SUBCOMITE DE CIBERSEGURIDAD DE LA ADMINISTRACIÓN PÚBLICA

1ª Reunión - Julio 2020

#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

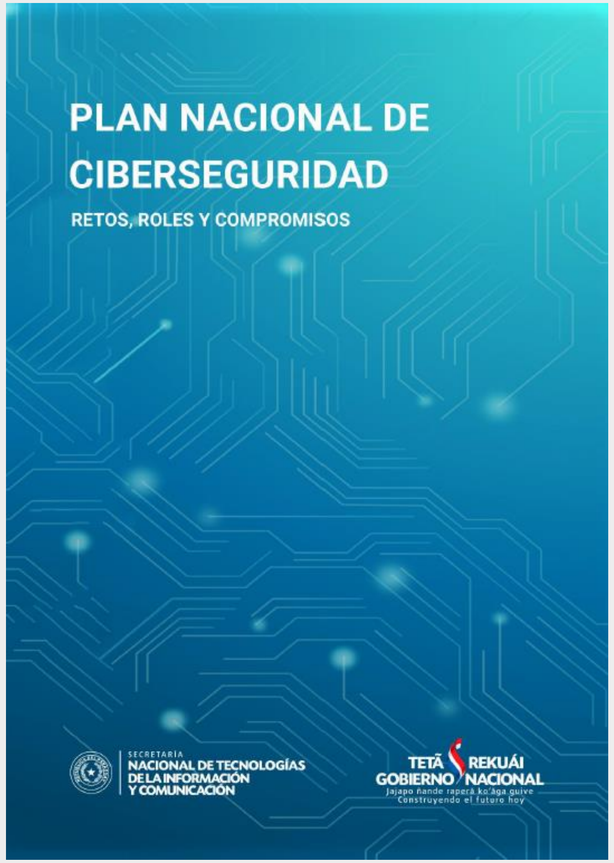
- ✓ Construcción de un **ecosistema digital seguro**, **confiable** y **resiliente**, incluyendo el sector público, privado, academia y ciudadanía.
- ✓ **Políticas** de protección de la información personal y gubernamental.
- ✓ **Protección** de sistemas, redes, procesos e información de los organismos 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



Eje Administración Pública – Objetivos y Líneas de acción

6.a.) La administración pública cuentan con una infraestructura adecuada en términos de TICs y ciberseguridad.

- Directrices y estándares para adquisición de productos y servicios TIC
- Especificaciones específicas de seguridad y estandarización de redes y sistemas
- Unidades Especializadas de Ciberseguridad

6.b.) Las gestiones gubernamentales de ciberseguridad se coordinan con cada agente responsable consciente de su función y papel referente a la ciberseguridad.

- Sistema Nacional de Ciberseguridad
- Asociación de profesionales del área dentro de la Administración Pública
- Buenas prácticas, guías y lineamientos de Ciberseguridad en el Gobierno
- Procedimientos y canales de comunicación directos entre instituciones

6.c.) Se promueve la cooperación entre los sectores público y privado.

- Convenios público-privado para intercambio de información de incidentes

6.d.) Se fortalece la cooperación regional e internacional en materia de ciberseguridad.

- Intercambio de información regional e internacionalmente

Sub-comité de Ciberseguridad de la Administración Pública

Compuesto por todos los Responsables de Seguridad de la Información de los OEE

- Grupo de trabajo colaborativo
- Foro de intercambio de conocimiento
- Instancia de coordinación de acciones e iniciativas de ciberseguridad en el Gobierno

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

Lineamientos y directivas en materia de ciberseguridad

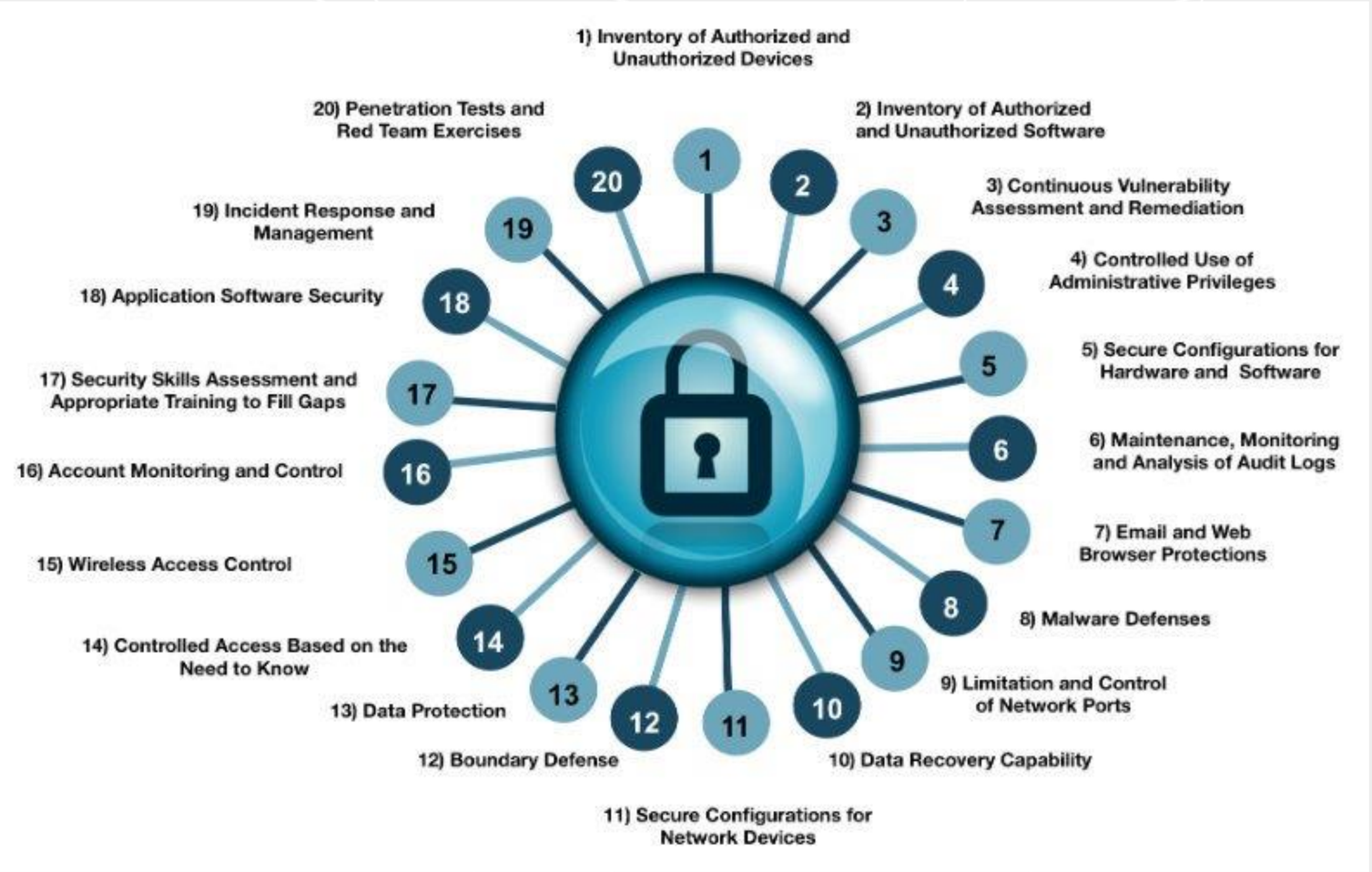
- Decreto Presidencial 2274/2018 – Capítulo 4 Ciberseguridad
- Controles críticos de Ciberseguridad (Res. MITIC 277/2020)
- Controles mínimos de seguridad del software (Res. MITIC N° 699/2019)
- Directivas de Ciberseguridad para Canales de Comunicación oficiales del Estado (Res. MITIC N° 432/2019)
- Modelo de Gobernanza de Seguridad de la Información en el Estado (Res. MITIC N° 733/2019)

Desafío actual → **Cumplimiento**

https://www.cert.gov.py

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

Controles Críticos de Ciberseguridad



- Basado en estándares de industria y comunidad (CSI Critical Security Control version 7)
- Controles mínimos, priorizados y prácticos
- 20 controles - 171 subcontroles
- Instrumento de medición común para instituciones
- Controles básicos obligatorios desde el 13/02
- GAP Analysis anual

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
- Vinculado al Estándar de software (MITIC / 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
- Encuesta de cumplimiento – Circular MITIC 01/2020
  - Fecha límite: 28/02/2020
  - Validación por parte de RSI

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

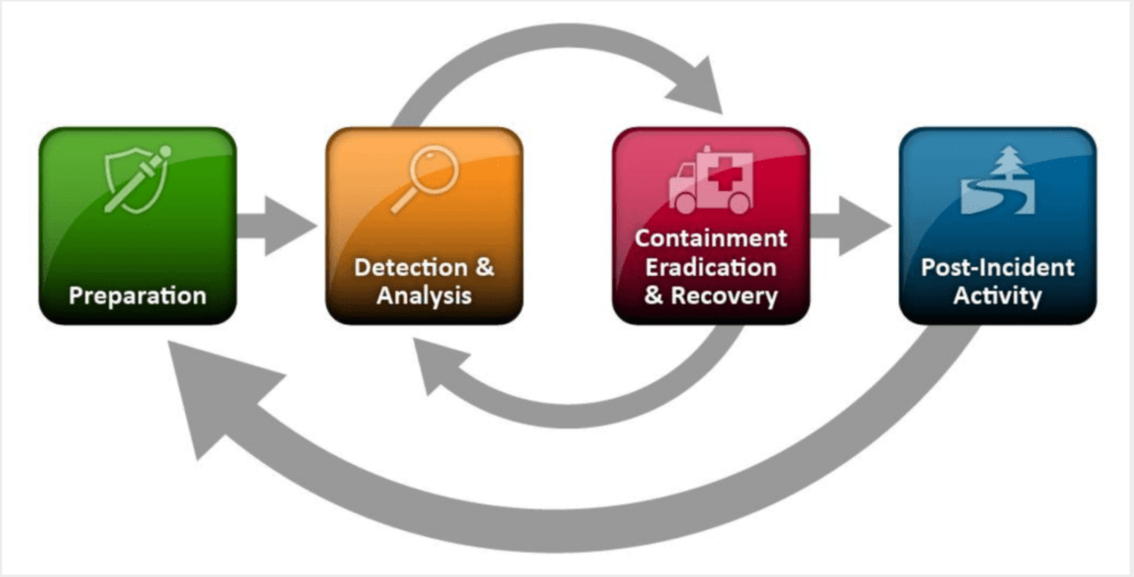
Servicios de Ciberseguridad proveídos por el MITIC

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

Gestión de incidentes cibernéticos

INCIDENTE CIBERNÉTICO: 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

- 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



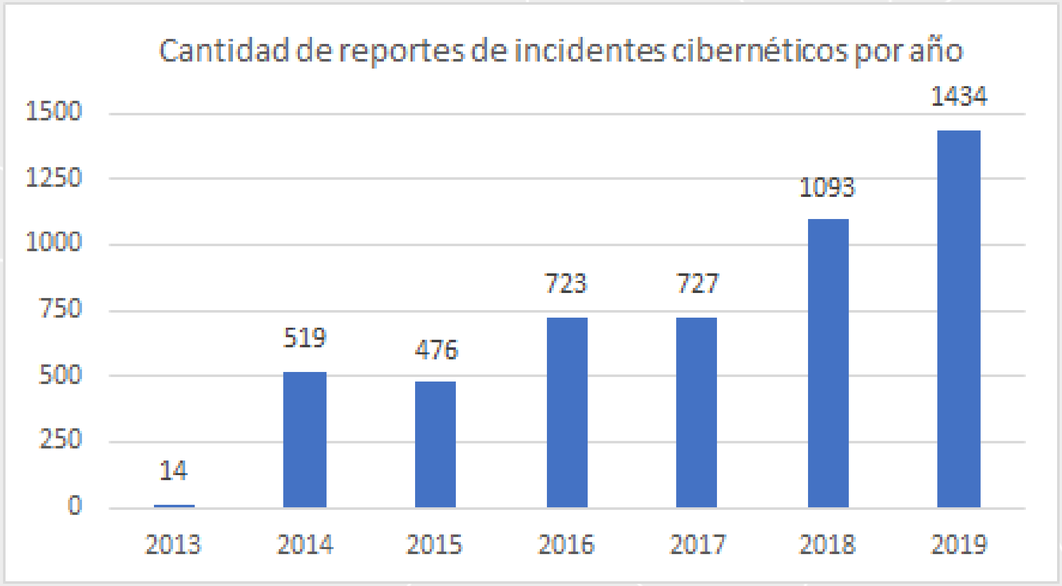
Obligatoriedad para OEEs de reportar incidentes cibernéticos (art. 44 / DP 2274)

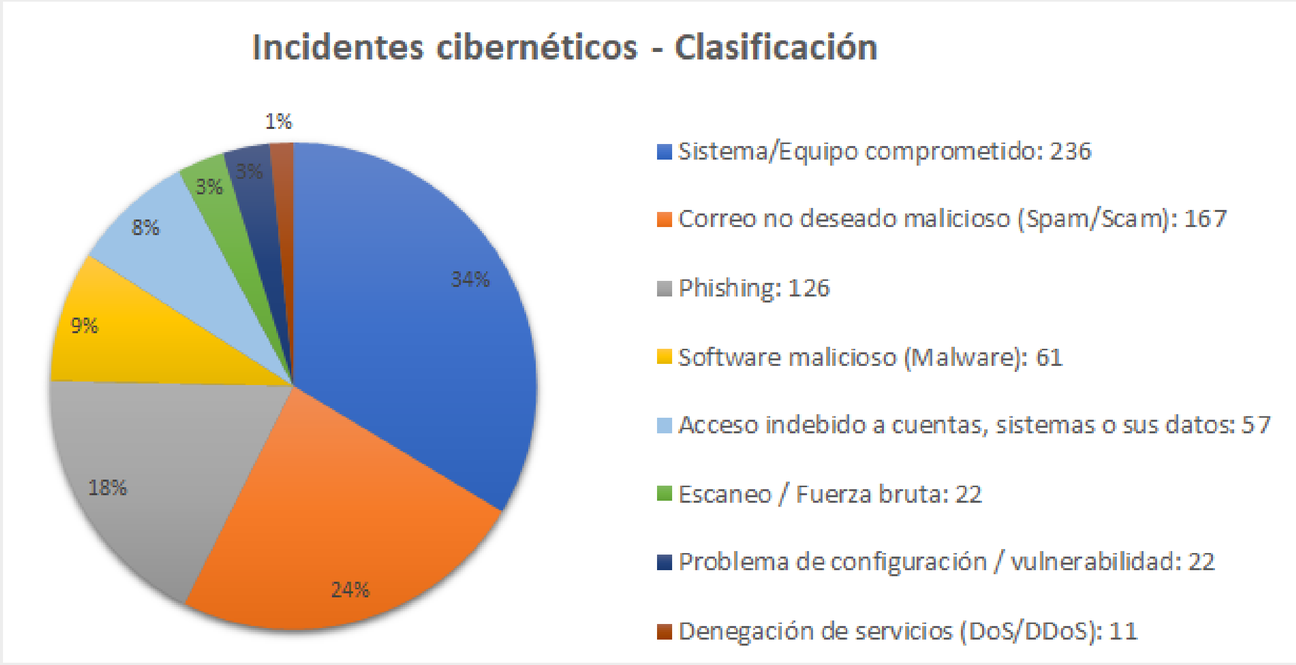
abuse@cert.gov.py

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

Gestión de Incidentes Cibernéticos

Periodo: 25/09/2013 - 20/07/2020	
Reportes recibidos	6143
Incidentes nuevos atendidos	1130
Investigaciones realizadas	4487





https://www.cert.gov.py/application/files/6515/8256/8110/Informe_Ciberseguridad_Paraguay_2019_-_final.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 repor
explotación masiva de las vu
2019-9621. Varios CSIRTs regi
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

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

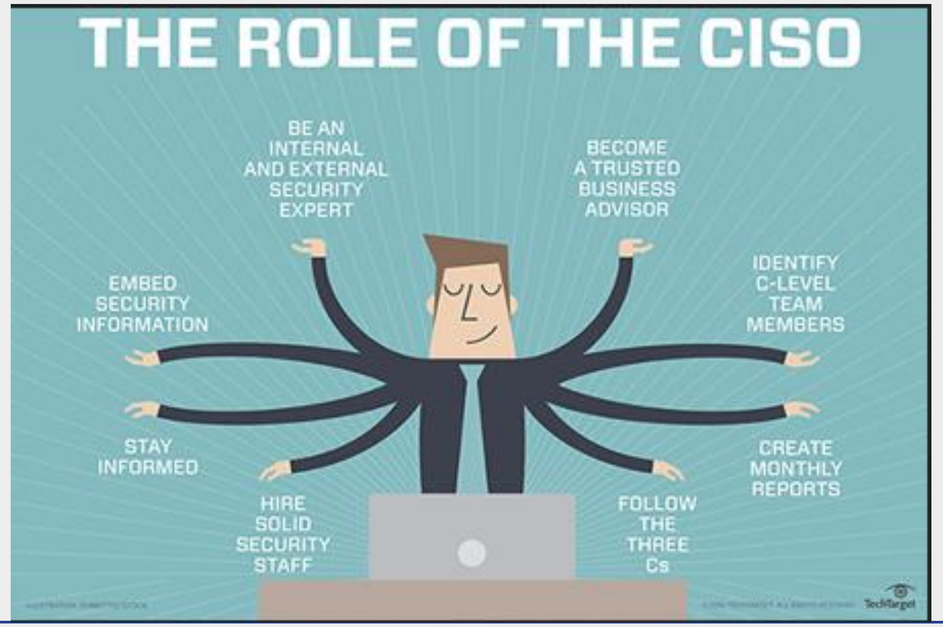
https://www.cert.gov.py/application/files/4815/8263/6300/RESOLUCION_MITIC_N_733-2019_-_Modelo_de_Gobernanza.pdf

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.



Primeros pasos recomendados

- Fortalecimiento del equipo humano – buscar talentos internos en la institución
- Conocer dónde estamos parados – auto-evaluación Controles críticos de Ciberseguridad
- Establecimiento de objetivos concretos, priorizados en base al resultado de la auto-evaluación y medibles
  - ✓ Lograr mayor visibilidad y control sobre activos (equipos, red, sistemas)
  - ✓ Mapear sistemas existentes y analizar su estado de vulnerabilidades
  - ✓ Mejorar conciencia de usuario + reglas de uso claras, simples, …
  - ✓ …
- Apoyo en servicios de CERT-PY / MITIC

Próximos pasos

- Próximas reuniones / talleres sobre temas específicos
  - Lineamientos de gestión y coordinación de incidentes cibernéticos
  - Controles críticos de ciberseguridad (medición, implementación)
  - Criterios mínimos de seguridad en sistemas de software en el Estado
  - …
- Validación de encuesta de cumplimiento de Directivas de ciberseguridad para canales de comunicación oficiales del Estado
- Envío de encuestas voluntarias para estudio sobre temas varios de interés (DevOps, estado actual de normativas aprobadas, …)

MUCHAS GRACIAS!

Presidencia de la
REPÚBLICA
del PARAGUAY

GOBIERNO
NACIONAL

mitic.gov.py
cert.gov.py