PRACTICA 1 LABORATORIO

1. **Explique la evolución de los ataques informáticos y previsiones par al futuro.**

1.1. Evolución de los ataques informáticos.

- **30 de abril de 1960, *(Core War)*** no fue un virus informático, sino más bien un juego mediante el cual se propagó uno de los primeros software con características maliciosas que afectaba la memoria de las computadoras y podía auto replicarse, fue una sencilla aplicación que competía con el resto de los programas que se ejecutaban en una computadora con el fin de obtener el control absoluto de la memoria del equipo. considerado como uno de los *precursores de los virus informático* de la historia de la computación.

- **30 de abril de 1971, (Creeper-virus)** fue creado por Bob Thomas fue especialmente escrito para atacar al sistema operativo Tenex. Cuando Creeper llegaba a una computadora, por lo general por intermedio de los nodos de la ARPANET, el malware se autoejecutaba y comenzaba a mostrar el siguiente mensaje: "Soy la enredadera, atrapame si puedes!".

- **30 de abril de 1982, (Elk Cloner virus)** es el primer virus informático conocido que tuvo una expansión real y no como un concepto de laboratorio. Rich Skrenta, un estudiante de instituto de 15 años, lo programó para los Apple II en 1982. se propagaba infectando los disquetes del sistema operativo de los computadores Apple II. Cuando la computadora arrancaba desde un disquete infectado, también lo hacía el virus de forma automática. se diseñó para ser molesto: en cada arranque nº 50 aparecia un poema.

- **30 de abril de 1985, (Primeros Troyanos)** se presentaban disfrazados, por un lado el virus que se escondía bajo una imagen de programa de mejora de gráficos llamado EGABTR, y por el otro el famoso juego llamado NUKE-LA.

- **30 de abril de 1987, (Virus Brain)** el primer virus que provocó mayores infecciones en la época, el cual comenzó a circular en el año 1986, y para 1987 había logrado extenderse por todo el mundo.
  había sido escrito para atacar el sistema MS-DOS y era totalmente compatible con IBM PC.
  Fue creado por un grupo de amigos oriundos de la ciudad de Lahore, Paquistán, quienes se encargaron de distribuirlo vendiendo copias del mismo insertadas en diskettes pirateados de programas comerciales, entre los que se encontraban los popul.

- **2 de Noviembre de 1988, (Gusano de Morri),** Morris Worm. Durante unas horas, aproximadamente el 10% de todas las máquinas de Internet se vieron afectadas por ese 'gusano'.es considerado el primer gusano (worm) y que además llevó a su creador a ser la primera persona condenada por la justicia bajo un delito de fraude y de abuso informático. Ahora Morris es profesor del MIT. la fiscalía argumentó que el gusano "no se trató de un error, sino de un ataque contra el gobierno de los Estados Unidos". Produjo fallos en cientos de computadoras.

- **30 de Junio de 1998, (CIH Virus)** El virus infectó los archivos ejecutables de Windows 95,98 y ME y fué capaz de permanecer residente en memoria de los ordenadores infectados para así infectar otros ejecutables.
  ¿Porqué?: Lo que lo hizo tan peligroso fué que en poco tiempo afectó muchos ordenadores,

podía reescribir datos en el disco duro y dejarlo inoperativo.
Curiosidades: CIH fué distribuido en algun que otro importante software como un Demo del juego de Activision “Sin”.

- **30 de Abril de 1999,** creado por David L. Smith y bautizado así por el nombre de una stripper **(Melissa, la “bailarina exótica” Word).** El archivo llegaba vía e-mail como documento de Word anexado, bajo el título "acá está ese documento que me pediste, no se lo muestres a nadie más". Tras instalarse, desactivaba opciones del procesador de texto y modificaba los documentos utilizados. Su esparcimiento fue rápido, puesto que ocupaba la libreta de direcciones de Outlook y se reenviaba a los primeros 50 contactos.

- **30 de Abril de 2000, (I love you, la temida “carta de amor”)** Onel de Guzmán lo creò, Filipinas, con lenguaje de Visual Basic, las "virtudes" de este virus eran innumerables: se autocopiaba y escondía en diversos ficheros, añadía registros, remplazaba archivos, se auto enviaba vía correo y copiaba contraseñas a través de una aplicación auto instalable.

- **2001, (SIRCAM gusano)** llegaba oculto dentro de un mensaje de correo electrónico. La primera línea del contenido del mensaje decía “Hola como estas?”.se propagaba muy rápido, enviándose automáticamente a todos los contactos que encuentra en la libreta de direcciones de las computadoras infectadas. También infectaba todas las terminales con Windows NT de una red.. Entre sus objetivos figuran obtener datos privados de los usuarios que infecta, agotar el espacio libre del disco rígido y borrar la información que contiene.

- **2001, (BUGBEAR virus)** Podía desactivar los programas de seguridad de la computadora, además de abrir una puerta trasera en el equipo infectado. Llegaba a través del correo electrónico, usando títulos como "Interesante", "Hola" o "Sólo para recordarte", para inducir al usuario a que abra el mensaje infectado. No hacía falta abrir ficheros.

- **2003, (SQL Slammer/Zafiro Virus)** Sólo 10 minutos tardó en dejar la red mucho más lenta en 2003. Su ataque fue increíblemente agresivo, pues aprovechó una falla en la base de datos del servidor SQL de Microsoft, saturando archivos en todo el mundo. Entre sus víctimas "ilustres" destacan el servicio ATM del Bank of América, el servicio de 911 de Seattle y la cancelación de vuelos de Continental Airlines. Su legado es haber obligado a que las grandes empresas mejoraran no sólo su seguridad.

- **2003,** El virus se propagó vía e-mail adjunto archivos como application.pif y thank_you.pif. Cuando se activaba se transmitía. El 10 de Septiembre de 2003 el virus se desactivó asimismo y ya no resultaba una amenaza, Microsoft ofreció en su día 250.000$ a aquel que identificara a su autor. Causando de 5 a 10 billones de dólares y más de un millón de ordenadores infectados.

- **11 de Agosto de 2003,** daba mensaje “Solo quiero decir que te quiero san!!” y “billy gates ¿Porqué haces posible esto? para de hacer dinero y arregla tu software!!” era activado abría un cuadro de diálogo en el cual el apagado del sistema era inminente.

- **30 de Abril de 2004, (MyDoom Virus)** crea una puerta trasera para acceder al sistema operativo.Busca distribuirse a través de las cuentas de correo. Además, envía una petición a un motor de búsqueda externo, por lo que en su momento logró generar algunos problemas de velocidad en Google. Su impacto en la industria es de US$ 38.500 millones, y hasta ahora no

tiene a un creador conocido. Microsoft más destructivo de la historia destruía el sector Zero del disco y para ese entonces (2005), no se tenía arreglo.

- **30 de Abril de 2006, (Nuwar,Tormenta Gusano)** es capaz de convertir el computador en un "zombie", pues quedan vulnerables al control remoto de parte del que envía el ataque. Una de sus apariciones más importantes fue para los JJ.OO. de Beijing 2008, donde "avisaban" de una catástrofe en China por un terremoto, invitando a revisar un correo con más información, lo que en realidad hacía descargar el virus. En 2007 se ganó el título del "peor" virus del año.

- **30 de Abril de 2012, DNSChanger, el saboteador de conexiones "Hijacker",** modifica la configuración del sistema para que toda navegación sea redirigida hacia otras páginas (por ejemplo, páginas con publicidad).

1.2. Previsiones para el futuro.

Hablando de ciberseguridad y ataques informáticos, no es fácil predecirlo. Es un sector cambiante y que evoluciona muy rápido. Sin embargo, muchos expertos y compañías del sector son capaces de vislumbrar lo que puede estar por venir, analizando las amenazas y tendencias en ciberseguridad observadas durante los últimos meses.
Las amenazas contra la privacidad de los datos o el ransomware sin duda son algunas de las principales tendencias en ciberseguridad que se apuntan para 2018, así como ataques contra infraestructuras críticas, malware o amenazas.
Hemos recopilado los análisis, informes y tendencias de fabricantes de seguridad, como **ESET**, **G DATA**, **Trend Micro, Panda o Check Point** y consultoras y empresas especializadas en transformación digital como **All4Sec o Entelgy.**

El ransomware
Sin duda, uno de las tendencias que más se repiten en todos los estudios e informes. ESET advierte de que **el ransomware seguirá siendo una de las fuentes de negocio de los cibercriminales en 2018**, ya que "aún hay muchas organizaciones dispuestas a pagar grandes sumas de dinero por recuperar sus sistemas comprometidos en lugar de contar con políticas de ciberseguridad que las mantengan protegidas ante cualquier amenaza".

Reglamentos de protección de datos
Ha sido uno de los temas sobre los que más se ha hablado, ya que el reglamento (GDPR) será de obligado cumplimiento. Desde All4Sec apuntan que la privacidad y la seguridad de los datos se han mantenido hasta ahora como dos áreas separadas en el marco de la ciberseguridad, pero **todo cambiará en 2018**. Y advierten: "un segmento particularmente sensible será el de las PYMEs que deberán darse cuenta de que son tan vulnerables o más que cualquier gran corporación".

Criptomonedas
Cada vez más gente está invirtiendo en unas divisas electrónicas cuyas cotizaciones no dejan de crecer, lo que provocará que "una vez más se reúnan **los ingredientes necesarios que colocan a estas monedas virtuales en el centro de la diana cibercriminal**

Internet de las cosas
El Internet de las Cosas no es una tendencia en sí misma. Es una realidad cotidiana. Los dispositivos inteligentes inundan hogares digitales y empresas. Eso sí, los riesgos de seguridad para sus comunicaciones y sistemas operativos crecerán al mismo ritmo. "A medida que aumentan las

capacidades de la tecnología y se implementan nuevos sistemas disruptivos en las nuevas industrias, estos se convertirán en los objetivos principales para el cibercrimen y la actividad maliciosa", explican desde Trend Micro. **El próximo año se estima que se utilizarán más de un millón de robots conectados en esta capacidad**, y es muy importante que todo aquel que utilice dispositivos conectados se asegure de que estén **debidamente protegidos**.

Robo de datos perdónales
Se descubrirán casos de robos de datos o se producirán nuevos aún más grandes que los vistos en los últimos años. Además, los expertos apuntan que los datos que los cibercriminales robaban a se han vendido tradicionalmente en la deep web, pero en 2018 se podrían consolidar nuevas formas de monetización, especialmente la extorsión, hasta ahora asociada mayoritariamente al ransomware.

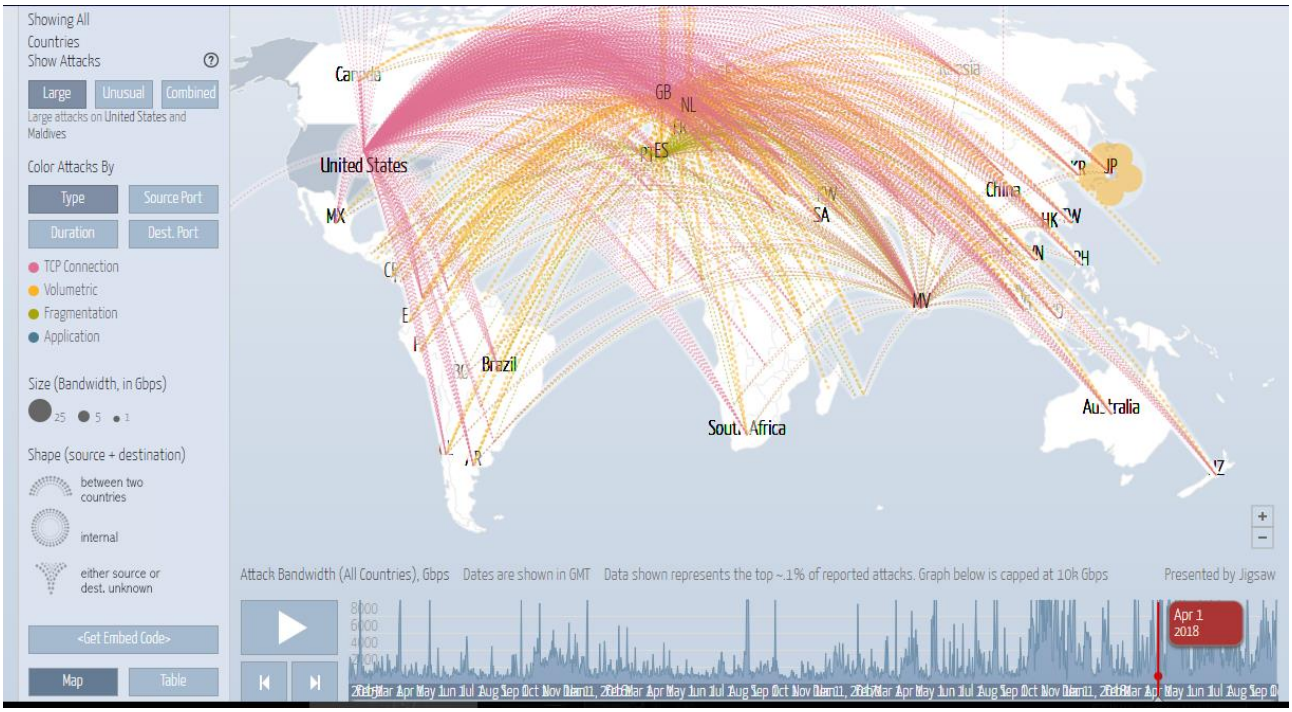
Más malware
Viejos conocidos regresarán con nuevos aires, aseguran desde ESET: "**En 2018 el malware seguirá explotando vectores de ataque conocidos**, que llevan funcionando incluso décadas, como los que utilizan código oculto en todo tipo de documentos"

En resumen los ataques informáticos van mutando junto con el desarrollo de la tecnología, las mejores formas de prevenir es con la implementación de políticas de seguridad de la información, la concientización y formación de los empleados, el uso de machine learning y el uso de la IA en la predicción de los atacantes.

2. **Explique una breve reseña histórica de la informática forense.**
El campo de la informática forense se inició en la década de 1980, poco después de que las computadoras personales se convirtieran en una opción viable para los consumidores. En 1984, fue creado un programa del FBI. Conocido por un tiempo como el Programa de Medios Magnéticos, que ahora se conoce como CART (CART, del inglés computer analysis and response team), o análisis de informática y equipo de respuesta. Poco después, el hombre al que se le atribuye ser el "padre de la informática forense", comenzó a trabajar en este campo. Su nombre era Michael Anderson, y era un agente especial de la División de Investigación Criminal del IRS. Anderson trabajó para el gobierno en esta capacidad hasta mediados de 1990, tras lo cual fundó New Technologies, Inc., un equipo que lleva la firma forense.
La disciplina continuó creciendo en la década de 1990, con la primera conferencia sobre la recopilación de pruebas de los equipos, celebrada en 1993. Dos años más tarde, la **IOCE** (IOCE, del **inglés international organization on computer evidence**), u organización internacional de evidencia informática fue establecida.
En 1997, se reconoció ampliamente que los funcionarios encargados de hacer cumplir la ley en todo el mundo tenían que ser bien versados en la forma de adquirir la evidencia de las computadoras, un hecho puesto de manifiesto en un comunicado del G8 en 1997. INTERPOL celebró un simposio sobre informática forense al año siguiente, y en 1999, el programa CART del FBI abordó 2000 casos individuales.
La carga de casos del CART del FBI continuó creciendo. Mientras que en 1999, el equipo analizó 17 terabytes de datos, para el año 2003 el grupo examinó 782 terabytes de datos en sólo un año. Con los avances en la informática y la proliferación del acceso a Internet en todo el mundo, la informática forense comenzó a desempeñar un papel más importante para los agentes del orden. Con el advenimiento de los teléfonos inteligentes y PDA, las formas en que la informática forense

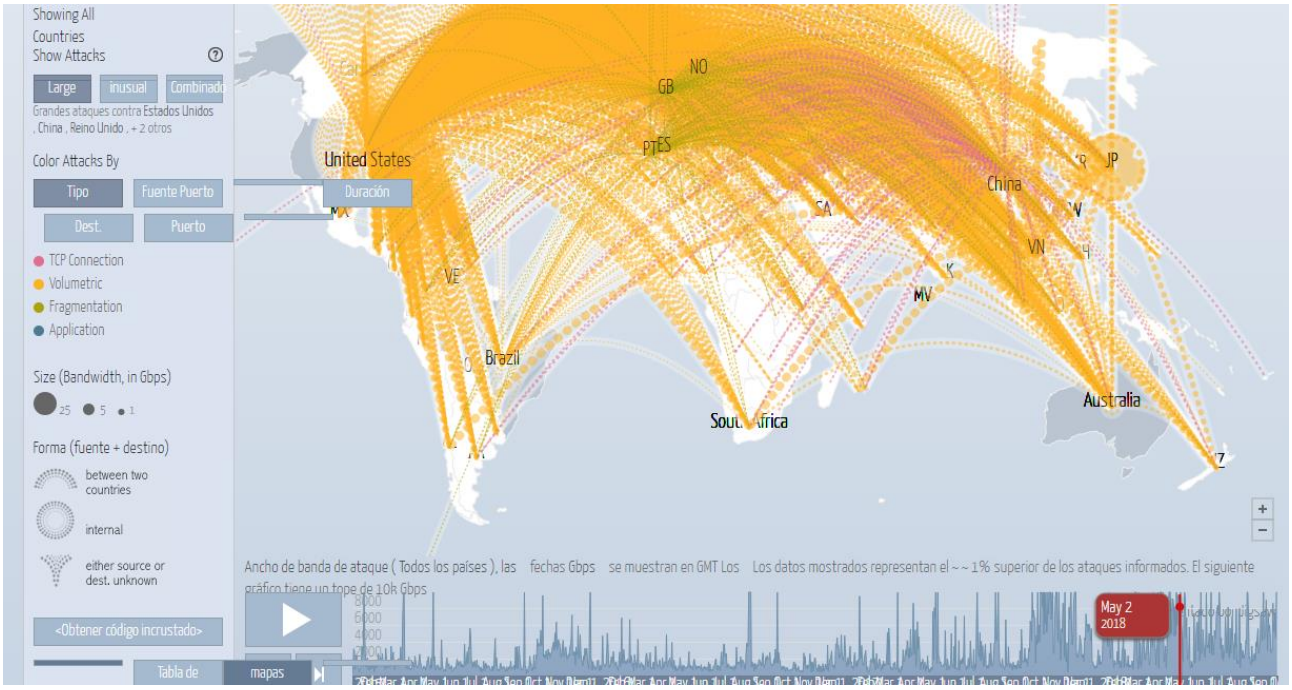
puede operar se ha vuelto aún más importante a medida que los delincuentes tienen muchas opciones para romper la ley mediante el uso de dispositivos de computación.

3. **Haga una breve explicación de los ataques DDOS entre países entre los meses de abril y agosto del 2018.**
   Los principales ataques DDOS en todo el mundo clasificados por meses de abril a agosto.
   Mes de abril.



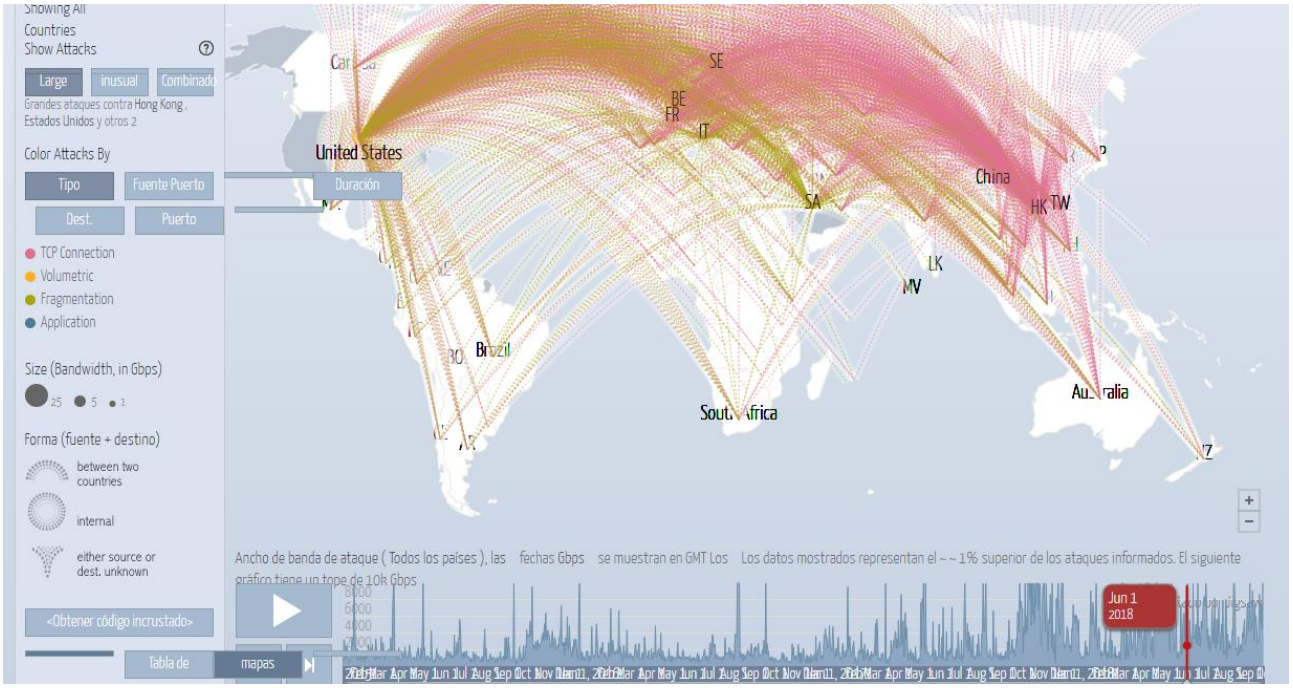
La imagen muestra los ataques realizados el mes de abril del 2018, los ataques DDOS (de conexión) se realizan principalmente del país de los estados unidos hacia los países de Australia, Sudáfrica, Brasil, china, Italia, pilipinas.

Mes de Mayo.



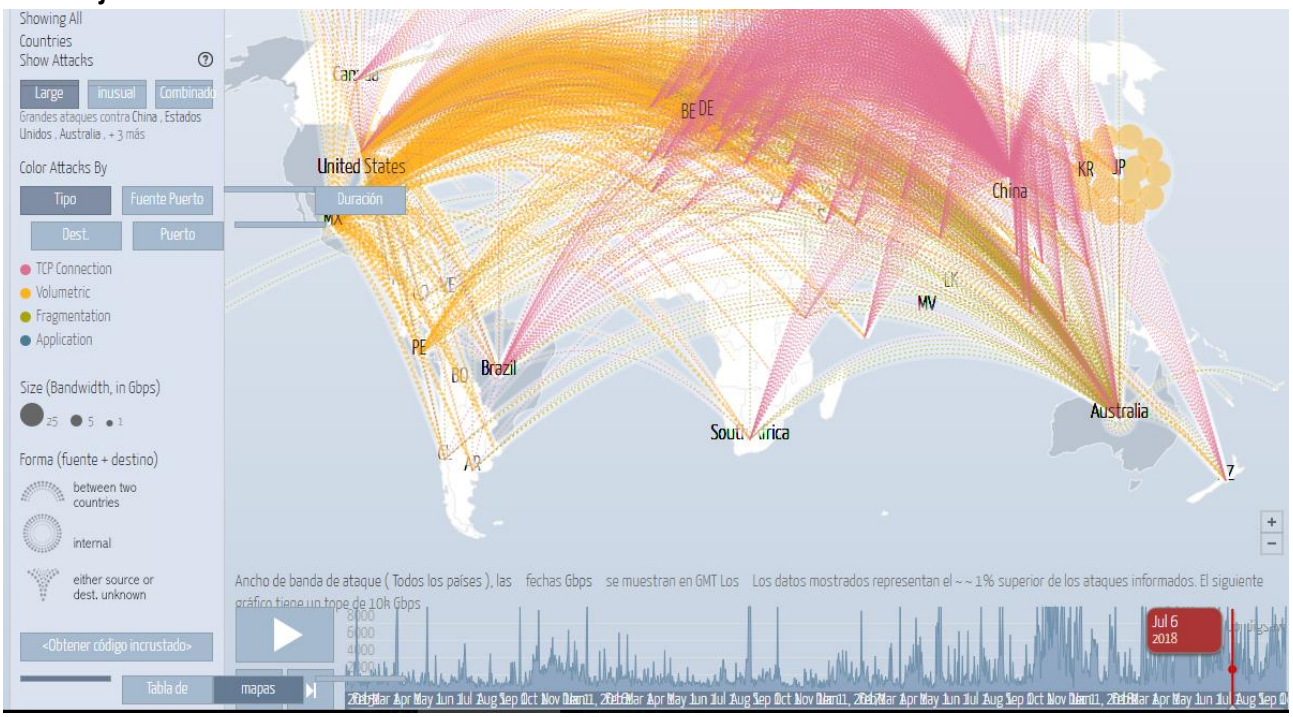
Como se puede observar los ataques DDOS incrementaron el mes de mayo del 2018, son más elevados del continente americano hacia el resto de los continentes como al europeo y asiático.

Mes de junio:

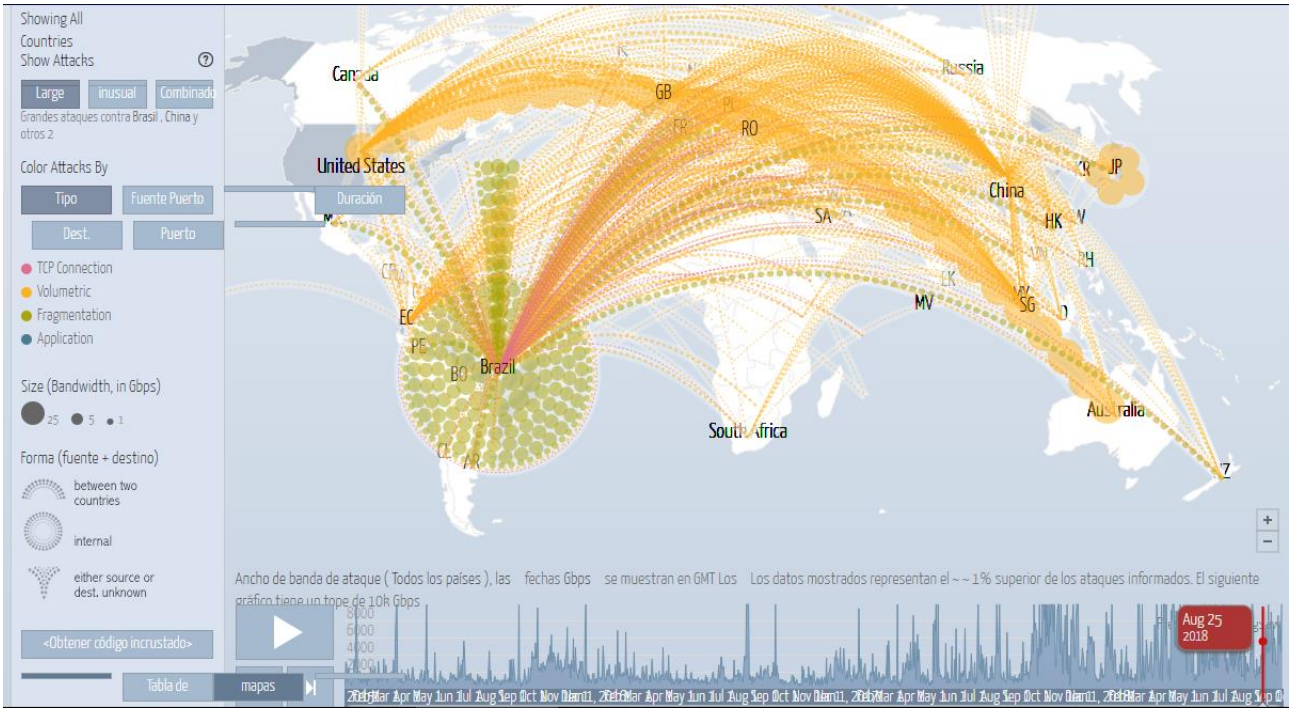


En este mes los ataques se incrementaron del país de china asi el resto de los países, como hacia el país de Italia y Australia.

Mes de julio



Mes de Agosto



En este último mes se puede observar cómo se incrementaron los ataques DDOS, entre los países de estados unidos, Australia. También se puede observar que este tipo de ataques se incrementó de manera considerable del país de Brasil hacia nueva Zelanda, china, Japón, Rusia.

4. **Haga una breve descripción del propietario o propietarios de 5 dominios web de Bolivia.**
   1. **Nombre de dominio: www.uatf.edu.bo**

CONTACTO TÉCNICO	
Razón Social :	Universidad Autonoma Tomas Frias
Nombre Completo :	**Lic. Alex Michel Diaz**
Correo Eléctronico :	webmaster@uatf.edu.bo
País :	Bolivia
Ciudad :	Potosi
Dirección :	Av. Civica esq. Av. Serrudo
Teléfono :	591-062-22365
FAX :	
PoBox :	

Breve descripción:

Nombre de propietario de nombre de dominio: *Lic. Alex Michel Diaz*
Fecha de nacimiento: *1 de febrero*
Familiares: *Juan Gonzalo Michel diaz(hernan), Juan Cristobal Diaz(sobrino).*

   2. **Nombre de Dminio: www.uajms.edu.bo**

CONTACTO TÉCNICO	
Razón Social :	UAJMS
Nombre Completo :	**Yesid Criales Bernal**
Correo Eléctronico :	yesid@uajms.edu.bo
País :	Bolivia
Ciudad :	Tarija
Dirección :	Campus universitario - El Tejar - DTIC - Bloque 14
Teléfono :	04-6633910
FAX :	04-6646917
PoBox :	51

Breve descripción:

Vive en: Cercado, Tarija, Bolivia

Lugar de orige: La Paz

3. Nombre de dominio: www.upds.edu.bo

CONTACTO TÉCNICO	
Razón Social :	Corporación Educativa Domingo Savio S.A.
Nombre Completo :	**Santiago Luis Vera Castañeda**
Correo Eléctronico :	santiago.vera@UPDS.edu.bo
País :	Bolivia
Ciudad :	Santa Cruz
Dirección :	Av. Japón 250
Teléfono :	3418541
FAX :	3426820
PoBox :	2869

4. Nombre de dominio: www.entel.bo

CONTACTO TÉCNICO	
Razón Social :	Entel SA
Nombre Completo :	Alejandro Córdova Liendo
Correo Eléctronico :	acordova@entel.bo
País :	Bolivia
Ciudad :	La Paz
Dirección :	Federico Suazo 1771
Teléfono :	72550505
FAX :	

PoBox :	4450

Breve descripción:

Vive en la ciudad de La Paz

Ciudad de Origen: Ourure

Nombre de Dominio: www.tigo.com.b

CONTACTO TÉCNICO	
Razón Social :	Telecel S.A.
Nombre Completo :	Tigo Tecnico
Correo Eléctronico :	nictecnicotigo@tigo.net.bo
País :	Bolivia
Ciudad :	Santa Cruz
Dirección :	Av. Viedma #648
Teléfono :	800178000
FAX :	
PoBox :	

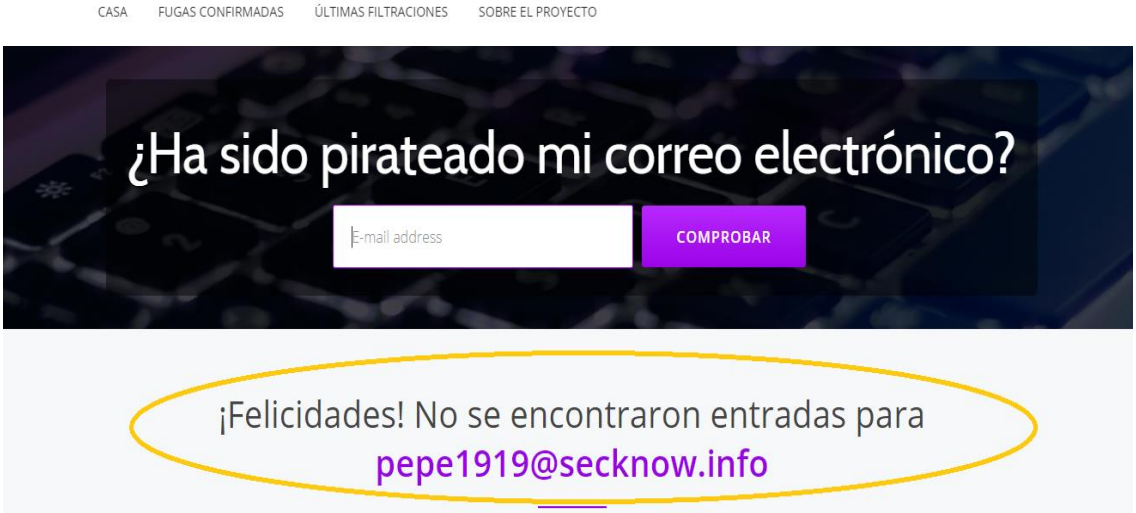
5. **Que información nos da la paginas https://hesidohackeado.com y como evitar esas vulnerabilidades.**

   La página "**https://hesidohackeado.com** " muestra si un correo electrónico está comprometido o expuesto, para que el usuario pueda tomar medidas de seguridad para proteger sus cuentas y proteger su identidad, si la cuenta está comprometida o expuesta la página te recomienda que cambies tu contraseña para proteger cualquier cuenta lo antes posible.

   Por ejemplo:

   Correo electrónico de prueba: ***pepe1919@secknow.info***

   Resultado de la página:



6. **Cuáles son las últimas novedades que hace el gobierno de Bolivia con respecto a la gestión de la TIC, la seguridad de sistemas y la informática forense.**

Estado TIC
Estado de las Tecnologías de Información y Comunicación en el Estado Plurinacional de Bolivia

El Estado TIC es el resultado de un esfuerzo conjunto para brindarle a las ciudadanas y ciudadanos bolivianos un mayor conocimiento sobre la realidad del tema, pues solo conociéndola es posible transformarla y mejorarla

Estado TIC pueda promover el debate y un mayor análisis de la población en general que nos permitan generar un norte colectivo, vital en la contribución de este norte digital que estamos construyendo en beneficio de todas y todos los bolivianos y las bolivianas. Es decir, que podamos plantear una Agenda Digital que esté a la altura de los retos por los que actualmente atraviesa nuestro país y nuestra revolución

Y es que en los últimos años el Estado boliviano ha invertido miles de millones de dólares para transformar el paisaje tecnológico del país. Desde la implementación de telecentros comunitarios, la distribución de ordenadores personales a los maestros y jóvenes de secundaria de todo el país, el espectacular lanzamiento del Satélite TK-1, el despliegue de redes de fibra óptica por todo el territorio, hasta el uso de firma digital. Nuestra patria ha dado inicio a una política pública de largo aliento, contenida en el punto cuarto de la Agenda Patriótica del Bicentenario 2025: soberanía tecnológica.

En resumen:

La AGETIC coordina sus políticas y actividades con las entidades públicas del Estado Plurinacional de Bolivia en diversas áreas como el desarrollo de infraestructura, políticas de seguridad de la información e investigación tecnológica.

El escenario principal para el relacionamiento de las entidades públicas con relación a las tecnologías de información y comunicación es el Consejo de Tecnologías de Información y Comunicación (CTIC), donde se debaten y elaboran normativas técnicas y proponen políticas para el sector público y la sociedad en general.

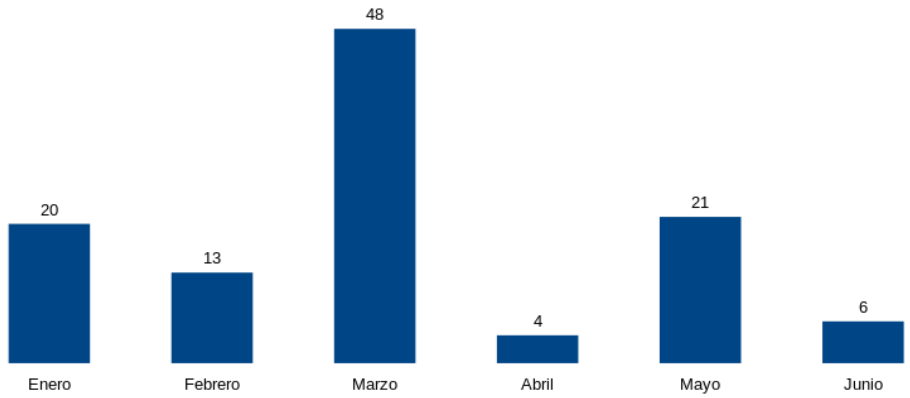
El principio rector para todas las instituciones del Estado Plurinacional es la soberanía tecnológica, la construcción de conocimiento en Bolivia con base en las necesidades de nuestro pueblo.

7. **¿Cómo es que se obtiene la lista de afectados por los ataques informáticos?**

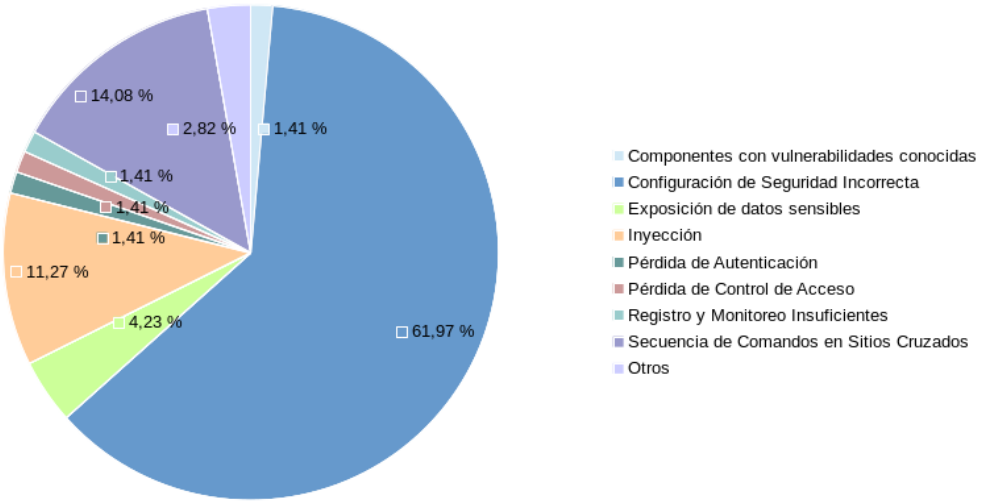
Para obtener una lista de afectados de ataques informáticos se lo puede realizar a través del **CGII** "**Centro de Gestión de Incidentes Informáticos**" https://www.cgii.gob.bo/es , este sitio comunica y otorgar información a todas las entidades del sector público acerca de incidentes informáticos y vulnerabilidades de que haya tomado conocimiento.

Por ejemplo, es así que el CGII atendió un total de 112 casos relacionados a incidentes y vulnerabilidades al primer semestre de la gestión 2018.

Cantidad de Incidentes y vulnerabilidades atentidos primer semestre 2018.



Vulnerabilidades atendidas al primer semestre 2018



Incidentes atendidos al primer semestre 2018