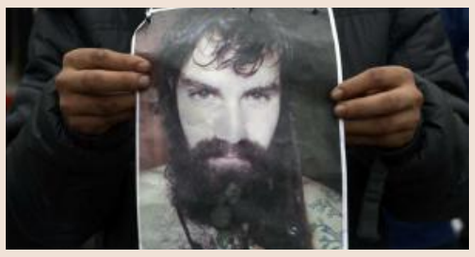


AGO 8, 2017 | 09:47

Argentina ofrece recompensa en desaparición forzada que

AGO 8, 2017 | 11:48

Francia pone en libertad condicinal a miembro de ETA

AGO 2, 2017 | 01:01

Empresarios locales no podrán importar gasolina

AGO 8, 2017 | 11:48

Psicólogos que diseñaron plan de torturas de la CIA irán a juicio

AGO 8, 2017 | 07:18

Maradona se ofrece como soldado de Maduro

NO HACE NINGUNA MENCIÓN SOBRE INTERVENIR Y HACKEAR EQUIPOS DE FORMA ILEGAL

Estrategia Nacional de Ciberseguridad arranca con desconfianza por espionaje

La falta de claridad en las acciones que forman parte de la estrategia pone en duda las capacidades del Estado para afrontar situaciones de seguridad, como los ataques informáticos e incluso, actividades relacionadas con el terrorismo o el crimen organizado.

JULIO SÁNCHEZ ONOFRE

AGO 7, 2017 | 8:07

COMPARTIR | FACEBOOK | TWITTER | LINKEDIN | ENVIAR | IMPRIMIR

Archivado en: Sociedad | Ciberseguridad | Derechos Humanos | Estrategia Nacional De Seguridad | Impreso | Politica

ÚLTIMAS NOTICIAS

Consejo Fiscal debe ser independiente y acorde a la realidad — 12:00 pm

Bolsas europeas cierran con pequeñas alzas — 11:54 am

Banca de desarrollo apoya dos proyectos eólicos de subastas de la CFE — 11:54 am

Francia pone en libertad condicional a miembro de ETA — 11:48 am

Psicólogos que diseñaron plan de torturas de la CIA irán a juicio — 11:48 am

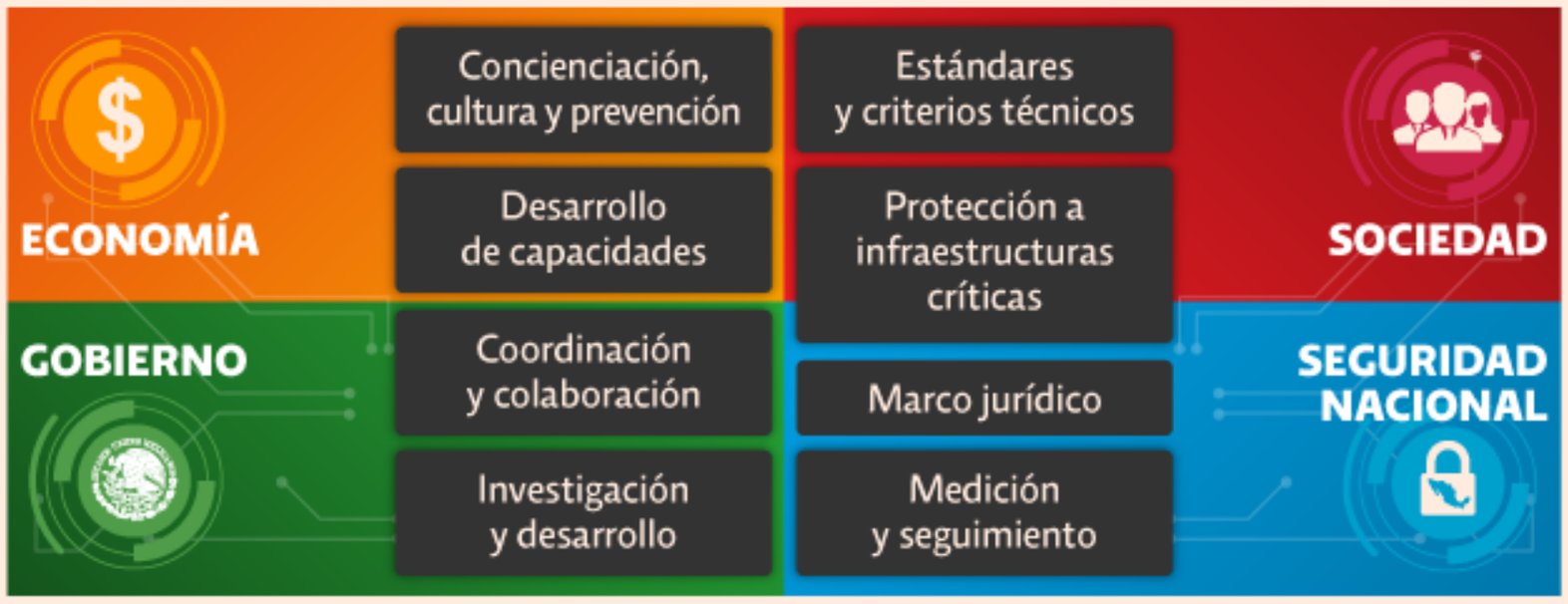
+ LEÍDO

1 Franklin entrará por Quintana Roo, pero se sentirá hasta Tamaulipas

EN CONSTRUCCIÓN LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

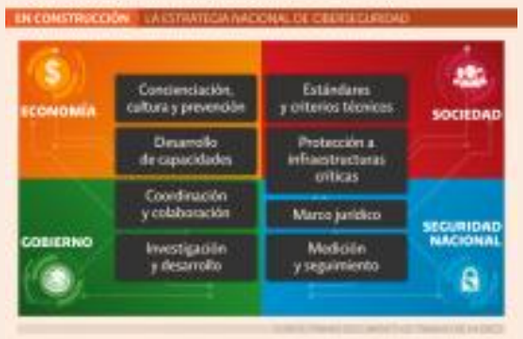
¿CUÁLES SON LOS OBJETIVOS DE LA ESTRATEGIA DE CIBERSEGURIDAD?

Hace tres años, el gobierno federal se comprometió a crear la Estrategia Nacional de Ciberseguridad; fue hasta este 2017 cuando se inició el diseño de esta política pública.



FUENTE: PRIMER DOCUMENTO DE TRABAJO DE LA ENCS

RELACIONADAS



¿Qué es la Estrategia Nacional de Ciberseguridad?

WannaCry, llamado de urgencia para Estrategia Nacional de Ciberseguridad

En el primer documento de trabajo para el diseño de la Estrategia Nacional de Ciberseguridad (ENCS), la Presidencia de la República estableció como el principio rector número uno la “perspectiva de derechos humanos en ciberseguridad”. Los expertos ven esto como una incongruencia tras el espionaje electrónico sistemático que el gobierno ha realizado en contra de activistas, periodistas, académicos y la sociedad civil mediante el uso de software malicioso, lo que se suma a la crisis de derechos humanos que vive el país.

En el documento, puesto a consulta pública por el gobierno, en ningún momento se hace mención al control sobre el uso de recursos y capacidades tecnológicas por parte del gobierno para intervenir comunicaciones y hackear equipos de forma ilegal, en contra de la sociedad civil. Expertos consultados por **El Economista** abogan por que esto sea discutido abiertamente en el diseño de la ENCS.

NOTICIA: Policía Federal quiere un Consejo Nacional de Ciberseguridad

“No valdría la pena tener una estrategia de ciberseguridad si no se velan los derechos más básicos, la legalidad más básica y la rendición de cuentas más básica para el ejercicio de mucho de lo que se está estableciendo en este documento, tal como lo hemos visto en los casos de abuso y espionaje ilegal”, dijo Juan Manuel Casanueva, director general de SocialTIC.

SocialTIC es parte del núcleo de organizaciones de la sociedad civil que se retiró de la Alianza para el Gobierno Abierto luego de documentarse el espionaje electrónico en contra de periodistas y activistas utilizando herramientas de uso exclusivo del gobierno mexicano, como es el software Pegasus, desarrollado por la firma israelí NSO Group. El gobierno, hasta el momento, no ha dado respuestas que permitan esclarecer este espionaje.

La ausencia de un planteamiento sobre estos controles en la ENCS contribuye a que persista el nivel de desconfianza de la sociedad hacia el gobierno, de acuerdo con Cédric Laurant, director del programa SonTusDatos de Artículo 12.

“Este documento no menciona el caso del Gobierno Espía para nada. Los casos

2 **Tras su división, bitcoin alcanza máximo histórico y supera los 3,300 dólares**

3 **5 noticias del día: 7 de agosto**

4 **Maradona se ofrece como soldado de Maduro**

5 **HBO GO desatiende a Profeco y a consumidores**

de espionaje hicieron que bajara el nivel de confianza hacia el gobierno actual", sostuvo.

Guillermo Larrea, abogado y experto en ciberseguridad del despacho jurídico Jones Day, considera que en el diseño de la ENCS se debe "hablar de un registro de productos que sean sensiblemente vulnerables al público general para su distribución en México".

NOTICIA: Día de Internet con un Estado mexicano débil en ciberseguridad

" Las labores de inteligencia del gobierno requieren de la obtención de información de distintos medios y creo que habría que ser muy claros cuáles son estas capacidades y hasta donde puede y no puede llegar esas labores de inteligencia", añadió Pablo Corona, vicepresidente de Seguridad de la Asociación de Internet.mx.

Con la falta de claridad en las acciones de inteligencia como parte de la ENCS, también quedan en duda las capacidades del Estado para afrontar situaciones de seguridad, desde temas propios del ambiente cibernético, como los ataques informáticos, hasta actividades relacionadas con el terrorismo o el crimen organizado.

Ciberseguridad nacional, con perspectiva limitada

En el apartado de Seguridad Nacional del documento, Presidencia hace patente las intenciones de realizar acciones en materia de "ciberdefensa" por parte de Fuerzas Armadas para la protección contra ataques cibernéticos nacionales e internacionales, algo de lo que se ha deslindado la Secretaría de la Defensa Nacional (Sedena) en diversas solicitudes de información realizadas por **El Economista**.

La Presidencia de la República argumenta en el documento que estas acciones son fundamentales para proteger los sistemas de infraestructura crítica, sobre todo aquellos que suministran energía, transporte, salud, agua y otros servicios públicos, cuya vulneración "podría ocasionar riesgos a la estabilidad social, económica y política del Estado Mexicano". Por ello también se plantea la elaboración de un Catálogo Nacional de Infraestructuras Críticas de la Información (CNICI).

NOTICIA: El sector manufacturero en México, el que menos invierte en ciberseguridad

Dmitry Bestuzhev, director del Equipo de Investigación y Análisis de Kaspersky Lab para América Latina, explicó que los ataques dirigidos deben ser la piedra angular en cualquier plan de seguridad para la protección de sistemas críticos.

"Al no ser así, nuevamente el modelo de seguridad se verá comprometido. Los últimos ataques ransomware de WannaCry y especialmente el de NotPetya son una clara muestra de que los ataques APT o ataques dirigidos en general, deben ser la parte medular de cualquier plan de seguridad", insistió el analista.

NOTICIA: Gobierno mexicano, sin reacción al ciberespionaje estadounidense

Ayala, de Arbor Networks, considera que el éxito del combate defensivo y la ciber-inteligencia sería la creación de un SOC (centros de operación utilizados para el monitoreo de la seguridad) y de un CERT Nacional Multicapa, donde se centralice la estrategia global de monitorización y respuesta a las ciberamenazas.

El experto propone que de estas entidades centralizadas se generen otros SOC y

CERT, “para poder atender oportunamente y con la especialidad requerida guiándose por libros de acción de las amenazas habituales para cada participante que conforma esta Estrategia de Seguridad Nacional, como son la sociedad, el gobierno, la Iniciativa Privada y la seguridad nacional”.

Alertas por el marco jurídico

Uno de los ejes transversales que ha puesto en alerta a la sociedad civil es la modificación de los marcos legales y jurídicos, sobre todo en la definición de conductas delictivas. Juan Manuel Casanueva, de SocialTIC, advirtió que esto puede abrir la puerta a restricciones en el ejercicio de los derechos en la esfera digital.

“Cuando hablamos de legislación y regulación orientada a mundos digitales, muchas veces al establecerse leyes y regulaciones se puede empezar a coartar algunas de las libertades más fundamentales, como la libertad de expresión”, dijo Casanueva.

NOTICIA: Encuentran malware espía en gobierno de México

Aún así, la homologación y adecuación de los marcos jurídicos es defendida por las autoridades.

Durante un foro organizado en el Senado por la Organización de Estados Americanos (OEA), Gustavo Parra Noriega, coordinador de Protección de Datos Personales del Instituto Nacional de Acceso a la Información y Protección de Datos Personales (INAI), dijo que aún falta tipificación de delitos en Internet a nivel estatal y federal, y ejemplificó que la suplantación de identidad sólo es tipificada en 18 legislaciones estatales y no a nivel federal.

NOTICIA: El espionaje digital es un problema de política en ciberseguridad

A su vez, la titular de la División Científica de la Policía Federal consideró que falta un marco jurídico donde sean tipificados los nuevos cibercrímenes.

“Cuando vemos que se pueda habilitar o limitar aspectos digitales por cuestiones de ciberseguridad, es fundamental que eso se precise bien conforme a la ley y que no se estén inventando nuevas leyes; que quede clarísimo cuáles son los puntos medios, cuando se va a velar la libertades de la sociedad en un contexto de internet libre y abierto versus una investigación criminal, la comisión y castigo de delitos específicos”, advirtió Casanueva, de SocialTIC.

julio.sanchez@eleconomista.mx

erp