CIBERSEGURIDAD EN PARAGUAY

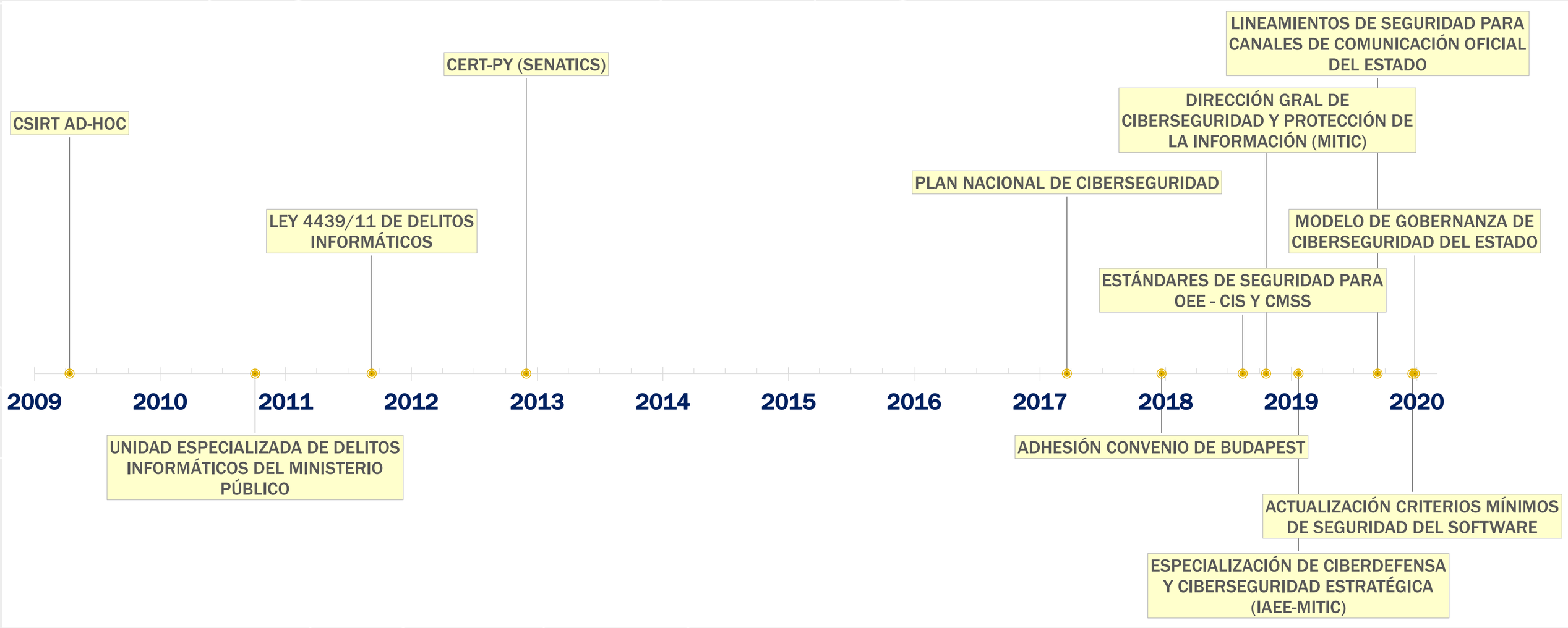
SITUACIÓN ACTUAL, PROYECTOS Y DESAFÍOS FUTUROS

#TRANSFORMACIÓNDIGITAL

Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

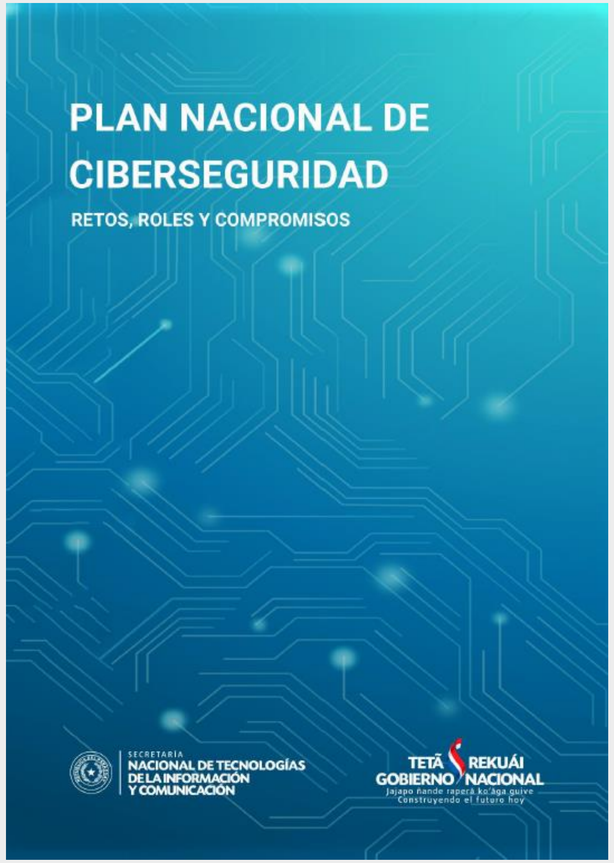
GOBIERNO NACIONAL

Antecedentes – Primeros esfuerzos en ciberseguridad

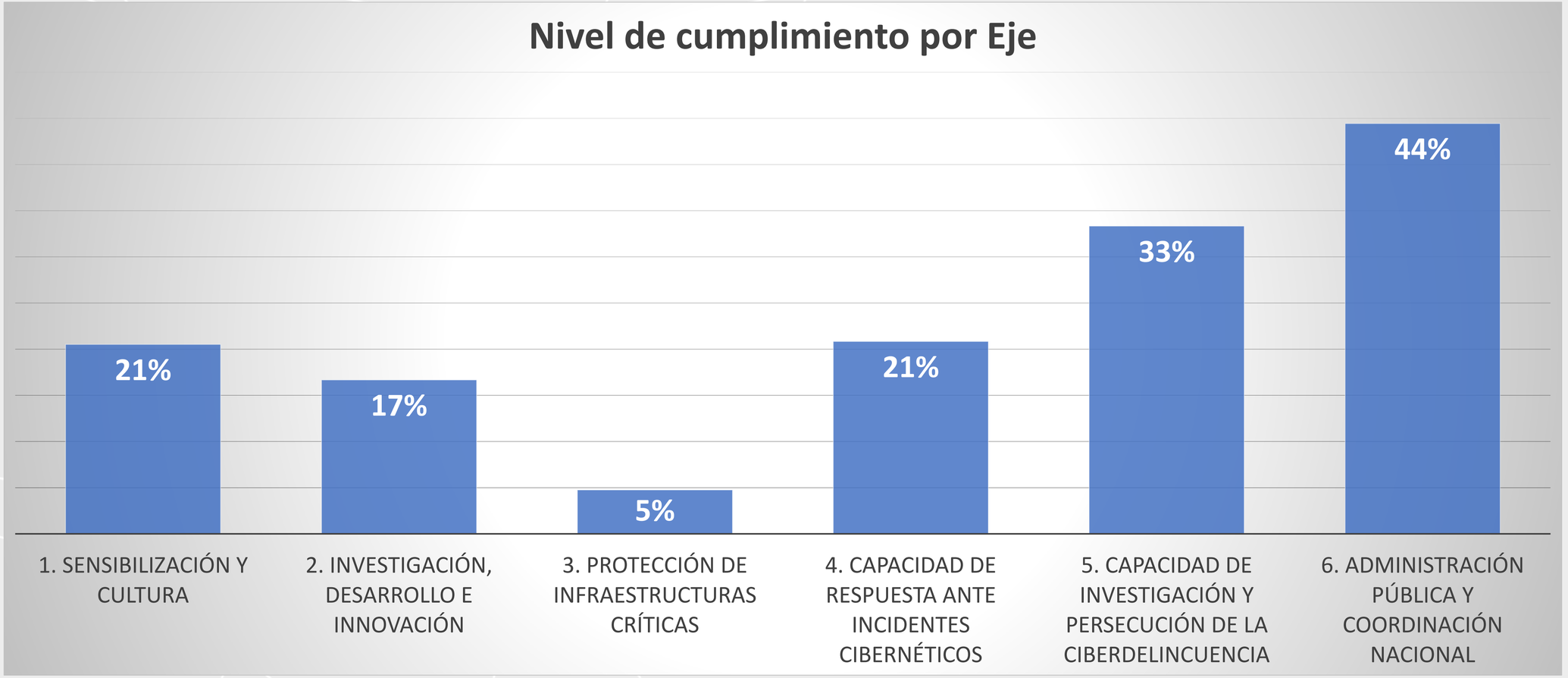


PLAN NACIONAL DE CIBERSEGURIDAD

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



PLAN NACIONAL DE CIBERSEGURIDAD



Plan Nacional de Ciberseguridad – Responsabilidad MITIC

- CERT-PY + SOC
- Alertas y boletines
- Intercambio de información de ciberseguridad

- Políticas, estándares, directivas
- Auditorías y gestión de vulnerabilidades
- Soluciones y sistemas de seguridad

- Campañas
- Cursos y talleres
- Congresos, seminarios y eventos de networking
- Ciberejericios y competencias
- Fomento de capacidades

- Modelo de Gobernanza de Ciberseguridad
- Plan Nacional de Ciberseguridad
- Coordinación interinstitucional

Servicios de Ciberseguridad proveídos por el MITIC

- Gestión de incidentes cibernéticos
- Boletines y alertas de Ciberseguridad
- Auditoría de vulnerabilidades
- Ciberejercicios – Simulacro de ciberataques

Algunos son solo para el Estado y solo puede ser solicitado por parte del RSI designado oficialmente

http://servicios.mitic.gov.py

Gestión de incidentes cibernéticos

INCIDENTE CIBERNÉTICO: Violación o amenaza inminente de violación a una política de seguridad de la información implícita o explícita, así como un hecho que comprometa la seguridad de un sistema (confidencialidad, integridad o disponibilidad)

- Software malicioso (Malware)
- Acceso sin autorización a cuentas / sistemas / datos
- Denegación de servicios (DoS/DDoS)
- Escaneo / Fuerza bruta
- Correo no deseado malicioso (Spam/Scam)
- Engaños (Phishing)
- Compromiso de Sistemas
- Ransomware

Obligatoriedad para OEEs de reportar incidentes cibernéticos (art. 44 / DP 2274)

abuse@cert.gov.py

https://www.cert.gov.py/servicios/gestion-de-incidentes-ciberneticos

DELITO INFORMÁTICO VS. INCIDENTE CIBERNÉTICO

Ministerio Público
República del Paraguay

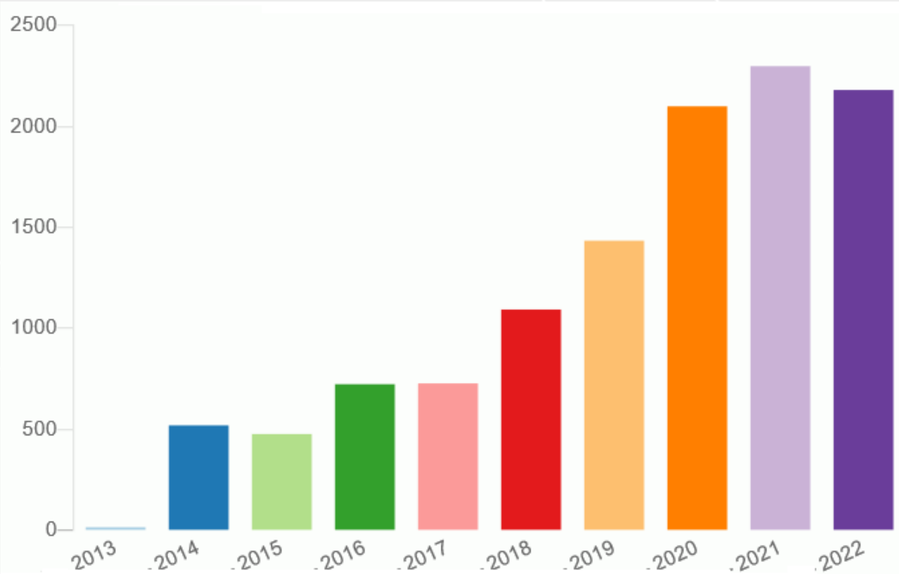
Fiscalía con la gente

CENTRO DE RESPUESTAS ANTE INCIDENTES CIBERNÉTICOS

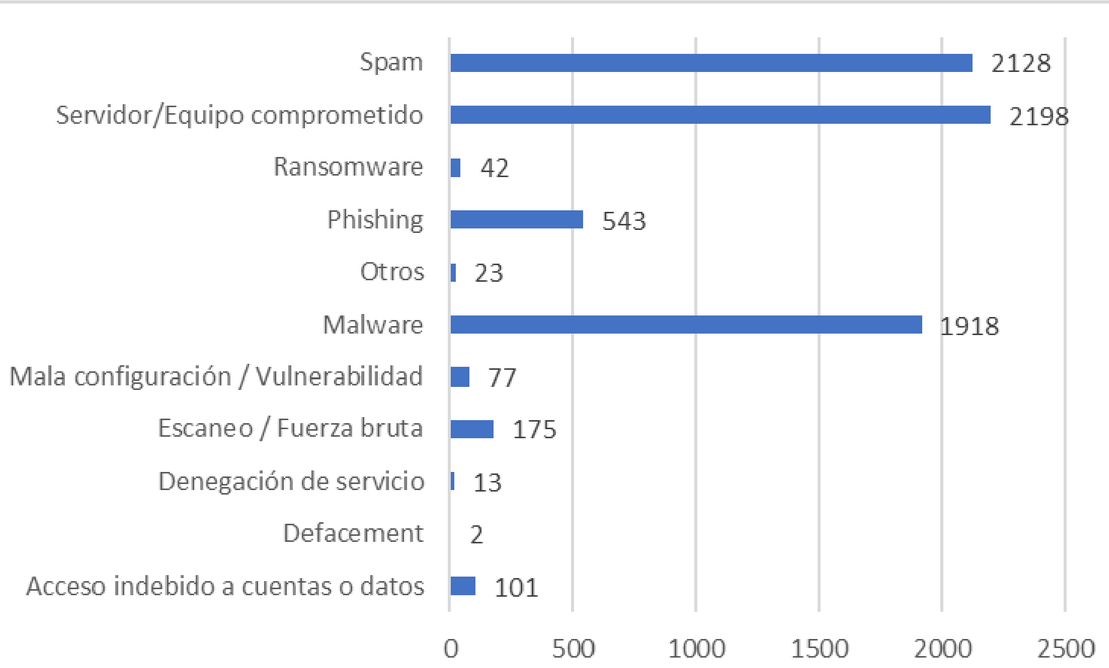
CERT-PY

Gestión de Incidentes Cibernéticos

25/09/2013 - 17/08/2022	
Reportes recibidos	11.566
Incidentes único atendidos	4.722
Investigaciones, coordinaciones y gestiones únicas	18.072



Created Year	Total de tickets
2013	14
2014	519
2015	476
2016	723
2017	727
2018	1093
2019	1434
2020	2100
2021	2299
2022	2181
Total	11566



https://www.cert.gov.py/application/files/7616/1521/7981/Informe_Ciberseguridad_Paraguay_2020_-_final-2.pdf

Boletines y alertas de ciberseguridad

Avisos reactivos ante amenazas que se consideran de alto riesgo para el ecosistema digital nacional (sistemas de información de instituciones públicas, empresas privadas o en los hogares)

- Página web: https://www.cert.gov.py/index.php/boletines
- Mailing list: https://cert.us5.list-manage.com/subscribe?u=3d17d9fcd0f236ff532fa0981&id=93edd5410a
- Twitter CERT-PY: https://twitter.com/certpy
- Facebook CERT-PY: https://www.facebook.com/CERT.Paraguay

Ministerio de TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

TETÃ REKUÁI GOBIERNO NACIONAL

BOLETÍN DE ALERTA

Boletín Nro.: 2019-01
Fecha de publicación: 30/04/19.
Fecha de actualización: 31/05/19
Tema: Explotación masiva de vulnerabilidades en ZIMBRA

Sistemas afectados:
Zimbra Colaboration Suite (ZCS).

Descripción:

Recientemente se han reportado múltiples co
explotación masiva de las vulnerabilidades CV
2019-9621. Varios CSIRTs regionales han inforr
estas vulnerabilidades.

¿Qué hay detrás de los engaños de Whatsapp?

23 abr. 2019 15:13

Nuevamente se ha detectado una oleada de engaños mediante mensajes de Whatsapp, esta vez fue con un anuncio de dinero disponible en nombre del Ministerio del Trabajo. No es la primera vez que vemos campañas falsas como ésta: como las ofertas de dinero siempre son interesantes, los ciberdelincuentes...

Fallo crítico en SQLite podría afectar a miles de apps

19 dic. 2018 14:18

El grupo Blade de Tencent ha descubierto un fallo de seguridad en SQLite, que permite realizar RCE, o provocar rupturas inesperadas del programa que utiliza este servicio.

Actualizaciones para múltiples productos Apple

https://www.cert.gov.py/servicios/boletines-y-alertas-de-ciberseguridad

Auditoría de vulnerabilidades de Sistemas Web

Pruebas de seguridad orientadas a encontrar fallas o debilidades en sistemas de software web del Estado

- Servicio bajo demanda
- Solo para sistemas con arquitectura web
- Exclusivo para OEEs
- Aplica a:
  - Aplicaciones web nuevas, antes de que entren a producción
  - Aplicaciones web existentes que todavía no hayan sido auditadas
- No es un pentesting – no hay explotación-persistencia

TIPOS:

- **Prueba externa:**
  - Blackbox
  - Greybox
- **Verificación de cumplimiento de criterios de seguridad del software**

https://www.cert.gov.py/servicios/auditoria-de-vulnerabilidades-de-sistemas-web

Lineamientos y directivas en materia de ciberseguridad

- Decreto Presidencial 2274/2018 – Capítulo 4 Ciberseguridad
- Modelo de Gobernanza de Seguridad de la Información en el Estado (Res. MITIC N° 733/2019)
- Controles críticos de Ciberseguridad (Res. MITIC 277/2020)
- Controles mínimos de seguridad del software (Res. MITIC Nº 699/2019)
- Reglamento de Reportes Obligatorios de Incidentes cibernéticos de Seguridad en el Estado (Res. MITIC 432/2020)
- Directivas de Ciberseguridad para Canales de Comunicación oficiales del Estado (Res. MITIC N° 432/2019)

Desafío actual → **Cumplimiento**

https://www.cert.gov.py

https://www.presidencia.gov.py/archivos/documentos/DECRETO2274_30nobos1.PDF

Gobernanza de la Seguridad de la Información en el Estado

Toda OEE debe contar con área de Seguridad de la Información, que reporte directamente a la Máxima Autoridad, transversal a todas las áreas de la institución

Objetivo del área de Seguridad de la Información:

- Velar por la seguridad de todos los activos de información de la institución en cuanto a su confidencialidad, integridad y disponibilidad.

- Modelo de gobernanza descentralizada
- Punto focal de coordinación con el MITIC en temas de ciberseguridad

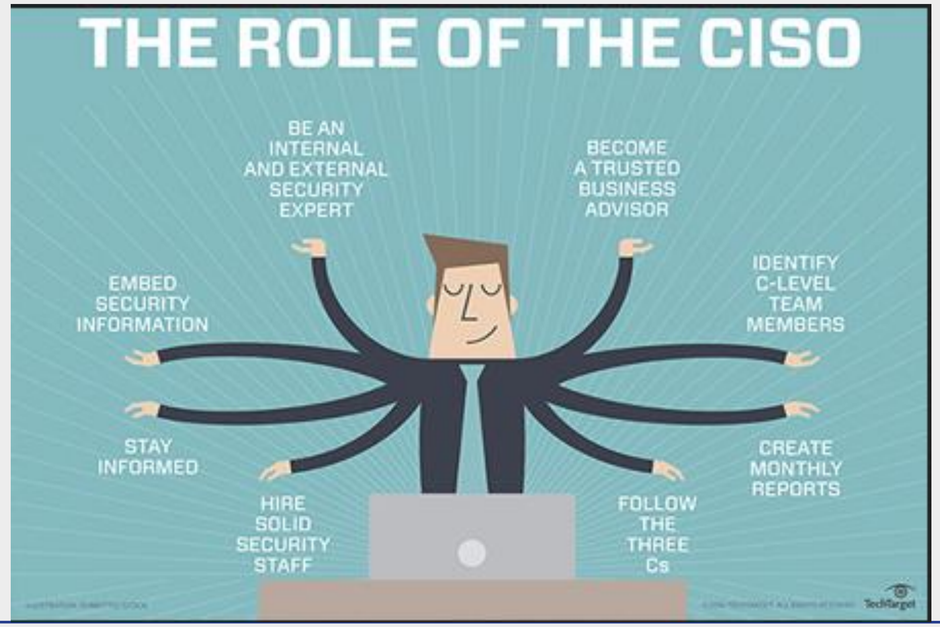
https://www.cert.gov.py/application/files/4815/8263/6300/RESOLUCION_MITIC_N_733-2019_-_Modelo_de_Gobernanza.pdf

Roles y Responsabilidades

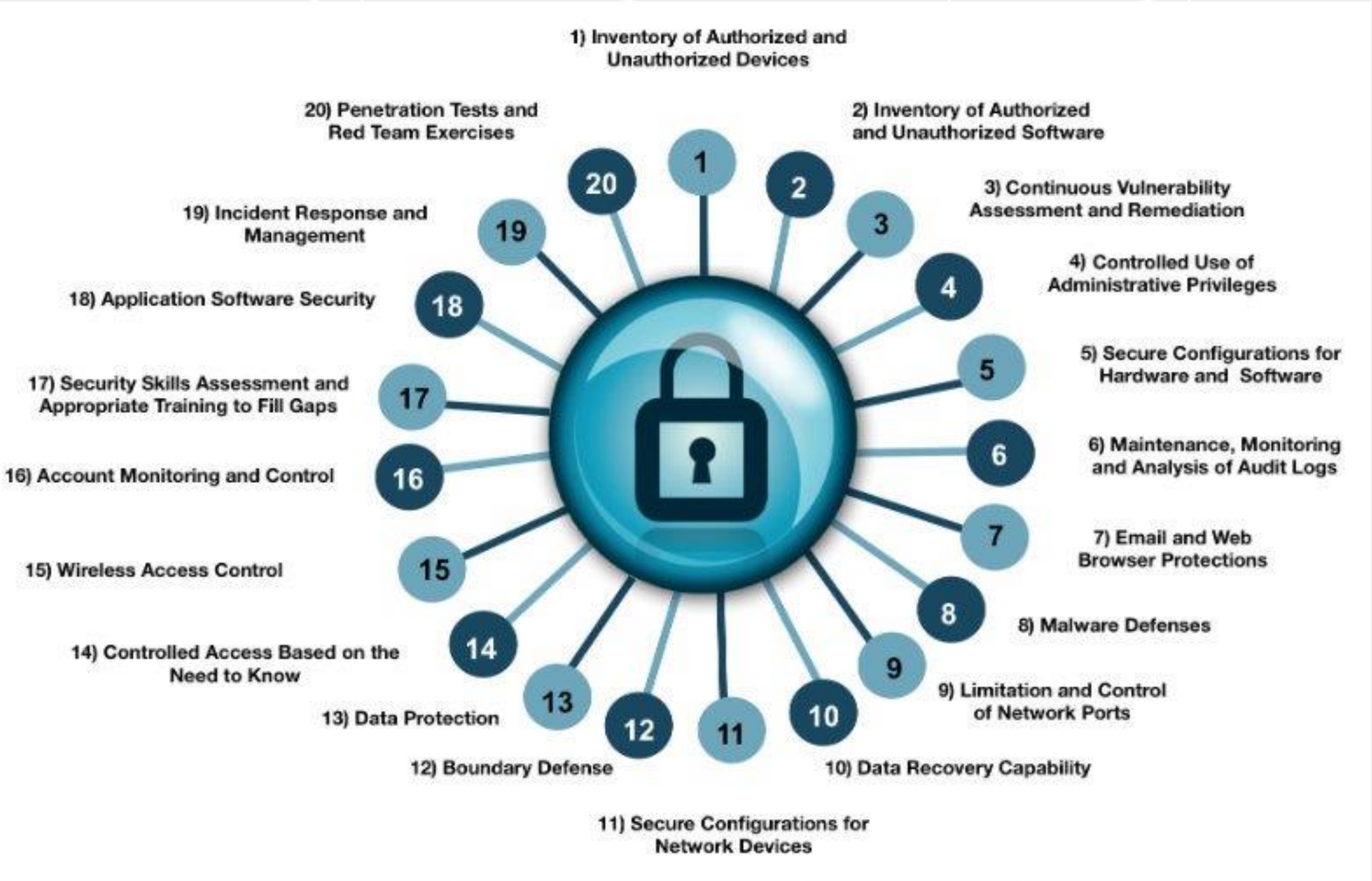
- Identificar y evaluar los **riesgos** y las **brechas** que afectan a los activos de información de la institución y proponer planes y controles para gestionarlos,
- Elaborar y velar por la implementación de un **plan o estrategia de seguridad** de la información,
- Elaborar, proponer y velar por el cumplimiento de las **políticas de seguridad** de la información de la institución,
- Proponer los planes de **continuidad de negocio** y **recuperación de desastre**s, 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.

Características ideales del área de Seguridad de la Información

- Debe poder reportar a la Máxima Autoridad
- Independiente de las áreas de Tecnologías o TIC (pero coordinado)
- No sustituye a Seguridad Informática, Seguridad TICs u otras áreas operativas
- Transversal y coordinado con todas las áreas de la institución - Capacidad de articulación
  - TIC / Informática
  - Comunicación
  - Legal / Jurídico
  - RRHH
  - Usuarios / Áreas operativas en general
- Habilidades blandas, formación continua, etc.



Controles Críticos de Ciberseguridad



- Alineado al eje 6 (Admin. Pública), objetivo 6.b, (Gestión coordinada), línea de acción 6.b.3
- Controles mínimos, priorizados y prácticos
- 20 controles - 171 subcontroles
- Basado en estándares de industria y comunidad (CSI Critical Security Control version 7)
- Instrumento de medición común para instituciones
- GAP Analysis anual

Promedio cumplimiento → 27 %

28 OEE han informado al menos un GAP Analysis

https://www.cert.gov.py/controles-criticos-seguridad

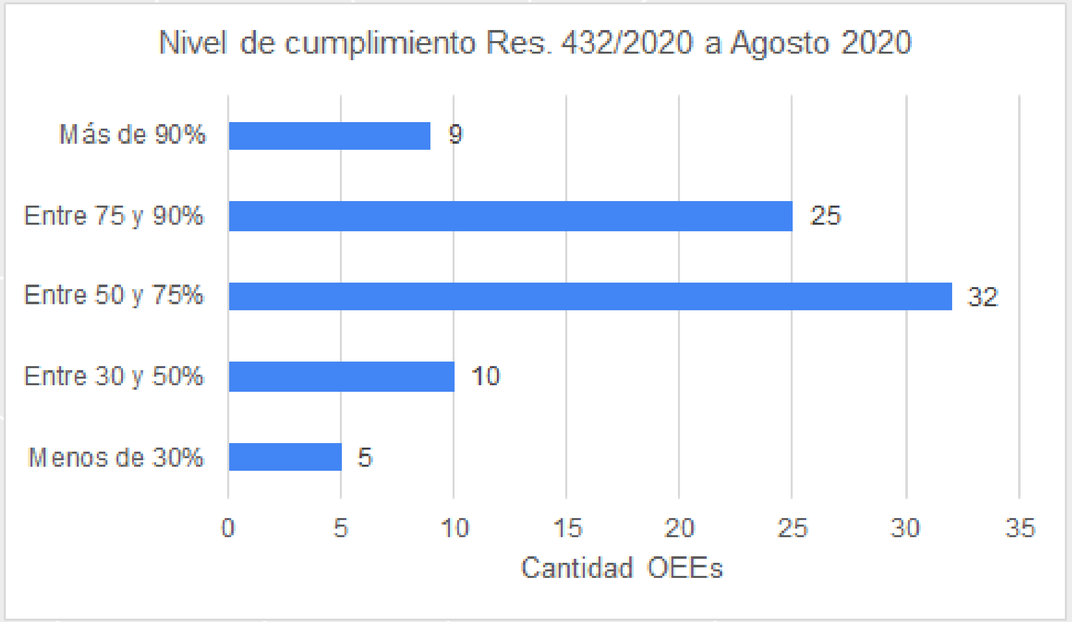
Criterios mínimos de seguridad para el desarrollo y adquisición del software

- Requerimientos mínimos, alineados a la "Guía de Controles Críticos de Ciberseguridad".
- Aplicable al software desarrollado y/o implementado “a medida”
  - Internamente por la institución
  - Adquirido de una empresa o desarrollador tercerizado
- NO es retroactivo
- Estándar aprobado por DNCP
- Auditoría de vulnerabilidades antes de entrar a producción

https://www.cert.gov.py/criterios-minimos-de-seguridad-de-software

Directivas de Ciberseguridad para Canales de Comunicación oficiales del Estado

- Aplica a a todas las cuentas de canales de comunicación oficiales del Estado:
  - Cuentas de redes sociales (Facebook, Twitter u otros)
  - Cuenta de correo electrónico institucional
  - Fanpage o canales administrados con cuentas particulares



https://www.cert.gov.py/*directivas-de-ciberseguridad-para-canales-de-comunicacion-oficiales-del-estado*

Formación de Capacidades

- Seminarios y Congresos
- Cursos:
  - Taller avanzado de Ciberataques
  - Cursos cortos
  - Curso “Seguridad en medios digitales”
- Webinar
- Simulacros y ciberejercicios
  - Simulacro de ciberataque para el sector financiero
  - Servicio de ciberejercicios para usuarios de instituciones públicas
- Especialización de Ciberdefensa y Ciberseguridad Estratégica – MITIC – IAEE
- Campañas de Concienciación de Ciberseguridad
- Programa MITIC – ENI – 51 cursos de ciberseguridad

Más de 2500 personas capacitadas en Ciberseguridad en los últimos 6 años

Formación de Capacidades

AGENDA DIGITAL

Fase 3 Mediano/Largo Plazo
Proyectos y servicios nuevos
2023-2025

SOC implementado y operativo 100%

Servicios operativos 100%

Ecosistema de ciberseguridad fortalecido

Mercado de ciberseguridad en crecimiento

Fase 2 Corto/Mediano Plazo
Proyectos y servicios básicos nuevos
2021-2022

- 21 Proyectos enmarcados en pilares del Plan Nacional de Ciberseguridad
- Planificación de proyectos a mediano/largo plazo
- Cooperación técnica SOC

Fase 1 Corto Plazo
Reanudación y fortalecimiento de servicios operativos permanentes
2019-2020

- Gestión de incidentes
- Boletines y alertas
- Auditorías vulnerabilidades

Tiempo de respuesta 48 hs
15 publicaciones, aumentar alcance 30%
30 sistemas de Gobierno

Inversión ≈ 4.000.000 USD

MUCHAS GRACIAS!

Presidencia de la
REPÚBLICA
del PARAGUAY

GOBIERNO
NACIONAL

mitic.gov.py