ESTADO DE LA CIBERSEGURIDAD en PARAGUAY

AÑO 2019

CERT-PY

Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

GOBIERNO NACIONAL

Paraguay de la gente

Tabla de Contenido

Tabla de Figuras

INTRODUCCIÓN

Este informe presenta el estado de la ciberseguridad en el Paraguay en un esfuerzo por fortalecer el intercambio de información, las capacidades y el nivel de conciencia en relación con las crecientes amenazas a la seguridad digital en la región.

Se presentan datos estadísticos históricos en base a los reportes de incidentes cibernéticos recibidos por el CERT-PY desde que empezó a operar a fines del año 2013, con un especial énfasis en los datos, estadísticas, tendencias y evolución a lo largo del año 2019. Se incluyen además algunos datos estadísticos de fuentes públicas y/o abiertas, tales como Kaspersky, Microsoft y Shadowserver, que permiten identificar algunas tendencias de las amenazas cibernéticas en nuestro país.

Por otra parte, también contiene un resumen del estado actual en materia de políticas y normativas de ciberseguridad, formación de capacidades y concienciación en Paraguay. Por último, un resumen del posicionamiento de Paraguay en los rankings globales y regionales de ciberseguridad respecto al resto del mundo, identificando los avances y los futuros desafíos.

Incidentes cibernéticos - CERT-PY

El **Centro de Respuestas a Incidentes Cibernéticos (CERT-PY)** es el organismo coordinador de incidentes cibernéticos que afectan al ecosistema digital nacional.

Se entiende por **incidente cibernético** a todo evento contra un sistema de información que produce la violación de una política de seguridad explícita o implícita, poniendo en riesgo la confidencialidad, integridad y disponibilidad del mismo.

El CERT-PY define las siguientes categorías de incidentes cibernéticos:

- **Compromiso de Sistemas:** por lo general, se trata de servidores comprometidos como por ejemplo una desfiguración de un sitio web (*defacement*), inyección de código malicioso, alojamiento de artefactos o archivos maliciosos (malware o archivos de phishing), entre otros.
- **Correo no deseado malicioso (Spam/Scam):** correos electrónicos maliciosos que son enviados desde cuentas de correo o servidores de correo comprometidos, o máquinas infectadas que forman parte de una spam-botnet. Los correos maliciosos pueden distribuir malware, campañas de phishing o pueden ser simplemente engaños o estafas (estafa nigeriana, *hoax* u otro tipo de mensajes engañosos).
- **Phishing:** por lo general, se trata de páginas web o formularios falsos, que buscan impersonificar alguna organización de confianza para que las víctimas ingresen sus credenciales y/o información personal en ella, y ésta sean obtenidas así por el atacante.
- **Software malicioso (Malware):** porciones de código malicioso que ejecuta acciones maliciosas en el sistema que es instalado; se puede tratar de un virus, troyano, gusano, script, ransomware, etc. pudiendo tener varios objetivos: robo de información, envío de spam, keylogger, control remoto del equipo infectado, entre muchas otras.
- **Acceso indebido a cuentas, sistemas o sus datos:** esta categoría describe un evento en el cual un atacante logra acceder de manera no autorizada a alguna cuenta o a algún conjunto de datos, a través de alguna técnica cibernética (explotación de vulnerabilidades, ingeniería social, malware, etc.).
- **Escaneo / Fuerza bruta:** se trata de un intento de acceso o explotación de un sistema, por lo general, desde una IP de un sistema que se encuentra comprometido. Engloba los intentos de acceso mediante adivinación o cracking de contraseña de un sistema publicado a Internet, escaneo de puertos, intento de explotación de una vulnerabilidad de un sistema publicado a Internet, etc.
- **Problema de configuración / vulnerabilidad:** esta categoría describe los problemas de configuración o sistemas vulnerables que son encontrados en Internet y que constituye un riesgo inminente, tales como servicios y/o información sensible públicamente expuestos, contraseñas por defecto, etc.

- **Denegación de servicios (DoS/DDoS):** se trata de ataques que dejan indisponible algún recurso, ya sea debido a un agotamiento de recursos o una inundación de tráfico o peticiones. Se divide a su vez en varias categorías: TCP Flood, Syn Flood, UDP Flood, reflexión DNS, reflexión NTP, SlowHTTP, entre otras. Puede ser simple (un único origen o un número limitado de IPs de origen) o distribuido (múltiples fuentes de ataque).

El CERT-PY brinda un servicio permanente de gestión de incidentes cibernéticos, disponible para cualquier persona u organización, sin ningún costo. Cualquier ciudadano, empresa, institución pública u organización extranjera puede reportar un incidente cibernético que afecte a un sistema de información del ecosistema digital nacional, propio o de terceros.

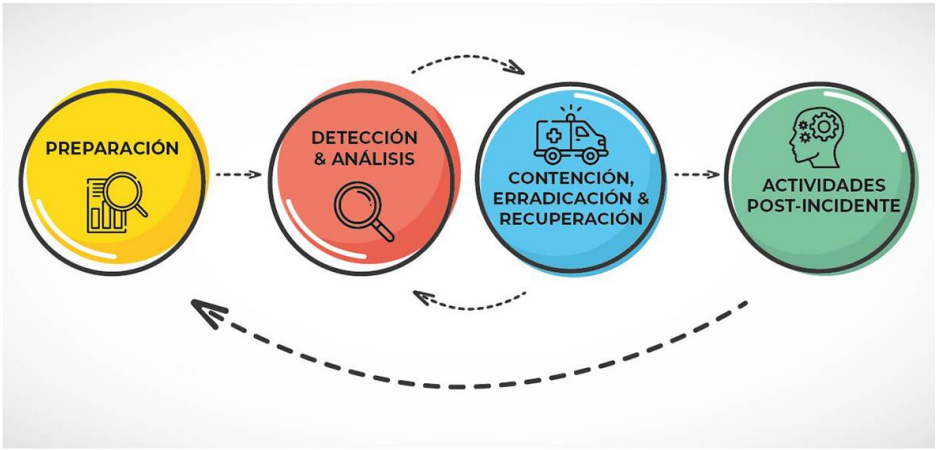


Figura 1. *Fases del proceso de Gestión de Incidentes Cibernéticos*

El alcance de la gestión de un incidente cibernético a cargo de los analistas del CERT-PY abarca: el **análisis preliminar** del incidente cibernético, la aplicación de **acciones de contención** inmediatas, la **investigación** y la propuesta de **recomendaciones pertinentes para la corrección y prevención** futura.

Los procedimientos de gestión de incidentes cibernéticos se encuentran alineados a los estándares internacionales y han sido establecidos con el objetivo de optimizar los tiempos de respuesta y resolución de incidentes cibernéticos, de una manera oportuna y eficaz.

Estadísticas históricas del Sistema de Gestión de Incidentes del CERT-PY

A continuación, se presentan estadísticas obtenidas a partir de los incidentes cibernéticos reportados y gestionados a través del servicio, desde su puesta en funcionamiento el 25/09/2013, hasta el 31/12/2019. Estos incidentes cibernéticos son reportados por los ciudadanos, funcionarios de gobierno, profesionales independientes y de empresas privadas, CSIRTs extranjeros, etc. o detectados por el CERT-PY de forma no sistemática, por lo que los incidentes no reportados no estarán reflejados en esta estadística.

- Reportes recibidos: 4986
- Cantidad total de Incidentes atendidos: 470
- Investigaciones realizadas: 770

Definiciones

Reporte de Incidente cibernético: es aquella notificación que se recibe de parte de una persona en la que se da a conocer un posible incidente cibernético.

Incidente cibernético: se refiere al caso que un analista crea, luego de verificar que uno o más de un reporte corresponde efectivamente a un incidente cibernético, de acuerdo a las definiciones establecidas.

Investigación: se refiere al análisis que se realiza sobre un determinado sistema o conjunto de sistemas involucrados en un incidente cibernético. Un incidente cibernético puede derivar en una o más de una investigación.

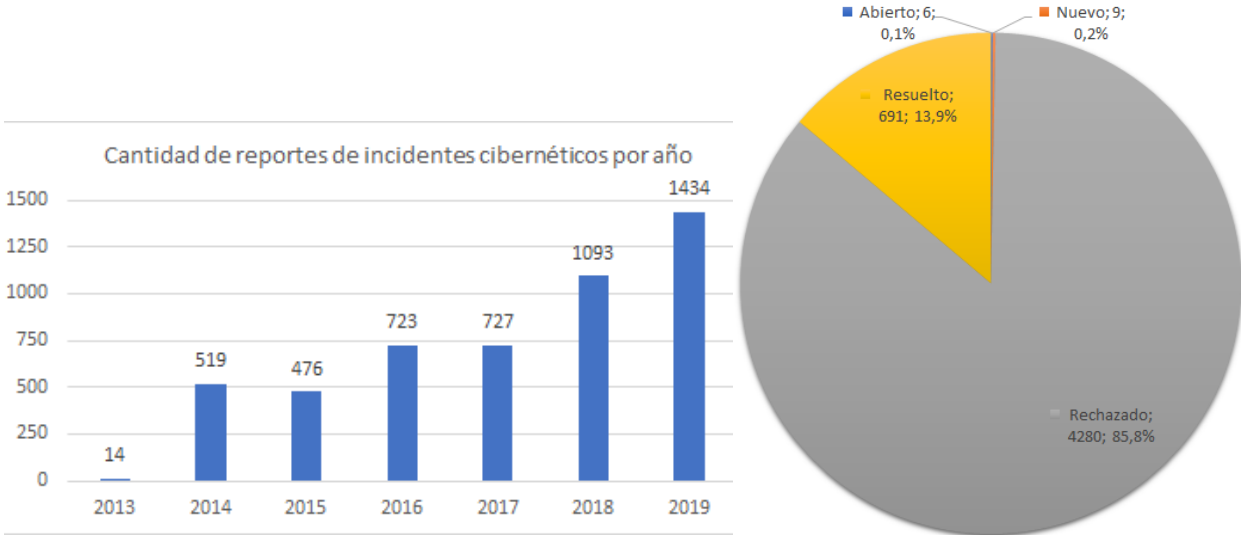


***Figura 2**. Reportes de Incidentes cibernéticos recibidos*

Figura 3. *Incidentes cibernéticos atendidos*

Figura 4. *Investigaciones realizadas*

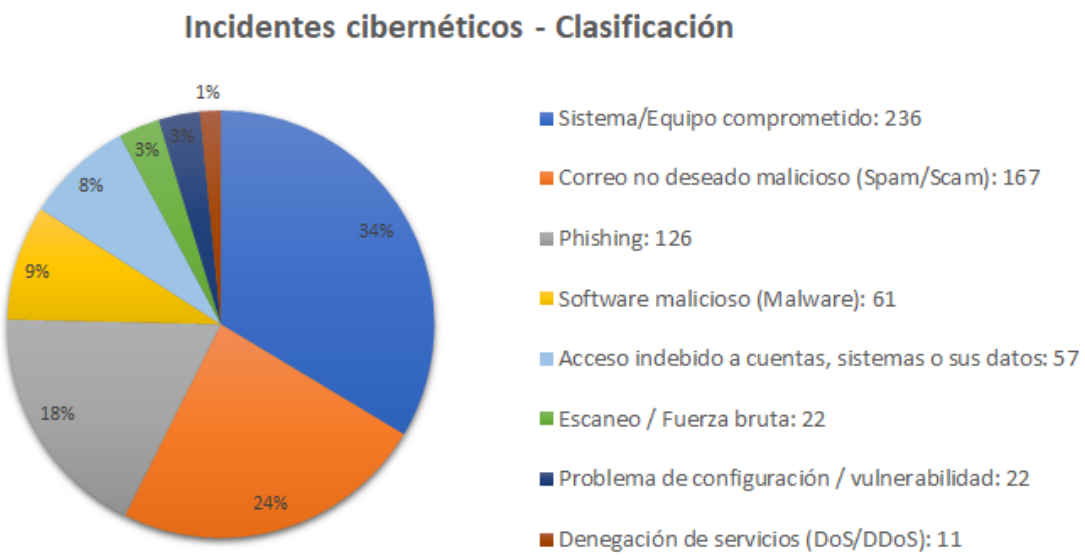


Figura 5. *Distribución porcentual de incidentes cibernéticos reportados, categorizados por tipo de incidentes*

La mayor cantidad de incidentes investigados son los **sistemas o equipos comprometidos**, tales como desfiguraciones de sitio web (*defacement*), servidores comprometidos que alojan códigos maliciosos, phishing u otro tipo de artefactos maliciosos, etc., **con un total de 236 incidentes atendidos.** En la mayoría de los casos, el compromiso se debió a páginas web con credenciales débiles (contraseñas fáciles y/o por defecto, tanto del CMS o componentes web o de SSH), en otros casos se debió a páginas web desactualizadas y vulnerables (plugins vulnerables, CMS vulnerables, programación a medida con errores, etc.). Los **ataques de denegación de servicio** son los menos reportados e investigados, **con un total de 11 incidentes**. Esto se debe, en parte, a que muchas víctimas de DoS/DDoS optan por reportarlo únicamente a su proveedor de servicio de Internet en el momento que están siendo atacados, en parte, debido a la sabida dificultad de llegar al origen real del ataque.

- **Gobierno:** 236 incidentes
- **Privado:** 90 incidentes
- **Extranjero**: 104 incidentes
- **Ciudadano:** 32 incidentes
- **Educativo:** 26 incidentes

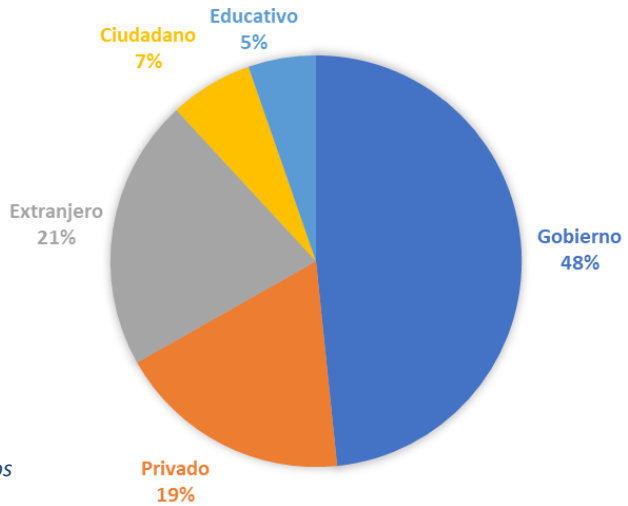


Figura 6*. Sectores afectados por incidentes cibernéticos*

Se observa un mayor número de incidentes cibernéticos que afectan a sistemas o redes de instituciones gubernamentales, con un total de 236 incidentes. Sin embargo, el número de incidentes relacionados a redes o sistemas de empresas privadas o de ciudadanos particulares es inferior. Esto probablemente se deba a que muchos ciudadanos e incluso profesionales del sector privado no conocen este servicio y/o no lo utilizan, por lo cual se observa una menor cantidad de incidentes del sector ciudadano y privado y se podría dar por diversas razones:

- las empresas privadas, especialmente las pequeñas/medianas, carece de mecanismos de detección de incidentes, por lo que no se enteran de los mismos;
- no consideran que los incidentes ameritan ser reportados;
- desconocen el rol del CERT-PY y/o el aporte o beneficio que le puede traer a su negocio;
- consideran innecesario o no rentable invertir en la investigación, resolución y prevención de los incidentes, por lo que optan por no reportarlo.

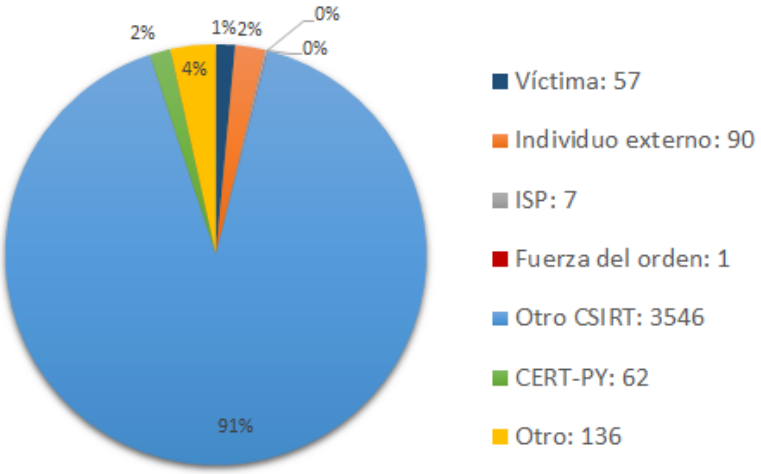


Figura 7. *Reportes de incidentes por tipo de denunciante*

Se puede ver que la gran mayoría de los reportes son generados por otros equipos de respuesta a incidentes cibernéticos (CSIRTs). Esto se debe, en parte al menos, a que los CSIRTs se dedican de manera permanente al reporte de incidentes e indicadores de compromiso, a diferencia de las propias víctimas, que muchas veces no reportan un incidente por diversas razones:

- ignoran que son víctimas de un ciberataque,
- no saben dónde y cómo reportarlo,
- desconocen la importancia o beneficio de reportarlo, etc.

Muchas veces un incidente corresponde a más de una categoría, por lo que las estadísticas por categorías no corresponden a incidentes únicos, sino a todos los incidentes atendidos que corresponden a una

determinada categoría. Por ejemplo, un sitio de phishing que está alojado en un servidor web, corresponde a la categoría phishing, pero también corresponde a la categoría de Servidor/Equipo comprometido.

Distribución temporal de incidentes cibernéticos

Desde el inicio del servicio, la mayor cantidad de reportes de incidentes cibernéticos se ha tenido en los meses de **noviembre**, con un pico de 735 reportes, seguido del mes de diciembre, con 493 reportes. En los meses de marzo se ha recibido la menor cantidad de incidentes, con 301 reportes recibidos.

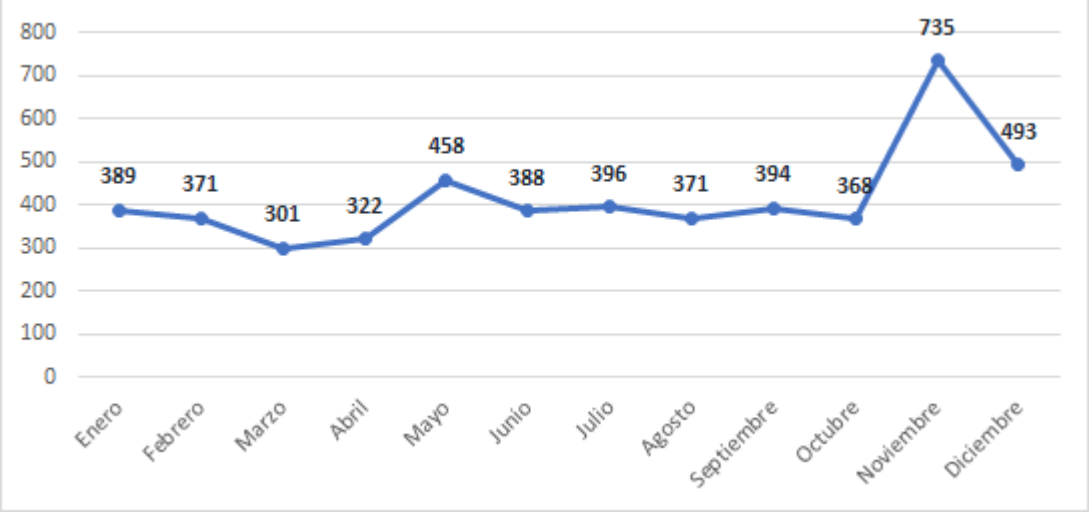


Figura 8. *Cantidad de reportes de incidentes cibernéticos por mes del año*

La mayor cantidad de reportes de incidentes cibernéticos se reciben los **lunes**, en los que se ha recibido un total de 1054 reportes, con un decrecimiento gradual durante la semana, hasta un mínimo los sábados y domingo, con 459 y 458 reportes respectivamente.

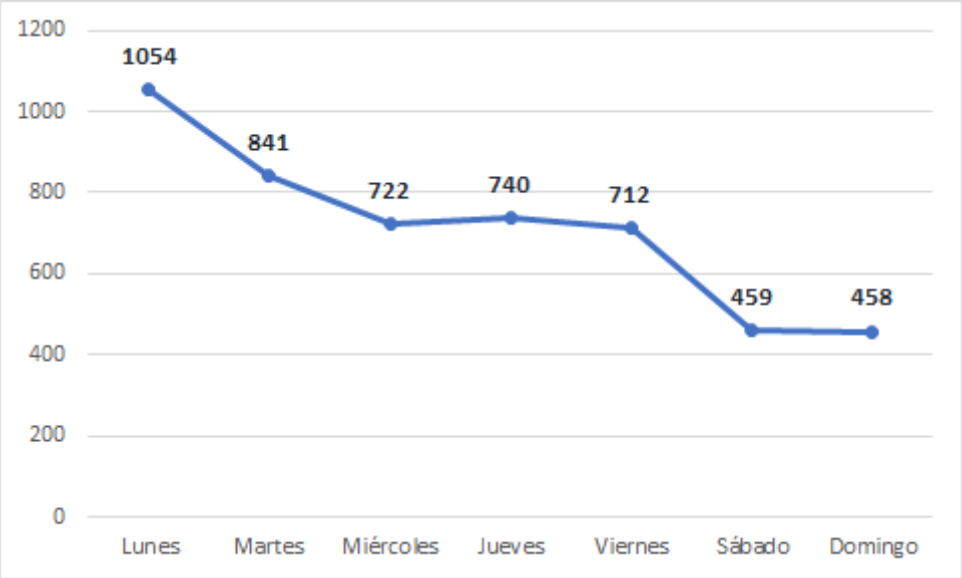


Figura 9. *Cantidad de reportes de incidentes cibernéticos por día de la semana*

Evolución del tiempo de respuesta y atención

Durante el año 2019 se realizó una reestructuración total del servicio de gestión de incidentes cibernéticos, que incluyó el diseño, elaboración e implementación de procedimientos técnicos formales escritos (*playbooks*), así como también la incorporación de analistas técnicos dedicados exclusivamente a la atención de los incidentes. Igualmente, se implementaron mejoras en el sistema de gestión de incidentes con la incorporación de métricas granulares, indicadores de correlación de incidentes, entre otras.

Estas mejoras permitieron mejorar enormemente los tiempos de respuesta y resolución de los incidentes cibernéticos, de una manera sostenible en el tiempo. Igualmente, permitió atender y resolver oportunamente un mayor número de reportes incidentes que anteriormente quedaban abandonados.

Las mejoras se implementaron de manera definitiva a partir de noviembre de 2019.

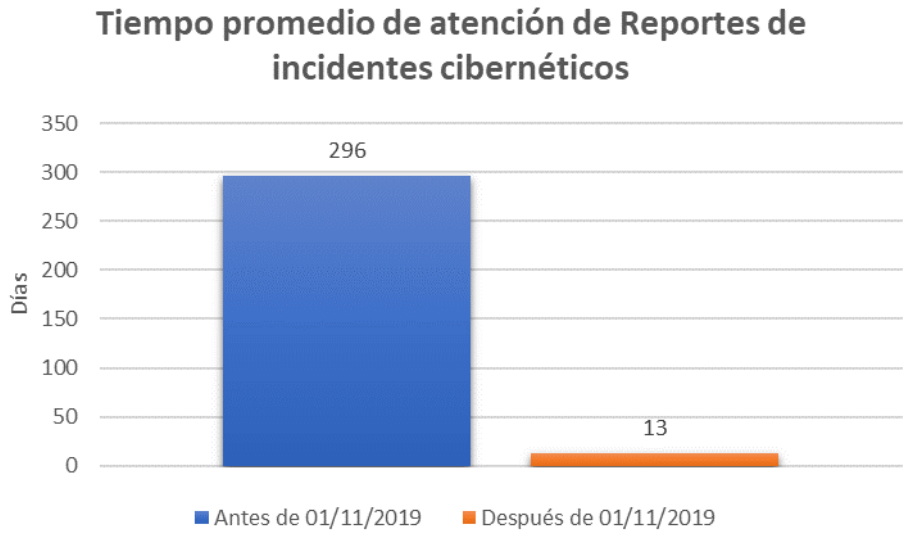


Figura 10. *Mejora del tiempo promedio de atención[1] de los reportes de incidentes cibernéticos*

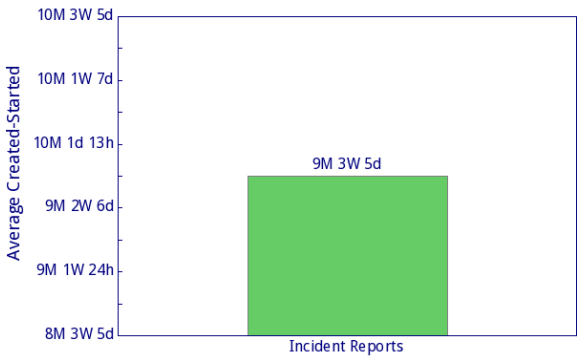


Figura 11. *Tiempo promedio de atención de los reportes de incidentes antes de 01/11/2019: 9 meses 3 semanas 5 días = 296 días*

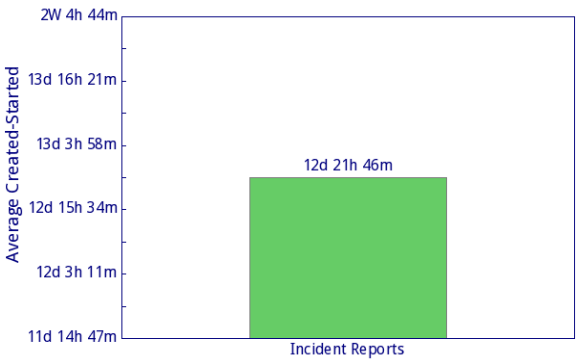


Figura 12*. Tiempo promedio de atención de los reportes de incidentes posterior a 01/11/2019: menos de 13 días*

[1] Se entiende como "tiempo de atención" al tiempo transcurrido desde que una persona realizó un reporte hasta que un analista lo abrió y realizó una acción por primera vez.

Tiempo promedio de resolución[2] de incidentes cibernéticos:

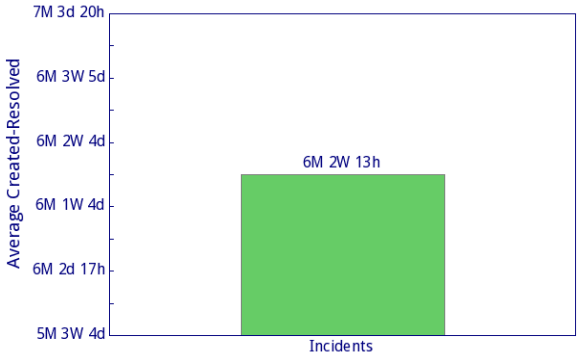


Figura 13. *Tiempo promedio de resolución de incidentes cibernéticos antes del 01/11/2019: 194,5 días*

Figura 14. *Tiempo promedio de resolución de incidentes cibernéticos posterior al 01/11/2019: menos de 35 horas*

Estas mejoras son reflejadas en la evolución histórica de los tiempos respuesta promedio y los porcentajes de resolución de incidentes cibernéticos a lo largo del tiempo, como puede observarse en los siguientes gráficos:

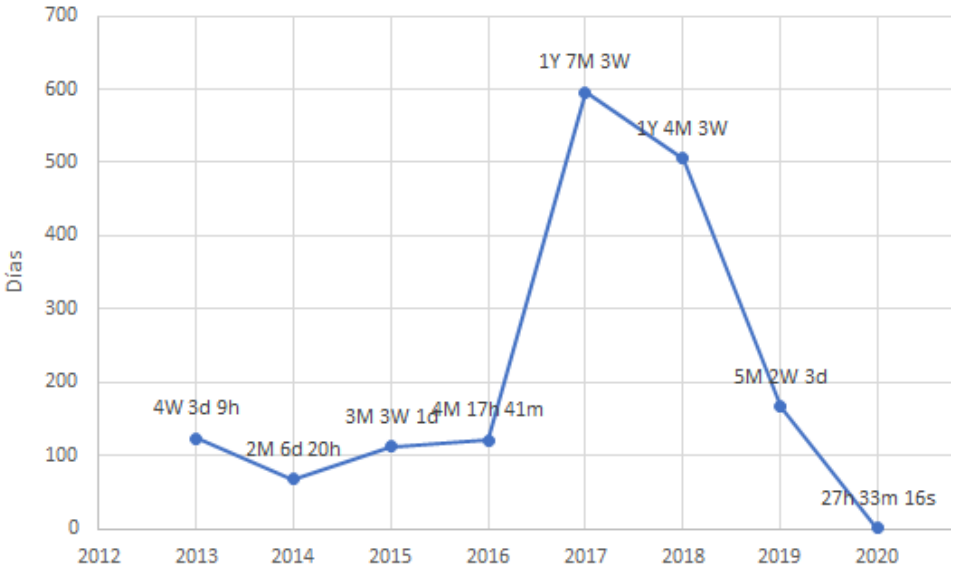


Figura 15. *Evolución histórica del tiempo promedio de atención de reportes (anual)*

[2] Se entiende como "tiempo de resolución" al tiempo transcurrido desde la creación de un incidente cibernético hasta que éste es resuelto (mitigado, controlad, corregido y/o derivado) y cerrado. En algunos casos, las acciones de corrección del incidente dependen exclusivamente del administrador; dichos casos se consideran resueltos y se cierran luego de que el administrador tomó conocimiento (derivación).

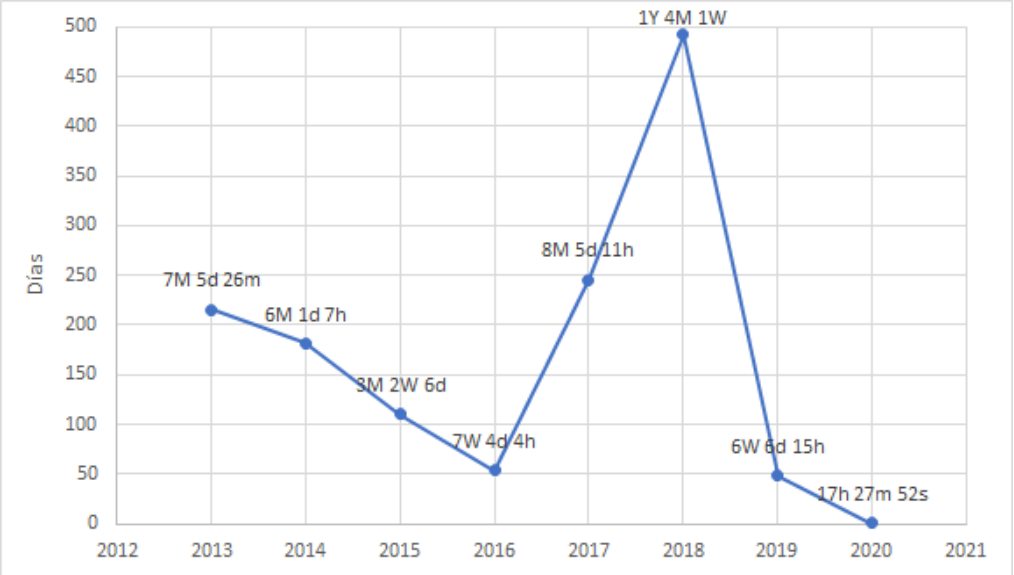


Figura 16. *Evolución histórica del tiempo promedio de resolución de incidentes (anual)*

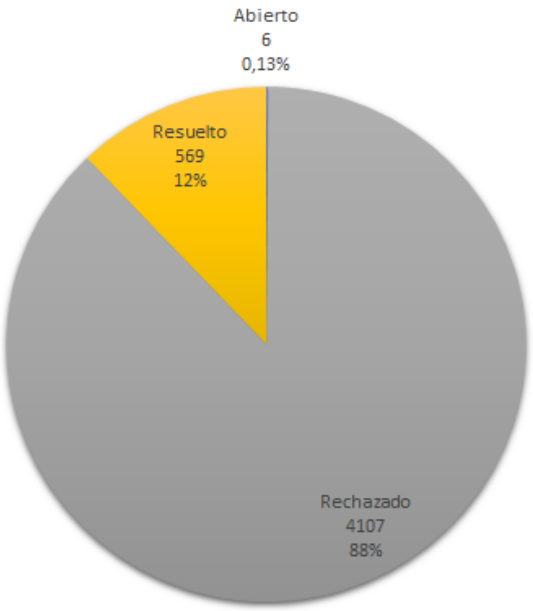


Figura 17. *Cantidad de reportes resueltos antes de 01/11/2019: 569 (12.1%)*

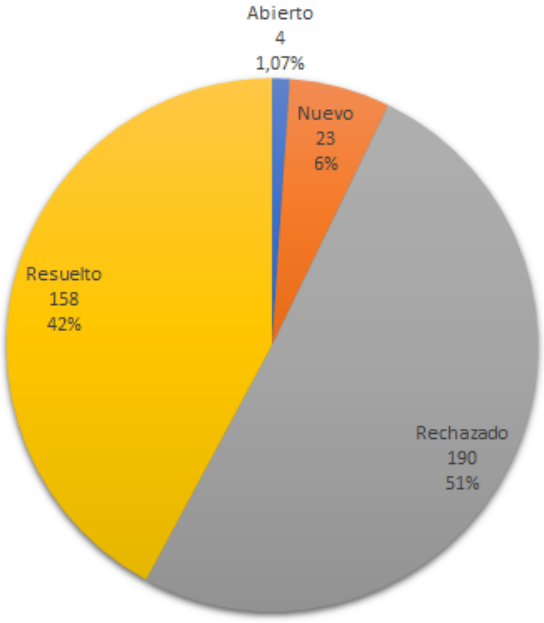


Figura 18. *Cantidad de reportes resueltos posterior al 01/11/2019: 158 (42%) - se registra una mejora de +29.9% en el ratio de resolución de reportes*

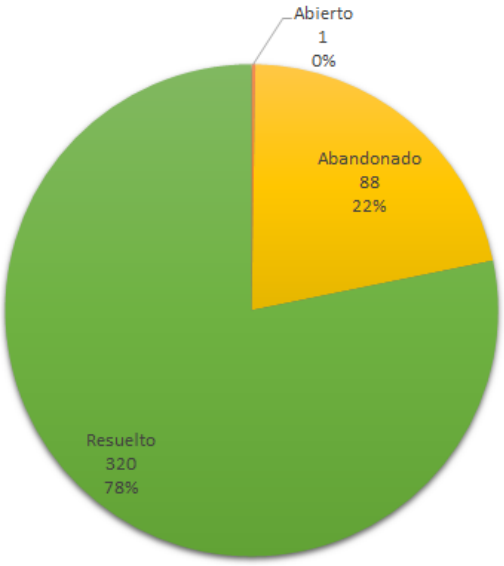


Figura 19. *Cantidad de incidentes resueltos antes de 01/11/2019: 320 (78.2%)*

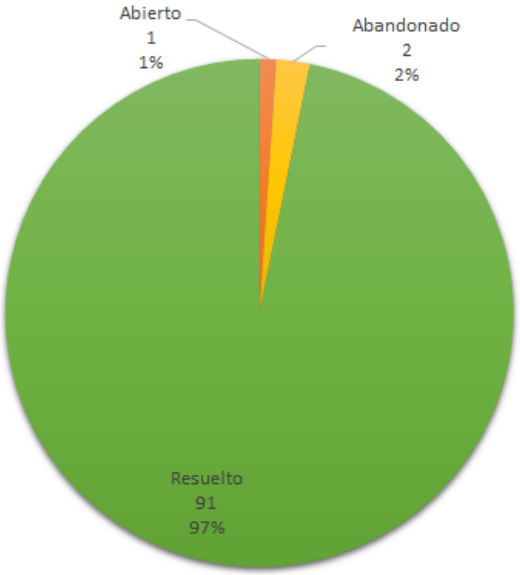


Figura 20. *Cantidad de incidentes resueltos posterior al 01/11/2019: 91 (96.8%) - se registra una mejora de +18.6% en el ratio de resolución de incidentes únicos atendidos*

Debe tenerse en cuenta que algunos incidentes no pueden ser resueltos debido a factores externos (la víctima no responde más, el responsable no toma las acciones solicitadas y no existe manera de obligarlo, etc.), en cuyo caso el incidente queda en estado “abandonado”.

Incidentes cibernéticos en el año 2019

En el año 2019 se ha recibido un total de 1.434 reportes de incidentes cibernéticos, de los cuales 161 se han resuelto, 5 continúan abiertos en investigación y 10 todavía no habían sido procesados a la fecha de la obtención de datos.

Estado	Ticket count
abierto	5
nuevo	10
rechazado	1258
resuelto	161
Total	1434

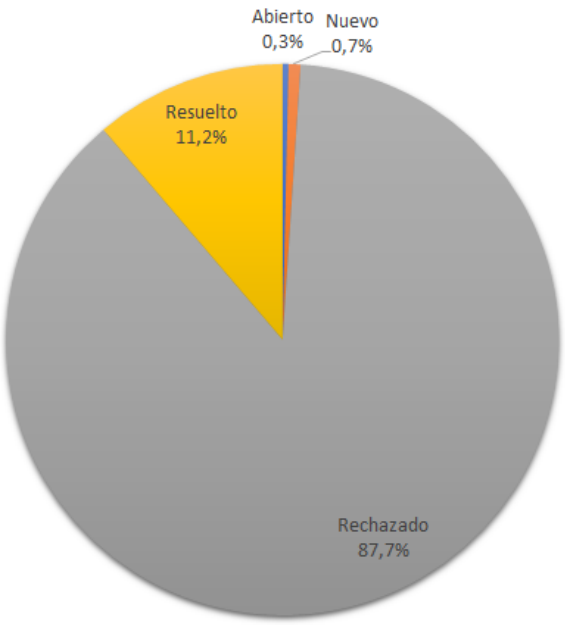


Figura 21. *Cantidad de Reportes de Incidentes en el año 2019*

1258 reportes han sido rechazados. El alto número de rechazo corresponde a diversos factores:

- reportes falsos, provenientes de cuentas de spam,
- reportes masivos que, hasta enero 2020, no podían ser procesados manualmente y debían rechazarse (Ver https://www.cert.gov.py/index.php/noticias/el-cert-py-incorpora-sistema-automatizado-de-notificacion-de-indicadores-de-incidentes-ciberneticos-iocs),
- falta de analistas dedicados a su atención hasta antes de noviembre de 2019; debido a ello, muchos reportes ya no eran válidos para ser atendidos[3].

En la siguiente figura se puede observar una mejora sustancial del tiempo promedio de atención de los reportes, con un promedio inicial de más de 9 meses en enero, hasta un promedio de menos de 9 días en diciembre.

[3] Debe tenerse en cuenta que un incidente debe ser gestionado en un rango de tiempo cercano a la ocurrencia de éste, de lo contrario la evidencia y/o los indicadores de compromiso que hayan sido reportados ya no son válidos y el caso no puede ser investigado, por lo cual debe rechazarse.

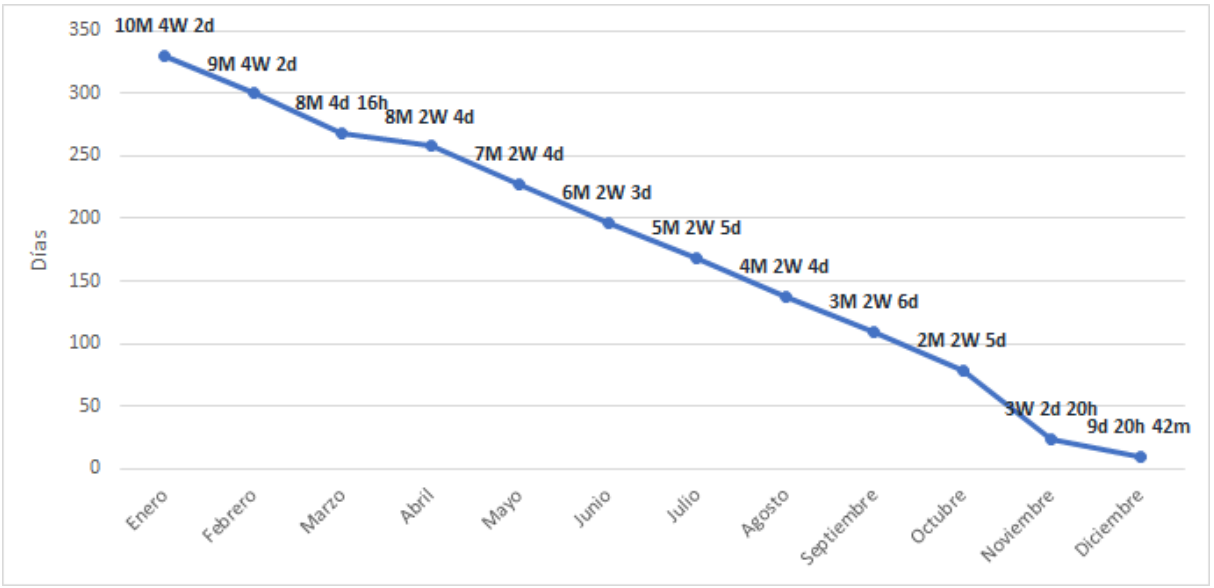


Figura 22. *Evolución del tiempo promedio de atención de reportes (mensual)*

Se puede observar una mejora importante en el tiempo promedio de solución de los incidentes a partir de noviembre, debido a las mejoras implementadas en los procesos de gestión de incidentes (Ver sección "Evolución de tiempo de respuesta y atención")

La mayor cantidad de reportes se ha recibido en el mes de noviembre (162 reportes), seguido de enero (149 reportes) y diciembre (142 reportes). Esto es consistente con el comportamiento histórico, con picos de incidentes cibernéticos hacia el final e inicio de año, coincidiendo con las fiestas, la época de turismo, periodos de vacaciones, etc.

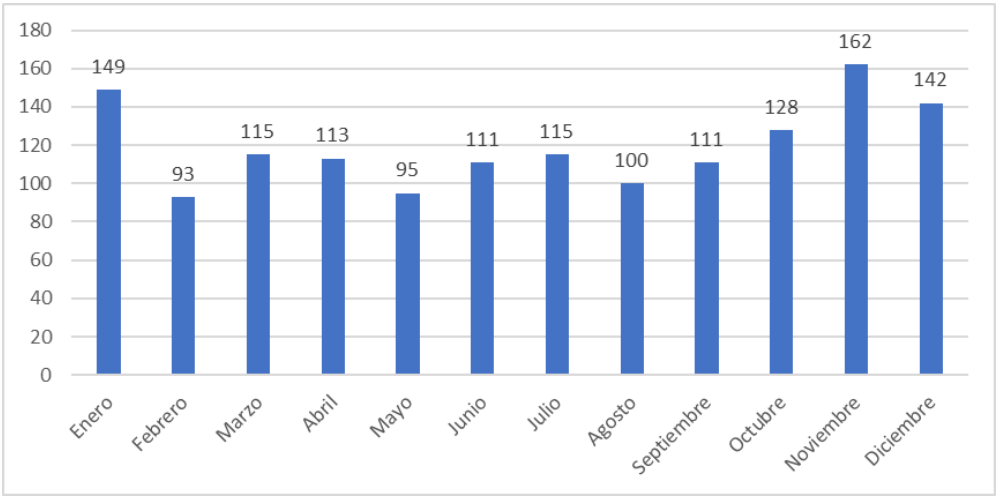


Figura 23. *Reportes de incidentes recibidos en el año 2019 por mes*

De esos reportes se ha detectado un total de 78 incidentes cibernéticos únicos, de los cuales 68 se han resuelto (87,2%). 10 incidentes se han abandonado por diversas razones, que escapan al alcance del CERT-PY (falta de respuesta de la víctima y/o organización involucrada en el caso, instancias de escalación agotadas, etc.).

Estado	Ticket count
abandoned	10
resuelto	68
Total	78

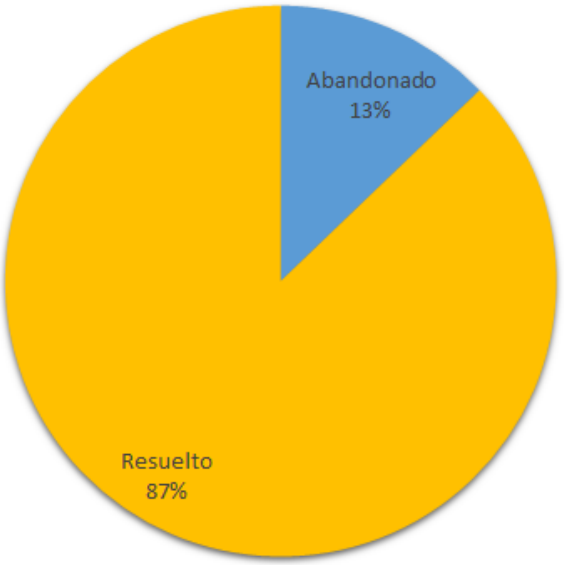


Figura 24. *Cantidad de Incidentes únicos en el año 2019*

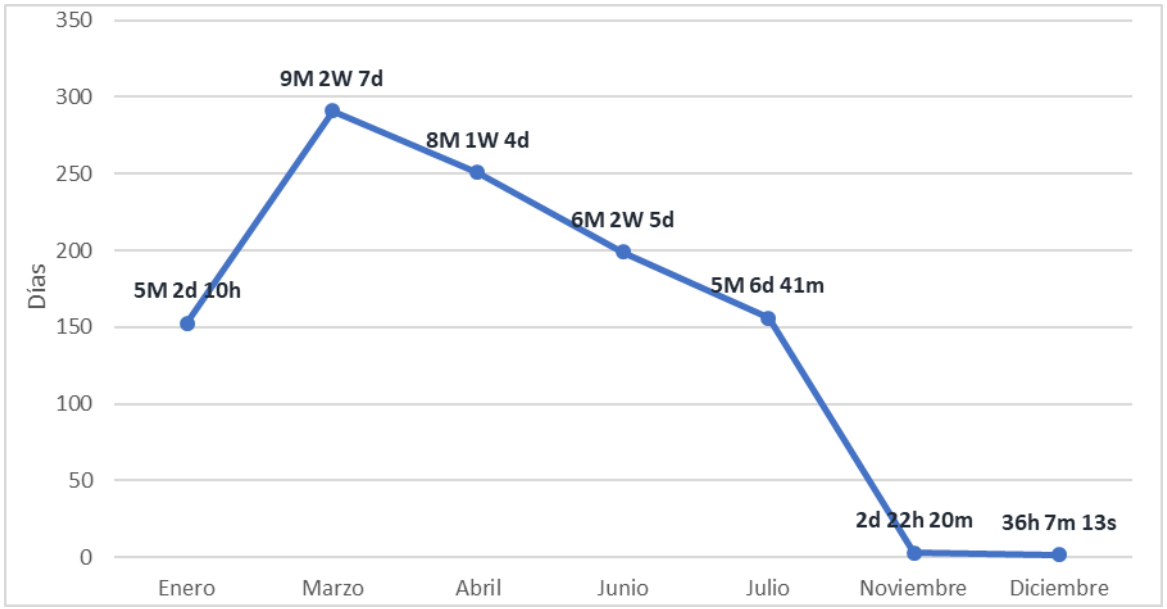


Figura 25. *Evolución del tiempo promedio de resolución de los incidentes cibernéticos (mensual)*

Estos incidentes cibernéticos han derivado en 181 investigaciones únicas, de las cuales 180 se han sido resueltas y 1 permanece activa.

Estado	Ticket count
abierto	1
resuelto	180
Total	181

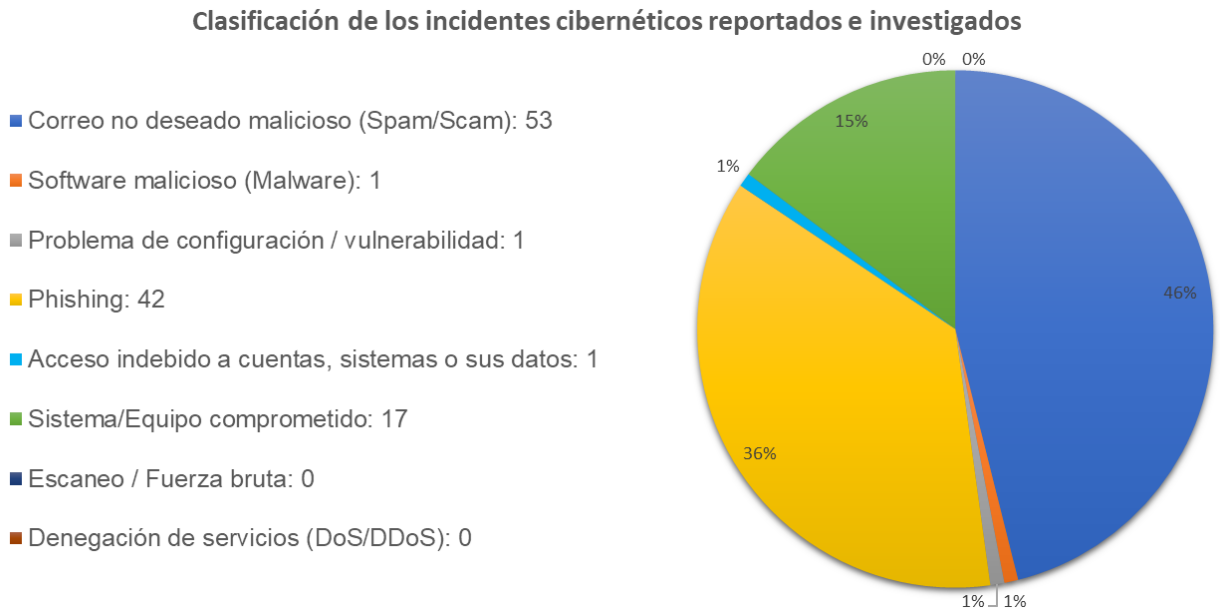


Figura 26. *Distribución porcentual de incidentes cibernéticos reportados en 2019, categorizados por tipo de incidentes*

Estadísticas obtenidas de fuentes externas abiertas

Vulnerabilidades explotadas por malware

De acuerdo a datos de Kaspersky, la tendencia en cuanto a explotación de vulnerabilidades ha sido la suite Microsoft Office, cuyas vulnerabilidades han sido las más explotadas por las diversas familias de malware, tanto para su implantación como para su distribución y propagación. En segundo lugar, se encuentran las vulnerabilidades de navegadores, seguido de las del sistema operativo Android.

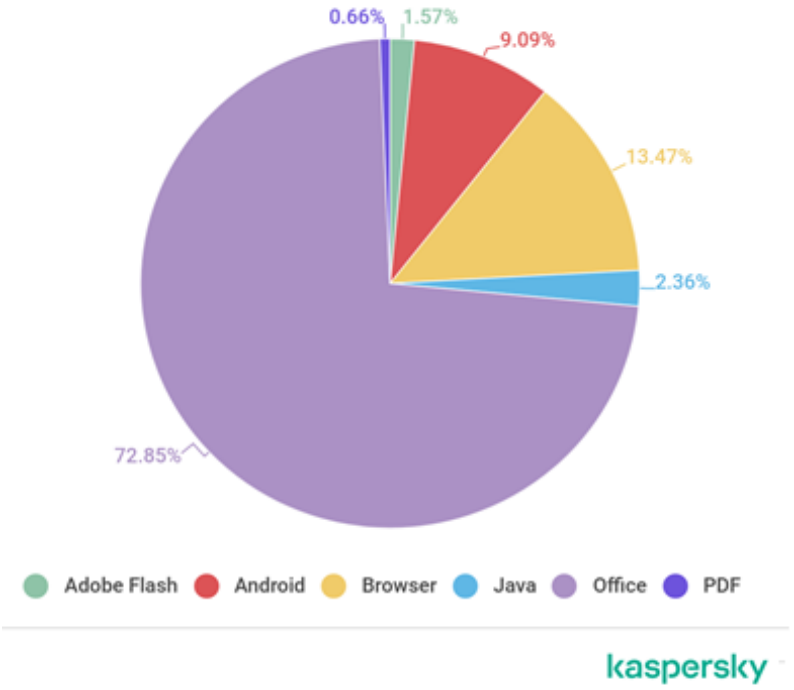


Figura 27. *Vulnerabilidades más explotadas mundialmente en 2019*

Luego de la publicación del conjunto de exploits conocido como ShadowBrokers, la gran mayoría de los intentos de explotación de vulnerabilidades, ya sea mediante ataques remotos a través de la red, o a través de malware, utilizan estos exploits.

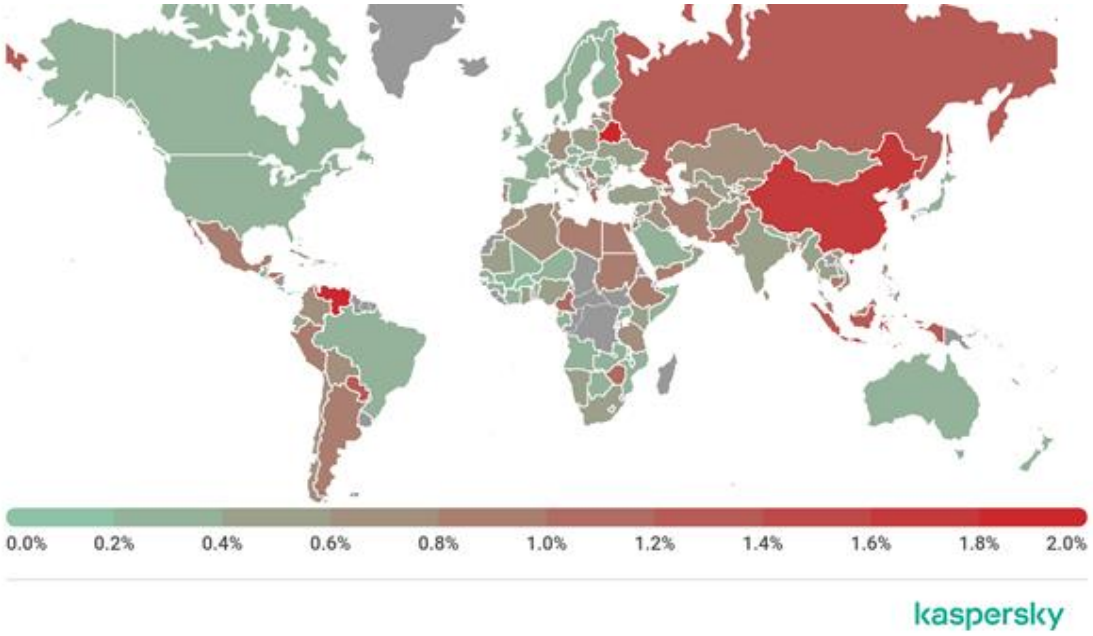
La vulnerabilidad CVE-2017-11882 que afecta a Microsoft Office y que ya fue descubierta en el 2017 sigue siendo la segunda más explotada.

1	Exploit.Win32.ShadowBrokers.ae	22.22%
2	Exploit.MSOffice.CVE-2017-11882.gen	7.78%
3	Exploit.Win32.ShadowBrokers.ab	6.67%
4	Exploit.Win32.ShadowBrokers.aa	6.67%
5	Exploit.Win32.ShadowBrokers.z	6.67%
6	Exploit.Win32.ShadowBrokers.ad	6.67%
7	Exploit.Win64.ShadowBrokers.c	6.67%
8	Exploit.Win64.ShadowBrokers.d	6.67%
9	Exploit.Script.Generic	5.56%
10	Exploit.AndroidOS.Lotoor.bg	5.56%

Figura 28. *Top 10 de vulnerabilidades más explotadas en Paraguay – Fuente: Kaspersky*[4]

Amenazas financieras

De acuerdo a datos de Kaspersky[5], entre los meses de abril a junio se observó un aumento en la cantidad de amenazas financieras detectadas en Paraguay (troyanos bancarios y malware para ATM/POS), por encima de la media (1,2%).



[4] Estadística obtenida de fuentes abiertas disponibilizadas por Kaspersky y obtenida de usuarios de sus productos

[5] Fuente: https://securelist.com/it-threat-evolution-q2-2019-statistics/92053/

	Country*	%**
1	Belarus	2.0
2	Venezuela	1.8
3	China	1.6
4	Indonesia	1.3
5	South Korea	1.3
6	Cyprus	1.2
7	Paraguay	1.2
8	Russia	1.2
9	Cameroon	1.1
10	Serbia	1.1

** Excluded are countries with relatively few Kaspersky product users (under 10,000).*

*** Unique users whose computers were targeted by banking Trojans as a percentage of all unique users of Kaspersky products in the country.*

***Figura 29**. Mapa de distribución de amenazas financieras en el mundo (Q2 2019) – Fuente: Kaspersky*[6]

	Name	Verdicts	%*
1	RTM	Trojan-Banker.Win32.RTM	32.2
2	Zbot	Trojan.Win32.Zbot	23.3
3	Emotet	Backdoor.Win32.Emotet	8.2
4	Nimnul	Virus.Win32.Nimnul	6.4
5	Trickster	Trojan.Win32.Trickster	5.0
6	Nymaim	Trojan.Win32.Nymaim	3.5
7	SpyEye	Backdoor.Win32.SpyEye	3.2
8	Neurevt	Trojan.Win32.Neurevt	2.8
9	IcedID	Trojan-Banker.Win32.IcedID	1.2
10	Gozi	Trojan.Win32.Gozi	1.1

*** Unique users attacked by this malware as a percentage of all users attacked by financial malware.*

***Figura 30**. Familias de malware bancarios más detectados en Paraguay – Fuente: Kaspersky*[7]

A nivel mundial, el troyano bancario RTM ha sido el más detectado, seguido de **ZBot**, así como también **Emotet**. En el caso de Emotet, se ha observado numerosas empresas paraguayas afectadas por el mismo, como un instrumento para el desvío de dinero a través de correos electrónicos impersonificados con instrucciones de pago falsas; Emotet era utilizado para robar credenciales de correo guardadas de los archivos de configuración de los clientes de correo (Outlook, Thunderbird, etc.) y navegador, para que

[6] Estadística obtenida por Kaspersky, basada en las métricas de los usuarios de sus productos en el segundo cuatrimestre de 2019

[7] Estadística obtenida por Kaspersky, basada en las métricas de los usuarios de sus productos en 2019

los criminales pudieran así espiar las conversaciones de correo en busca de mensajes comerciales en los que se haga referencia a pagos o cobros de dinero mediante transferencias internacionales. En un momento oportuno, las bandas criminales impersonifican al cliente y/o proveedor con quien la empresa mantuvo la conversación, y le envían un mensaje con una instrucción de pago distinta a la acordada, bajo algún tipo de pretexto (ej.: "Hemos tenido problemas con la cuenta bancaria que le indiqué anteriormente, puede realizar la transferencia a esta otra cuenta? …"). El daño patrimonial reportado en Paraguay causado por Emotet, en un periodo comprendido únicamente de enero 2018 a octubre 2018, ascendía a casi 450.000USD[8]. Se debe tener en cuenta que no todas las empresas denuncian estos casos, por lo que el daño patrimonial puede ser más elevado.

Amenazas mediante navegación web

Si bien, Paraguay no se sitúa en el Top 20 de países de riesgo, de acuerdo a datos de Kaspersky[9], en al menos 6,05% de los usuarios[10] se detectaron intentos de infecciones de malware con origen en la navegación por Internet.

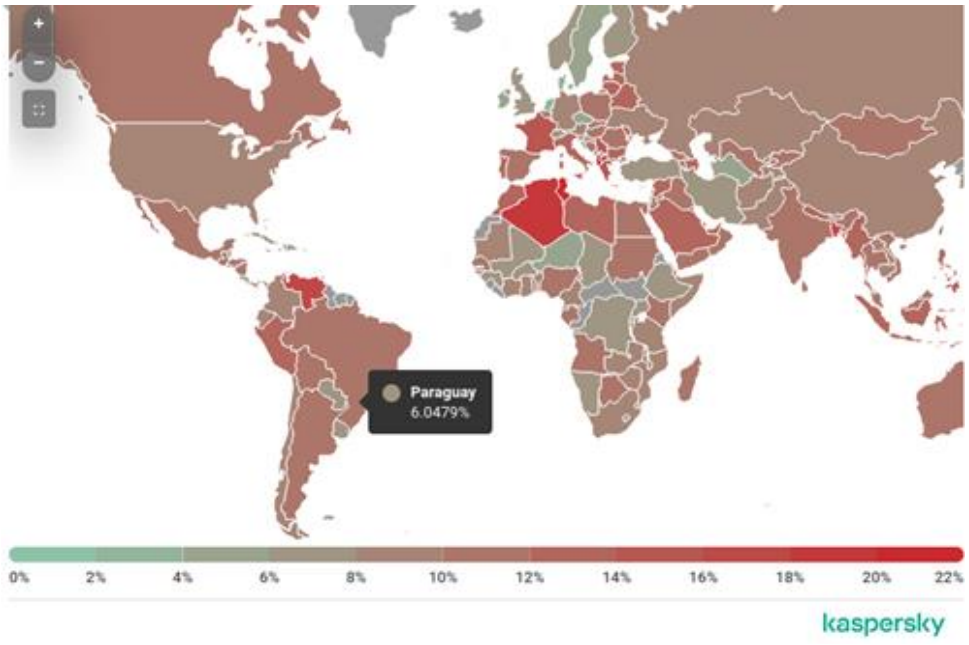


***Figura 31**. Mapa de distribución de amenazas mediante navegación web en el mundo (Q3 2019)- Fuente: Kaspersky[11]*

[8] Datos obtenidos del Ministerio Público en base a las denuncias recibidas por la Unidad Especializada de Delitos Informáticos
[9] Fuente: https://securelist.com/it-threat-evolution-q3-2019-statistics/95269/
[10] Estadística obtenida a partir del antivirus Kaspersky, por lo que el universo de la misma son únicamente los usuarios de sus productos
[11] Estadística obtenida a partir del antivirus Kaspersky, por lo que el universo de la misma son únicamente los usuarios de sus productos

1	Trojan.Script.Generic	74.98%
2	Trojan.Multi.Preqw.gen	13.35%
3	Trojan.Script.Miner.gen	3.83%
4	Trojan.PHP.Agent.kx	1.68%
5	Trojan.Script.Agent.bg	1.45%
6	Trojan-Downloader.Win32.BrainInst.gen	1.19%
7	Trojan-PSW.Script.Generic	0.49%
8	Backdoor.HTTP.TeviRat.gen	0.44%
9	Trojan.Script.Redirector.gen	0.3%
10	Trojan.Script.Iframer	0.28%

Figura 32. *Top 10 de amenazas web más detectadas en Paraguay – Fuente: Kaspersky*[12]

Una de las amenazas mediante navegación web son los ataques del tipo drive-by download. De acuerdo a datos de Microsoft[13], a pesar de las variaciones de detección de ataques del tipo drive-by download, el promedio general de Paraguay se mantuvo igual al año pasado (0,01%), inferior a la media mundial (0,08%). Se debe tener en cuenta que esta tasa de detección se basa únicamente en datos de navegación indexados mediante el navegador Bing.

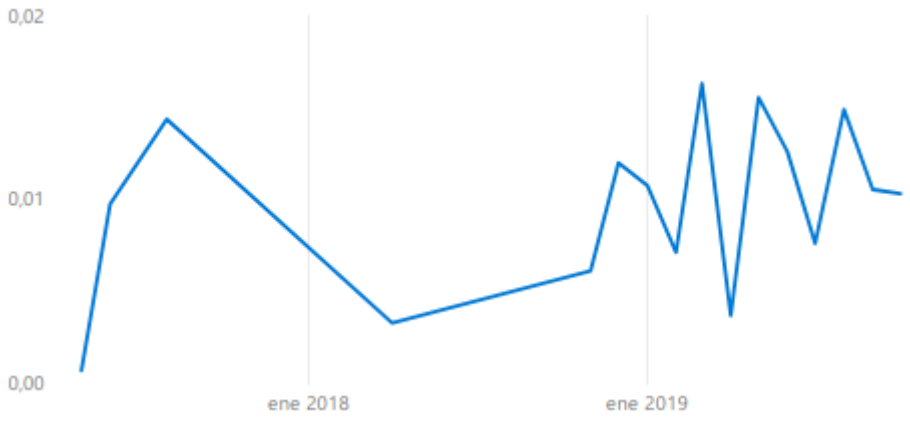


Figura 33. *Evolución histórica de las detecciones de ataques de drive-by download – Fuente: Microsoft*[14]

[12] Estadística obtenida a partir del antivirus Kaspersky, por lo que el universo de la misma son únicamente los usuarios de sus productos
[13] Fuente: https://www.microsoft.com/securityinsights/Driveby
[14] Estadística obtenida por Microsoft, basada en las métricas de los usuarios de sus productos

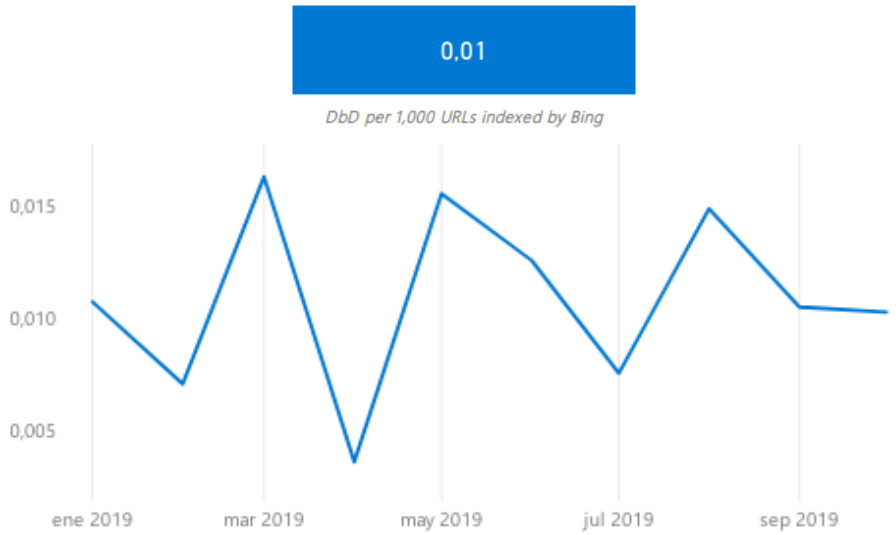


Figura 34. *Evolución de las detecciones de ataques de drive-by download en 2019 – Fuente: Microsoft*[15]

Detecciones de Malware

De acuerdo a los datos de Microsoft[16], si bien, en el 2019 hubo una disminución del porcentaje de detección de infecciones de malware, tanto a nivel mundial como también en Paraguay, la media de infecciones en Paraguay (4,81%) sigue siendo superior a la media mundial (3,24%). En marzo se tuvo un pico de infecciones por malware, con un promedio de 6,42% de detecciones.

Figura 35. Evolución histórica de detección de malware – Fuente: Microsoft[17]

[15] Estadística obtenida por Microsoft, basada en las métricas de los usuarios de sus productos

[16] Fuente: https://www.microsoft.com/securityinsights/Malware

[17] Estadística obtenida por Microsoft, basada en las métricas de los usuarios de sus productos

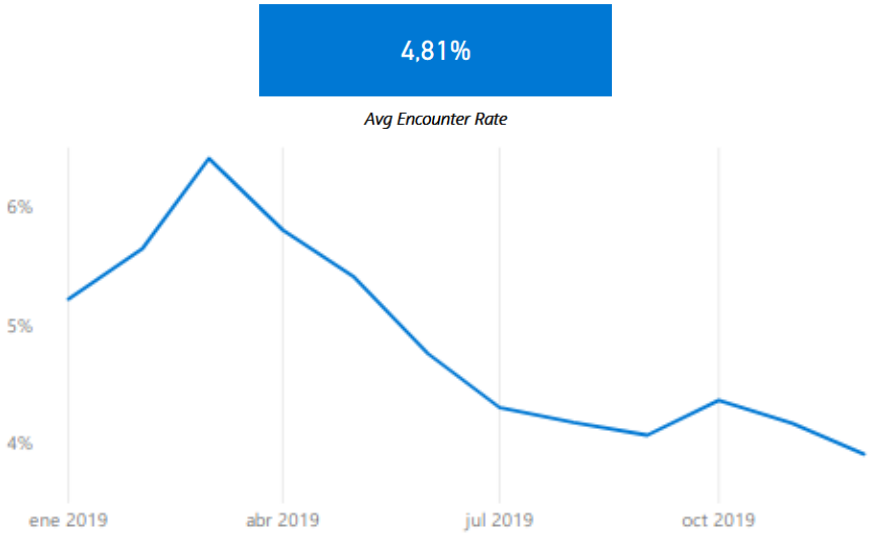


Figura 36. *Evolución de detección de malware en 2019 – Fuente: Microsoft*[18]

Amenazas de infecciones locales

De acuerdo a datos de Kaspersky[19], en aproximadamente 18,5% de los usuarios[20] se ha encontrado algún tipo de archivo o objeto malicioso que ha logrado ingresar al equipo de la víctima, ya sea mediante un dispositivo removible (USB, disco duro, etc.), un malware dropper[21] no detectado o una infección manual como parte de un ataque más avanzado. Este porcentaje es ligeramente inferior a la media mundial, 21.1%.

[18] Estadística obtenida por Microsoft, basada en las métricas de los usuarios de sus productos
[19] Fuente: https://securelist.com/it-threat-evolution-q3-2019-statistics/95269/
[20] Estadística obtenida a partir del antivirus Kaspersky, por lo que el universo de la misma son únicamente los usuarios de sus productos
[21] Un malware dropper es es un software diseñado para instalar algún tipo de malware en el sistema operativo donde ha sido ejecutado. El código malicioso puede estar contenido dentro del propio programa para evitar ser detectado por el antivirus o descargarse automáticamente desde Internet cuando el dropper se ejecuta

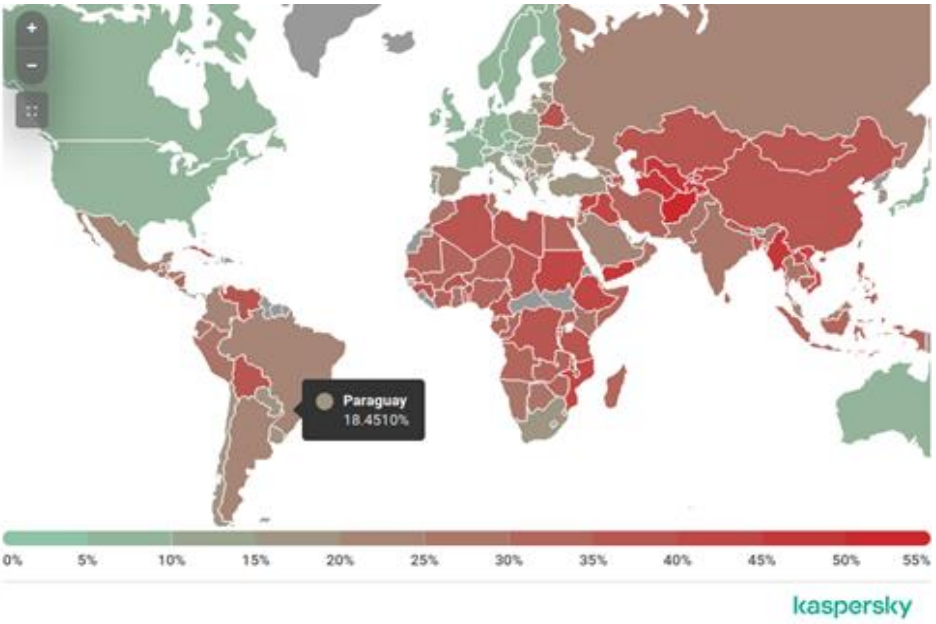


***Figura 37**. Mapa de distribución de equipos con infecciones locales en el mundo (Q3 2019). Fuente: Kaspersky*[22]

De acuerdo a las estadísticas de la empresa Kaspersky, la mayor cantidad de infecciones detectadas en Paraguay está relacionado a cracks o activadores de Microsoft (por ejemplo, crack o copia pirata de Microsoft Office). Esto está relacionado con el alto uso de programas pirata o sin licencia, los cuales representan un riesgo de seguridad, por múltiples motivos:

- el software "crackeado" puede esconder código malicioso
- el software "crackeado" no tiene acceso a las actualizaciones o parches de seguridad, por lo que las vulnerabilidades que sean descubiertas no serán corregidas, y por ende, será un posible punto de entrada para un ciberataque

[22] Estadística obtenida a partir del antivirus Kaspersky, por lo que el universo de la misma son únicamente los usuarios de sus productos

1	HackTool.MSIL.HackKMS.a	28.62%
2	HackTool.MSIL.HackKMS.d	10.54%
3	DangerousObject.Multi.Generic	6.66%
4	HackTool.MSIL.KMSAuto.dh	6.25%
5	HackTool.MSIL.KMSAuto.di	3.77%
6	Trojan.WinLNK.Agent.gen	3.67%
7	Trojan.WinLNK.Agent.qk	3.33%
8	HackTool.Win32.KMSAuto.c	3.29%
9	Trojan-Ransom.Win32.Wanna.m	2.23%
10	HackTool.MSIL.HackKMS.e	2.09%

Figura 38. *Top 10 de infecciones detectadas en Paraguay – Fuente: Kaspersky*[23]

Minería de criptomonedas

Se observa una importante disminución en la detección de infección mediante software malicioso de minería de criptomonedas, de un promedio de 0,17% en 2018 a un promedio actual de 0,07%, ligeramente inferior a la media mundial (0,08%). En el pasado, el mayor pico de infecciones se dio entre febrero a abril del 2018, con un promedio cercano a 0,4%

Figura 39. *Evolución histórica de detección de infecciones vinculados a minería de criptomonedas – Fuente: Microsoft*[24]

[23] Estadística obtenida a partir del antivirus Kaspersky, por lo que el universo de la misma son únicamente los usuarios de sus productos
[24] Estadística obtenida por Microsoft, basada en las métricas de los usuarios de sus productos

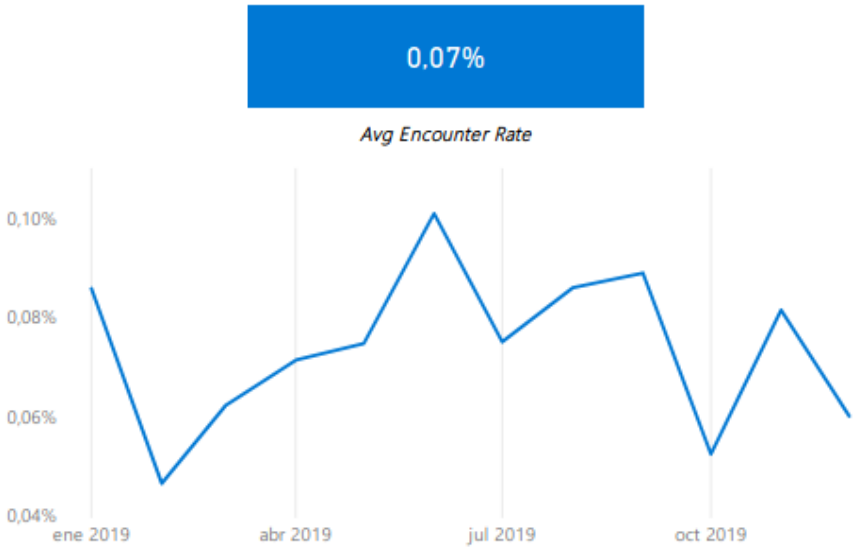


***Figura 40**. Detección de infecciones vinculadas a minería de criptomonedas en 2019 – Fuente: Microsoft*[25]

Ransomware

Al igual que en el resto del mundo, en Paraguay se observa una disminución de las detecciones de ransomware, teniendo actualmente un promedio de detección de 0.02%, ligeramente menor que la media mundial (0,03%). El año pasado, la detección promedio en Paraguay era de 0,05%. La mayor cantidad de infecciones por ransomware se detectaron en noviembre, con un aumento generalizado a partir de octubre. Esto coincide con la tendencia de aumento de los incidentes cibernéticos con fines financieros de fin de año (desde octubre a enero).

[25] Estadística obtenida por Microsoft, basada en las métricas de los usuarios de sus productos

Figura 41. *Evolución histórica de las detecciones de ransomware – Fuente: Microsoft*[26]

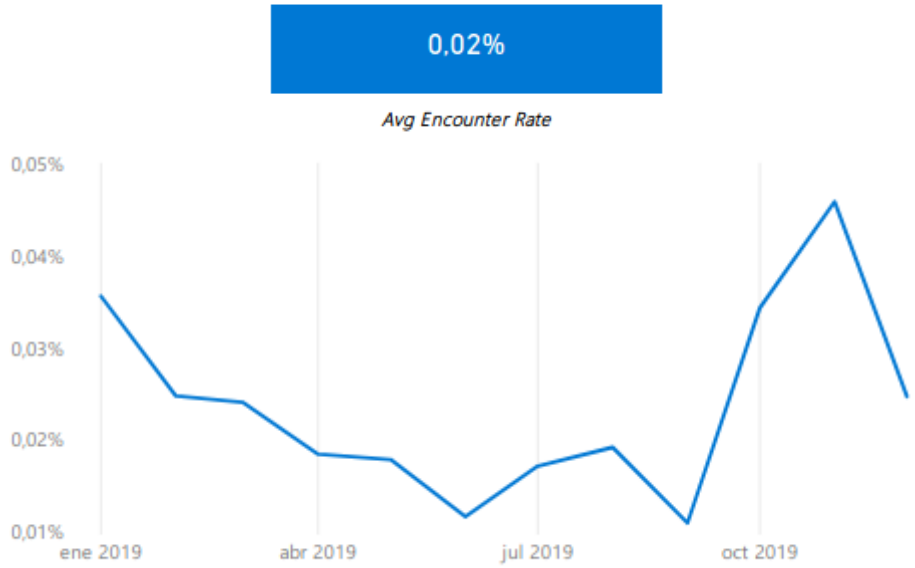


Figura 42. Evolución de detecciones de ransomware en 2019 – Fuente: Microsoft[27]

[26] Estadística obtenida por Microsoft, basada en las métricas de los usuarios de sus productos
[27] Estadística obtenida por Microsoft, basada en las métricas de los usuarios de sus productos

Correos maliciosos

Según datos de Kaspersky, el 17% de los correos electrónicos maliciosos analizados tiene como adjunto un archivo que descarga el malware Emotet. También se ve un aumento sustancial de los correos del tipo "Hoax": correos falsos que no contienen malware ni enlaces de phishing, sino que buscan engañar o extorsionar a la víctima, mediante alguna historia falsa. Un ejemplo es el correo en el que una persona se presenta como un "hacker" que invadió nuestra máquina y descubrió material de pornografía y que exige dinero para no divulgarlo[28]. Se trata de un engaño mediante una historia completamente falsa, que sin embargo tiene una alta efectividad, muchas víctimas lo creen y pagan.

También se observa un alto volumen de correos con archivos adjuntos que explotan la vulnerabilidad CVE-2017-11882, constituyendo éste el malware dropper más popular por parte de los criminales para la distribución de varias familias de malware.

1	Trojan.Script.Generic	21.7%
2	Trojan.Script.Emotet.gen	17.04%
3	Hoax.Script.Mailoy.gen	15.22%
4	DangerousObject.Multi.Generic	8.03%
5	Trojan.Win32.Agentb.gen	5.47%
6	Exploit.MSOffice.CVE-2017-11882.gen	5.14%
7	Backdoor.MSIL.Androm.gen	2.25%
8	Trojan.HTML.Fraud.gen	1.54%
9	Trojan.MSOffice.SAgent.gen	1.15%
10	Exploit.Win32.CVE-2017-11882.gen	1.1%

Figura 43. Top 10 de amenazas distribuidas por correo electrónico en Paraguay[29]

Ataques de red

De acuerdo a datos de Kaspersky[30], a nivel de ataques de red, la técnica más observada en Paraguay en el 2019 es el ataque de fuerza bruta de RDP (Remote Desktop Protocol) o Escritorio Remoto. Seguidamente, se observa la explotación de vulnerabilidades de SMB, tales como MS17-010, CVE-2017-0147, NetAPI-BOF. También se observa una alta frecuencia de los intentos de explotación de CVE-2018-1273 que afecta al framework Spring.

[28] Más información: https://www.cert.gov.py/index.php/noticias/mensajes-extorsivos-por-correo-su-cuenta-ha-sido-hackeda
[29] Estadística obtenida a partir del antivirus Kaspersky, por lo que el universo de la misma son únicamente los usuarios de sus productos
[30] Fuente: https://securelist.com/it-threat-evolution-q3-2019-statistics/95269/

1	Bruteforce.Generic.Rdp.a	12.45%
2	Bruteforce.Generic.Rdp.d	8.27%
3	Intrusion.Win.MS17-010.o	2.76%
4	Bruteforce.Generic.Rdp.b	0.65%
5	Bruteforce.Generic.Rdp.c	0.51%
6	Intrusion.Win.MS17-010.p	0.38%
7	Intrusion.Win.NETAPI.buffer-overflow.exploit	0.1%
8	Intrusion.Win.CVE-2017-0147.sa.leak	0.04%
9	Intrusion.Generic.CVE-2018-1273.exploit	0.02%
10	Intrusion.Win.SMBv3TreeConnect.test.exploit	0.01%

***Figura 44**. Top 10 de ataques de red detectadas en Paraguay – Fuente: Kaspersky*[31]

Denegación de servicio saliente y entrante de Paraguay

De acuerdo al mapa de Digital Attack Map, se registra un aumento generalizado de la frecuencia y el volumen de los ataques de DDoS a partir de mediados del 2019. El mayor pico en el que **se observó la participación de sistemas paraguayos** se registró entre el 09 y 10 de diciembre de 2018 **con un pico total de casi 100Gbps de tráfico**, combinando flujo de **ataques salientes y entrantes**, es decir, ataques de denegación de servicio que han tenido como víctima sistemas paraguayos, así como también IPs paraguayas que han participado de ataques de denegación de servicio contra sistemas extranjeros. Muchos de los ataques de DDoS superaron 60Mbps.

El ataque de DDoS más largo observado se dio desde el 21 de noviembre 2018 hasta el 12 de enero 2019 (52 días), siendo Paraguay el origen (máquinas comprometidas formando parte de una botnet) y teniendo a sistemas de Irlanda como víctimas.

[31] Estadística obtenida a partir del antivirus Kaspersky, por lo que el universo de la misma son únicamente los usuarios de sus productos

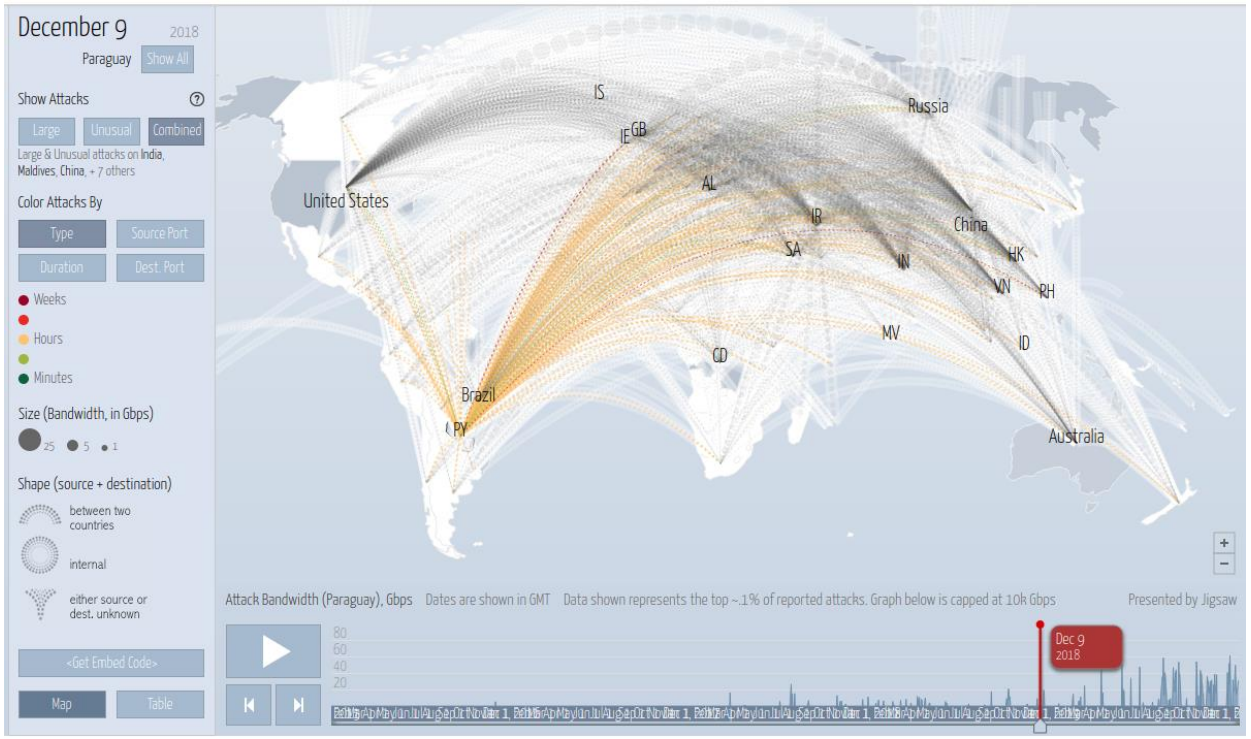
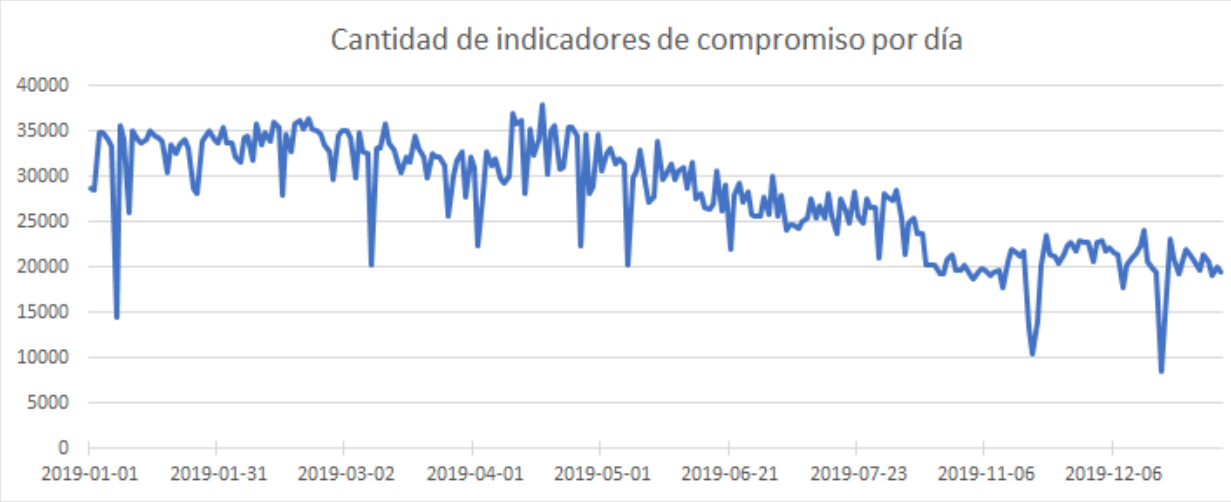


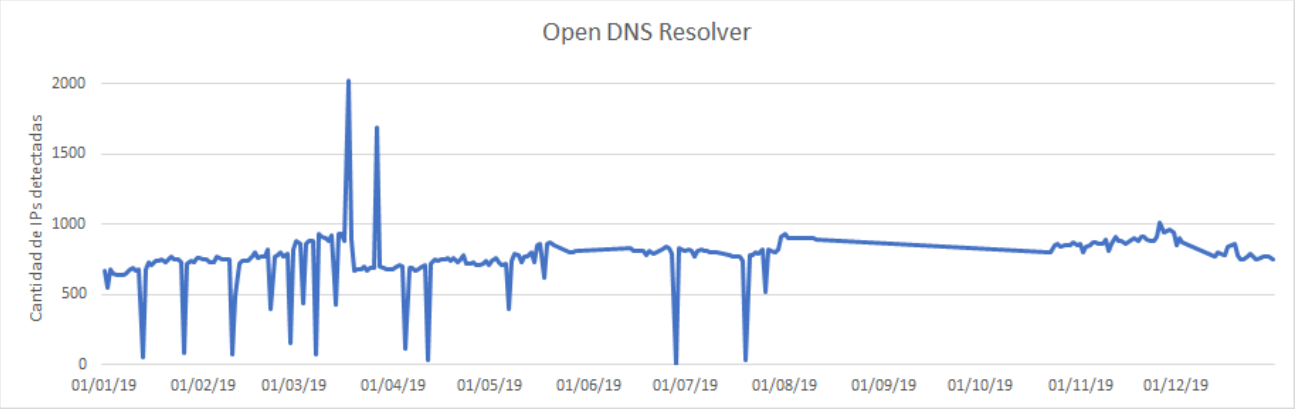
Figura 45. *Instantánea de tráfico de denegación de servicio saliente y entrante capturado por Digital Attack Map el 09/12/2018 de Paraguay*

Otras fuentes de datos específicas para Paraguay - Shadowserver

- Cantidad promedio de eventos de IoCs recibidos diariamente: ~ 27.831[32]

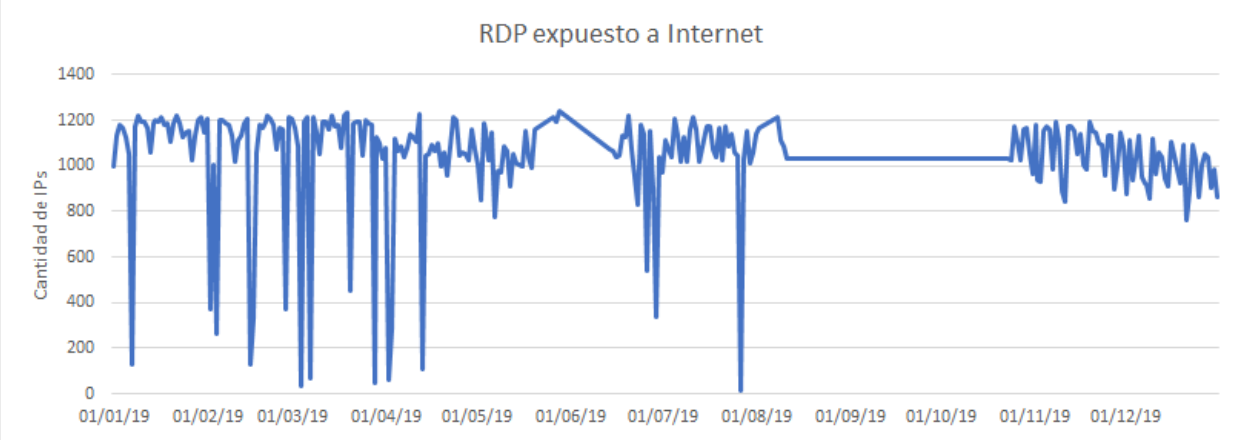


- En general, servicios vulnerables y/o expuestos reportados diariamente: ~ 22.938
- Servidores DNS Openresolver: cantidad promedio de IPs diarias ~ 763 (a través de ellos se pueden realizar enormes ataques de denegación de servicio)

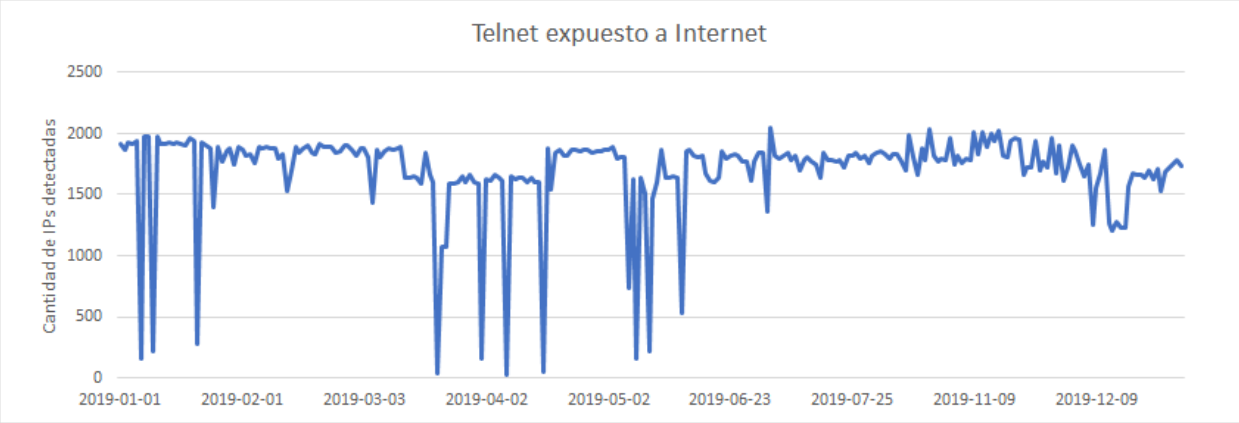


[32] Algunos días del año no se han recibido eventos debido a interrupciones temporales del servicio de notificación, por lo cual estos días no han sido tomado en cuenta para el cálculo de la distribución temporal. Entre mediados de agosto y octubre se produjo una interrupción de más de un mes debido a cambios en la infraestructura de recepción de notificaciones.

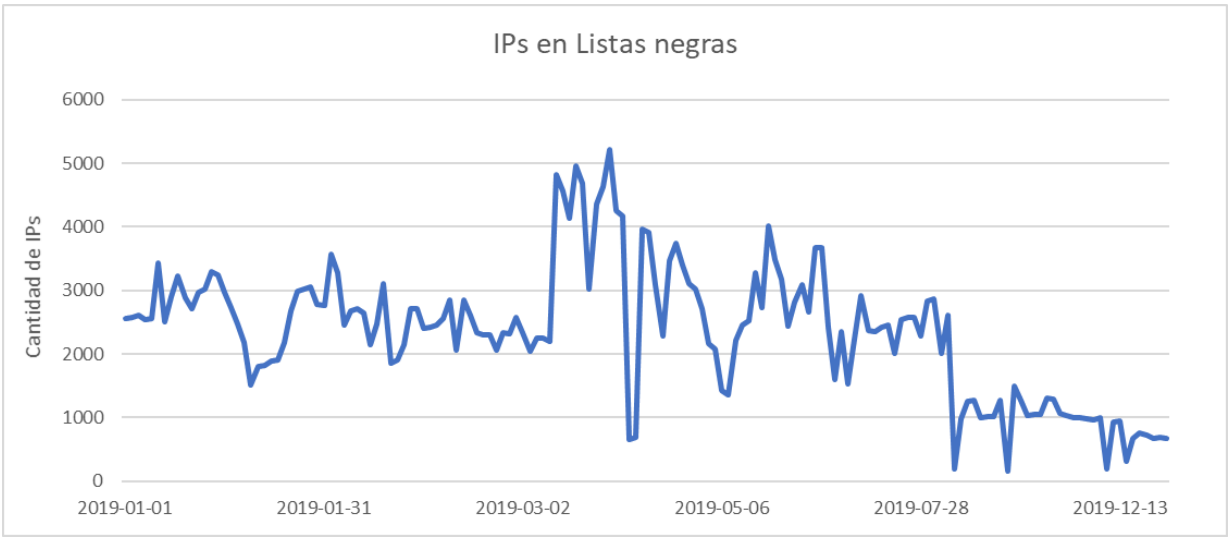
- Cantidad promedio de IPs detectadas diariamente con RDP expuesto a Internet: ~1.041



- Distribución IPs detectadas diariamente con Telnet expuesto a Internet: ~1.696
- Cantidad de IPs únicas con Telnet expuesto a Internet: 6.816



- 133 IPs únicas participaron de ataques de denegación de servicio distribuido de amplificación.
- 1846 IPs únicas realizaron ataques de fuerza bruta a otros sistemas.
- Promedio diario de IPs en lista negra (spam, infecciones, actividad maliciosa, etc): ~ 2.360
- Cantidad de IPs únicas que entraron en lista negra: 13.355



- Cantidad promedio de IPs infectadas con malware, pertenecientes a una botnet, visualizadas por día: ~ 479
- Cantidad de IPs únicas infectadas con malware, pertenecientes a una botnet: 43.263
- Más de 143 familias de malware únicas detectadas en IPs paraguayas. Las más detectadas son las siguientes:

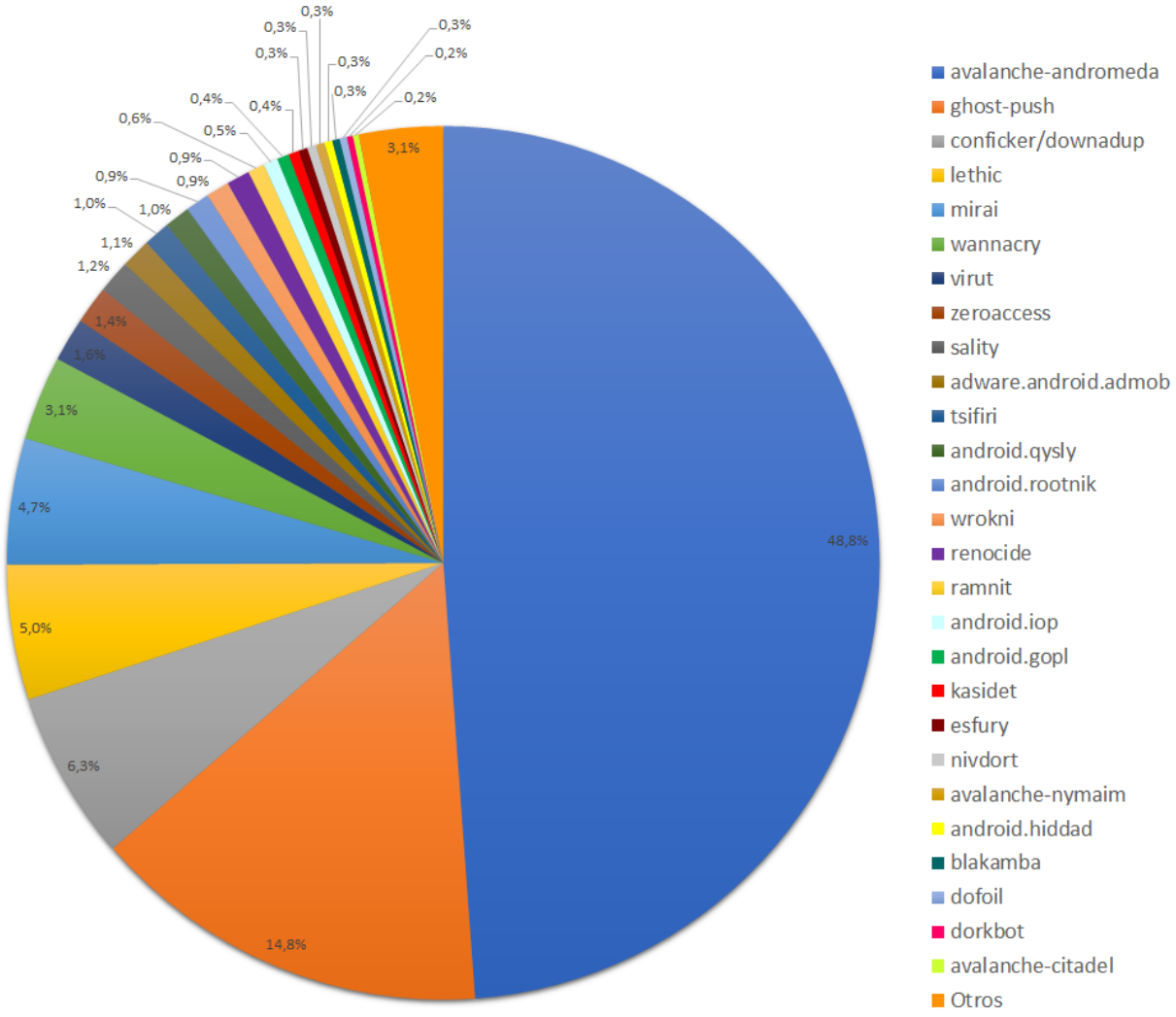


Figura 46. *Cantidad de infecciones únicas por familia de malware*[33]

Podemos ver que la mayor cantidad de detecciones de infecciones son de Andromeda, también conocido como Gamarue. Se trata de un malware que afecta computadoras con sistema operativo Windows, las computadoras infectadas pasan a ser parte de una botnet, los cuales son capaces de descargar datos, configuraciones de sitios remotos y ejecutar archivos arbitrarios. Se trata de una de las mayores botnets modulares basadas en HTTP, la cual llevaba varios años en activo e infectando computadoras para incrementar así el tamaño de la botnet. El objetivo principal de un bot de Andromeda era distribuir otras familias de malware para llevar a cabo un ataque masivo a nivel global. Sus funcionalidades incluyen:

[33] Estadísticas obtenidas a través de operaciones de sinkholing (ver nota #31) y/o compartición de datos de terceros de confianza

- Descargar y ejecución de software adicional.
- Robo de credenciales de acceso a algunos sitios web.
- Creación de proxy de salida en la máquina infectada.

Los métodos de infección pueden ser diversos, sin embargo, los más habituales son:

- Enlaces de confianza enviados a través de correos electrónicos de phishing o mediante redes sociales.
- Copiándose a sí mismo en dispositivos removibles o de red

Generalmente se distribuye a través de sitio web comprometidos (que fueron explotados para este propósito) y/o servidores de descarga legítimos como SourceForge.net.

Una operación internacional llevada a cabo en coordinación por Europol y otras fuerzas del orden ha desactivado esta botnet a fines del 2017, mediante operaciones de sinkholing[34]. Esto explica el alto ratio de detección, debido a que, como los servidores de Comando y Control (C&C) están bajo el control de organismos de seguridad, estos son capaces de detectar e informar todas las máquinas infectadas que siguen conectándose con los C&C.

La mayoría de las detecciones están relacionados con la botnet Avalanche, una botnet que servía para distribuir varias familias de malware, incluso bots de otras botnets (como por ejemplo, Andrómeda). Se trata de una red fast-flux, una técnica DNS usada por botnets para esconder sitios de phishing y descarga de malware detrás de una red siempre cambiante de hosts comprometidos actuando como proxies. Se trata de una infraestructura de red global del tipo “crime-as-a-service” utilizado por cibercriminales para realizar ataques de phishing, campañas de distribución de malware y esquemas de transferencias bancarias ilegales. Es utilizado por otras botnets como un servicio o plataforma de distribución de bots. Algunas familias de malware que utilizan la red Avalanche para su distribución son TeslaCrypt, Andrómeda, Nymaim, Rovnix, URLZone, Bugat (alias Feodo, Geodo, Cridex, Dridex, Emotet) y muchas otras. Esta botnet fue controlada a fines del 2016, a través de una de las mayores operaciones internacionales de sinkholing[35].

[34] Operaciones controladas, por lo general, a través de organismos de aplicación de la ley, en las que se logra redirigir el tráfico desde las máquinas infectadas a sistemas controlados por estos organismos, interceptando así el tráfico de comunicación entre la máquina infectada (bot) y el servidor C&C.

[35] https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation

Delitos Informáticos

Los delitos informáticos son todas las acciones dirigidas a lesionar la integridad, disposición y confiabilidad de datos y de sistemas informáticos, así como aquellas conductas que atentan contra el patrimonio de las personas utilizando herramientas tecnológicas e informáticas. Los delitos informáticos se encuentran tipificados de acuerdo a la Ley Nº 4439/11. Según las Resoluciones Nº 3459/10 y 4408/11, los tipos penales de competencia exclusiva de la Unidad Especializada en Delitos Informáticos son los siguientes: Acceso indebido a datos, interceptación, preparación al acceso indebido a datos, alteración de datos, acceso indebido a sistemas informáticos, sabotaje a sistemas informáticos, alteración de datos relevantes, falsificación de tarjetas de crédito y débito y estafa mediante sistemas informáticos.

Es importante tener en cuenta que el CERT-PY gestiona únicamente incidentes cibernéticos, no así los delitos informáticos[36]. Algunos delitos informáticos constituyen también incidentes cibernéticos y viceversa, pero no todo delito es un incidente, ni todo incidente es un delito. Por ejemplo: un acoso o estafa a través de medios informáticos (por ej. a través de redes sociales) no se considera un incidente cibernético, sin embargo, constituye un delito. Cuando el CERT-PY recibe un reporte que corresponde a un delito informático pero que no constituye un incidente cibernético, éste es derivado directamente al Ministerio Público, quienes llevan las estadísticas específicas de este y otros tipos de delitos.

Hecho Punible	Año 2013	Año 2014	Año 2015	Año 2016	Año 2017	Año 2018	Año 2019	Total
A determinar	86	193	212	208	157	103	82	**1041**
Acceso indebido a datos Art. 146b	5	0	2	1	0	6	0	**14**
Acceso indebido a sistemas informáticos Art. 174b	20	12	43	77	176	191	252	**771**
Alteración de datos Inc 1°	0	0	0	0	0	2	0	**2**
Alteración de datos Inc 3°	32	57	41	38	31	10	11	**220**
Alteración de datos relevantes para la prueba	1	16	22	12	0	0	0	**51**
Alteración de datos relevantes para la prueba Inc 2°	0	10	30	0	0	0	0	**40**
Estafa mediante sistemas informáticos	5	10	25	68	90	126	170	**494**
Estafa mediante sistemas informáticos INC 1°	0	1	0	0	0	7	8	**16**
Extorsion	0	0	0	0	1	0	0	**1**
Falsificación de tarjetas de débito o de crédito y otros medios electrónicos de pagos Art. 248b	5	0	0	1	4	63	118	**191**
Interceptación de datos Art. 146c	0	0	1	0	0	3	0	**4**
Lesion de confianza	0	0	0	1	0	0	0	**1**

[36] Debe tenerse en cuenta que las investigaciones realizadas por el CERT-PY y el Ministerio Público tienen una naturaleza y un alcance completamente distinto, pero complementarios. Mientras que el CERT-PY busca encontrar el origen del problema (la vulnerabilidad o problema de seguridad que fue explotado) para controlarlo, corregirlo, y evitarlo en un futuro, el Ministerio Público busca encontrar al culpable, de modo a poder imponer una sanción o pena.

Orden posterior y orden autonoma (Comiso autonomo)	0	0	0	0	0	0	1	**1**
Pornografia relativa a niños y adolescentes	1	70	311	311	119	298	849	**1959**
Pornografia relativa a niños y adolescentes Inc 1°	2	59	1	0	1	0	0	**63**
Pornografia relativa a niños y adolescentes Inc 4°	0	0	20	0	0	0	0	**0**
Producción de documentos no auténticos	0	1	1	0	0	0	0	**2**
Producción de moneda no auténtica	0	0	1	0	0	0	0	**0**
Producción inmediata de documentos públicos de contenido falso	0	0	1	0	0	0	0	**0**
Producción inmediata de documentos públicos de contenido falso Inc 1°	0	0	1	0	0	0	0	**0**
Revelación de secretos privados por funcionarios o personas con obligación especial	1	0	0	0	0	0	0	**1**
Sabotaje de sistemas informáticos Inc 1°	1	3	6	5	7	4	1	**27**
Sabotaje de sistemas informáticos Inc 2°	1	0	0		0	0	0	**1**
Violación del secreto de la comunicación Inc 1°	0	1	2	2	0	0	0	**5**
Violación del secreto de la comunicación Inc 2°	0	1	1	0	0	0	0	**2**
Total de delitos por año	**160**	**434**	**721**	**724**	**586**	**813**	**1492**	**4930**

Figura 47. *Delitos informáticos denunciados al Ministerio Público*

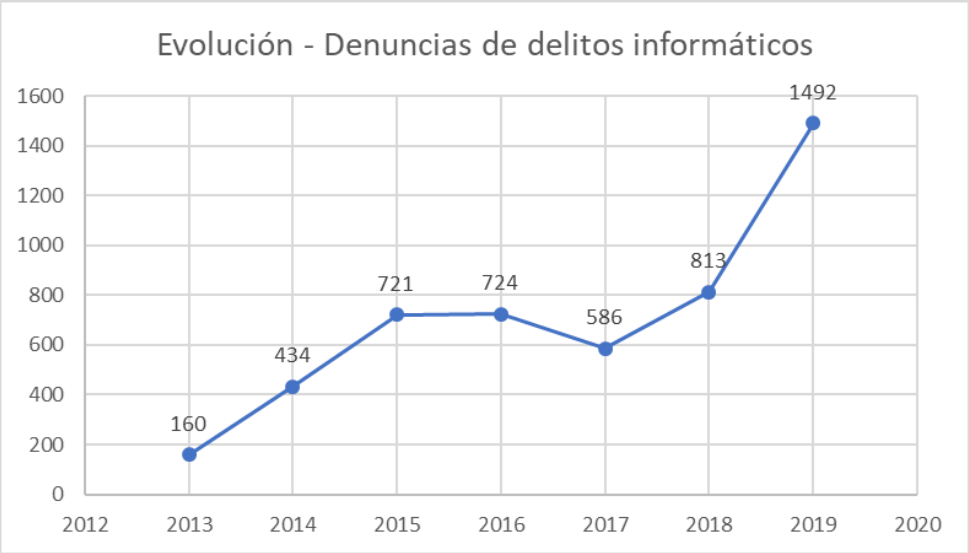


Figura 48. *Evolución de la cantidad de denuncias de delitos informáticos recibidos por el Ministerio Público por año*

Políticas, estándares y normativas en materia de Ciberseguridad

En materia de políticas de ciberseguridad, actualmente se encuentran aprobados y vigentes los **Controles Críticos de Ciberseguridad**, como un estándar para los organismos y entidades del Estado (OEE), mediante la Resolución N° 115.18 de la SENATICs. Se trata de un conjunto de acciones, priorizadas, ampliamente analizadas y de efectividad probada que pueden ser tomadas por las organizaciones para mejorar su nivel de ciberseguridad, basados en los CIS Controls, un estándar internacional reconocido. Se trata de una iniciativa para estandarizar, ordenar, priorizar y medir los esfuerzos en ciberseguridad que están llevando a cabo los organismos paraguayos, de modo a construir un ciberespacio seguro y resiliente.

La Resolución establece la obligatoriedad de implementar los primeros 6 controles (Controles Básicos) a partir del 13 de febrero de 2020, para todos aquellos OEE bajo el ámbito de la Resolución, siendo igualmente recomendable su adopción por las instituciones que están fuera del alcance del MITIC. Se elaboró una planilla de evaluación con una escala de evaluación ponderada, de modo a que las instituciones puedan realizar un autodiagnóstico permanente respecto a los avances en la implementación de dichos controles.

Además, en el 2019 se ha actualizado los **Criterios mí-nimos de seguridad para el desarrollo y adquisición del software**, mediante la Resolución N° 699/2019 del MITIC. Los principales cambios en dicha directiva son:

- se estableció la obligatoriedad de planificar, diseñar e implementar los sistemas de software nuevos acorde a los criterios, independientemente a que se trate de un desarrollo realizado internamente, tercerizado a través de contrataciones o adquisiciones o donado
- se estableció la obligatoriedad de realizar auditorías de vulnerabilidades a todo sistema de software nuevo antes de entrar en producción, acorde a los mencionados criterios
- se estableció la obligatoriedad de realizar también auditorías a todo sistema existente y que nunca haya sido auditado, en un plazo no mayor a 6 meses, de modo a gestionar las posibles vulnerabilidades que puedan existir
- se eliminó TLS 1.1 como un estándar de cifrado aceptable, estableciéndose como mínimo la utilización de TLS 1.2 o superior

Mediante la Resolución MITIC Nro. 432/2019 se aprobaron las "**Directivas de Ciberseguridad para Canales de Comunicación oficiales del Estado**", de uso obligatorio para todos los organismos y entes del Estado. El objetivo de estas directivas es proteger las cuentas oficiales de comunicación gubernamental, resguardando no solo el acceso a las mismas, sino también el contenido de las comunicaciones asociadas a éstas.

Se trata de directivas concretas y prácticas que deben ser aplicadas a todas las cuentas de canales de comunicación oficiales del Estado: cuentas de redes sociales (Facebook, Twitter u otros), cuentas de correo electrónico institucional u otros canales de comunicación digitales. Las directivas también aplican a las cuentas particulares de funcionarios que estén vinculadas a la administración de fanpage u otros canales oficiales gubernamentales.

En general, todo funcionario público o persona responsable de administrar una cuenta de comunicación oficial gubernamental debe aplicar estas directivas en dicha cuenta. Se ha reforzado la difusión, socialización y capacitación a los miembros del Equipo de Comunicadores del Estado (ECOE), quienes son los principales responsables de las cuentas de comunicación oficiales del Estado.

Además, en los últimos días de diciembre se ha aprobado el **Modelo de Gobernanza de Seguridad de la Información del Estado**, mediante la Resolución N° 733/2019. Se trata de una directiva mediante la cual todas las instituciones del Estado deben contar con un **área de Seguridad de la Información**.

El objetivo de esta área es velar por la seguridad de todos los activos de información de la institución en cuanto a su confidencialidad, integridad y disponibilidad.

Sus responsabilidades engloban los siguientes aspectos:

- Identificar y evaluar los **riesgos** y las brechas que afectan a los activos de información de la institución y proponer planes y controles para gestionarlos
- Elaborar y velar por la implementación de un **plan o estrategia de seguridad** de la información
- Elaborar, proponer y velar por el cumplimiento de las **políticas** de seguridad de la información de la institución
- Proponer los planes de **continuidad de negocio** y **recuperación de desastres** en el ámbito de las tecnologías de la información.
- Supervisar la administración del **control de acceso** a la información.
- Supervisar el **cumplimiento normativo** de la seguridad de la información.

Dicha área debe poder reportar a la Máxima Autoridad y debe ser independiente de las Direcciones de TIC o tecnología, entendiéndose que Seguridad de la Información y Ciberseguridad son áreas transversales, con roles y responsabilidades distintos a Tecnología. Además, las normas y estándares internacionales muchas veces recomiendan esa independencia, como una manera de evitar conflicto de intereses. La Resolución igualmente aclara que Seguridad de la Información no sustituye, de ninguna manera, a Seguridad Informática, Seguridad TICs o cualquier otra área operativa, las cuales normalmente tienen entre sus funciones la implementación de los controles tecnológicos. Todas estas áreas deben trabajar de manera coordinada con Seguridad de la Información, bajo la premisa que ciberseguridad es un eje transversal a toda la institución.

Con esta política de Estado, que marca un hito en el modelo de madurez de la ciberseguridad como país, se busca generar un modelo de gobernanza descentralizado, entendiendo que la ciberseguridad es un

tema de responsabilidades compartidas y compromiso de todas las partes. Si bien, el Ministerio de Tecnologías de la Información y Comunicaciones constituye la Autoridad central en materia de ciberseguridad, ésta es solamente para establecer los planes, políticas, proyectos e iniciativas tendientes a mejorar la ciberseguridad a nivel nacional y particularmente en el Estado - sin embargo, la adopción, implementación y apropiación de estas iniciativas debe ser asumida por cada una de las instituciones. Los Responsables de Seguridad de la Información serán la contraparte activa de este compromiso.

Formación de capacidades en Ciberseguridad

Desde la creación del CERT-PY en el año 2012, la formación de capacidades en ciberseguridad ha sido uno de los principales ejes de acción, para fomentar el uso seguro de las TICs y la gestión de seguridad de la información, tanto mediante cursos técnicos y de concienciación, así como también eventos más generales en forma presencial y en línea, como una estrategia de fomentar un ecosistema sostenible que pueda abordar los desafíos futuros en materia de ciberseguridad.

Desde el MITIC se ha organizado, co-organizado y/o acompañado varios eventos de formación de capacidades de ciberseguridad, entre ellos cursos, talleres, congresos, seminarios, etc. En el año 2019 se ha capacitado un total de 783 personas, entre ciudadanos, funcionarios públicos, y profesionales independientes y de empresas privadas.

En vista a la poca oferta formativa formal en materia de Ciberseguridad, también en el año 2019 se ha creado la **Especialización de Ciberdefensa y Ciberseguridad Estratégica**, en coordinación entre el Instituto de Altos Estudios Estratégicos (IAEE) y el MITIC. La primera edición ha contado con 42 egresados.

Además, algunas universidades públicas y privadas cuentan con especializaciones y maestrías con énfasis o enfoques de de seguridad de la información y/o auditoría informática.

En materia de concienciación, se ha identificado la necesidad de reforzar este aspecto en las instituciones gubernamentales, especialmente. Es por ello que en el 2019 el MITIC ha lanzado un nuevo **servicio de Ciberejercicios**, a través de simulacros de ciberataques, cuyo objetivo es conocer y mejorar el nivel de concienciación de los usuarios de una organización en materia de seguridad de la información, a través de metodologí-as prácticas. Una de estas metodologí-as es el simulacro de ciberataques, a través de pruebas y técnicas muy similares a las que utiliza un atacante real, pero en un ambiente controlado. El objetivo es exponer a los usuarios de la organización a una amenaza de ciberseguridad controlada, específicamente, un escenario de phishing. Luego se evalúa el actuar de los mismos, se elabora un informe y se realiza actividades de concienciación, que incluyen charlas, socialización de consejos de seguridad, etc. Para medir la efectividad de esta concienciación, se realiza una repetición del ciberejercicio, de modo a determinar si hubo un actuar más consciente por parte de los usuarios.

De acuerdo a los resultados de los ciberejercicios realizados, en promedio el 12% de los usuarios caen en el phishing y envían sus datos. El 18% ingresa en el enlace; si bien, no todos estos usuarios envían sus credenciales, esto igual supone un riesgo, ya que en un caso real, se podría tratar de un ataque de drive-by download, en cuyo caso con el solo hecho de abrir el enlace, la víctima podría quedar infectada.

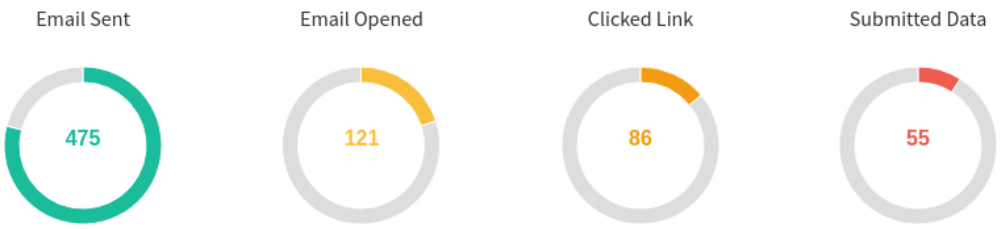


Figura 49. *Estadísticas resultantes de simulacro de phishing en instituciones públicas*

También se ha realizado ciberejercicios sectoriales y prácticos, con un primer ejercicio orientado al sector financiero.

Ranking Global y en las Américas en Ciberseguridad

De acuerdo al **National Cyber Security Index (NCSI)**, Paraguay se sitúa actualmente en la posición Nro. 41 a nivel internacional[37], y en 2do lugar en Latinoamérica, precedido únicamente por Chile[38]. El NCSI es un ranking internacional, elaborado por el e-Governance Academy (eGA), una organización sin fines de lucro conjunta entre el Gobierno de Estonia, Open Society Institute (OSI) y el Programa de Desarrollo de Naciones Unidas (PNUD). El objetivo de este índice es medir el nivel de preparación de un país para prevenir amenazas cibernéticas y gestionar incidentes cibernéticos, y representa un nivel de madurez en materia de ciberseguridad.

***Figura 50**. Posicionamiento de Paraguay en el ranking NCSI*

El índice abarca un total de 149 países, con un total de 46 indicadores, que son completados de manera continua por cada país mediante evidencia pública (enlaces a página web y/o leyes, decretos o resoluciones aprobadas), que es verificada de manera independiente por funcionarios del programa[39]. Paraguay ha sido incluido en el índice a finales del año 2018, en cuyo momento se había posicionado en el lugar 62 en el ranking global, con un 39% de cumplimiento. Actualmente, se alcanzó un cumplimiento del 56%.

Las principales debilidades, de acuerdo a este índice, se encuentra en los indicadores relativos a operaciones cibernéticos en el ámbito militar (17% de cumplimiento), así como también el manejo de crisis cibernética a nivel político estratégico (20%), protección de servicios digitales privados (20%), así como también la capacidad de gestión y análisis de información de amenazas (20% de cumplimiento).

[37] Fuente: https://ncsi.ega.ee/country/py/
[38] Fuente: https://ncsi.ega.ee/ncsi-index/
[39] Fuente: https://ncsi.ega.ee/methodology/

Las mayores fortalezas se dan en el aspecto de combate al cibercrimen desde el punto de vista del marco legal (100% de cumplimiento), políticas en materia de ciberseguridad (100% de cumplimiento), y servicios de identificación digital y confianza (89% de cumplimiento).

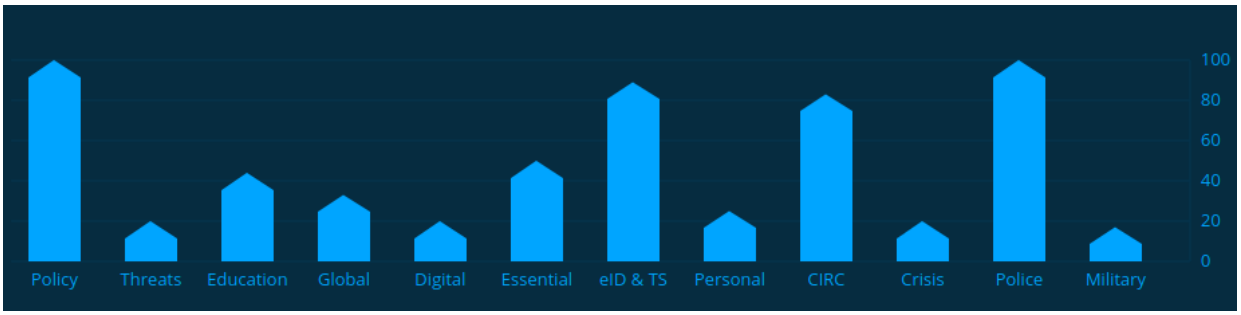


Figura 51. *Nivel de cumplmiento de indicadores de NCSI por área*

Para este estudio, la información correspondiente a Paraguay fue obtenida en primer lugar por parte de funcionarios de la organización en Estonia a partir de las fuentes públicas, y fue complementada con información proveída por el MITIC. A la fecha de la publicación del presente informe, es el único estudio internacional conocido basado en información actualizada de cada país, debido a su metodología de colección, revisión y publicación continua.

En otro estudio reconocido en el ámbito, el Global Cybersecurity Index (GCI)[40], elaborado por la Unión Internacional de Telecomunicaciones (ITU), en su última edición publicada en el 2018, Paraguay se posiciona a Paraguay en el puesto 66, de un total de 175 países, con un cumplimiento del 60,3 % de los indicadores de dicho estudio y 3ros en Latinoamérica, detrás de México y Uruguay. Este estudio ha sido publicado por última vez en el año 2018. En publicaciones anteriores, en el año 2017[41], Paraguay había ocupado el puesto 86 de un total de 193 países (32,6% de cumplimiento)[42]. En otra edición publicada en el año 2014[43], Paraguay obtuvo el puesto 22 de un total de 29 posibles posiciones (20,6 de cumplimiento)[44]. En el año 2019 no se ha publicado ninguna nueva edición del estudio.

Cabe destacar que esta primera versión del estudio contó con un índice de respuesta muy bajo, con pocos indicadores, y pocos mecanismos de validación de evidencia, por lo que los resultados podrían no ser representativos en comparación a las siguientes versiones. La información relativa a Paraguay incluida en

[40] Fuente: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
[41] El estudio fue realizado el año previo, 2016, con los resultados disponibles hasta ese año
[42] Fuente: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf
[43] El estudio fue realizado el año previo, 2013, con los resultados disponibles hasta ese año
[44] Fuente: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-S.pdf

esa edición del estudio no era correcta a la fecha de la realización del estudio. Si bien, participaron 196 países, la metodología y los indicadores utilizados generaron una gran cantidad de empates (todos se agruparon en 29 posiciones). A partir de la segunda edición del estudio (2017) se ajustó la metodología y los indicadores de modo a reflejar mejor la realidad.

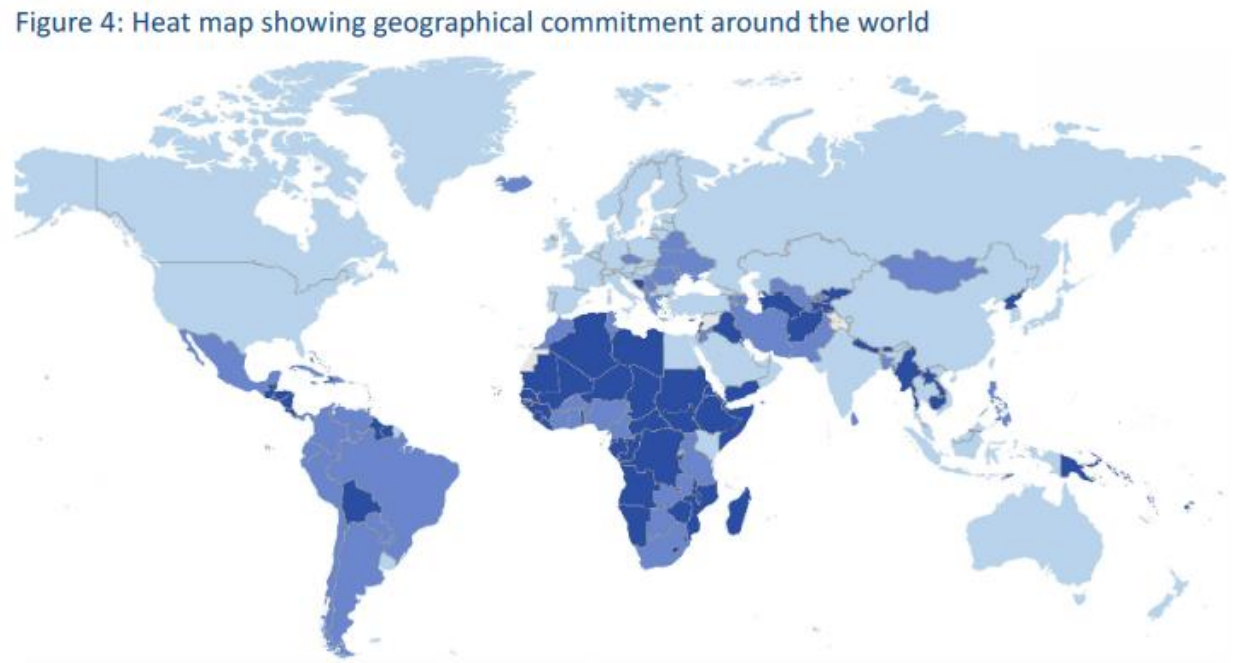


Figura 52. Comparación de países - GCI 2018[45]

[45] Nivel de compromiso: azul claro (más elevado) a azul oscuro (más bajo)

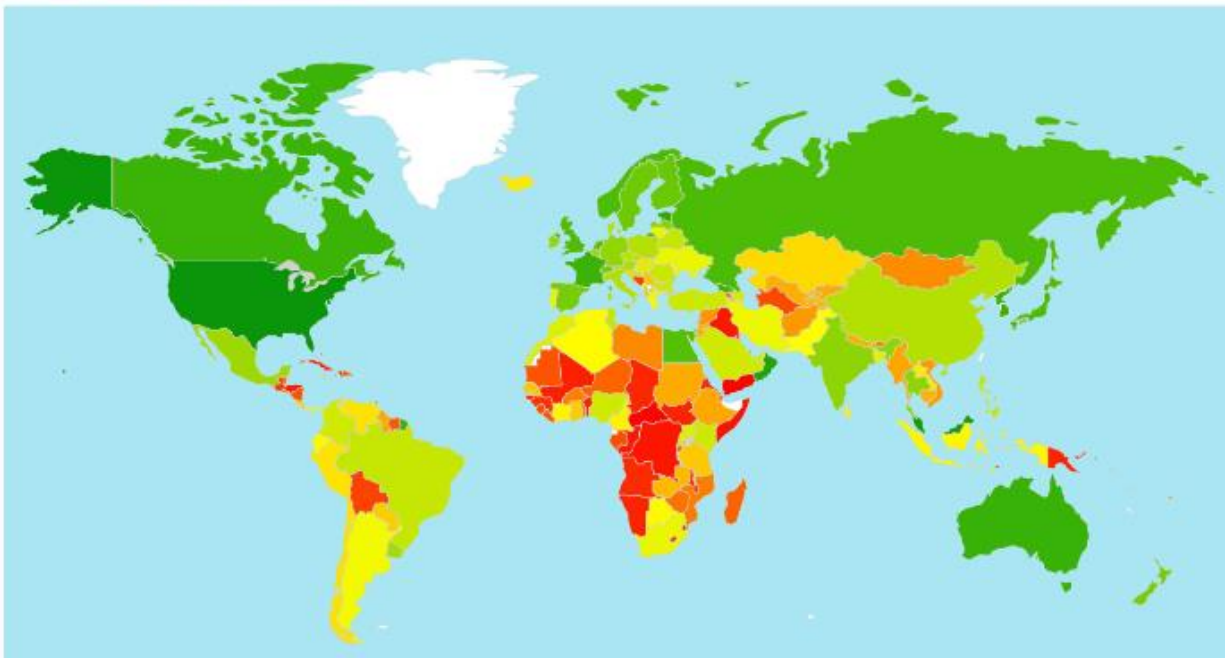
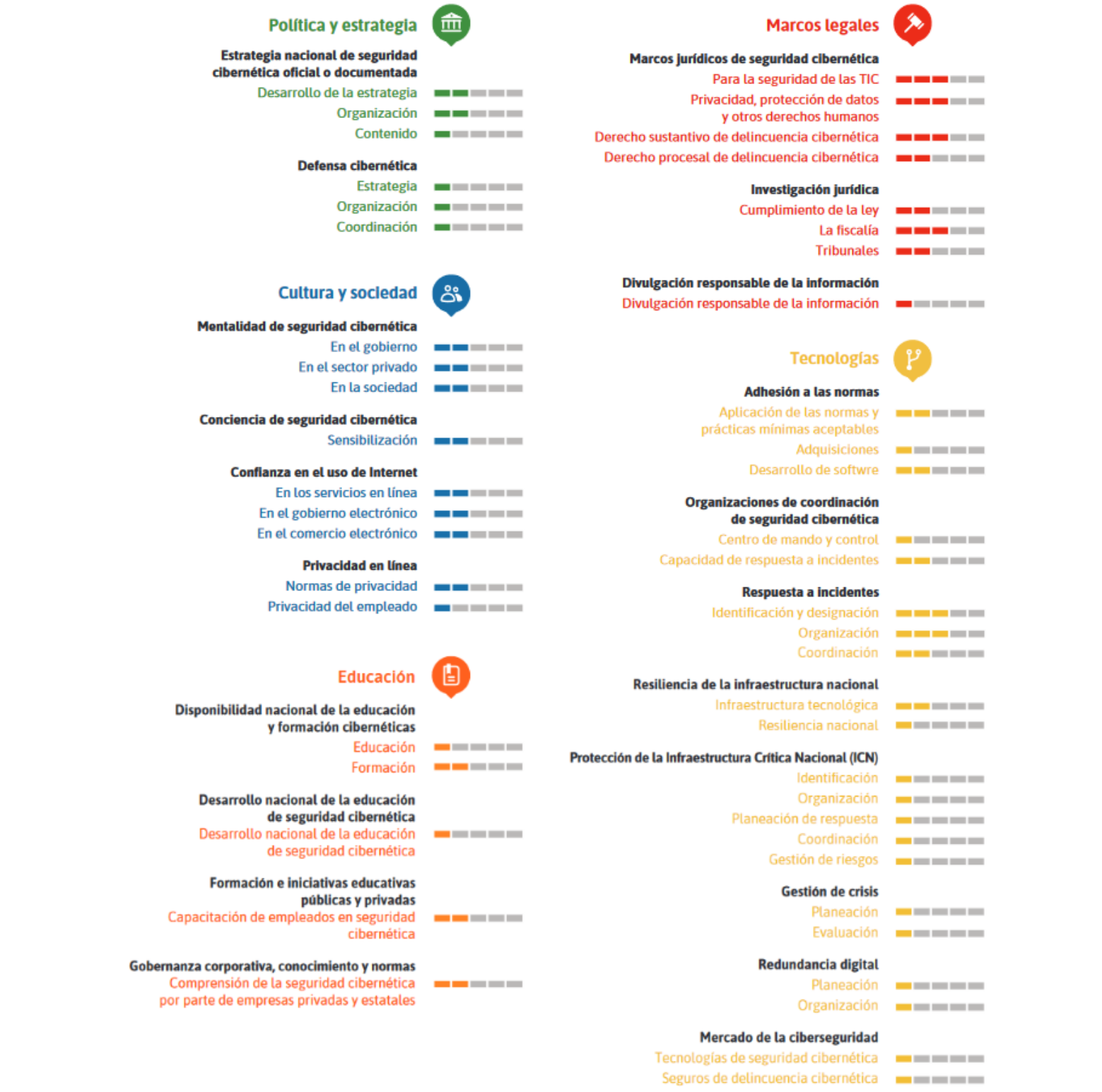


Figura 53. *Comparación de países - GCI 2017*[46]

La información para este estudio es proveída por parte de Conatel, organismo representante de Paraguay ante la ITU.

La Organización de Estados Americanos (OEA), el Banco Interamericano de Desarrollo (BID) y el Global Cyber Security Capacity Centre (GCSCC) de la Universidad de Oxford han elaborado un estudio denominado "Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?", publicado en el 2016. A diferencia de los estudios NCSI y GCI, no se trata de un índice o ranking, sino una medición cualitativa de 49 indicadores de madurez en materia de ciberseguridad, con una metodología mixta que incluye una encuesta de auto-evaluación a los Estados Miembros y una validación y complemento con información adicional a partir de fuentes abiertas, de tal manera a elaborar un perfil de cada país. Además, el estudio abarca únicamente los países miembros de la OEA de Latinoamérica y el Caribe. En dicho estudio, realizado con información disponible a mediados del 2015, el perfil de Paraguay respecto a la preparación en materia de ciberseguridad ha sido el siguiente:

[46] Nivel de compromiso: Verde (más elevado) a rojo (más bajo)


Política y estrategia
Estrategia nacional de seguridad cibernética oficial o documentada
Desarrollo de la estrategia
Organización
Contenido
Defensa cibernética
Estrategia
Organización
Coordinación
Cultura y sociedad
Mentalidad de seguridad cibernética
En el gobierno
En el sector privado
En la sociedad
Conciencia de seguridad cibernética
Sensibilización
Confianza en el uso de Internet
En los servicios en línea
En el gobierno electrónico
En el comercio electrónico
Privacidad en línea
Normas de privacidad
Privacidad del empleado
Educación
Disponibilidad nacional de la educación y formación cibernéticas
Educación
Formación
Desarrollo nacional de la educación de seguridad cibernética
Desarrollo nacional de la educación de seguridad cibernética
Formación e iniciativas educativas públicas y privadas
Capacitación de empleados en seguridad cibernética
Gobernanza corporativa, conocimiento y normas
Comprensión de la seguridad cibernética por parte de empresas privadas y estatales
Marcos legales
Marcos jurídicos de seguridad cibernética
Para la seguridad de las TIC
Privacidad, protección de datos y otros derechos humanos
Derecho sustantivo de delincuencia cibernética
Derecho procesal de delincuencia cibernética
Investigación jurídica
Cumplimiento de la ley
La fiscalía
Tribunales
Divulgación responsable de la información
Divulgación responsable de la información
Tecnologías
Adhesión a las normas
Aplicación de las normas y prácticas mínimas aceptables
Adquisiciones
Desarrollo de softwre
Organizaciones de coordinación de seguridad cibernética
Centro de mando y control
Capacidad de respuesta a incidentes
Respuesta a incidentes
Identificación y designación
Organización
Coordinación
Resiliencia de la infraestructura nacional
Infraestructura tecnológica
Resiliencia nacional
Protección de la Infraestructura Crítica Nacional (ICN)
Identificación
Organización
Planeación de respuesta
Coordinación
Gestión de riesgos
Gestión de crisis
Planeación
Evaluación
Redundancia digital
Planeación
Organización
Mercado de la ciberseguridad
Tecnologías de seguridad cibernética
Seguros de delincuencia cibernética

Se puede observar una mayor fortaleza en los indicadores relativos al marco legal, y una mayor debilidad en cuanto a Política y Estrategias, así como también en aspectos de Tecnología. Posterior a esta edición publicada en el 2016, no se ha publicado todavía ninguna nueva edición.