La seguridad cibernética en América Latina y el Caribe: un esfuerzo multiateral

CEPAL

Mensajes principales

La seguridad cibernética representa un esfuerzo coordinado a nivel nacional.

Demanda un marco normativo e institucional y una política pública con lineamientos claros sobre la protección de datos.

La cooperación internacional es clave para enfrentar las amenazas cibernéticas.

Las alianzas entre sector público y privado es indispensable para una estrategia efectiva de seguridad cibernética.

Se requiere un marco regulatorio e institucional y una política clara que asegure la gobernanza efectiva…

- Una estrategia nacional de ciberseguridad requiere de un ente de coordinación centralizado que pueda definir y dirigirla
- La ciberseguridad tiene varias formas y grados de impacto sobre: personas, empresas, gobiernos.
- Las distintas amenazas al uso y mal uso de los datos requiere de mecanismos de respuesta operative y de esfuerzos conjuntos dentro de un país y entre países, para abordar los ciber riesgos:

  - El tratamiento a los programas informáticos maliciosos: malware, spyware, data breaches y ransomware.

  i) robo de datos especialmente sensibles; ii) manipulación de datos; iii) obstaculizar el funcionamiento de sistemas informáticos (incluidos los que controlan infraestructuras críticas), iv) borrar, v) suprimir o vi) bloquear el acceso a datos, vii) programas de extorsión, espionaje cibernético, etc.

NACIONES UNIDAS
CEPAL

Dimensión de la importancia: sistemas críticos de datos y seguridad cibernética

- Incluye infraestructura crítica**:** clave para los países desde la perspectiva de:

i. defensa,

ii. seguridad nacional,

iii. economía,

iv. salud,

v. orden público

vi. política

- Impactos sobre sectores: servicios públicos y gubernamentales alimentación, combustible, transporte, comunicaciones, finanzas, e industrias.
- Impacto sobre la sociedad: agota fondos del tesoro público, atentar contra los servicios públicos, red electéctrica, telecomunicaciones y el suministro de bienes y servicios esenciales

Construcción de una agenda holística de ciberseguridad

Capacidad de respuesta de los gobiernos frente ataques cibernéticos en distintos ámbitos…

- El **tamaño, diversidad y dinamismo estructuras económico – sociales,** clave para mitigar los efectos de los ataques cibernéticos. Particularmente el impacto sobre las instituciones.
- Sobre los riesgos cibernéticos: **ataques a distintos niveles de gobierno** hay consideraciones variadas, que muestra entre otras cosas la diversificación económica para atender dichos riesgos.
- En términos de estructura **“política**” un ataque se dirige al uso de datos personales para fines políticos obtenidos de manera ilícita.
- Sistemas de datos efectivos que protejan a personas de robo de identidad, y a organismos públicos de posible fraude.
- Construcción de talento y tecnología de ciberseguridad para enfrentar los desafíos

La efectividad de respuesta de los gobiernos a los ataques cibernéticos revela su capacidad institucional y de gobernanza

NACIONES UNIDAS

CEPAL

Ciberseguridad en el flujo transfronterizo de datos… requiere de esfuerzos multilaterales

- El acceso a datos transfronterizos. Es una excepción al principio de territorialidad que permite el acceso transfronterizo unilateral sin necesidad de asistencia mutua en situaciones limitadas. (Art. 32.b C de B)
- Dos situaciones:
  - Cuando los datos sean accesibles al público (fuente abierta)
  - Cuando una Parte ha accedido o recibido datos de fuera del territorio, a través de un sistema informático de su territorio y ha obtenido el consentimiento legal y voluntario de la persona con autoridad legal para revelar los datos a través de ese sistema.
- La cooperación internacional entre actores públicos y privados involucra temas como: privacidad y protección de datos personales (sensibles), el acceso a los datos almacenados en jurisdicciones extranjeras o en la nube y aspectos relacionados con soberanía nacional.
- Limitar el poder de los monopolios de datos. Los efectos de la red, la falta de portabilidad de datos y derechos de usuario sobre sus datos y la débil protección de la privacidad ayudan a los “data- opolies” a mantener un dominio.
- Se requiere de una mayor coordinación entre los encargados de hacer cumplir las leyes antimonopolio y los funcionarios de protección de la privacidad y del consumidor para garantizar que existan las condiciones para una competencia de privacidad efectiva y una economía inclusiva.

NACIONES UNIDAS

CEPAL

- En la región, el tema de la ciberseguridad se asocia fundamentalmente a la protección de datos, por lo tanto el fortalecimiento de la política de protección de datos debe incluir necesariamente la seguridad cibernética.
- En la discusión actual, el poder de los datos personales y su valor creciente, requiere de una mayor protección ante múltiples ataques. Este es un tema central en las iniciativas internacionales, las cuales entre otras cosas, busca que el usuario que accede a cualquier plataforma pueda proporcionar y controlar su información y que esta quede debidamente cautelada.
- La colaboración público – privada es fundamental en el éxito de una política de ciberseguridad efectiva, en la detección de riesgos asociados al uso y mal uso de datos, en la mitigación de los daños que un ataque pueda producir a la privacidad y a la custodia de los datos considerados sensibles.
- Un esfuerzo multilateral requiere de marcos amplios que contemplen las formas y grados variados del impacto de los ciberataques sobre las empresas, gobiernos y sistemas de información. Desde posibles daños a la infraestructura crítica de un país, los alcances de los programas maliciosos y un marco para el flujo transfronterizo de datos.
- Una estrategia regional en ciberseguridad tiene un doble efecto: que las personas tomen conciencia sobre el valor de sus datos y los protejan; y que los reguladores puedan dimensionar con mayor precisión los alcances de un ecosistema digital, elemento esencial en términos de valor, riesgos y rentabilidad.

Algunas recomendaciones:

Diseño de estrategia
i. marco normativo e institucional
ii. sistema de datos críticos
iii. cooperación internacional
iv. desarollo y gestión de capacidades técnicas

NACIONES UNIDAS
CEPAL