ESTADO DE LA CIBERSEGURIDAD en PARAGUAY

AÑO 2020

CENTRO DE RESPUESTAS ANTE INCIDENTES CIBERNÉTICOS

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 y tendencias en base a los reportes de incidentes cibernéticos recibidos por el CERT-PY durante el año 2020, así como también datos históricos y evolutivos en base a los incidentes gestionados desde los inicios de sus operaciones en el año 2013. 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. En el informe de este año se han incluido datos y estadísticas respecto al nivel de cumplimiento de algunas de estas normativas, las cuales fueron recabadas principalmente a través de encuestas oficiales y obligatorias a las Instituciones gubernamentales. Esto permite tener una idea más aproximada del nivel de madurez, gestión y protección del Estado, en materia de ciberseguridad, así como identificar falencias y aspectos a reforzar.

En el informe de este año se ha incorporado información acerca de la inversión realizada en Ciberseguridad por el Gobierno paraguayo, así como también sobre los recursos humanos que el Estado destina en Tecnología, y específicamente en Ciberseguridad. Esta información es obtenida a través del análisis de los datos abiertos públicos disponibilizados por la Dirección Nacional de Contrataciones Públicas y la Secretaría de la Función Pública, respectivamente.

Por último, se incluye 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.

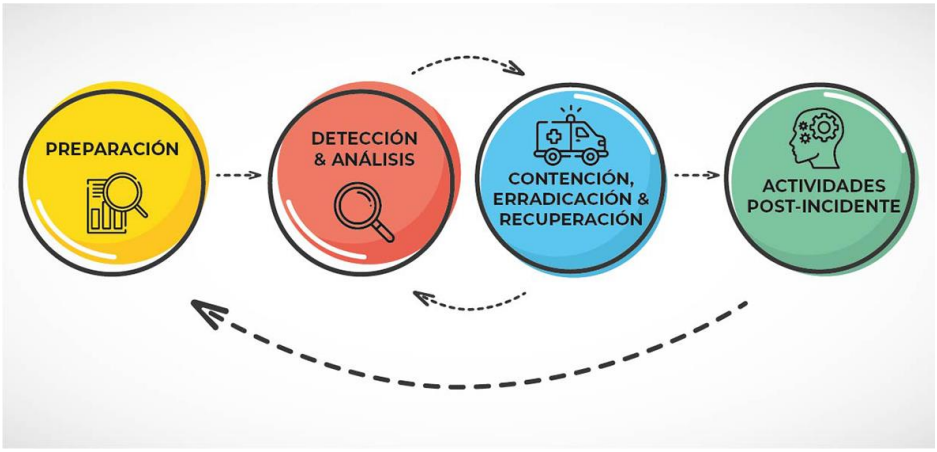


Figura 1. Fases del proceso de Gestión de Incidentes Cibernéticos

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.

Incidentes cibernéticos en el año 2020

A continuación, se presentan estadísticas obtenidas a partir de los incidentes cibernéticos reportados y gestionados a través del servicio del año 2020, desde el 01/01/2020, hasta el 31/12/2020. 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 que no hayan sido reportados no estarán reflejados en esta estadística.

- Reportes recibidos: 2101
- Cantidad total de Incidentes atendidos: 1358
- Investigaciones realizadas: 6598

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.

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 758 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.) y también sistemas comprometidos por malware mayormente siendo partes de Botnets como por ejemplo Emotet y Avalanche. Los **ataques de denegación de servicio y los accesos indebidos a cuentas/datos/sistemas** son los menos reportados e investigados, **con un total de 11 y 6 incidentes respectivamente**. 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. Además, es importante mencionar que los accesos indebidos a cuentas muchas veces son gestionados directamente con los proveedores de los servicios y/o redes sociales como ser Google, Facebook y/o Instagram y la mayoría no son notificados al CERT-PY

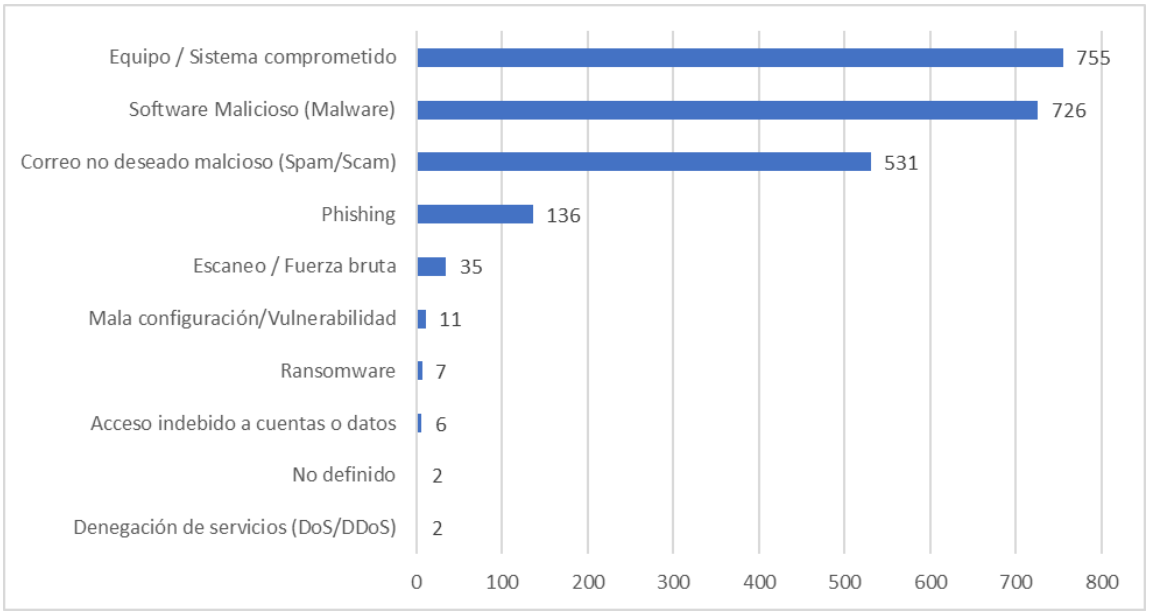


Figura 2. Cantidad de incidentes cibernéticos reportados en el año 2020, categorizados por tipo de incidentes

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.

- **Gobierno:** 123 incidentes
- **Privado:** 753 incidentes
- **Extranjero**: 469 incidentes
- **Ciudadano:** 20 incidentes
- **Educativo:** 2 incidentes

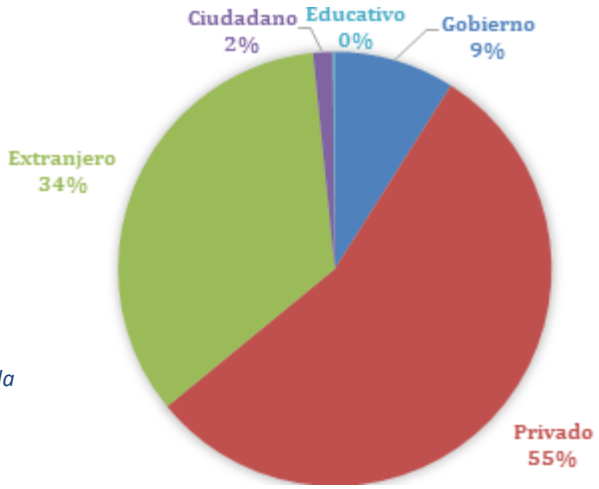


Figura 3. Clasificación de incidentes por organización afectada

Se observa un mayor número de incidentes cibernéticos que afectan a sistemas o redes de empresas privadas, con un total de 753 incidentes. Sin embargo, el número de incidentes relacionados a redes o sistemas de instituciones de gobierno o de ciudadanos particulares es inferior. Esto marca una tendencia diferente respecto a años anteriores, donde los incidentes reportados eran, mayoritariamente, de instituciones de Gobierno. Esto se debe, entre otras cosas, a que se ha logrado automatizar reportes que eran recibimos de otros CSIRTs/CERTs alrededor del mundo los cuales informan al CERT-PY sobre sistemas comprometidos dentro del territorio, la mayoría refieren a dominios de organizaciones privadas, los cuales anteriormente no eran procesados. Por otra parte, se observa todavía que muchos ciudadanos e incluso profesionales independientes no conocen este servicio y/o no lo utilizan, por lo cual se observa una menor cantidad de incidentes del sector ciudadano, lo cual se podría dar por diversas razones:

- Los hogares, los profesionales independientes e incluso las PYMES, 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.

La criticidad de los incidentes gestionados se asigna de acuerdo con los siguientes criterios:

- Criticidad alta:
    - Se encuentra afectado un activo de información gubernamental nacional y el impacto es alto (afecta la imagen institucional, problemas legales, afectan gravemente procesos institucionales, datos institucionales sensible).
    - Los ataques o amenazas activas que tienen alta probabilidad de afectar un alto número de víctimas nacionales en un futuro inmediato o cercano
    - Los ataques que causan la indisponibilidad de un servicio esencial o crítico y/o que afecta a un alto número de ciudadanos.
    - Los ataques que comprometen la confidencialidad de datos críticos, sensibles y/o privados de ciudadanos, empresas y/o instituciones nacionales
    - Los ataques que comprometen la integridad de datos o sistemas críticos y que afecta a un alto número de ciudadanos
- Criticidad media:
    - Se encuentra afectado un activo de información gubernamental nacional y el impacto no es alto.
    - Los ataques que causan la indisponibilidad de un servicio importante o que afecta a un alto número de ciudadanos.
    - Los ataques mediante los que se compromete la confidencialidad de datos de un número reducido de ciudadanos y/o empresas.
    - Los ataques que comprometen la integridad de datos o sistemas importantes pero que afecta a un número reducido de ciudadanos

- Criticidad baja:
    - Los ataques genéricos que utilizan técnicas y/o herramientas genéricas conocidas y con un objetivo que no está dirigido específicamente a víctimas nacionales
    - Los intentos de ataque mediante activos no críticos comprometidos y que no generó un impacto alto, ni desde el punto de vista de disponibilidad, confidencialidad e integridad

En el año 2020 se han reportado 3 incidentes de criticidad alta (0,22%), 75 incidentes de criticidad media y 1280 incidentes de criticidad baja.

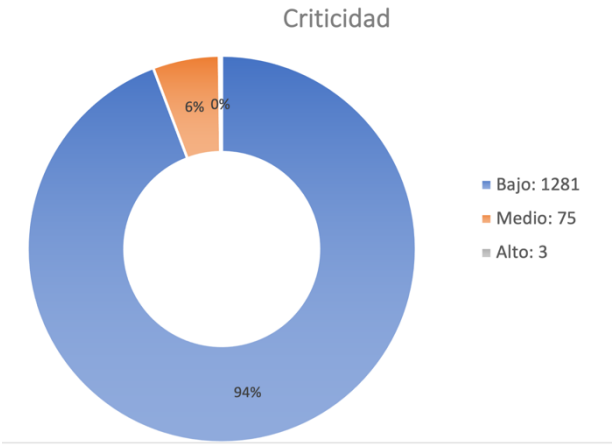


Figura 4. Clasificación de los incidentes por criticidad

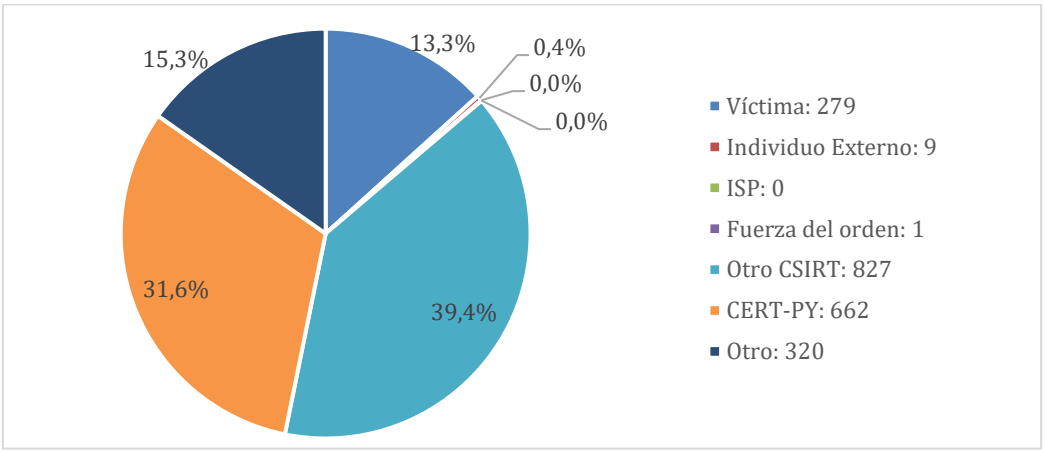


Figura 5. Reportes de incidentes por tipo de denunciante durante el año 2020

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.

Del total de 2.101 reportes de incidentes cibernéticos, 1784 de ellos se han resuelto. Esto representa una mejora significativa frente al 2019, en el que solamente el 11.2% de los incidentes pudo ser resuelto exitosamente.

Estado	Ticket count
rechazado	317
resuelto	1784
Total	2101

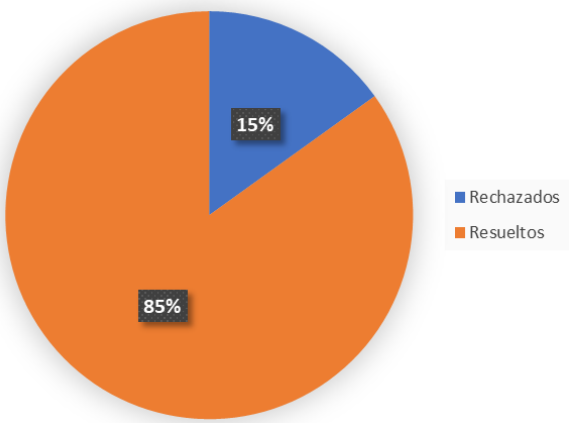


Figura 6. Porcentaje de resolución de Reportes en el año 2020

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

- Reportes que nos correspondían a un incidente cibernético
- Reportes falsos, provenientes de cuentas de spam publicitario
- Respuestas por parte de actores involucrados en una investigación que erróneamente se envían a la dirección de correo de recepción de incidentes
- Pedido de asistencia sobre delitos informáticos cuya investigación no correspondía al CERT-PY y que son derivados directamente a la Policía y/o Fiscalía.

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”. Del total de 1.358 incidentes únicos gestionados, 1.341 (99%) se han resuelto. Solamente el 1% ha sido abandonado. Esto representa una mejora significativa frente al 2019, en el que el 13% de los incidentes tuvo que ser abandonado sin resolución.

Estado	Ticket count
abandoned	17
resuelto	1341
Total	1358

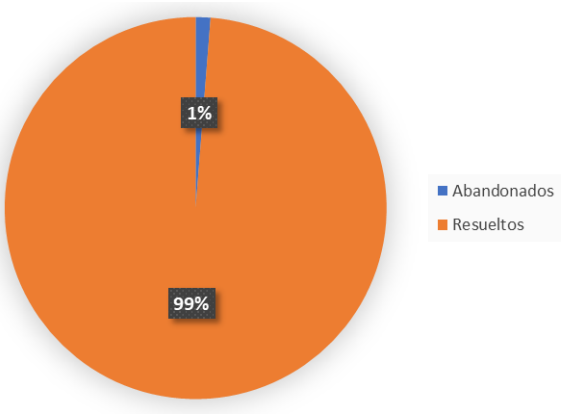


Figura 7. Porcentaje de resolución de Incidentes únicos en el año 2020

En el año 2020, la mayor cantidad de reportes se ha recibido en el mes de **julio** (217 reportes), con un pico de 217 reportes, seguido del mes de noviembre, con 189 reportes. En el mes de diciembre se ha recibido la menor cantidad de incidentes, con 147 reportes recibidos. Esto marca una tendencia diferente a años anteriores, donde los picos se registraban en los últimos meses del año. En julio hubo un aumento de incidentes de spam y phishing, alguno de ellos utilizando el COVID-19 y temas afines como anzuelo.

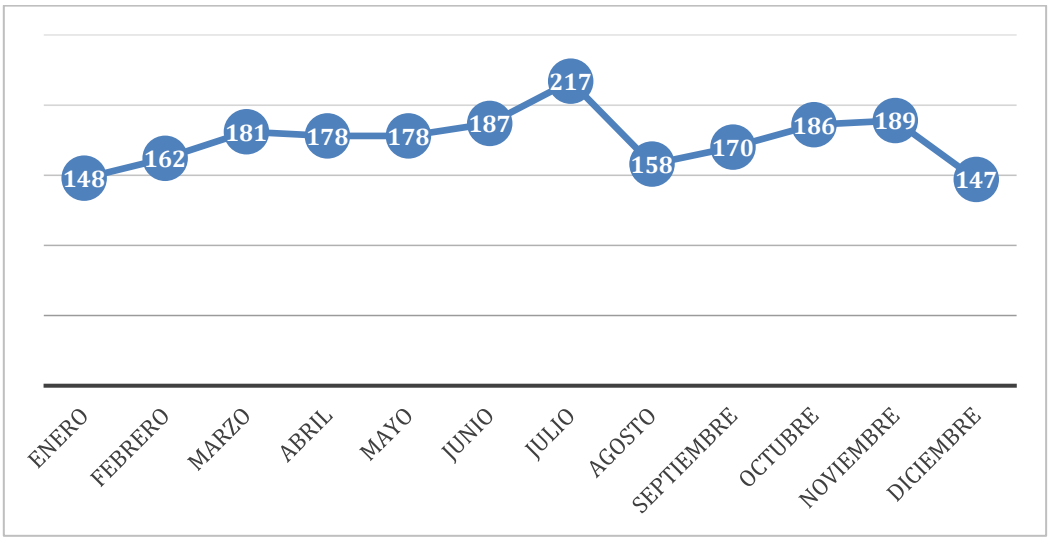


Figura 8. Cantidad de reportes de incidentes cibernéticos por mes del año

La mayor cantidad de reportes de incidentes cibernéticos se recibieron los días **martes y lunes**, en los que se ha recibido un total de 400 y 384 reportes respectivamente, con un decrecimiento gradual durante la semana, hasta un mínimo los sábados y domingo, con 174 y 184 reportes respectivamente. Esta tendencia es similar a la de otros años.

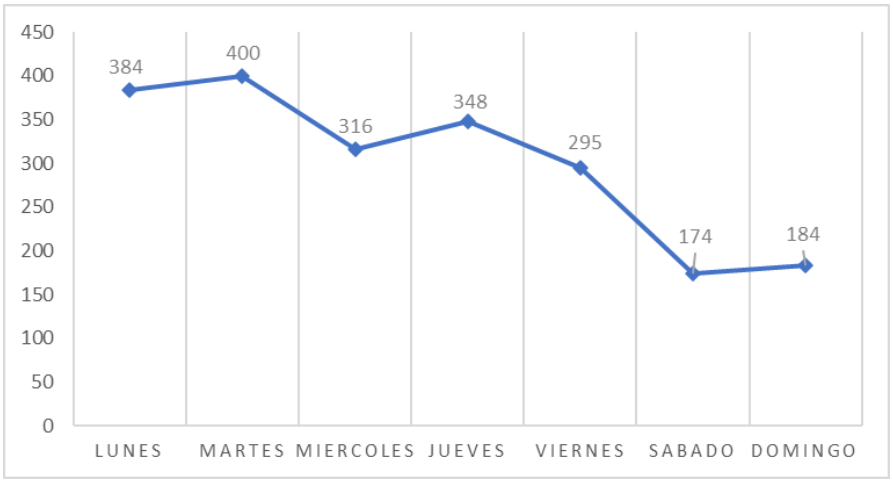


Figura 9. Cantidad de reportes de incidentes cibernéticos por día de la semana

En la siguiente figura se puede observar una mejora sustancial del tiempo promedio de atención de los reportes desde el mes de junio. Esto se debe a mejoras que se hicieron en el sistema de gestión de incidentes en la manera de registrar las métricas, así como también gracias a ajustes y mejoras en los procedimientos de atención de reportes y el crecimiento del equipo de analistas, siendo actualmente inferior a 24 horas.

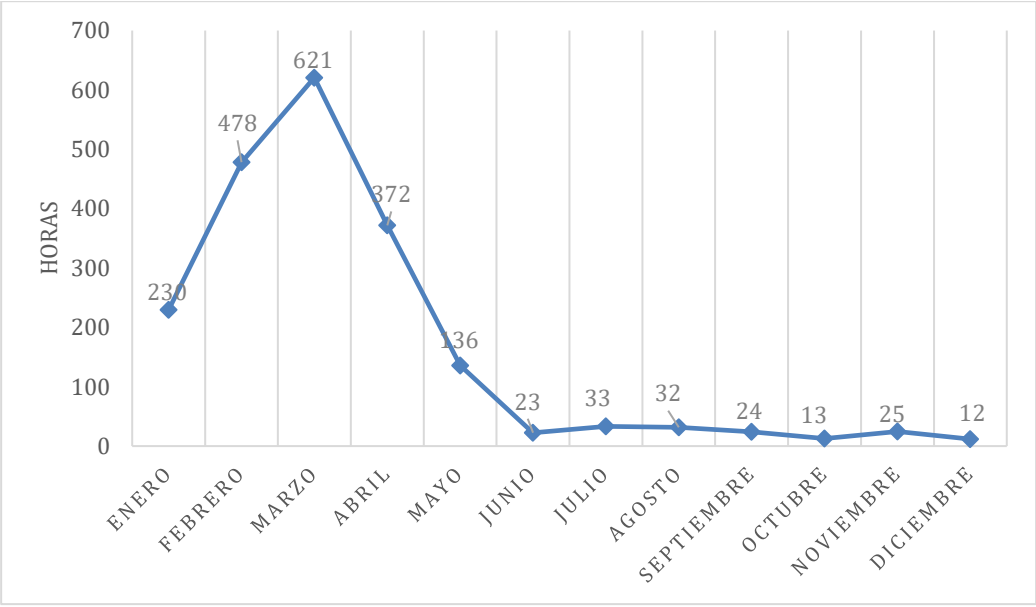


Figura 10. Evolución del tiempo promedio de atención de reportes en el año 2020 (mensual)

Incidentes resaltantes

A lo largo del año 2020 se ha observado un aumento sostenido de robos o "secuestros" de cuentas de Whatsapp, a través de múltiples mecanismos, principalmente, ingeniería social. Los criminales intentan registrar una cuenta de Whatsapp con el número telefónico de una víctima, a quien, a través de ingeniería social, convencen para que le proporcione el código de verificación que Whatsapp envía al número al momento del registro. Las excusas son variadas: desde hacerse pasar por un empleado de la telefónica o un conocido quien erróneamente envió el código son solo alguno de los ganchos utilizados por los criminales, quienes se comunican telefónicamente o por Whatsapp con la víctima para que ésta, sin ser consciente, le proporcione el código. Con dicho código, el criminal es capaz de registrar el número de la víctima, quien pierde acceso a su cuenta de Whatsapp.

Los objetivos, en estos casos, por lo general, son extorsivos: el criminal le solicita dinero a los contactos de la víctima haciéndose pasar por ésta, o en algunos casos, a la propia víctima, para devolverle la cuenta. En el último trimestre del año se observó que los criminales producían intencionalmente un bloqueo en el envío de códigos de verificación de Whatsapp, de tal manera a controlar la cuenta por más tiempo. Más información sobre estas técnicas se puede encontrar en el siguiente artículo:

- https://www.cert.gov.py/noticias/cuidado-con-el-robo-de-cuentas-de-whatsapp
- https://www.cert.gov.py/noticias/conoce-mas-sobre-los-metodos-empleados-por-ciberatacantes-para-el-secuestro-de-cuentas-de-whatsapp

Una técnica prácticamente idéntica se ha utilizado para el secuestro de cuentas de billeteras electrónicas. En todos los casos, los criminales se apoyaron en técnicas de ingeniería social mediante las cuales logran convencer a las víctimas de proporcionarles los códigos de verificación e incluso el código de verificación de 2 pasos, por lo general, haciéndose pasar por un funcionario de la telefónico o de otra empresa de confianza. En algunos casos, se han hecho pasar por funcionarios de instituciones públicas en el marco de algún programa de ayuda del Gobierno. Luego de controlar la billetera de la víctima, los criminales las utilizan para transferirse el dinero que se encuentra en ellas. El CERT-PY, así como la Policía y el Ministerio Público han emitido múltiples alertas al respecto: https://www.cert.gov.py/noticias/como-funcionan-las-estafas-usuarios-de-billeteras-electronicas-mediante-ingenieria-social

A mediados de julio se observó muchos casos de secuestro de cuentas de Whatsapp con una variante que no involucraba ingeniería social, sino el compromiso del buzón de voz ("voice mail hacking"). La técnica consiste en que el criminal registra el número de la víctima, pero solicita que el código de verificación se envíe a través de una llamada, en vez del SMS. Luego, basándose en debilidades del mecanismo de acceso y autenticación del buzón de voz de muchas compañías telefónicas que permiten el acceso remoto y con claves, por lo general, por defecto, el criminal ingresa al buzón de la víctima, escucha el código que previamente se envió, y con eso es capaz de concretar el registro del número de la víctima. Esta técnica, conocida como *voicemail hacking*, ya había sido observada y alertada a inicios del año, luego de algunos casos sonados en Brasil, en los que criminales utilizaron esta técnica para acceder

a cuentas de Telegram, correo electrónico y otras cuentas de autoridades y políticos brasileños. Sin embargo, a mediados de año empezó a verse esta técnica también en nuestro país, de manera masiva, para el secuestro de cuentas de Whatsapp. Cabe destacar que en esta técnica, no es necesaria ninguna acción por parte de la víctima, es suficiente con que ésta no atienda la llamada. Es por ello que la mayoría de los ataques ocurrieron a la madrugada. En este caso, el CERT-PY ha emitido alertas específicas, así como también se ha dado aviso a las compañías telefónicas. Alguna de ellas han robustecido el mecanismo de acceso y verificación al buzón de voz, a través de claves aleatorias. Algunas de las alertas pueden leerse aquí:

- https://www.cert.gov.py/noticias/secuestro-de-buzon-de-voz-tecnica-utilizada-por-los-atacantes-para-obtener-acceso-cuentas-de-usuarios
- https://www.mitic.gov.py/noticias/aumentan-casos-de-secuestro-de-whatsapp-traves-del-buzon-de-voz
- https://twitter.com/CERTpy/status/1229730695842541568

En el primer cuatrimestre se han comprobado algunos casos de acceso indebido a cuentas digitales (correo electrónico, redes sociales, Whatsapp y otros) a través de la técnica de SIM Swapping. Si bien, esta técnica no es nueva y ya había sido observada en años anteriores en nuestro país, en los casos ocurridos en el 2020 se ha observado la aplicación de esta técnica para el espionaje dirigido de personas vinculadas a la política y al periodismo de investigación. El SIM Swapping consiste en una técnica mediante la cual el criminal, a través de ingeniería social, logra convencer y/o engañar a un empleado de la telefónica para que cancele el chip de la víctima y lo reimprima posteriormente y se lo entregue al criminal. Con el chip y el número telefónico de la víctima en su poder, el criminal es capaz de autenticarse en todas las cuentas digitales que la víctima ha asociado a su número de teléfono, a través de los mecanismos de recuperación de contraseña, los cuales, por lo general, tienen la opción de mandar el código o enlace de acceso por SMS al número de la víctima, el cual, al estar en manos del criminal, logra el acceso a dichas cuentas. Se puede encontrar más información en las alertas emitidas:

- https://cert.gov.py/noticias/ataques-sim-swapping-que-son-como-protegerte
- https://www.cert.gov.py/application/files/3715/8827/1884/BOL-CERT-PY-2020-12_-_Incremento_en_casos_de_SIM_Swapping_para_robo_de_informacion_de_cuentas_vinculadas.pdf

Evolución Histórica y datos acumulados de incidentes cibernéticos

A continuación, se presentan estadísticas obtenidas a partir de todos los incidentes cibernéticos reportados y gestionados a través del servicio de gestión de incidentes cibernéticos del CERT-PY, desde su puesta en funcionamiento el 25/09/2013, hasta el 31/12/2020.

- Reportes recibidos: 7087
- Incidentes únicos gestionados: 1828
- Investigaciones, coordinaciones y gestiones únicas realizadas: 7368

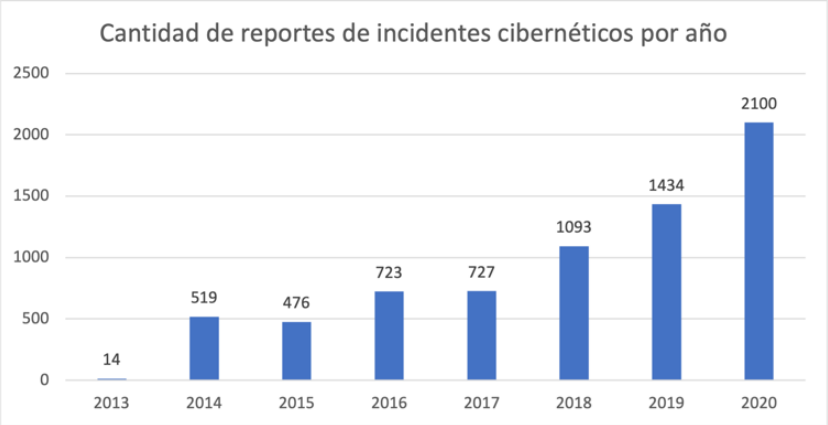


Figura 11. Evolución histórica de cantidad de Reportes de Incidentes cibernéticos recibidos

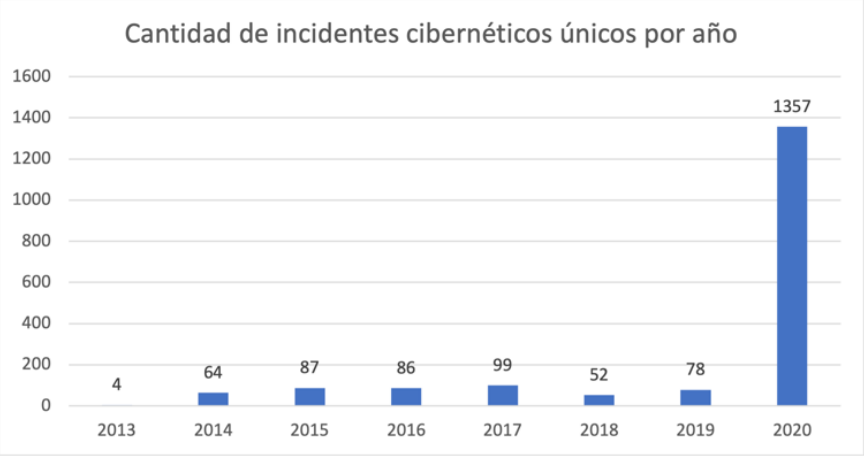


Figura 12. Evolución histórica de cantidad de Incidentes cibernéticos únicos atendidos

Figura 13. Evolución histórica de cantidad de investigaciones, coordinaciones y gestiones únicas realizadas

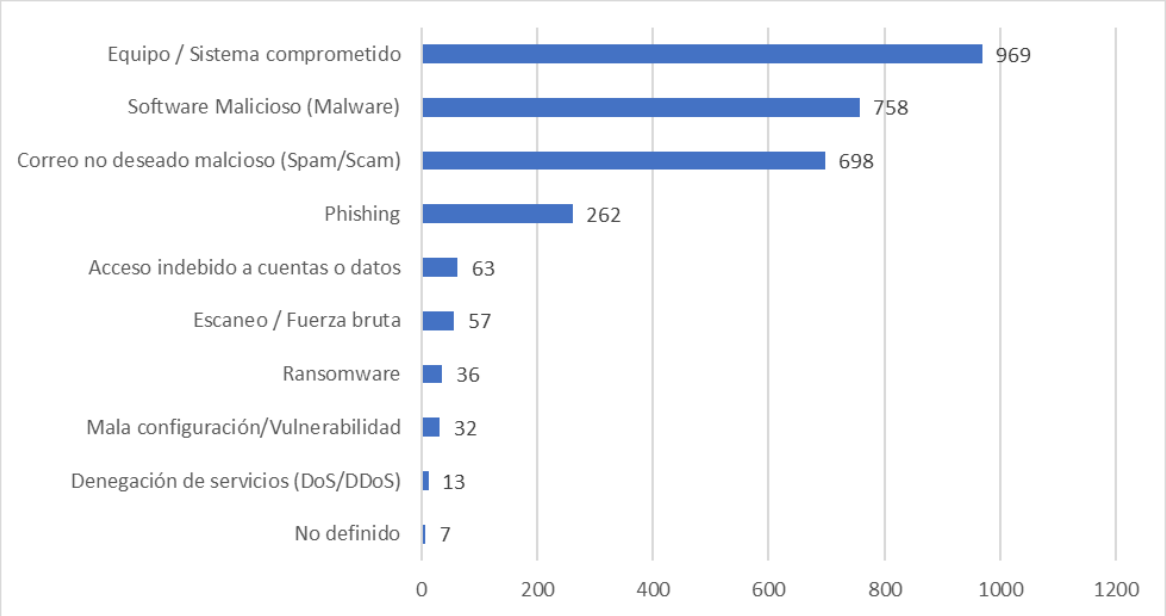


Figura 14. Cantidad histórica de incidentes cibernéticos reportados, categorizados por tipo de incidente. 2013 - 2020

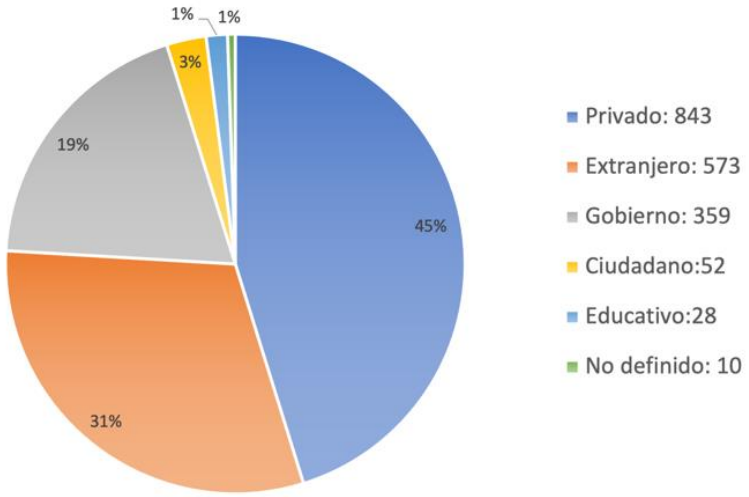


Figura 15. Distribución porcentual histórica de Sectores afectados por incidentes cibernéticos. 2013 - 2020

La mayor cantidad de incidentes afectan a redes o sistemas de empresas privadas, esto se remarca especialmente desde el 2020 luego de la implementación de sistemas automatizado de reportes (ver Sección "Incidentes cibernéticos en el año 2020"), volcando la tendencia anterior al 2020 en la que, históricamente, se gestionaba mayor cantidad de incidentes que afectaban al sector gubernamental.

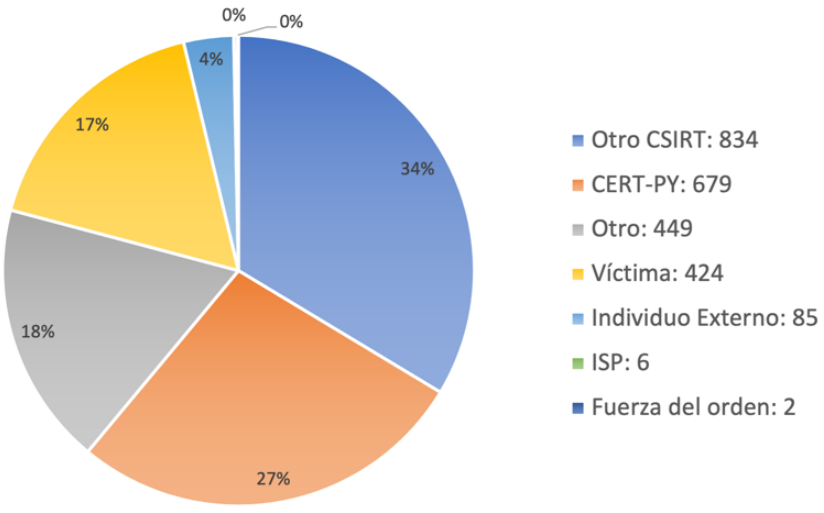


Figura 16. Distribución porcentual histórica Reportes de incidentes por tipo de denunciante. 2013 - 2020

Evolución histórica del tiempo de respuesta y atención

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

Esto se refleja en la mejora de 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. 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:

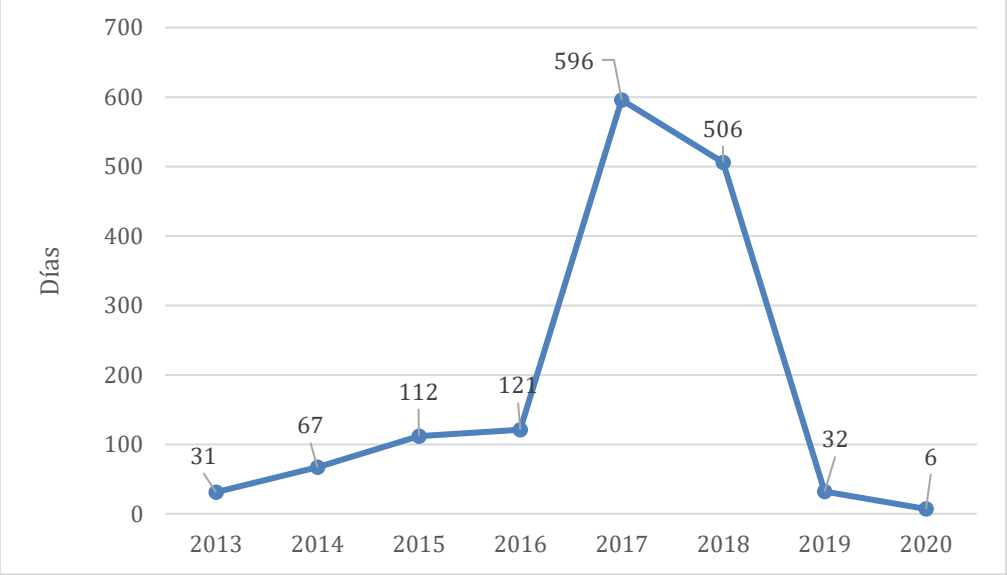


Figura 17. Evolución histórica del tiempo promedio de atención de reportes (anual)

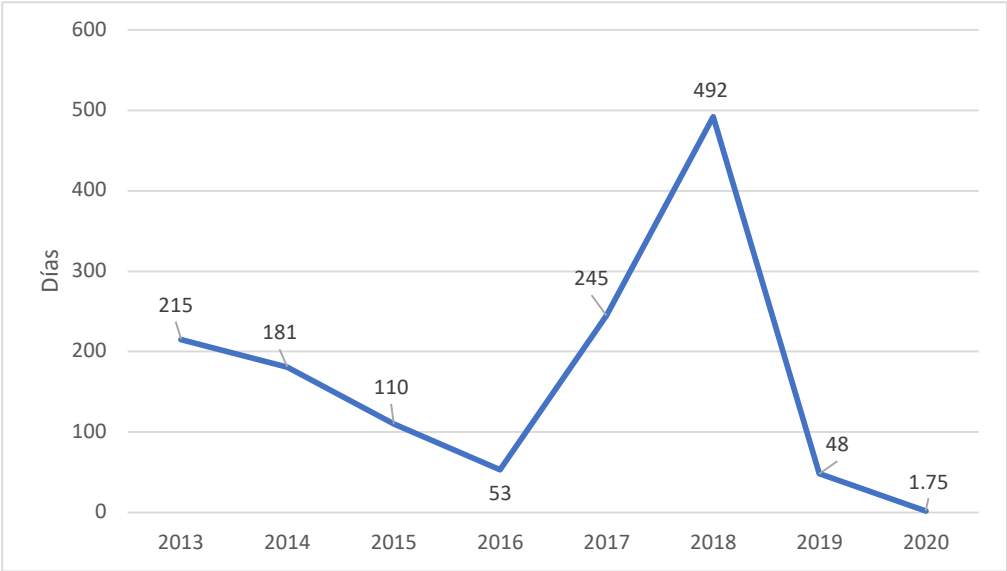


Figura 18. Evolución histórica del tiempo promedio de resolución de incidentes (anual)

Distribución temporal histórica de incidentes cibernéticos

Desde el inicio del servicio de gestión de incidentes, la mayor cantidad de reportes de incidentes cibernéticos se ha tenido en total fue durante el mes de **noviembre** clara diferencia con el 2020 que fue julio, con un pico de 924 reportes, seguido del mes de diciembre, con 639 reportes. En el mes de marzo se ha recibido la menor cantidad de incidentes, con 147 reportes recibidos.

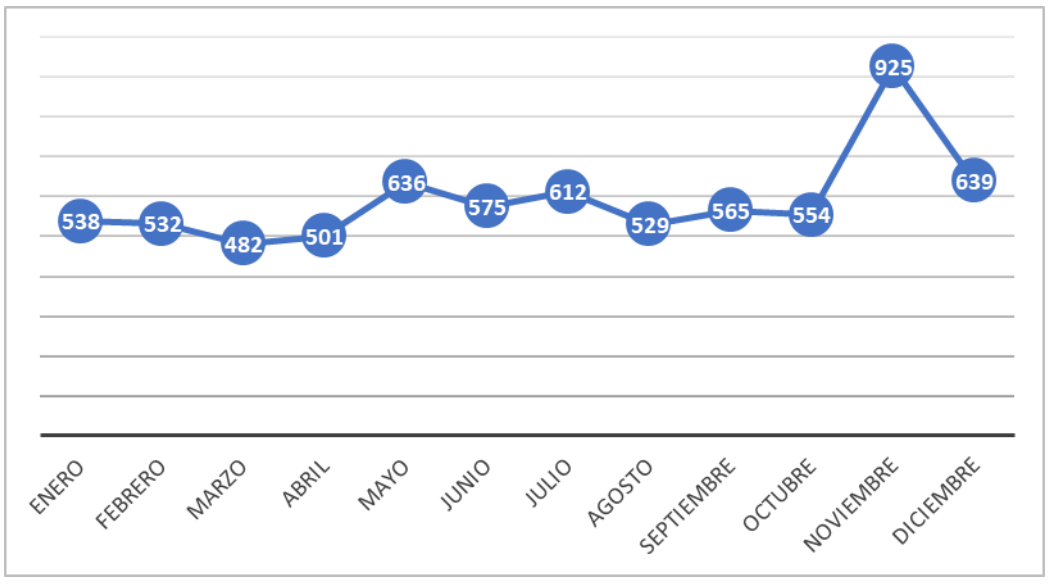


Figura 19. Cantidad histórica acumulada de reportes de incidentes cibernéticos por mes del año. 2013 - 2020

La mayor cantidad de reportes de incidentes cibernéticos se recibieron los lunes **y martes**, en los que se ha recibido un total de 1447 y 1239 reportes respectivamente, con un decrecimiento gradual durante la semana, hasta un mínimo los sábados y domingo, con 643 y 621 reportes respectivamente.

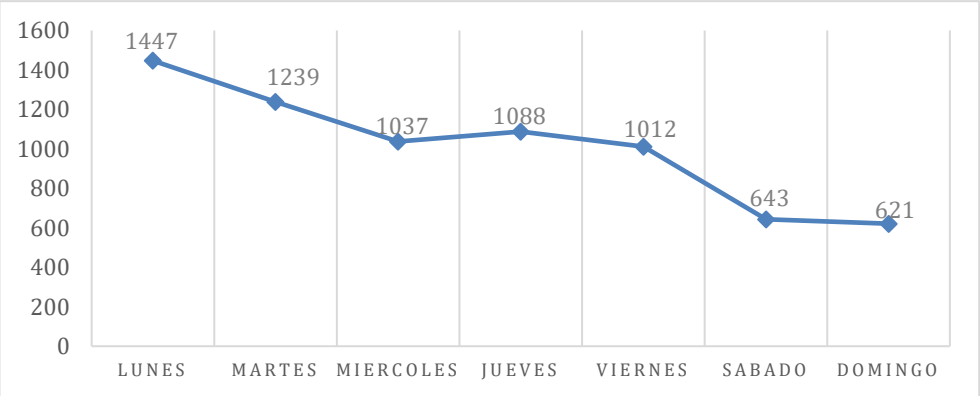


Figura 20. Cantidad histórica acumulada de reportes de incidentes cibernéticos por día de la semana. 2013 - 2020

Estadísticas obtenidas de fuentes externas abiertas

Vulnerabilidades

De acuerdo a los datos de Shodan, las vulnerabilidades más presentes en servicios expuestos a Internet en el rango de IPs paraguayas son las siguientes:

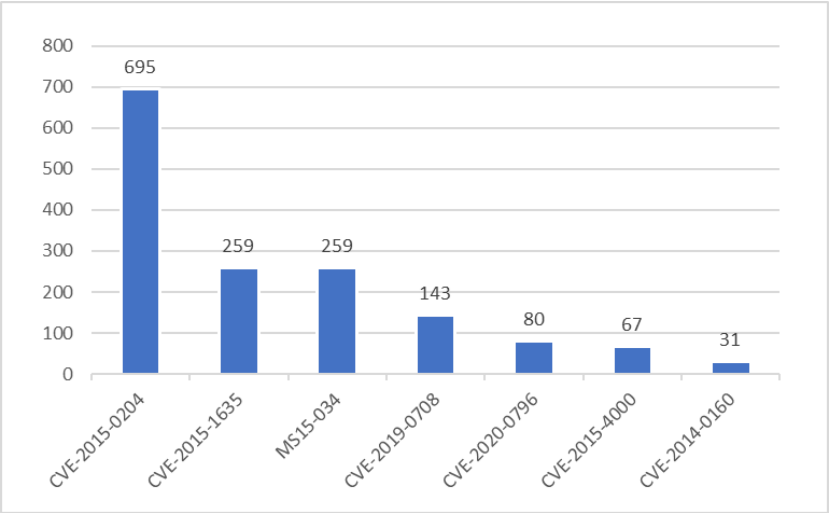


Figura 21. Vulnerabilidades más frecuentes en servicios expuestos en Internet de Paraguay

Se puede observar que la vulnerabilidad más frecuente es FREAK (CVE-2015-0204), una debilidad criptográfica en los protocolos SSL / TLS. En segundo lugar, se observan vulnerabilidades de ejecución remota de código en el servicio HTTP.sys . También se puede observar que al menos 143 servicios de Escritorio Remoto (Remot Desktop Protocol (RDP)) expuestos a Internet y vulnerables a CVE-2019-0708, una vulnerabilidad de ejecución remota de código. Al menos 80 IPs tienen expuesto el servicio SMB, utilizado para compartición de recursos de la red, vulnerable a CVE-2020-0796, una vulnerabilidad de ejecución remota de código. Debe tenerse en cuenta que, el solo hecho de exponer a Internet el servicio de SMB constituye una mala práctica con altísimos riesgos.

De acuerdo con 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.

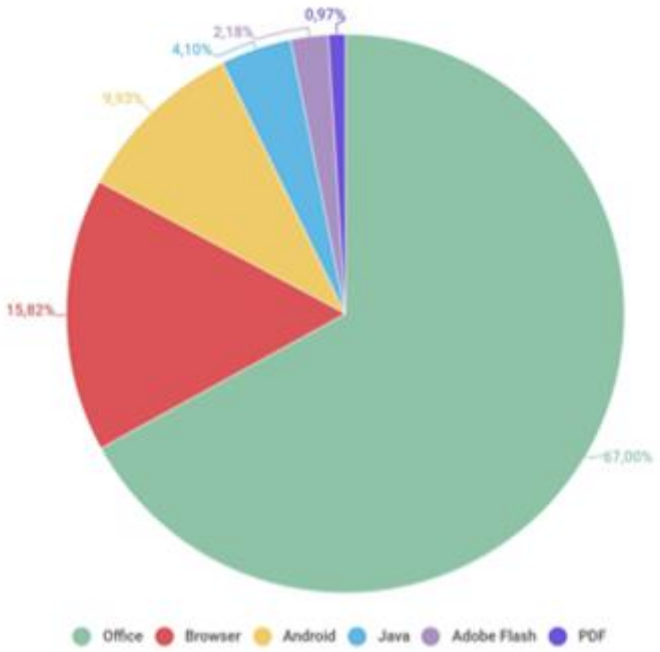


Figura 22. Vulnerabilidades más explotadas mundialmente en 2020

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.

Entre las vulnerabilidades más frecuentemente explotadas en Paraguay se encuentran aquellas relacionadas al bypass del Control de Cuenta de Usuarios de Windows (User Account Control (UAC)). A diferencia del año pasado, se empiezan a encontrar más intentos de explotación de vulnerabilidades en sistemas Linux. La vulnerabilidad CVE-2017-11882 que afecta a Microsoft Office y que ya fue descubierta en el 2017 sigue estando muy presente.

1	Exploit.Script.Generic	42.86%
2	Exploit.Win32.UACSkip.vho	8.33%
3	Exploit.Linux.Enoket.a	7.14%
4	Exploit.MSOffice.CVE-2017-11882.gen	5.95%
5	Exploit.Linux.Lotoor.g	4.76%
6	Exploit.AndroidOS.Lotoor.bg	3.57%
7	Exploit.Win64.CVE-2015-1701.a	3.57%
8	Exploit.Win32.CVE-2015-2387.foou	3.57%
9	Exploit.IphoneOS.Vortex.a	3.57%
10	Exploit.MSWord.CVE-2014-1761.a	2.38%

Figura 23. Top 10 de vulnerabilidades más explotadas en sistemas de Paraguay – Fuente: Kaspersky[1]

Amenazas financieras - Ghimob

De acuerdo con datos de Kaspersky[2], Ghimob es un troyano bancario parte de la familia Tétrade, se ha tiene como objetivos dispositivos móviles aplicando aplicaciones financieras de bancos, fintechs, cambios de monedas y criptomonedas en países como: Brasil, Paraguay, Perú, Portugal, Alemania, Angola y Mozambique.

Ghimob, una vez que se completa la infección crea una puerta trasera y el cibercriminal puede acceder al dispositivo infectado de forma remota, completando la transacción fraudulenta con el teléfono de la víctima, para evitar las medidas de seguridad implementadas por las instituciones financieras y todos sus sistemas de antifraude. Incluso si el usuario tiene un patrón de bloqueo de pantalla, Ghimob puede grabarlo y luego reproducirlo para desbloquear el dispositivo. Cuando el ciberdelincuente está listo para realizar la transacción, puede insertar una pantalla negra como superposición o abrir algún sitio web en pantalla completa, de modo que mientras el usuario mira esa pantalla, el delincuente realiza la transacción en segundo plano utilizando la aplicación financiera que se ejecuta, en el teléfono de la víctima que el usuario ha abierto o en el que ha iniciado sesión.

Desde un punto de vista técnico, Ghimob también es interesante porque utiliza C&C (Command and Control) con respaldo protegido por Cloudflare, oculta su C&C real con DGA y emplea varios otros trucos, haciéndose pasar por un fuerte competidor en este campo. Pero aún, no hay señales de MaaS (malware-as-a-service). En comparación con BRATA o Basbanke, otra familia de troyanos bancarios móviles

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

[2] Fuente: https://securelist.com/ghimob-tetrade-threat-mobile-devices/99228/

originarios de Brasil, Ghimob es mucho más avanzado con mejores funciones y tiene una gran persistencia.
Durante los meses de Julio, Agosto y Septiembre en Paraguay, se vio que 1.3% de los usuarios de Kaspersky tuvieron detecciones de malware bancarios[3] .

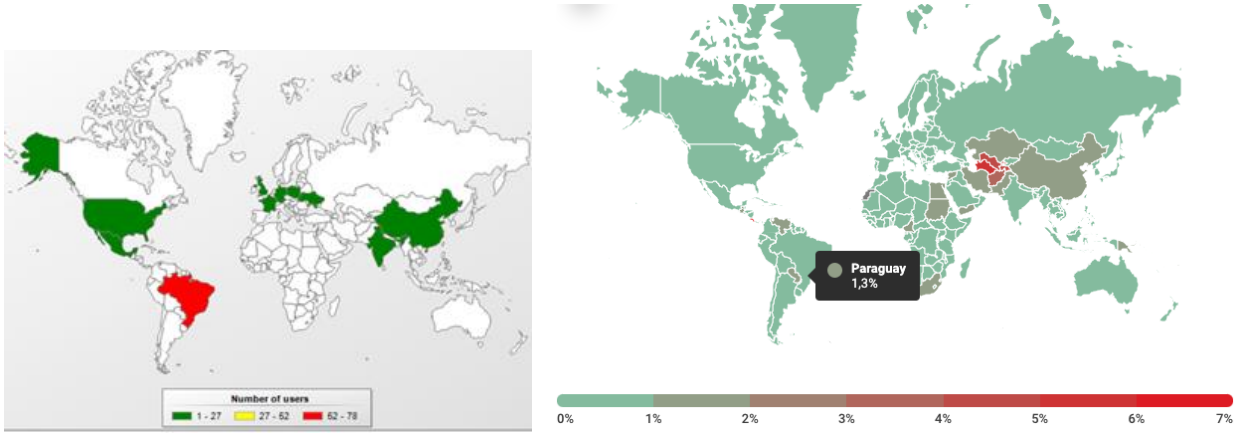


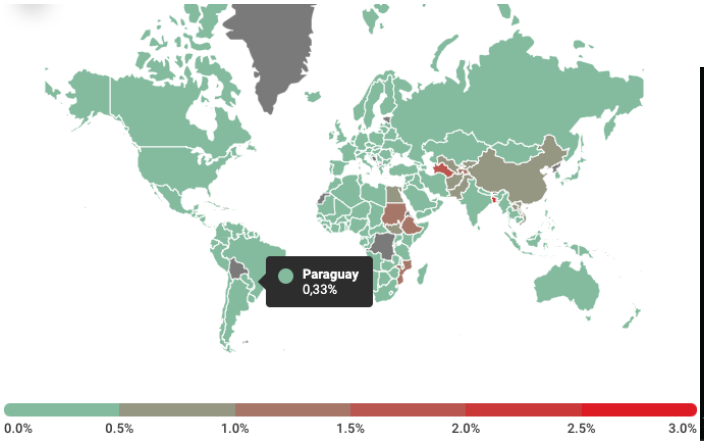
Figura 24. Distribución geográfica de Ghimob

Ransomware

De acuerdo con datos de Kaspersky[4], durante los meses de Julio, Agosto y Septiembre, en Paraguay se registraron detecciones de ransomware los cuales representaron 0,33% de las detección totales de antivirus mencionado. Actualmente, Paraguay se encuentra en la posición #41 en cuanto a ocurrencia de ataques de ransomware.

Hasta hoy en día WannaCry sigue siendo el ransomware con mayor actividad y con más detecciones hechas por Kaspersky, tanto a nivel global como también específicamente en Paraguay.

[3] Fuente: https://securelist.com/it-threat-evolution-q3-2020-non-mobile-statistics/99404/
[4] Fuente: https://securelist.com/it-threat-evolution-q3-2020-non-mobile-statistics/99404/



1	Trojan-Ransom.Win32.Wanna.m	63.68%
2	Trojan-Ransom.Win32.Cryptor.vho	24.43%
3	Trojan-Ransom.Win32.Wanna.zbu	6.84%
4	Trojan-Ransom.Win32.Encoder	2.06%
5	trojan-ransom.win32.Agent.vho	0.84%
6	Trojan-Ransom.Win32.Crypmodng.gen	0.31%
7	trojan-ransom.win32.Crypren.gen	0.22%
8	Trojan-Ransom.Win32.Encoder.ctu	0.18%
9	Trojan-Ransom.Win32.Blocker.pef	0.13%
10	Trojan-Ransom.Win32.Agent.fir	0.13%

Figura 25. TOP 10 de Ransomware detectados por Kasperky en Paraguay

Amenazas mediante navegación web

Si bien, Paraguay no se sitúa en el Top 20 de países de riesgo, de acuerdo con datos de Kaspersky[5], en al menos 6,0479% de los usuarios[6] se detectaron intentos de infecciones de malware con origen en la navegación por Internet.

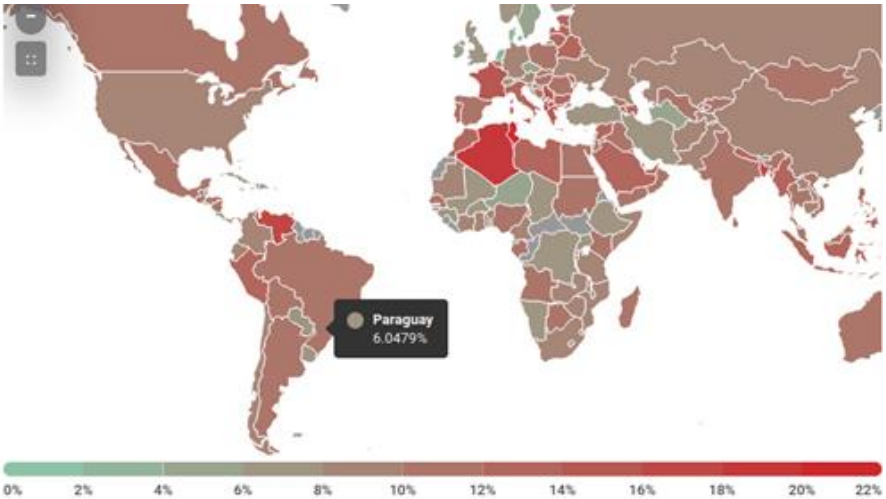


Figura 26. Mapa de distribución de amenazas mediante navegación web en el mundo (2020)- Fuente: Kaspersky[7]

[5] Fuente: https://securelist.lat/kaspersky-security-bulletin-2020-statistics/92035/
[6] Estadística obtenida a partir del antivirus Kaspersky, por lo que el universo de la misma son únicamente los usuarios de sus productos
[7] 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 27. Top 10 de amenazas web más detectadas en Paraguay – Fuente: Kaspersky[8]

Amenazas de infecciones locales

De acuerdo a datos de Kaspersky[9], en aproximadamente 16,03% de los usuarios[10] se ha encontrado algún tipo de archivo u objeto malicioso que ha logrado ingresar al equipo de la víctima, ya sea mediante un dispositivo removible (USB, disco duro, etc.), un malware dropper[11] no detectado o una infección manual como parte de un ataque más avanzado. Este porcentaje es ligeramente inferior a la media mundial, 21.1%.

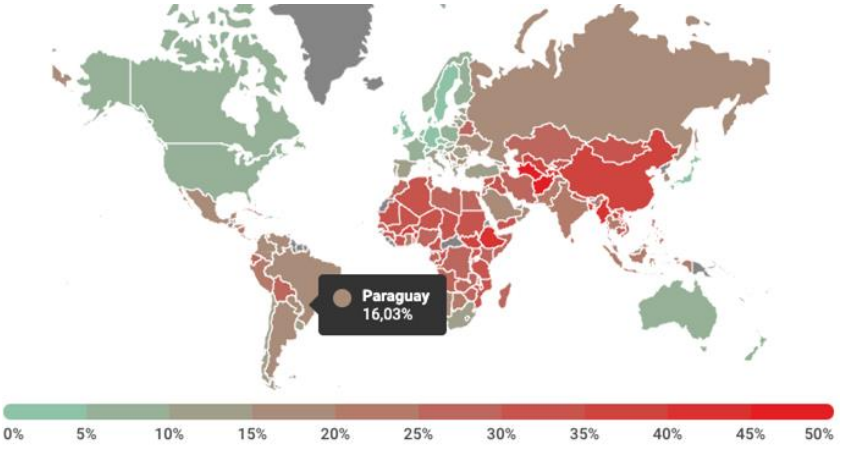


Figura 28. Mapa de distribución de equipos con infecciones locales en el mundo (Q3 2020). Fuente: Kaspersky[12]

[8] Estadística obtenida a partir del antivirus Kaspersky, por lo que el universo de la misma son únicamente los usuarios de sus productos
[9] Fuente: https://securelist.com/it-threat-evolution-q3-2020-non-mobile-statistics/99404/
[10] Estadística obtenida a partir del antivirus Kaspersky, por lo que el universo de la misma son únicamente los usuarios de sus productos
[11] 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
[12] Estadística obtenida a partir del antivirus Kaspersky, por lo que el universo de la misma son únicamente los usuarios de sus productos

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

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 29. Top 10 de infecciones detectadas en Paraguay – Fuente: Kaspersky[13]

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[14]. Se trata de un engaño mediante una historia completamente falsa, que sin embargo tiene una alta efectividad, muchas víctimas lo creen y pagan.

Cabe destacar que el 27 de enero del 2021, EUROPOL y varios organismos de aplicación de la ley han realizado una operación para desmantelar la botnet EMOTET. No solo han tomado control de la infraestructura de comando y control, sino que, a través de uno de los servidores controlados, han inyectado una modificación en el malware a través de una actualización controlada, una "bomba de

[13] Estadística obtenida a partir del antivirus Kaspersky, por lo que el universo de la misma son únicamente los usuarios de sus productos
[14] Más información: https://www.cert.gov.py/index.php/noticias/mensajes-extorsivos-por-correo-su-cuenta-ha-sido-hackeda

tiempo" en el código del malware que ejecutará una rutina de desinstalación del malware el próximo 25 de abril. Eso significa que, muy probablemente, la/s máquina/s infectada/s se desinfecten automáticamente en esa fecha, sin que se requiera acciones adicionales por parte de los usuarios. Se puede encontrar más información en el siguiente boletín: https://www.cert.gov.py/noticias/operacion-internacional-para-desbaratar-emotet-la-botnet-mas-grande-del-mundo

Además de Emotet, también se observa un alto volumen de correos con archivos adjuntos que explotan la vulnerabilidad CVE-2017-11882, una vulnerabilidad de ejecución remota de código que afecta a Microsoft Office, constituyendo éste el dropper de malware más popular por parte de los criminales para la distribución de varias familias de malware.

1	Trojan.MSOffice.SAgent.gen	33.94%
2	DangerousObject.Multi.Generic	24.05%
3	Exploit.MSOffice.CVE-2017-11882.gen	5.85%
4	Trojan.Win32.Badun.gen	5.13%
5	Trojan-PSW.MSIL.Agensla.gen	5.09%
6	Trojan.Script.Generic	4.57%
7	Trojan-Downloader.Script.Generic	2.34%
8	Hoax.Script.Mailoy.gen	2.03%
9	Trojan.MSIL.Inject.gen	1.35%
10	Trojan-Downloader.MSOffice.Agent.gen	1.18%

Figura 30. Top 10 de amenazas distribuidas por correo electrónico en Paraguay[15]

Ataques de red

De acuerdo con datos de Kaspersky[16], a nivel de ataques de red, la técnica más observada en Paraguay en el 2020 es el ataque de fuerza bruta de RDP (Remote Desktop Protocol) o Escritorio Remoto. Le siguen las explotaciones de ciertas vulnerabilidades de SMB, tales como MS17-010, CVE-2017-0147, NetAPI-BOF Otra vulnerabilidad que se observa que es escaneada frecuentemente es identificada como Intrusion.Win.NETAPI.buffer-overflow.exploit, un ataque se se dirige a equipos con Windows e intenta explotar un error en el analizador de canonización de rutas de la biblioteca NetAPI de Servidor a través de una solicitud RPC especialmente diseñada. Un ataque usa SMB como un protocolo subyacente para realizar solicitudes RPC; por lo tanto, opera a través de los puertos TCP 139 y 445. En la 9ª posición se

[15] Estadística obtenida a partir del antivirus Kaspersky, por lo que el universo de la misma son únicamente los usuarios de sus productos
[16] Fuente: https://securelist.com/it-threat-evolution-q3-2019-statistics/95269/

observa una alta frecuencia de los intentos de explotación de CVE-2018-1273 que afecta al framework Spring.

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 31. Top 10 de ataques de red detectadas en Paraguay – Fuente: Kaspersky[17]

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 finales 2019 e inicio del 2020. El mayor pico en el que **se observó la participación de sistemas paraguayos** se registró entre el 29 de mayo y 1 de junio del 2020 **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.

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

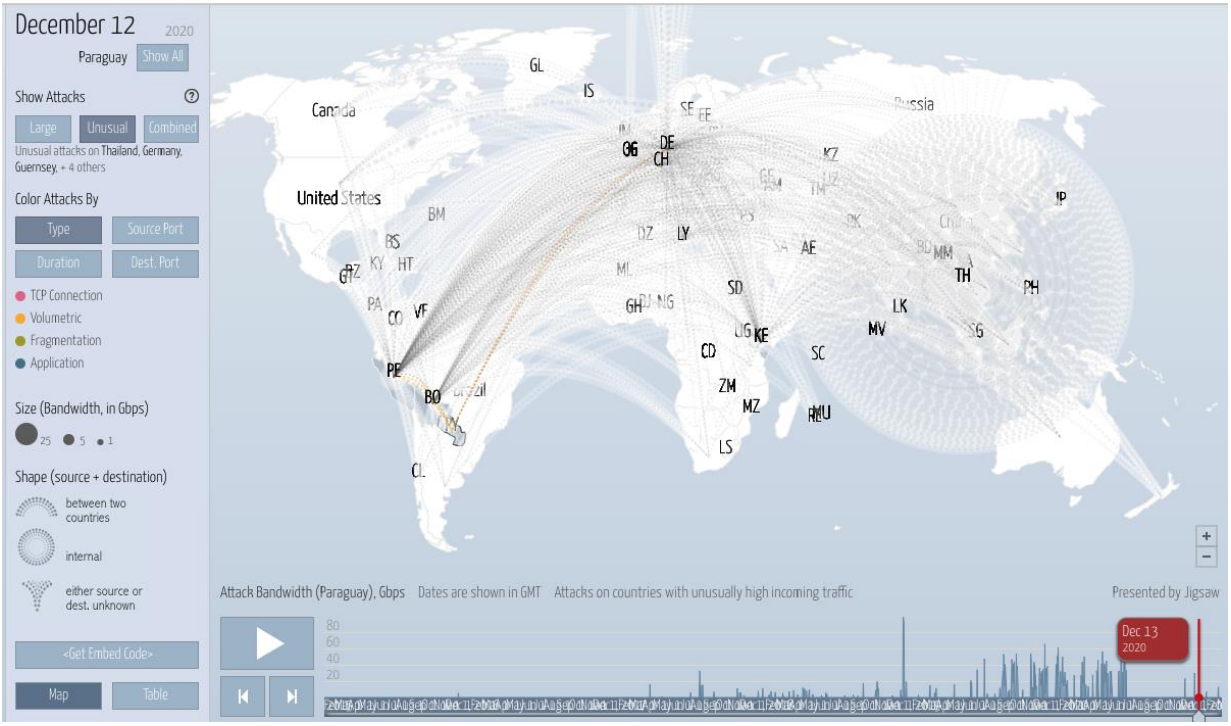


Figura 32. Instantánea de tráfico de denegación de servicio saliente y entrante capturado por Digital Attack Map el 13/12/2020 de Paraguay

De acuerdo con los datos proveídos por **Netscout**[18], otro proveedor de servicios, se registraron 1650 ataques de DoS a servicios paraguayos, con un poco de volumen de 114 Gbps. La máxima duración de un ataque fue de 1 día y 9 horas. Las técnicas de ataque más utilizadas fueron Fragmentación de IP y Amplificación DNS.

Figura 33. Resumen de ataques DDoS en Paraguay en el 2020 según Netscout

[18] Datos proveidos por https://horizon.netscout.com/

De acuerdo a los datos de Netscout[19], la mayor cantidad de los ataques a servicios paraguayos recibidos tuvieron como origen EE.UU. como 34.9%, Brasil con un 26.2% y Argentina con un 26.1%.

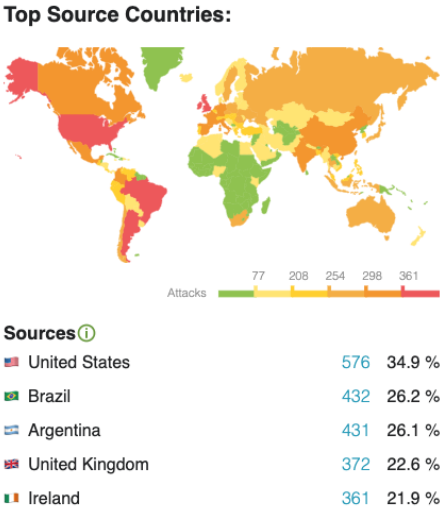


Figura 34. Top 5 de paises de los cuales se originaron ataques DDoS hacia el Paraguay

La mayor cantidad de ataques de DDoS según Netscout[20] se dieron los meses de Abril, Enero y Julio, y el 48.82% de todos los ataques duraron entre 10 min a 1 hora.

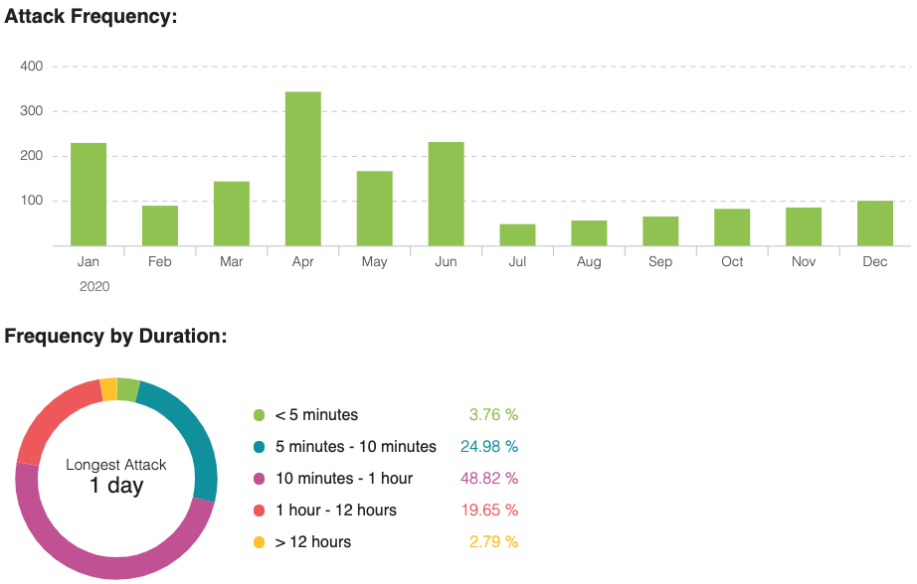


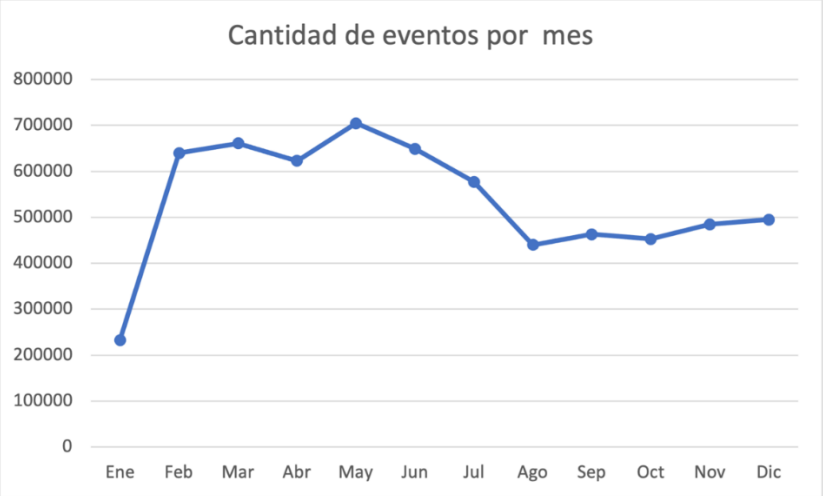
Figura 35. Frecuencia de ataques de DDoS - NETSCOUT

[19] Datos proveidos por https://horizon.netscout.com/
[20] Datos proveidos por https://horizon.netscout.com/

Otras fuentes de datos específicas para Paraguay - Shadowserver

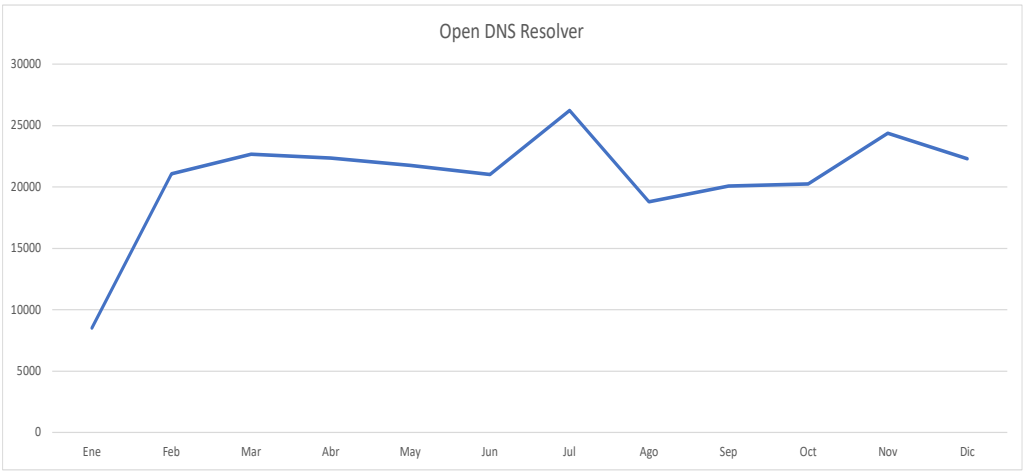
Diariamente el CERT-PY recibe un gran volumen de indicadores de compromisos (Indicators of Compromise - IoC)[21] y reportes de exposiciones que involucran a IPs o dominios paraguayos, de diversas fuentes, entre ellas Shadowserver Foundation, una organización sin fines de lucro dedicada al intercambio de información de amenazas de ciberseguridad con la cual el CERT-PY ha establecido un acuerdo.

- Cantidad promedio de eventos de IoCs recibidos diariamente: ~ 35.192

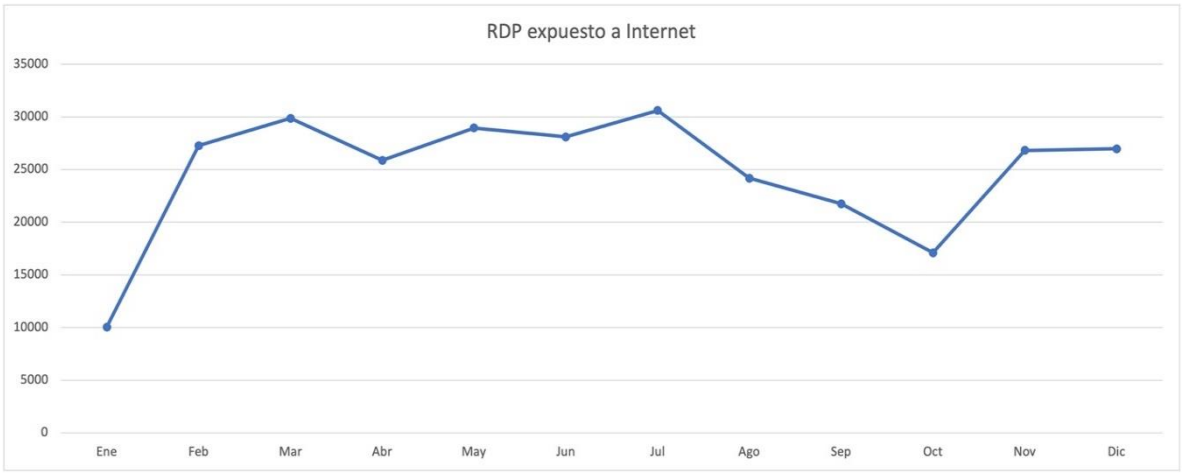


- En general, servicios vulnerables y/o expuestos reportados diariamente: ~ 14.922
- Se reportaron un total de 190.664 IPs únicas con servicios vulnerables, expuestos o comprometidos por malware.
- Servidores DNS Openresolver: cantidad promedio de IPs diarias ~683 (a través de ellos se pueden realizar enormes ataques de denegación de servicio)

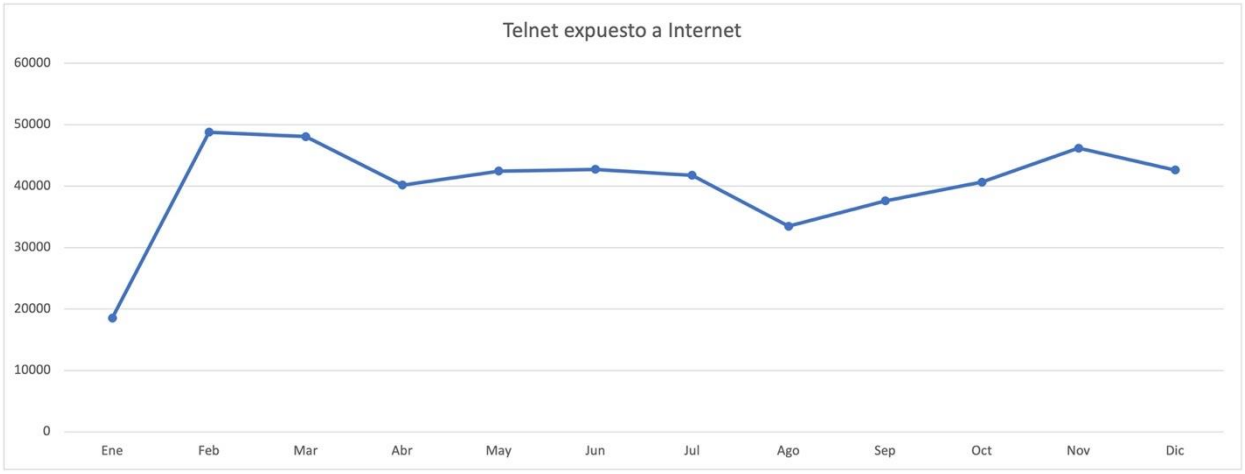
[21] IoC es algún tipo de dato o información que sirve para identificar si un sistema se ha visto involucrado o afectado por un incidente de seguridad, siendo un indicador de probable compromiso.



- Cantidad promedio de IPs detectadas diariamente con RDP expuesto a Internet: ~815



- Distribución eventos recibidos diariamente con Telnet expuesto a Internet: ~1.323
- Cantidad de IPs únicas con Telnet expuesto a Internet: 8.804



- 238 IPs únicas participaron de ataques de denegación de servicio de amplificación distribuido.
- 1.504 IPs únicas realizaron ataques de fuerza bruta a otros sistemas.
- Promedio diario de IPs en lista negra (spam, infecciones, actividad maliciosa, etc): ~ 443
- Cantidad de IPs únicas que entraron en lista negra: 15.990

- Cantidad promedio de IPs infectadas con malware, pertenecientes a una botnet, visualizadas por día: ~ 1.528
- Cantidad de IPs únicas infectadas con malware, pertenecientes a una botnet: 59.073
- Más de 240 familias de malware únicas detectadas en IPs paraguayas. Las más detectadas son las siguientes:

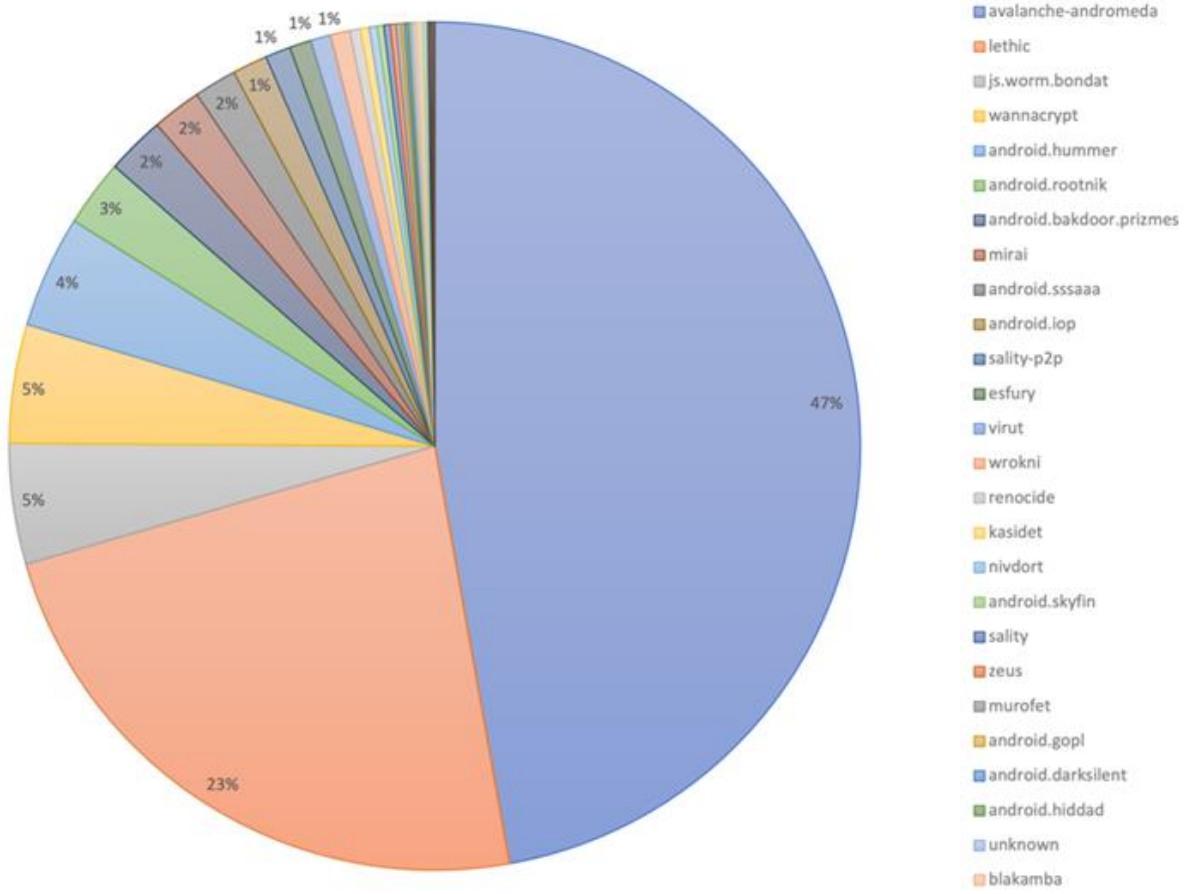


Figura 36. Cantidad de infecciones únicas por familia de malware[22]

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:

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

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

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[23]. 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[24], pero aún así existen muchas máquinas en los que se encuentra el bot, el cual, aunque no representa una amenaza activa, consume recursos de la máquina y la red y podría, eventualmente, ser reactivada por criminales.

[23] 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.

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

Plan Nacional de Ciberseguridad

El Plan Nacional de Ciberseguridad es un documento estratégico que sirve como fundamento para la coordinación de las políticas públicas de ciberseguridad, integrando a todos los sectores en el desarrollo de las Tecnologías de la información y comunicación (TIC) en un ambiente cibernético confiable y resiliente. Es la hoja de ruta del Estado paraguayo en cuanto a las estrategias, planes e iniciativas de ciberseguridad, en busca de objetivos concretos y líneas de acción bien definidas en dicho Plan.

Este Plan, que se encuentra aprobado mediante el Decreto PE 7052/17, ha sido elaborado bajo el liderazgo de la Presidencia de la República del Paraguay, a través de la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATIC), (hoy en día, Ministerio de Tecnologías de la Información y Comunicaciones – MITIC) y en coordinación con el Ministerio de Relaciones Exteriores, con la participación de los diversos sectores involucrados en el tema de la ciberseguridad en Paraguay, bajo el apoyo y facilitación de la Organización de los Estados Americanos (OEA).

Consta de 7 ejes:

1. Sensibilización y Cultura
2. Investigación, Desarrollo e Innovación
3. Protección de Infraestructuras Críticas
4. Capacidad de Respuesta ante Incidentes Cibernéticos
5. Capacidad de Investigación y Persecución de Ciberdelincuencia
6. Administración Pública
7. Coordinación Nacional

El Plan consta de 20 objetivos estratégicos misionales y 60 líneas de acción operativas alineadas a esos objetivos. Se debe notar que los primeros 6 ejes tienen un sentido estratégico, mientras que el último eje (Coordinación Nacional) consta de objetivos y líneas de acción tendientes a la operativización y seguimiento del propio Plan.

En febrero del 2020 la Comisión Nacional de Ciberseguridad ha aprobado un mecanismo de medición que permitan medir el grado de cumplimiento de las diferentes acciones del Plan Nacional de Ciberseguridad. Se adoptó un mecanismo de medición cualitativo, con una escala definida de 3 niveles:

Nivel 1 (rojo)	**No se realizó ninguna o prácticamente ninguna acción**
Nivel 2 (amarillo)	**Se realizó alguna iniciativa o acción pero de manera esporádica, no sistematizada ni sostenible**
Nivel 3 (verde)	**La línea de acción se implementó de manera permanente y sostenible a través de alguna iniciativa aprobada por un instrumento legal (ley, decreto, resolución, etc.) y/o un programa con presupuesto fijo establecido**

En febrero del 2020, a través de la Comisión Nacional de Ciberseguridad, se realizó la primera medición utilizando este método, arrojando el siguiente resultado:

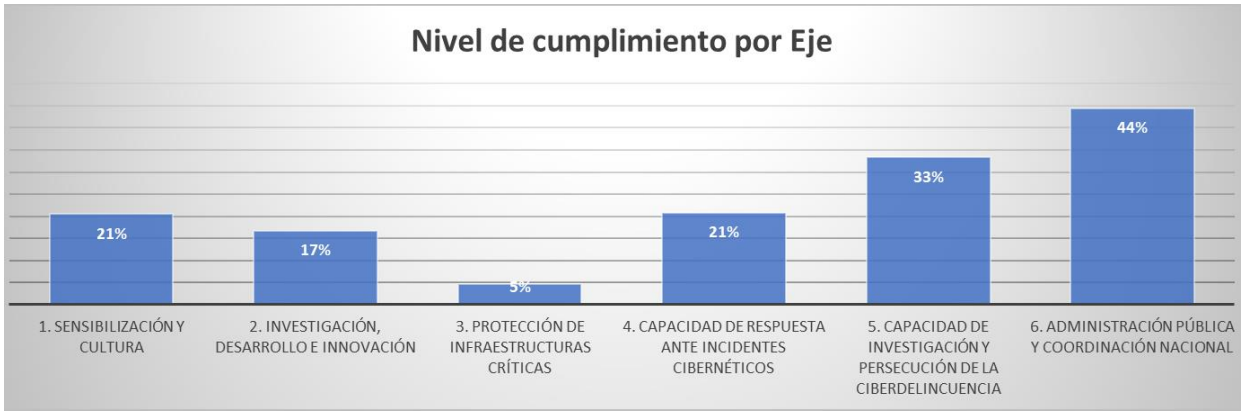
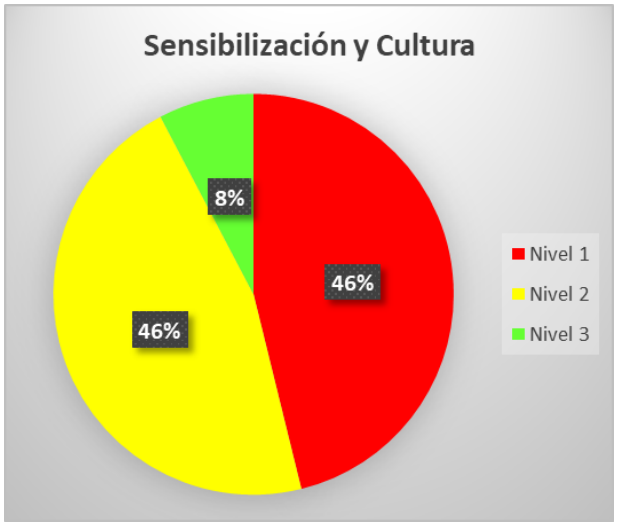


Figura 37. Nivel de avance global del Plan Nacional de Ciberseguridad - Febrero 2020



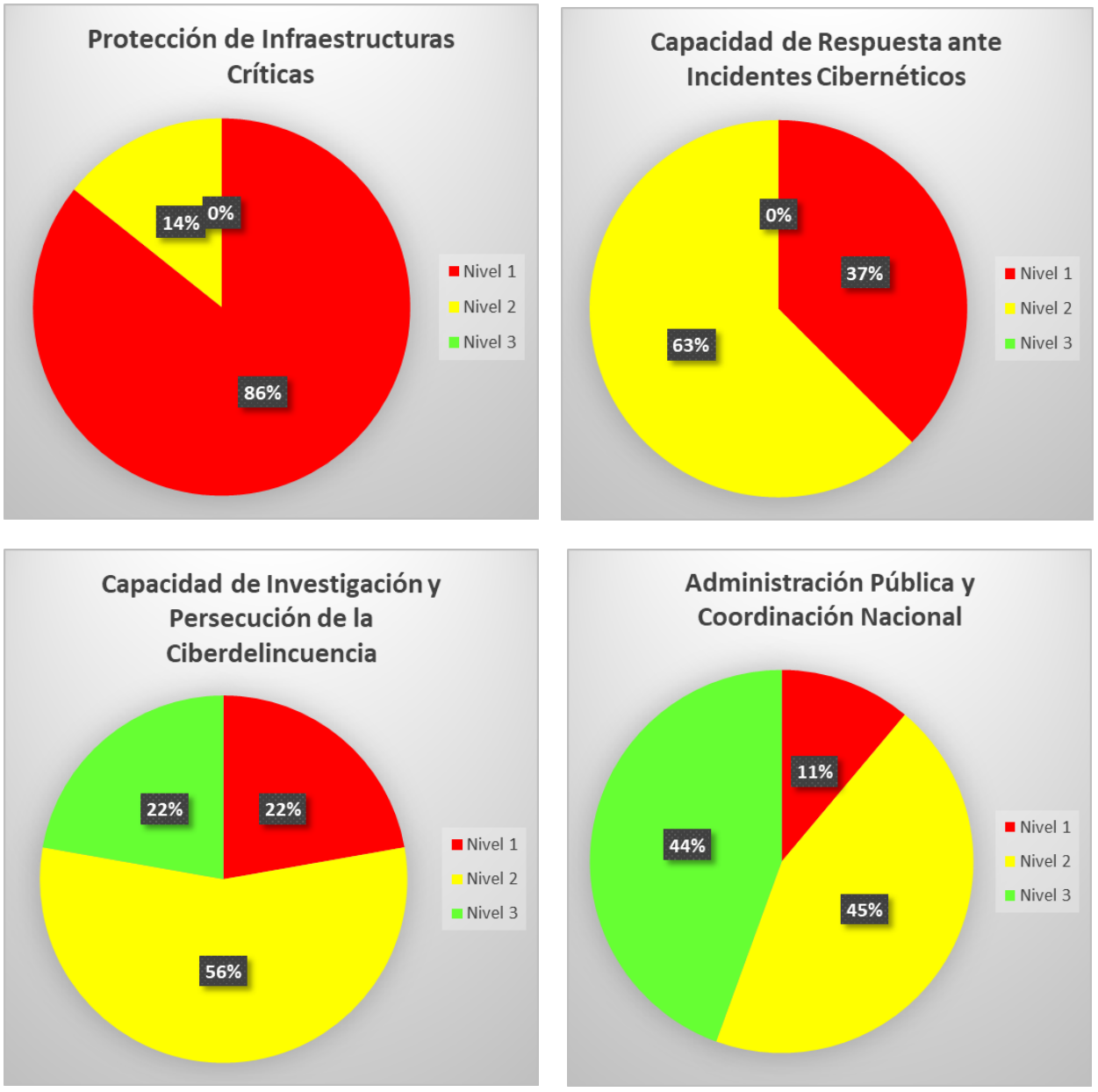


Figura 38. Nivel de cumplimiento de líneas de acción del PNC por eje - Febrero 2020

Políticas, estándares y normativas en materia de Ciberseguridad

Desde finales del año 2018 se han diseñado y aprobado diversas políticas, estándares, directivas y normativas en materia de ciberseguridad, aplicables, principalmente, para las instituciones gubernamentales. En el año 2020 se han realizado diversos esfuerzos para medir el nivel de cumplimiento de dichas normativas. En materia de políticas de ciberseguridad, actualmente se encuentran aprobados y vigentes:

Modelo de Gobernanza de Seguridad de la Información del Estado

Aprobado mediante la Resolución Nº 733/2019 del MITIC. Se trata de una directiva mediante la cual se establece que todas las instituciones del Estado deben contar con un **área de Seguridad de la Información**, con el objetivo de 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.

Hasta el momento, de 136 instituciones públicas, 72 instituciones (52%) ya han designado formalmente a un Responsable de Seguridad de la Información.

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.

Al respecto, el MITIC ha realizado una encuesta a los Responsables de Seguridad de la Información de 49 instituciones arrojando los siguientes resultados más resaltantes:

Solo el 26% de las instituciones tienen áreas de Seguridad de la Información o Ciberseguridad cuya función principal es este aspecto. En el 10% de las instituciones, el Responsable de Seguridad de la Información lo es a tiempo parcial, sin ser su función principal, debiendo realizar otras funciones. En muchos casos (21 instituciones, 30%) el Responsable de Seguridad de la Información es el mismo Director de TIC, debiendo dividir su tiempo, atención y recursos en ambos aspectos.

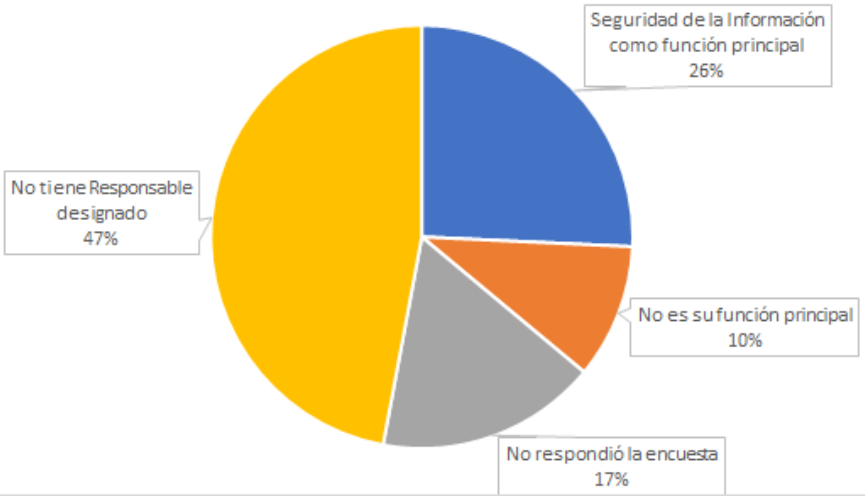


Figura 39. Direcciones o áreas de Seguridad de la Información en las instituciones Estado.

En cuanto al tiempo dedicado a los roles y responsabilidades de ciberseguridad, el 35% de los Responsables de Seguridad de la Información designados formalmente, lo realiza de forma regular, el 29% una o dos veces por mes, el 16% todos los días, el 12% hasta 3 días a la semana, el 6% más de 3 horas diarias, el 2% menos de 3 horas diarias.

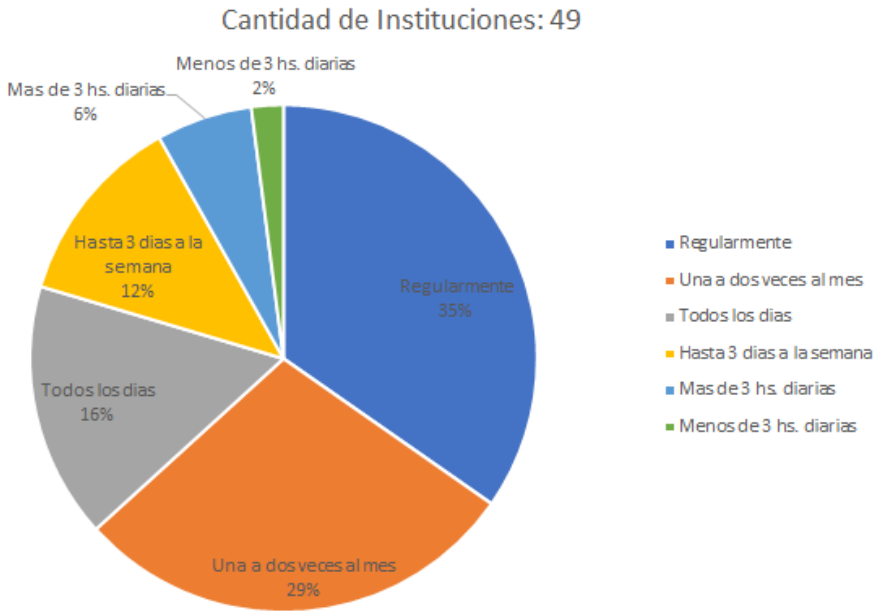


Figura 40. Tiempo dedicado a los Roles y Responsabilidades de un RSI en el Estado

Solo 18 instituciones (13%) cuenta con un área de Seguridad de la Información incluido **formalmente** en el organigrama de la institución. El 60% de las instituciones no lo tiene definido en el Organigrama. En el 11% de las instituciones, el área de Seguridad de la Información o Ciberseguridad depende del área de TIC. Apenas en el 8% (11 instituciones) tiene un área específica definida formalmente en el organigrama y dependiente de la Máxima Autoridad. La gran mayoría de estas áreas se componen de apenas una persona (ver sección “Recursos Humanos”)

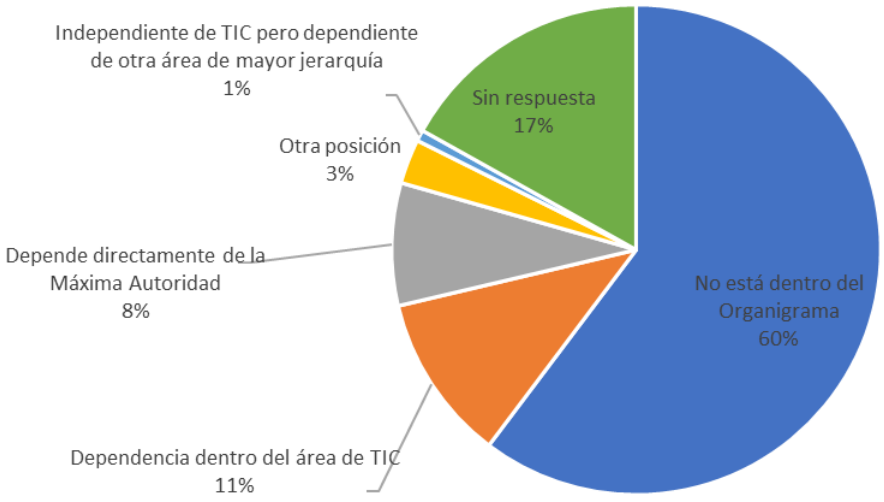


Figura 41. Nivel de jerarquía e interdependencia del área de Seguridad de la Información en el Estado

Respecto a las normas, políticas y procedimientos de seguridad aprobados y conocidos por sus usuarios, del total de 49 instituciones analizadas, el 44,9% tiene de forma parcial, el 30,6% no tiene, y el 24,5% cuenta con normas de seguridad aprobadas.

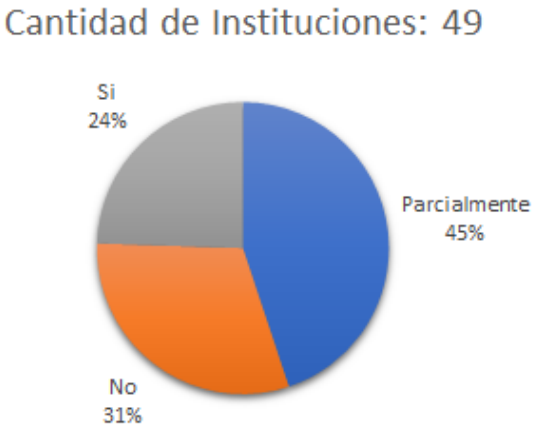


Figura 42. Normas, políticas y procedimientos de seguridad aprobados y conocidos por usuarios en Instituciones pública

Además en el marco del Decreto presidencial N° 6234/2016, en el que se declara de interés las TIC y se define la estructura mínima con que deben contar las instituciones, el MITIC tiene registro de la designación formal de 80 Directores de Tecnologías de la Información y Comunicación en sus instituciones. 56 instituciones (41%) no han designado formalmente un Director de TIC.

Los Controles Críticos de Ciberseguridad

Es un estándar para los organismos y entidades del Estado (OEE), aprobado y actualizado mediante la Resolución Nº 277/2020 del MITIC. 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 aplicación de la Resolución, siendo igualmente recomendable su adopción por parte de 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, desde el 2021 las instituciones tendrán a disposición un sistema único centralizado, desde donde pueden cargar el diagnóstico de cumplimiento de los Controles Críticos de Ciberseguridad, y generar reportes e históricos, respecto al avance de los mismos.

En una encuesta realizada los Responsables de seguridad de la información de 49 instituciones del Estado, sobre los diagnósticos de seguridad formales del estado de la seguridad en sus instituciones (GAP Analysis o similar, ya sea utilizando los Controles Críticos de Ciberseguridad u otro marco de referencia), se observa que el 31% no tiene definido, el 27% lo hace de forma regular, el 22% nunca lo ha realizado, el 12% al menos una vez en los últimos 2 años.

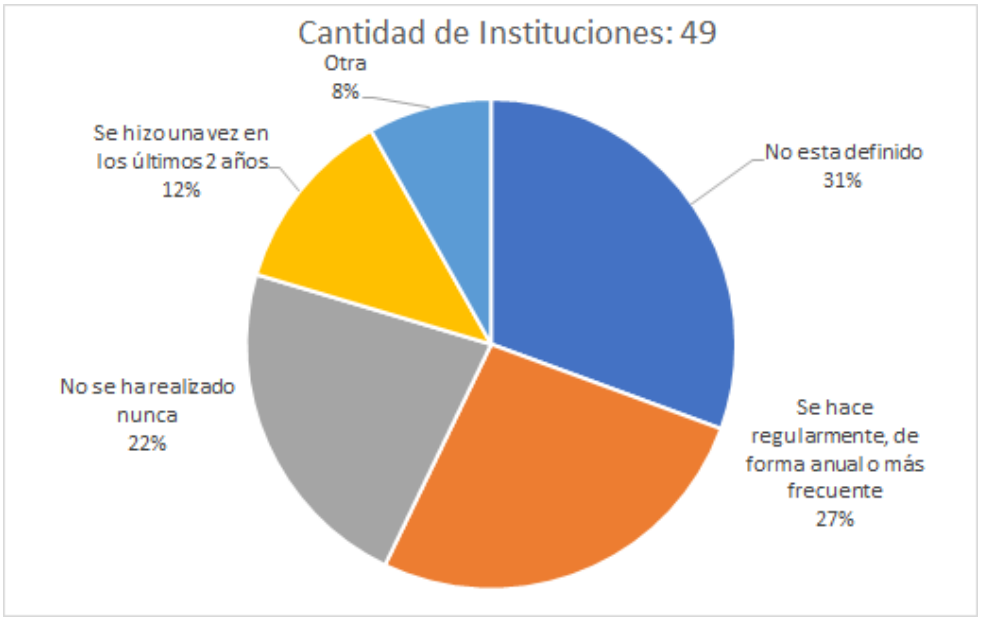


Figura 43. Frecuencia de diagnósticos de seguridad formales del estado de la seguridad en instituciones públicas

En cuanto al área encargada operativamente de la implementación y mantenimiento de los Controles Críticos de Seguridad, en el 33% lo realiza en área de TIC, en el 31% lo hace Responsable de Seguridad Informática, en el 18% el Responsable de seguridad de la Información, 8% no tiene definido o no se encarga nadie.

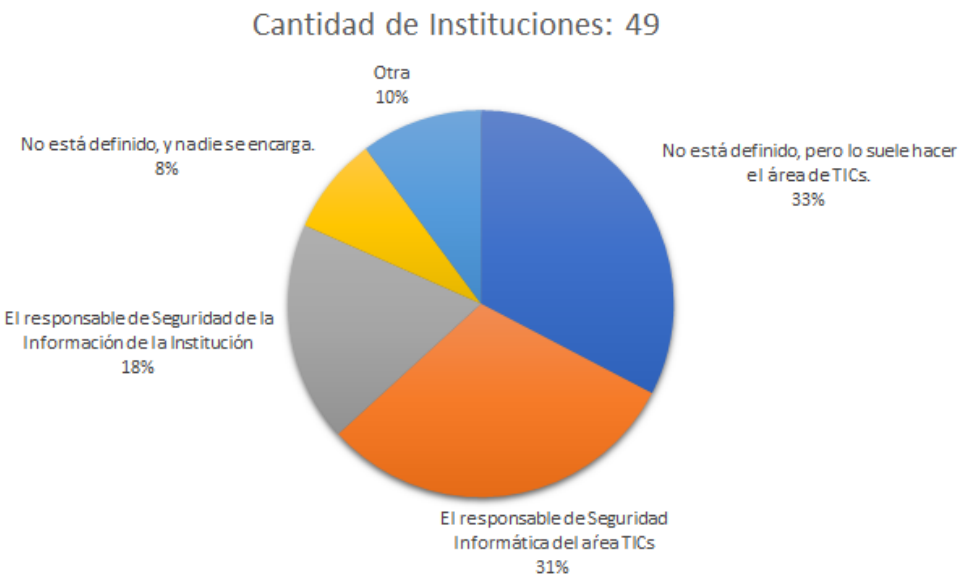


Figura 44. Área encargada operativamente de la implementación y mantenimiento de Controles Críticos de Seguridad

Respecto al monitoreo y revisión para un diagnóstico o evaluación del estado de la seguridad, en el 29% de los casos lo realiza el Responsable de Seguridad Informática, el 26% lo hace el Responsable de Seguridad de la Información, el 27% el área TIC, 10% nadie.

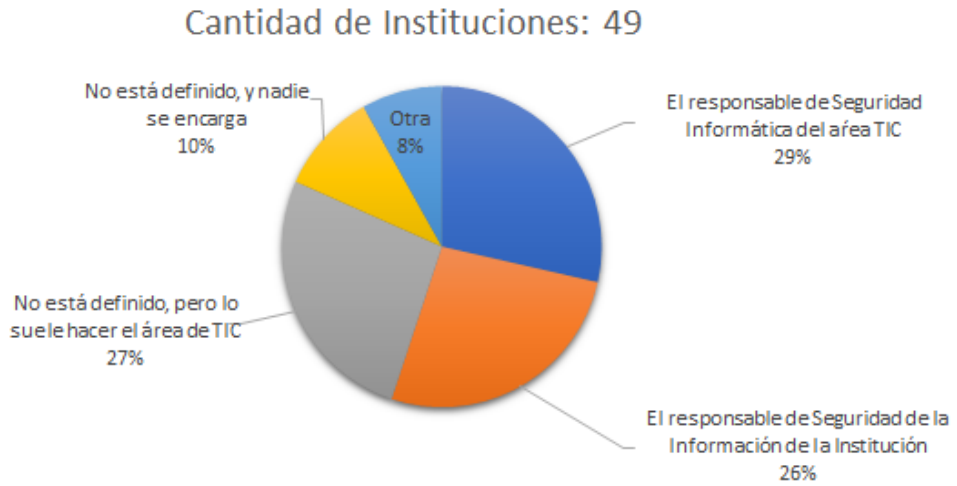


Figura 45. Área encargada del monitoreo y revisión para un diagnóstico o evaluación del estado de la seguridad

Criterios mínimos de seguridad para el desarrollo y adquisición del software

Fueron aprobados y actualizados mediante la Resolución Nº 699/2019 del MITIC. Los principales cambios en dicha directiva, respecto al anterior 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**

Esta normativa no limita que la auditoría de vulnerabilidades debe ser tercerizada; las instituciones podrían hacerlo con recursos internos propios o mediante la contratación de una empresa tercerizada, así como también a través del servicio gratuito que brinda el MITIC. De acuerdo al portal de la DNCP, solamente 5 instituciones cuentan o han contado con servicios de auditorías de vulnerabilidades durante el año 2020. Además, 7 instituciones han solicitado y usufructuado el servicio del MITIC, desde la vigencia de dicha directiva. En total, 18 sistemas diferentes fueron auditados mediante dicho servicio.

Las Directivas de Ciberseguridad para Canales de Comunicación oficiales del Estado

Aprobado mediante la Resolución N°. 432/2019 del MITIC, 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.

En una encuesta realizada a los administradores y/o responsables de los Canales de Comunicación del Estado, ha arrojado el siguiente resultado:

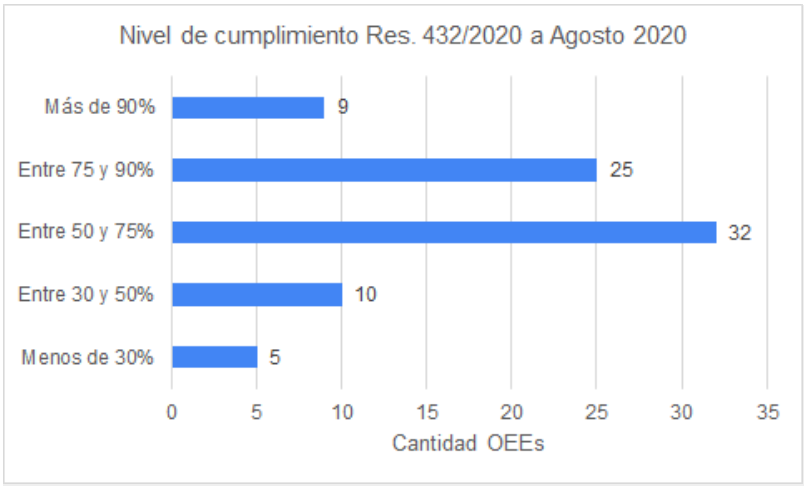


Figura 46. Nivel de cumplimiento Res. MITIC Nro. 432/2020 - Rango de fecha encuestado: Febrero - Agosto 2020

Las instituciones públicas que, de acuerdo a dicha encuesta, han alcanzado un cumplimiento de al menos 90% de las directivas son:

1. Dirección General de Estadística, Encuestas y Censos (DGEEC)
2. Entidad Binacional Yacyretá (EBY)
3. Ministerio de Defensa Nacional (MDN)
4. Ministerio de Obras Públicas y Comunicaciones (MOPC)
5. Ministerio de Tecnologías de la Información y Comunicaciones (MITIC)
6. Petróleos Paraguayos (PETROPAR)
7. Autoridad Reguladora Radiológica y Nuclear (ARN)
8. Secretaria de la Función Pública (SFP)
9. Crédito Agrícola de Habilitación (CAH)

En cuanto a la robustez de las contraseñas en podemos concluir que 47 de las instituciones analizadas (58%) tienen contraseñas robustas en todas sus cuentas oficiales (cuenta de administración de página web, redes sociales, correo institucional oficial), definiendo contraseña robusta como aquella, mínimamente, tiene 12 caracteres y combina minúsculas, mayúsculas, números, caracteres especiales. 31 de las instituciones (38%) tiene, al menos, una contraseña poco robusta. 3 instituciones tienen contraseñas inseguras en todas sus cuentas.

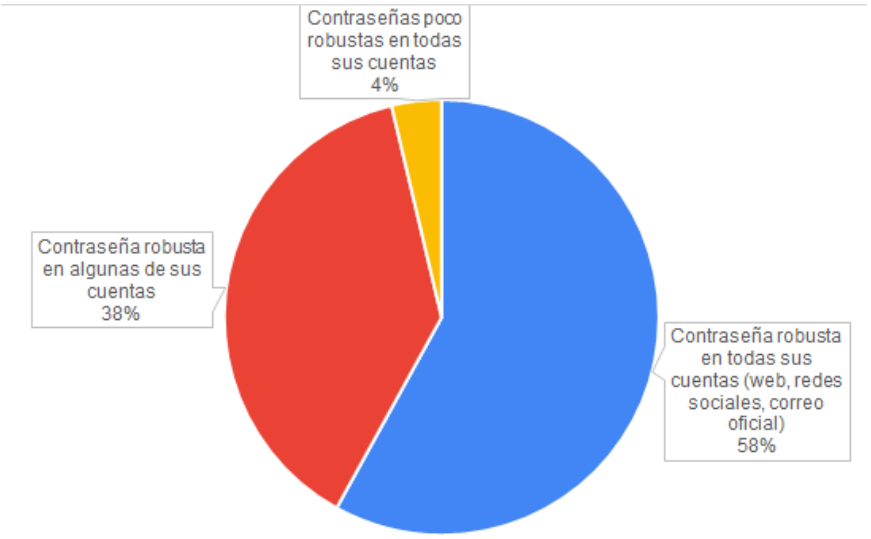


Figura 47. Robustez contraseña de cuentas de comunicación oficiales - Rango de fecha encuestado: Febrero - Agosto 2020

En cuanto al uso de autenticación de doble factor, solo 19 instituciones (24%) lo tiene activado y configurado en todas las cuentas, incluido la página web. 22 instituciones (27%) lo tienen implementado en algunas cuentas, por lo general, en sus redes sociales pero no en la página web. 40 instituciones (49%) no utilizan autenticación de doble factor en ninguna cuenta.

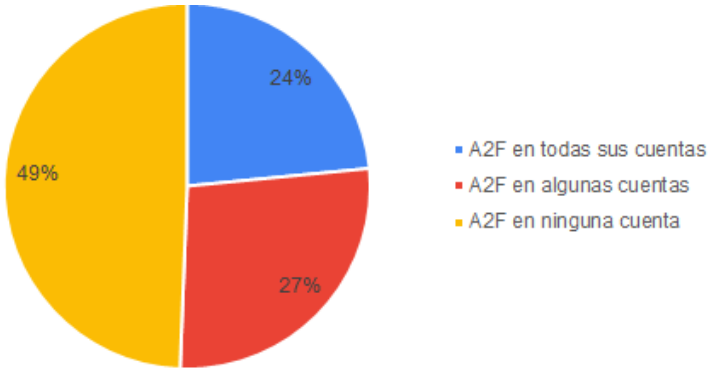


Figura 48. Uso de Autenticación de doble factor en cuentas oficiales - Rango de fecha encuestado: Febrero - Agosto 2020

34 instituciones (43%) tienen todas sus cuentas de redes sociales verificadas (check azul), 31 instituciones han verificado solo alguna de sus cuentas, y 13 (16%) todavía no han verificado ninguna. La verificación, si bien, no previene un compromiso de una cuenta, aporta mayor confianza en la cuenta, además de facilitar el proceso de recuperación en caso de un incidente con ésta.

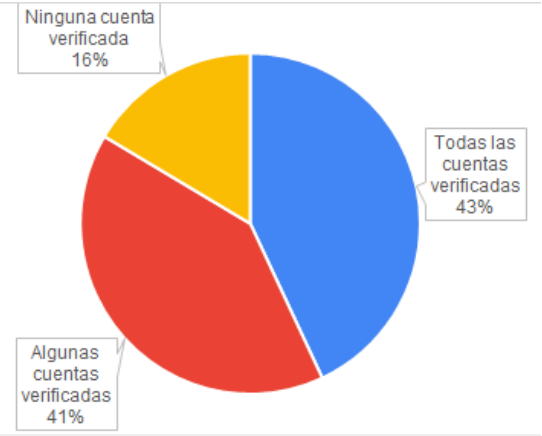


Figura 49. Uso de Autenticación de doble factor en cuentas oficiales - Rango de fecha encuestado: Febrero - Agosto 2020

Otros datos obtenidos:

- 32 instituciones (40%) analizadas utilizan alguna cuenta de correo institucional oficial de manera compartida, dificultando, entre otras cosas, la identificación de responsabilidades y trazabilidad en la misma.
- El 60% de las instituciones tienen configuradas contraseñas de inicio de sesión y contraseñas de desbloqueo de pantalla en todos los dispositivos en los que se utilizan las cuentas oficiales institucionales.
- 44 instituciones (54%) cuenta con procedimientos claros y conocidos para todos los administradores de cuentas oficiales mediante los cuales deben reportar los incidentes, así como también cambiar las contraseñas inmediatamente ante una sospecha de compromiso. 25 instituciones (31%) tienen procedimiento parcialmente conocidos, y 12 de ellas (15%) no tienen ningún tipo de procedimiento

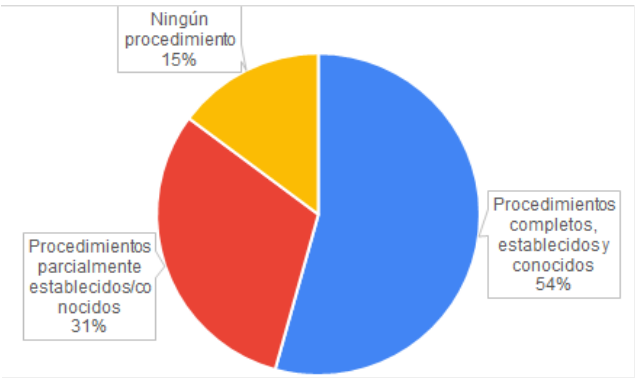


Figura 50. Procedimientos de gestión de incidentes en el manejo de cuentas oficiales - Rango de fecha encuestado: Febrero - Agosto 2020

El reporte obligatorio de incidentes cibernéticos al MITIC

Mediante la Resolución N° 346/2020 del MITIC, se aprobó el reglamento que aprueba e implementa el reporte obligatorio de incidentes de seguridad por parte de los Organismos y Entidades del Estado del ámbito de la ley del MITIC.

Este reglamento establece que todo funcionario público debe reportar cualquier posible incidente cibernético de seguridad al Responsable de Seguridad de la Información (RSI), o, en su defecto, al Director de la UETIC de su Institución. Y es obligación de éstos reportar todo incidente cibernético de seguridad al CERT-PY enviando un correo electrónico a abuse@cert.gov.py, incluyendo una descripción del mismo, así como también cualquier dato que pueda ayudar a investigar el incidente.

Establece además las pautas generales de acción del CERT-PY frente a los reportes recibidos, definiendo el alcance de acción, los niveles y criterios de criticidad, así como también la confidencialidad con la que se manejarán los detalles de los incidentes que le son reportados.

Establece los lineamientos que se deben tener en cuenta en cuanto a la gestión comunicacional de un incidente cibernético, debiendo ésta ser realizada de manera coordinada entre la institución afectada, las áreas técnicas, las áreas comunicacionales, así como también el MITIC, de manera a informar de manera clara, certera y transparente, sin comprometer la investigación, conforme a las guías y lineamientos establecidos, velando por los derechos de todas las personas que fueran afectados por el incidente.

En la encuesta realizada a los Responsables de Seguridad de la Información, se consultó si la institución ha sufrido algún tipo de Incidente de Seguridad de la Información, en los últimos 2 años, y el 53% ha indicado de no ha sufrido incidentes de seguridad, el 39% si lo ha sufrido, y el 8% desconoce.

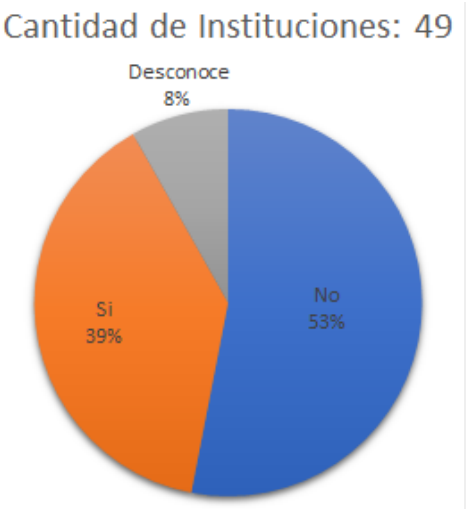


Figura 51. Incidentes de Seguridad de la Información, en los últimos 2 años, en instituciones públicas

Inversión de Ciberseguridad en el Estado

En el año 2020 se han realizado 87 procesos únicos de adquisición de bienes y servicios relacionados específicamente a Ciberseguridad en el Estado Paraguayo, de acuerdo a los datos publicados en el Portal de Contrataciones Públicas[25]. La inversión total para la adquisición de estos bienes y servicios es de **Gs. 43.707.425.158** (aprox. **USD 6.500.000**).

La mayor cantidad de procesos de adquisición ha sido de antivirus corporativos, con 39 adquisiciones, seguido de soluciones de Firewall y seguridad perimetral. Adquisiciones de soluciones de ciberseguridad más específicas o avanzadas tales como Gateway de seguridad de correo, Protección DNS, Centralización y monitoreo de logs han sido poco frecuentes. Servicios de ciberseguridad tales como Auditorías de vulnerabilidades, Análisis GAP, pentesting o similares han sido escasos.

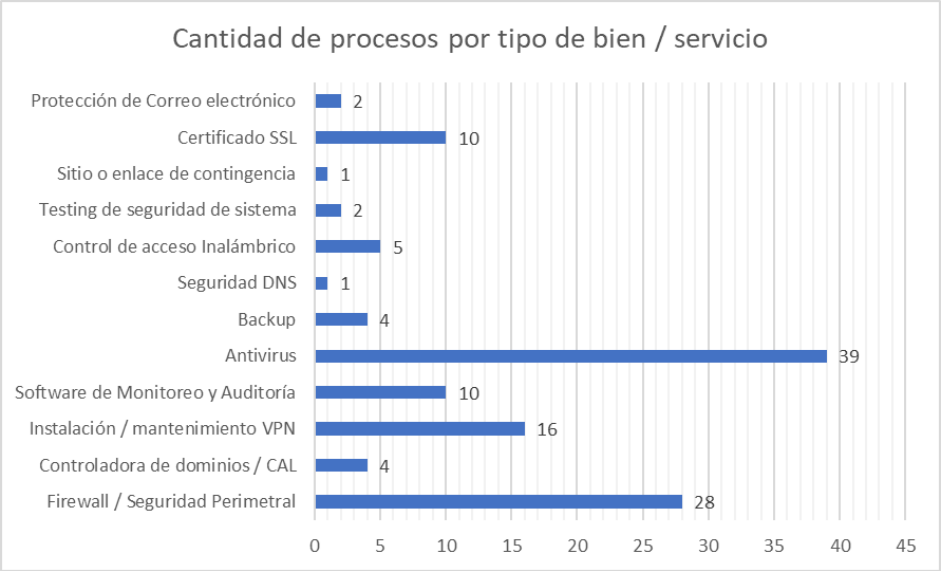


Figura 52. Cantidad de procesos por tipo de bien o servicio por parte de OEEs en 2020

En cuanto al volumen de inversión, el mayor monto corresponde a soluciones de Firewall y seguridad perimetral, con Gs. 16.769.296.373 (aprox. USD 2.500.000), seguido de licencias CAL para controladoras de dominio, con Gs. 8.585.552.700 (aprox. USD 1.300.000).

[25] Datos obtenidos a partir del análisis de datos de https://www.contrataciones.gov.py/datos/ . El análisis se ha realizado a partir de filtros de ítems de Categoría 5 del Código de Catálogo relacionados a ciberseguridad. Aquellos procesos de adquisición en las que el OEE no hubiera especificado explícitamente un item, o aquellos procesos de adquisición que no hayan sido publicados en el Portal de Contrataciones Públicas, podrían no verse reflejados en estas estadísticas

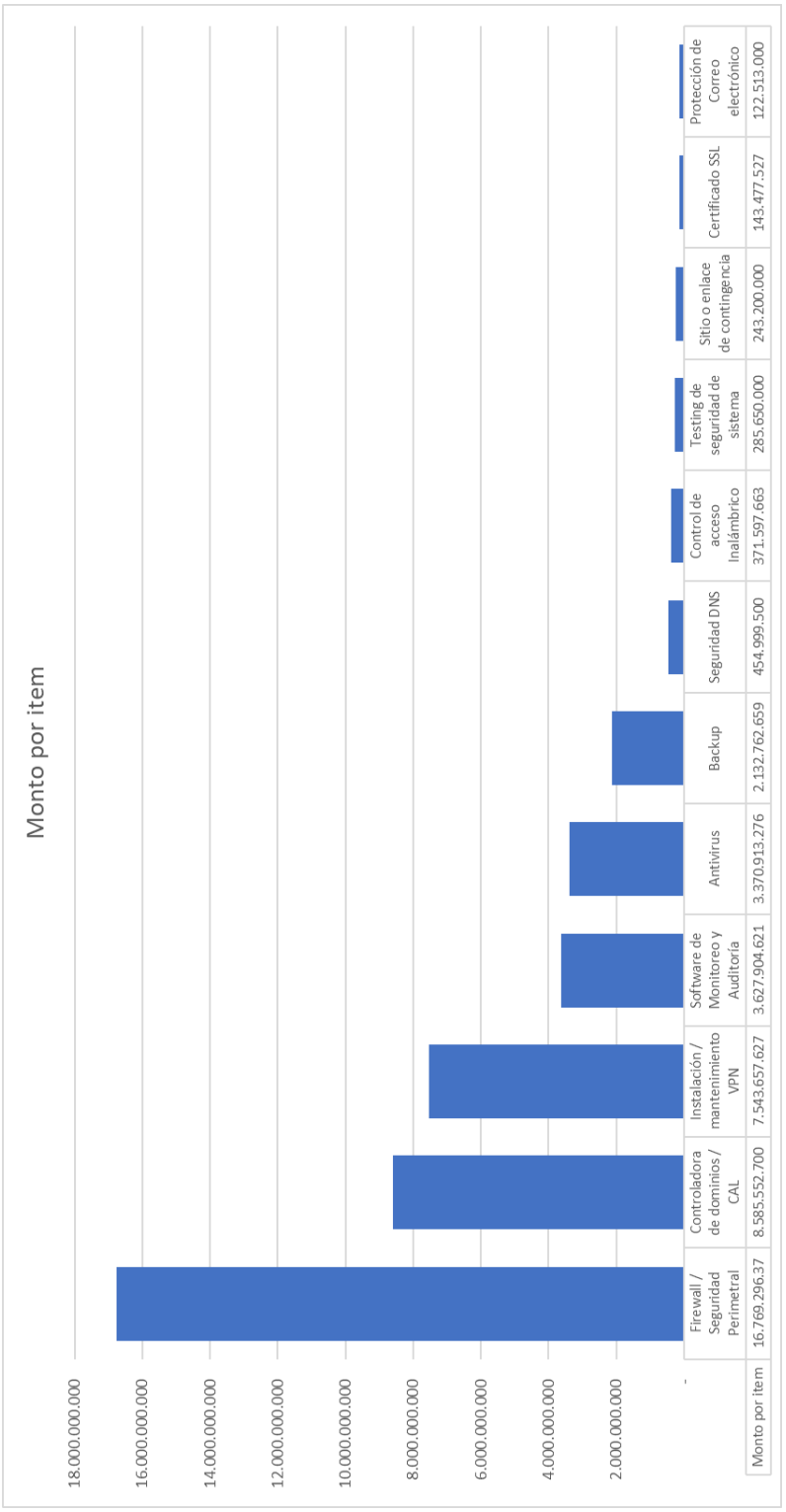


Figura 53. Inversión en ciberseguridad clasificada por rubro a lo largo del 2020

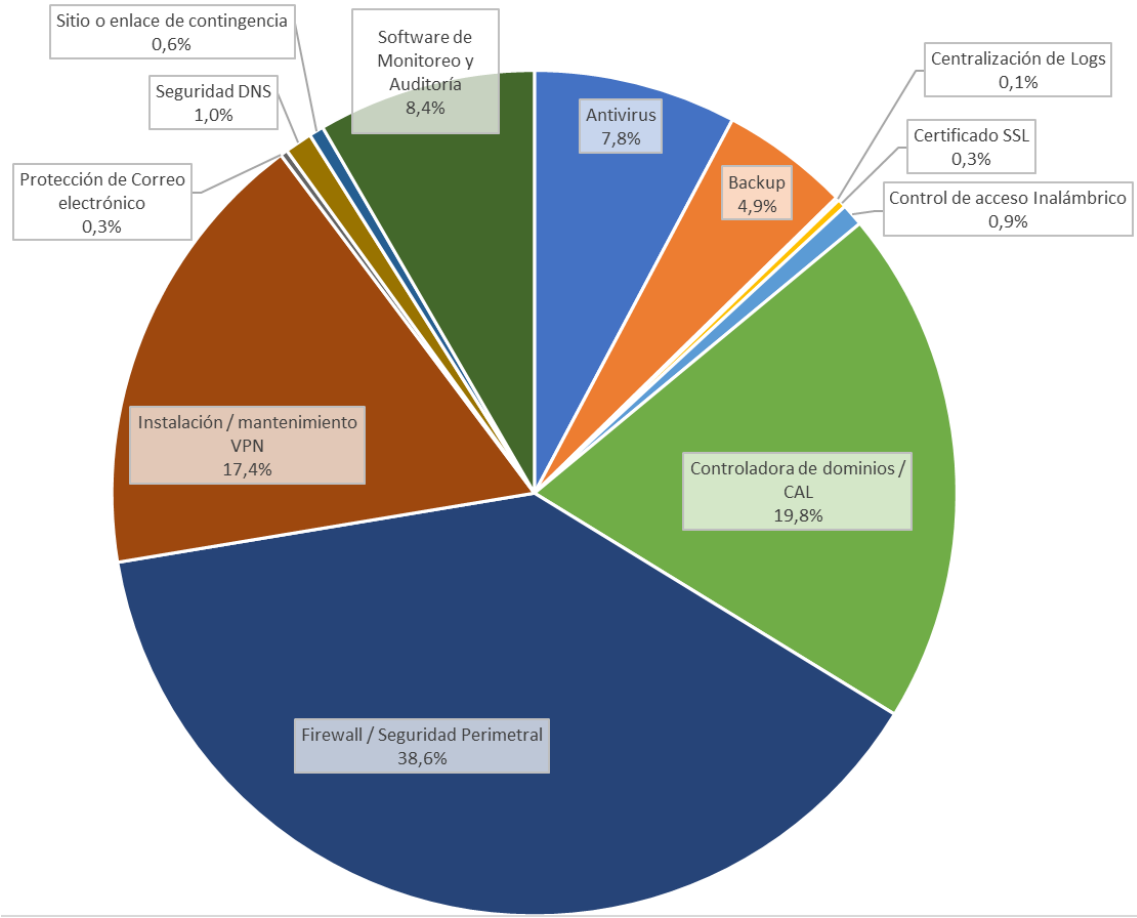


Figura 54. Distribución porcentual de la inversión en ciberseguridad en el 2020 por rubro

Las inversiones han sido realizadas por 57 instituciones únicas, siendo las mayores del Ministerio del Interior (Gs. 8.598.822.236), Banco Central del Paraguay (Gs. 5.420.145.338) y Secretaría del Estado de Tributación (Gs. 4.234.458.941), respectivamente.

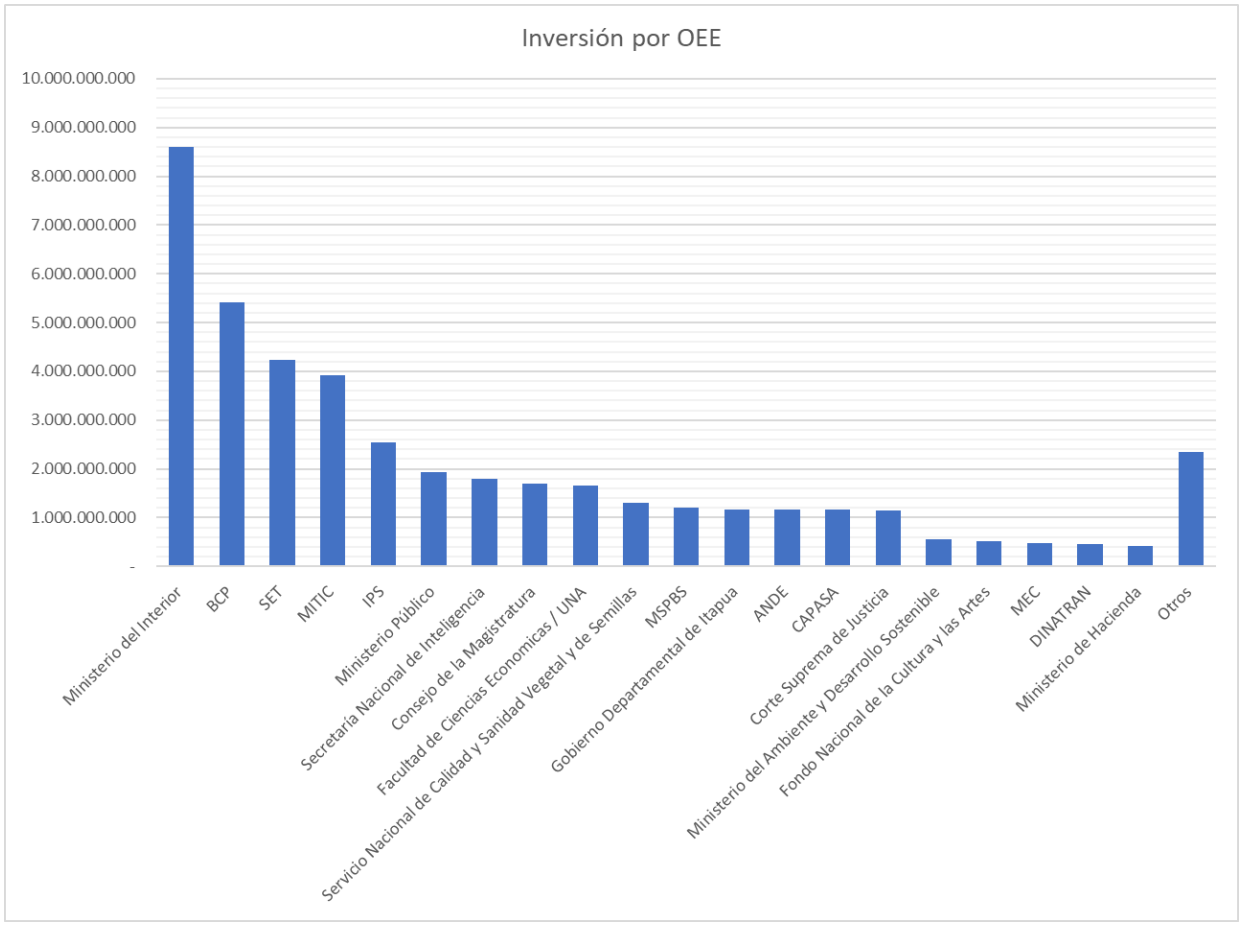


Figura 55. Inversión por OEE en 2020

Recursos humanos

Actualmente, de acuerdo a los datos de la Secretaría de la Función Pública[26], el Estado Paraguayo cuenta con 289.167 funcionarios públicos activos, entre personal permanente y contratado. En las áreas relacionadas a las TIC, se cuenta con **818 funcionarios**, lo cual apenas representa aproximadamente el 0,29% del total de funcionariado. Esto incluye desarrolladores, administradores de redes y sistemas, seguridad informática, soporte técnico y gestión TIC en general.

El salario promedio de los funcionarios de áreas de TIC es de **Gs. 7.277.617**, con salarios muy variables entre las diferentes instituciones, que varían desde Gs. 700.000 hasta Gs. 30.804.400.

[26] Información obtenida a través del análisis de los datos abiertos de la SFP al mes de noviembre 2020, obtenidos del sistema SICCA, complementada por las nóminas de funcionarios publicada en formato abierto por OEEs que no reportan al SICCA. Aquellos funcionarios cuya institución hayan indicado incorrecta o incompletamente sus funciones, podrían no verse reflejadas en este análisis

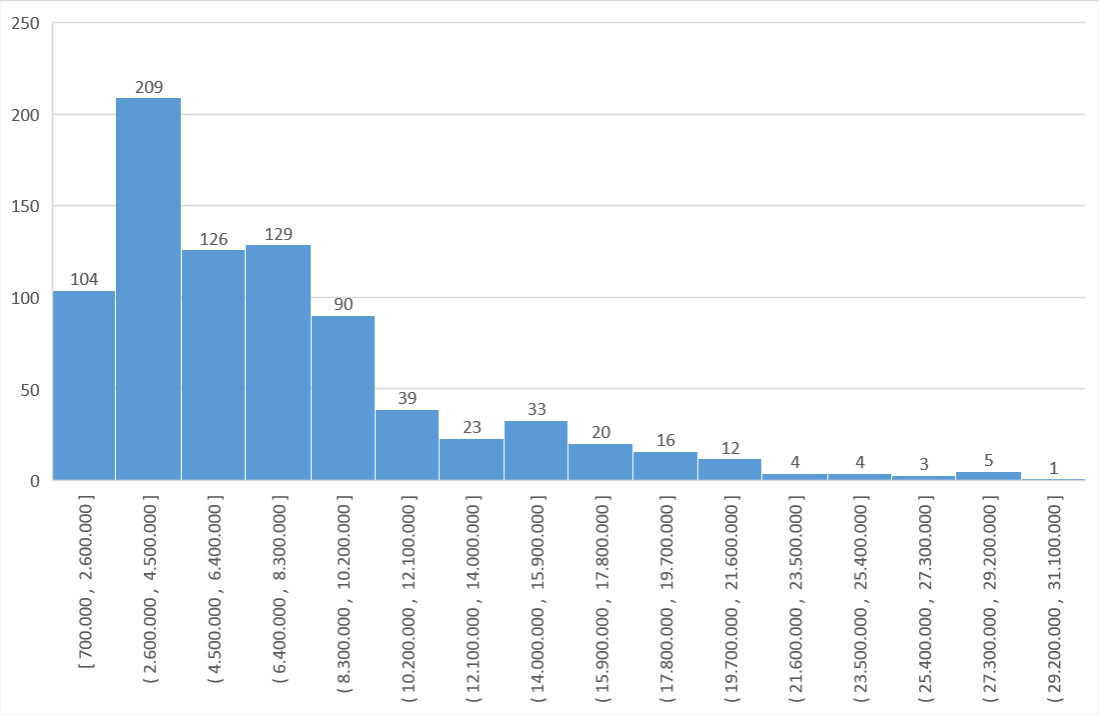


Figura 56. Distribución salarial de cargos relacionados a las TIC en el Estado

En cuanto a la formación académica profesional de los funcionarios designados en funciones relacionadas a las TIC y ciberseguridad, podemos resaltar los siguientes datos:

- Alrededor del 43%[27] tienen formación de nivel terciario relacionados a las TIC (tecnicatura, licenciatura, ingeniería o postgrado afines a las TIC).
- Al menos el 7% de los funcionarios de TIC tiene una formación en carreras no afines a las TIC (contabilidad, derecho, psicología, administración de empresas, etc.).
- Aproximadamente el 1% tiene maestrías afines a las TIC.
- Alrededor del 35% no cuenta con ningún título técnico ni universitario (bachiller y/o estudiantes).

Se observa un mayor porcentaje de funcionarios hombres (81%) frente a las mujeres. El promedio salarial de las mujeres en TIC es de Gs. 7.783.339, ligeramente superior al de los hombres que es Gs. 7.155.599.

En los niveles gerenciales, se puede comprobar que 61 Responsables de Seguridad de la Información (86%) son hombres, frente a 10 mujeres (14%). Como Directores de TIC, se mantiene la proporción, con 80 hombres (85%) y 14 mujeres (15%).

[27] El campo "Profesión" del sistema SICCA no se encuentra estandarizado, por lo que varía el nivel de detalle de información que declaran las instituciones. Títulos que no hayan sido indicados correcta o completamente en dicho sistema podrían no verse reflejados en este análisis.

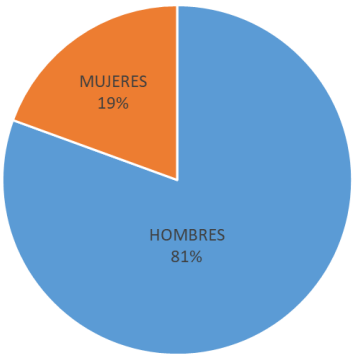


Figura 57. Funcionarios en funciones relacionadas a las TIC por género

La mayoría de las instituciones cuenta con escaso o nulo personal dedicados a las tareas y proyectos de seguridad de la información o ciberseguridad. Esto se refleja en una gran dificultad de llevar adelante las iniciativas, proyectos y tareas operativas requeridas para una adecuada protección de las redes, sistemas y datos del Estado. La amplia mayoría, 57% de las instituciones, no cuenta con ninguna persona que se dedique de manera exclusiva o mayoritariamente a funciones relacionadas a ciberseguridad. El 12% de las instituciones tienen una persona dedicado a ello con dedicación exclusiva o principal; el 11% tiene un equipo de dos personas. Apenas el 3% (4 instituciones) tienen un equipo humano de 3 a 4 personas dedicadas exclusivamente a ciberseguridad o seguridad de la información.

Figura 58. Recursos Humanos con dedicación exclusiva o primaria a tareas de ciberseguridad en OEEs

Del total de 171 OEEs del Estado registrados en la SFP hay, en total, **78 funcionarios** designados a actividades de ciberseguridad, seguridad de la información, seguridad informática y/o auditoría TIC. Cabe destacar que algunos de éstos están designados a estas actividades solo a tiempo parcial; en algunos casos, la designación es solo de carácter formal, sin dedicarse a ello de manera operativa.
El promedio salarial de los funcionarios de ciberseguridad es de **Gs. 8.460.700**.

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 TIC 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.

Desde 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, la segunda edición del año 2020 ha contado con 25 egresados.

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

En el año 2020, el MITIC en alianza con Coursera y la organización ENI - Estrategia Nacional de Innovación, puso a disposición de ciudadanos paraguayos más de 35.000 cupos con inscriptos de 253 ciudades del país, que permite la formación en diversos temas, entre ellos 51 cursos de ciberseguridad, a los cuales 433 alumnos se han inscripto en al menos un curso.

Además en una encuesta realizada a los Responsables de Seguridad de la Información del Estado, se ha visto mayor necesidad de capacitación en los siguientes temas: Gestión de la Seguridad de la Información, Administración segura y protección de sistemas TI (servidores, base de datos, end-point, etc.), Seguridad en redes / networking y Gestión de Incidentes cibernéticos de Ciberseguridad, por lo que el MITIC seguirá realizando los esfuerzos necesarios para cubrir la demanda, en la medida de sus posibilidades.

Las necesidades de formación requeridas por los Responsables de Seguridad de la Información del Estado que tienen mayor demanda son: Gestión de la Seguridad de la Información, Administración segura y protección de sistemas TI (servidores, base de datos, end-point, etc.), Seguridad en redes / networking, Estrategias y técnicas de Concienciación a usuarios, entre otros.

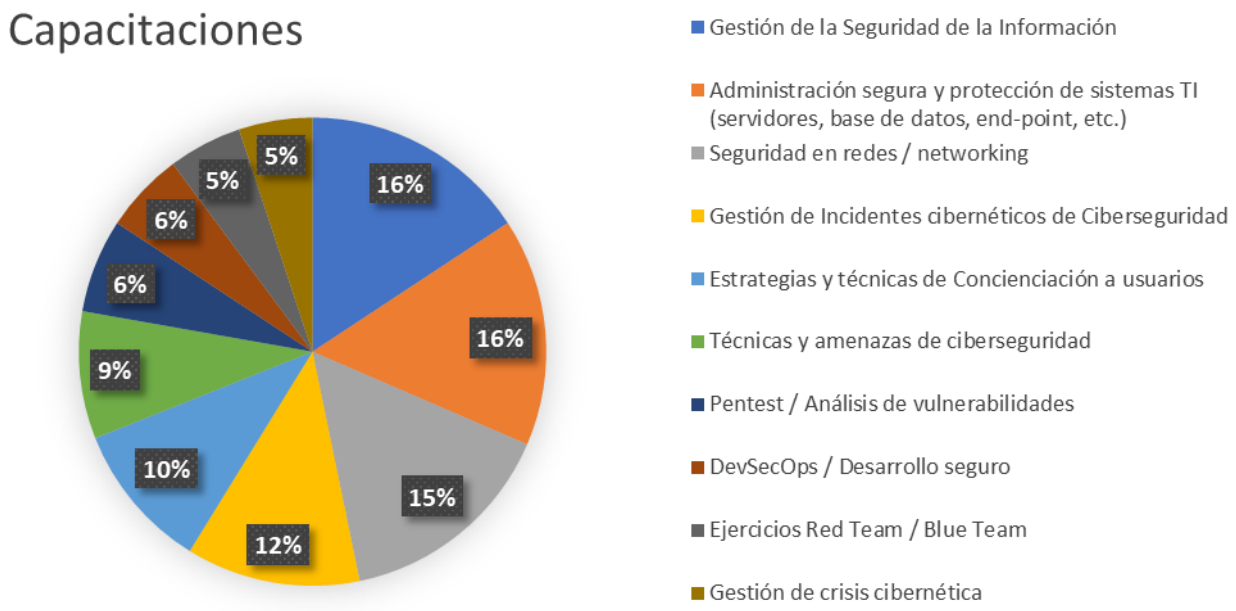


Figura 59. Necesidades de formación específica por parte de los RSI del Estado

Ranking Global y en las Américas en Ciberseguridad

National Cyber Security Index (NCSI)

De acuerdo al **National Cyber Security Index (NCSI),** Paraguay se sitúa actualmente en la posición Nro. 39 a nivel internacional, y en 2° lugar en Latinoamérica, precedido únicamente por Chile, alcanzando un cumplimiento del 57%.

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 60. Posicionamiento de Paraguay en el ranking NCSI

Actualmente, el índice abarca un total de 160 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.

Las principales debilidades, de acuerdo a este índice en la última edición, 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 (25%), así como también la capacidad de gestión y análisis de información de amenazas (20% de cumplimiento). 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).

Respecto al año anterior, se ha observado una mejoría en cuanto al análisis e información de amenazas cibernéticas que aumentó debido a que desde noviembre de 2019 se mejoró la sistematización de datos, métricas y estadísticas de amenazas e incidentes del CERT-PY, lo cual, entre otras cosas, posibilitó la generación del presente informe anual, así como su incorporación mediante el servicio de alertas de amenazas tempranas.

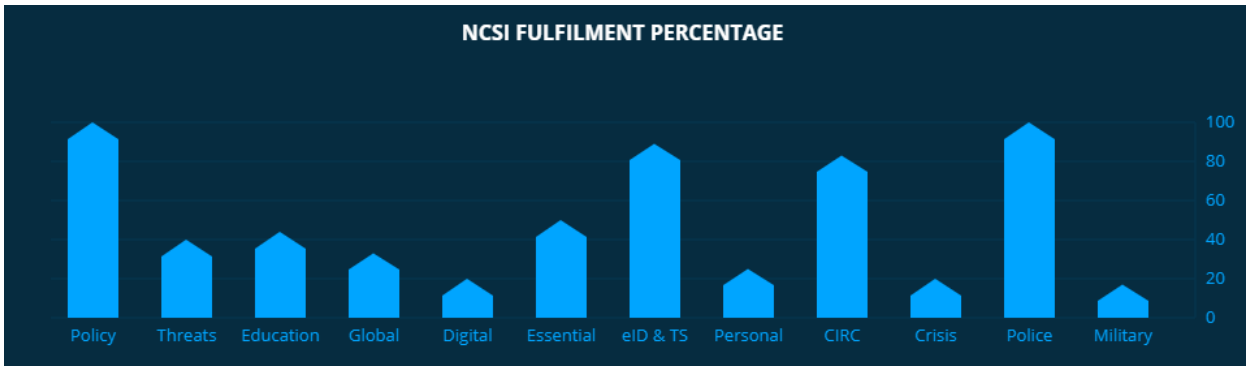
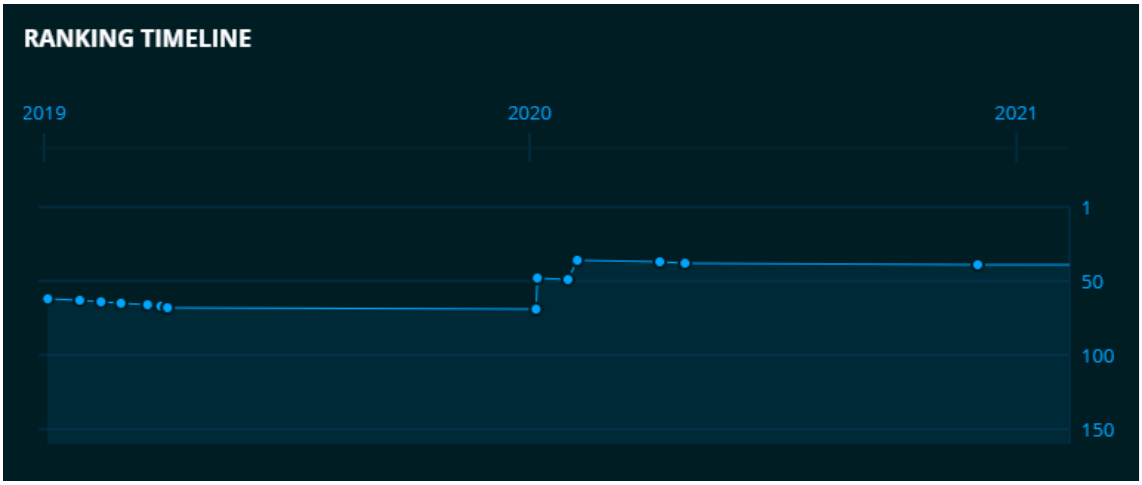


Figura 61. Nivel de cumplmiento de indicadores de NCSI por área

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.



Global Cybersecurity Index (GCI)

Es otro estudio reconocido en el ámbito, el Global Cybersecurity Index (GCI), 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, por lo que no hay variación de la posición de Paraguay respecto al año pasado. La información para este estudio es proveída por parte de Conatel, organismo representante de Paraguay ante la ITU.

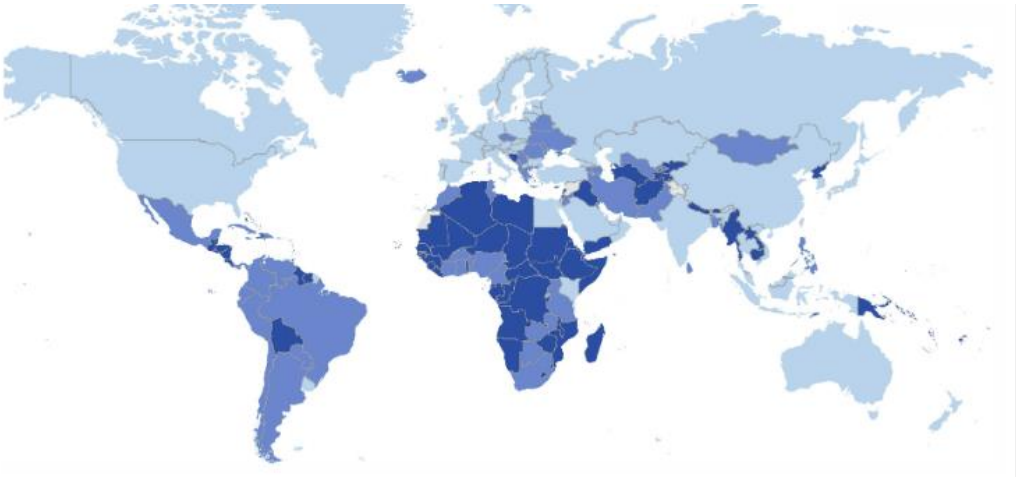


Figura 62. Comparación de países - GCI 2018

Informe "Ciberseguridad: Riesgos, Avances y el Camino a seguir en América Latina y el Caribe"

Este reporte es la segunda edición del año 2020 de una publicación exclusiva desarrollada a partir de un modelo del Centro de Seguridad de la Universidad de Oxford (Global Cyber Security Capacity Centre (GCSCC)). El informe contiene datos relevantes sobre las diferentes dimensiones del estado de ciberseguridad de 32 Estados Miembros de la OEA, y muestra los avances logrados por la región en materia de ciberseguridad.

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.

El Modelo de Madurez de la Capacidad de Ciberseguridad (CMM, por sus siglas en inglés) de las naciones, corresponden a aspectos esenciales y específicos de la ciberseguridad y se mide en 5 dimensiones:

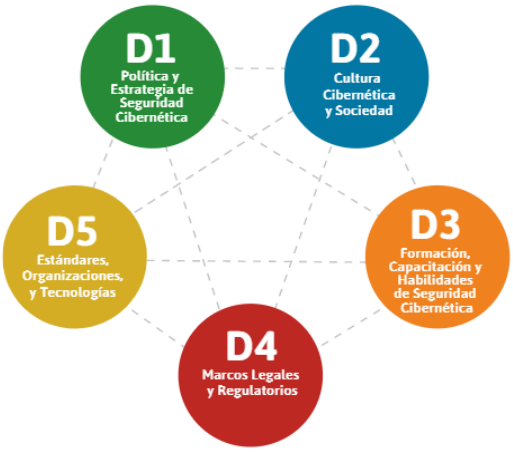
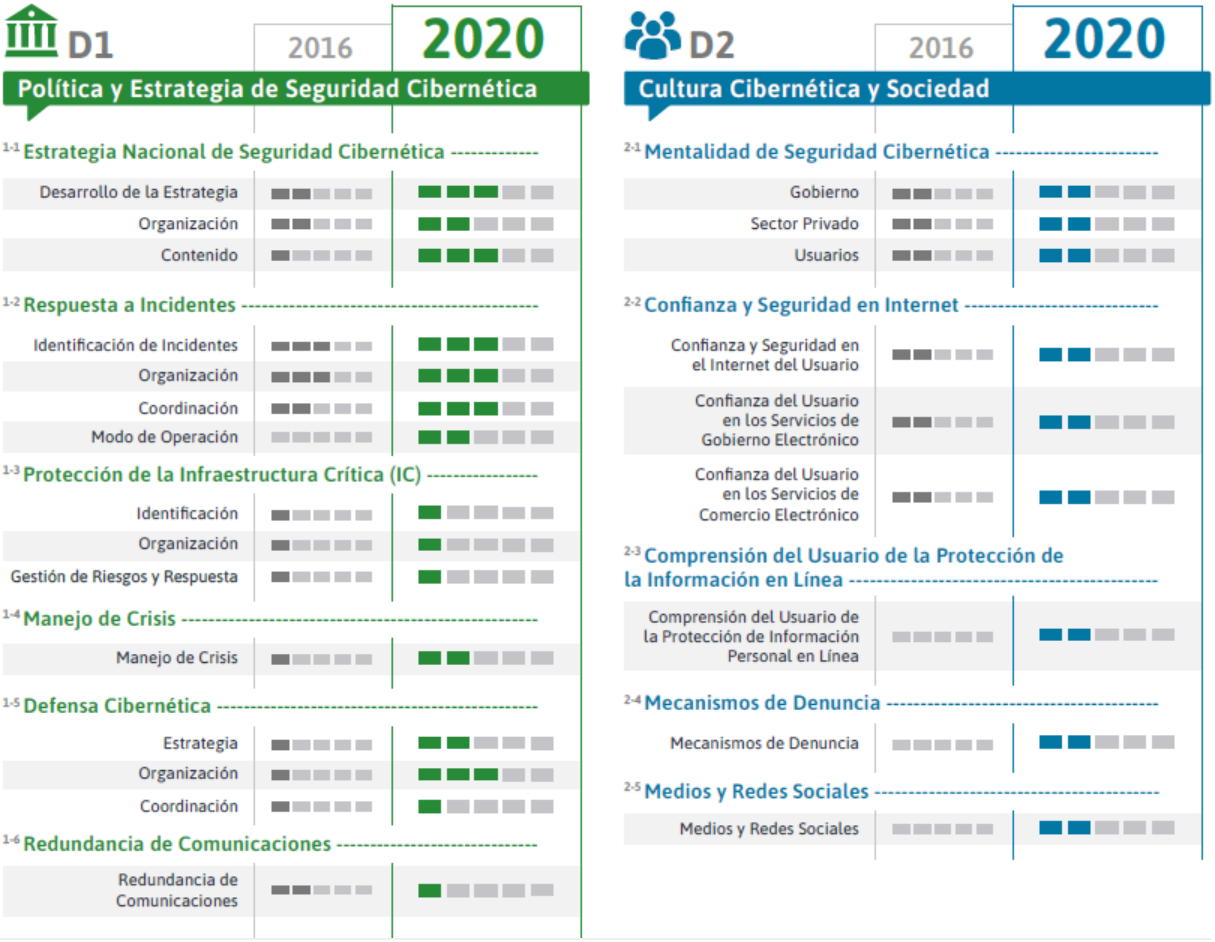


Gráfico 2: Las cinco dimensiones del CMM

En el último estudio, el perfil de Paraguay respecto a la preparación en materia de ciberseguridad ha sido el siguiente:




D3
2016
2020
Formación, Capacitación y Habilidades de Seguridad Cibernética
3-1 Sensibilización
Programas de Sensibilización
Sensibilización Ejecutiva
3-2 Marco para la Formación
Provisión
Administración
3-3 Marco para la Capacitación Profesional
Provisión
Apropiación
D4
2016
2020
Marcos Legales y Regulatorios
4-1 Marcos Legales
Marcos Legislativos para la Seguridad de las TIC
Privacidad, Libertad de Expresión y Otros Derechos Humanos en Línea
Legislación Sobre Protección de Datos
Protección Infantil en Línea
Legislación de Protección al Consumidor
Legislación de Propiedad Intelectual
Legislación Sustantiva Contra el Delito Cibernético
Legislación Procesal Contra el Delito Cibernético
4-2 Sistema de Justicia Penal
Fuerzas del Orden
Enjuiciamiento
Tribunales
4-3 Marcos de Cooperación Formales e Informales para Combatir el Delito Cibernético
Cooperación Formal
Cooperación Informal
D5
2016
2020
Estándares, Organizaciones y Tecnologías
5-1 Cumplimiento de los Estándares
Estándares de Seguridad de las TIC
Estándares en Adquisiciones
Estándares en el Desarrollo de Software
5-2 Resiliencia de la Infraestructura de Internet
Resiliencia de la Infraestructura de Internet
5-3 Calidad del Software
Calidad del Software
5-4 Controles Técnicos de Seguridad
Controles Técnicos de Seguridad
5-5 Controles Criptográficos
Controles Criptográficos
5-6 Mercado de Seguridad Cibernética
Tecnologías de Seguridad Cibernética
Seguro Cibernético
5-7 Divulgación Responsable
Divulgación Responsable

En cuanto a las mejoras respecto al anterior informe, se pueden observar avances en cuanto al Desarrollo y Contenido de Estrategias Nacionales de Seguridad Cibernética y Marco Legal, además de ser agregados aspectos nuevos en la medición, en los cuales Paraguay tiene debilidades como Mecanismos de Denuncias y Medios y Redes Sociales, Calidad de Software, Controles Técnicos de Seguridad, Cumplimiento de estándares, Controles Criptográficos, entre otros.