UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

Estudio y análisis de ataques informáticos en Ecuador durante el estado de pandemia de COVID-19

AUTOR:

Suastegui Jaramillo, Luis Eduardo

Trabajo de titulación previo a la obtención del título de

INGENIERO EN TELECOMUNICACIONES

TUTOR:

M. Sc. Romero Paz, Manuel de Jesús

Guayaquil, Ecuador

07 de marzo del 2022

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

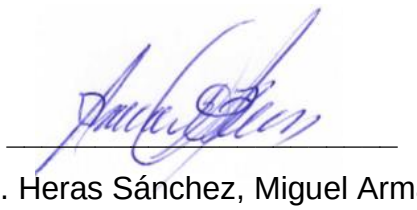
CERTIFICACIÓN

Certificamos que el presente trabajo de titulación fue realizado en su totalidad por el Sr. **Suastegui Jaramillo**, **Luis Eduardo** como requerimiento para la obtención del título de **INGENIERO EN TELECOMUNICACIONES.**

TUTOR

M. Sc. Romero Paz, Manuel de Jesús

DIRECTOR DE LA CARRERA



M. Sc. Heras Sánchez, Miguel Armando

Guayaquil, a los 7 días del mes de marzo del año 2022

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Suastegui Jaramillo, Luis Eduardo**

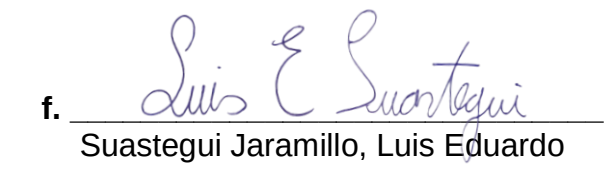
DECLARO QUE:

El Trabajo de Titulación, **"Estudio y análisis de ataques informáticos en Ecuador durante el estado de pandemia de COVID-19"** previo a la obtención del título de **Ingeniero en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 7 días del mes de marzo del año 2022

EL AUTOR

f. 

Suastegui Jaramillo, Luis Eduardo

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Suastegui Jaramillo, Luis Eduardo**

Autorizo a la Universidad Católica de Santiago de Guayaquil a la publicación en la biblioteca de la institución del Trabajo de Titulación, **"Estudio y análisis de ataques informáticos en Ecuador durante el estado de pandemia de COVID-19"**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

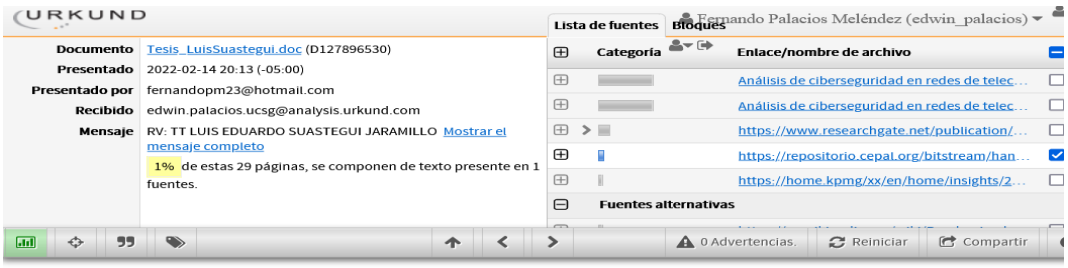
Guayaquil, a los 7 días del mes de marzo del año 2022

EL AUTOR

f. _____

Suastegui Jaramillo, Luis Eduardo

REPORTE DE URKUND



FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

Estudio y análisis de ataques informáticos en Ecuador durante el estado de pandemia de COVID-19

AUTOR:

Suastegui Jaramillo, Luis Eduardo

Trabajo de titulación previo a la obtención del título de

INGENIERO EN TELECOMUNICACIONES

TUTOR:

M. Sc. Romero Paz, Manuel de Jesús

Guayaquil, Ecuador

TUTOR

M. Sc. Romero Paz, Manuel de Jesús

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

M. Sc. ROMERO PAZ, MANUEL DE JESUS

DECANO

f. _____

M. Sc. HERAS SANCHEZ, MIGUEL ARMANDO

DIRECTOR DE LA CARRERA

f. _____

M. Sc. PALACIOS MELENDEZ, EDWIN FERNANDO

OPONENTE

ÍNDICE

Índice de Figuras

RESUMEN

A lo largo del primer trimestre de 2020, a medida que avanzaba la pandemia de COVID-19, se produjeron casi tres millones de ciberataques en América Latina y el Caribe. Solo en marzo de 2020, la incidencia de virus informáticos en la región aumentó en un 131 por ciento en comparación con marzo de 2019. Posteriormente, en febrero del 2021, se da a conocer a la ciudadanía ecuatoriana el primer ataque informático con repercusión nacional, donde por medio de un ataque del tipo “Secuestro de datos” realizado a una institución financiera la información de identificación personal de un gran número de ciudadanos fue expuesta a internet. Este evento puso en evidencia la fragilidad de los sistemas informáticos a nivel nacional e inicia una serie de incidentes informáticos que afectan la confidencialidad, integridad y disponibilidad de los sistemas de comunicación de instituciones públicas y privadas. Este trabajo de titulación presenta un estudio en profundidad de los distintos vectores de ataques usados por los cibercriminales, sus técnicas, tácticas y procedimientos en los distintos incidentes informáticos divulgados públicamente en los tres primeros trimestres del 2021.

Palabras Claves: Ransomware, Malware, COVID-19, Ciberseguridad, Threat Hunting, Respuesta a Incidente

CAPÍTULO 1: INTRODUCCIÓN

1.1 Introducción

La pandemia de coronavirus ha creado nuevos desafíos para las empresas ecuatorianas a medida que se adaptan a un modelo operativo en el que trabajar desde casa se ha convertido en la "nueva normalidad". Las empresas están acelerando su transformación digital y la ciberseguridad es ahora una gran preocupación. Las implicaciones operativas, legales y de cumplimiento podrían ser considerables si se descuidan los riesgos de ciberseguridad.

Las restricciones impuestas por el gobierno y los distintos organismos de salud en respuesta a la pandemia de coronavirus han animado a los empleados a trabajar desde casa e incluso "quedarse en casa". Como consecuencia, la tecnología se ha vuelto aún más importante tanto en nuestra vida laboral como personal. A pesar de este aumento de la necesidad de tecnología, es notable que muchas organizaciones todavía no ofrecen un entorno de trabajo remoto "ciberseguro". Este último punto ha quedado en evidencia debido a los diferentes ataques informáticos que han sufrido las distintas empresas nacionales, tanto públicas como privadas.

1.2 Antecedentes

A medida que el bloqueo global de 2020 se convirtió en una estrategia universal para controlar la pandemia de COVID-19, el distanciamiento social provocó una dependencia masiva al uso de las tecnologías y del ciberespacio, cambiando el mundo hacia la economía digital. A pesar de su efectividad para el trabajo remoto y las interacciones en línea, las alternativas del ciberespacio provocaron varios desafíos a nivel de ciberseguridad. Los cibercriminales sacaron provecho de la ansiedad global y lanzaron ciberataques contra víctimas desprevenidas, poblando rápidamente los buzones de correos electrónicos de una gran parte de la población. De igual modo, muchas de las vulnerabilidades existentes en los

servidores fueron explotadas afectando la confidencialidad, integridad y disponibilidad de la información.

1.3 Definición del Problema

La ciberdelincuencia prosperó durante la pandemia, impulsada por el aumento del phishing y el ransomware. Los ciberdelincuentes recaudaron millones de dólares de las empresas durante la pandemia de COVID-19, utilizando tácticas como el phishing, la ingeniería social y otras herramientas de piratería del sector. Casi el 85% de las filtraciones de datos exitosas involucraron defraudar a humanos, en lugar de explotar fallas en el código de computadora. Aunque las técnicas específicas varían según la industria, el 61% de todas las violaciones de datos son el resultado de esquemas que intentan robar las credenciales de inicio de sesión, como esquemas de phishing.

1.4 Justificación del Problema

Con el estudio y análisis a realizar se desea evidenciar los incidentes de ciberdelincuencia en Ecuador durante el estado de pandemia para ilustrar cómo los actores de amenazas perpetraron fraudes informáticos contra valiosos activos de información. Intentando simplificar los aspectos técnicos de la ciberseguridad y extrae lecciones valiosas de los impactos que los ciberataques COVID-19 ejercen en las redes informáticas a nivel nacional.

1.5 Objetivos del Problema de Investigación

1.5.1 Objetivo General

Realizar un análisis de los tipos y formas de ciberataques que han afectado a las instituciones públicas y privadas en el Ecuador durante el estado de pandemia de COVID-19.

1.5.2 Objetivos Específicos

- Especificar el impacto de los ciberataques acontecidos durante el estado de pandemia de COVID-19 en Ecuador.
- Caracterizar el ciclo de respuesta ante un incidente informático.

- Sintetizar las lecciones aprendidas en cada uno de los incidentes informáticos para establecer mitigaciones de ciberataques durante la pandemia.

1.6 Hipótesis

La hipótesis planteada establece que debido al estado de pandemia de COVID-19 los ciberataques e incidentes informáticos en ecuador tuvieron un incremento notable, tanto en entidades públicas como privadas. Ocasionando un perjuicio en la integridad, confidencialidad y disponibilidad de la información.

1.7 Metodología de Investigación

Los métodos empleados en el siguiente trabajo fueron el descriptivo, documental y analítico, dado que se realizará un estudio de los diferentes incidentes de seguridad registrados en ecuador durante el estado de pandemia de COVID-19, para así poder sintetizar las lecciones aprendidas en cada uno de los incidentes con la finalidad de establecer métodos heurísticos de detección aplicables a ciberataques de la misma naturaleza.

CAPÍTULO 2: FUNDAMENTACIÓN TEÓRICA

Ningún negocio es completamente inmune al riesgo de los ataques cibernéticos y, a medida que avanzaba la pandemia de COVID-19, los patrones y las exposiciones al riesgo cibernético se hicieron más evidentes. Durante la pandemia de COVID-19, las vulnerabilidades se manifestaron principalmente como fallas y debilidades desconocidas que los atacantes aprovecharon para comprometer la privacidad de los datos corporativos y la información personal confidencial.

2.1. Vulnerabilidades y exposiciones

2.1.1. Vulnerabilidades

Una vulnerabilidad es cualquier debilidad o falla en un sistema informático que, si no se resuelve, podría exponer el sistema a peligros potenciales o aumentar los riesgos de posibles ataques cibernéticos, y podría ser explotada por una amenaza para causar daño o consecuencias indeseables. Una vulnerabilidad representa una debilidad en el sistema que es capaz de dar al agente amenazante la oportunidad de comprometer (Paul, 2016) parte o todo el sistema.

Durante la pandemia de COVID-19, las vulnerabilidades se manifestaron principalmente como fallas y debilidades desconocidas en los recursos digitales, lo que planteó diversos niveles de riesgo que los atacantes aprovecharon para eludir el sistema. La forma desesperada y urgente de responder a las intervenciones médicas, sociales y personales de COVID-19 en todo el mundo, generó diferentes tipos de vulnerabilidades en la tecnología, el comportamiento digital (Desk, 2020) y el factor humano, todos de los cuales contribuyeron en gran medida a la tasa alarmante de desafíos de ciberseguridad experimentados en el momento de la crisis.

2.1.2. Exposiciones

Una exposición es una medida de la medida en que una amenaza y una vulnerabilidad pueden combinarse para colocar el sistema en riesgo de ciberataque, lo que lleva a un compromiso o explotación real. De acuerdo

con un estudio realizado por Kaspersky Lab, las vulnerabilidades en Microsoft Office Suite son las más explotadas por los ciberdelincuentes, representando el 72,85 % de las vulnerabilidades en el periodo de pandemia como se muestra en la Figura 2.1. Las razones clave que impulsaron el aumento de los incidentes de ciberdelincuencia en la pandemia de COVID-19 fueron el comportamiento en línea de las personas, la ansiedad por acceder a la información actualizada sobre la enfermedad, así como redes de datos inadecuadamente protegidas, exacerbadas por limitaciones de trabajo remoto sin precedentes (Doffman, 2020).

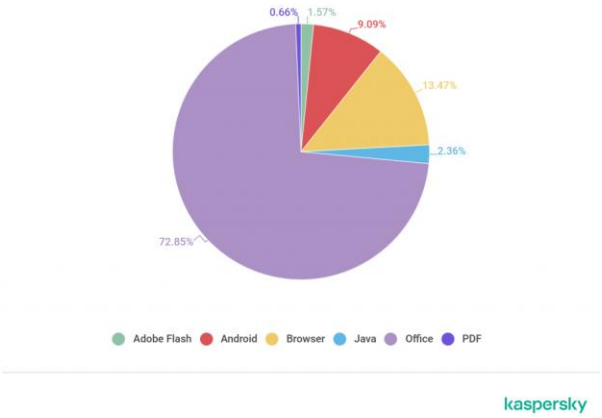


Figura 2.1: Distribución de explotaciones utilizados en ataques informáticos
Fuente: Kaspersky Lab. (2020)

2.1.3. Industrias Expuestas

Si bien la tasa de exposición a las vulnerabilidades de seguridad cibernética fue generalizada durante la pandemia, ciertas industrias y sectores fueron evidentemente más propensos a las violaciones reales de la seguridad de los datos que otros debido a su participación directa en la gestión de los datos de la pandemia o por el valor asignado a la categoría. de los datos que generaron, administraron o tuvieron en custodia.

Las instituciones de salud fueron los objetivos de ataque más vulnerables en términos de los beneficios comerciales para los atacantes y los impactos potenciales que tendría un compromiso. Las instituciones estaban involucradas en la generación, el uso o la gestión de datos confidenciales de atención médica que requerían altos niveles de

confidencialidad y privacidad, lo que los convirtió en activos valiosos y atractivos para los piratas informáticos.

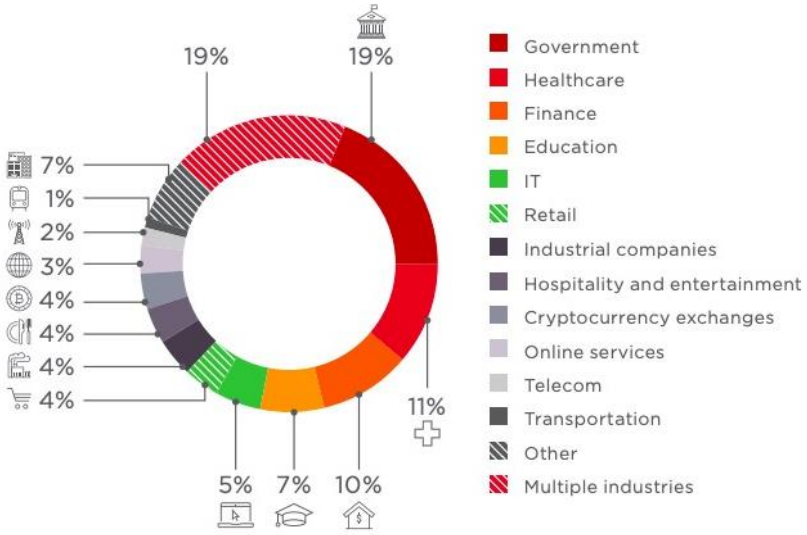


Figura 2.2: Categorías de víctimas entre organizaciones
Fuente: PTsecurity. (2020)

2.2. Vulnerabilidades técnicas y operativas

2.2.1. Sistemas de seguridad obsoletos

La principal vulnerabilidad técnica que los atacantes buscaron para ayudar en sus hazañas durante la crisis fue la aplicación que ejecutaba una versión caducada del sistema de seguridad. Los atacantes identificarían fácilmente dichas aplicaciones durante el reconocimiento previo al ataque. De acuerdo con la cadena de eliminación cibernética de Martin Lockheed (Assante & Lee, 2015), el reconocimiento es un paso indispensable de cada ataque cibernético durante el cual el atacante inspecciona los parámetros del sistema subyacente para detectar puntos vulnerables en el sistema de destino y se toma el tiempo para planificar la mejor manera de explotarlos y posiblemente evadir la detección.

Un sistema de seguridad caducado supone un desafío para sus funcionalidades y un riesgo para las redes en las que opera. Los sistemas de seguridad que tienen licencias no renovadas son incapaces de suprimir amenazas más nuevas y pueden exponer toda la red a mayores riesgos de ataque.

2.2.2. Brecha de capacidad

Como rutina, cualquier deficiencia en la capacidad técnica de la fuerza laboral interna para contrarrestar los delitos cibernéticos plantea un desafío para las organizaciones, especialmente aquellas que dependen de servicios subcontratados para sus operaciones. La creación de conciencia sobre la ética operativa para la seguridad en línea es un componente esencial de la protección del ciberespacio para usuarios individuales y corporativos.

2.2.3. Exposiciones de red y conectividad

Aunque la seguridad de las soluciones de conectividad no es negociable, se sabe que la mayoría de las empresas operan con datos desprotegidos además de prácticas de seguridad de red deficientes, lo que las hace vulnerables a la pérdida de datos (K. U. Okereafor & Adebola, 2020). Las soluciones de conectividad son esenciales para el intercambio eficiente de datos a través de diversas redes informáticas. Sin embargo, las vulnerabilidades relacionadas con la conectividad explicaron la alta tasa de éxito de varias infracciones dirigidas contra aplicaciones de trabajo remoto, como las fallas de seguridad de zoom.

2.3. Amenazas cibernéticas y explotaciones

2.3.1. Amenazas cibernéticas

Por lo general, cualquiera o lo que sea que intente socavar (K. Okereafor & Djehaiche, 2020a) un sistema o servicio digital con intenciones maliciosas se considera una amenaza potencial. El dominio del cibercrimen en la pandemia de COVID-19 se caracterizó en gran medida por amenazas cibernéticas delictivas organizadas. Desde el punto de vista operativo, cada amenaza cibernética aprovecha la presencia de una debilidad del sistema o una vulnerabilidad humana para lanzar un ataque cibernético para obtener una ventaja financiera, obtener un rescate, realizar espionaje, infligir acoso en línea, propagar una ideología, expresar dolor o hacer travesuras.

Los incidentes de COVID-19 mostraron claramente que las amenazas de ciberseguridad están evolucionando a un ritmo rápido y se están volviendo cada vez más sofisticadas (Drugs & Crime, 2020), a menudo con

apariencias que tienden a evadir las técnicas de detección tradicionales (Ferbrache, 2020) y hacen que ganen persistencia en el sistema (K. Okereafor & Marcelo, 2020).

2.3.2. Explotaciones cibernéticas

Lamentablemente, en medio de la crisis de COVID-19, los autores de malware y los ingenieros sociales estaban ocupados explotando la urgencia de la situación para su propio beneficio personal, ya que las ciberamenazas nunca escaseaban. Los ciberdelincuentes aprovecharon la crisis global para lanzar ataques cibernéticos coordinados en redes porosas, particularmente en sistemas dirigidos que albergan vulnerabilidades no mitigadas. Sus actividades y hazañas cibernéticas negaron el acceso rápido tan necesario a los registros de salud, datos médicos, información clínica y datos de laboratorio requeridos por los médicos de primera línea, los cuidadores y el personal de emergencia para responder a las demandas de salud del momento. Esto agravó aún más la situación.

También se atacaron ataques similares contra los activos informáticos y la infraestructura digital de las organizaciones logísticas y los financiadores de la salud involucrados en el traslado de suministros médicos a través de las áreas de necesidad. En la mayoría de los incidentes, las amenazas eran tan sofisticadas como si los piratas informáticos realmente estuvieran cosechando las recompensas del trabajo preliminar que habían establecido y ensayado varios meses antes de que llegara el COVID-19 (K. Okereafor & Adelaiye, 2020).

El malware y las amenazas más dominantes utilizados por los piratas informáticos durante la pandemia fueron ransomware, virus, exploits de ingeniería social, adware, gusanos, caballos de Troya, bombas lógicas, phishing dirigido, ataques de intermediarios, espionaje y acoso cibernéticos.

2.3.3. Malware

Un software malicioso (malware) es cualquier software hostil cuyo diseño es deliberadamente perjudicial y destructivo en su funcionamiento. La

única intención del autor del malware es causar daños y resultados no deseados a su sistema de destino. En el momento en que un malware penetra a su víctima, realiza acciones disruptivas, incluida la alteración y destrucción no autorizadas de los datos, las cuales podrían restringir significativamente la disponibilidad de los datos. La exposición de datos confidenciales resultantes de la acción de malware sigue siendo la ruina de las infracciones de privacidad. Un malware también podría causar un mal funcionamiento impredecible de la computadora.

Los tipos más comunes de malware incluyen virus, gusanos, troyanos, ransomware, bots o botnets, adware, spyware, rootkits, malware sin archivos y publicidad maliciosa.

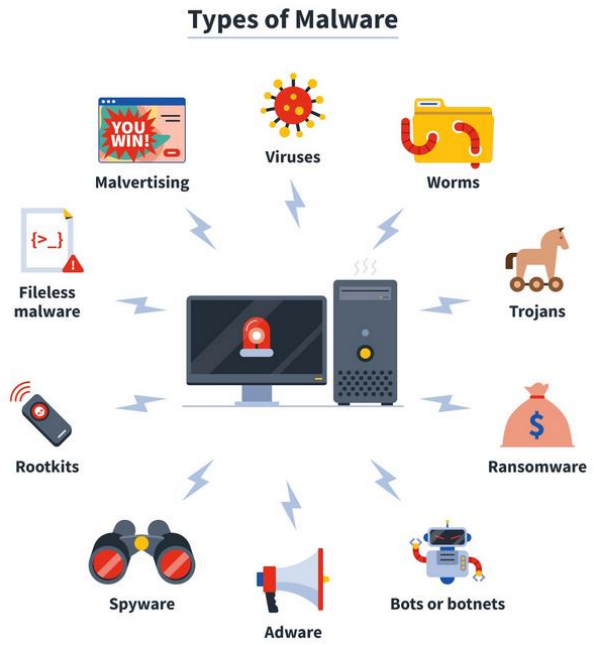


Figura 2.3: Los tipos de malware más comunes
Fuente: Norton. (2018)

2.3.4. Ransomware

Un ransomware es un malware que evita que su víctima acceda al sistema o archivo infectado, bloqueando las funciones de inicio de sesión y cifrando (Ferbrache, 2020) los datos críticos de la víctima, respectivamente (Kurniawan & Riadi, 2018), mientras exige un rescate (Raywood, 2020) dentro de un plazo muy ajustado. El ransomware se dirige tanto a usuarios corporativos como residenciales (Sahi, 2017), y generalmente está

incrustado en un archivo adjunto de correo electrónico o en un enlace de descarga en el que se puede hacer clic, que instala en secreto la carga útil del malware en el fondo del sistema poroso de la víctima desprevenida. Se clasifica como un vector de ataque sofisticado con muchas variaciones y familias (Jadha, 2017).

2.3.5. Virus de computadora

Un virus informático (o simplemente virus) es un malware que altera negativamente la estructura o composición de otros programas informáticos en el sistema afectado y, en el proceso, inserta su propio código destructivo en el nuevo host. Por lo general, un nuevo huésped vulnerable desencadena un virus debido a una defensa deficiente o mecanismos de protección inadecuados.

Durante la crisis del COVID-19, era obvio que la atención de la mayoría de los usuarios del ciberespacio se centraba en las noticias sobre el tratamiento, la cura, la vacuna y la propagación de enfermedades, al punto que cada recurso en línea que pretendía estar relacionado con la pandemia era atractivo y atractivo. casi siempre aceptado como genuino e ingenioso. La desesperación y el pánico global allanaron el camino para que piratas informáticos maliciosos empaquetaran virus informáticos disfrazados de ingeniosas actualizaciones de COVID-19 y apuntaran a sistemas y redes porosas.

2.3.6. Adware y spyware

Un adware (abreviatura de malware publicitario) es cualquier malware que se camufla como un anuncio comercial en línea de un producto, servicio o concepto no solicitado, mientras alberga un código destructivo que puede dañar el sistema en caso de infección. Un spyware es un malware que recopila en secreto información de un recurso digital sobre una persona u organización sin su conocimiento y puede enviar dicha información a otra entidad, tomando el control de la computadora sin el consentimiento del propietario (Jadha, 2017).

2.3.7. Gusano informático

Un gusano informático es un código de malware autoexistente, que se propaga en una red vulnerable al escanear y replicarse a través de los nodos de la red sin necesidad de un activador externo como el que se puede obtener en un virus informático. Una vez que una red se infecta con gusanos, la replicación a todas las partes y componentes porosos de la red comprometida se vuelve inevitable, excepto si se apaga todo el sistema, se aíslan los sistemas individuales y se lleva a cabo una desinfección de seguridad exhaustiva con una herramienta de eliminación de malware adecuada. Estos procedimientos son necesarios en la secuencia correcta para purgar eficazmente el sistema de infecciones por gusanos y garantizar que los códigos de malware no persistan incluso después.

2.3.8. Caballo de Troya

Los piratas informáticos utilizan un caballo de Troya (Machteld, 1984) para instalar en secreto software dañino en el sistema informático de su víctima presentando un recurso disfrazado para parecer inicialmente útil, beneficioso, normal o deseable (Bhargava, 2020). La víctima de un malware de caballo de Troya es engañada por su apariencia inocente en la forma de un enlace de URL en el que se puede hacer clic, un software descargable o un archivo adjunto de correo electrónico inofensivo con una etiqueta pegadiza incluida como arma furtiva de ciberataque.

2.3.9. Spear Phishing

Spear phishing es una amenaza de correo electrónico de seguridad cibernética en la que el atacante envía un mensaje de correo electrónico aparentemente personalizado pero engañoso de una manera inteligente para obtener PII confidencial o datos confidenciales de un objetivo desprevenido, generalmente un destinatario vulnerable de alto perfil como el de una organización. oficial de seguridad, administrador de sistemas, director ejecutivo de la empresa, un trabajador de salud de primera línea, un líder notable en la sociedad o alguien estrechamente relacionado con estas categorías de objetivos.

Es una forma avanzada de la amenaza de phishing simple y más generalizada en la que un pirata informático malintencionado intenta utilizar un mensaje de correo electrónico engañoso y deshonesto para adquirir de manera fraudulenta información confidencial de una víctima, a menudo haciéndose pasar por la identidad de un remitente conocido, frecuente o de confianza. Dichos ataques toman varias formas, a menudo combinan múltiples tácticas para crear la impresión de legitimidad, autenticidad y un sentido de urgencia que requiere una acción inmediata por parte del objetivo.

La técnica de spear phishing es más específica (Cole, 2020) y, por lo general, involucra a los atacantes que realizan una investigación de antecedentes sobre sus objetivos para crear un correo electrónico personalizado o personalizado que parece provenir de fuentes confiables. Es una estafa de suplantación de identidad que utiliza el correo u otras comunicaciones electrónicos para engañar a los destinatarios para que entreguen información confidencial (K. Okereafor & Adelaiye, 2020). Por ejemplo, el campo "De" en un correo electrónico de spear phishing puede contener una dirección de correo electrónico falsa y engañosa, lo que lleva al destinatario a creer erróneamente que el mensaje es de un remitente familiar. El número de intentos de phishing centrados en COVID-19 aumentó en al menos un 400 % (Desk, 2020).

2.3.10. Ataque de hombre en el medio

El ataque Man-in-the-middle, también conocido como ataque de secuestro, es una amenaza de ciberseguridad en la que el atacante intercepta en secreto, se inserta, desvía, altera o interrumpe potencialmente la sesión de comunicación en tiempo real entre dos o más personas o sistemas. que creen que se están comunicando directamente entre sí. El motivo del ataque man-in-the-middle es recolectar información confidencial personal o corporativa, credenciales de inicio de sesión, secretos comerciales, información financiera y otros datos privados para uso inmediato o ataque posterior.

Durante la pandemia de COVID-19, los servicios más susceptibles al ataque man-in-the-middle fueron las videoconferencias, los seminarios web y

las sesiones de trabajo remotas. La compulsión de adherirse a los protocolos y prácticas de distanciamiento social significaba que una fuerza laboral masiva que trabajaba de forma remota (Sahi, 2017) accedería a los recursos de la red e intercambiaría datos en línea con diversos grados de protección, algunos deficientes, otros fuertes y, sin embargo, algunos completamente inexistentes.

La disparidad en la perspectiva de seguridad de las redes impulsó el aumento exponencial en la incidencia de ataques de secuestro, la mayoría de los cuales solo fueron utilizados por los atacantes para obtener información de espionaje relevante para lanzar un ataque mayor, como el fraude de identidad, la escalada de privilegios y el ransomware.

La respuesta al brote de la pandemia dio lugar a un aumento del teletrabajo (E. Berrueta & Izal, 2019) y, a medida que los empleados migraban a sus hogares para trabajar de forma remota, los ciberdelincuentes también se centraron en las vulnerabilidades de los sistemas y redes de teletrabajo para obtener acceso no autorizado a las organizaciones corporativas de todos los sectores. Una técnica particular comúnmente utilizada por los atacantes cibernéticos fue interceptar datos importantes a lo largo de un canal de comunicaciones y realizar cambios en ellos antes de enviarlos al receptor previsto que no está al tanto de la alteración, pero cree que es de una parte confiable. La técnica supuso un gran riesgo para los esfuerzos mundiales por controlar la propagación de la COVID-19, ya que los datos médicos confidenciales sobre la prevalencia de la enfermedad se enfrentaban a la amenaza de ser eludidos por los ciberdelincuentes, que disponían de múltiples herramientas de piratería para infiltrarse en redes porosas e interceptar la transmisión de datos con impactos de largo alcance.

2.3.11. Espionaje cibernético

El espionaje cibernético es el uso ilegal de herramientas automatizadas y redes informáticas para monitorear y rastrear el comportamiento digital o la movilidad física de un objetivo, principalmente con el fin de obtener información confidencial ilícita sin el consentimiento y permiso del objetivo, a

menudo con intenciones o explotación maliciosas. (Ferbrache, 2020), que potencialmente impacta la seguridad nacional o corporativa y la seguridad pública.

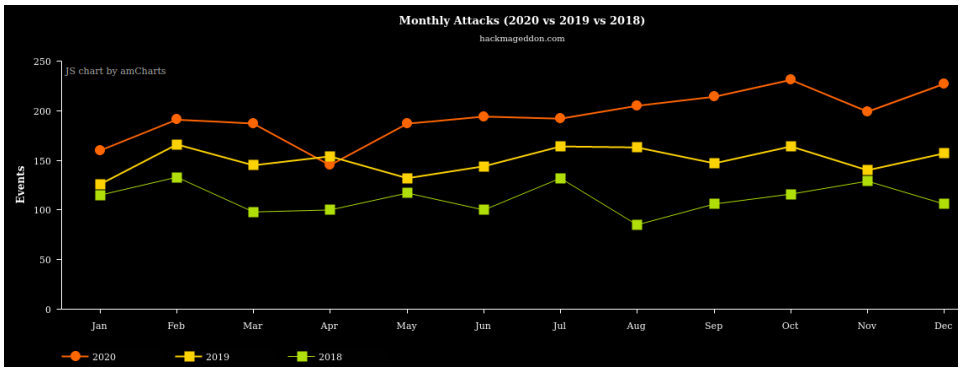


Figura 2.4: Eventos de ciberseguridad registrados en los últimos tres años
Fuente: Hackmageddon. (2020)

Debido a la movilidad restringida impuesta por las medidas de confinamiento por el COVID-19, y especialmente la imposición de restricciones de movimiento, cierre de fronteras y embargo a las reuniones sociales, los piratas informáticos maliciosos vieron la oportunidad de espiar a sus objetivos utilizando herramientas digitales para rastrear tendencias de movimiento, monitorear huellas en línea, intentar el robo de identidad y, en algunos casos, interceptar conversaciones telefónicas y sesiones de videoconferencia, para obtener información confidencial relacionada con una víctima individual, una institución gubernamental, un competidor, un grupo rival o una organización corporativa.

A lo largo de la pandemia, especialmente durante e inmediatamente después del bloqueo masivo, el espionaje cibernético o el reconocimiento malicioso se identificó como un preludio de la mayoría de las brechas de seguridad y, en la mayoría de los casos, sirvió como ayuda para los piratas informáticos, que confiaron en su combinación con la ingeniería social, para recopilar en secreto la inteligencia inicial necesaria para lanzar ataques más coordinados.

2.3.12. Acoso cibernético

El acoso cibernético es el acto de victimizar o acosar a una persona o grupo de personas que usan Internet u otras plataformas en línea, incluidos,

entre otros, correo electrónico, SMS, blogs, foros en línea, redes sociales, etc. La mayoría de los incidentes de acoso cibernético se originan anónimamente ya que el atacante oculta su identidad para evadir el reconocimiento. Ocultándose bajo el anonimato del remitente, la intención maliciosa del acoso cibernético es hacer que la(s) víctima(s) se sienta(n) miserable(s) o torturada(s) psicológicamente al infligir abuso emocional o verbal a través de palabras, imágenes, videos, falsificaciones profundas, animación, grabación de sonido manipulada, voz sintetizada, u otros contenidos que sean insultantes, ofensivos, despectivos, odiosos, abusivos, amenazantes o molestos.

En casos extremos, el acoso cibernético relacionado con las redes sociales desencadena un discurso de odio, al amplificar las teorías de conspiración (K. Okereafor & Marcelo, 2020) a través de la publicación de contenidos obscenos, imágenes indecentes o escepticismo extremo entre culturas, afiliaciones religiosas, inclinaciones políticas e ideologías diversas. Las redes sociales han creado un mundo en el que cualquier individuo puede potencialmente llegar a tantas personas como los principales medios de comunicación, promoviendo así, sin darse cuenta, el antagonismo anónimo utilizando el ciberespacio como campo de batalla de la guerrilla y el ciberacoso como arsenal.

En los casos en los que el acoso cibernético no representa una falsedad absoluta o una calumnia contra la víctima, a menudo propaga el mensaje aparentemente genuino como una burla o ridículo, de manera sarcástica, simplemente para intimidar y perseguir a la víctima.

La pandemia de COVID-19 vio una gran cantidad de acoso cibernético dirigido contra líderes políticos e instituciones influyentes a través de publicaciones electrónicas difamatorias, propaganda en las redes sociales y contenido de audio y video viral anónimo. Las violentas críticas en línea siguieron algunas decisiones precipitadas en el momento del cierre que, inicialmente, ciertos sectores del público consideraron explotadoras o inhumanas. Algunas de las amenazas que se propagaron a través de

correos electrónicos en cadena no solicitados, publicaciones en redes sociales y tweets en línea venían con fuertes sensibilidades emocionales, desprecio y obscenidades.

2.3.13. Ingeniería social

La ingeniería social es el dudoso arte de explotar la debilidad humana para obtener información confidencial o secreta o para obtener acceso no autorizado. Los ciberdelincuentes y los estafadores de Internet utilizan esta técnica de explotación psicológica para recuperar información confidencial que puede reutilizarse para lanzar más ataques.

La mayoría de los fraudes en línea que tuvieron lugar durante la pandemia se centraron en piratas informáticos maliciosos que pudieron manipular a personas inocentes y empleados para que realizaran acciones o divulgaran información confidencial por curiosidad para recibir supuestos incentivos de COVID-19, o en respuesta a la miedo y pánico hábilmente creado por el atacante sobre el tema COVID-19. Estas personas inocentes normalmente son inofensivas y no causarían daño, pero por lo general son engañadas o manipuladas para que hagan algo que normalmente no harían (K. Okereafor & Marcelo, 2020).

A lo largo de la pandemia, los estafadores utilizaron la ingeniería social para manipular hábilmente a las personas y llevar a cabo ataques emocionales dirigidos a las debilidades humanas mediante la ansiedad, el pánico, la desesperación, la urgencia, el miedo, la lealtad, la compasión, la confusión, el respeto, la honestidad, la persuasión, etc. En cada caso, el La ansiedad e incertidumbre que rodeaba la propagación del COVID-19, y la curiosidad creada por el ciberatacante, llevaron a un inusual aferramiento a los sistemas digitales para saber más sobre la situación, proliferando así los incidentes de ataque de ingeniería social. Los ingenieros sociales suelen emplear piggybacking, tailgating, espionaje y shoulder surfing como parte de sus herramientas de engaño.

Muchos ataques cibernéticos relacionados con la ingeniería social de COVID-19 ocuparon titulares sensacionalistas debido al estado de las víctimas, así como a las afiliaciones políticas, diplomáticas y comerciales que representan.

CAPÍTULO 3: ESTUDIO DE ATAQUES INFORMATICOS EN ECUADOR DURANTE EL ESTADO DE PANDEMIA COVID-19

3.1. Antecedentes del COVID-19

3.1.1. Naturaleza

La nueva enfermedad infecciosa, formalmente denominada CoV, pero luego rebautizada como COVID-19 por la Organización Mundial de la Salud (OMS), es una nueva cepa de la familia más grande de coronavirus (CoV) que causa enfermedades que van desde el resfriado común hasta enfermedades más graves como el síndrome respiratorio de Oriente Medio (MERS-CoV) y el síndrome respiratorio agudo severo (SARS-CoV). Antes de la pandemia, la cepa COVID-19 nunca se había identificado previamente en humanos (Paul, 2016). Categorizado como una enfermedad zoonótica, el patógeno del coronavirus se transmite entre animales y personas específicamente a través de patógenos compartidos con animales salvajes o domésticos.

También hay indicaciones novedosas que sugieren que la transmisión aérea (Tilton, 2006) podría ser posible en espacios cerrados y recintos mal ventilados. A la fecha de realizar esta investigación, se están realizando investigaciones para autenticar algunas de estas hipótesis.

Los modos secundarios de transmisión incluyen contactos directos con gotas supervivientes del patógeno del coronavirus que quedan en superficies aisladas o compartidas como escáneres biométricos de huellas dactilares manijas de puertas, teclados de cajeros automáticos, rieles de escaleras, teclados de control de ascensores, carros de compras, billetes, tableros de mesa, telas, cartón y plásticos (Lee & Rotoloni, 2016), papel, botones de maquinaria, monitores de computadora con pantalla táctil, teclados de computadora, botones de teléfono con pantalla táctil, etc.

3.1.2. Origen

El 31 de diciembre de 2019, la Comisión Nacional de Salud de China (NHC) informó a la oficina de la OMS en China de una misteriosa enfermedad respiratoria similar a una neumonía en Wuhan, la capital de la provincia de Hubei, en el centro de China, con una causa desconocida. Más tarde, el 7 de enero de 2020, después de informar previamente a 44 pacientes sospechosos con la misteriosa enfermedad, las autoridades sanitarias chinas identificaron y anunciaron el nuevo coronavirus como la causa del brote (Organizatio, 2020).

Tras el informe de China sobre la primera muerte relacionada con el nuevo coronavirus, un hombre de 61 años con varias afecciones médicas subyacentes el 9 de enero de 2020, el NHC del país compartió más tarde la secuencia genética del nuevo coronavirus con la OMS el 12 de enero de 2020, en el que proporcionó información que podría ayudar a otros países a realizar pruebas y rastrear a las personas potencialmente infectadas.

Aunque existen numerosas teorías contradictorias y no confirmadas hasta la fecha, sobre el origen del virus, una de las cuales afirma que el virus podría haberse originado en otro lugar fuera de China o incluso podría haber existido en todo el mundo sin identificar antes de Wuhan. descubrimiento en diciembre de 2019, la narrativa global más dominante parece asociar el origen de la ola de la enfermedad de diciembre de 2019 con un mercado al aire libre en Wuhan, China. Sin embargo, las opiniones populares en Beijing que no aceptan que el virus se originó en China tienden a argumentar que solo porque el país reportó el virus por primera vez y rastreó muchos de los primeros casos hasta Wuhan, no significa necesariamente que provenga de allí (Organizatio, 2020).

Cuando el virus apareció por primera vez en Wuhan, China, en diciembre de 2019, incluso los expertos en salud pública internacional más experimentados nunca anticiparon que se propagaría rápidamente para crear la peor crisis mundial de salud pública en más de 100 años. La

propagación fue monumental y generalizada, y la mayoría de sus impactos en la civilización son permanentes, incluido su vínculo con la ciberseguridad.

3.1.3. Propagación

El 21 de enero de 2020, la OMS confirmó la transmisión de persona a persona del virus que se había extendido a Corea del Sur (Drugs & Crime, 2020), Tailandia y Japón y había infectado a un total de 222 personas, incluidas las infecciones entre los servicios de salud, trabajadores y cuidadores que tenían un conocimiento mínimo del modo de transmisión de la enfermedad en ese momento.

El 30 de enero de 2020, la OMS declaró el brote como Emergencia de Salud Pública de Importancia Internacional (ESPII) tras su rápida propagación mundial, y el 11 de febrero de 2020, tras la propagación incesante a más países y territorios y la potenciales conspicuos de infecciones más generalizadas, la OMS elevó su estado de emergencia sanitaria a pandemia, y cambió el nombre de la enfermedad a coronavirus 2019 - COVID-19 (K. Okereafor & Marcelo, 2020) en un comunicado emitido por el Director General de la OMS, Tedros Adhanom Ghebreyesus explica que "CO" significa "corona", "VI" para "virus" y "D" para "enfermedad", mientras que "19" corresponde al año, ya que el brote se identificó por primera vez en diciembre de 2019.

Etiquetar el brote como una pandemia intensificó el pánico global, ya que los países comenzaron a tomar medidas para proteger su importación y propagación dentro de sus territorios. La evacuación masiva de ciudadanos se volvió desenfrenada en todo el mundo y abundaban los rumores de cierres inminentes por molestias. En ese momento, el total de estadísticas mundiales de infección según el Informe de situación 22 de la OMS era simplemente de 43.103 casos de 25 países y territorios, y China representaba el 99,083% de esa cifra (Organizatio, 2020).

Debido a su rápida propagación como PHEIC, se especuló que, dependiendo de las medidas de control y otros factores, los casos pueden

presentarse en oleadas de diferentes alturas, con ondas altas que señalan un impacto mayor, ya diferentes intervalos.

3.1.4. Vínculo con la ciberseguridad

Siempre que surge una nueva crisis, los actores criminales suelen ser los primeros en explotar a víctimas inocentes en momentos de miedo, incertidumbre y duda como la pandemia del COVID-19 que provocó tanta ansiedad y pánico en la sociedad y los negocios. Aparte de su impacto extraordinario, la pandemia también generó delitos cibernéticos únicos que afectaron a la sociedad y las empresas.

Irónicamente, mientras los países y territorios estaban ocupados implementando medidas para contener la pandemia, los delincuentes cibernéticos y los estafadores informáticos también idearon estrategias para aprovechar la terrible crisis para infiltrarse en redes de datos porosas y activos digitales, dada la propagación del virus en un estilo típico de incendio forestal. En consecuencia, a medida que el impacto global de la pandemia crecía en medio de una mayor aprensión y angustia emocional, cada recurso en línea que supuestamente estaba relacionado con la enfermedad o la pandemia se convirtió en una fuente de atención, incluso cuando el mundo seguía anticipando una solución duradera, una vacuna o terapia curativa. Desafortunadamente, la angustia emocional de los tiempos difíciles hizo que las víctimas potenciales fueran aún más vulnerables a la explotación del ciberespacio en manos de estafadores en línea y grupos de piratas informáticos.

En medio de la investigación en curso, los ciberdelincuentes se aprovecharon del pánico, el miedo y la desesperación globales para lanzar ciberataques masivos contra sistemas vulnerables y para robar valiosos datos confidenciales utilizando una combinación de correos electrónicos de phishing y técnicas de ingeniería social para propagar las computadoras. virus, ransomware, etc. Las infracciones cibernéticas relacionadas con COVID-19 también incluyeron el acoso cibernético que fue perpetrado desenfrenadamente a través de la difusión de victimización asistida por

computadora, falsificaciones profundas, afirmaciones de los medios sin fundamento y noticias falsas, con los perpetradores escondidos bajo el anonimato de plataformas de redes sociales y microblogs.

El vínculo entre COVID-19 y la seguridad cibernética es que los delincuentes cibernéticos, incluidos los piratas informáticos y los estafadores en línea, sacaron provecho de la pandemia para lanzar ataques informáticos masivos contra víctimas desprevenidas. Robaron identidades e interrumpieron transacciones digitales utilizando versiones sofisticadas de técnicas de ciberataque convencionales que se modificaron específicamente para coincidir con el patrón de vulnerabilidades relacionadas con COVID-19. Los ciberdelincuentes se aprovecharon de la mayor ansiedad de las personas durante la pandemia, utilizaron una combinación de ingeniería social, estafas por correo electrónico de phishing y ransomware, y los engañaron para que hicieran clic y compartieran enlaces que robaban información. Los adversarios simplemente sacaron provecho del entorno pandémico para comprometer y manipular sistemas inadecuadamente protegidos para sus beneficios.

Además, cada nueva estrategia adoptada o implementada para minimizar la propagación del virus o para facilitar la recuperación temprana de los infectados se convirtió en una oportunidad para que los piratas informáticos y los estafadores en línea atacaran sistemas vulnerables y se aprovecharan de los usuarios desprevenidos del ciberespacio. Esencialmente, los ciberdelincuentes explotaron sin piedad los temores del COVID-19.

La despiadada extorsión de las víctimas a través de la vergüenza pública, la victimización y la estigmatización debido a su estado de salud o condición médica demostró aún más hasta qué punto los ciberdelincuentes explotaron la pandemia de COVID-19 para obtener beneficios ilícitos, en cuyo proceso igualmente infligió daño emocional a los usuarios de computadoras cuyos datos fueron robados o sus servicios en línea interrumpidos.

3.2. Roles de ciberseguridad en una pandemia

Desde el inicio, las expectativas sobre la capacidad de la ciberseguridad suelen ser altas para garantizar un ciberespacio seguro, especialmente frente a las interrupciones debidas a la pandemia. Una pandemia por sí sola no detiene ni promueve las actividades de delitos cibernéticos, pero puede desencadenar una cadena de eventos anormales que podrían conducir a oleadas elevadas de delitos cibernéticos. Este escenario de efecto dominó se desarrolló completamente en la pandemia de COVID-19.

Fue el aumento de los casos de delitos cibernéticos lo que finalmente encendió el enfoque en las intervenciones de ciberseguridad, con un énfasis no solo en rastrear los indicadores de compromiso (IoC) sino también en mitigar los impactos de las infracciones cibernéticas tanto como sea posible. En consecuencia, la demanda global de ciberseguridad en las organizaciones y la informática privada ha aumentado significativamente más que nunca, y en los próximos 30 años, la ciberseguridad seguirá siendo la carrera más buscada a nivel mundial (K. Okereafor & Djehaiche, 2020b).

Dado el efecto de la pandemia en el aumento del patrocinio de los servicios y recursos en línea, las expectativas de ciberseguridad eran justificables, desde apoyar la adhesión a la ética del ciberespacio hasta mitigar las filtraciones de datos cuya ocurrencia podría atribuirse a acciones, reacciones e inacciones sociales del estilo de vida, ajustes impuestos para hacer frente a la pandemia en sí. Gran parte de los incidentes de COVID-19 reflejaron los patrones de las personas que comenzaron a trabajar desde casa en cumplimiento de las advertencias de bloqueo o emprendieron algunas acciones reaccionarias perjudiciales mientras se adherían a los requisitos de los protocolos de distanciamiento social.

En primera instancia, el enfoque fundamental de la ciberseguridad nunca pasó de abordar los problemas de protección del ciclo de vida de los datos desde su creación hasta su eliminación. Las expectativas se basaron en la protección integral de datos en los siguientes tres casos:

- De forma proactiva: por ejemplo, mediante el uso de un firewall bien configurado u otras contramedidas preventivas para interceptar los patrones de ciberataques antes de que terminen infiltrándose en la red de datos y eludiendo los activos digitales que conducen a resultados no deseados.
- Instantáneamente: por ejemplo, aplicando un sistema de detección de intrusiones u otras contramedidas de detectives para detectar correos electrónicos no deseados en el momento de su aparición en el servidor de correo, o para identificar otros patrones de tráfico de red hostiles que indiquen un ciberataque.
- De forma retroactiva: por ejemplo, mediante el uso de la gestión de incidentes, análisis forense y otras contramedidas de respuesta para auditar, reconstruir e investigar un incidente después de que haya ocurrido.

Por otro lado, la pandemia creó una oportunidad para que las personas y las organizaciones vean más allá de lo ordinario, examinen sus activos digitales, identifiquen problemas en la red, detecten deficiencias de almacenamiento y sean más conscientes de los impactos de seguridad en su infraestructura. Si bien la gestión del ciclo de vida de los datos era imperativa, los entornos operativos y la naturaleza de la infraestructura dentro de la cual los datos debían ser procesados o transmitidos, respectivamente, requerían mayor atención.

La combinación de estos fue todo lo que se necesitaba para proporcionar una justificación para los roles de prevención, detección y respuesta de la seguridad cibernética en la pandemia de COVID-19.

3.2.1. Rol de prevención

Un papel importante de la ciberseguridad es la prevención de daños potenciales o daños reales a los datos y recursos digitales. Por extensión, esta función incluye la protección de los sistemas de procesamiento de datos, la protección de las personas que administran los datos, así como la

protección del entorno alrededor del cual residen o pasan los datos mientras se procesan.

Durante la pandemia, se anticiparon particularmente los roles preventivos para determinar los riesgos para los datos en línea y la privacidad en varios servicios del ciberespacio a través de una evaluación proactiva del impacto de la privacidad, un rol que sufrió contratiempos peculiares como resultado de las ansiedades e incertidumbres de la pandemia. Tres componentes de la evaluación se enfocaron de la siguiente manera:

- Riesgos reales derivados de las características específicas del sistema o servicio.
- Amenazas existentes por el alcance del servicio.
- Vulnerabilidades en la tecnología empleada y cómo se usa la tecnología.

La ciberseguridad también incluye las mejores prácticas, políticas, estándares y marcos que protegen las aplicaciones y los datos corporativos de ser amenazados por los actores de amenazas. Estos proporcionan orientación para la regulación y protección en múltiples niveles. En el pico de la crisis de COVID-19, justo cuando la prevención de intrusiones en la red tenía una gran demanda, la expectativa era que todas las medidas preventivas preexistentes entrarían en juego para ofrecer funciones superiores de prevención de pérdida de datos (DLP) para prevenir amenazas en diversas formas. Las amenazas anticipadas incluían fraude por correo electrónico, robo de identidad, secuestro de red inalámbrica, ataque a base de datos, denegación de servicio distribuida (DDoS), ataque de intermediario, problemas de comunicaciones remotas, espionaje, etc.

3.2.2. Rol de detección

A menudo se dice en el ámbito de la seguridad que “la prevención es ideal, pero la detección es imprescindible” (Lee & Rotoloni, 2016). Es impracticable garantizar y lograr una prevención absoluta del 100% de las acciones de amenaza debido a muchos factores, incluida la naturaleza

dinámica del panorama de amenazas, además de la superioridad siempre cambiante del poder de ataque del adversario. Por esta razón, un enfoque proactivo estándar en la industria es el uso de sistemas de detección y alerta.

Este fue un enfoque particularmente adecuado y preferido durante la pandemia, dado que las defensas internas de primer nivel no podían garantizarse sustancialmente en circunstancias tan caóticas en las que se hacía mucho hincapié en mantenerse con vida a expensas de mantener la seguridad en línea. Este enfoque requería una identificación de amenazas adecuada utilizando herramientas de seguridad y metodologías de gestión de emergencias para identificar las amenazas de seguridad activas con anticipación. Los piratas informáticos aprovecharon la sensación de urgencia sabiendo que había un tiempo limitado para que las personas actuaran en medio de defensas débiles en redes remotas. La detección proactiva estaba en el centro ya que los ciberataques generalmente siguen pasos específicos para lanzar un ataque, evitar la detección y profundizar en un sistema comprometido (Scroxton, 2020).

En el proceso de atacar un sistema y evadir la detección, el adversario explota procedimentalmente a un usuario vulnerable o un punto final poroso, se oculta y establece una puerta trasera sin dejar de ser lo más sigiloso posible. En una situación ideal, todos los comportamientos anormales del atacante, también conocidos como eventos de interés (EoI) o IoC deben anticiparse, detectarse rápidamente, analizarse y tomarse las acciones adecuadas, pero las peculiaridades de la pandemia comprometen toda adherencia al ideal, por la mayoría de los usuarios.

Las acciones de detección que podrían tomarse en respuesta a EoI e IoC incluyen eliminar amenazas, identificar y remediar fuentes de vulnerabilidades y reparar sistemas a través de parches actualizados. De la misma manera que los sistemas operativos necesitan estar actualizados y completamente parcheados, la seguridad de los endpoints también requiere

actualizaciones automáticas de forma regular (Tilton, 2006) para cumplir con sus funciones de detective.

3.2.3. Rol de respuesta

Las operaciones de ciberseguridad están incompletas sin un plan deliberado para responder a los incidentes, asumiendo que los roles de prevención y detective no pueden detener o identificar amenazas activas debido a un poder de ataque superior.

Los roles de respuesta se activan si tanto la prevención como la detección no pueden interceptar o repeler un ciberataque. Se implementan como soluciones de amenazas para responder al incidente de amenaza resultante mediante la adopción de acciones de mitigación para minimizar la posibilidad de nuevos ataques, reducir su impacto, disminuir su propagación y facilitar la recuperación temprana de dicho desastre. Las soluciones de amenazas aíslan o contienen amenazas utilizando estrategias y herramientas que reducen el impacto de las amenazas de seguridad activas, especialmente aquellas que ya han ido más allá de las defensas de seguridad corporativas y penetraron la red de datos.

Al ejercer estas funciones preventivas, detectivescas y de respuesta, la ciberseguridad ofrece tres categorías de dicha protección sobre los datos, a saber:

- Protección contra el acceso no autorizado a los datos, también conocida como protección de confidencialidad.
- Protección contra la modificación ilegal de datos, también conocida como protección de la integridad.
- Protección contra retrasos en el acceso a los datos por parte de personas autorizadas, también conocida como protección de disponibilidad.

Estas tres categorías de protección de datos se denominan colectivamente tríada CIA por sus siglas en inglés (es decir, confidencialidad, integridad y disponibilidad, respectivamente). La tríada CIA es un modelo

que proporciona dirección para el desarrollo, formulación y mantenimiento de políticas de seguridad de la información dentro de organizaciones corporativas o entre usuarios individuales. Orienta a las organizaciones y personas sobre cómo mantener seguros sus datos confidenciales mientras están en reposo, en movimiento o en proceso. Para evitar confundir el acrónimo del modelo con la Agencia Central de Inteligencia, a veces también se lo conoce como la tríada AIC (es decir, Disponibilidad, Integridad y Confidencialidad).

La tríada de la CIA es muy esencial para brindar protección a los datos a lo largo de su ciclo de vida. La Figura 3.1 muestra la dependencia del ciclo de vida de los datos de la CIA, de la cual los datos obtienen relevancia para la protección en cada etapa.

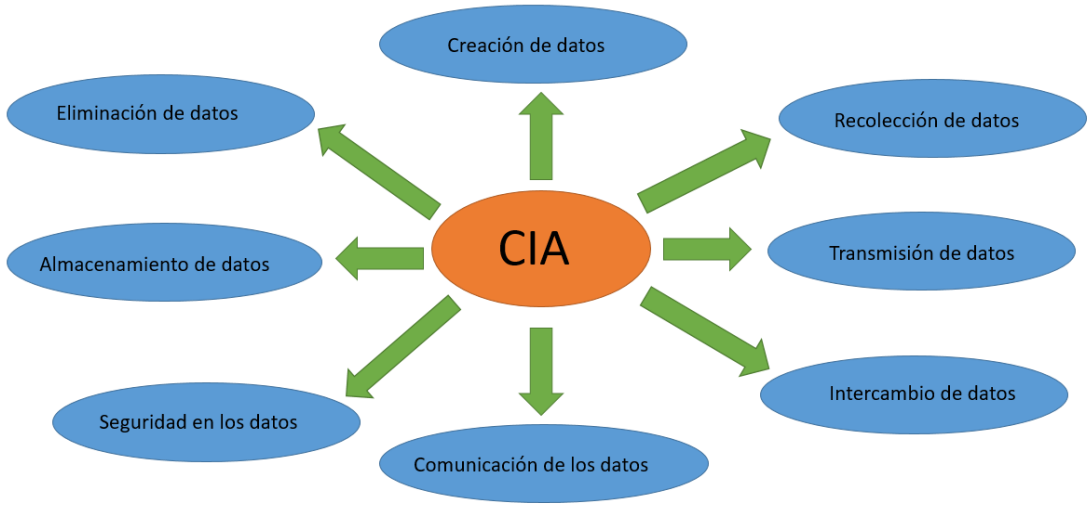


Figura 3.1: Ciclo de vida de los datos protegidos por la tríada CIA
Fuente: Autor

Como las fases del ciclo de vida de los datos se ilustran como grupos que rodean la tríada de la CIA, cada fase depende completamente de la CIA para la protección total.

3.2.4. Confidencialidad de los datos

A medida que avanzaba la pandemia y la información mantenía su dinamismo, los roles de confidencialidad de datos se volvieron cada vez más exigentes como parte integral de la seguridad del ciberespacio y la protección digital. La confidencialidad es la garantía de que las personas

autorizadas no pueden acceder a los datos y que lo que se comunica está a salvo de la divulgación no autorizada, de principio a fin. La confidencialidad deficiente expone datos confidenciales y privados de las víctimas a personas y servicios no autorizados.

Como el aspecto de seguridad más obvio de la tríada de la CIA, la confidencialidad brinda la capacidad de ocultar información de la vista de terceros no autorizados. Es quizás el más atacado, ya que está amenazado por el espionaje y el robo de datos por parte de los ciberdelincuentes. El cifrado proporciona una medida técnica para garantizar la confidencialidad de los datos transferidos de una computadora a otra, oa través de múltiples redes, como Internet.

3.2.5. Integridad de los datos

La integridad de los datos se refiere a la seguridad de que no se modifican de forma no autorizada o por personas y medios no autorizados. El daño a la integridad de los datos fue una gran amenaza para las empresas durante la pandemia de COVID-19, en la que los activos de información electrónica que fueron víctimas de ciberataques sufrieron diversas formas de modificación no autorizada en el contenido y manipulaciones ilegales en su contexto.

La integridad de los datos garantiza que los datos sean una representación precisa de su original, al evaluar si se han visto comprometidos con códigos maliciosos o no autorizados. Cualquier cosa que potencialmente altere la originalidad de la información a través de medios ilegítimos, compromete su integridad. Los verificadores de integridad preservan la privacidad y garantizan el consentimiento al evitar la manipulación o alteración ilegal de los datos.

3.2.6. Disponibilidad de los datos

Se dice que los datos están disponibles cuando son de libre acceso para las partes autorizadas sin demoras, contratiempos ni dificultades. A medida que duró la pandemia de COVID-19, los incidentes aislados de robo

de datos y violaciones de la privacidad llevaron naturalmente a desafíos de disponibilidad. Los ataques de denegación de servicio y eliminación de datos amenazaban la disponibilidad. Por ejemplo, las dificultades de accesibilidad que generalmente se encuentran en un caso de ransomware cuando el adversario bloquea un archivo electrónico, una terminal de computadora o un recurso en línea a través del cifrado a la espera de un rescate mientras amenaza con eliminarlo o exponerlo.

El componente de disponibilidad de la fase de creación de datos se mantiene mediante la adopción de medidas para garantizar que el acceso a los datos no se vea obstaculizado por contratiempos técnicos o relacionados con el sistema, como códigos de recuperación lentos y limitaciones de velocidad de Internet. Desde el punto de vista de la seguridad, es esencial que la información sea fácilmente accesible para la parte autorizada para evitar consecuencias mayores. Por ejemplo, al negar el acceso a un sitio web secuestrado, un grupo de piratas informáticos podría parecer popular o parecer que está propagando una determinada ideología al inculcar un trauma psicológico asociado con el ataque.

3.3. Ataques informáticos en Ecuador durante el estado de pandemia COVID-19

Los impactos potenciales de los ataques cibernéticos en las organizaciones y las personas difieren según una serie de factores (K. Okereafor & Adelaiye, 2020), incluida la intención de los adversarios, su sofisticación y capacidades, su familiaridad con los procesos automatizados, así como la naturaleza y la porosidad del recurso objetivo.

La pandemia de COVID-19 y el aumento de la tasa de ciberataques que invocó tuvieron implicaciones más amplias que se extendieron más allá de los objetivos inmediatos, y muchas de esas implicaciones muestran indicios de perpetuidad. Es la tendencia de permanencia de los impactos de los ataques cibernéticos inducidos por COVID-19 lo que convirtió a algunos de ellos en una fuente importante de preocupación.

Durante la pandemia, las brechas de seguridad cibernética que surgieron de diversas amenazas y exploits tuvieron diversos grados de impacto en individuos, organizaciones, gobiernos, grupos y la sociedad. Era evidente que el aumento de las transacciones en línea abriría vías potenciales para la piratería y otros eventos cibernéticos maliciosos dirigidos a sistemas vulnerables de valor comercial, utilizando correos electrónicos de phishing como herramienta de propagación de malware e ingeniería social como táctica.

3.3.1. Robo de identidad

El robo de identidad y el uso indebido de datos, incluida la divulgación no autorizada y la destrucción de datos, normalmente surgirían como impactos del espionaje cibernético y los ataques de phishing dirigido a la información corporativa expuesta.

A medida que avanzaba la pandemia, y que la adopción de servicios en línea se convirtió en la alternativa ampliamente aceptada para las actividades del espacio de trabajo, el ocio y los negocios en respuesta a los requisitos del protocolo de distanciamiento social, también significó que la exposición y el riesgo de robo de datos confidenciales protegidos inadecuadamente por los estafadores de Internet aumentarían. Los sistemas de trabajo desde el hogar mal asegurados fueron los objetivos de teletrabajo más vulnerables y afectados, en particular mediante el ataque de intermediario a través de la popular variante de bombardeo con zoom.

Los incidentes de interceptación de datos confidenciales que se transmiten a través de canales de telecomunicaciones inseguros y terminales de teletrabajo mal protegidos se convirtieron en el combustible para transacciones bancarias fraudulentas, evaluaciones no autorizadas, ventajas de rescate y arsenal para futuros delitos cibernéticos.

Según la naturaleza y la confidencialidad de los datos corporativos robados, la pérdida de secretos comerciales amenazaba la capacidad de supervivencia de las organizaciones afectadas. Por ejemplo, en el sector de

la atención de la salud, la pérdida o la modificación no autorizada de los registros médicos de los pacientes exponía a los pacientes a riesgos de diagnóstico y prescripción erróneos, los cuales tenían la tendencia a largo plazo de provocar muertes.

Durante la pandemia, hubo impactos de gran alcance en muchos otros sectores, que afectaron las operaciones en el gobierno, las instituciones financieras, el comercio minorista, el comercio electrónico y la hospitalidad.

3.3.1.1. Cibercriminales comprometen banco privado más grande de Ecuador

A inicios del mes de febrero del 2021, un grupo de cibercriminales llamado 'Hotarus Corp' comprometió la seguridad del banco más grande del país, utilizando un ransomware basado en PHP para cifrar un sitio web. Poco tiempo después, los atacantes publicaron en un foro de piratas informáticos la venta de los archivos robados como se muestra en la Figura 3.2, los registros suman más de 6 mil combinaciones de nombres de usuario y contraseñas hash.

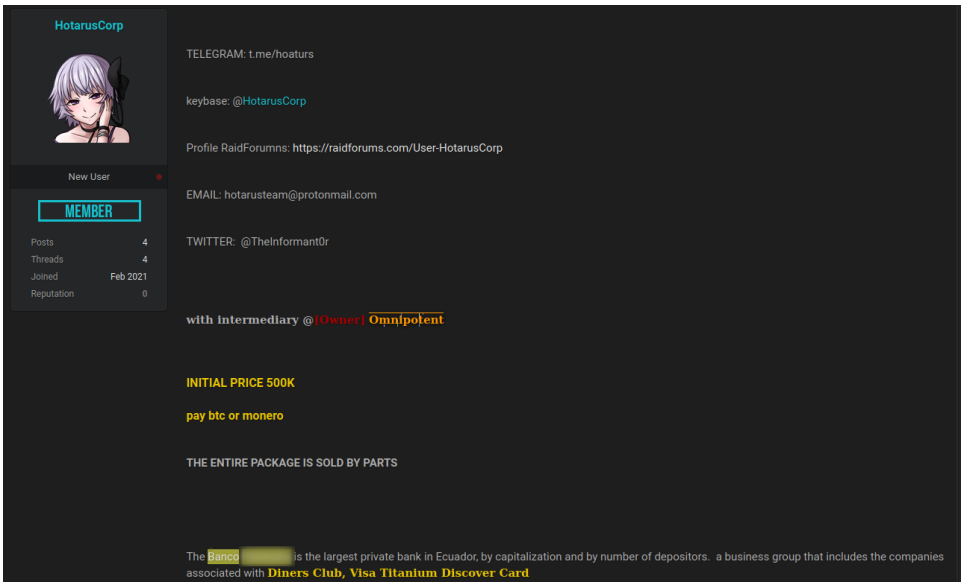


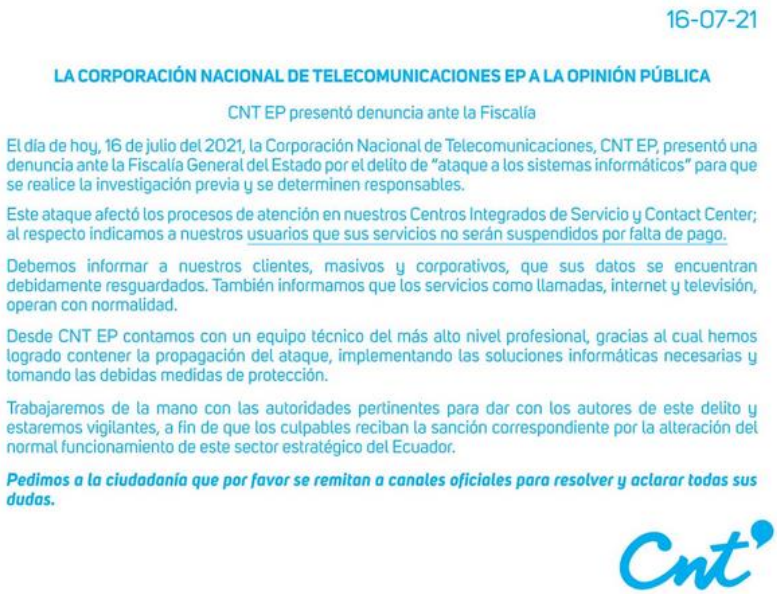
Figura 3.2: Venta de la información robada en foro de piratas informáticos
Fuente: Autor

Muchos servicios del banco se interrumpieron, incluida la banca en línea, la aplicación móvil y la red de cajeros automáticos, muchos clientes

abarrotaron las sucursales bancarias que permanecieron abiertas los días posteriores al ciberataque.

3.3.1.2. Empresa estatal de telecomunicaciones es afectada por ransomware

A mediados de julio del 2021 la Corporación Nacional de Telecomunicación (CNT) estatal de Ecuador sufrió de un ataque de ransomware que interrumpió las operaciones comerciales, el portal de pagos y la atención al cliente como se muestra en la Figura 3.3.



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

Figura 3.3: Anuncio en la web sobre el ciberataque
Fuente: Autor

En el comunicado de prensa de CNT, la compañía afirma que los datos corporativos y de clientes están seguros y no han sido expuestos. Sin embargo, la banda RansomEXX afirma haber robado 190 GB de datos y haber compartido capturas de pantalla de algunos de los documentos en la página de filtración de datos ocultos.

Al igual que otras bandas de ransomware, RansomEXX compromete una red a través de credenciales compradas, las cuales usan para ingresar a servidores expuestos a internet con el servicio RDP abierto. Una vez que obtienen acceso a la red, se propagan silenciosamente por toda la red mientras roban archivos no cifrados para usarlos en intentos de extorsión.

Después de obtener acceso a una contraseña de administrador, implementan el ransomware en la red y cifran todos los dispositivos.

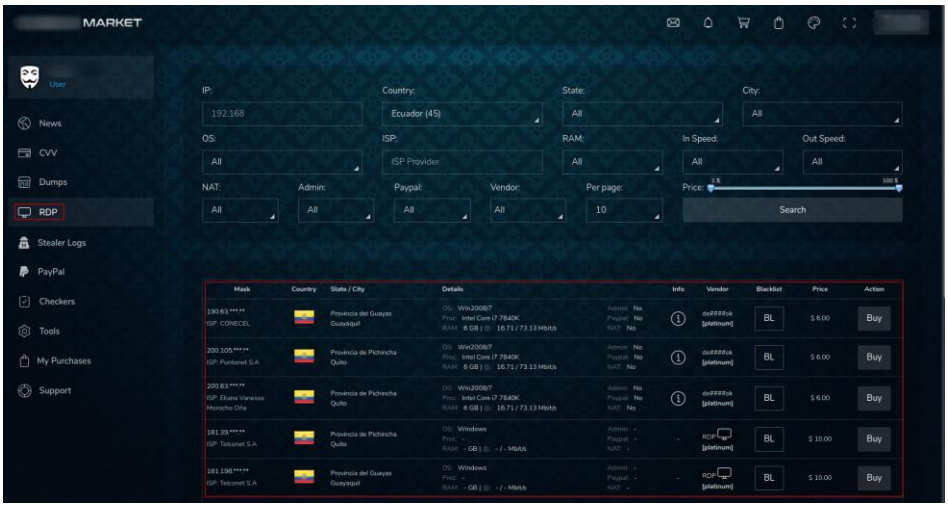


Figura 3.4: Portal web de venta de credenciales RDP robadas
Fuente: Autor

3.3.2. Problemas de privacidad

Las fugas de datos proliferaron durante la pandemia de COVID-19 debido a la proliferación de infracciones cibernéticas debido a redes mal protegidas y sistemas de teletrabajo inseguros que fueron incapaces de prevenir, detectar o responder de manera proactiva al creciente número de amenazas cibernéticas que caracterizaron el período.

Por lo general, los litigios desencadenados por violaciones de la privacidad y la protección de datos pueden ir más allá de la mera difamación, y los litigios civiles ahora dan forma a importantes normas de ciberseguridad (Scroxton, 2020). Esto plantea dudas sobre la propiedad de los datos y la responsabilidad por la responsabilidad después de una inversión de privacidad vinculada a una violación de ciberseguridad.

3.3.3. Ataques del tipo DDoS

Una denegación de servicio distribuida (DDoS) es un ciberataque en el que el atacante sobrecarga deliberadamente el sistema de destino con mucho tráfico de red no válido, p. enviando una gran cantidad de mensajes innecesarios a un servidor, hasta el punto de que supera su capacidad para hacer frente al tráfico legítimo de la red, lo que provoca un mal

funcionamiento, reinicios incesantes o una falla total (K. Okereafor & Marcelo, 2020).

El objetivo malicioso de un DDoS es interrumpir las operaciones normales del sistema haciendo que sus recursos sean inaccesibles y no disponibles para los usuarios previstos y, en el proceso, creando una oportunidad para que el atacante lleve a cabo el robo de información, la alteración de datos o la instalación de código dañino. , entre muchos otros posibles exploits.

Durante la pandemia de COVID-19, hubo varias brechas de seguridad que reflejaron el perfil de los ataques DDoS con impactos negativos en el rendimiento del sistema. La mayoría de los incidentes DDoS se utilizaron en las etapas iniciales de los respectivos ataques para que los servidores críticos y los recursos informáticos se ocuparan con un tráfico innecesario excesivo mientras el exploit no se detectaba (Bhargava, 2020).

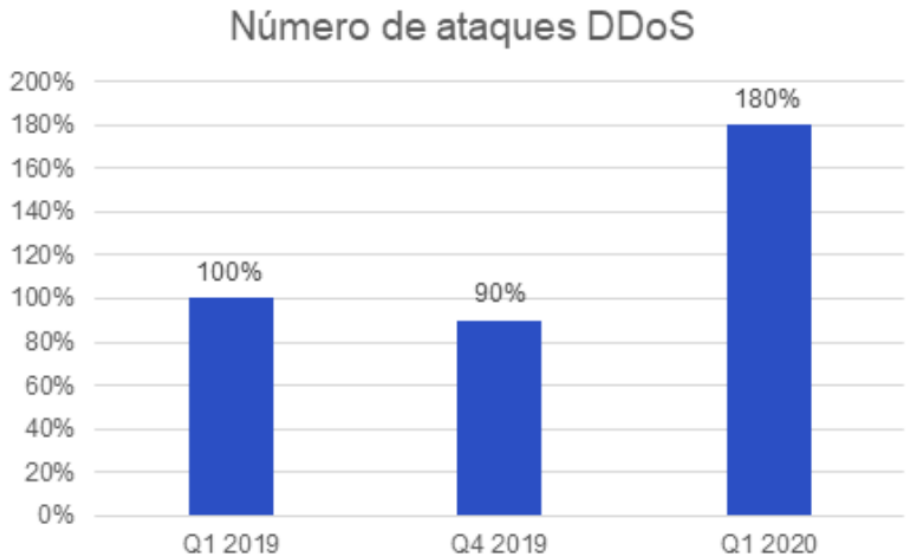


Figura 3.5: Ciclo de vida de los datos protegidos por la tríada CIA
Fuente: Kaspersky Lab. (2020)

Los ataques DDoS generalmente se mitigan utilizando herramientas de seguridad adecuadas que combinan detección con prevención. Los sistemas de detección y prevención de intrusiones (IDS e IPS) detectan automáticamente los patrones que presentan el riesgo de inundar la red con

tráfico innecesario y truncan su progresión de manera proactiva o alertan a un agente humano para una intervención manual.

3.3.4. Problemas de accesibilidad de datos

Las dificultades para acceder a los datos durante la pandemia de COVID-19 dejaron impactos memorables. También planteó preguntas importantes sobre la apertura, el intercambio y el uso de datos en beneficio de contener la propagación del virus, el tratamiento de los pacientes y la toma de decisiones informadas.

Por su propia naturaleza, ciertos tipos de ciberamenazas, en particular ransomware, denegación de servicio y acción de virus, pueden tener un impacto abrumador en los sistemas digitales. Durante la pandemia, esta clase de amenazas inhabilitó aplicaciones vitales, redujo el rendimiento de la red y condujo a redes inoperativas, lo que obstaculizó el fácil acceso a los datos para las organizaciones afectadas (Ferbrache, 2020).

Las redes lentas o inaccesibles que surgieron de las brechas de seguridad representaron una pesadilla para las organizaciones de servicios que dependían de la pronta disponibilidad de datos en el punto de necesidad a lo largo de la cadena de respuesta de COVID-19. El impacto de la inaccesibilidad de los datos podría sentirse cuando los líderes de salud pública que tomaron las decisiones difíciles restringieron el acceso a datos de alta calidad sobre preguntas clave como:

- ¿A dónde es probable que se propague la enfermedad?
- ¿La información meteorológica de dos días respalda las operaciones de vuelo?
- ¿Hay áreas prioritarias que debemos contener para limitar una mayor propagación?
- ¿Cuánto fondo de emergencia necesitamos para adquirir sistemas de soporte vital?
- ¿Dónde están las comunidades más vulnerables?

3.3.5. Pérdida de datos

Todas las hazañas resultaron en pérdidas. El ransomware provocó la pérdida de datos cuando las víctimas se mostraron renuentes a pagar el rescate. El abuso de contraseñas que condujo al compromiso de la cuenta de usuario resultó en el robo de datos e impuso enormes costos en la pérdida de datos. La acción de malware y el espionaje cibernético dieron como resultado la destrucción de datos y la logística impactada que condujo a la pérdida del patrocinio del cliente y la exposición de información confidencial (Doffman, 2020).

3.3.6. Daño a la reputación

La reputación de una organización es un activo preciado y, por lo tanto, nada podría ser tan dañino como el escándalo que sigue a un delito cibernético, especialmente los incidentes de alto perfil que involucran múltiples amenazas y exploits.

En primer lugar, da la impresión inicial de falta de preparación y mala cultura de Ciberseguridad, lo que podría afectar los niveles de confianza de los clientes que han confiado sus datos a la organización en confianza. En segundo lugar, genera sospechas de colaboración interna que pone en grave riesgo la marca, los productos, los servicios y la reputación de la organización y, potencialmente, afecta su competitividad en el mercado. En tercer lugar, los litigios y las investigaciones que siguen a un delito cibernético pueden ser escandalosos y potencialmente revelar secretos ocultos, lo que podría disminuir aún más la credibilidad de la organización (Romagna, 2020).

Para las organizaciones de redes sociales, las empresas de comercio electrónico y las tiendas minoristas en línea, un ataque podría ser tan devastador como tener que comenzar de nuevo para reconstruir la base de datos de clientes y atraer nuevos clientes ofreciendo incentivos costosos a los clientes o socios comerciales en un esfuerzo para mantener las relaciones y retener la lealtad a la marca después del incumplimiento,

situación que podría empeorar si el incidente se repite en una rápida sucesión.

El incidente de Twitter del 15 de julio de 2020, en el que se piratearon varias cuentas de usuarios de alto perfil pertenecientes a Joe Biden, Bill Gates, Barack Obama, Elon Musk y otros 127, creó sospechas en la mente de millones de sus clientes globales, lo que llevó a una disminución casi instantánea del patrocinio del gigante de microblogging y redes sociales, y provocó una caída del 4 % en sus acciones a las pocas horas del incidente (Cole, 2020).

Una brecha en la seguridad de Twitter que permitió a los piratas informáticos acceder a las cuentas de líderes influyentes, magnates de la tecnología y ejecutivos de empresas sacudió la confianza en una plataforma que los políticos y los directores ejecutivos utilizan para comunicarse con el público y, en especial, planteó dudas sobre la colusión interna. En lo que pareció una demostración de desconfianza de alto nivel, el presidente Donald Trump evitó usar Twitter para anunciar la degradación de su director de campaña de 2020, Brad Parscale (Scroxton, 2020) momentos después del ataque, y optó por usar Facebook en su lugar.

En las industrias financiera y de atención de la salud, la pérdida de tarjetas de crédito, credenciales bancarias o registros médicos a través de infracciones de ciberseguridad podría tener un impacto abrumador en la perspectiva general de los clientes y pacientes bancarios, respectivamente, con una mentalidad de desconfianza sobre la seguridad en línea de sus servicios financieros. transacciones y datos médicos confidenciales. La supuesta filtración de unos 230 000 resultados de personas que tomaron la prueba de COVID-19 (Ferbrache, 2020) de la base de datos del gobierno de Indonesia en mayo de 2020 generó preocupaciones sobre la reputación del gobierno en la gestión de los datos de los ciudadanos.

3.3.7. Pérdida de ingresos

Además de los contratiempos no financieros, logísticos y operativos, un ciberataque casi siempre conlleva grandes pérdidas financieras. Tales pérdidas económicas generalmente se distribuyen entre el costo de llevar a cabo las operaciones de respuesta y recuperación de incidentes de ciberseguridad, la pérdida debido a la disminución de los ingresos como resultado de la retirada del patrocinio de los clientes, el costo incurrido por el valor de la información robada o el valor de los datos dañados.

Por ejemplo, en el hackeo de cuentas de alto perfil de Twitter del 15 de julio, las pérdidas comerciales reales y percibidas que surgieron del ataque coordinado de ingeniería social y la estafa telefónica que tuvo como objetivo a algunos de los empleados de Twitter con acceso a herramientas y sistemas internos podrían ha incluido:

- Costo cualitativo de la disminución de la lealtad del cliente.
- Coste de optimizar la concienciación sobre Ciberseguridad entre los empleados.
- Costo de retirar el patrocinio de los socios comerciales.
- Costo de consultoría en respuesta a incidentes informáticos (CIR).
- Costo de reconfigurar los sistemas sospechosos de haber sido afectados por el ataque.
- Costo de instalación de sistemas adicionales de seguridad de protección y detección de anomalías.
- Costo de litigios, investigaciones y remediación.
- Costo de adquisición e implementación de sistemas de predicción de incidentes más inteligentes.

3.3.8. Interrupción del servicio para individuos

A nivel individual, los impactos de un ciberataque podrían ser aún más devastadores para la seguridad en línea de la víctima, especialmente cuando los datos privados han sido expuestos o la información confidencial ha sido comprometida por un hacker malicioso. Los impactos pueden trascender desde la interrupción inmediata de las transacciones en línea

hasta un espionaje cibernético, acoso cibernético y acoso en línea más severos debido a información confidencial que puede haberse filtrado a manos equivocadas.

3.3.9. Escalada del crimen

Como es difícil separar la seguridad física de la Ciberseguridad, el crimen lucha en un ambiente donde la seguridad es inexistente o inadecuada. Hubo deficiencias ambientales aisladas inducidas por COVID-19 que inadvertidamente promovieron el crimen en la sociedad como resultado de las malas garantías de seguridad en los centros de datos físicos y otros activos tangibles. Los casos de ataques de robo en instalaciones informáticas abundaron, ya que los delincuentes aprovecharon la confusión del bloqueo para intensificar los incidentes delictivos.

3.3.10. Fatalidad

Los casos extremos de ataques cibernéticos que implicaron la pérdida o el retraso en el acceso a información crítica que salva vidas entre los centros de salud y las instituciones médicas resultaron en muertes. Dichas muertes se debieron a los efectos de las ciberamenazas que causaron daños o alteraciones no autorizadas de los datos médicos, incluida la PII y la PHI de los pacientes, y provocaron la falta de información o información inexacta para la toma de decisiones rápidas sobre procedimientos de emergencia, administración de medicamentos, hospitalización, y atención al paciente.

CAPÍTULO 4: MITIGACIONES DE CIBERATAQUES DURANTE LA PANDEMIA

La naturaleza y la frecuencia de los incidentes de seguridad cibernética durante la pandemia de COVID-19 requerían un enfoque que brindara múltiples capas de protección para los activos digitales y, sin embargo, ofreciera rendimiento con interrupciones mínimas del servicio. Dado su alcance y sofisticación, solo un modelo de defensa en profundidad podría haber abordado suficientemente su imprevisibilidad.

Un modelo de ciberseguridad de defensa en profundidad es la aplicación simultánea de varias medidas de control a un activo de valor único para optimizar la eficacia. Las medidas de control integran el trabajo de enfoque de defensa en profundidad de manera complementaria, asegurando que en todo momento el activo se encuentra resguardado por dos o más capas de protección para la máxima seguridad.

4.1. Escenario de Defensa en Profundidad

Un servidor de autenticación para la base de datos de identidad electrónica nacional alojada en una máquina virtual remota que está situada detrás de tres firewalls basados en hardware con redundancia en cadena, dentro de un centro de datos con seguridad biométrica que está equipado con sistemas de control ambiental y soluciones de gestión de incendios y conectado a tres servidores de Internet. -frente a las redes, además de estar a cargo de guardias armados de servicio por turnos que rutinariamente reciben información de seguridad y se someten a simulacros de incendio programados en el punto de reunión cada tres días (Kurniawan & Riadi, 2018).

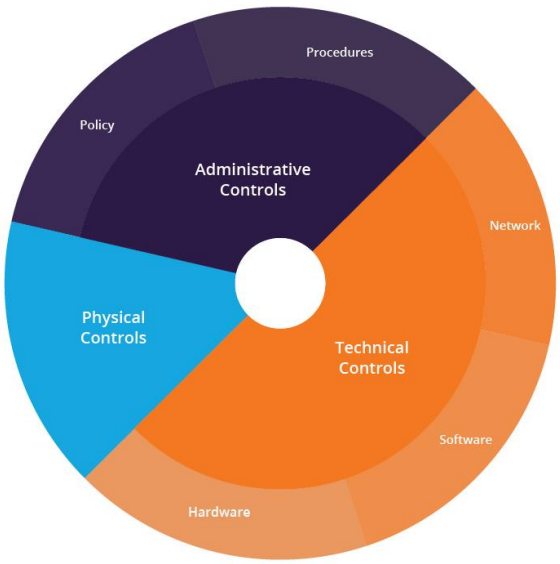


Figura 4.1: Arquitectura de defensa en profundidad: seguridad en capas
Fuente: Imperva. (2020)

4.2. Contramedidas administrativas

Las políticas y directrices técnicas se han convertido en una contramedida fundamental por varias razones. Además de guiar la estandarización de las intervenciones de Ciberseguridad, también realizan un seguimiento de los ajustes de comportamiento de los consumidores digitales en respuesta a la dinámica del ciberespacio, como el aumento digital ocasionado por la pandemia de COVID-19.

Las organizaciones corporativas y otras entidades encontraron consuelo en cumplir con las pautas de ciberseguridad en línea, pero no estaban seguras del origen y la autenticidad de las pautas por temor a ser víctimas de estafas en línea orquestadas. Al abordar los problemas, ya medida que circulaban los avisos de alerta temprana, las organizaciones con tales responsabilidades se esforzaron por emitir directivas apropiadas. En algún momento, la Academia de la Organización Mundial de la Salud lanzó una aplicación móvil para ayudar a las personas a buscar información sobre el COVID-19. La aplicación, que estaba disponible para dispositivos Android e iOS, automatizó los pasos para buscar y obtener información y estadísticas

auténticas de COVID-19 desde una plataforma confiable (Cole & Ring, 2006).

4.3. Contramedidas físicas

Las contramedidas físicas son controles de seguridad que se basan en intervenciones tangibles para proteger los activos. Ya sea que se trate de sistemas de vigilancia CCTV para monitorear áreas restringidas, como un centro de datos de nivel 3 o personal de seguridad armado que protege contra intrusos que usan trampas para hombres, las contramedidas físicas brindan seguridad a nivel operativo e incluyen lo siguiente: máquina biométrica de tiempo y asistencia, perro rastreador , vallado perimetral, credencial de empleado, punto de reunión, supresor de incendios, detector de movimiento, circuito cerrado de televisión, sistema de control ambiental, suelo técnico, bandeja portacables, etc. (Lewandowsky & Cook, 2020).

4.4. Contramedidas técnicas

Las contramedidas técnicas representan los activos de seguridad tangibles utilizados para proteger las redes de datos o los recursos informáticos contra varios tipos de compromiso o para minimizar los impactos de ataques reales. Incluyen sistemas de software y hardware que realizan funciones preventivas, de detección y reactivas, como software antivirus, herramienta de monitoreo de red, software de encriptación, etc (Romagna, 2020).

El cifrado es un aspecto de la contramedida técnica utilizada para proteger los documentos que se intercambian entre las partes para garantizar la integridad de los datos y la identificación del usuario. COVID-19 vio una cantidad cada vez mayor de transacciones selladas en línea utilizando tales tecnologías para respaldar documentos para bienes raíces, publicar contratos, órdenes de compra, transferencia de consentimiento, etc. Por ejemplo, la herramienta DocuSign permite a las partes usar firmas electrónicas de forma remota para respaldar acuerdos contractuales en una variedad de dispositivos (Satoshi, 2008).

4.5. Perillas de control

La categorización de las contramedidas de seguridad por los respectivos controles de seguridad equilibra su efectividad de acuerdo con el modelo de defensa en profundidad. Las perillas de control son medidas de seguridad implementadas para administrar amenazas y riesgos de seguridad dirigidos a redes y sistemas informáticos vulnerables. Se revisan cinco perillas de control (Agate & O'Rorke, 2016).

4.5.1. Control Preventivo

Los sistemas de control preventivo protegen los activos digitales (incluidos los datos) de amenazas conocidas y desconocidas, ya sea minimizando el riesgo, reduciendo la exposición o deteniendo la progresión de la amenaza. Estas medidas están diseñadas para evitar que se produzcan errores, inexactitudes, irregularidades o fraudes en primer lugar. También ayudan a evitar la pérdida de datos y garantizan la seguridad en línea al garantizar la confidencialidad, la integridad y la disponibilidad (Yulisman, 2020).

4.5.1.1. Zoom intervención preventiva

En el pico de la pandemia, cuando los países habían cerrado sus fronteras en cumplimiento de los protocolos de confinamiento, y cuando se hizo evidente que las tecnologías remotas serían alternativas prácticas para las reuniones corporativas y las interacciones laborales, Zoom, la empresa de videotelefonía en línea, optimizó su función de sala de espera. Permitir que un administrador de reunión virtual lleve a cabo una evaluación previa de los participantes de la reunión antes de admitirlos en una sesión de videoconferencia en vivo (Scroxton, 2020).

La funcionalidad de la sala de espera de Zoom representa una perilla de control preventivo típica que verifica previamente a los participantes potenciales de la reunión y minimiza el riesgo de bombardeo de zoom donde un intruso usa el ataque de intermediario para interceptar y/o grabar las conversaciones de la reunión. Esto neutraliza los esfuerzos del intruso para infiltrarse sin ser detectado para capturar información confidencial o publicar

contenido ofensivo que podría dañar la reputación y activar la privacidad (Spadafora, 2020).

4.5.1.2. Intervención preventiva antimalware

De importancia para el período de la pandemia fue la instalación de una herramienta antimalware efectiva, como un software antivirus diseñado para identificar contenidos que son potencialmente dañinos para la computadora, particularmente aquellos disfrazados como recursos de coronavirus. Tener una herramienta antimalware funcional en dispositivos conectados a Internet resultó ser un enfoque rentable para los usuarios que la adoptaron.

Una buena solución antivirus o antimalware puede aplicar un mecanismo de detección avanzado para detectar las cadenas de códigos maliciosos más comunes y puede tomar medidas para proteger los sistemas y los datos. Antes de elegir e instalar una herramienta antivirus, se espera que los usuarios verifiquen las características de rendimiento, confirmen el soporte disponible de los proveedores de software antivirus y mantengan el software antivirus completamente actualizado para lograr la máxima eficiencia (Agate & O'Rorke, 2016).

4.5.2. Control correctivo

Los controles correctivos complementan las contramedidas receptivas para arreglar lo que se ha visto comprometido por una infracción cibernética, al activar acciones de recuperación y recuperación.

4.5.3. Control de disuasión

Las contramedidas disuasorias están destinadas a desanimar al atacante prolongando el ataque con la esperanza de que, al dificultar el ataque, el adversario pueda renunciar a sus esfuerzos. P.ej. el uso de una contraseña segura tiene como objetivo alargar el tiempo que le toma al pirata informático malicioso descifrar usando fuerza bruta o ataque de diccionario.

4.5.4. Control receptivo

Los controles receptivos son contramedidas reactivas, requeridas después de una infracción. Están diseñados para descubrir la causa raíz, facilitar una recuperación más rápida, limitar el impacto general y prevenir la propagación.

CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

El cibercrimen ha sido una gran amenaza para la economía mundial y el comercio digital. Cuando no se controlan, los delitos cibernéticos afectan directamente la seguridad individual y el bienestar del público en general, y siguen siendo un medio potencial que puede impulsar acciones radicales e ideológicas como la guerra asimétrica y el terrorismo. Los impactos del ciberdelito imponen graves consecuencias tanto a las organizaciones individuales como a las corporativas.

El patrón de delitos cibernéticos relacionados con COVID-19 claramente dejó enormes consecuencias en la confidencialidad de los datos además de la integridad de la información y la disponibilidad de los sistemas que procesan los datos. Una comprensión de la tríada CIA y los impactos que su relegación puede ejercer en el ciberespacio son ingredientes esenciales para proteger el flujo de información desde su creación hasta el momento en que se vuelve obsoleta y finalmente se destruye mediante una técnica apropiada como la eliminación.

La tríada de la CIA es aplicable en una amplia gama de escenarios prácticos, incluida la acción del atacante de jaque mate de acceder al historial de Internet de un usuario, proteger los datos cifrados en el ciberespacio y verificar que un mensaje electrónico permanece sin cambios mientras está en tránsito o almacenamiento. Una brecha en cualquiera de los tres componentes de la CIA puede tener impactos de gran alcance en los otros dos y, en casos extremos, puede causar serios problemas de seguridad para las partes involucradas.

Una revisión de los incidentes de COVID-19 que afectan a los componentes de la CIA revela el vacío que se crea cuando no hay equilibrio entre los roles preventivo, de detección y de respuesta. Esta revelación ayuda a evitar problemas de cumplimiento, garantiza la continuidad del negocio y previene daños a la reputación de individuos y organizaciones,

todos los cuales son consecuencias de violaciones activas de ciberseguridad.

5.2. Recomendaciones

Como ocurre con todos los incidentes de seguridad, la combinación de contramedidas administrativas, físicas y técnicas generó grandes expectativas durante la pandemia de COVID-19. Eran convenientes para el logro de un ciberespacio más seguro.

A pesar de la solidez de la seguridad implementada para detectar y prevenir ataques cibernéticos que se hicieron pasar por información sincera sobre el coronavirus en línea, era importante que los usuarios digitales tuvieran un plan para recuperarse de las infracciones cibernéticas activas y mitigar sus impactos. Esencialmente, la recuperación debía imitar el enfoque de defensa en profundidad que comprende una combinación de perillas de control preventivas, de detección, de respuesta, correctivas y disuasorias.

REFERENCIAS

Agate, J., & O'Rorke, O. (2016). Data protection in media litigation. *Communications Law*, *21*(2), 46-48

Assante, M. J., & Lee, R. M. (2015). *The industrial control system cyber kill chain*. SANS Institute.

Bhargava, A. (2020). In the New. *Malwarebytes*. https://blog.malwarebytes.com/author/abhargava/Cole, E. (2020). Phishing: You Are A Target. In *Secure Anchor Consulting*.

Cole, E., & Ring, S. (2006). *Insider Threat: Protecting the Enterprise from Sabotage*. Syngress Publishing Inc.

Desk, N. (2020). Hacker Allegedly Breaches Govt Database on COVID-19 Test-takers. *The Jakarta Post*. https://www.thejakartapost.com/news/2020/06/20/hacker-allegedly-breaches-govt-database-on-covid-19-test-takers.html

Doffman, Z. (2020). *Hackers Attack Microsoft Windows Users: Dangerous Threat Group Exploits 'COVID-19 Fear.* https://press.malwarebytes.com/2020/03/16/hackers-attack-microsoft-windows-users-dangerous-threat-group-exploits-covid-19-fear/

E. Berrueta, E. M., D. Morato, & Izal, M. (2019). A Survey on Detection Techniques for Cryptographic Ransomware. In *IEEE Access* (Vol. 7, pp. 144925-144944,). https://doi.org/10.1109/ACCESS.2019.2945839

Ferbrache, D. (2020). The Rise of Ransomware During COVID-19: How to Adapt to the New Threat Environment. *KPMG*.

Jadha, S. (2017). Spyware and trojan horses. *International Journal for Scientific Research & Development (IJSRD*, *5*(8), 94-99

Kurniawan, A., & Riadi, I. (2018). Detection and analysis cerber ransomware based on network forensics behavior. *International Journal of Network Security*, *20*(5), 836-843

Lee, W., & Rotoloni, B. (2016). Emerging Cyber Threats Report 2016. In *Institute for Information Security and Privacy (IISP*. Georgia Institute of Technology.

Lewandowsky, S., & Cook, J. (2020). *The Conspiracy Theory Handbook*. George Mason University.

Machteld, J. (1984). *Mellink, Troy and the Trojan War: A symposium held at Bryn Mawr College*. Bryn Mawr College Publications, Bryn Mawr.

Okereafor, K., & Adelaiye, O. (2020). Randomized cyber attack simulation model: A cybersecurity mitigation proposal for post COVID-19 digital era. *International Journal of Recent Engineering Research and Development (IJRERD*, *05*(07), 61-72

Okereafor, K., & Djehaiche, R. (2020a). A review of application challenges of digital forensics. *International Journal of Simulation Systems Science and Technology*, *21*(2), 35 1-35 7

Okereafor, K., & Djehaiche, R. (2020b). New approaches to the application of digital forensics in cybersecurity: A proposal. *International Journal of Simulation: Systems, Science and Technology (IJSSST*, *21*(2), 36 1-36 6

Okereafor, K., & Marcelo, A. (2020). Addressing cybersecurity challenges of health data in the COVID-19 pandemic. *International Journal in IT & Engineering*, *8*(6), 1-12

Okereafor, K. U., & Adebola, O. (2020). Tackling the cybersecurity impacts of the coronavirus outbreak as a challenge to internet safety. *International Journal in IT and Engineering (IJITE*, *8*(2), 1-14

Organizatio, W. H. (2020). *Report of the WHO-China Joint Mission on Coronavirus Disease 2019 (COVID-19*. World Health Organization.

Paul, M. (2016). *Digital identity: Issue analysis*. Consult Hyperion.

Raywood, D. (2020). Garmin Confirms Cyber-attack as Ransomware Recovery Rumored. *Info Security Magazine*.

Romagna, M. (2020). Hacktivism: Conceptualization, techniques, and historical view. In *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 743–769). Palgrave Macmillan.

Sahi, S. K. (2017). A study of WannaCry ransomware attack. *International Journal of Engineering Research in Computer Science and Engineering (IJERCSE*, *4*(9), 5-7

Satoshi, N. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.

Scroxton, A. (2020). Zoom Making Progress on Cyber Security and Privacy, says CEO. *Computer Weekly*. https://www.computerweekly.com/news/252485510/Zoom-making-progress-on-cyber-security-and-privacy-says-CEO

Tilton, C. (2006). *Biometric standards – An overview*. Daon Inc.

Yulisman, L. (2020, June 21). Indonesia probes alleged hacking of Covid-19 test data. *The Straits Times*. https://www.straitstimes.com/asia/se-asia/indonesia-probes-alleged-hack-of-covid-19-test-data

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Suastegui Jaramillo, Luis Eduardo** con C.C: #0917738239 autor del trabajo de titulación: **Estudio y análisis de ataques informáticos en Ecuador durante el estado de pandemia de COVID-19** previo a la obtención del título de **INGENIERO EN TELECOMUNICACIONES** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 07 de marzo de 2022

f. _____

Nombre: Suastegui Jaramillo, Luis Eduardo

C.C: 0917738239

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACION			
TEMA Y SUBTEMA:	Estudio y análisis de ataques informáticos en Ecuador durante el estado de pandemia de COVID-19		
AUTOR(ES)	Suastegui Jaramillo, Luis Eduardo		
REVISOR(ES)/TUTOR(ES)	M. Sc. Romero Paz, Manuel de Jesús		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Educación Técnica para el Desarrollo		
CARRERA:	Ingeniería en Telecomunicaciones		
TITULO OBTENIDO:	Ingeniero en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	07 de marzo de 2022	**No. DE PÁGINAS:**	51
ÁREAS TEMÁTICAS:	Sistemas telemáticos y seguridad en redes		
PALABRAS CLAVES/ KEYWORDS:	Ransomware, Malware, COVID-19, Ciberseguridad, Threat Hunting, Respuesta a Incidente		

RESUMEN/ABSTRACT (150-250 palabras):
A lo largo del primer trimestre de 2020, a medida que avanzaba la pandemia de COVID-19, se produjeron casi tres millones de ciberataques en América Latina y el Caribe. Solo en marzo de 2020, la incidencia de virus informáticos en la región aumentó en un 131 por ciento en comparación con marzo de 2019. Posteriormente, en febrero del 2021, se da a conocer a la ciudadanía ecuatoriana el primer ataque informático con repercusión nacional, donde por medio de un ataque del tipo "Secuestro de datos" realizado a una institución financiera la información de identificación personal de un gran número de ciudadanos fue expuesta a internet. Este evento puso en evidencia la fragilidad de los sistemas informáticos a nivel nacional e inicia una serie de incidentes informáticos que afectan la confidencialidad, integridad y disponibilidad de los sistemas de comunicación de instituciones públicas y privadas. Este trabajo de titulación presenta un estudio en profundidad de los distintos vectores de ataques usados por los cibercriminales, sus técnicas, tácticas y procedimientos en los distintos incidentes informáticos divulgados públicamente en los tres primeros trimestres del 2021.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593980084137	**E-mail:** luis.suastegui02@cu.ucsg.edu.ec
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE)::	**Nombre:** Palacios Meléndez, Edwin Fernando	
	Teléfono: +593-9-67608298	
	E-mail: edwin.palacios@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	