INICIATIVAS DE CIBERSEGURIDAD EN PARAGUAY

#TRANSFORMACIÓNDIGITAL

Ministerio de
TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN

GOBIERNO
NACIONAL

Nuevo rol, nuevas atribuciones

Secretaría
NACIONAL DE TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN

Ministerio de
TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN

Viceministerio de Tecnologías de la Información y Comunicación

Viceministerio de Comunicaciones

Conectividad e Infraestructura

Gobierno Electrónico

Inclusión Digital y TICs en Educación

Innovación Productiva y Economía Digital

Ciberseguridad y Protección de la Información

Nuevo rol, nuevas atribuciones

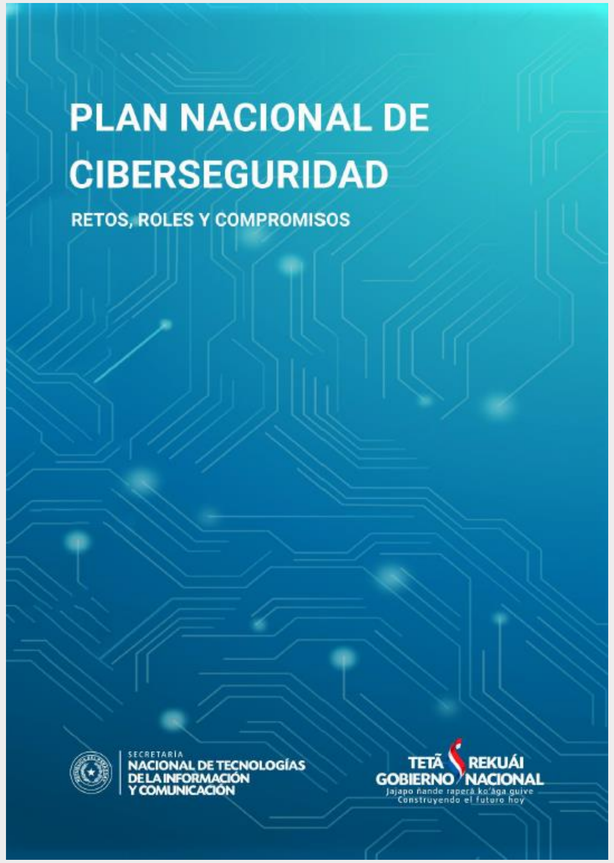
- ✓ Construcción de un **ecosistema digital seguro**, **confiable** y **resiliente**, incluyendo el sector público, privado, academia y ciudadanía.
- ✓ **Políticas** de protección de la información personal y gubernamental.
- ✓ **Protección** de sistemas, redes, procesos e información de los organismos y entidades del **Estado**.
- ✓ Planes y **estrategias** de ciberseguridad a nivel **nacional**
- ✓ **Autoridad** en Ciberseguridad, prevención, gestión y control de **incidentes cibernéticos**
- ✓ Definición y protección de la **Infraestructura tecnológica crítica**

Objetivos Estratégicos

- **Proteger los sistemas de información del Gobierno y la Infraestructura crítica**
- **Crear un ecosistema e industria de ciberseguridad**
- **Construir la capacidad de hacer frente a las ciberamenazas**
- **Fomentar la concienciación y construir capacidades 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 – 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

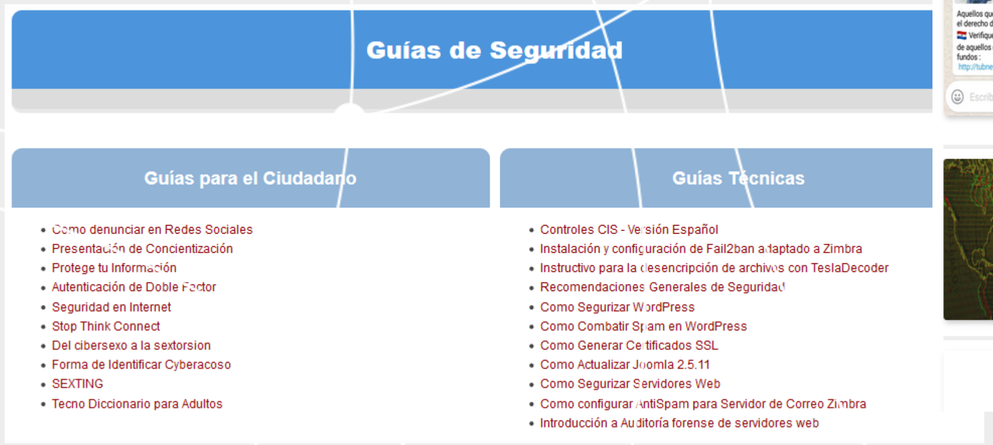
- Modelo de Gobernanza de Ciberseguridad
- Plan Nacional de Ciberseguridad
- Coordinación interinstitucional

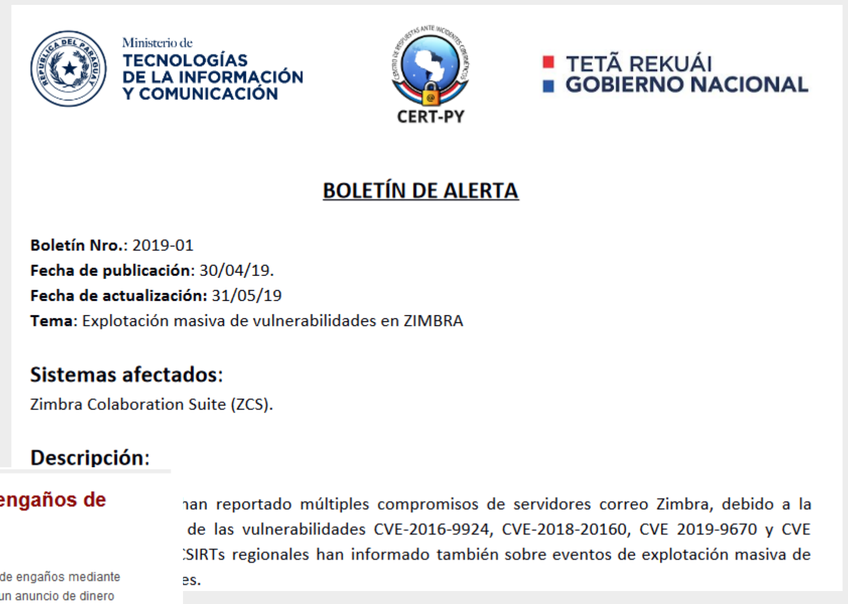
Gestión de Incidentes Cibernéticos

Periodo: 17/12/2013 - 19/06/2019	
Reportes recibidos	4241
Incidentes nuevos atendidos	418
Investigaciones realizadas	612

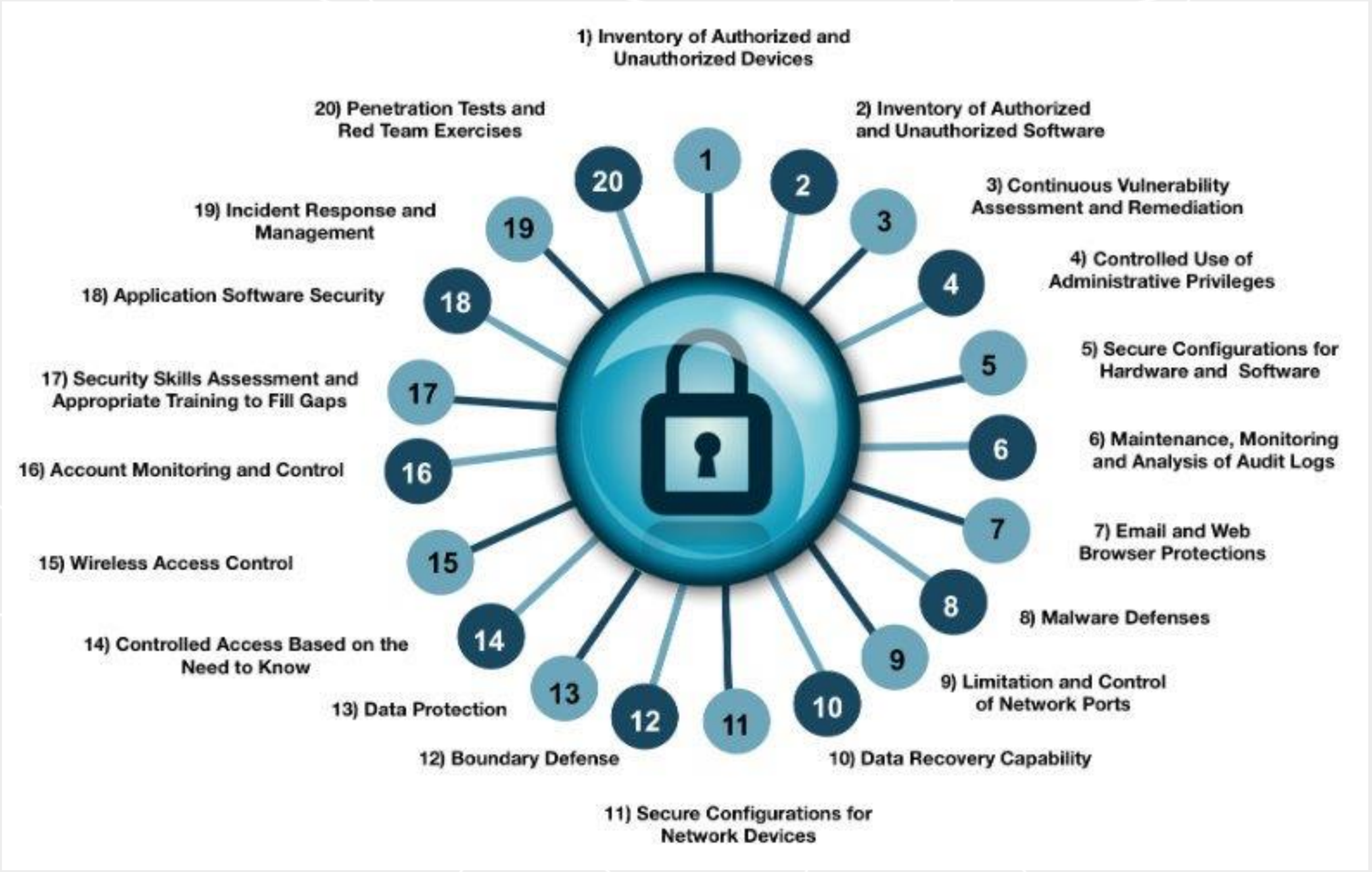
Servicios preventivos

- Auditorías de vulnerabilidades
- Difusión de boletines y noticias de ciberseguridad





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

Promedio cumplimiento ⇨ 16%

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

Nuevos lineamientos y directivas en materia de ciberseguridad

- Directivas de Ciberseguridad para Canales de Comunicación oficiales del Estado
- Modelo de Gobernanza de Seguridad de la Información en el Estado
- Manual de Políticas de Seguridad de la Información para Instituciones Gubernamentales
  - Política de Protección de Contraseña
  - Política de Uso seguro del Correo Electrónico
  - Politica de Proteccion de los puestos de trabajo
  - …

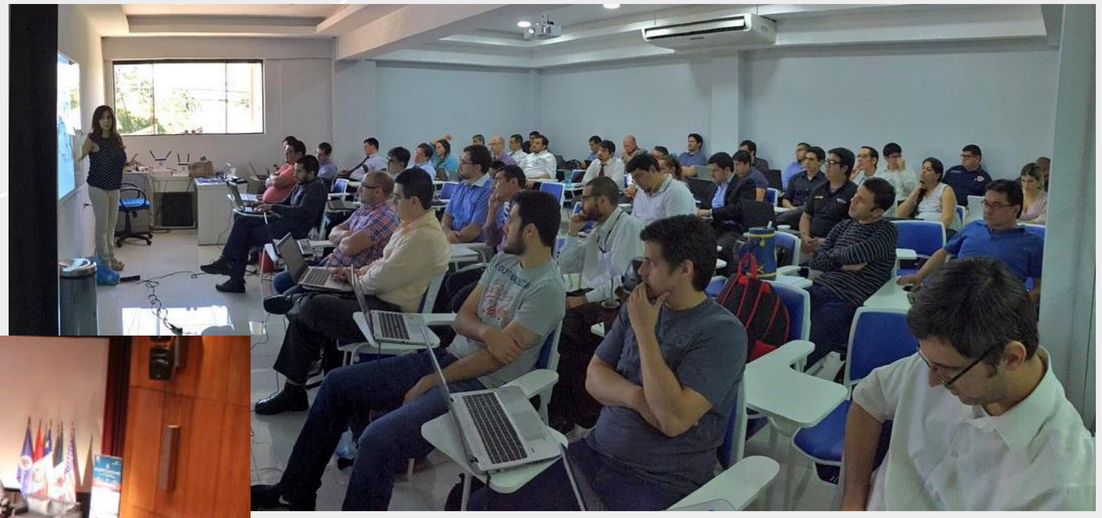
Resoluciones próximas a aprobarse, conforme Decreto N° 2274

Formación de Capacidades

- Seminarios y Congresos
- Cursos:
  - Taller avanzado de Ciberataques
  - Cursos cortos
- 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

Más de 500 personas capacitadas en Ciberseguridad en los últimos 5 años

Formación de Capacidades



AGENDA DIGITAL

Fase 3 Mediano/Largo Plazo
Proyectos y servicios nuevos
2021-2023

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
2019-2020

- 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

- Gestión de incidentes
- Boletines y alertas
- Auditorías vulnerabilidades

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

Inversión ≈ 7.000.000 USD

MUCHAS GRACIAS!

Presidencia de la
REPÚBLICA
del PARAGUAY

GOBIERNO
NACIONAL

mitic.gov.py