimiento podría originar una paranoia colectiva en la ciudadanía debido a los diversos sucesos que pueden acontecer.

Esto sumado a la falta de implementación de mecanismos de seguridad que permitan resguardar y proteger los datos de los usuarios, las empresas y de la nación podría volverse una realidad. Con la poca o nula divulgación de la Estrategia Nacional de Ciberdefensa del Ecuador, sumado con la falta de interés por parte del gobierno de turno por mejorar el estado actual de la seguridad informática del país, no se podría lograr contener una oleada de ataques que se realicen a las diversas infraestructuras críticas que administran y controlan los diversos sectores estratégicos, generando perdidas abismales en la economía y pudiendo desatar un caos interno debido al pánico que tales ataques producen.

Este panorama nacional se interpretaría en que el Ecuador actualmente está expuesto a ser vulnerado por cualquier individuo u organización e incluso país, que tenga interés en apoderarse de nuestros recursos mediante el ataque a sus plataformas digitales que administran, controlan y regulan los sectores estratégicos.

7. Discusión

Los factores más destacables obtenidos de la investigación son el impacto socioeconómico que los ciberataques han generado en el país, y la falta de inversión en el campo de ciberseguridad del Ecuador. Ambos resultados exponen el nivel de inseguridad que existe en materia de seguridad informática y esto se puede evidenciar con base a los diversos casos de éxito en los ataques que han recibido las entidades públicas y privadas del país.

En estudios similares como el de José Enrique Alvarado Chang denominado "Análisis de Ataques Cibernéticos hacia el Ecuador" o el de Robert Vargas Borbúa, Luis Recalde Herrera y Rolando P. Reyes Ch, denominado "Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa"; se pueden evidenciar que los resultados son semejantes al de este estudio, ya que en ambos se llega a conclusiones idénticas, como por ejemplo: la falta de inversión en infraestructura de ciberseguridad por parte del estado y la falta de divulgación de políticas de seguridad en todas las escalas (Enrique et al., 2020; Vargas Borbúa et al., 2017).

No obstante, como algunos puntos diferenciadores de este estudio frente a los antes mencionados, es que este estudio se realizó con datos actualizados de los últimos 5 años. Además, tales estudios evalúan superficialmente el impacto socio-económico que ha tenido en el país, mientras que en este se exponen cifras y ejemplos de las secuelas que han tenido los ataques más relevantes del último lustro. Así mismo, este estudio aborda esta problemática desde una perspectiva técnica que se enfoca directamente en las repercusiones que han dejado los ataques en el país.

Sin embargo, en el presente estudio solo se consideran dos factores, el económico y el social. La investigación se centra en conocer el impacto causado por los ataques en ambos sectores y que repercusiones han dejado, pero no se centra en otros aspectos igualmente importantes como son: Político, Legal, Psicológico, etc.

Además, la falta de información sobre: la cantidad de ataques que se reciben diariamente, las detecciones encontradas en las diferentes entidades del país, las pérdidas económicas a nivel micro y macro y otros parámetros, han imposibilitado evaluar más a fondo como afectan directa o indirectamente al sector socio-económico del país.

Pero, por otro lado, este estudio ha permitido profundizar sobre los casos de ciberataques recientes y cuál ha sido su impacto con el nivel de infraestructura actual. Dicho de otra manera, en este estudio se recopila y analiza los ataques y su impacto en el último lustro y encara el éxito de estos ciberataques con el nivel de seguridad actual que se tiene en el Ecuador, teniendo en cuenta la "Estrategia Nacional de Ciberseguridad.".

8. Conclusiones

Con base a los resultados obtenidos en la recopilación teórica y al análisis realizado, se puede concluir que:

- Las pérdidas a nivel económico del país se podrían considerar alrededor de los cientos de millones de dólares, lo cual representa cifras muy significativas que se pierde por la falta de inversión en infraestructura y capacitación en materia de ciberseguridad y protección de datos.
- Los ataques mayormente recurrentes que se lanzan a plataformas del país son del tipo Ransomware, e inclusive actualmente se han desarrollado modelos de negocios basados en estos como lo es Ransomware-as-a-Service.
- A nivel social, la ciudadanía ignora la importancia acerca de cómo la información y los datos actualmente se han convertido en una moneda de cambio en todo el mundo. Esto sumado a la creciente demanda de Internet en la mayoría de lugares del país han contribuido para que la cantidad de ciberataques exitosos en el país se vea incrementado.
- A pesar de contar con la "Estrategia Nacional de Ciberseguridad" la realidad es que tal política de seguridad informática es muy poco conocida, tanto en entidades públicas y privadas como en la ciudadanía, por lo que su implementación es casi nula.
- Ataques hacia entidades importantes del país como el Banco Pichincha, Ministerio de Salud Pública y CNT han provocado que la ciudadanía desconfié de su seguridad y sus servicios, dañando su imagen y la reputación de tales instituciones.

9. Recomendaciones

Con base a lo analizado en la metodología y las conclusiones obtenidas, se puede recomendar que:

- Se debe impulsar la divulgación de la "Estrategia Nacional de Ciberseguridad" tanto en el ámbito laboral como en el ciudadano, debido a que se debe concientizar a la sociedad ecuatoriana acerca de la importancia de la información y los riesgos existentes.
- A pesar de contar con un organismo de protección informática nacional como el Comando Conjunto Cibernético, este es muy poco conocido por lo que no existe mucha información sobre sus objetivos y funciones. No obstante, tal organismo puede ser esencial para la lucha contra el ciberterrorismo hacia el país. Por tanto, se recomienda que se haga exposiciones acerca de sus funciones y como esta institución está luchando contra los delitos cibernéticos que suceden diariamente.
- Se recomienda aumentar la inversión por parte del gobierno en la mayoría de plataformas digitales gubernamentales, centrándose en reforzar la seguridad informática en las infraestructuras criticas puesto que como se evidencia en este estudio son las más afectas debido a su valor para el país.

10. Bibliografía

247 News Agency. (2023). Alert about vaccine database leak against COVID-19 in Ecuador. *Https://247newsagency.Com*. https://247newsagency.com/technology/154287.html

Abrams, L. (2021). *Cyberattack shuts down Ecuador's largest bank, Banco Pichincha*. Bleeping Computer. https://www.bleepingcomputer.com/news/security/cyberattack-shuts-down-ecuadors-largest-bank-banco-pichincha/

AenorEcuador. (2019). *Sector minería, petróleo y energía*. https://www.aenorecuador.com/certificacion/mineria-e-hidrocarburos

AS/COA. (2022). *LatAm in Focus: Cyber Attacks in Costa Rica Expose a Regional Threat*. https://www.as-coa.org/articles/latam-focus-cyber-attacks-costa-rica-expose-regional-threat

Asamblea Nacional del Ecuador. (2014). *LEY ORGANICA DE RECURSOS HIDRICOS USOS Y APROVECHAMIENTO DEL AGUA*. www.lexis.com.ec

Asif, S. (2020). *Argentina's largest telecom hacked with hackers demanding $7.5 million*. HackRead. https://www.hackread.com/argentina-telecom-hacked-hackers-demand-7-5-million/

ASOBANCA. (2021). *Boletín Macroeconómico*.

Avast. (2023). *Qué es la ingeniería social y cómo evitar estos ataques*. https://www.avast.com/es-es/c-social-engineering#topic-3

Banco Central del Ecuador. (2005). *5. ANÁLISIS DE SECTORES ESTRATÉGICOS 5.1 Sector eléctrico (A junio de 2005) 1*.

Banco Central del Ecuador. (2015). *Sector Minero*. 4.

Cámara de Industrias de Guayaquil. (2012). *Desarrollo de las Industrias Básicas en Ecuador*.

Centro de Respuestas a Incidentes de Seguridad Informática. (2021). *Banco Pichincha sufre ciberataque*. Escuela Politécnica Nacional. https://www.csirt-epn.edu.ec/como-tener/225-ciberataque-banco-pichincha

Chang, orge E. A. (2020). *ANÁLISIS DE ATAQUES CIBERNÉTICOS HACIA EL ECUADOR*.

COCIBER. (2018). *¿Quienes Somos?* https://cociber.ccffaa.mil.ec/quienes-somos/

Corral Rosales. (2022). *CNT suffered "highly sophisticated" cyberattack.* https://corralrosales.com/en/cnt-cyberattack-teleamazonas/

Dirección General de Estudios. (2004). DIAGNOSTICO DEL SECTOR TELEFONICO ECUATORIANO. *Apunte de Economía*, 73.

Edición Médica. (2022). *El Ministerio de Salud tendrá un incremento del 12% a su presupuesto para el 2023*. https://www.edicionmedica.ec/secciones/gestion/ministerio-de-salud-tendra-un-incremento-del-12-por-ciento-a-su-presupuesto-para-el-2023-99959#

El Universo. (2023). *Alertan sobre filtración de base de datos de vacunación contra el COVID-19 de Ecuador* |. https://www.eluniverso.com/larevista/tecnologia/alertan-sobre-filtracion-de-base-de-datos-de-vacunacion-contra-el-covid-19-de-ecuador-nota/

Enrique, J., Chang, A., Juan, T., & Aguirre, B. (2020). ANÁLISIS DE ATAQUES CIBERNÉTICOS HACIA EL ECUADOR. *Revista Científica Aristas*, *2*(1).

ESET. (2022). *Security Report Latinoamerica 2022*.

Fortes, I. A., & Rueda, A. G. (2011). Factores determinantes del desarrollo económico y social. *Fundación Unicaja*.

Fortinet. (2022). *Brazil is the second country that suffers the most cyber attacks in Latin America*. BNAmericas. https://www.bnamericas.com/en/news/brazil-is-the-second-country-that-suffers-the-most-cyber-attacks-in-latin-america

Fortinet. (2023). *¿Qué es un ciberataque y los tipos de ataques en la red?* |. https://www.fortinet.com/lat/resources/cyberglossary/types-of-cyber-attacks

Freedom House. (2022). *Ecuador: Freedom on the Net 2022 Country Report*. https://freedomhouse.org/country/ecuador/freedom-net/2022

Gobierno Electrónico de Ecuador. (2019). *Principales Ciberamenazas en Ecuador*. https://www.gobiernoelectronico.gob.ec/principales-ciberamenazas-en-ecuador/

Guerrero, J., & Carlos, J. (2021). *Ciberdefensa en las Fuerzas Armadas del Ecuador para el 2021*.

Heimdal Security. (2022). *Ecuador's CNT Hit With RansomEXX Ransomware Attack*. https://heimdalsecurity.com/blog/ransomexx-ransomware-impacts-ecuadors-corporacion-nacional-de-telecomunicaciones-cnt/

IBM. (2021). *Seguridad basada en la defensa por capas - Documentación de IBM*. https://www.ibm.com/docs/es/i/7.3?topic=security-layered-defense-approach

IEEE Innovation at Work. (2020). *Three Reasons Why Latin America is Under Cyber Attack*. https://innovationatwork.ieee.org/latin-america-is-under-cyber-attack/

INEC. (2010). *Encuesta de Estratificación del Nivel Socioeconómico*. https://www.ecuadorencifras.gob.ec/encuesta-de-estratificacion-del-nivel-socioeconomico/

INTERPOL. (2023). *Working Group highlights cyber threats across the Americas*. https://www.interpol.int/News-and-Events/News/2022/INTERPOL-Working-Group-highlights-cyber-threats-across-the-Americas

Juan Manuel Harán. (2022). *Ciberataque afecta al Senado de Puerto Rico*. WeLiveSecurity. https://www.welivesecurity.com/la-es/2022/01/28/ciberataque-afecta-senado-puerto-rico/

Kaspersky. (2022). *¿Qué es el ransomware? | Protección contra el ransomware* |. https://latam.kaspersky.com/resource-center/threats/ransomware

Kerner, S. M. (2022). *Colonial Pipeline hack explained: Everything you need to know*. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

La Posta. (2022). Entrevista para La Posta sobre la situación con el hack de CNT. In *Youtube*. https://www.youtube.com/watch?v=aZKSsvkbmf8&t=276s

Martín, P. C. (2011). *POLÍTICA ECONÓMICA: CRECIMIENTO ECONÓMICO, DESARROLLO ECONÓMICO, DESARROLLO SOSTENIBLE*.

MARTÍN, P. J. Z. S. (2019). Análisis de los factores que inciden en el desarrollo socio-económico de Ecuador. Periodo 1989-2018. *Universidad Católica Santiago de Guayaquil*, 7–23.

Ministerio de Telecomunicaciones y de la sociedad de la información. (2023). *Estrategia Nacional de Ciberseguridad del Ecuador*.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2008). *NORMAS CONSTITUCIONALES - SECTORES ESTRATÉGICOS CONSITUCIÓN DE LA REPÚBLICA DEL ECUADOR*.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2019). *Más de 40 millones de ataques al Ecuador neutralizados desde el retiro del asilo a Julian Assange*. https://www.telecomunicaciones.gob.ec/mas-de-40-millones-de-ataques-al-ecuador-neutralizados-desde-el-retiro-del-asilo-a-julian-assange/

Mouna, J., Ben, A. R. L., & Ben, A. A. (2014). *Classification of security threats in information systems*.

Oficina de Seguridad del Internauta. (2018). *¿Qué son los ataques DoS y DDoS?* https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos#

QUEZADA, A. G. A., & PALADINES, E. C. (2009). EVALUACIÓN DE LA TENDENCIA TECNOLÓGICA ACTUAL TANTO EN REDES COMO EN PROTOCOLOS. *Facultad de Ingeniería En Electricidad y Computación*, 190.

Ridaura, M. A. M. (2021). *El estudio del caso Amazon*.

Sainz, I. (2019). Diseñar para divergencias y convergencias. Enfoques del DCG para los procesos de lectura por placer en la Red. *Exploraciones, Intercambios y Relaciones Entre El Diseño y La Tecnología*, 57–79. https://doi.org/10.16/CSS/JQUERY.DATATABLES.MIN.CSS

Salazar Méndez, D. D., Mauricio, M., Maldonado, T., Beatriz, M., & Tapia, R. (2021). *Revista Científica de Ciencias Jurídicas, Criminología y Seguridad FISCALÍA GENERAL DEL ESTADO COMITÉ EDITORIAL*.

Schmidt, A. (2014). *The Estonian yberattacks*.

Shafiullah, K., Noor, M., Kok-Keong, L., & Ayesha, S. (2008). *Passive Security Threats and Consequences in IEEE 802.11 Wireless Mesh Networks*.

Superintendencia de Bancos. (2021). *Acciones de la Super de Bancos frente a Ciberataque de entidad controlada*. https://www.superbancos.gob.ec/bancos/acciones-de-la-super-de-bancos-frente-a-ciberataque-de-entidad-controlada/

Unión Internacional de Telecomunicaciones. (1991). ARQUITECTURA DE SEGURIDAD DE LA INTERCONEXIÓN DE SISTEMAS ABIERTOS PARA APLICACIONES DEL CCITT. *COMITÉ CONSULTIVO INTERNACIONAL TELEGRÁFICO Y TELEFÓNICO*.

Usuarios Digitales. (2023). *¿Debemos tener fe en comunicados que indican que no han sido hackeados?* https://twitter.com/usuariosdigital/status/1633136928324300800?s=20

Vargas Borbúa, R., Reyes Chicango, R. P., & Recalde Herrera, L. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa/ Cyber-defense and cybersecurity, beyond the virtual world: Ecuadorian model of cyber-defense governance. *URVIO - Revista Latinoamericana de Estudios de Seguridad*, *20*, 31. https://doi.org/10.17141/URVIO.20.2017.2571

Vecchia, F. Della. (2022). *Esenciales de Forbes: cuánto dinero perdería una empresa si es víctima de un ciberataque - Forbes Ecuador*. https://www.forbes.com.ec/money/esenciales-forbes-cuanto-dinero-perderia-una-empresa-victima-ciberataque-n15790

WeLiveSecurity. (2021). *Banco Pichincha sufrió ataque informático que afectó parte de sus servicios.* ESET. https://www.welivesecurity.com/la-es/2021/10/14/banco-pichincha-sufrio-ataque-informatico/

11. Anexos

Anexo 1. Ciber amenazas registradas en el Ecuador

N°	Ciberamenazas en Ecuador	Desviación de la clasificación según tendencias internacionales	Ciberamenazas 2018 de la *ENISA
1	Suplantación de identidad	↑	Software malicioso
2	Correo no deseado	↑	Ataques basados en la web
3	Software malicioso	↓	Ataques de aplicaciones web
4	Fuga de información	↑	Suplantación de identidad
5	Amenaza interna	↑	Negación de Servicio
6	Manipulación física/daño/robo/pérdida	↑	Correo no deseado
7	Robo de identidad	↑	Redes de bots
8	Ataques de aplicaciones web	↓	Violación de datos
9	Programa de secuestro de datos	↑	Amenaza Interna
10	Negación de servicio	↓	Manipulación física/daño/robo/pérdida
11	Ataques basados en la web	↓	Fuga de información
12	Violación de datos	↓	Robo de identidad
13	Redes de bots	↓	Minería de criptomonedas maliciosa
14	Minería de criptomonedas maliciosa	↓	Programa de secuestro de datos
15	Espionaje cibernético	→	Espionaje cibernético

Fig. 10: Principales Ciberamenazas del Ecuador.
Fuente: Gobierno Electrónico del Ecuador y NDR Cyber Security.

Anexo 2. Estadística de los delitos cibernéticos registrados en el Ecuador

ART. COIP	TIPO PENAL /ARTICULO	2017	2018	2019	2020	2021[4]	TOTAL
103	Pornografía con utilización de niñas, niños o adolescentes	103	104	81	113	95	**496**
104	Comercialización de pornografía con utilización de niñas, niños o adolescentes	26	9	17	18	15	**85**
173	Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	158	202	165	152	152	**829**
174	Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos	12	14	16	7	7	**56**
178	Violación a la intimidad	1.660	2.062	2.038	1.985	1.346	**9.091**
186	Estafa	13.911	14.268	16.918	18.415	16.272	**79.784**
188	Aprovechamiento ilícito de servicios públicos	102	130	194	99	72	**597**
190	Apropiación fraudulenta por medios electrónicos	959	1.448	1.744	2.280	3.962	**10.393**
192	Intercambio, comercialización o compra de información de equipos terminales móviles	-	-	-	1	1	**2**
193	Reemplazo de identificación de terminales móviles	4	2	-	3	-	**9**
194	Comercialización ilícita de terminales móviles	24	14	7	285	10	**340**
195	Infraestructura ilícita	-	5	7	-	-	**12**
211	Supresión, alteración o suposición de la identidad y estado civil	52	81	54	23	28	**238**
229	Revelación ilegal de base de datos	22	44	34	30	23	**153**
230	Interceptación ilegal de datos	63	41	86	73	35	**298**
231	Transferencia electrónica de activo patrimonial	54	37	50	76	170	**387**
232	Ataque a la integridad de sistemas informáticos	85	86	111	95	86	**463**
233	Delitos contra la información pública reservada legalmente.	14	12	5	5	4	**40**
234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	218	236	242	295	274	**1.265**
366	Terrorismo	12	120	65	13	17	**227**
Total general por años		**17.480**	**18.914**	**21.834**	**23.968**	**22.569**	**104.765**

Fig. 11: Estadística de ciberdelitos registrados en el Ecuador en el último lustro.
Fuente: Fiscalía General del Estado.

Anexo 3. Delitos informáticos tipificados en Código Orgánico Integral Penal (COIP) del Ecuador

	ART.	TIPO PENAL	PENA PRIVATIVA
Pornografía Infantil	103	Pornografía con utilización de niñas, niños o adolescentes	13 a 17 años
	104	Comercialización de pornografía con utilización de niñas, niños o adolescentes	10 a 13 años
Acoso sexual "Grooming"	173	Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	1 a 3 años
Ofertas de servicios sexuales a través de medios electrónicos "Sexting"	174	Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos	7 a 10 años
Delitos contra el derecho a la intimidad	178	Violación a la intimidad	1 a 3 años
Estafa	186	Estafa	5 a 7 años
Aprovechamiento de servicios públicos	188	Aprovechamiento ilícito de servicios públicos	6 meses a 2 años
Apropiación fraudulenta por medios electrónicos	190	Apropiación fraudulenta por medios electrónicos	1 a 3 años
Delitos referentes a terminales móviles y su información de identificación	191	Reprogramación o modificación de información de equipos terminales móviles.	1 a 3 años
	192	Intercambio, comercialización o compra de información de equipos terminales móviles	1 a 3 años
	193	Reemplazo de identificación de terminales móviles	1 a 3 años
	194	Comercialización ilícita de terminales móviles	1 a 3 años
	195	Infraestructura ilícita	1 a 3 años
Delitos contra la identidad	211	Supresión, alteración o suposición de la identidad y estado civil	1 a 3 años
Suplantación de Identidad	212	Suplantación de identidad	1 a 3 años
Revelación ilegal de información en base de datos	229	Revelación ilegal de base de datos	1 a 3 años
Interceptación ilegal de datos	230	Interceptación ilegal de datos	3 a 5 años
Fraude informático y muleros	231	Transferencia electrónica de activo patrimonial	3 a 5 años
Daños Informáticos, Malware, ataques de DoS y DDoS	232	Ataque a la integridad de sistemas informáticos	3 a 5 años
Delitos contra la información pública reservada	233	Delitos contra la información pública reservada legalmente.	5 a 7 años
Acceso no autorizado a sistemas informáticos, telemáticos o de telecomunicaciones	234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	3 a 5 años
Delitos de Terrorismo	366	Terrorismo	10 a 13 años

Fig. 12: Ciberdelitos y su sanción tipificados en el COIP.
Fuente: Fiscalía General del Estado.

Anexo 4. Certificación de traducción del resumen

English Speak Up Center

Nosotros "English Speak Up Center"

CERTIFICAMOS que

La traducción del resumen del Proyecto de Titulación "ANÁLISIS COMPARATIVO DE LOS DIFERENTES TIPOS DE ATAQUES INFORMÁTICOS PERPETRADOS EN SECTORES ESTRATÉGICOS EN EL ECUADOR Y SU REPERCUSIÓN ECONÓMICO-SOCIAL EN EL ÚLTIMO LUSTRO." documento adjunto solicitado por la señorita Alexis Vicente Pardo Sánchez con cédula de ciudadanía número 1104115439 ha sido realizada por el Centro Particular de Enseñanza de Idiomas "English Speak Up Center"

Esta es una traducción textual del documento adjunto. El traductor es competente y autorizado para realizar traducciones.

Loja, 16 de mayo de 2023

Mg. Sc. Elizabeth Sánchez Burneo
DIRECTORA ACADÉMICA

DIRECCIÓN: SUCRE 207-46 ENTRE AZUAY Y MIGUEL RIOFRIO | TELÉFONO: 099 5263 264