Gonzalo García - Belenguer
Oficial de Proyecto del Programa de Ciberseguridad
Ggarcia-Belenguer@oas.org
@OASGonzalo

Organización de los Estados Americanos

¿Qué es la Seguridad Cibernética?

No existe una definición universal.

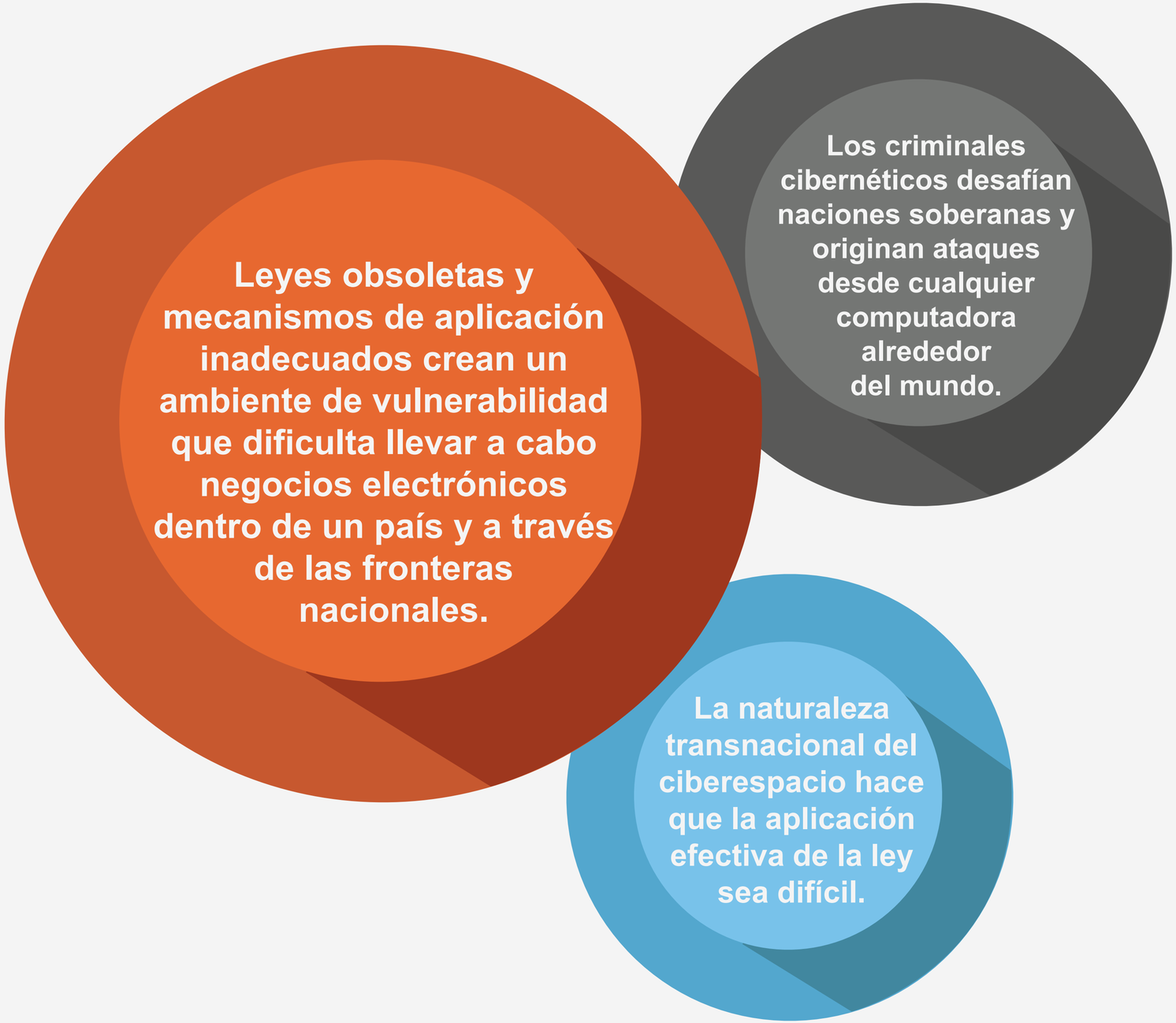
La actividad o el proceso, habilidad o capacidad, referentes a los sistemas de información y comunicación y la información contenida en estos sistemas están protegidos contra el daño, el uso o la modificación no autorizados, o la explotación.

Estrategias, políticas y normas relativas a la seguridad de las operaciones en el ciberespacio, y abarca todos los tipos de reducción de amenazas, la reducción de la vulnerabilidad, la disuasión, la participación internacional, la respuesta a incidentes, resiliencia, y las políticas y actividades de recuperación, incluidas las operaciones de redes informáticas, integridad de la información, aplicación de la ley, la diplomacia, militares y misiones de inteligencia con respecto a su relación con la seguridad y la estabilidad de la infraestructura mundial de la información y las comunicaciones.(Adaptado de: CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, *DHS National Preparedness Goal; White House Cyberspace Policy Review*, Mayo 2009).

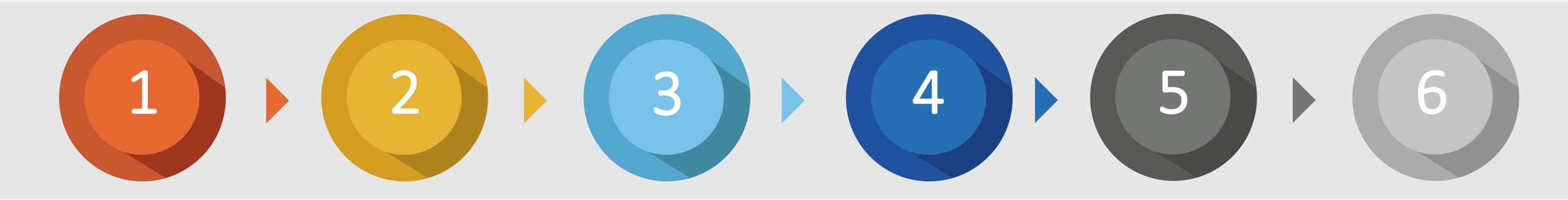
Los objetivos generales de la seguridad cibernética son: Disponibilidad, Integridad – la cual puede incluir autenticidad y no repudio – y Confidencialidad.

¿Qué es el Crimen Cibernético?

Es un crimen facilitado por un sistema informático o directamente en contra un sistema informático. Además, el crimen cibernético también incluye delitos tradicionales realizados a través de Internet. Por ejemplo: los crímenes de odio, fraude en Internet, el robo de identidad, y el robo de cuentas de tarjetas de crédito son considerados como delitos cibernéticos cuando las actividades ilegales se comenten mediante el uso de una computadora y el Internet.



Beneficios de la impementación de Medidas Nacionales de Seguridad Cibernética



1. Proteger sus intereses nacionales.
2. Garantizar la estabilidad económica y la continuidad del negocio.
3. Asegurar que las infraestructuras críticas y los datos estén protegidos y seguros.
4. Salvaguardar los activos de tecnología.
5. Garantizar la seguridad ciudadana.
6. Fomentar la innovación empresarial y capitalizar las ganancias económicas de los avances tecnológicos.

Desarrollo de una Estrategia Nacional de Seguridad Cibernética

¿Por qué desarrollar una Estrategia Nacional de Seguridad Cibernética?

- La evolución de la sofisticación de los ataques cibernéticos que amenazan a las empresas, la privacidad de los datos personales y la seguridad nacional debe ser respondida de manera por una respuesta dinámica y proporcional.
- **Sin una respuesta estratégica, los esfuerzos nacionales en materia de seguridad cibernética serán insostenibles, esporádicos, duplicados e ineficientes.**
- La creciente dependencia de los gobiernos sobre las TICs y el ciberespacio, la vulnerabilidad consecuente, así como la creciente exposición a amenazas y riesgos de ataques.

Austrian Cyber Security Strategy

Federal Ministry of the Interior

Cyber Security Strategy for Germany

Australian Government

CYBER SECURITY STRATEGY

Canada's Cyber Security Strategy

FOR A STRONGER AND MORE PROSPEROUS CANADA

GOBIERNO NACIONAL
REPÚBLICA DE PANAMÁ

CSIRT
Equipo de Respuesta a Incidente de Seguridad de la Información | Computer Security Incident Response Team

National Strategy for Cybersecurity and Protection of Critical Infrastructure

Information systems defence and security

France's strategy

Premier ministre
Agence Nationale de la Sécurité des Systèmes d'Information

LATIN AMERICAN +CARIBBEAN CYBER SECURITY TRENDS

Published June, 2014

Organization of American States

Symantec.

Document Conpes 3701

National Council on Economic and Social Policy
Republic of Colombia
National Planning Department

POLICY GUIDELINES ON CYBERSECURITY AND CYBERDEFENSE

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.

Qué no hacer

Evite la copia de otras estrategias / políticas. Algunas estrategias pueden haber sido desarrolladas de acuerdo con los esfuerzos existentes o estructuradas con base en las estrategias anteriores (UK CSS2) o empezadas desde cero (Trinidad y Tobago).

No excluya a los principales interesados y sus iniciativas cuando determine los actores necesarios, a fin de asegurar la implementación exitosa de la estrategia.

Actores Relevantes

- Involucrar a todos los ministerios competentes responsables por la seguridad, la prevención, la gestión de crisis, las relaciones exteriores, justicia, telecomunicaciones, protección de datos.
- Identificar los propietarios de todas las infraestructuras y servicios críticos. Ejemplos típicos incluyen la energía, el transporte, las finanzas, las telecomunicaciones, la salud, etc. Involucrar propietarios de las infraestructuras críticas concretas en lugar de asignar responsabilidades a un sector específico.
- Involucrar a los actores del sector privado como las telecomunicaciones, proveedores de servicios de Internet y empresas TIC, el sector bancario, el sector de energía, etc, con el fin de fomentar la participación en el desarrollo de la estrategia.
- Involucrar a la sociedad civil y la área académica para ayudar a ejecutar el componente de sensibilización de la estrategia. Una mayor conciencia nacional permitirá a los ciudadanos a entender mejor los riesgos de seguridad cibernética, lo que les permitirá tomar medidas de manera proactiva para disminuir o mitigar los riesgos.
- Involucrar a los grupos de interés nacional con el fin de incorporar los intereses de los diferentes grupos de actores.

Redacción de la Estrategia

En la formulación de la estrategia se debe identificar las áreas clave que se alinean con los objetivos nacionales y considerar las tendencias internacionales.

Temas emergentes en las estrategias de seguridad cibernética a considerar:

- Fortalecimiento de la red nacional de seguridad, incluida la protección de las infraestructuras críticas.
- Construcción de conciencia y de la capacidad nacional.
- El establecimiento de un cuerpo de gobierno con la responsabilidad para coordinar actores nacionales en seguridad cibernética.
- Creación de un marco jurídico de seguridad cibernética (normas para la seguridad cibernética y herramientas para combatir el delito cibernético).
- Fomentar la colaboración público-privada / colaboración y el intercambio de información por medio de mecanismos confiables.
- El desarrollo de una cultura de seguridad cibernética.
- Cooperación y participación internacional.

Cada país es único

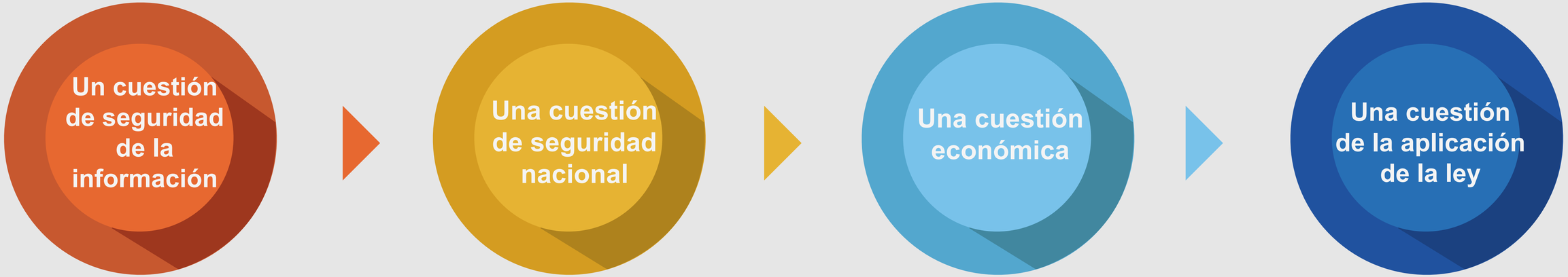
Una misma estrategia no sirve para todos

ENISA: El desarrollo de una estrategia integral puede plantear muchos desafíos. Un documento que incluya todos los requisitos sobre lo que debería ser, se puede hacer fácilmente. Sin embargo, es poco probable lograr un impacto real en términos de la mejora de la seguridad cibernética y la resiliencia de un país. Para desarrollar una estrategia es necesario lograr la cooperación y el acuerdo entre una amplia gama de partes interesadas en un curso de acción común - esto no será una tarea fácil.

Microsoft: Una estrategia nacional de seguridad cibernética esboza una visión y articula las prioridades, principios y enfoques para entender y gestionar los riesgos a nivel nacional. Las prioridades de las estrategias nacionales de seguridad cibernética variarán según el país.

OEA (2004): Una estrategia eficaz de seguridad cibernética deberá reconocer que la seguridad de la red de sistemas de información que comprenden el Internet requiere una alianza entre el gobierno y la industria.

Diferentes Enfoques para Redactar



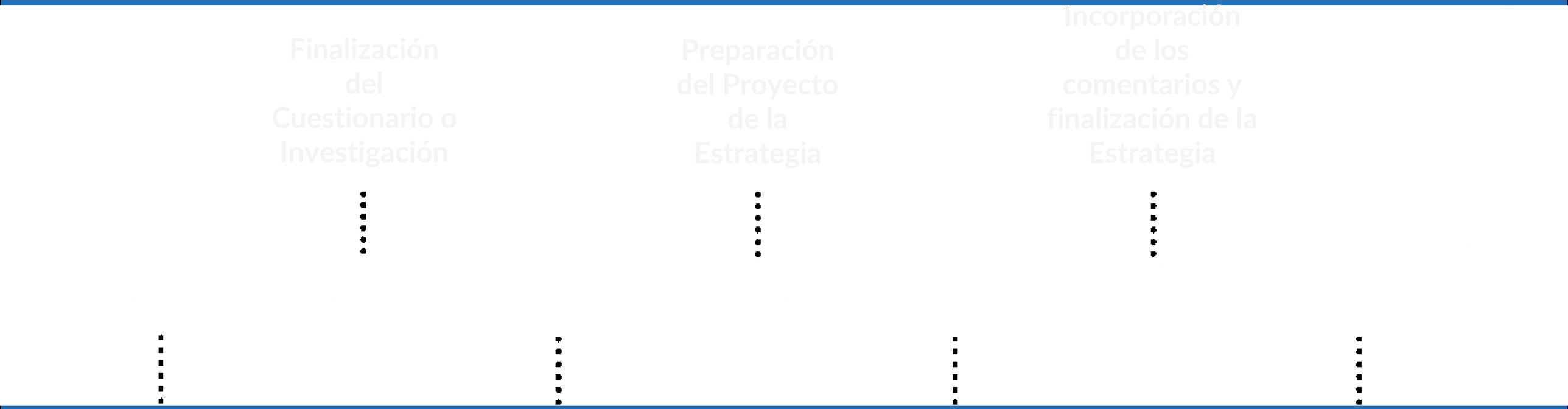
Centrado en la lucha contra las amenazas a la infraestructura de la información por medios técnicos tales como firewalls, software anti-virus o software de detección de intrusos.

Abordar las amenazas a la seguridad cibernética como amenazas a la seguridad nacional.

La resistencia de la seguridad cibernética es vista como una necesidad de la comunidad de negocios dada la constante evolución esta dependerá de la infraestructura de las TIC para los procesos y servicios de oficina.

Los crímenes cibernéticos son vistos como una amenaza para la seguridad cibernética y se centra en las medidas para detectar y procesar los crímenes habilitados con la tecnología hasta los delitos cometidos en contra de los sistemas informáticos.

Ciclo de redacción

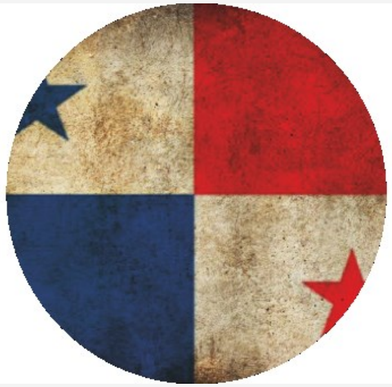


olombia

011

Trinidad and Tobago

2013



Panama

2013

amaica

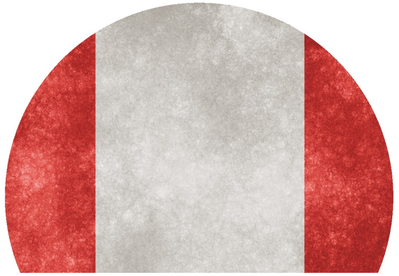
015

ca

s

mbia

ocess

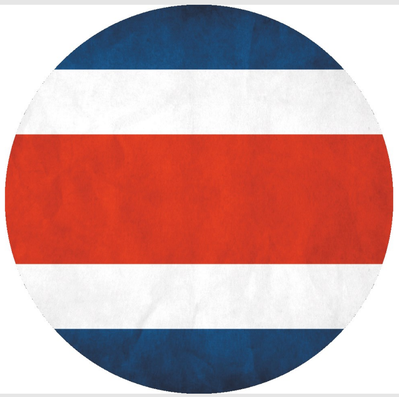


ú

ocess

aguay

rocess



Costa Rica

rocess

Dominican Republic

In progress

Barbados

equest received

Suriname

In process

Colombia
2014

Colombia
2015

Costa Rica

OEA Cyber @OEA_Cyber · Jun 30

Misión de Asistencia Técnica en #CRC x desarrollo de Estrategia Nacional #ciberseguridad junto a @micittcr @SUTEL_CR

View translation

OEA Cyber, OEA, MICITT and SUTEL

Paraguay

OEA Cyber @OEA_Cyber · Jul 21

#OEA colabora con @SENATICs revisando 1er borrador para desarrollar Estrategia Nacional #ciberseguridad en Paraguay

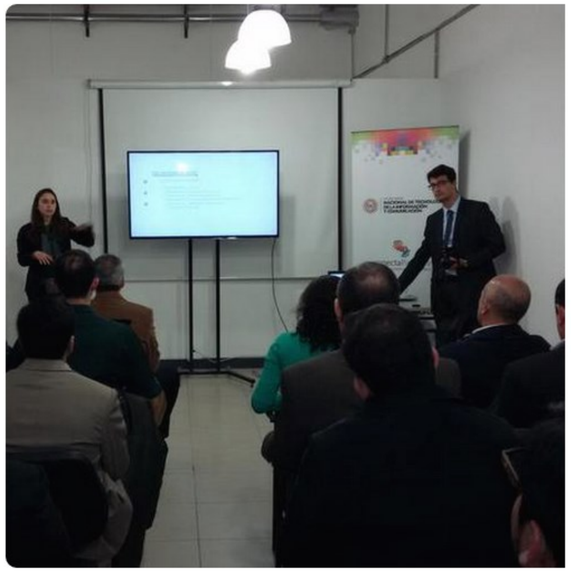
You, OEA, SENATICs Paraguay and David Ocampos

OEA Cyber retweeted

SENATICs Paraguay @SENATICs · Jul 23

3ra jornada de trabajos multisectoriales sobre el Plan Nacional de Ciberseguridad @OEA_oficial

David Ocampos, Herman Mereles, Javier Quiñónez and 5 others



Vista general de los componentes de la Estrategia Nacional de Seguridad Cibernética

Componentes de la Estrategia

- Concéntrese en áreas clave que se puedan ser accionadas y medidas para una implementación exitosa.
- Las áreas clave deben estar alineadas con los objetivos nacionales para el desarrollo del país y la política de seguridad nacional (si esta existe).
- Examine la experiencia de su propio país en lo que respecta a la seguridad cibernética.
- Identifique las actividades actuales que formarían parte de la estrategia nacional.

Componentes de la Estrategia

Declaración de propósitos

Áreas Focales

Plan de Acción

Objetivos/Metas

Revisión

?

Esquema básico de una Estrategia

Declaración de Propósitos
Proporciona el tono general de la estrategia de seguridad cibernética incluyendo cualquier vínculos entre otras posiciones políticas nacionales existentes.

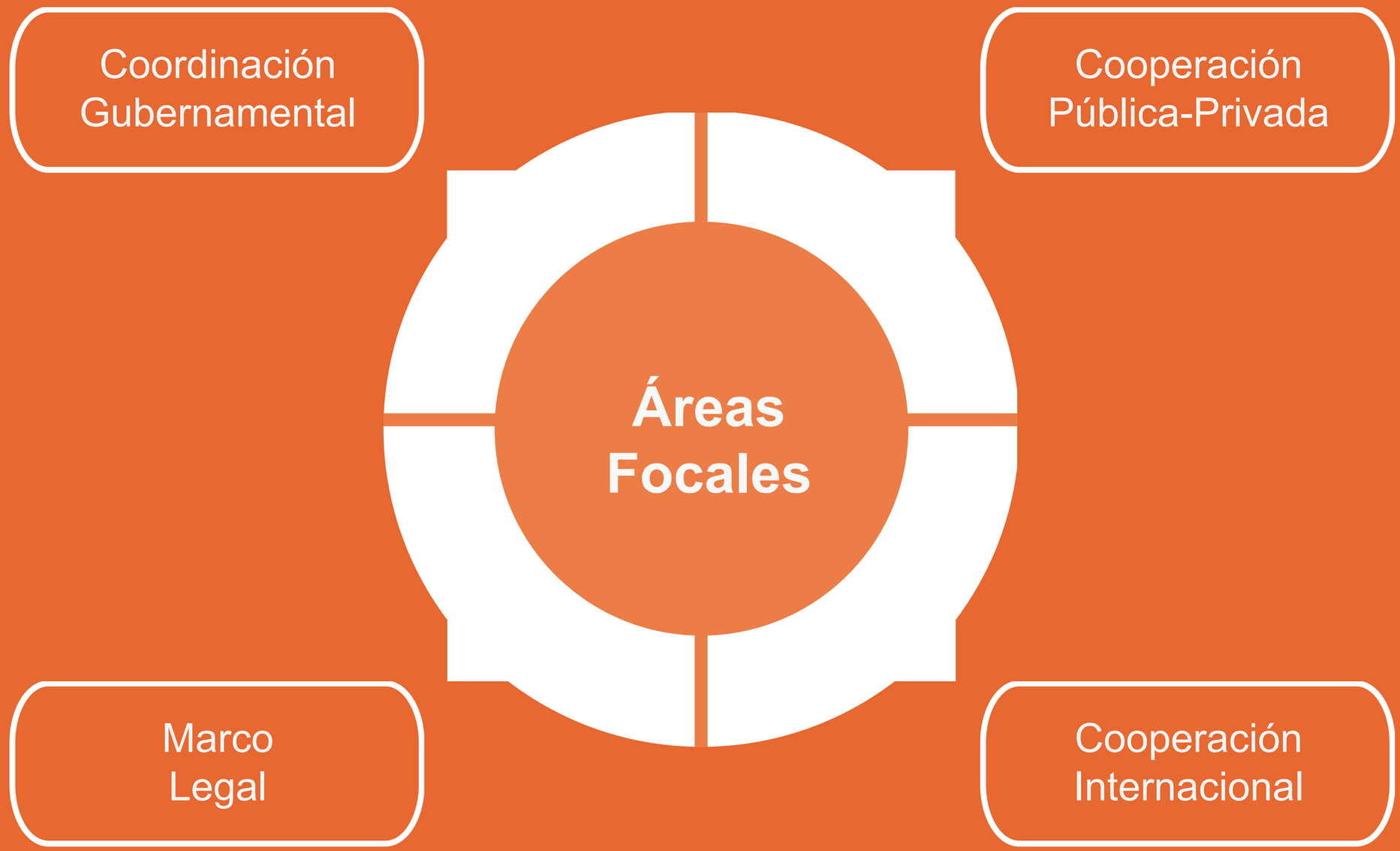
Introducción
Proporciona un contexto para la Estrategia, incluyendo actual panorama de amenazas a nivel nacional e internacional, las estadísticas sobre ataques cibernéticos y la penetración de Internet y una perspectiva general sobre la seguridad cibernética y la necesidad de una estrategia.

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.


Coordinación Gubernamental
Cooperación Pública-Privada
Áreas Focales
Marco Legal
Cooperación Internacional

Áreas Focales

Francia

- Para convertirse en una potencia mundial de defensa cibernética.
- Salvaguardar la capacidad de Francia para tomar decisiones a través de la protección de la información relacionada con su soberanía.
- Fortalecer la seguridad cibernética de las infraestructuras nacionales críticas.
- Garantizar la seguridad en el ciberespacio.

Reino Unido

- Para hacer frente a la delincuencia cibernética y ser uno de los lugares más seguros del mundo para hacer negocios en el ciberespacio.
- Para ser más resistente a los ataques cibernéticos y más capaz de proteger nuestros intereses en el ciberespacio.
- Para ayudar a dar forma a un ciberespacio abierto, estable y vibrante que el público del Reino Unido puede utilizar con seguridad y que apoya las sociedades abiertas.
- El Reino Unido tiene los conocimientos, habilidades y capacidades transversales que se necesita para sustentar todos nuestros objetivos de seguridad cibernética.

Plan de Acción

Plan de Acción

- Una estrategia sin un plan para ponerla en práctica, es sólo un pedazo de papel.
- Una estrategia debe ser un documento vivo y de constante trabajo.
- Desarrollar un plan de acción para apoyar las áreas clave identificadas y asignar la responsabilidad a las agencias específicas y plazos para su conclusión.
- Puede haber varias actividades unidas a un área clave, por lo que un mecanismo de seguimiento sobre el progreso de estas actividades deben estar señalado.

Plan de Acción

El país es resistente a los ataques cibernéticos.

Establecimiento de un Plan de Contingencia Nacional de Seguridad Cibernética.

- Establecimiento de estructuras provisionales y medidas para los incidentes de recuperación.
- Realizar ejercicios de Seguridad Cibernética Nacional.
- Revisión de los planes de emergencia existentes, dirigido especialmente a la debilidades.

Otro ejemplo

Sensibilización

Todos los australianos son conscientes de los riesgos cibernéticos, asegurar sus computadoras y sus identidades.

- Educar y capacitar a todos los australianos con la información y las herramientas para protegerse en Internet.
- Desarrollar campañas de educación para las escuelas.

Ejemplo 3 – Katar

3.1 Vision

Establish and maintain a secure cyberspace to safeguard national interests and preserve the fundamental rights and values of Qatar's society.

3.2 Objectives

To achieve this vision, Qatar seeks to fulfill the following objectives:

Objective 1:	Objective 2:	Objective 3:	Objective 4:	Objective 5:
Safeguard national CII.	Respond to, resolve, and recover from cyber incidents and attacks through timely information sharing, collaboration, and action.	Establish a legal and regulatory framework to enable a safe and vibrant cyberspace.	Foster a culture of cyber security that promotes safe and appropriate use of cyberspace.	Develop and cultivate national cyber security capabilities.

Objective 1: Safeguard national CII.	
Initiative	**Action**
Assess the risk to CII	▪ Develop a national CII risk management framework to guide the identification of CII assets and organizations; assessment of threats, vulnerabilities, and consequences; and development of risk profiles ▪ Conduct regular risk assessments of CSOs and other organizations with CII ▪ Conduct dependency and interdependency assessments to identify systemic risks that cut across critical sectors
Implement cyber security controls and standards to mitigate risk to CII	▪ Establish and maintain a CII cyber security standard and maturity model, including specific cyber security controls ▪ Conduct regular evaluations and audits of CSOs to measure the effectiveness of cyber security programs and controls ▪ Develop risk management strategies to protect the most critical services, systems, and organizations and track implementation of those strategies ▪ Share information on risks and risk management strategies across sectors to enable the prioritization of mitigation actions and the investment of resources
Analyze cyber security trends and threats to CII and provide timely reports to stakeholders	▪ Create sector-specific or organizational security operations centers or threat intelligence centers
Ensure the use of trustworthy technology products and services	▪ Develop the capability to evaluate and certify ICT products and systems for use in critical sectors ▪ Develop guidelines that specify security requirements for ICT and cyber security service providers
Continuously monitor the security of CII	▪ Establish a capability to conduct continuous diagnostics and monitoring of networks to better understand risks, promote preventive measures, detect and treat infected devices, and notify affected users

Organización de los
Estados Americanos

Programa de Seguridad Cibernética

Comité Interamericano contra el Terrorismo
Secretaría de Seguridad Multidimensional

1889 F St., NW — 8VO Piso
Washington D.C.

T: (202) 370 – 4904
F: (202) 458 – 3857

cybersecurity@oas.org
www.oas.org/cyber

WWW.OAS.ORG/CYBER