CERT-PY

ESTADO de la CIBERSEGURIDAD en PARAGUAY

Año 2022

Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

GOBIERNO NACIONAL

Paraguay de la gente

Tabla de Contenido

Introducción

Este informe presenta el estado de la ciberseguridad en el Paraguay en el año 2022, 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 2022, 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 de ciberseguridad, 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.

Además se incluye información estadística acerca de los Delitos Informáticos reportados durante los años 2021 y 2022 al Ministerio Público.

Términos

CERT-PY: Centro de Respuestas ante Incidentes Cibernéticos.

MITIC: Ministerio de Tecnologías de la Información y Comunicación.

OEE: Organismos y Entidades del Estado.

RSI: Responsable de Seguridad de la Información.

SFP: Secretaría de la Función Pública.

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).

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.

- **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 en 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, DP 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).

- **Ransomware:** Según CISA "es una forma de malware en constante evolución diseñada para cifrar archivos en un dispositivo, inutilizando cualquier archivo y los sistemas que dependen de ellos. Luego, los actores malintencionados exigen un rescate a cambio del descifrado". Los actores de ransomware a menudo amenazan con vender o filtrar datos extraídos o información de autenticación si no se paga el rescate.[OBJ]

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 2022

A continuación, se presentan estadísticas obtenidas a partir de los incidentes cibernéticos reportados y gestionados a través del servicio de gestión de incidentes cibernéticos del año 2022, desde el 01/01/2022, hasta el 31/12/2022. Estos, 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:** 3668
- **Cantidad total de Incidentes atendidos:** 2083
- **Investigaciones realizadas:** 6290

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 717 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, Avalanche, este año también vimos presencia de la botnet Hajime. Los problemas de configuración y ataques de ransomware son los menos reportados e investigados, con un total de 16 y 7 incidentes respectivamente, con respecto año anterior tuvimos un ligero aumento el número de casos de ransomware. También tenemos 0 incidentes relacionados con ataques de DoS/DDoS, 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, 15 incidentes relacionados con acceso indebido a cuentas/sistemas/datos, 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.

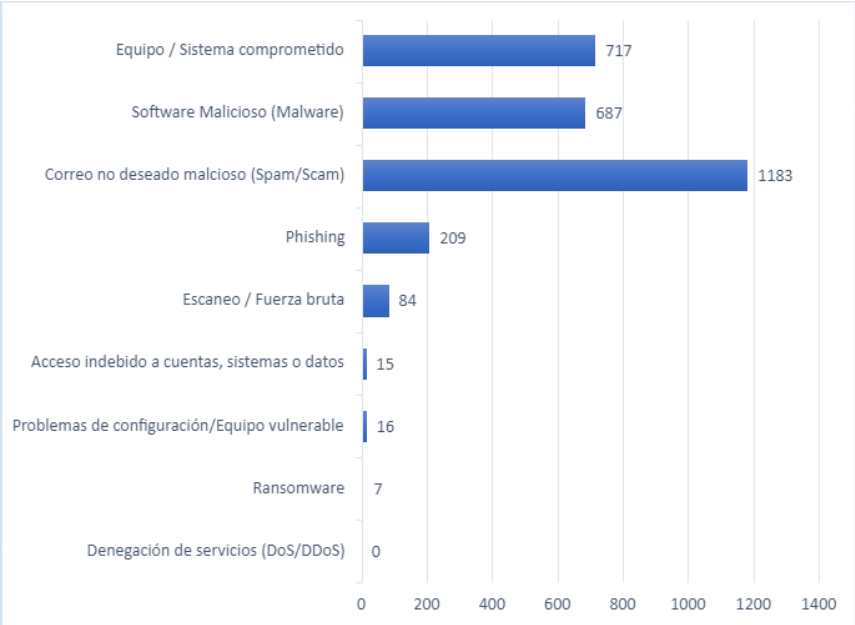


Figura 2. Cantidad de incidentes cibernéticos reportados en el año 2022, categorizados por tipo de incidentes

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: 105 incidentes
- Privado: 702 incidentes
- Extranjero: 1266 incidentes
- Ciudadano: 22 incidentes
- Educativo: 4 incidentes

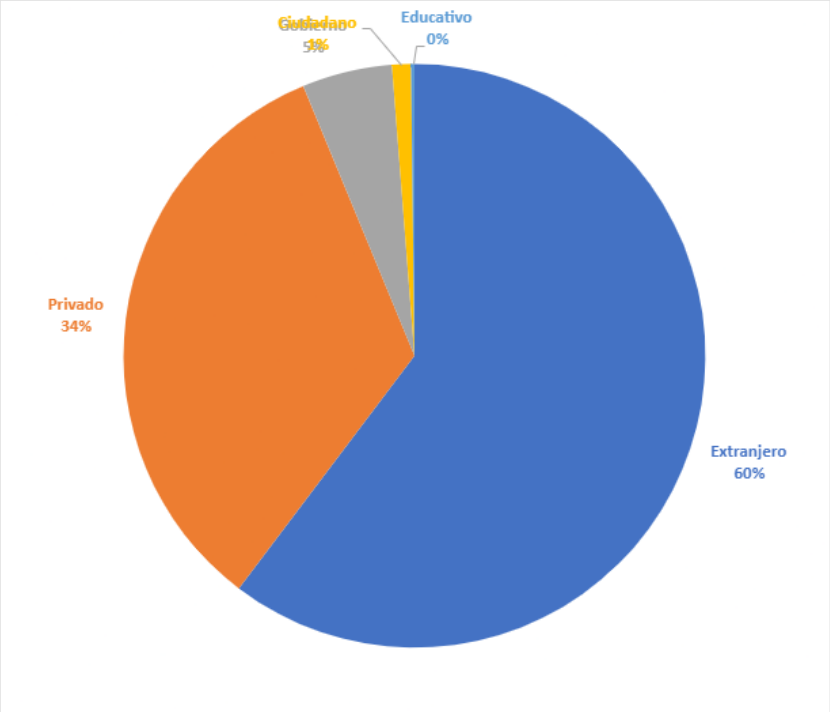


Figura 3. Cantidad de Incidentes por tipo de afectado

La mayoría de incidentes cibernéticos provienen desde el extranjero, durante el año 2022 se contabilizaron 1266 reportes, en cuanto a nivel nacional los incidentes que afectan a sistemas o redes de empresas privadas, con un total de 702 incidentes. Sin embargo, el número de incidentes relacionados a redes o sistemas de instituciones de gobierno o de ciudadanos mantiene su tendencia con respecto a años anteriores en inferior cantidad. Esta tendencia se mantiene al del año pasado. 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 percibe que muchos ciudadanos e incluso profesionales independientes no conocen este servicio y/o no lo utilizan, en comparación con años anteriores se mantiene un ratio de escasa cantidad de incidentes del sector ciudadano reportados, lo cual se podría dar por diversas razones:

- Los hogares, los profesionales independientes e incluso las PYMES, carecen de mecanismos de detección de incidentes, por lo que no se enteran de los mismos;
- Los hogares, PYMES 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;

- Los afectados por incidentes cibernéticos consideran innecesario o no rentable invertir en la investigación, resolución y prevención de los incidentes, por lo que optan por no reportarlo.
- A nivel de gobierno podemos remarcar que muchas instituciones públicas no cuentan con equipos TICs propios y/o encargados de seguridad de la información.

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 sensibles).
  - 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 2022 se han reportado 8 incidentes de criticidad alta (2%), 252 incidentes de criticidad media (12%) y 1823 incidentes de criticidad baja (88%).

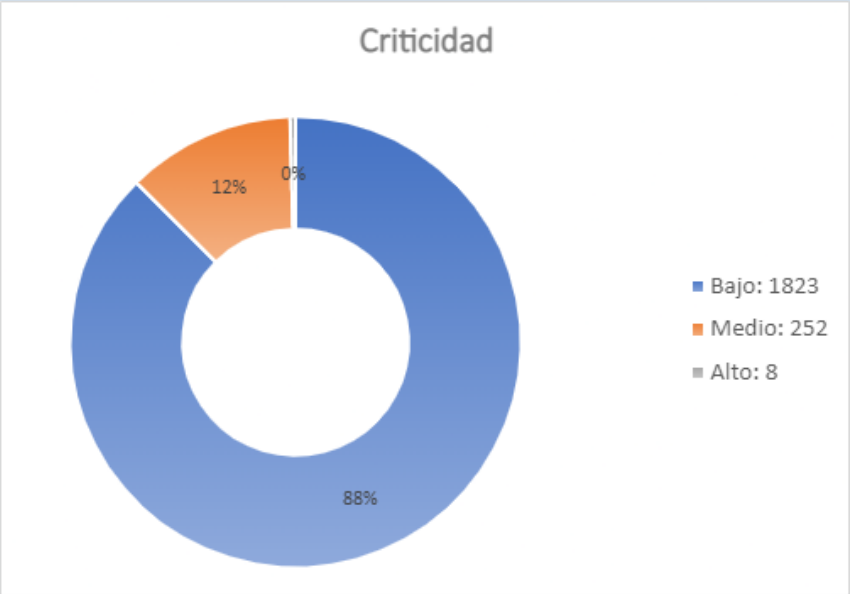


Figura 4. Clasificación de los incidentes por criticidad año 2022

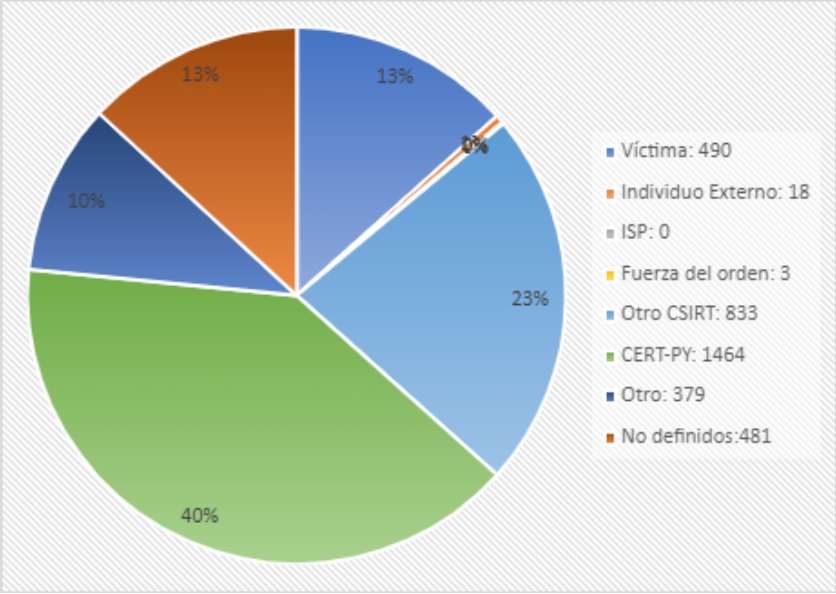


Figura 5. Reportes de incidentes por tipo de denunciante durante el año 2022

En el gráfico figura 5, observamos que la mayoría de los reportes son generados por el CERT-PY con el 40% y por otros equipos de respuesta a incidentes cibernéticos (CSIRTs) con el 23%. Comparando con otros años se incrementa el porcentaje de reportes generados por el CERT-PY

y disminuye el porcentaje de reportes enviados desde CSIRTs externos, dicho comportamiento se marca debido al aumento de la proactividad. También acrecienta esta situación el hecho de que los CSIRTs extranjeros y el CERT-PY 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 3668 reportes de incidentes cibernéticos, 2756 de ellos se han resuelto esto representa al 75%. En relación a años anteriores el porcentaje de resolución mantenía en una leve mejoría porcentual, el año 2022 disminuyó el porcentaje de incidentes resueltos a pesar de que en cantidad aumentó el número de incidentes. El número de reportes rechazados se incrementó, por diversos motivos, situación distinta frente a los años anteriores.

	Reportes Recibidos
Rechazados:	912
Resueltos:	2756
Total	**3668**

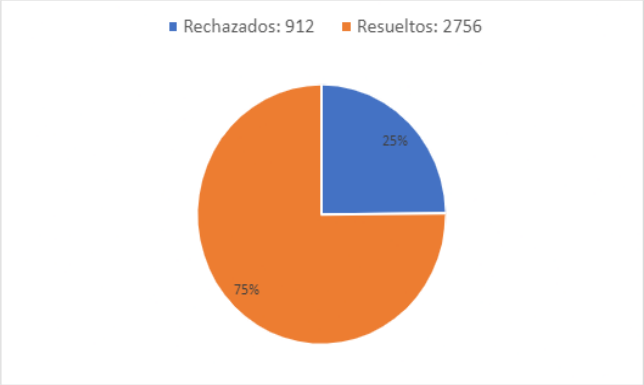


Figura 6. Reportes Recibidos

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

- Reportes que no corresponden a un incidente cibernético
- Reportes falsos, provenientes de cuentas de spam publicitario
- Respuestas por parte de sistemas, 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 2083 incidentes únicos gestionados, 2057 (99%) se han resuelto. Solamente el 1% ha sido abandonado. Este porcentaje se mantiene igual que en años anteriores pero con un mayor número de incidentes manejados.

	Incidentes Únicos
Rechazados:	26
Resueltos:	2057
Total	**2083**

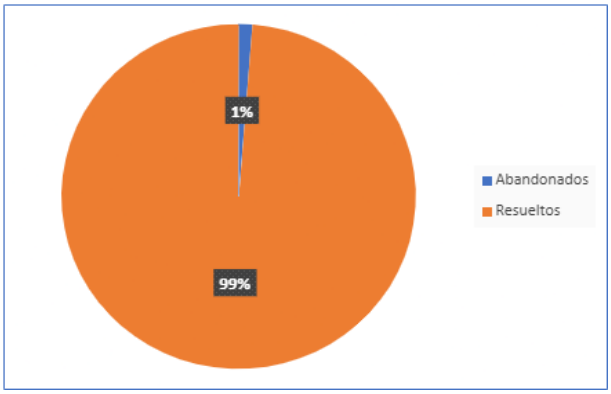


Figura 7. Incidentes Únicos

En el año 2022, la mayor cantidad de reportes se ha recibido en el mes de agosto, con un pico de 375 reportes, seguido del mes de junio, con 369 reportes, en comparación con otros años donde el mes de abril poseía tendencia a ser el más del pico de reportes, el año 2022 corresponde al mes de agosto. El menor número de incidentes se ha recibido en el mes de enero.

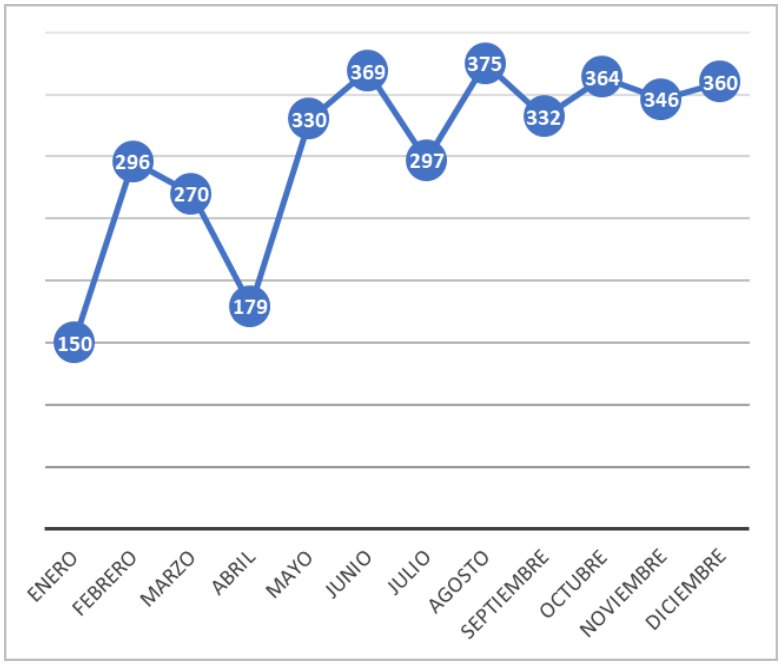


Figura 8. Cantidad de reportes de incidentes cibernéticos por mes del año

La mayor cantidad de reportes de incidentes cibernéticos se recibieron los días martes y miércoles, en los que se ha recibido un total de 645 y 651 reportes respectivamente, con un decrecimiento gradual durante la semana, hasta un mínimo los sábados y domingo, con 327 y 315 reportes respectivamente. Esta tendencia se ha incrementado con respecto al año anterior y también a otros años.

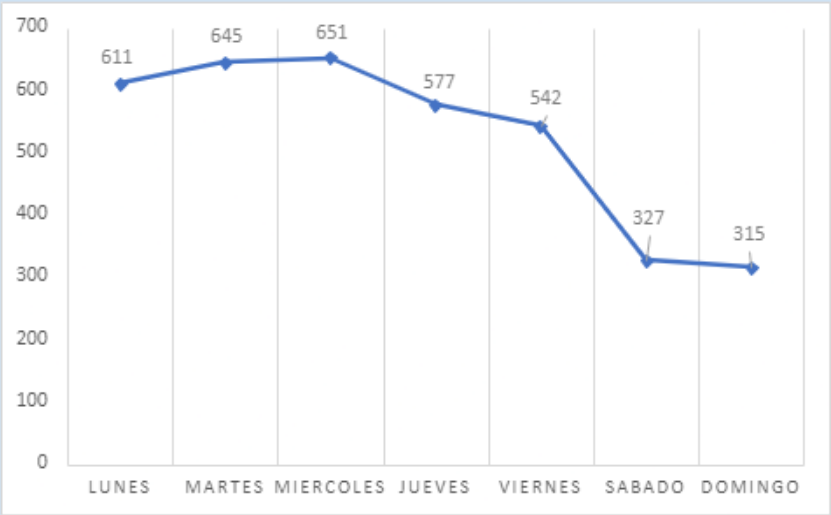


Figura 9. Cantidad de reportes de incidentes cibernéticos por día de la semana

En la siguiente figura se puede observar una mejora del tiempo promedio de atención de los reportes durante todo el año con respecto al 2022, este año hemos bajado el tiempo de atención a menos de 24 horas en casi todo los meses. Vemos el pico de atención de 91 horas en el mes de noviembre y la omisión de tiempo de atención del mes de octubre, todo esto debido a los problemas de sistemas e infraestructura que hemos tenido durante el mes de octubre.

Figura 10. Evolución del tiempo promedio de atención de reportes en el año 2022 (mensual)

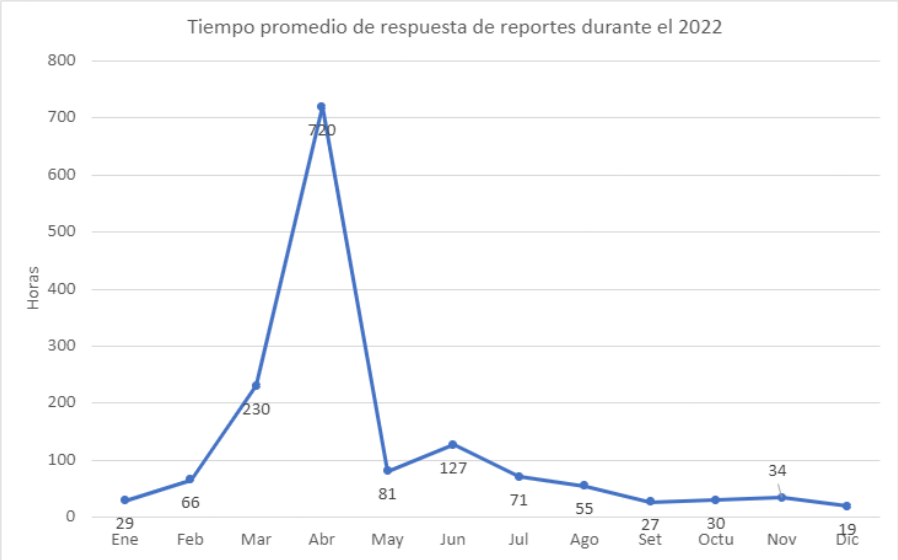


Figura 11. Evolución del tiempo promedio de atención o respuesta de reportes en el año 2022 (mensual)

Incidentes resaltantes

A lo largo del año 2022 se ha observado en mayormente la explotación de vulnerabilidades ya sea para ataques de ransomware, explotación de vulnerabilidades conocidas, compromiso de sistemas y el aumento del phishing dirigido al sistema financiero.

A inicios del 2022 durante el mes de enero, realizamos una tarea proactiva que consiste en alertar, emitir un boletín la explotación de una mala configuración en manejadores de contenido, en la cual se generaban resultados de búsquedas con contenido del tipo spam. Procedimos a realizar una operación en búsqueda de sitios web afectados vulnerables dentro del territorio paraguayo. Contactamos con alrededor de 39 entidades cuyos sitios web se encontraban vulnerables.

El CERT-PY ha gestionado un incidente relacionado con una debilidad en una aplicación web que permitía a un actor malicioso, realizar consultas masivas a dicha aplicación, que le permitiría recolectar información de la misma.

Iniciamos el enero alertando sobre con boletines de seguridad relacionados con productos de Microsoft entre las más destacables el error Y2K22, los parches de parche de seguridad para las

vulnerabilidad CVE-2022-21907 que permite la ejecución remota de código a través del protocolo HTTP en microsoft y CVE-2022-21893 que permite la ejecución remota de código en protocolo RDP, a continuación sus respectivos enlaces:

- https://www.cert.gov.py/wp-content/uploads/2022/02/BOL-CERT-PY-2022-02_Vulnerabilidad_en_protocolo_HTTP_de_Windows.pdf
- https://www.cert.gov.py/wp-content/uploads/2022/02/BOL-CERT-PY-2022-01_Microsoft_lanza_una_solucion_de_emergencia_para_el_error_del_ano_2022.pdf
- https://www.cert.gov.py/wp-content/uploads/2022/02/BOL-CERT-PY-2022-04__RCE_en_RDP_de_Windows_CVE-2022-21893-TS01.pdf

Durante el mes de febrero el CERT-PY colaboró con una investigación sobre los privilegios y accesos del sistema de seguimiento de órdenes de captura de la Policía Nacional, validando el comportamiento realizado por los operadores del sistema. Se verificaron los niveles de acceso al sistema. Se entregaron las debidas recomendaciones para el mejoramiento de la protección de la información a los responsables de la institución.

- https://www.ultimahora.com/cambiaron-delito-orden-captura-presunto-narco-herido-n2984610
- https://www.ultimahora.com/policia-que-borro-orden-captura-presunto-narco-dice-que-fue-un-error-n2984456

También durante el mes de febrero realizamos varias alertas sobre vulnerabilidades este mes, mayormente orientado a software o productos de origen opensource como Zimbra ampliamente utilizada en el gobierno y organizaciones, Zabbix, el servicio Samba con sus respectivos boletines de seguridad

- https://www.cert.gov.py/wp-content/uploads/2022/02/BOL-CERT-PY-2022-07_Multiples_vulnerabilidades_en_Samba.pdf
- https://www.cert.gov.py/wp-content/uploads/2022/03/BOL-CERT-PY-2022-10_Multiples_vulnerabilidades_detectadas_en_Zabbix_Web_Frontend.pdf
- https://www.cert.gov.py/wp-content/uploads/2022/02/BOL-CERT-PY-2022-08_Vulnerabilidad_de_Cross-Site_Scripting_XSS_en_Zimbra_8.8.15.pdf

En el mes de Agosto el CERT-PY ha gestionado 2 incidentes de ransomware que han afectado a 2 organizaciones paraguayas, una de ellas del sector público y otra del sector privado, estos incidentes han causado la paralización de sus operaciones completamente por al menos 4 días, estas organizaciones se enfrentaron al ransomware Hive V4 y V5, entre otros eventos de ransomware que han ocurrido de forma aislada.

Durante el transcurso de los meses posteriores, han sido reportado al CERT-PY múltiples incidentes relacionados con estafas financieras llevadas a cabo a través de técnicas de phishing dirigido a clientes de entidades financieras, se ha elaborado una investigación en la cual se ha documentado el mecanismo de robo de las credenciales de las víctimas y la infraestructura digital empleada por los delincuentes para sus campañas de estafa. Lo que llamó la atención fue que los delincuentes utilizaban publicidades de Google o Google Ads para propagar sus enlaces de phishings, además de correos de SPAM. Una vez que los clientes del/los banco/s afectados accedían a estos sitios de phishing e ingresaban sus credenciales bancarias en los formularios maliciosos esta información era enviada a canales de Telegram manejados por los ciberdelincuentes. Toda esta información obtenida en el marco de nuestra investigación se ha comunicado al departamento de Cibercrimen de la Policía Nacional.

Durante el transcurso del año se han reportado varias vulnerabilidades para el servidor de correo Zimbra y Microsoft Exchange. El servidor de correo Zimbra ha sido objetivo recurrente para incidentes cibernéticos relacionados con la explotación activa de vulnerabilidades como CVE-2022-41352, CVE-2022-27925, CVE-2022-30333, CVE-2022-27924 entre las más explotadas por actores maliciosos, derivando inclusive en filtraciones masivas en países de la región latinoamericana.

También el servidor de correos Microsoft Exchange no se libró de vulnerabilidades críticas, muchas de ellas explotadas en campañas de ataques por Ransomware. CERT-PY ha informado a través de su servicio de boletines de seguridad, sobre vulnerabilidades del tipo Día-0 (Zero-Day) con el boletín BOL-CERT-PY-2022-38. El dicho boletín se alertaba de la explotación de 2 vulnerabilidades de forma combinada se podría lograr la ejecución remota de código en el activo vulnerable. El CERT-PY además de alertar por correo electrónico del caso, procedió a realizar una operación proactiva para identificar la mayoría de activos (servidores de correos MS Exchange) posibles dentro del ecosistema paraguayo a través de nuestras fuentes de información abierta. El detalle de las operaciones realizadas incluidas la operación sobre Microsoft Exchange la explicamos en la sección Operaciones.

Durante el mes de Octubre recibimos reportes de ataques realizados por la banda hacktivista Guacamaya que afectaron principalmente al servidor de correos Zimbra. Se explotaron principalmente las siguientes vulnerabilidades [1]:

- CVE-2022-37042, para evitar los requerimientos administrativos
- CVE-2022-27925, para acceder a recursos sin autenticación necesaria a través de problemas en el path del mismo (Authenticated path-traversal)
- CVE-2022-27924, escalación de privilegios.

Entre los documentos filtrados por este grupo se reportaron supuestos documentos de una OEE del gobierno de México llamada Secretaría de la Defensa Nacional (Sedena).

Cerrando el mes de Octubre una telefónica paraguaya reportó un ataque a su infraestructura digital que paralizó gran parte de su operativa, principalmente a su servicio de billetera digital. Pasarón varios días para poner todos su servicios en línea nuevamente. El incidente en cuestión además de afectar a la telefónica también afectó a miles de ciudadanos paraguayos que se vieron imposibilitados de retirar o enviar dinero por sus canales además de otros problemas con sus servicios[2] [3].

[1] https://www.eleconomista.com.mx/tecnologia/Varios-hackers-ya-habian-infectado-a-la-Sedena-antes-de-Guacamaya-20221003-0070.html#
[2] https://www.revistaplus.com.py/2022/11/01/personal-paraguay-sufre-ataque-a-sus-sistemas-informaticos/
[3] https://www.hoy.com.py/nacionales/ciberataque-a-empresa-telefonica-impide-a-miles-utilizar-sus-billeteras-electronicas

personal | flow

Personal Informa:

Que, hemos sufrido un ataque malintencionado por parte de personas inescrupulosas a nuestro sistema informático.

Que, gracias a los procedimientos de prevención, los servicios continúan operativos y aunque hay afectaciones, éstas son mínimas.

Que, en ningún momento han dejado de funcionar los principales servicios como internet, telefonía móvil y flow gracias a los sistemas de seguridad de la compañía.

Que, funcionarios de nuestra empresa trabajan intensamente sobre la red interna, en la certeza que serán reestablecidos en la brevedad.

Que nuestros canales de comunicación en redes sociales se encuentran a disposición para canalizar consultas, ya que el call center es uno de los sistemas afectados.

Seguimos trabajando para garantizar la calidad de servicio.

Agradecemos su comprensión.

SÁBADO, 29 DE OCTUBRE DE 2022
© REVISTA PLUS RESEARCH

Figura 12. Notificación del 29/10/2022 proveída por la telefónica sobre el incidente en cuestión

personal | flow

Personal Envíos S.A Informa:

Que a raíz del ataque malintencionado, que ya fuera informado con anterioridad, seguimos trabajando para reestablecer los servicios afectados.

Que la plataforma de Billetera Personal fue aislada del incidente de manera proactiva a fin de evitar cualquier riesgo de afectación a la integridad de los datos y de los fondos que se encuentran depositados en las cuentas de dinero electrónico, por lo que aclaramos que NO existe ninguna pérdida de fondos depositados.

Que todos los saldos de las billeteras electrónicas están 100% garantizados mediante el depósito de dichos saldos en una cuenta de fideicomiso abierta en una entidad financiera y cuyos beneficiarios son cada uno de los titulares de cuenta de dinero electrónico.

Que colaboradores de la empresa trabajan intensamente sobre la red, en la certeza que serán reestablecidos durante las próximas horas.

Pedimos disculpas ante todos los inconvenientes ocasionados.

MARTES, 1 DE NOVIEMBRE DE 2022
© REVISTA PLUS RESEARCH

Figura 13. Notificación del 1/11/2022 proveída por la telefónica sobre el incidente en cuestión

Operaciones

El CERT-PY también realiza campañas preventivas o proactivas de contacto a instituciones cuyos servicios online hayan sido reportados o hayamos detectado como vulnerables, o que estén en peligro inminente de un incidente cibernético, por ejemplo cuando encontramos problemas de servicios mal configurados y/o peligro de exposición de datos u otros. Utilizando fuentes abiertas como Shodan, reportes de Shadow Server e información de contactos de dominio

Durante el año 2022, hemos realizados campañas de contactos para:

- Problema Configuración - SPAM bot abuse en sitios web
    - Hemos alertado a las organizaciones afectadas que Bots de SPAM están explotando una mala configuración presente en varios sitios web, específicamente se trata del buscador interno de cada página web, para indexar al buscador de Google enlaces maliciosos
    - Hemos creado una guía al respecto, para evitar el inconveniente:
        - https://www.cert.gov.py/application/files/7816/4330/8170/GUIA-Contra-SPAM-en-WordPress.pdf
    - La cantidad de organizaciones alertas vulnerables al respecto fueron de 19 organizaciones todas públicas
- Revocación de Certificados TLS/SSL para Let's Encrypt
    - Hemos alertado a Instituciones públicas y/o de gobierno, privadas sobre la revocación programada de certificados de raíz del proveedor Let's Encrypt, que afectaría a millones de certificados firmados, lo cual una vez revocado el certificado los certificados TLS/SSL utilizados para realizar conexiones seguras se verían afectados
    - Hemos creado varias noticias alertando sobre el hecho, antes de que ocurra y luego
        - https://www.cert.gov.py/noticias/lets-encrypt-comenzara-a-revocar-ciertos-certificados-ssl-tls/
        - https://www.cert.gov.py/noticias/lets-encrypt-revoca-mas-de-3-millones-de-certificados-debido-a-un-error-en-su-ca/

- La cantidad de organizaciones alertadas que eran vulnerables es de 39 entre instituciones públicas y privadas

- Vulnerabilidad en el servidor de correo Zimbra:
  - CVE-2022-24682: Hemos alertado a varias organizaciones sobre una vulnerabilidad, , que comienza con una serie de correos electrónicos de phishing dirigidos (spear phishing) e incluyen la explotación de la vulnerabilidad llamada Cross-Site Scripting (XSS). Donde la explotación exitosa de esta vulnerabilidad permitiría a un atacante ejecutar JavaScript arbitrario en sesión activa de Zimbra del usuario
  - Al respecto hemos elaborado una un boletín de seguridad:
    - https://www.cert.gov.py/application/files/9716/4400/2554/BOL-CERT-PY-2022-08_Vulnerabilidad_de_Cross-Site_Scripting_XSS_en_Zimbra_8.8.15.pdf
  - La cantidad de organizaciones alertadas con la vulnerabilidad presente fue de 34, todas públicas
- Vulnerabilidad detectada en Plugin de Wordpress ECWID:
  - CVE-2022-2432: Esta vulnerabilidad se debe a una incorrecta validación de datos de entrada a través de la función, La explotación exitosa de esta vulnerabilidad permitiría a un atacante realizar Cross-Site Request Forgery (CSRF) y modificar el ecwid_store_id, que identifica de manera única la tienda.
    - Al respecto hemos elaborado un elaborado un boletin de seguridad https://www.cert.gov.py/wp-content/uploads/2022/08/BOL-CERT-PY-2022-33-Vulnerabilidad-de-cross-site-request-forgery-detectada-en-plugin-de-WordPress.pdf
  - La cantidad de organizaciones alertadas vulnerables al plugin 32 instituciones privadas
- Vulnerabilidad de Día-0 (Zero-Day), en servidores de correo Microsoft Exchange:
  - ProxyNotShell es el conjunto de dos vulnerabilidades de seguridad (CVE-2022-41082, CVE-2022-41040) que afectan a Microsoft Exchange Server que permitirían a un atacante remoto realizar ataques del tipo server-side request forgery (SSRF) y ejecución remota de código (RCE)
    - Al respecto hemos elaborado un boletín de seguridad https://www.cert.gov.py/wp-content/uploads/2022/09/BOL-CERT-PY-2022-38-Vulnerabilidades-de-dia-cero-en-Microsoft-Exchange-Server.pdf

- Han sido alertados en esta operación 74 organizaciones entre privadas y públicas
- Sistemas Vulnerables de FortiGate y FortiProxy: hemos alertado a las organizaciones que poseen dispositivos de la marca afectada que se estaban explotando activamente.
  - La vulnerabilidad crítica denominada CVE-2022-40684, la explotación exitosa de dicha vulnerabilidad permitiría a un atacante no autenticado en el equipo realizar operaciones deliberadas en la interfaz administrativa
    - Al respecto hemos elaborado un boletín de seguridad https://www.cert.gov.py/wp-content/uploads/2022/10/BOL-CERT-PY-2022-41-Vulnerabilidad-de-omision-de-autenticacion-en-FortiGate-y-FortiProxy.pdf
  - Hemos alertado en esta operación a un total de 27 organizaciones entre privadas y públicas

En total durante el transcurso del año hemos realizado un total de 6 operaciones proactivas sobre instituciones paraguayas tanto del sector privado y público, en resumen fueron contactados 225 organizaciones

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 31/12/2022.

- Reportes recibidos: 13046
- Incidentes únicos gestionados: 5449
- Investigaciones, coordinaciones y gestiones únicas realizadas: 20270

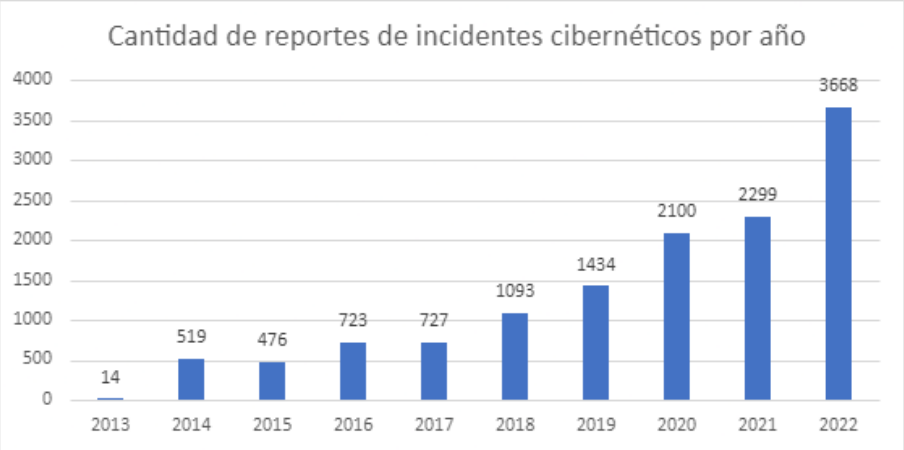


Figura 14. Evolución histórica de cantidad de Reportes de Incidentes cibernéticos recibidos

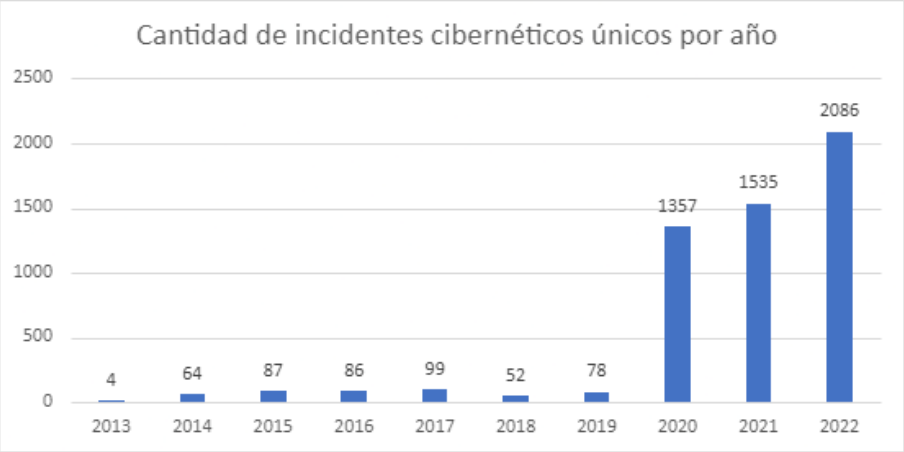


Figura 15. Evolución histórica de cantidad de Incidentes cibernéticos únicos atendidos

Figura 16. Evolución histórica de cantidad de investigaciones, coordinaciones y gestiones únicas realizadas

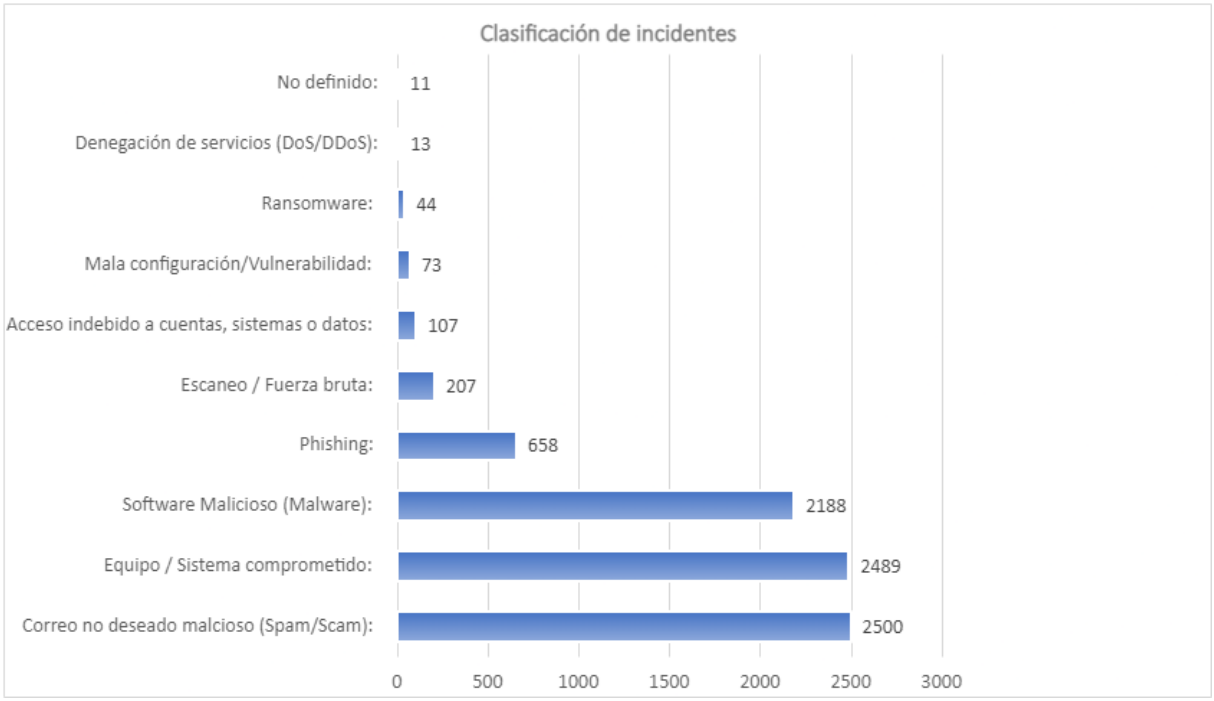


Figura 17. Cantidad histórica de incidentes cibernéticos reportados, categorizados por tipo de incidente. 2013 - 2022

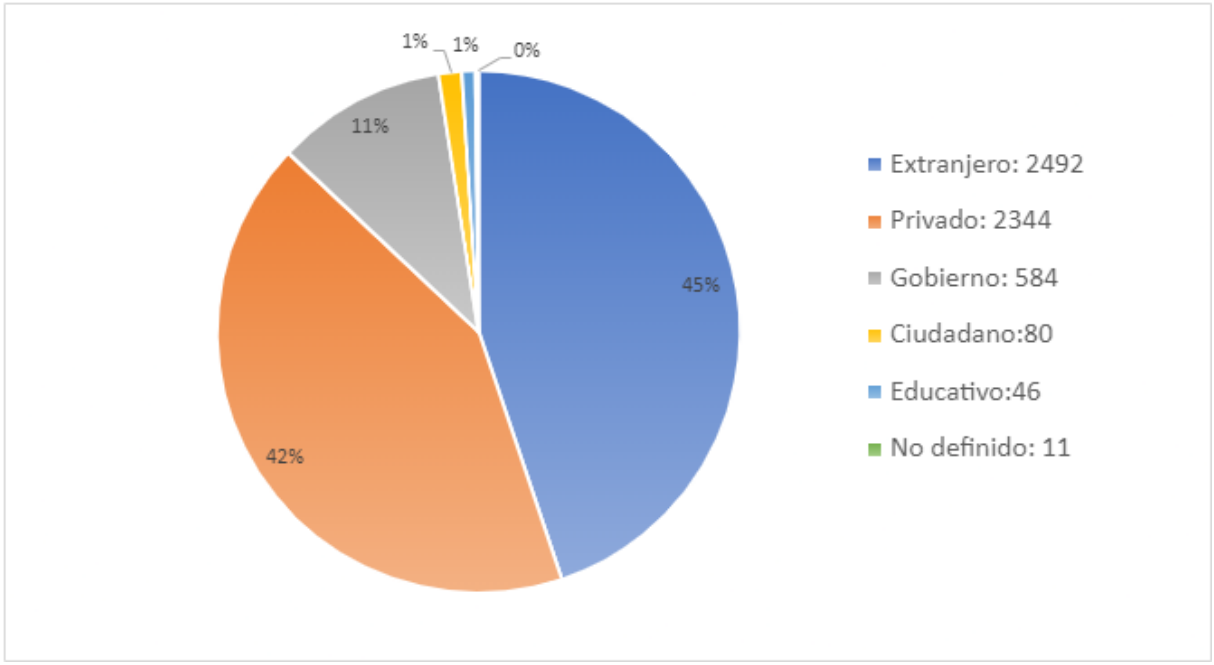


Figura 18. Distribución porcentual histórica de sectores afectados por incidentes cibernéticos. 2013 - 2022

La mayor cantidad de incidentes afectan a redes o sistemas de empresas privadas, esto se remarca especialmente desde el 2020 luego se han implementado sistemas de automatización

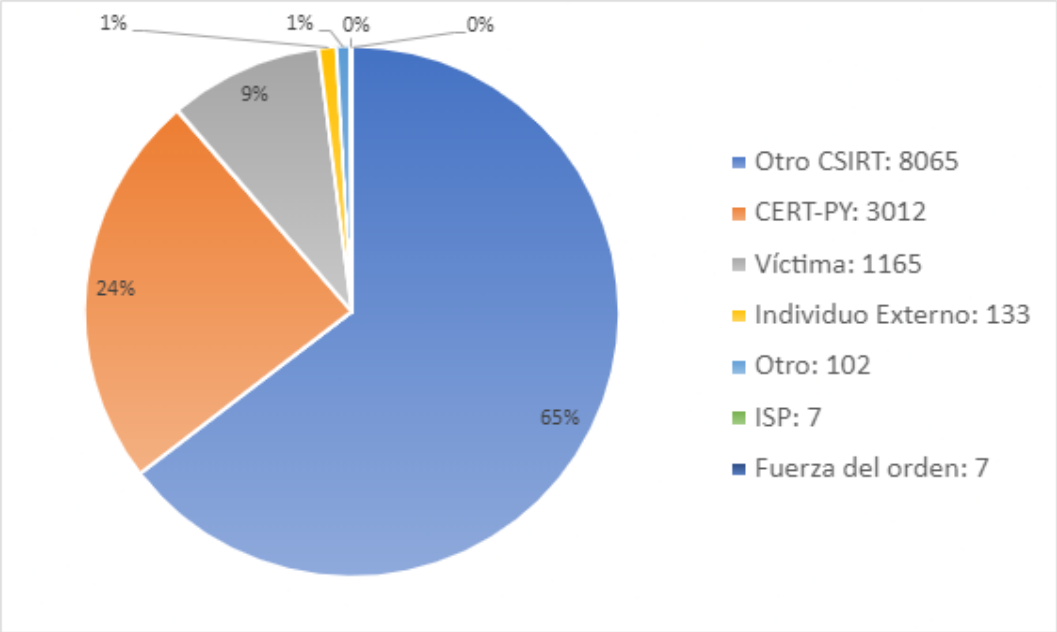


Figura 19. Distribución porcentual histórica Reportes de incidentes por tipo de denunciante. 2013 - 2022

Evolución histórica del tiempo de respuesta y atención

En el 2022 se ha incrementado el tiempo de respuesta de reportes, comparado con el año anterior, aunque se cuentan con más procesos de reportes automatizados, el incremento del tiempo de respuesta se debe al aumento del número de casos de reportes de incidentes, debido a la tendencia de automatización, también el CERT-PY ha comenzado a recibir reportes automatizados, además de que los reportes se han evolucionado volviéndose más sofisticados, tal situación ha impactado en el tiempo de respuesta y atención al nivel deseado.

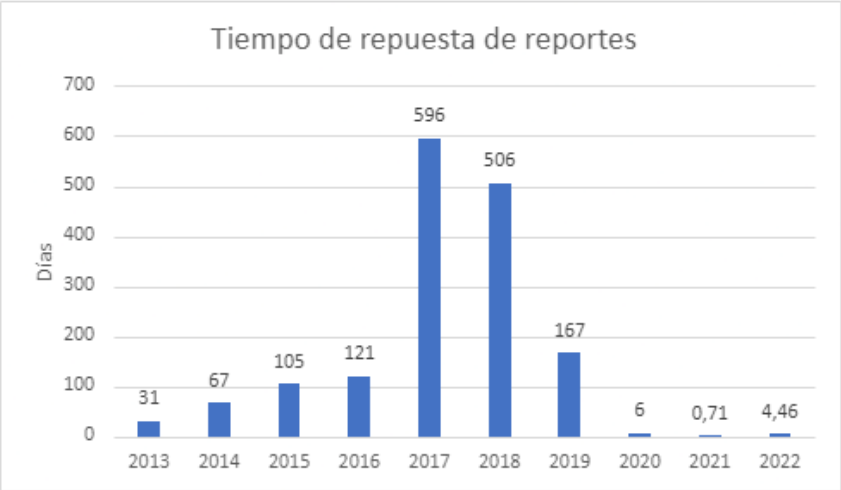


Figura 20. Evolución histórica del tiempo promedio de atención de reportes

Figura 21. Evolución histórica del tiempo promedio de resolución de incidentes (anual)

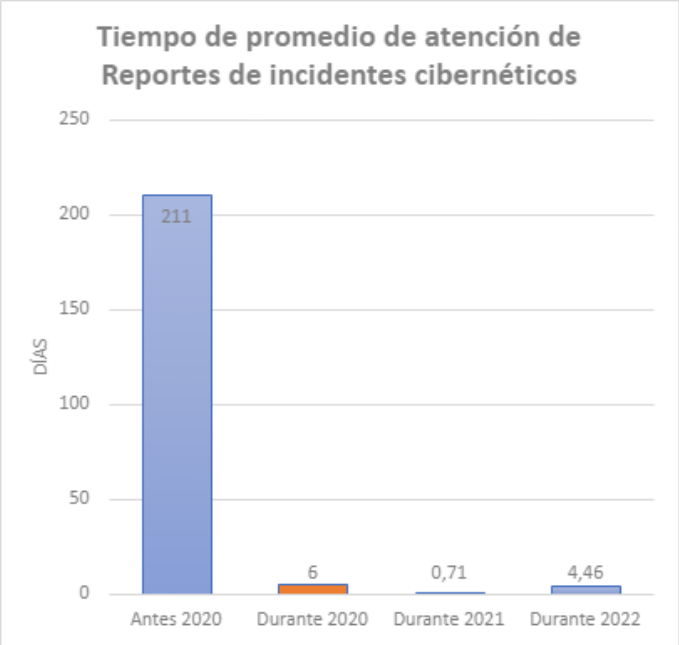


Figura 22. Tiempo promedio de atención de Reportes de Incidentes Cibernéticos.

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** que mantiene la tendencia con el año anterior, seguido del mes de mayo, con 1234 reportes. En el mes de octubre se ha mantenido la tendencia con respecto al año anterior en recibir la menor cantidad de incidentes, con 910 reportes recibidos, en números generales, se evidencia un incremento del número de incidentes de forma anual.

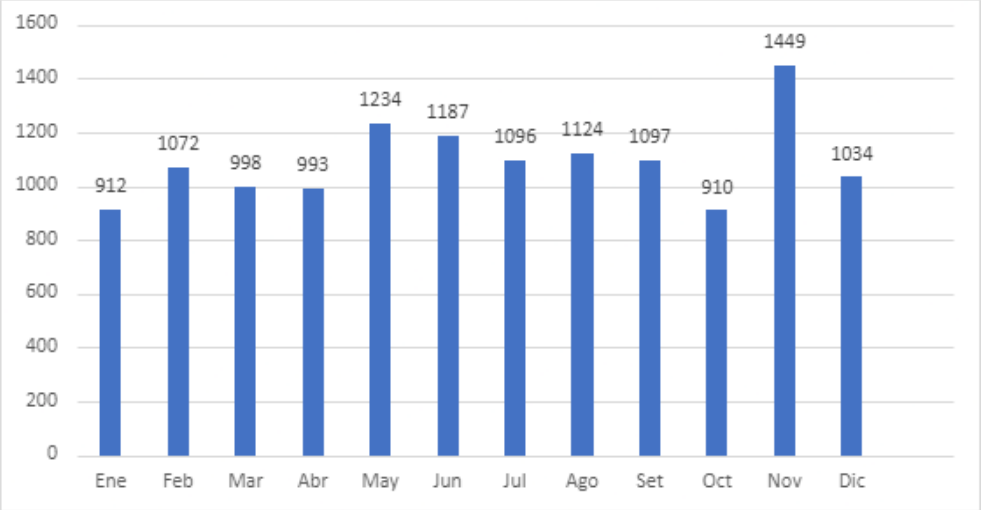


Figura 23. Cantidad histórica acumulada de reportes de incidentes cibernéticos por mes del año. 2013 - 2022

La mayor cantidad de reportes de incidentes cibernéticos se recibieron los **lunes y martes**, en los que se ha recibido un total de 2477 y 2339 reportes respectivamente, con un decrecimiento gradual durante la semana, hasta un mínimo **los sábados y domingo**, con 1132 y 1094 reportes respectivamente.

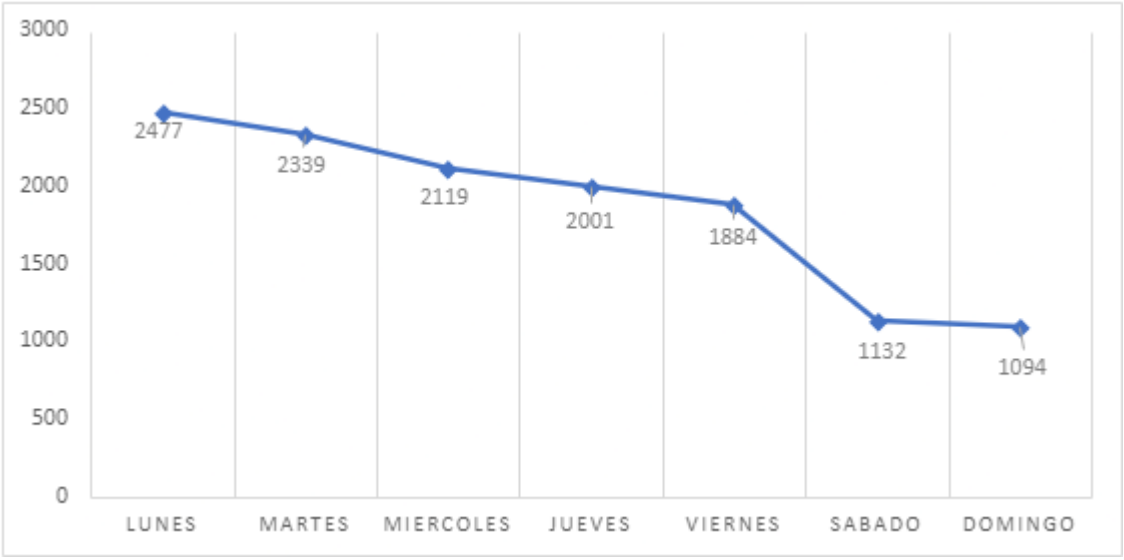


Figura 24. Cantidad histórica acumulada de reportes de incidentes cibernéticos por día de la semana. 2013 - 2022

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:

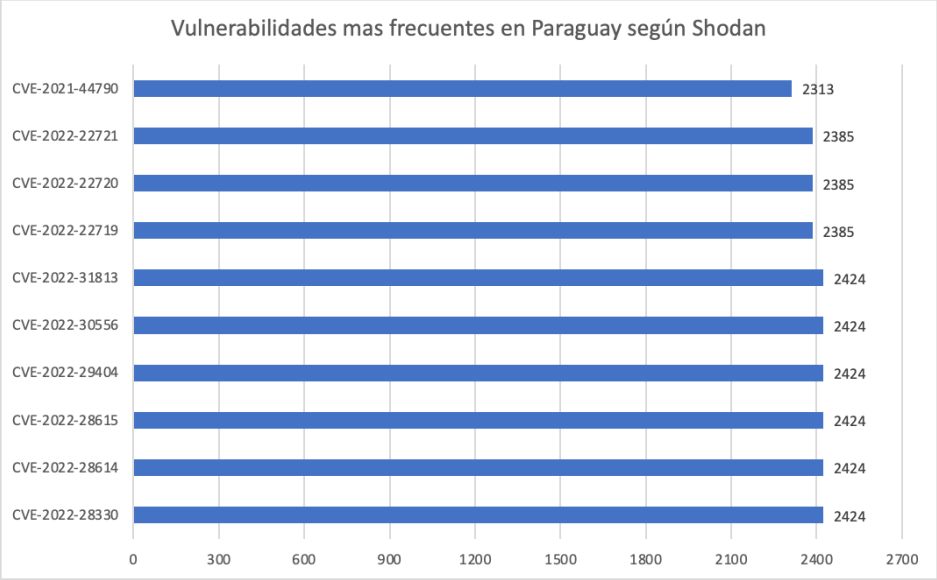


Figura 25. Vulnerabilidades más frecuentes en servicios expuestos en Internet de Paraguay

La mayoría de las vulnerabilidades afecta al servidor web Apache, esto hace relación con que dicho servidor web es muy popular en el ambiente TICs del país y también a nivel mundial.

Podemos resaltar CVE-2021-44790 con criticidad crítica y una puntuación 9.1, la cual afecta a Apache HTTP Server version 2.4.53 y anteriores pueden bloquearse o revelar información debido a una lectura más allá de los límites en ap_strcmp_match() cuando se proporciona con un búfer de entrada extremadamente grande. Si bien ningún código distribuido con el servidor puede ser coaccionado en dicha llamada, los módulos de terceros o los scripts lua que usan ap_strcmp_match() pueden hipotéticamente verse afectados.

También podemos comentar sobre la vulnerabilidad CVE-2021-44790 con criticidad crítica y una puntuación 9.8, debido a que una solicitud cuyo cuerpo está cuidadosamente elaborado puede causar un desbordamiento de búfer en el analizador multiparte mod_lua

(r:parsebody() llamado desde scripts Lua). El equipo de httpd de Apache no tiene conocimiento de un exploit para la vulnerabilidad, aunque podría ser posible crear uno. Este problema afecta a Apache HTTP Server 2.4.51 y versiones anteriores.

La vulnerabilidad CVE-2022-31813 con criticidad crítica y una puntuación de 9.8 afecta a Apache HTTP Server en su versión 2.4.53 y versiones anteriores, es posible que no envíen los encabezados X-Forwarded-* al servidor de origen según el mecanismo de salto por salto del encabezado de conexión del lado del cliente. Esto se puede usar para omitir la autenticación basada en IP en el servidor/aplicación de origen.

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.

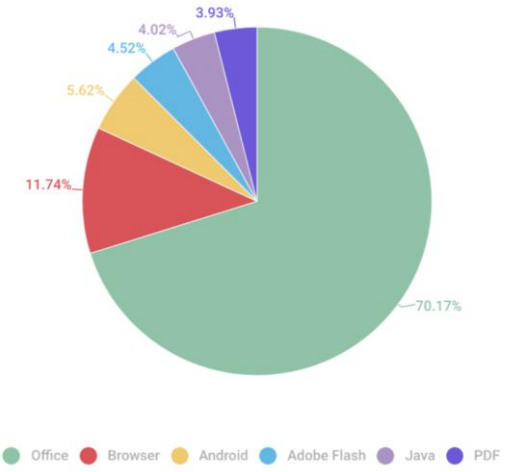


Figura 26. Vulnerabilidades más explotadas mundialmente en 2022[4]

Kaspersky reportó que nuevamente vieron una tendencia al alza en la popularidad de los ataques que utilizan la suite Microsoft Office (70,17%). Esto se debió a dos vulnerabilidades fáciles de explotar (CVE-2021-40444 y CVE-2022-30190) encontradas en rápida sucesión. Los

[4] Kaspersky Security Bulletin 2022. Statistics

ciberdelincuentes también continuaron usando las vulnerabilidades antiguas, pero aún actuales: CVE-2017-11882, CVE-2018-0802, CVE-2017-8570 y CVE-2017-0199. Como resultado, la cantidad de activaciones únicas en respuesta a los intentos de explotar las vulnerabilidades de Microsoft Office aumentó en más de 20% con respecto al reporte del año pasado[5].

Según Kaspersky, entre los ataques de red que pudieron analizar, la fuerza bruta de contraseñas para varios servicios de red, como RDP, Microsoft SQL Server y SMB, sigue siendo popular. También siguen en demanda los exploits de Equation Group, en particular EternalBlue y EternalRomance para sistemas Microsoft Windows obsoletos y sin parches. Se encontraron varias vulnerabilidades graves en el controlador del sistema de archivos de red (NFS), sobre todo CVE-2022-24491 y CVE-2022-24497. En teoría, estos pueden usarse para llevar a cabo ataques RCE mediante el envío de un mensaje de red especialmente diseñado a través del protocolo NFS. Entre las vulnerabilidades más destacadas para las versiones de Windows Server está la falsificación de LSA (CVE-2022-26925): "un atacante no autenticado puede llamar a un método de interfaz LSARPC que forzará al controlador de dominio de Windows a autenticarlo". Un revuelo mediático fue causado por dos vulnerabilidades en Microsoft Exchange Server (CVE-2022-41040, CVE-2022-41082), denominadas ProxyNotShell por su similitud en términos de explotación con las vulnerabilidades ProxyShell reportadas el año 2021. Al final del 2022, se encontraron dos vulnerabilidades (CVE-2022-22965, CVE-2022-22947) en marcos web como Spring Framework y Spring Cloud Gateway[6].

Amenazas financieras

Según Kaspersky, para evaluar y comparar el riesgo de ser infectado por troyanos bancarios y malware de cajeros automáticos/puntos de venta (POS) en todo el mundo, para cada país se calculó la proporción de usuarios de productos de Kaspersky que enfrentaron esta amenaza durante el período del informe como porcentaje de todos los usuarios de sus productos en el país.

[5] Kaspersky Security Bulletin 2022. Statistics
https://securelist.com/ksb-2022-statistics/108129/

[6] Kaspersky Security Bulletin 2022. Statistics
https://securelist.com/ksb-2022-statistics/108129/

Durante los meses de Julio, Agosto y Septiembre en Paraguay, se vio que 2.8% de los usuarios de Kaspersky tuvieron detecciones de malware bancarios[7] .

	Country or territory*	%**
1	Turkmenistan	4.7
2	Afghanistan	4.6
3	Paraguay	2.8
4	Tajikistan	2.8
5	Yemen	2.3
6	Sudan	2.3
7	China	2.0
8	Switzerland	2.0
9	Egypt	1.9
10	Venezuela	1.8

Figura 27. TOP 10 países y territorios por porcentaje de usuarios atacados

Tendencias de victimología del Ransomware

De acuerdo con datos de Dragos[8], durante el cuarto trimestre de 2022, Dragos siguió tendencias en la victimología de los grupos de ransomware que también afectaron a Paraguay. Sin embargo, esto no determina el enfoque permanente de estos grupos, ya que la victimología puede cambiar con el tiempo. Dragos observó siete grupos de ransomware más que afectan a sectores

[7] Fuente: https://securelist.com/it-threat-evolution-in-q3-2022-non-mobile-statistics/107963/
[8] Fuente: https://www.dragos.com/blog/industry-news/dragos-industrial-ransomware-analysis-q4-2022/

industriales y regiones del mundo en este último trimestre que en el tercer trimestre de 2022. Según su análisis del período del cuarto trimestre de 2022, Dragos observó algunos de los grupos de ransomware más activos que afectan a las siguientes industrias:

- AlphaV: energía, alimentos y bebidas, petróleo y gas, manufactura
- BIANLIAN: energía, ingeniería, alimentos y bebidas, minería, productos farmacéuticos y manufactura.
- Black Basta: alimentos y bebidas, manufactura
- Karakurt: energía, alimentos y bebidas, petróleo y gas, productos farmacéuticos y manufactureros.
- Lockbit 3.0: alimentos, bebidas y manufactura
- Royal: energía, alimentos y bebidas, petróleo y gas, productos farmacéuticos y manufactura.
- **Avos Locker solo impactó a Paraguay**
- El EQUIPO DAIXIN solo impactó a Indonesia
- DONUT solo afectó a EE. UU.

Denegación de servicio saliente y entrante de Paraguay

De acuerdo con los datos proveídos por Netscout, otro proveedor de servicios, se registraron 6.09k ataques de DoS a servicios paraguayos, con un poco de volumen de 88.9 Gbps. La máxima duración de un ataque fue de 2 días. Las técnicas de ataque más utilizadas fueron TCP null, UDP y Amplificación CLDAP.

Figura 28. Resumen de ataques DDoS en Paraguay en el 2022 según Netscout

De acuerdo a los datos de Netscout[9], la mayor cantidad de los ataques a servicios paraguayos recibidos tuvieron como origen EE.UU. con 36,3%, Brasil con un 28,5% y Alemania con un 27,2%.

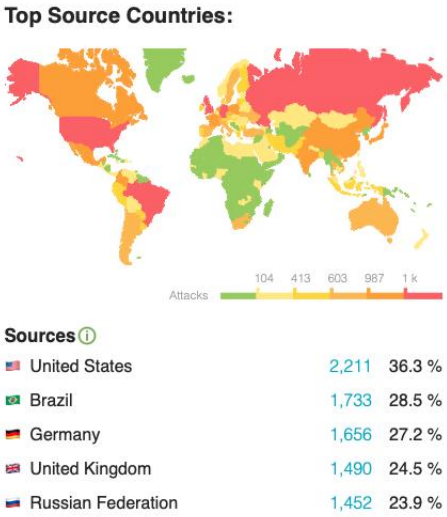


Figura 29. Top de países de los cuales se recibió ataques

La mayor cantidad de ataques de DDoS según Netscout[10] se dieron los meses de Octubre, Noviembre y Diciembre, y el 35,22% de todos los ataques duraron entre 5 min a 10 min y el 29,47% de estos duraron entre 10 min a 1 hora.

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

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

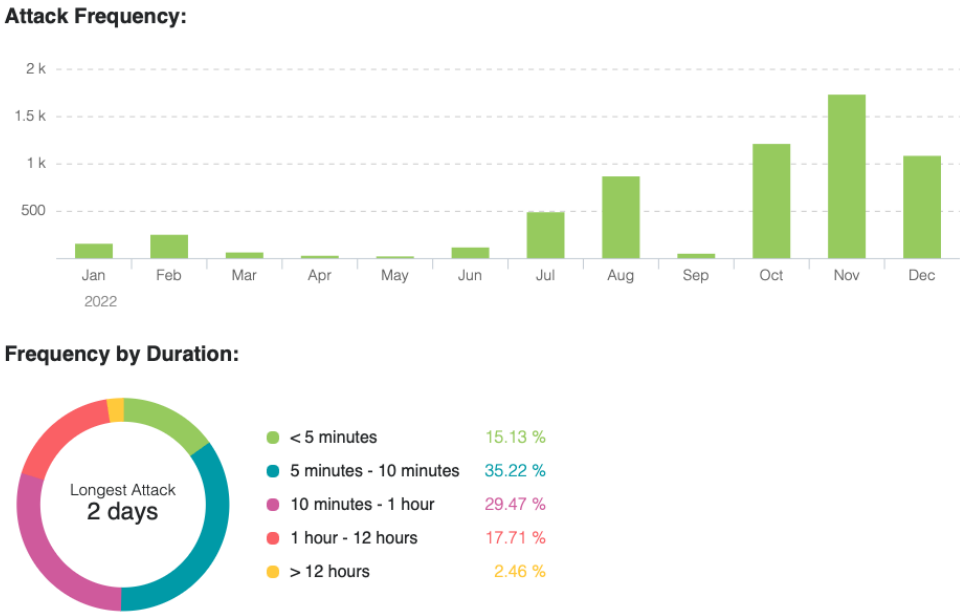


Figura 30. Frecuencia de ataques de DDoS - NETSCOUT

Otras fuentes de datos específicas para Paraguay - Shadowserver

Diariamente el CERT-PY recibe un gran volumen de indicadores de compromisos (Indicators of Compromise - IoC)[11] 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: ~ 19.663
- Se excluye el mes de Enero del 2022 debido un problema en la subscripción con Shadowserver, ese mes no recibimos reportes

[11] 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.

Figura 31.Cantidad de eventos reportados por Shadowserver en el 2022

- Se reportaron un total de 328.908 IPs únicas con servicios vulnerables, expuestos o comprometidos por malware.
- Servidores DNS OpenResolver: cantidad promedio de IPs diarias ~1104 (a través de ellos se pueden realizar enormes ataques de denegación de servicio)
- 20.995 IPs únicas con DNS OpenResolver configurado.

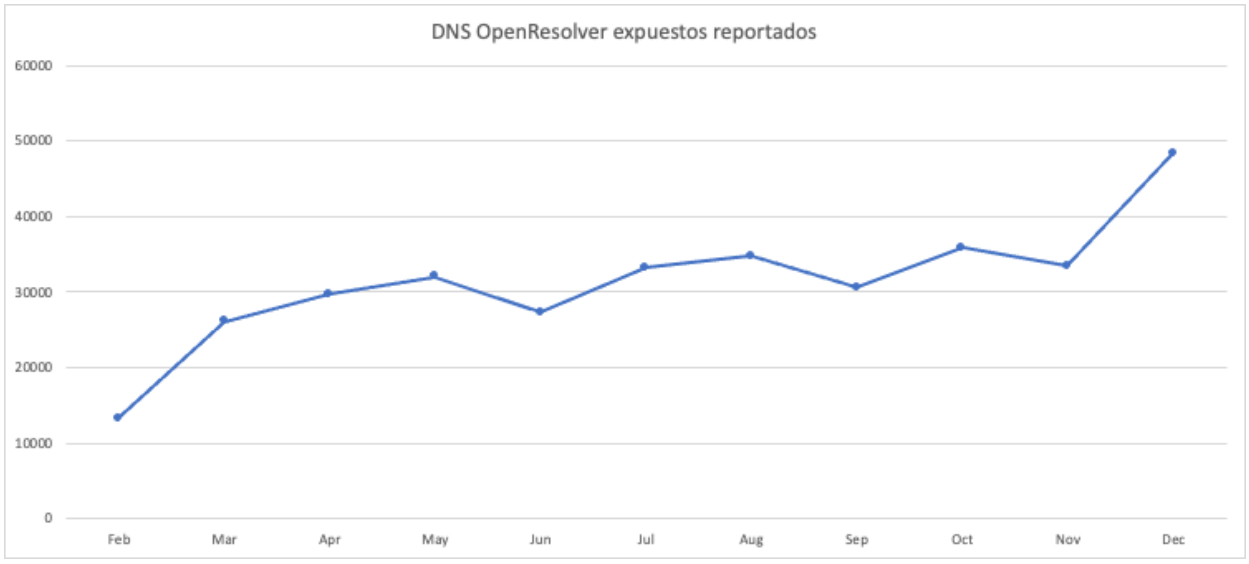


Figura 32. Distribución mensual de reportes DNS Open Resolver expuestos enviados por Shadowserver

- Cantidad promedio de IPs detectadas diariamente con RDP expuesto a Internet: ~665

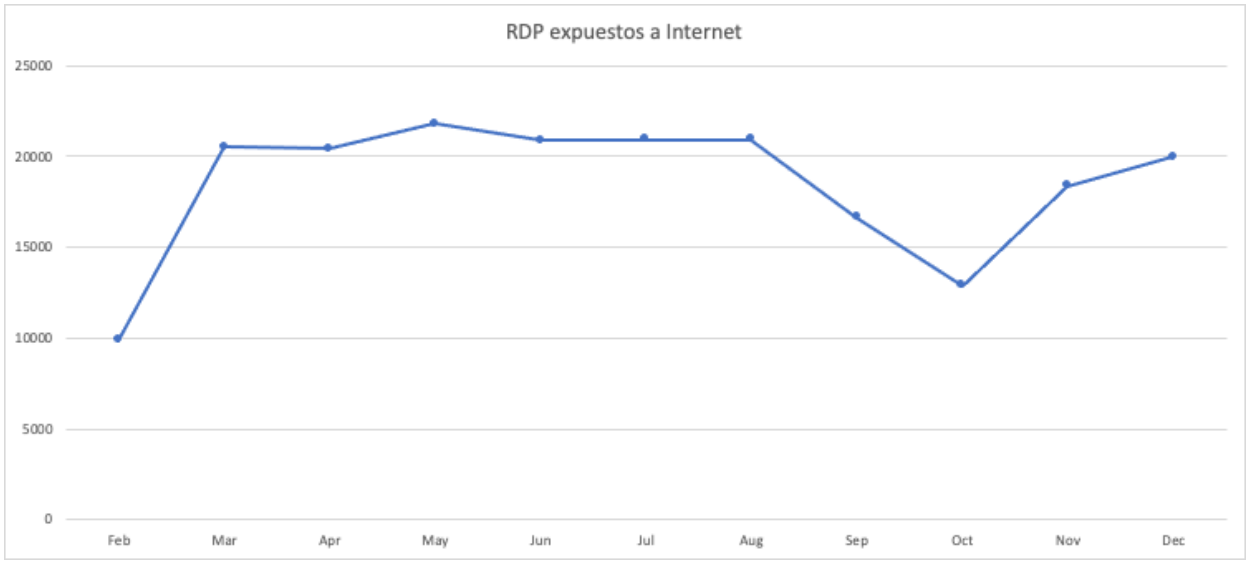


Figura 33. Distribución mensual de reportes de RDP expuestos a Internet enviados por Shadowserver

- Distribución eventos recibidos diariamente con Telnet expuesto a Internet: ~930
- Cantidad de IPs únicas con Telnet expuesto a Internet: 8.682

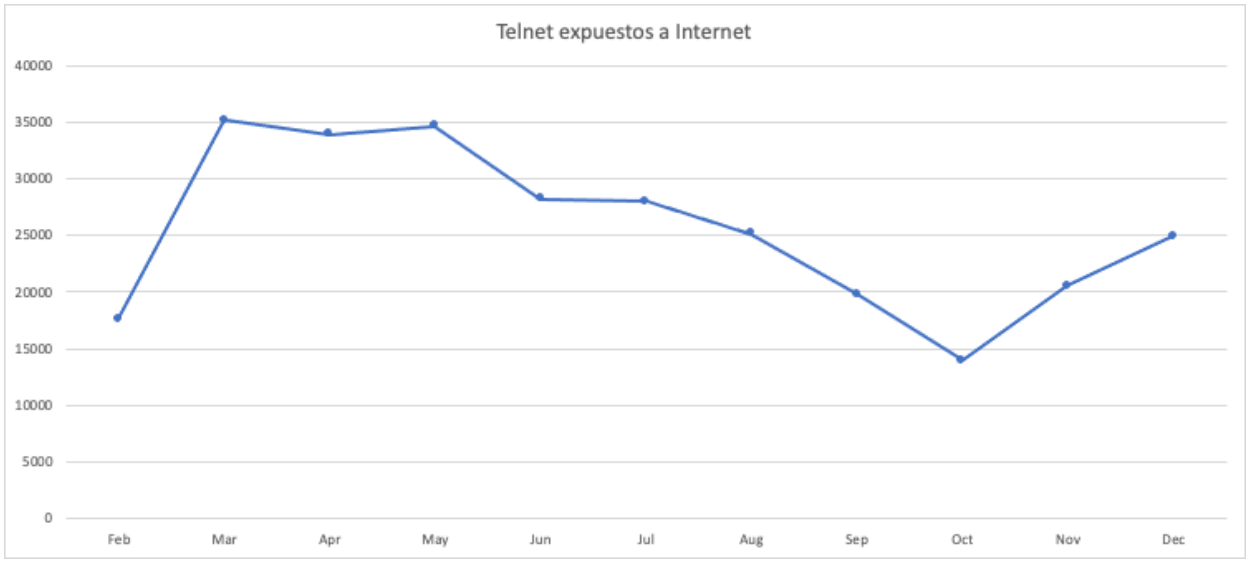


Figura 34. Distribución de reportes de Telnet expuestos enviados por Shadowserver

- 1666 IPs únicas participaron de ataques de denegación de servicio de amplificación distribuido.
- 949 IPs únicas realizaron ataques de fuerza bruta a otros sistemas.
- Cantidad promedio de IPs infectadas con malware, pertenecientes a una botnet, visualizadas por día: ~ 1174
- Cantidad de IPs únicas infectadas con malware, pertenecientes a una botnet: 30.050.

- Más de 134 familias de malware únicas detectadas en IPs paraguayas por Shadowserver. Las más detectadas son las siguientes:

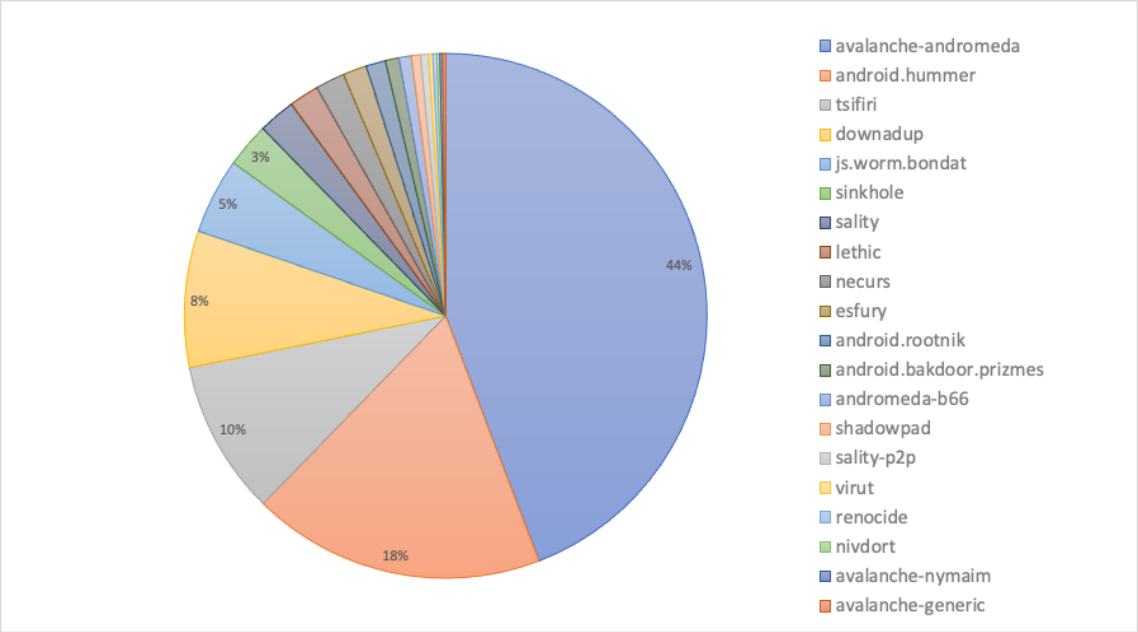


Figura 35. Cantidad de infecciones únicas por familia de malware[12]

La mayor cantidad de detecciones 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.

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.

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

- Copiándose a sí mismo en dispositivos removibles o de red

Generalmente se distribuye a través de sitios 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[13]. 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[14], 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.

También podemos ver que la segunda mayor cantidad de detección de infecciones son de Android Hummer, el cual es un troyano que se ejecuta en los sistemas operativos Android. Cuando un dispositivo está infectado, Hummer "rootea" el dispositivo para obtener privilegios de administrador y luego agrega anuncios emergentes al teléfono. Luego impulsa los juegos

[13] 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.

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

móviles e instala aplicaciones pornográficas en segundo plano. Cuando un usuario intente desinstalarlos, se volverán a instalar.

Según TechRepublic "la familia de troyanos Hummer podría ser una de las más grandes de la historia. Si bien la cantidad total de nuevas infecciones está disminuyendo, la cantidad promedio de dispositivos infectados es de 1.190.000, una cantidad mayor que la de cualquier otro troyano para teléfonos móviles. Esas son malas noticias para los usuarios de Android...".

También podemos ver en tercer lugar detecciones relacionadas con Tsifiri. El cual es una forma de ransomware que encripta los archivos de un usuario hasta que se paga un rescate. Se descubrió por primera vez en noviembre de 2019 y desde entonces se ha utilizado para dirigirse tanto a usuarios individuales como a organizaciones.

Investigaciones y desarrollo

Implementación de una Red Nacional de Honeypot para la seguridad de las redes de telecomunicaciones.

Durante este 2022 se colaboró con el Trabajo Final de Tesis de Grado del Sr. Romualdo Bizzo, el cual plantea "Implementación de una Red Nacional de Honeypot para la seguridad de las redes de telecomunicaciones" para brindar mayor visibilidad sobre la infraestructura nacional y los ataques sufridos en tiempo real. Este proyecto aún está en fase de investigación y desarrollo.

Este proyecto de investigación propone la implementación de una red nacional de honeypot, con la intención de generar visibilidad del tráfico de la red a través de la colecta y análisis de los datos generados por los sensores. Los honeypots son herramientas permiten observar los patrones de comportamientos de los atacantes mediante la observación en tiempo real del tráfico de la red, a partir de estas observaciones se pueden crear estrategias de defensa en el ciberespacio. Se estableció como objetivo general “Lograr visibilidad del tráfico de la red de las infraestructuras digitales del país a través de la implementación de una red nacional de Honeypot”. Se logró la implementación de la red a través de la instalación de un servidor que recolecta los datos generados por los sensores autónomos instalados en distintas infraestructuras localizadas en Paraguay, a partir de estos datos se han realizado varios análisis en los cuales se pudo detectar ataques de fuerza bruta, ejecución de comandos y envío de correos spam, pudiendo ser identificada la IP y el país de origen.

Durante el periodo analizado, los sensores estuvieron activos por 31 días. Durante este periodo se obtuvieron una cantidad total de 1.647.724 eventos registrados por tres sensores honeypot.

Figura 36. Número total de ataques recibidos durante un mes. Periodo del 12 de Octubre al 12 Noviembre 2022.

Los ataques registrados se originaron desde varias partes del mundo. El país del cual se recibió más ataques fue Estados Unidos con un 20,11%, seguido por Brasil con un 15,67%, en tercer lugar, China con un 13,95%, seguido por Vietnam con un 8,19%, en total el 57,92% de todos los ataques provinieron de estos países. En general se observa que la mayoría de los ataques provienen de países asiáticos y sudamericanos, correspondiéndole con las tendencias generales de incidentes cibernéticos.

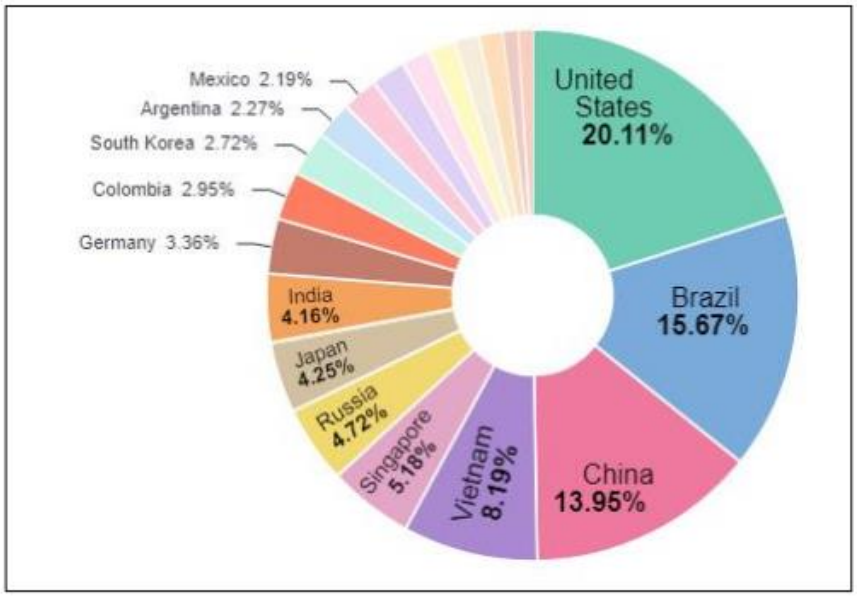


Figura 37. Porcentaje de ataques recibidos divididos por país.

Enlace del proyecto: https://www.oxyops.live.

Delitos Informáticos

Los delitos informáticos son todas las acciones dirigidas a lesionar la integridad, disposición y confiabilidad de datos y de sistemas informáticos, así como aquellas conductas que atentan contra el patrimonio de las personas utilizando herramientas tecnológicas e informáticas.

La Unidad Especializada de Delitos Informáticos dependiente del Ministerio Público fue creada para combatir los hechos punibles cometidos a través del uso de la tecnología que a su vez requieran un tratamiento especializado, desde la investigación, recolección, manejo de evidencia y prueba digital.

A su vez, dentro de la Policía Nacional, en la Dirección contra hechos punibles económicos y financieros, se encuentra la División Especializada contra Delitos Informáticos, qué es la unidad encargada de investigar, reprimir y prevenir, los hechos punibles a nivel nacional cometidos mediante el uso medios tecnológicos y de comunicación

Los delitos informáticos se encuentran tipificados de acuerdo a la Ley Nº 4439/11. Según las Resoluciones del Ministerio Público Nº 3459/10 y 4408/11, los tipos penales de competencia exclusiva de la Unidad Especializada en Delitos Informáticos son los siguientes:

Acceso indebido a datos, Interceptación, Preparación al acceso indebido a datos, Alteración de datos, Acceso indebido a sistemas informáticos, Sabotaje a sistemas informáticos, Alteración de datos relevantes, Falsificación de tarjetas de crédito y débito y, Estafa mediante sistemas informáticos.

Es importante tener en cuenta que el CERT-PY gestiona únicamente incidentes cibernéticos, no así los delitos informáticos[15]. Algunos delitos informáticos constituyen también incidentes cibernéticos y viceversa, pero no todo delito es un incidente, ni todo incidente es un delito. Por ejemplo: un acoso o estafa a través de medios informáticos (por ej. a través de redes sociales) no se considera un incidente cibernético, sin embargo, constituye un delito. Cuando el CERT-PY recibe un reporte que corresponde a un delito informático pero que no constituye un incidente

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

cibernético, éste es derivado directamente al Ministerio Público, quienes llevan las estadísticas específicas de este y otros tipos de delitos.

A continuación se muestra información estadística sobre la cantidad de causas investigadas por la Unidad de Delitos Informáticos del Ministerio Público durante los años 2021 y 2022 y la cantidad de personas condenadas por delitos informáticos[16].

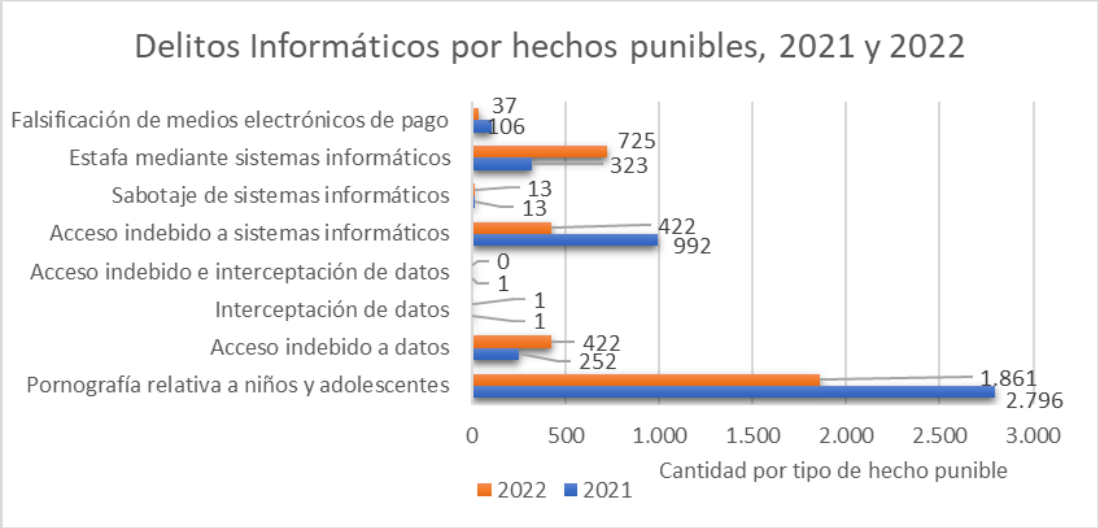


Figura 38. Cantidad de causas por hechos punibles años 2021 y 2022.

[16] Información obtenida por la Dirección de Transparencia y Acceso a la Información Pública del Ministerio Público.

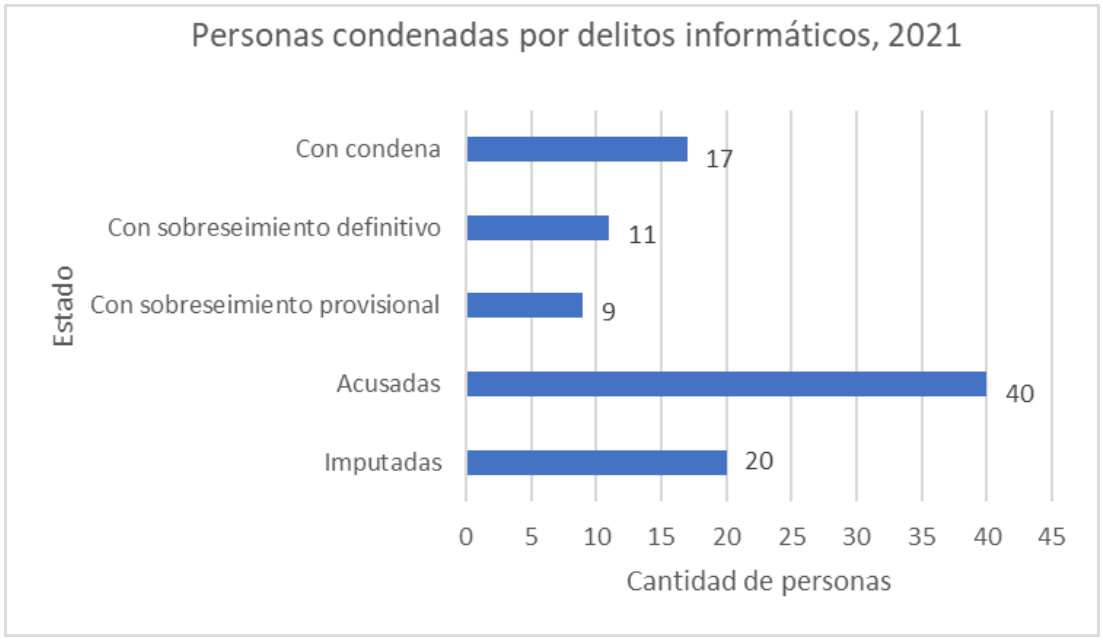


Figura 39. Personas condenadas por delitos informáticos en el año 2021.

Plan Nacional de Ciberseguridad

Por Decreto PE 7052/17 se aprobó el Plan Nacional de Ciberseguridad, 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. Esté plan se desarrolló bajo el liderazgo de la Presidencia de la República del Paraguay, a través de la entonces Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs), en coordinación con el Ministerio de Relaciones Exteriores (MRE), 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), y constituye 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 que 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**

Y a su vez, estos ejes tienen 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.

El mismo Decreto dispone un Coordinador Nacional de Ciberseguridad, establece entre otras funciones, presidir una Comisión Nacional de Ciberseguridad y Subcomités especializados y define además, las instituciones públicas integrantes de dicha comisión.

Para 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

La primera medición del año 2020 realizada por medio de la Comisión Nacional de Ciberseguridad utilizando este método, arrojó el siguiente resultado:

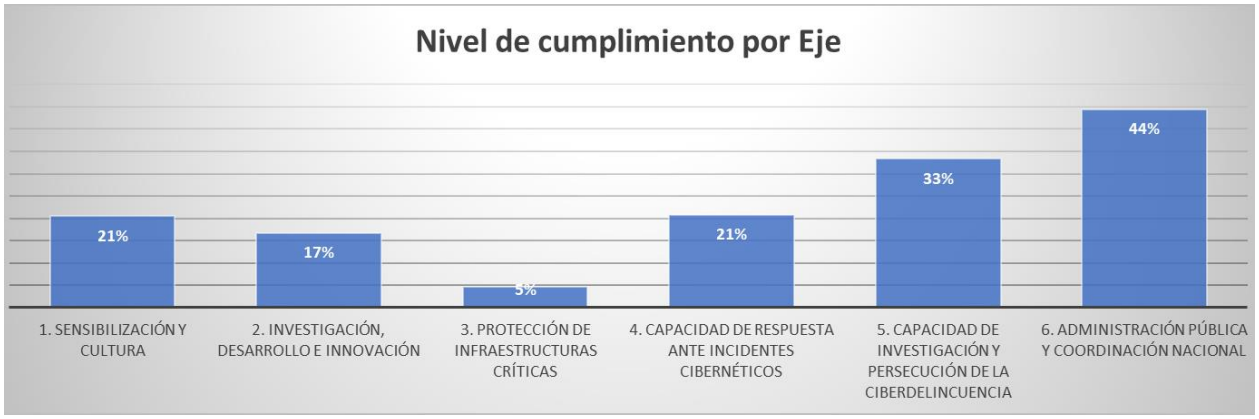


Figura 40. Nivel de avance global del Plan Nacional de Ciberseguridad, Febrero 2020.

Políticas, estándares y normativas en materia de Ciberseguridad

La seguridad cibernética es una preocupación cada vez más importante para el gobierno. Con el aumento de amenazas en línea cada vez más frecuentes y sofisticadas, es esencial contar con políticas, estándares y normativas claras en materia de ciberseguridad, que garanticen la protección de la seguridad: confidencialidad, integridad y disponibilidad y la continuidad de las operaciones en entornos digitales, que afectan a los ciudadanos y la infraestructura crítica del país.

En tal sentido, el gobierno paraguayo, desde finales del año 2018, ha diseñado, aprobado y socializado una serie de políticas, estándares, directivas y normativas en materia de ciberseguridad, aplicables, principalmente para las instituciones gubernamentales. Y desde el año 2020 se han realizado diversos esfuerzos para medir el nivel de cumplimiento de dichas normativas.

También, con el objetivo de conocer el nivel de madurez de ciberseguridad en el gobierno, en el año 2022, el MITIC realizó una encuesta a los **Responsables de Seguridad de la Información**[17] de Instituciones públicas, compuesta de preguntas relacionadas con prácticas de seguridad de la información, como la utilización de las normativas vigentes emitidas por el MITIC, las políticas y procedimientos de seguridad de la información internas, la gestión de incidentes y de riesgos de seguridad, la formación de capacidades en ciberseguridad, entre otros temas importantes.

Respecto a existencia y nivel de madurez de implementación de políticas de seguridad de la información generales y específicas en instituciones públicas, según la encuesta, de un total de 84 encuestados, el **4,76%** indicó que sí tienen políticas de seguridad generales y específicas, y **el grado de madurez de implementación es alto**; el **46,43%** indicó que sí tienen políticas de seguridad generales y específicas, pero **el grado de madurez de implementación es medio o bajo.** Un **5,95%** de los encuestados indicó que sí tienen políticas de seguridad generales y específicas, pero **el grado de madurez de implementación es nulo.** Por último, el **34,52%** de los encuestados indicó que **no cuentan con políticas de seguridad formales**, mientras que el **8,33%** respondió **"otro"**. Aunque una parte significativa de las instituciones encuestadas tienen

[17] https://www.cert.gov.py/modelo-de-gobernanza-de-seguridad-de-la-informacion/

políticas de seguridad generales y específicas, todavía hay un porcentaje considerable que no las tienen implementadas o que tienen un grado de madurez bajo o nulo en su implementación.

A continuación se detallan las normativas emitidas por la Dirección General de Ciberseguridad y Protección a la Información del Ministerio de Tecnologías de la Información y Comunicación (MITIC):

Modelo de Gobernanza de Seguridad de la Información del Estado

Es una directiva mediante la cual se establece que todas las instituciones del Estado deben contar con un área de Seguridad de la Información y un Responsable 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. Fue aprobado por Resolución MITIC Nº 733/2019 y 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 conflictos 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.

Los Responsables de Seguridad de la Información constituyen el punto de contacto oficial para todas las comunicaciones y gestiones en iniciativas, proyectos y servicios de Ciberseguridad entre el MITIC y las demás instituciones públicas y estos además conforman el Subcomité de Ciberseguridad de la Administración Pública. Es responsabilidad de cada institución mantener actualizada la información de contacto del Responsable de Seguridad de la Información, de modo a mantener un canal de comunicación fluido.

Del total de 156 OEE registrados en la SFP, en el año 2022, 89 funcionarios correspondientes al **57%** del total **fueron designados a actividades de ciberseguridad, seguridad de la información, seguridad informática y/o auditoría TIC**, que representa una disminución del 13% respecto al año anterior. Cabe destacar que algunas grandes instituciones del Estado tienen subdivisiones con cierta independencia y por ese motivo tienen más de un Responsable de Seguridad de la Información (por ejemplo el Ministerio de Hacienda, la Corte Suprema de Justicia, el Ministerio de Justicia, y otros).

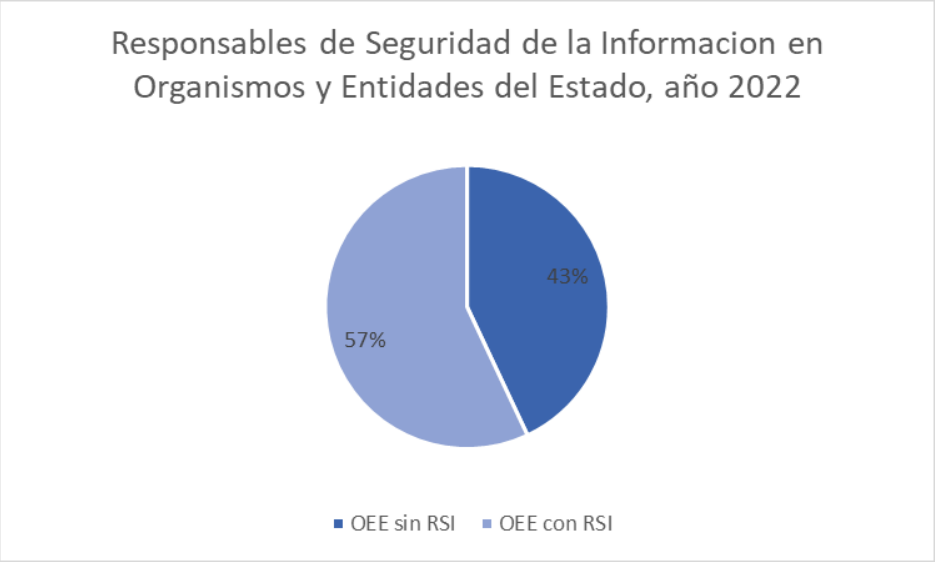


Figura 41 - Responsables de Seguridad de la Información en OEE designados formalmente hasta el año 2022.

Entre los principales hallazgos de la encuesta respondida por 84 instituciones, se destaca que el nivel de madurez en ciberseguridad varía ampliamente entre ellas. En general, se puede decir que solo el 23% de las instituciones públicas encuestadas **presentan un alto nivel de madurez en ciberseguridad**, mientras que un **40% tienen un nivel medio** y el **37% restante un nivel bajo.**

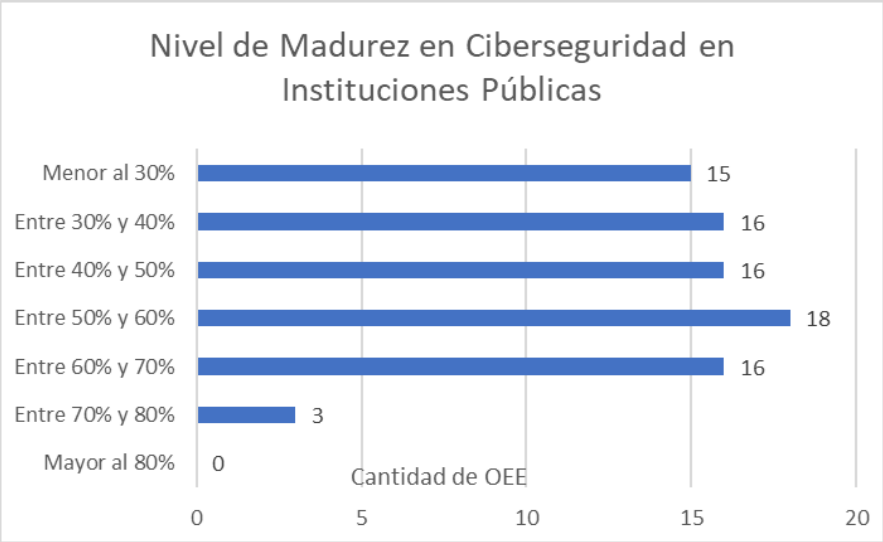


Figura 42. Nivel de madurez en ciberseguridad, año 2022.

Entre las instituciones que tienen un alto nivel de madurez en ciberseguridad, se destacan aquellas que han implementado políticas y procedimientos claros y bien definidos, tienen un enfoque proactivo en la detección y respuesta a incidentes, y cuentan con un personal capacitado y dedicado a la ciberseguridad. Por otro lado, aquellas instituciones que presentan un nivel bajo de madurez en ciberseguridad carecen de políticas y procedimientos claros y bien definidos, tienen una falta de concienciación y formación en ciberseguridad por parte del personal, y no cuentan con la inversión necesaria en herramientas y recursos de ciberseguridad. Aunque hay algunas instituciones públicas que han logrado un alto nivel de madurez en ciberseguridad, aún hay una cantidad significativa que tienen áreas de mejora importantes en cuanto a la protección de sus activos y datos críticos.

Respecto a la **organización de la Seguridad de la Información** dentro de las instituciones públicas, existen diversas formas. Un **17,86%** de las instituciones encuestadas **tienen al área de Seguridad de la Información dependiendo directamente de la Máxima Autoridad**, lo que indica un alto compromiso abordado por la más alta instancia. Por otro lado, el **32,14%**, la incluye **como dependencia dentro del área de TIC**, lo que indica que en estas instituciones se considera que la seguridad de la información es un tema íntimamente relacionado con las TIC, por lo que se le asigna a la misma nivel de importancia dentro del área de TIC. El **5,95%**, respondió que es una unidad independiente de TICs, pero está incluida **como dependencia dentro de un área distinta a TIC**. Sin embargo, un **41,67%** de las instituciones encuestadas indicó que **no tiene la Seguridad de la Información dentro de su organigrama institucional,** dando una menor importancia y

corriendo el riesgo de que la seguridad de la información no sea abordada de manera adecuada. Por último, un **2,38%** de las instituciones encuestadas indicó que tienen **otras formas de organización**. Es importante destacar que resulta fundamental que la misma tenga un nivel jerárquico adecuado que refleje la importancia que se le debe otorgar. De esta manera, se garantiza una protección adecuada de la información y se minimizarán los riesgos.

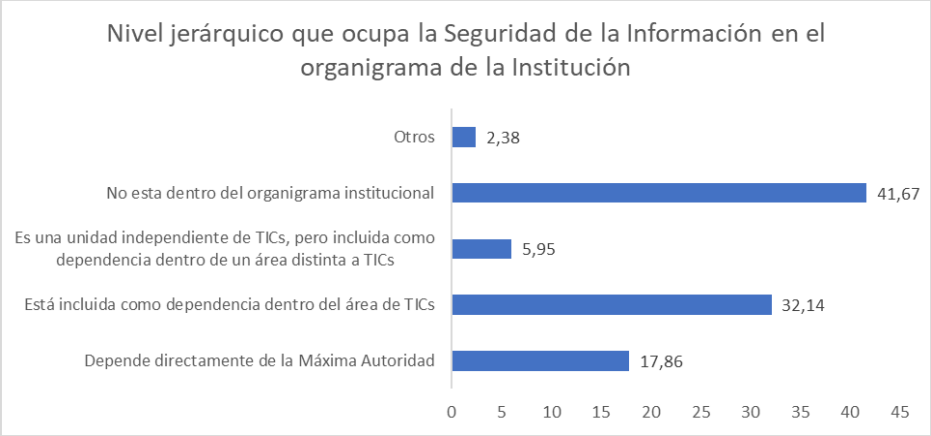


Figura 43. Nivel jerárquico de la Seguridad de la Información en Instituciones Públicas, año 2022.

En cuanto a la **formación específica en TIC y/o Ciberseguridad,** el **36,9%** de los RSI del Estado **tienen formación profesional de carrera de grado afín a las TIC,** lo que indica que cuentan con una base sólida en el área. Por otro lado, el **29,76%** de los RSI del Estado cuentan además **con formación específica en Ciberseguridad**, lo que les permite tener una comprensión detallada de los riesgos y amenazas que enfrentan los sistemas informáticos y estar preparados para prevenir y gestionar incidentes de seguridad. Además, un **16,67%** de los RSI del Estado **tienen formación específica en TIC y/o Ciberseguridad, a pesar de que su carrera de grado no está relacionada con las TIC.** El **10,71%** de los RSI del Estado **son autodidactas en TIC y/o Ciberseguridad**, adquiriendo conocimientos a través de cursos en línea, tutoriales y otras fuentes de información. Finalmente, el **5,95%** de los RSI del Estado **no tienen formación específica en TIC y/o Ciberseguridad**, lo que podría indicar una brecha en las habilidades y conocimientos necesarios para enfrentar los retos actuales en el ámbito tecnológico y de la ciberseguridad.

El **35,71%** de los encuestados **indicó que no hay ninguna persona dedicada exclusiva o principalmente a las funciones de ciberseguridad en su organización**. Por otro lado, el **36,90%** señaló que **solo una persona se dedica a estas funciones**; el **17,86%** indicó que **dos personas se dedican a la ciberseguridad**. Solo el **8,33%** indicó que **entre 3 y 5 personas se dedican a las**

funciones relacionadas con la ciberseguridad, mientras que solo el **1,19%** de los encuestados indicaron que **más de 5 personas se dedican a estas funciones**.

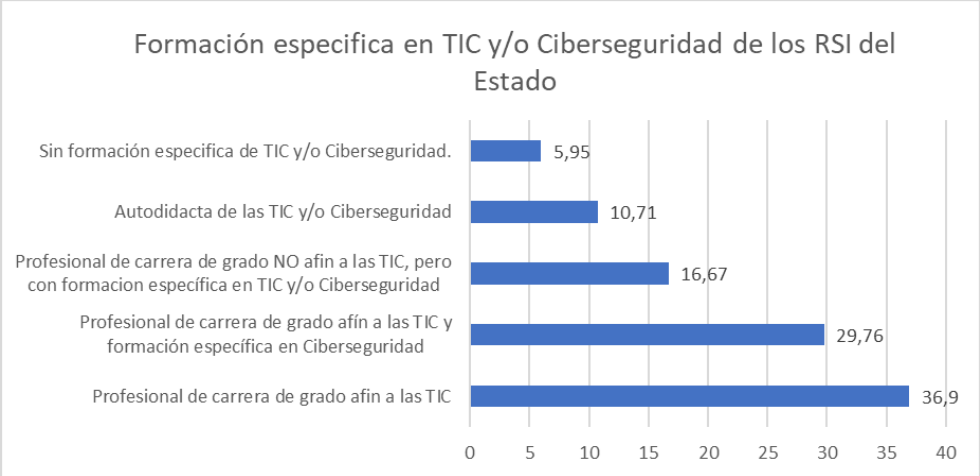


Figura 44. Formación específica en TIC y/o Ciberseguridad de los RSI, año 2022.

En cuanto al **tiempo que las personas dedican a los roles y responsabilidades de ciberseguridad**, un **11,90%** de los encuestados afirmó una **dedicación completa y exclusiva**, lo que indica un alto nivel de compromiso y dedicación a esta área. Por otro lado, un **10,71%** afirmó dedicar **un rango de 20 a 30 horas semanales**, lo que indica una dedicación parcial pero significativa. Un porcentaje mayor, el **17,86%**, indicó que dedica **un rango de 10 a 20 horas semanales**, lo que indica una dedicación parcial, pero aún así considerable. Por otro lado, el **34,52%** indicó que dedica **ocasionalmente** tiempo a la ciberseguridad, **no más de una vez por semana**. Esto podría ser preocupante ya que la seguridad cibernética es una tarea continua y la falta de dedicación constante puede aumentar el riesgo de incidentes. El **22,62%** de los encuestados afirmó que sólo dedica tiempo a la ciberseguridad **cuando hay incidentes de seguridad**, lo que indica una actitud más reactiva que proactiva. Finalmente, el **2,38%** de los encuestados indicó que tienen **otros niveles** de dedicación a la ciberseguridad que no están cubiertos por las opciones de la encuesta.

Por otra parte, respecto a la **cantidad de personas que trabajan en seguridad**, el **35,71%** indicó que **ninguna persona se dedica a las funciones de seguridad de la información**. Por otro lado, el **36,90%** indicó que **solamente una persona se dedica a estas funciones**, mientras que el **17,86%** indicó que **dos personas se dedican a esto**. En cuanto a los grupos más grandes de personas, el **8,33%** indicó que **entre tres a cinco personas se dedican a estas funciones**, y solo el **1,19%** indicó **más de cinco personas.**

Respecto a la **existencia de un inventario detallado y continuo, manual o automatizado, de los activos tecnológicos de la Institución**, el **39,29%** indicó que **sí tienen un inventario con información detallada y actualizada de todos los activos tecnológicos de la organización**. El **34,52%** de los encuestados indicó que **parcialmente tienen un inventario con información detallada y actualizada de algunos de los activos tecnológicos de la organización.** Un **16,67%** de los encuestados indicó que **parcialmente tienen un inventario con información detallada de algunos de los activos tecnológicos de la organización, pero no está actualizada.** Por otro lado, el **8,33%** de los encuestados indicó que **nunca han realizado un inventario detallado y continuo** de los mismos. Un **1,19%** respondió con **"otros"**.

Otro aspecto importante, es que según los datos proporcionados, se puede observar que la mayoría de los encuestados (**71,43%**) **indica que no tienen un presupuesto específico asignado para la ciberseguridad**. Un porcentaje significativo (**13,10%**) **seleccionó la opción "Otro"**, lo que podría indicar que tienen una asignación de presupuesto diferente para la estrategia de ciberseguridad y continuidad de negocio. Sin embargo, solo una pequeña proporción asigna **más del 50% de su presupuesto a estos objetivos** (**1,19%**). En cambio, un porcentaje considerable asigna un presupuesto menor, con **un 5% o menos** (**7,14%**), **entre un 6% y 10%** (**4,76%**), o **entre un 11% y 15%** (**2,38%**). Estos datos sugieren que la asignación de presupuesto para la estrategia de ciberseguridad y continuidad de negocio varía ampliamente.

Controles Críticos de Ciberseguridad (CIS Controls)

Es un estándar aprobado y actualizado mediante la Resolución MITIC Nº 277/2020**,** y es un conjunto de acciones priorizadas, ampliamente analizadas y de efectividad probada (basado en los CIS Controls, un estándar internacional reconocido), que deben ser tomados por los OEE para estandarizar, ordenar, priorizar y medir los esfuerzos en ciberseguridad que están llevando a cabo, de modo a construir con un ciberespacio seguro y resiliente y de esta manera mejorar su nivel de ciberseguridad.

La Resolución establece la obligatoriedad de implementar los primeros 6 controles (Controles Básicos) a partir del año 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.

Desde el año 2021 se puso a disposición un sistema único centralizado desde donde los OEE pueden evaluar el cumplimiento de cada control, cargar la evaluación de cumplimiento en la plataforma y generar reportes e históricos de los diagnósticos. De igual manera se cuenta con una planilla de evaluación con una escala de evaluación ponderada si desean realizarla de forma manual.

Según los resultados de la encuesta reciente a los RSI de Instituciones Públicas, la mayoría de las instituciones han realizado diagnósticos o evaluaciones formales del estado de la seguridad de la información con alguna frecuencia. De los encuestados, el **45,24%** afirmó hacer estas evaluaciones **regularmente, de forma anual o más frecuente**, mientras que el **28,57%** dijo haberlas realizado **solo una vez en los últimos dos años**. El **22,62%** declaró que **nunca se habían realizado estas evaluaciones.**

Actualmente, de 156 instituciones de gobierno, 31 equivalente al **20% del total, han utilizado el sistema y completado una evaluación que les permite medir su nivel de madurez en ciberseguridad**, para a partir de allí poder tomar acciones priorizadas encaminadas al mejoramiento de la ciberseguridad.

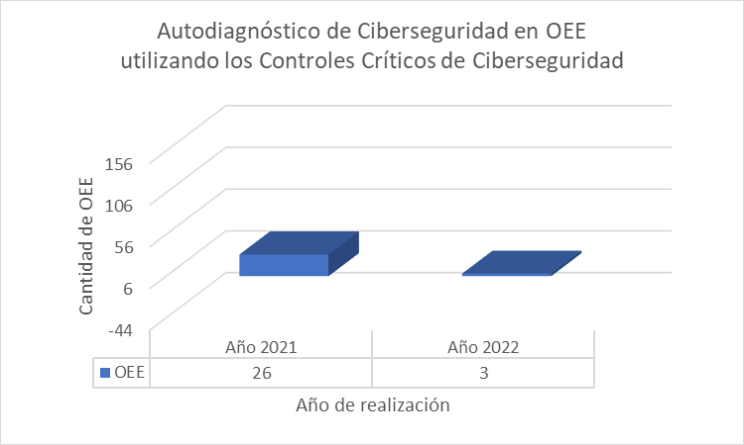


Figura 45. Medición del Nivel de Madurez en Ciberseguridad del año 2022.

Listado de Instituciones públicas que han completado al menos un autodiagnóstico usando el sistema del estándar de los Controles Críticos de Ciberseguridad CIS Controls en los años 2021, 2022, 2023
2021

1. **Administración Nacional de Electricidad (ANDE)**. *Ha realizado 2 evaluaciones, y la última en el 2021 .*
2. **Agencia Espacial del Paraguay (AEP)**. *Ha realizado 1 evaluación.*
3. **Comisión Nacional de Valores (CNV)**. *Ha realizado 2 evaluaciones, y la última en el 2021.*
4. **Compañía Paraguaya de Comunicaciones S.A. (COPACO)**. *Ha realizado 1 evaluación.*
5. **Consejo de la Magistratura (CONMAG)**. *Ha realizado 1 evaluación.*
6. **Defensoría del Pueblo (DP).** *Ha realizado 1 evaluación.*
7. **Dirección General de Estadística, Encuestas y Censos (DGEEC).** *Ha realizado 1 evaluación.*
8. **Dirección Nacional de Transporte (DINATRAN).** *Ha realizado 1 evaluación.*
9. **Empresa de Servicios Sanitarios del Paraguay S.A. (ESSAP).** *Ha realizado 1 evaluación.*
10. **Facultad de Ciencias Exactas y Naturales (FACEN).** *Ha realizado 1 evaluación.*
11. **Facultad de Ciencias Veterinarias (FCV).** ***Ha realizado 1 evaluación.***
12. **Fondo Ganadero (FD).** *Ha realizado 3 evaluaciones, y la última en el 2022.*
13. **Fondo Nacional de la Cultura y las Artes (FONDEC).** *Ha realizado 1 evaluación.*
14. Gabinete Civil de la Presidencia de la República. *Ha realizado 1 evaluación.*
15. **Industria Nacional de Cemento (INC).** *Ha realizado 1 evaluación.*
16. **Instituto Nacional de Tecnología, Normalización y Metrología (INTN).** *Ha realizado 1 evaluación.*
17. **Ministerio de la Niñez y Adolescencia (MINNA)**. *Ha realizado 1 evaluación.*
18. **Ministerio de Relaciones Exteriores (MRE).** *Ha realizado 1 evaluación.*
19. **Ministerio de Tecnologías de la Información y Comunicación (MITIC).** *Ha realizado 2 evaluaciones, y la última en el 2021.*
20. **Secretaría de Desarrollo para Repatriados y Refugiados Connacionales (SEDERREC).** *Ha realizado 2 evaluaciones, y la última en el 2021.*
21. **Secretaría de Emergencia Nacional (SEN).** *Ha realizado 1 evaluación.*
22. **Secretaria de Prevención de Lavado de Dinero o Bienes (SEPRELAD).** *Ha realizado 1 evaluación.*
23. **Secretaría Nacional Anticorrupción (SENAC).** *Ha realizado 1 evaluación.*
24. **Secretaría Nacional por los Derechos Humanos de las Personas con Discapacidad (SENADIS).** *Ha realizado 1 evaluación.*
25. **Servicio Nacional de Calidad y Sanidad Vegetal y de Semillas (SENAVE).** *Ha realizado 3 evaluaciones, y la última en el 2022.*
26. **Tribunal Superior de Justicia Electoral (TSJE).** *Ha realizado 1 evaluación.*
27. **Vicepresidencia de la República del Paraguay.** *Ha realizado 1 evaluación.*

2022

28. **Consejo Nacional de Ciencia y Tecnología (CONACYT).** *Ha realizado 2 evaluaciones, y la última en el 2022.*
29. **Dirección General de los Registros Públicos (DGRP).** *Ha realizado 1 evaluación.*
30. **Dirección Nacional de Contrataciones Públicas (DNCP).** *Ha realizado 2 evaluaciones, y la última en el 2022.*

2023

31. **Secretaría de la Función Pública (SFP).** *Ha realizado 2 evaluaciones, y la última en el 2023.*

Segun la encuesta, acerca del **área que se encarga operativamente de la implementación y mantenimiento de los Controles Críticos de Ciberseguridad: CIS Controls**, arrojo el siguiente resultado: **27,38%** lo realiza **el responsable de Seguridad Informática del área de TICs**, **8,33%** lo hace **el responsable de Seguridad de la Información de la Institución**, **41,67%** indico que **suele ser el área de TICs** la encargada, **13,10% no está definido y/o nadie se encarga**, y el **9,52%** respondio que **otra área o departamento es la encargada.**

Por otra parte, **respecto al área encargada del monitoreo y revisión de los diagnósticos o evaluaciones del estado de la seguridad en la institución**, el **26,19%** de ellos mencionó que **el responsable de Seguridad Informática del área TICs** es quien se encarga de esta tarea. El **11,90%** de los encuestados indicó que es **el responsable de Seguridad de la Información** de la Institución quien se encarga de esto. El **50%** de los encuestados indicó que **no está definido** quién se encarga, **pero suele ser el área de TICs.** Un **5,95%** de los encuestados respondió que **no está definido y nadie se encarga** de ello. Por último, el **5,95%** de los encuestados respondió con **"otro".**

Además, el **23,81%** de los encuestados indico que **realizan una evaluaciones o mediciones de seguridad o riesgo, independientemente del GAP análisis basado en los Controles CIS**, el 41,67% **no realiza ningún control adicional**, y el **34,52% solamente usa los controles CIS.**

Criterios mínimos de seguridad para el desarrollo y adquisición del software

Aprobados y actualizados mediante la Resolución Nº 699/2019 del MITIC, alineado con la "Guí-a de Controles Crí-ticos de Ciberseguridad" establece aquellos criterios de seguridad mí-nimos que una institución debe contemplar en los requerimientos para el desarrollo y adquisición de software e implementaciones con software de terceros, y son aplicables al software desarrollado internamente por las instituciones públicas, adquirido de una empresa o desarrollador tercerizado y/o a través de donaciones a la institución. Los criterios abarcan los siguientes puntos principales:

- Soporte y gestión continua del software
- Gestión segura de usuarios, sesiones y privilegios
- Autenticación y gestión segura de credenciales
- Generación y gestión adecuada de registros de auditoría

- Codificación segura, siguiendo estándares y buenas prácticas reconocidas de la industria (ejemplo: OWASP)
- Utilización de protocolos de red cifrados, basado en protocolos estándar.

Según los resultados obtenidos en la encuesta, respecto cumplimiento de los *Criterios Mínimos de Seguridad de Software en los sistemas desarrollados a medida y/o donados*, el 11,90% indicó que **todos** los sistemas de su institución fueron evaluados y que **todos** cumplen con los criterios mínimos de seguridad de software. Un 19,05% indicó que **todos** los sistemas fueron evaluados y **la mayoría** cumple con estos criterios. Un 7,14% de los encuestados indicó que **todos** los sistemas fueron evaluados y **algunos** cumplen con estos criterios. Por otro lado, el 1,19% de los encuestados indicó que **todos** los sistemas fueron evaluados y **ninguno** cumple. Un 36,90% de los encuestados respondió que **no saben** si se han realizado evaluaciones de cumplimiento en los sistemas. Un 11,90% de los encuestados indicó que se han realizado evaluaciones en **algunos** sistemas, y de estos, la **mayoría** cumple con los criterios mínimos de seguridad de software. Otro 11,90% de los encuestados indicó que se han realizado evaluaciones en **algunos** sistemas, y de estos, **algunos** cumplen con estos criterios.

En cuanto a la **auditoría de vulnerabilidades,** esta normativa no limita que la misma deba 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 a los resultados obtenidos acerca de la realización de pruebas de penetración o auditorías de vulnerabilidad en los sistemas de las instituciones encuestadas, tanto en su infraestructura como en la web, el **1,19%** indicó que **sí** se han realizado pruebas en **todos** sus sistemas, y que **han mitigado** las amenazas encontradas. El **36,90%** de los encuestados indicó que se han realizado pruebas en **algunos** sistemas, y que **han mitigado** las amenazas encontradas. Un **9,52%** de los encuestados indicó que se han realizado pruebas en **algunos** sistemas, pero aún **no han mitigado** las amenazas encontradas. Por otro lado, el **45,24%** de los encuestados indicó que **nunca** han realizado pruebas de penetración o auditorías de vulnerabilidad en sus sistemas. Un **7,14%** de los encuestados respondió "otros".

Además, en el año 2022 el MITIC atendió 10 solicitudes de servicio de auditoría de vulnerabilidades, solicitados por 6 instituciones públicas diferentes, ha disminuido el número de instituciones interesadas en el servicio de auditoría de vulnerabilidades a sistemas web en

relación al año anterior 2021, a pesar de que se ha comunicado a la mayoría de las instituciones sobre la obligación de realizar dichas tareas.

Directivas de Ciberseguridad para Canales de Comunicación oficiales del Estado

Aprobadas mediante la Resolución MITIC N° 432/2019, de uso obligatorio para todos los organismos y entes del Estado tiene como objetivo 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 Responsables de Seguridad de la Información y/o responsables de los Canales de Comunicación del Estado durante el año 2022, sobre el nivel de cumplimiento de la directiva, arrojó el siguiente resultado:

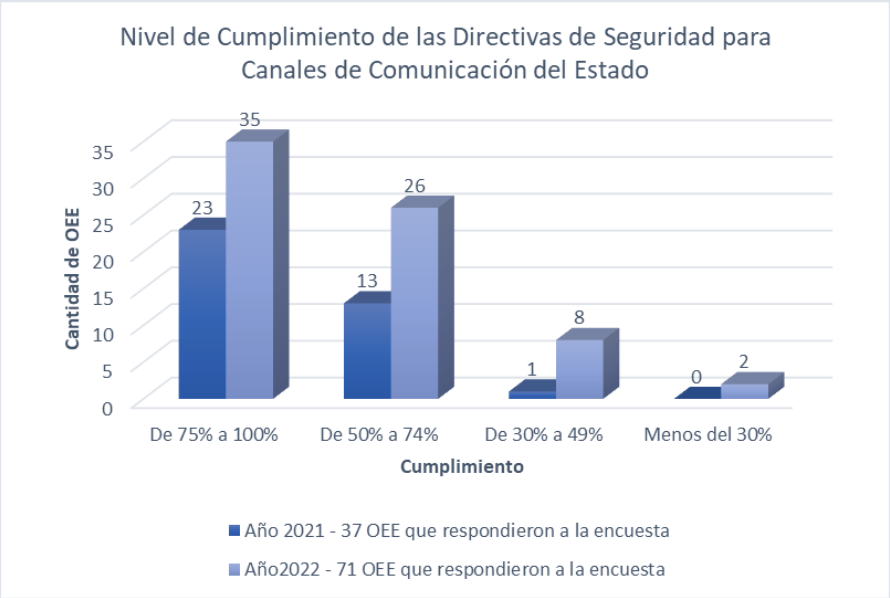


Figura 46. Nivel de cumplimiento Res. MITIC Nro. 432/2020 - Rango de fecha encuestado: Diciembre 2022.

Entre las instituciones con que han declarado un nivel de cumplimiento respecto a esta directiva, con porcentaje mayor al 85% se encuentran: ANNP, CODENA, CONACOM, CNV, COPACO, CSJ, DNCP, ERSSAN, EMG, FONDEC, INC, ITAIPU, MJ, MINNA, MTESS, MADES, SENAD, SEDECO, SENADIS, SFP, TSJE.

Reporte obligatorio de incidentes cibernéticos

Es un reglamento que implementa el reporte obligatorio de incidentes de seguridad por parte de los Organismos y Entidades del Estado, aprobado mediante la Resolución MITIC N° 346/2020, y 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 manejan 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 el año 2022 el CERT-PY recibió el reporte de 1.745 incidentes que corresponden a instituciones públicas. Y, de acuerdo con los datos recopilados en la encuesta, sobre la situación actual de **incidentes de seguridad de la información en los últimos dos años en sus respectivas instituciones**, 38 participantes, que representan el **45,24%** de los encuestados, indicaron que **la Institución ha experimentado algún tipo de Incidente de Seguridad de la Información**. Por otro lado, 41 participantes, lo que representa el **48,81%** de los encuestados, indicaron que **la Institución no ha experimentado ningún Incidente de Seguridad de la Información**. Un pequeño porcentaje de **5,95%** de los encuestados **indicaron desconocer si la Institución ha sufrido algún Incidente de Seguridad de la Información**.

En cuanto al nivel de concienciación del funcionario ***cuando hay sospechas de un Incidente de Seguridad, ¿sabe que hacer? ¿se cuenta con un procedimiento escrito, aprobado y socializado?***, los resultados indicaron que, el **13,10%** de los encuestados **cuentan con un procedimiento institucional escrito, aprobado y socializado** que incluye roles y responsabilidades de todos los involucrados en la gestión de incidentes de seguridad. El **22,62%** respondieron **que tienen un procedimiento interno, pero que solamente contempla las acciones del área de Tecnologías de la Información y Comunicaciones (TIC)**. El **33,33%** de los encuestados indicaron **que no tienen ningún tipo de procedimiento para gestionar incidentes de seguridad.** El **26,19%** de los encuestados respondieron **que no tienen un procedimiento escrito, pero que lo han informado verbalmente**. Un **4,76%** de los encuestados seleccionaron **"Otro".**

Respecto al grado de implementación de la ***Directiva de Protección contra el Ransomware***[18]***,*** el **9,52%** de los encuestados indicaron haber realizado **el 100% de los controles requeridos**. Por otro lado, el **26,19%** aplicó las medidas **parcialmente, al menos en un 50%**, mientras que el **20,24%** las aplicó **parcialmente pero en un porcentaje mayor al 50%**. Sin embargo, también se observa que el **23,81%** de los participantes indicaron haber tomado conocimiento de la Directiva,

[18] https://www.cert.gov.py/wp-content/uploads/2022/02/CIRCULAR_MITIC_01-21.pdf

pero **aún no la han aplicado**. Además, el **20,24%** de los encuestados **afirmaron no tener conocimiento de la existencia de la directiva** en cuestión.

Por otra parte, existe una variedad de respuestas en cuanto a la existencia y estado de un plan de contingencia y continuidad del negocio basado en un análisis de riesgos. Un **9,52%** afirma contar con un plan formal, escrito, aprobado y probado regularmente, lo cual indica que hay una preparación adecuada para hacer frente a situaciones adversas. Por otro lado, un **7,14% i**ndica que sí tienen un plan formal, escrito y aprobado, pero que nunca ha sido probado, lo que podría implicar la necesidad de llevar a cabo pruebas para asegurar su efectividad. Un **51,19%** de los participantes indican que saben qué hacer y lo hacen, pero que no cuentan con un plan formalizado en un documento, lo que sugiere una preparación informal pero sin una estructura documentada. Un **25%** indicó que nunca han desarrollado un plan de contingencia y continuidad del negocio, lo cual podría representar un riesgo en términos de preparación para enfrentar situaciones imprevistas. Finalmente, un **7,14%** mencionó tener una situación distinta a las opciones presentadas.

Formación de capacidades en Ciberseguridad

Uno de los principales ejes de acción del CERT-PY y hoja de ruta en el Plan Nacional de Ciberseguridad, para promover y fomentar el uso seguro de las TIC y la gestión adecuada de la seguridad de la información, es la formación de capacidades en ciberseguridad como una estrategia de fomentar un ecosistema sostenible que pueda abordar los desafíos futuros en materia de ciberseguridad.

Algunas de las acciones llevadas a cabo periódicamente son cursos y talleres técnicos y de concienciación, así como también eventos más generales, como congresos, seminarios, desafíos etc., dirigidos a múltiples sectores como Responsables de Seguridad de la Información del Estado y Directores TIC del Estado, Comunidad de profesionales en TIC y Ciberseguridad, Ciudadanía en Gral, son realizados en forma tanto presencial como en línea debido a las facilidades de este método se ha vuelto común también una asistencia virtual multitudinaria.

Muchas universidades públicas y privadas cuentan con diplomados, especializaciones y maestrías con énfasis o enfoques de seguridad de la información y/o auditoría informática. Así mismo, el MITIC apoya iniciativas como la del Instituto de Altos Estudios Estratégicos que en coordinación entre ambas instituciones, creó el Programa de Especialización en Ciberdefensa y Ciberseguridad Estratégica (PECCE) abierto a todo público interesado. En su cuarta edición del año 2022 contó con 20 nuevos egresados totalizando desde su primera edición 108 egresados.

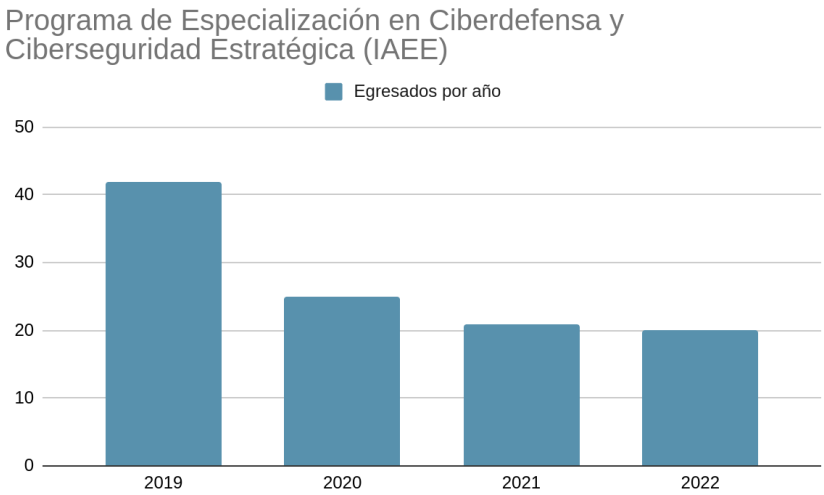


Figura 47. Egresados del IAEE por año.

Además, la ciudadanía en general tiene a disposición desde el año 2021 el curso "Seguridad en los medios digitales" dentro del Portal de Cursos del MITIC: https://www.cursos.gov.py/portada , que cuenta con 15 ediciones recurrentes. El curso agrupa los mínimos temas que todo ciudadano debe conocer para navegar de forma segura y desde su primera edición en noviembre de 2021 hasta diciembre de 2022 cuenta con 1837 participantes y 1228 que aprobaron el curso.

El MITIC fomenta el desarrollo de habilidades de ciberseguridad en las mujeres de la industria de las tecnologías de la información y comunicaciones (TIC), por lo que por tercer año consecutivo Paraguay se sumó al Cyberwomen Challenge en formato virtual, una iniciativa organizada por la Organización de los Estados Americanos (OEA) y Trend Micro que busca contribuir al cierre de la disparidad de género en la industria y disminuir la brecha de especialistas en ciberseguridad. El desafío consiste en un workshop técnico online del tipo "Capture the Flag" de 6 horas de duración que está basado en simulaciones de ciberseguridad y escenarios reales que son completados con la guía de un experto. Las participantes, deben resolver alrededor de 30 desafíos en equipos formados aleatoriamente y competir entre sí para lograr el mayor número de respuestas correctas.

En el 2022, se llevó a cabo la 5ª edición del Cyberwomen Challenge y 3ª en Paraguay y estuvo enfocada en el tema "Identificación de Nivel de Riesgo y la Protección de Infraestructura de Nube", en el cual, 15 participantes conocieron nuevas herramientas que permiten llevar a cabo un análisis sobre los incidentes de seguridad, incrementando la visibilidad y proporcionando un

panorama completo de la evolución de un ataque en vez de verlo en silos. Esto ayuda a minimizar la brecha de investigación de incidentes y agiliza los procesos de análisis y respuesta.

La concienciación en ciberseguridad es un aspecto fundamental para garantizar la protección de la información y la seguridad de una institución. Según los datos recopilados en la encuesta, se observa que las actividades de concienciación en ciberseguridad en Instituciones de Gobierno se realizan con diferentes frecuencias. Un **7,14%** indicó que se llevan a cabo actividades **trimestrales** de concienciación en ciberseguridad. Un **3,57%** señaló que estas actividades se realizan de manera **semestral**. Por otro lado, un **40,48%** de los encuestados indicó que se lleva a cabo **una vez al año**. Un **35,71%** respondió que **nunca** han realizado actividades de concienciación en ciberseguridad en la institución. Un **13,10%** mencionó "otro" como respuesta, lo que podría indicar la existencia de algunas prácticas diferentes en términos de frecuencia de actividades de concienciación en ciberseguridad.

Ranking en Ciberseguridad Global y en las Américas

El **National Cyber Security Index (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. De acuerdo al NCSI, Paraguay se sitúa actualmente en la posición N° 44 a nivel internacional, y en 1° lugar en Latinoamérica, alcanzando un cumplimiento del 64%.

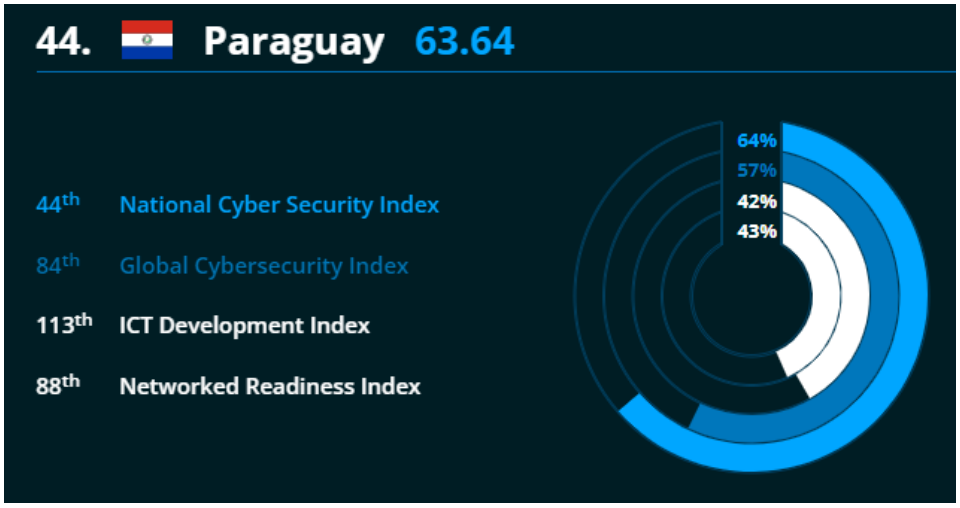


Figura 48. Posicionamiento de Paraguay en el ranking NCSI 2022

Actualmente, el índice abarca un total de 161 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 para Paraguay, de acuerdo a este índice en la última edición, se encuentran en los indicadores relativos a la protección de servicios digitales privados (20%), así como también la protección de datos personales (25% 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), servicios de identificación digital y confianza (100% de cumplimiento), y respuesta a ciber incidentes (89% de cumplimiento).

Respecto al año anterior, se ha observado una mejoría en los indicadores relativos a operaciones cibernéticos en el ámbito militar (de 17 a 50% de cumplimiento).

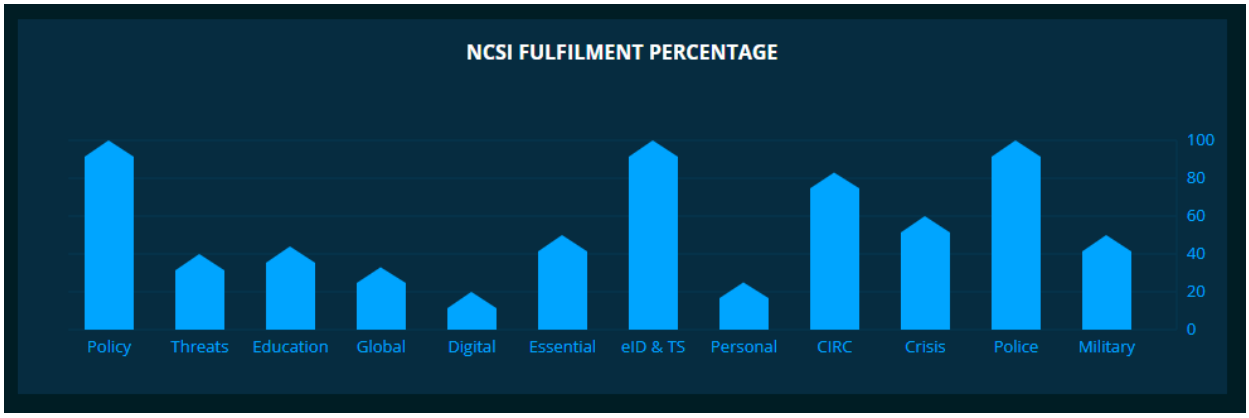


Figura 49. Nivel de cumplimiento de indicadores de NCSI por área 2022

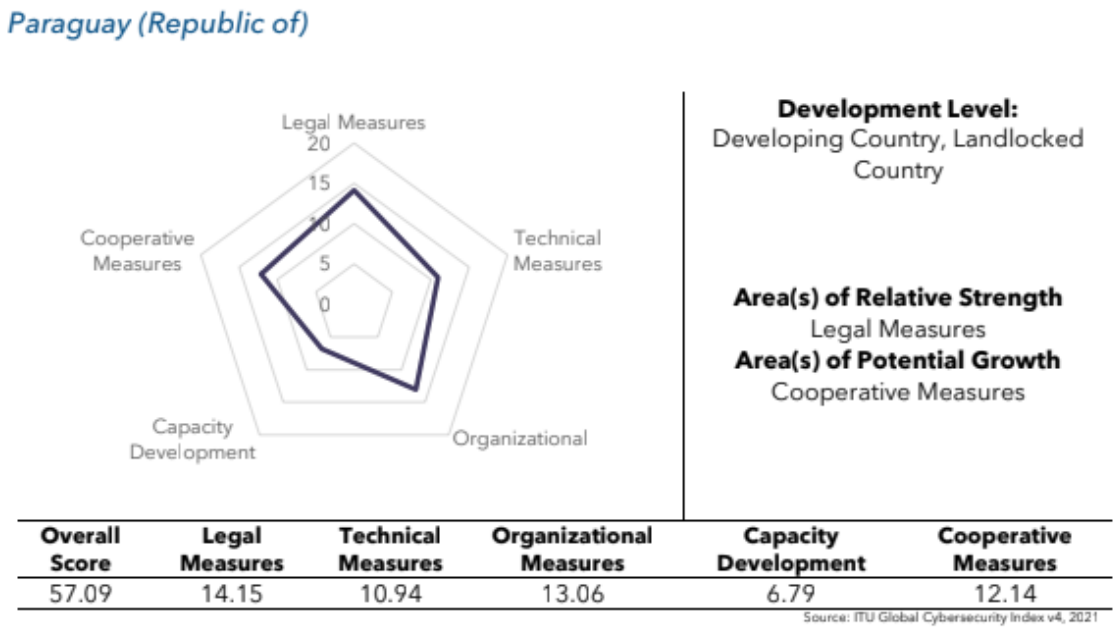
Para este estudio, la información correspondiente a Paraguay fue obtenida en primer lugar por parte de funcionarios de la organización en Estonia a partir de las fuentes públicas, y fue complementada con información proveída por el MITIC. A la fecha de la publicación del presente informe, es el único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

En la última edición del Índice de Ciberseguridad Global (ICG) de la Unión Internacional de Telecomunicaciones (UIT), elaborado por la Unión Internacional de Telecomunicaciones (ITU), publicada en el 2020, muestra un compromiso creciente en todo el mundo para afrontar y reducir las amenazas a la ciberseguridad. Paraguay se posiciona en el puesto 84, de un total de 182 países, con un cumplimiento del 57 % de los indicadores de dicho estudio y en el puesto 11 de un total de 35 países en Latinoamérica. La información para este estudio es proveída por parte de Conatel, organismo representante de Paraguay ante la ITU.

Los 5 pilares fundamentales que forman parte de los componentes básicos inherentes de una cultura nacional de ciberseguridad con actores multidisciplinarios abarca el GCI se basan en medidas:

- Legales
- Técnicas
- Organizacionales
- Formación de capacidades
- Cooperación

Cabe destacar que este estudio no es comparable en relación a las ediciones anteriores, debido a que la participación, metodología e indicadores difieren de forma a que no es posible reflejar la realidad.



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
57.09	14.15	10.94	13.06	6.79	12.14

Source: ITU Global Cybersecurity Index v4, 2021

Figura 50. Nivel de cumplimiento de indicadores de NCSI para Paraguay

La segunda edición del año 2020, y la última de la publicación del **Informe "Ciberseguridad: Riesgos, Avances y el Camino a seguir en América Latina y el Caribe"** 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 autoevaluación 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:

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

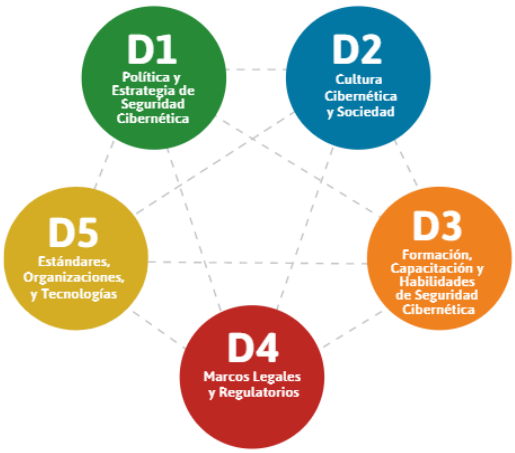


Gráfico 2: Las cinco dimensiones del CMM

Figura 51. Las cinco dimensiones del CMM

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.