SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

PLAN NACIONAL DE CIBERSEGURIDAD

Un desafío compartido

"La verdadera seguridad se halla más bien en la solidaridad que en el esfuerzo individual aislado"
Fiódor Dostoyevski

Ciberseguridad: Riesgos y Amenazas

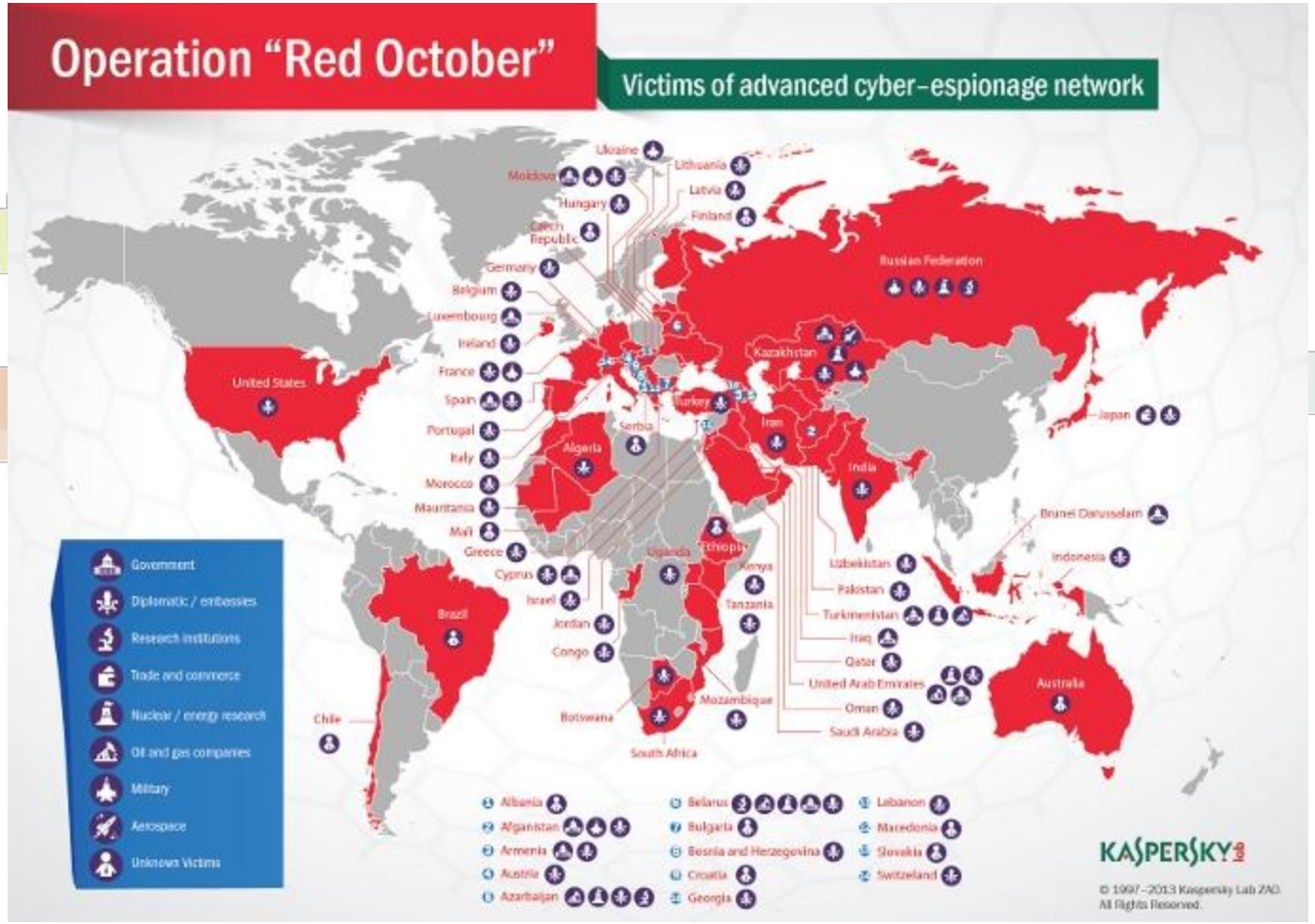
SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Ciberataques alrededor del mundo (I)

Ciberataques alrededor del mundo (II)



Algunos primeros esfuerzos

- CSIRT ad-hoc
- Creación de Unidad Especializada de Delitos Informáticos del Ministerio Público
- Creación y puesta en marcha del CERT-PY
- Modificación de la Legislación (Ley 4439/11)
- Formación en seguridad de la información:
  - Certificaciones como CCNA Security, CEH, CISSP, etc.
  - Maestría en TICs con énfasis en Auditoría y Seguridad de la Información
- Adhesión al Convenio de Budapest
- Campañas de concientización:
  - Conectate Seguro
  - Fiscalía en la Escuela

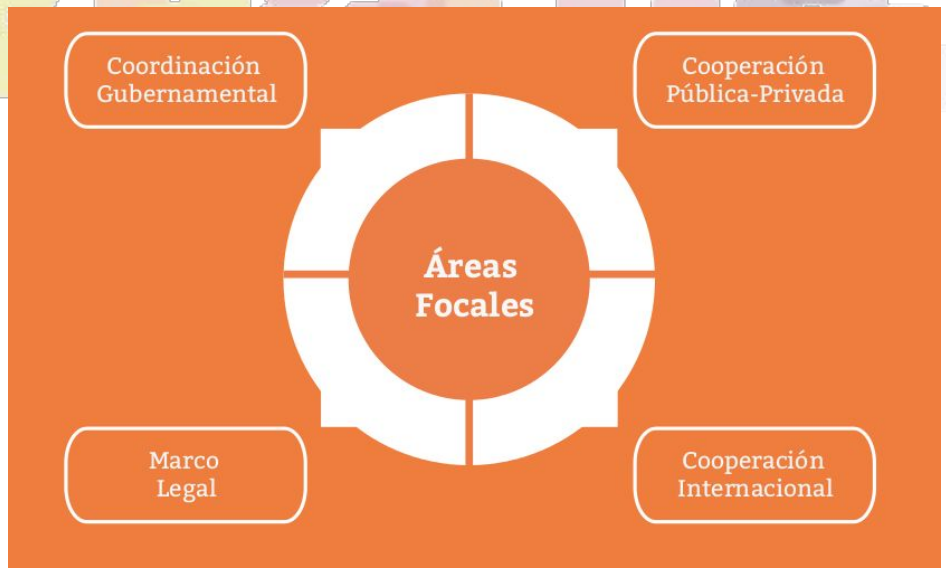
SECRETARÍA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

¿Qué es el Plan Nacional de Ciberseguridad?

Es la base de políticas gubernamentales y nacionales que establece las líneas de acción a ser adoptados por una nación para fortalecer la seguridad de sus activos críticos y lograr un ciberespacio seguro, confiable y resiliente.



¿Por qué un Plan Nacional?

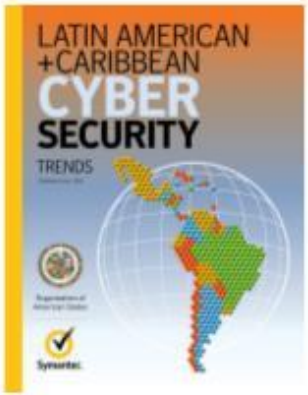
- La evolución de la sofisticación de los ataques cibernéticos debe ser respondida de manera **dinámica y proporcional**.
- Sin una respuesta estratégica, los esfuerzos nacionales en materia de seguridad cibernética serán **insostenibles, esporádicos, duplicados e ineficientes**.
- Una c**reciente dependencia** de los gobiernos sobre las TICs y el ciberespacio.

Beneficios de un Plan Nacional de Ciberseguridad

Aspectos claves para una estrategia exitosa

1. Compromiso en niveles clave: encontrar una persona que propugne la estrategia
2. Dónde estamos: hacer un balance y evaluación.
3. Dónde queremos llegar en 5-10 años.
4. Identificar e involucrar a actores claves.
5. Identificar los pasos y los hitos: la planificación de acciones.
6. Asegurar objetivos medibles y alcanzables: revisión y ajuste.
7. Estimación del costo de las actividades.

Una misma Estrategia no sirve para todos..

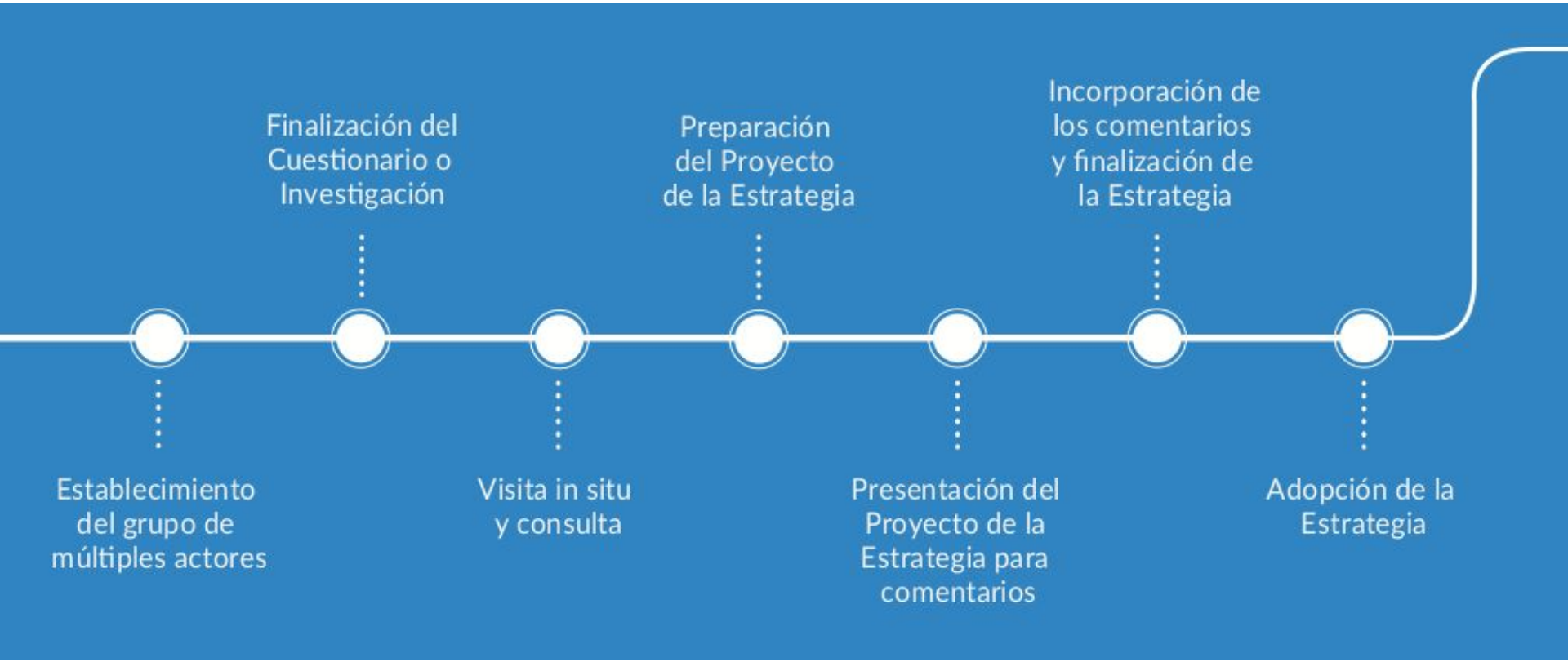


SECRETARÍA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Fases de desarrollo del Plan Nacional

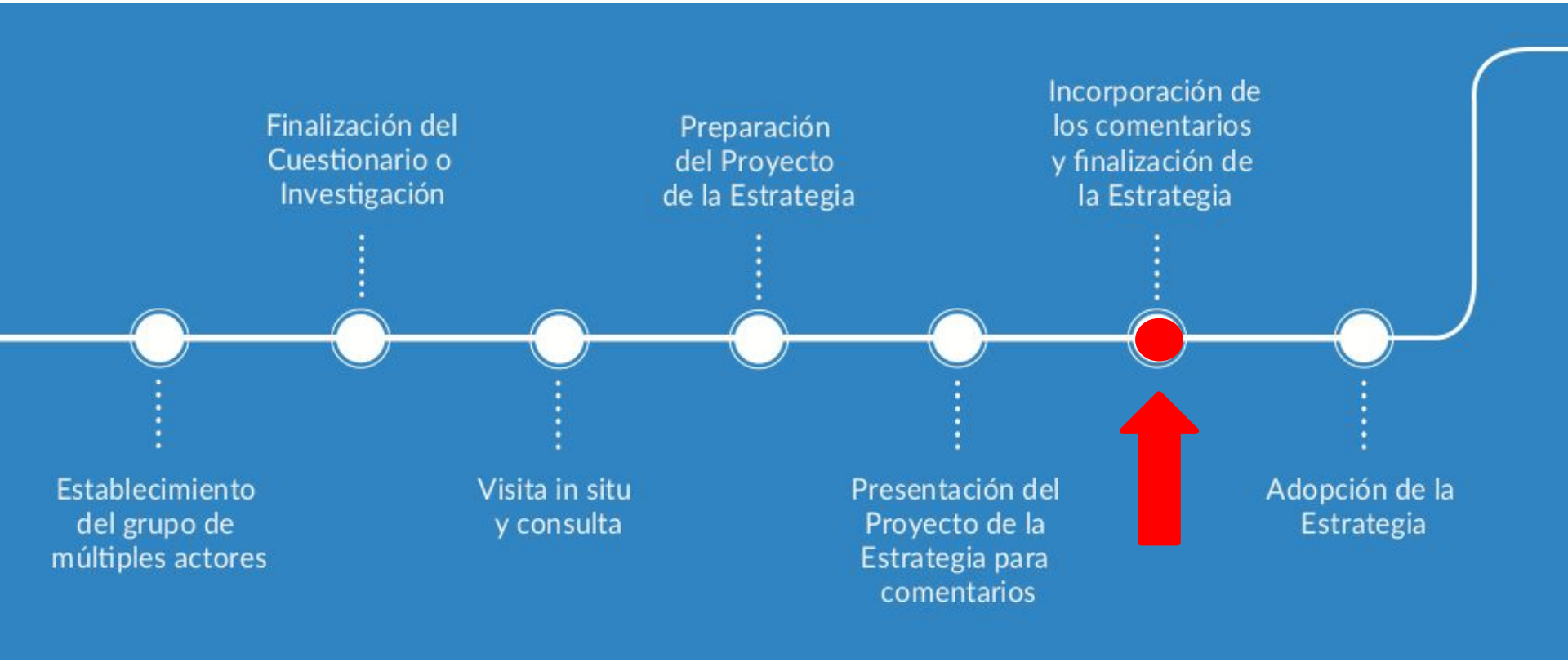


SECRETARÍA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Donde estamos hoy?



Actores involucrados

- Presidencia de la República
- Poder Legislativo
- Organismos Gubernamentales:
  - Senatics
  - Conatel
  - Ministerio de Defensa
  - Policía Nacional
  - Ministerio Público
  - Ministerio de RREE
- Academia:
  - Universidades
  - Centro Nacional de Computación
- Industria y Sector Privado:
  - ISPs
  - Sector Financiero
  - Fabricantes
  - Desarrolladores de software
- Organizaciones Civiles
- Organismos Internacionales

DATO: 125+ personas involucradas

SECRETARÍA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Reuniones multisectoriales

Esquema de un Plan Nacional

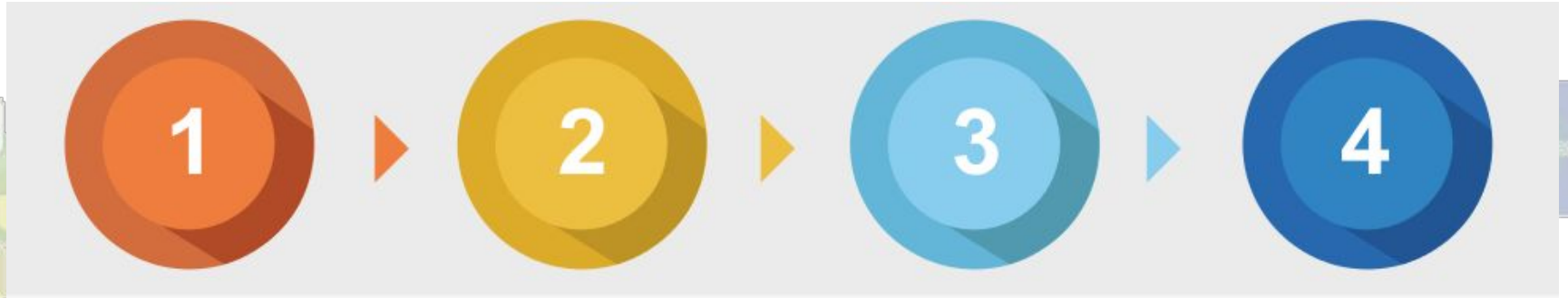
Esquema de un Plan Nacional (I)

Declaración de Propósitos	Proporciona el tono general de la estrategia de seguridad cibernética incluyendo cualquier vínculos entre otras posiciones políticas nacionales existentes.
Introducción	Proporciona un contexto para la Estrategia, incluyendo actual panorama de amenazas a nivel nacional e internacional, las estadísticas sobre ataques cibernéticos y la penetración de Internet y una perspectiva general sobre la seguridad cibernética y la necesidad de una estrategia.
Principios Rectores	Los principios rectores se mantendrán como valores fundamentales durante toda la estrategia.
Pilares/Áreas Focales	Estos representan temas amplios que informarán los objetivos.
Objetivos/Metas	Estos son los principales objetivos que se enmarcan en las esferas de actividad general de actuación.
Plan de Acción	Este esquema de actividades específicas se debe seguir trabajando para cumplir los objetivos establecidos. También puede incluir plazos y costos asociados.

Ejes de Acción

- Sensibilización y Cultura
- Investigación, Desarrollo e Innovación
- Protección de Infraestructuras Críticas
- Capacidad de Respuesta ante Incidentes Cibernéticos
- Capacidad de Investigación y Persecución
- Coordinación Nacional

Implementación de un Plan Nacional



1. Todo buen plan hay que involucrar a los actores relevantes.
2. Identificar una entidad responsable de cada actividad y alocar presupuesto.
3. Desarrollar un mecanismo de seguimiento: Esto podría ser realizado por un organismo público, interinstitucional o un grupo de trabajo interministerial definido como el coordinador de la estrategia.
   Esta será la entidad que tiene la responsabilidad general del ciclo de vida y de la documentación de la estrategia.
4. La estructura de la entidad coordinadora, sus responsabilidades exactas y sus relaciones con los otros actores interesados deben estar claramente definidos (ENISA, 2012).

Plan de Acción - Ejemplo (I)

Pilares	Objetivos	Líneas de Acción	Entidad Implementadora	Plazo
Sensibilización y Cultura	**a. Las campañas de sensibilización pública son conocidas por el público en general y promovidas, y el comportamiento de seguridad cibernética se convierte en una parte de la cultura de los ciudadanos.**	• Llevar a cabo un estudio/encuesta de referencia nacional sobre la sensibilización sobre seguridad cibernética entre los ciudadanos, considerando los aspectos demográficos con el propósito de identificar necesidades específicas de cada grupo.		
		• Desarrollar campañas temáticas de sensibilización pública entre diversos grupos demográficos en Paraguay.		
		• Desarrollar campañas de sensibilización de manera coordinada entre las distintas entidades gubemamentales, para evitar la duplicación de esfuerzos y garantizar un mensaje más amplio y de mayor impacto.		
		• Incluir avisos con recomendaciones de buenas prácticas de seguridad cibemética (ej. uso de antivirus, *firewall*) dirigidos a los usuarios antes que se conecten al Internet por plazas públicas, por otro servicios de acceso gratuito a Internet o por cualquier red abierta disponible al público general.		
		• Contar con el apoyo de las operadoras y prestadores de servicios de Internet en la implementación de avisos con recomendaciones de prácticas de seguridad cibernética cuando el usuario utilizar alguno de sus servicios.		
	b. Los programas enfocados en la protección de menores son coordinados entre las distintas entidades gubernamentales, teniendo	• Asegurar que los programas de incentivo al uso de las TICs por niños y niñas en las escuelas sea acompañado por material educativo a los estudiantes y padres para el buen uso del equipo (ej. hoja de consejos de seguridad estudiantil, contrato de "código		

Plan de Acción - Ejemplo (II)

Capacidad de Respuesta ante Incidentes Cibernéticos	**a. El intercambio de información sobre incidentes cibernéticos se convierte en una práctica común entre el sector privado, ciudadanos y el CERT-PY.**	• Establecer una base de datos nacional actualizada de los incidentes e incluir la alerta temprana sobre amenazas.		
		• Establecer convenios de colaboración y cooperación entre el sector privado y el gobiemo, por medio del CERT-PY, para el intercambio de información sobre incidentes cibernéticos.		
		• Desarrollar un Código de Conducta voluntario para los Operadores de la infraestructura de telecomunicaciones que incluya el compromiso de compartir información sobre incidentes con el CERT-PY y entre los demás.		
		• Crear una base de datos de todos los equipos de respuesta a incidentes privado, público y académico.		
	b. La unidad encargada por la respuesta incidentes cuentan con una infraestructura y con las herramientas adecuadas para conducir sus respectivas tareas de manera oportuna y eficaz.	• Fortalecer los recursos técnicos y la infraestructura del CERT-PY para coordinar mejor a nivel nacional con todos los actores.		
Capacidad de Investigación y Persecución de la Ciberdelincuencia	**a. Los agentes responsables por la investigación de incidentes cibernéticos son capacitados y poseen el conocimiento necesario**	• Desarrollar e implementar un programa de capacitación para las fuerzas del orden en delincuencia cibemética, incluyendo pruebas y análisis forense digital.		

Coordinación Nacional

- Comité Nacional de Seguridad Cibernética impulsado por SENATICs
- Criterios para la definición de los Miembros del Comité (técnico + poder de decisión)
- Comité divido en subcomités multi-institucionales
- Subcomités encargados de la implementación de los ejes del Plan Nacional
- Calendario de reuniones para el seguimiento y monitoreo de la implementación del Plan Nacional
- Revisión/Complementación del Plan – 3 años

Proceso de revisión permanente

1

La estrategia no debe ser estática. Considere lo siguiente:

- Frecuencia de revisión.
- Nivel de aprobación necesaria para la adopción de cambios.
- Terminologías y mención de cosas específicas externas al control nacional.

2

Determine la mejor persona para evaluar la eficacia de la estrategia:

- Los actores originales, o
- EL punto nacional de contacto de seguridad cibernética.

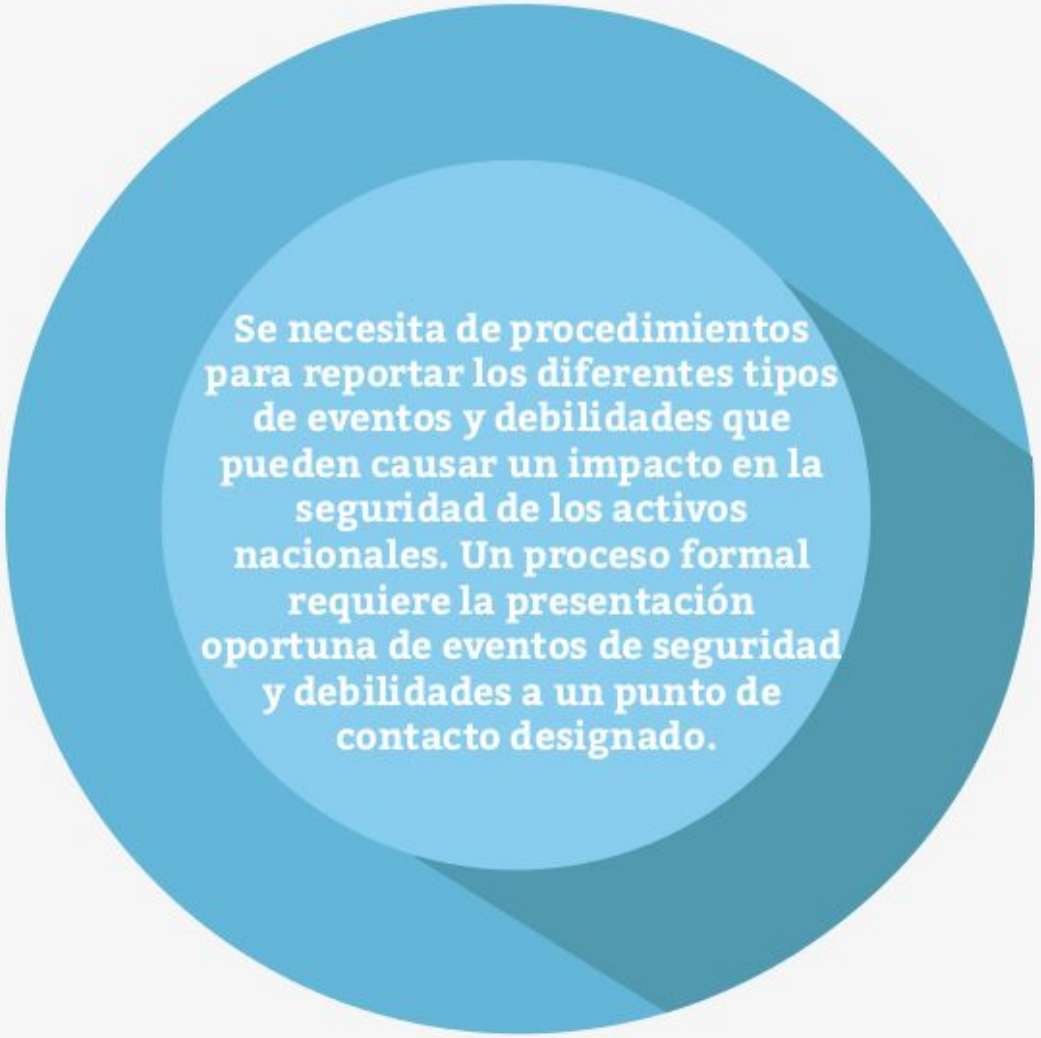
SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Capacidad de Respuesta a Incidente

¿Cómo se encaja el CSIRT en su estrategia de seguridad cibernética...



Capacidad de Respuesta a Incidentes (I)

- Talleres:
  - Taller Amparo: formación de CSIRTs sectoriales
  - Taller sobre Sistemas de Control Industrial e Infraestructura Crítica
- Jornadas de Capacitación para funcionarios de Gobierno
- Campañas de sensibilización ciudadana:
  - Conectate Seguro

SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Muchas gracias!

CENTRO DE RESPUESTAS ANTE INCIDENTES CIBERNÉTICOS
CERT-PY

@CERTpy

/CERT-Py

www.cert.gov.py

https://www.senatics.gov.py/plan-nacional-de-ciberseguridad

denuncias: abuse@cert.gov.py
contacto: cert@cert.gov.py