



INICIATIVAS DE CIBERSEGURIDAD EN PARAGUAY

#TRANSFORMACIÓNDIGITAL



Ministerio de
**TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN**

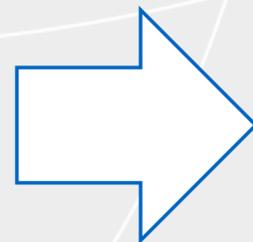
 **GOBIERNO
NACIONAL**



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**

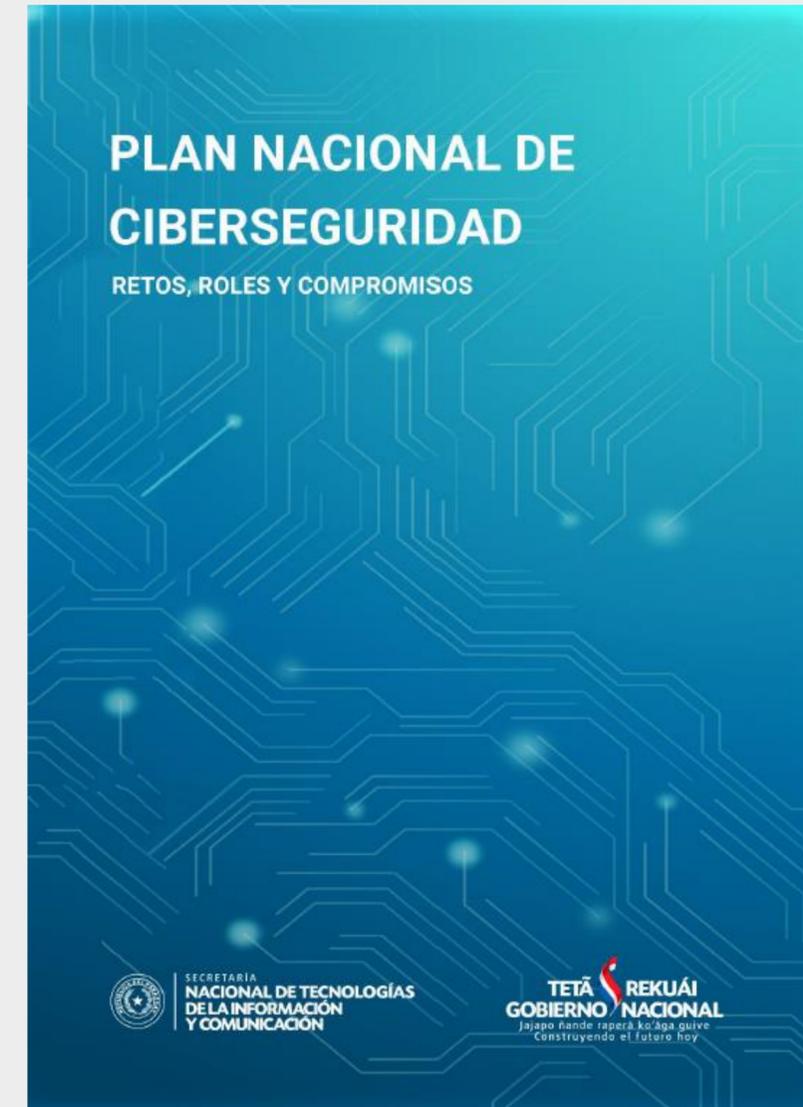
Objetivos Estratégicos

- **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

Gestión de incidentes

Protección de Infraestructura crítica y Gobierno

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

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

Concienciación y capacitación

Sistema Nacional de Ciberseguridad

- 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



Ministerio de
**TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN**



**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 Collaboration Suite (ZCS).

Descripción:

han reportado múltiples compromisos de servidores correo Zimbra, debido a la de las vulnerabilidades CVE-2016-9924, CVE-2018-20160, CVE 2019-9670 y CVE .SIRTs regionales han informado también sobre eventos de explotación masiva de es.

Guías de Seguridad

Guías para el Ciudadano

- Como denunciar en Redes Sociales
- Presentación de Concientización
- Protege tu Información
- Autenticación de Doble Factor
- Seguridad en Internet
- Stop Think Connect
- Del cibersexo a la sextorsion
- Forma de Identificar Cyberacoso
- SEXTING
- Tecno Diccionario para Adultos

Guías Técnicas

- Controles CIS - Versión Español
- Instalación y configuración de Fail2ban adaptado a Zimbra
- Instructivo para la descriptura de archivos con TeslaDecoder
- Recomendaciones Generales de Seguridad
- Como Segurizar WordPress
- Como Combatir Spam en WordPress
- Como Generar Certificados SSL
- Como Actualizar Joomla 2.5.11
- Como Segurizar Servidores Web
- Como configurar AntiSpam para Servidor de Correo Zimbra
- Introducción a Auditoría forense de servidores web



¿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.

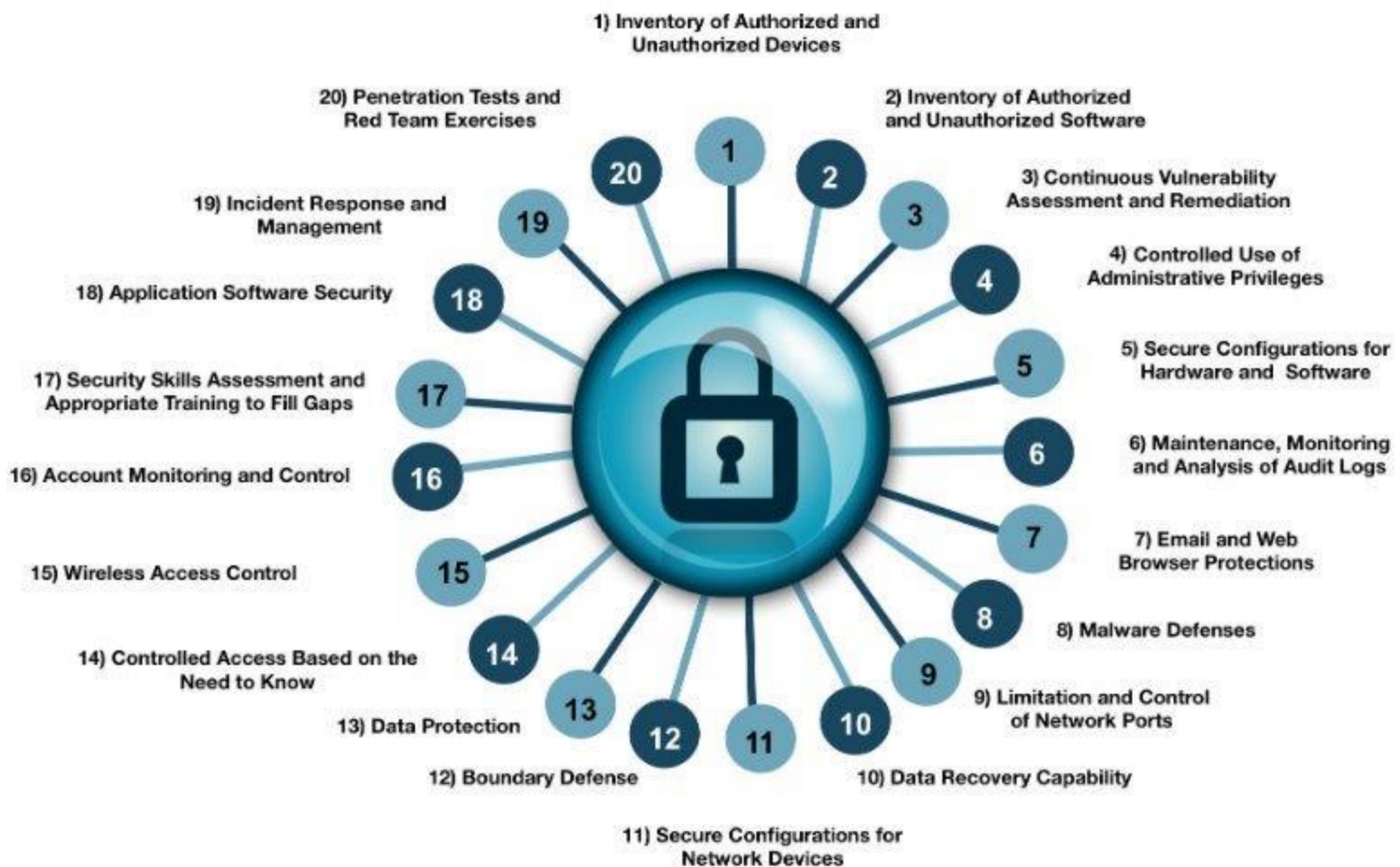
Actualizaciones para múltiples productos Apple

Regístrese para recibir nuestros

Boletines de Seguridad

 **Suscripción**

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
 - Política de Protección 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



AGENDA DIGITAL





MUCHAS GRACIAS!



Presidencia de la
REPÚBLICA
del **PARAGUAY**

 **GOBIERNO**
NACIONAL

mitic.gov.py

