AGO 10, 2017 | 10:39

Inversión extranjera en AL caerá 5% : Cepal

AGO 3, 2017 | 08:22

Roche se corona como mayor farmacéutica del mundo

AGO 11, 2017 | 10:28

¿En que país es más barata la belleza?

AGO 11, 2017 | 07:17

Necesidades y tentaciones en la Estrategia Nacional de

AGO 9, 2017 | 09:04

Estrategia Nacional de Ciberseguridad: gobierno bajo ataque

AGO 11, 2017 | 07:17

Necesidades y tentaciones en la Estrategia Nacional de

AGO 3, 2017 | 08:22

Roche se corona como mayor farmacéutica del mundo

AGO 11, 2017 | 10:28

¿En que país es más barata la belleza?

AGO 10, 2017 | 10:39

Inversión extranjera en AL caerá 5% : Cepal

AGO 11, 2017 | 10:37

Fed podría retrasar alza de tasas

EXPERTOS VEN CON BUENOS OJOS EL ARRANQUE DE LOS TRABAJOS

Estrategia de Ciberseguridad debe ser obligatoria para todos

Los llamados a implementar una política pública en ciberseguridad son cada vez más insistentes y urgentes ante el crecimiento de las amenazas informáticas.

JULIO SÁNCHEZ ONOFRE

AGO 8, 2017 | 7:55

COMPARTIR FACEBOOK | TWITTER | LINKEDIN | ENVIAR | IMPRIMIR

Archivado en: Tecnociencia | Ciberseguridad | Derechos Humanos | Estrategia Nacional De Ciberseguridad | Impreso

ÚLTIMAS NOTICIAS

¿Cuál es el problema de la fuga de cerebros? 11:22 am

Riesgos para México sobre el TLCAN han disminuido: Fitch 11:12 am

PGR confirma que restos hallados en Tamaulipas son de española Pilar Garrido 11:10 am

Blizzard remasterizará StarCraft 11:06 am

Producción industrial crece apenas 0.1% en junio 10:57 am

+ LEÍDO

1 **Firmas telecom hacen frente contra Telmex-Telcel**

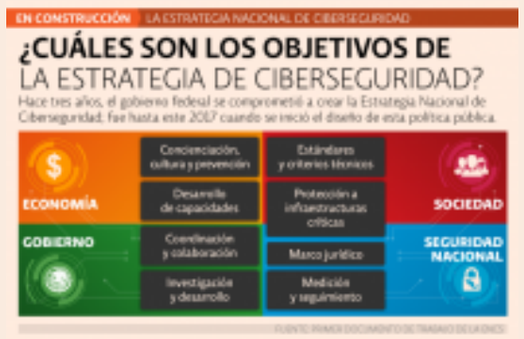
2 **Mujeres, con poca participación en directorio de empresas de la BMV**

3 **¿Dónde se podrá observar el eclipse de sol en México?**

4 **Vista Oil & Gas consigue 650 millones de dólares en la BMV**

5 **La inversión e impacto de la marca Márquez están en riesgo**

RELACIONADAS



- Estrategia Nacional de Ciberseguridad arranca con desconfianza por espionaje
- ¿Qué es la Estrategia Nacional de Ciberseguridad?

COMPARTIR

Me gusta

"México será, para el año 2030, un país mejor preparado y resiliente ante ciberataques, y un actor relevante en el escenario internacional en mejores prácticas en la cultura de ciberseguridad". Esto quedó plasmado en el primer documento de trabajo de la Estrategia Nacional de Ciberseguridad (ENCS), una política pública que, hace tres años, el gobierno federal se comprometió a crear en su Programa para la Seguridad Nacional 2014-2018.

NOTICIA: WannaCry, llamado de urgencia para Estrategia Nacional de Ciberseguridad

Fue hasta el 2017 cuando, junto con la Organización de los Estados Americanos (OEA), comenzó el diseño de esta política a través de foros y una consulta pública que estará abierta hasta el próximo 11 de agosto.

El primer documento de trabajo de la ENCS establece objetivos estratégicos de ciberseguridad en Economía, Sociedad, Gobierno y Seguridad Nacional, con ocho ejes transversales: concientización, cultura y prevención; desarrollo de capacidades; coordinación y colaboración; investigación y desarrollo; estándares y criterios técnicos; protección de infraestructuras críticas de la información; marco jurídico; medición y evaluación.

NOTICIA: Policía Federal quiere un Consejo Nacional de Ciberseguridad

Expertos consultados por **El Economista** ven con buenos ojos el arranque de los trabajos y el documento que pretende sentar las bases de una política urgente ante el crecimiento de las amenazas cibernéticas. Aún así apuntan que esta primera versión está enmarcada en buenas intenciones y vaguedades, por lo que el verdadero reto está por venir.

Una política sin miras a ser obligatoria

Si bien aún es muy pronto para calificar el diseño de la ENCS, los expertos advierten varios elementos que podrían ser contraproducentes si persisten hasta el final del proceso. Uno de ellos es el carácter "voluntario y cooperativo" de esta política pública para entes públicos, sector privado y sociedad civil, planteándose obligatoria únicamente para el Ejecutivo federal.

“A partir de la lectura del documento, observamos que un plan estratégico tiene que ser obligatorio para todas las partes; de lo contrario, la seguridad de un país se verá comprometida a nivel conceptual y en la vida real. Esto se debe a que varios organismos gubernamentales tendrán que trabajar de forma indirecta, directa o incluso subcontratando los servicios del sector privado. Si no existe obligación por parte del sector privado, todo el esquema de seguridad se verá comprometido”, advirtió Dmitry Bestuzhev, director del Equipo de Investigación y Análisis de Kaspersky Lab para América Latina.

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

En esto coincide Carlos Ayala, analista de Arbor Networks, quien consideró que “ lo voluntario genera opcionalidad, y la opcionalidad, inacción; la inacción claramente se contrapone con la cooperación ”.

El carácter voluntario que plantea el documento se suma al escepticismo sobre la perspectiva que tendrá esta política pública. Cédric Laurant, director del programa SonTusDatos de Artículo 12, condenó que se trate de una estrategia que quita responsabilidad al sector privado, así como la obligación de transparentar sus prácticas de protección de datos y respuestas ante vulneraciones.

“Hasta 45% de las vulneraciones de las empresas son ocasionadas por empleados o exempleados que accedieron a documentos por falta de procedimientos de seguridad. Eso no lo veo y tampoco se compromete a crear los presupuestos suficientes para que se haga”, refirió el especialista.

Juan Manuel Casanueva, director general de SocialTIC, criticó que en este primer documento se manejen con la misma prioridad muchos aspectos de concientización de la sociedad, de educación, de información, con el resto de las esferas de acción . Su recomendación es crear diferentes capas de prioridad, empezando por las estructuras básicas del país; después los espacios vitales, con esferas como la financiera y la económica, y por último, la sociedad.

“Si nos basamos en la lógica de gobierno abierto, es mucho mejor que el gobierno brinde los espacios para que grupos de la sociedad civil, con una mirada mucho más transgeneracional, trabajen a nivel educativo. Que las instituciones educativas puedan abordar estas temáticas desde sus propios ámbitos y que sean grupos educativos transgeneracionales los que generen sensibilización y educación a la sociedad”, dijo.

“ Existen casos penosos de campañas de gobierno en materia de derechos digitales, y me refiero a la de *sexting* del INAI, que tienen una carga ideológica con la que limitan libertades básicas de la población . Posiblemente, ahí el Estado no debería estar metiéndose directamente en la educación a la población y dejarlo a grupos de la sociedad civil”, agregó.

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

Este escenario obliga a que en el proceso de diseño se incluyan los mecanismos específicos para dar claridad a las acciones y las responsabilidades de los involucrados en la ejecución de una política de ciberseguridad.

“La visión de la asociación es que la estrategia tenga las cosas claras sobre cómo identificar a las partes interesadas en estos temas; que establezca mecanismos claros de comunicación; que identifique cuáles son las actividades para implementar los planes de contingencias en los casos no previstos y que se establezcan acciones específicas de cómo se aterrizará la estrategia”, dijo Pablo Corona, vicepresidente de Seguridad de la Asociación de Internet.mx.

Una carrera contra el tiempo

En la línea de tiempo delineada por Presidencia se prevé la construcción de la ENCS durante el 2017, para completar su implementación a lo largo del 2018, "con el fortalecimiento institucional y jurídico para fortalecer la coordinación al interior de la Administración Pública Federal, y fortalecer la colaboración del Ejecutivo con los otros entes públicos, y con sectores privado, academia y social".

Estos planes se empalman con la elección presidencial de julio del 2018, lo que genera incertidumbre, ya que en el primer documento no se muestra claramente cómo asegurar su implementación y continuidad transexenial.

NOTICIA: Gobierno mexicano, sin reacción al ciberespionaje estadounidense

"Me parece importante que el gobierno, la industria, la academia y la comunidad técnica no solamente consideren año y medio para implementarlo, sino que incorporen las medidas que le permitirán subsistir al documento. Yo pienso que este documento, en un año, no va a sobrevivir, así que pondría en otro eje la necesidad de continuidad de este plan en materia de ciberseguridad", dijo Laurant, de SonTusDatos.

La industria tecnológica del país, en voz del vicepresidente de Seguridad de la Asociación de Internet.mx, comparte en cierta medida esta visión. "Esta estrategia se está haciendo en un momento en que están cerca los temas electorales y por lo tanto, hay que considerarlos. Una de las preocupaciones es que los mecanismos queden claros para saber cómo se van a aterrizar las acciones, no sólo en el corto, sino en el mediano y largo plazos, y el establecimiento de las responsabilidades, regulaciones y presupuestos que tengan que integrarse", consideró Corona.

Lo cierto es que los llamados a implementar una política pública en ciberseguridad son cada vez más insistentes y urgentes ante el crecimiento de las amenazas informáticas.

NOTICIA: Encuentran malware espía en gobierno de México

En el 2016, México fue el segundo país de América Latina donde se detectaron mayores amenazas cibernéticas, sólo superado por Brasil, de acuerdo con un análisis de Symantec. El año pasado, México concentró 2.09% de las amenazas globales. Este volumen lo posiciona cerca de Vietnam, el décimo país más atacado del mundo, que concentró 2.16% de las ciberamenazas.

A nivel mundial, los costos financieros del cibercrimen ascendieron a 125,900 millones de dólares en el 2016. En México, el impacto llegó a los 5,500 millones de dólares, según Symantec.

julio.sanchez@eleconomista.mx

erp