ieee.es
Instituto Español de Estudios Estratégicos

Documento
Informativo

02/2015 01 de abril de 2015

David Ramírez Morán

LA VISIÓN INTERNACIONAL DE LA CIBERSEGURIDAD

LA VISIÓN INTERNACIONAL DE LA CIBERSEGURIDAD

Resumen:

A nivel global, regional e incluso nacional se están elaborando informes sobre el grado de compromiso de los estados en cuestiones de ciberseguridad. Estos trabajos utilizan diferentes criterios para determinar este grado de compromiso aunque es posible identificar factores comunes entre ellos. Los resultados de estos informes permiten realizar comparaciones entre las naciones. Constituyen, por tanto, una fuente de información de interés que puede ser utilizada para la toma de decisiones en la implantación de normativas y políticas de uso seguro de los sistemas de información.

Abstract:

Several reports on the commitment of the states on cybersecurity matters are being developed on a global, regional and even national basis. These works use different criteria to determine the level of commitment although common factors exist among them. The results of these reports allow for the comparison of the nations. So, they constitute an interesting source of information to be used for decision taking in the implantation of regulations and policies for the safe use of information systems.

Palabras clave:

Ciberseguridad, compromiso, evaluación, NNUU, UIT, UE, UNASUR, OEA.

Keywords:

Cybersecurity, commitment, evaluation, UN, ITU, EU, UNASUR, OAS.

INTRODUCCIÓN

En la ciberseguridad, al igual que en todos los aspectos de la seguridad, los Estados juegan un papel fundamental. La regulación, la gestión y el establecimiento de mecanismos que aseguren los derechos y deberes de los usuarios es una labor fundamental para conseguir el uso seguro de los sistemas de información que permite explotar las ventajas asociadas a la sociedad conectada.

Una pregunta que surge con frecuencia en los eventos relacionados con la ciberseguridad es la duda sobre el puesto que ocupa un determinado país en términos de ciberseguridad, tanto de forma absoluta como de forma relativa. Es difícil proporcionar una respuesta concreta y precisa en un campo donde la evolución se produce de forma vertiginosa y sistemas que un día son seguros pueden verse atacados por una nueva vulnerabilidad en cualquier momento.

Frente a esta incertidumbre, está generalmente aceptado que el compromiso de los estados con la ciberseguridad es un ingrediente imprescindible para la utilización segura de los sistemas de información por los ciudadanos. Este compromiso establece los derechos y obligaciones de los actores involucrados (usuarios, proveedores, etc.) y permite contar con los mecanismos necesarios para tomar las medidas necesarias en el caso de la vulneración de los derechos de los usuarios.

La evaluación del compromiso con la ciberseguridad de los estados es un ejercicio complicado que depende de un amplio número de factores. En esta línea están surgiendo numerosas iniciativas que pretenden obtener una imagen precisa con la que comparar y detectar los puntos de mejora en los que puede trabajar un país.

Las iniciativas se están produciendo en ámbitos con distintos alcances, desde global, como es el caso de Naciones Unidas a través de la Unión Internacional de Telecomunicaciones, regional, como son la Unión Europea, la Organización de Estados Americanos o la Unión de Naciones Suramericanas, o incluso nacional en aquellos casos donde no existe un organismo internacional en el que se reúnen los intereses en el campo de la ciberseguridad de los miembros de la región.

Aunque se ha intentado dar una cobertura global, en el caso de África no se ha identificado un documento específico en el que se recogieran específicamente datos de la zona.

LA UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

La UIT publicó el 9 de diciembre de 2014, en el ITU Telecom World 2014 celebrado en Doha, el Global Cybersecurity Index[1], un trabajo de investigación en el que se elaboraba un índice con el que evaluar el compromiso con la ciberseguridad de las naciones. Se pidió la participación voluntaria de los países rellenando un formulario que se centraba en cinco aspectos para realizar la evaluación:

- Medidas legales
  - Legislación penal
  - Reglamentación y conformidad
- Medidas técnicas
  - CERT-CIRT-CSIRT
  - Normas
  - Certificación
- Medidas orgánicas
  - Política
  - Hoja de ruta para la gobernanza
  - Organismo responsable
  - Análisis comparativos nacionales
- Capacitación
  - Desarrollo de la normalización
  - Desarrollo de la mano de obra
  - Certificación profesional
  - Certificación de los organismos
- Cooperación
  - Cooperación intraestatal
  - Cooperación intraorganismos
  - Colaboraciones público-privadas
  - Cooperación internacional

1 http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

En total, en la edición de 2014, participaron 104 países mientras que para aquellos que no remitieron la información, hasta un total de 194, se hizo una estimación a partir de la información disponible. La primera posición del ranking la ocupa Estados Unidos, seguido de cerca por Canadá. España figura en el puesto 29 de la lista aunque queda clasificada en 9ª posición empatada con otros países debido a la reducida granularidad de las puntuaciones.

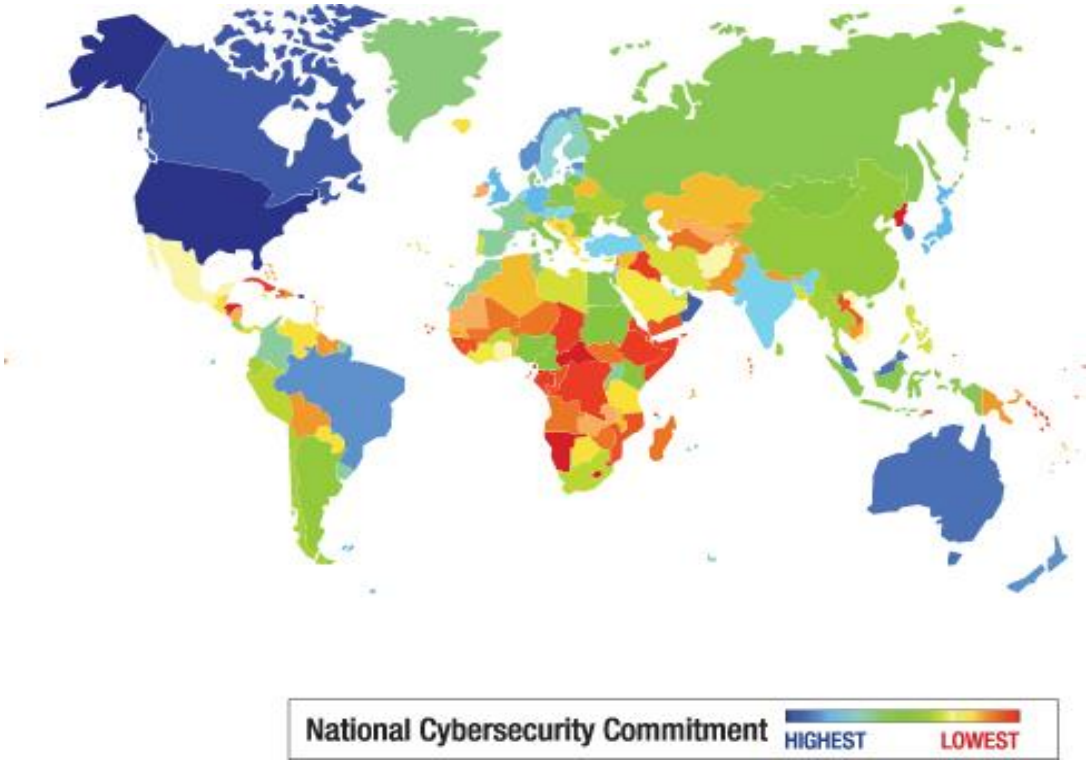

Figura 1. Grado de compromiso nacional (Fuente: ITU y ABI Research)

En Iberoamérica el nivel de compromiso toma valores medios salvo excepciones puntuales, tanto positivas como es el caso de Brasil como negativas en el caso de Honduras, igualando o incluso superando los valores medios registrados en el continente asiático, aunque por debajo de los que obtienen los países europeos.

Tan significativo como la parte alta de la tabla es la parte baja. A este respecto, el continente africano y oriente próximo concentran las menores calificaciones de la lista de países, como se observa en el mapa de colores elaborado en el estudio.

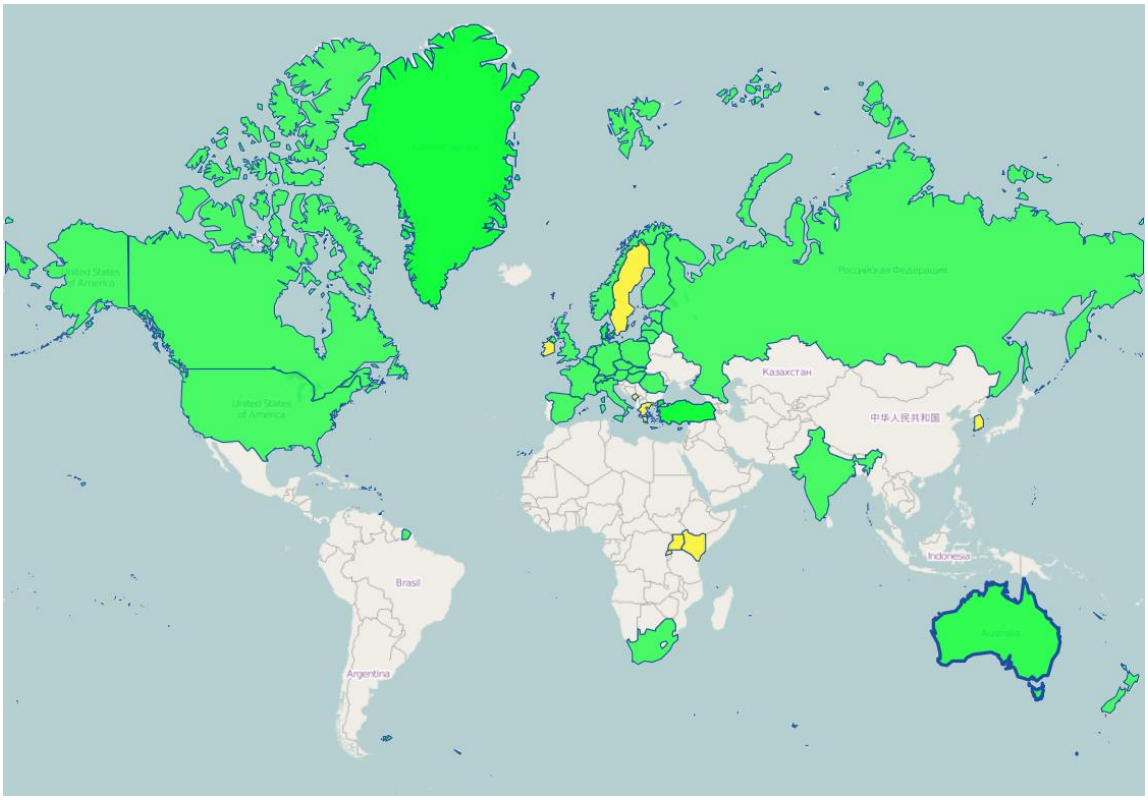

Figura 2. Países con estrategia de ciberseguridad (Fuente: ENISA)

LA VISIÓN DE LA UNIÓN EUROPEA

La evaluación de la ciberseguridad de un país por parte de la Unión Europea presta una especial atención a la existencia de una estrategia de ciberseguridad. En su página web[2] es posible consultar la lista de países que cuentan actualmente con una estrategia o que están en el proceso de su elaboración.

Por regiones destaca Europa donde un porcentaje elevado de los países ya tienen publicada la estrategia o están en proceso de su elaboración (Irlanda, Suecia y Montenegro). Quedan fuera de esta lista Portugal, Islandia, Suiza, Eslovenia, Bosnia, Serbia, Croacia, la ex-república yugoslava de Macedonia, Albania, Bulgaria, Moldavia, Ucrania y Bielorrusia.

En Norteamérica tanto Estados Unidos como Canadá cuentan también con su propia estrategia de ciberseguridad.

2 https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

En Sudamérica es significativo que sólo un país cuenta con estrategia de ciberseguridad, Trinidad y Tobago, mientras que el resto de territorios de la zona que cuentan con una estrategia son los territorios de ultramar de Francia, Reino Unido y Holanda. El resto de países no cuentan con estrategia de ciberseguridad, o al menos no se lo han comunicado a ENISA.

Del continente asiático tienen estrategia de ciberseguridad India, Rusia y, aunque todavía está en preparación, Corea del Sur. Cabe destacar la ausencia en esta lista de Japón y de todos los países del sudeste asiático, el primero por la profunda penetración que tienen las nuevas tecnologías en su población y los otros por la intensa actividad económica y comercial que se está concentrando en la zona. También es destacable la ausencia de China en esta lista, lo cual choca con la intensa actividad cibernética que se les atribuye internacionalmente.

En el territorio africano solamente cuatro países aparecen reflejados, Sudáfrica, que ya cuenta con una estrategia de ciberseguridad y Kenia, Uganda y Ruanda, que están preparándola.

En Oceanía cuentan con estrategia de ciberseguridad los dos principales países de la zona, Australia y Nueva Zelanda, como cabe esperar fruto de su estrecha relación con Estados Unidos, Reino Unido y Canadá, formando el grupo denominado Five Eyes que colabora en actividades de ciberseguridad.

En contraste con este criterio, países que no cuentan con una estrategia de seguridad obtienen una buena calificación en el informe elaborado por la UIT, como por ejemplo Brasil, Japón, Omán o Colombia, que superan o igualan la clasificación de España.

LAS ORGANIZACIONES INTERNACIONALES AMERICANAS

Junto al punto de vista global que proporciona la ITU y el centrado en la Unión Europea de ENISA, en el territorio americano hay dos organizaciones internacionales entre cuyos intereses figura la ciberseguridad: la Organización de Estados Americanos (OEA) y la Unión de Naciones Suramericanas (UNASUR).

La OEA elaboró en 2004 la Estrategia de Ciberseguridad[3] basada en tres pilares: CICTE, CITEL y REJMA, constituidos por grupos de expertos.

3 AG/RES. 2004 Cyber security strategy (Resolution) http://www.oas.org/cyber/documents/resolution.pdf

- CICTE persigue la formación de una red de vigilancia, alerta y aviso interamericana para diseminar rápidamente la información de ciberseguridad y responder a las crisis, incidentes y amenazas a la seguridad informática.
- CITEL consiste en la identificación y adopción de normas técnicas para una arquitectura de internet segura.
- REMJA asegura que los Estados Miembros de la OEA cuentan con las herramientas legales necesarias para proteger a los usuarios de internet y las redes de información.

En 2012 se reafirmó por parte de los Estados Miembros el compromiso con la Estrategia[4] añadiendo la promoción de la colaboración público privada y la elaboración de estrategias de ciberseguridad por parte de las naciones.

La OEA también publica periódicamente informes sobre ciberseguridad donde se incluyen las principales tendencias sobre ciberseguridad de la región latinoamericana y se hace una descripción de la evolución de la implantación de medidas de ciberseguridad por parte de los Estados Miembros. En su informe de 2014 se hace un detallado análisis sobre todos los países de la región[5], a excepción de Cuba, por no pertenecer actualmente a la organización.

Dentro de UNASUR existe desde 2012 una iniciativa para promover la ciberseguridad entre sus Estados Miembros[6]. El pasado mes de febrero se anunciaba la puesta en marcha de un proyecto para mejorar la conectividad mediante la interconexión por fibra óptica de las redes de los Estados Miembros, lo que contribuirá a incrementar la velocidad de conexión[7], considerada hasta 16 veces más lenta y hasta 20 veces más cara que en los países desarrollados, y a reducir el coste para los usuarios. Con esta nueva interconexión «se da respuesta a la necesidad de generar procesos de valor añadido y de dotar con autopistas de información con las que fortalecer la independencia y la ciberdefensa de la región», de acuerdo a las declaraciones del Secretario General de Unasur, Ernesto Samper.

LA REGIÓN DE ASIA PACÍFICO

En esta región no consta un organismo internacional que aglutine u orqueste las acciones

4 Declaration strengthening cyber-security in the americas.
http://www.oas.org/cyber/documents/Declaration.pdf
5 Latin American + Caribbean Cyber Security Trends June 2014
http://www.oas.org/cyber/documents/OAS-Symantec_Cyber_Security_Report_ENG.pdf
6 Licenciada Candela Justribó. Ciberdefensa: Una visión desde la UNASUR pp 3-6
http://sedici.unlp.edu.ar/bitstream/handle/10915/44716/Documento_completo.pdf?sequence=1
7 La Unasur quiere tener el primer anillo de fibra óptica hecho en Latinoamérica
http://www.infobae.com/2015/02/10/1626008-la-unasur-quiere-tener-el-primer-anillo-fibra-optica-hecho-latinomaerica

sobre ciberseguridad. Se cuenta con un documento elaborado por el Australian Strategic Policy Institute[8] en el que se analiza el compromiso de los países de la zona en lo que respecta a la ciberseguridad de acuerdo a cuatro indicadores:

- Gobernanza
  - Estructura organizacional
  - Legislación/regulación
  - Aspectos internacionales: gobernanza y tecnología/políticas
  - CERT
- Militar
  - Rol de los militares en el ciberespacio
- Negocio
  - Diálogo gobierno-industria
  - Economía digital
- Social
  - Consciencia pública
  - Conectividad a internet

De acuerdo a este informe, lideran la clasificación Japón y Singapur, que muestran un elevado grado de madurez en todos los aspectos analizados (al igual que EEUU y Reino Unido, que aparecen en el informe a título comparativo) seguidos de cerca por Australia y Corea del Sur. En el otro extremo se encuentran Camboya, Papúa Nueva Guinea y la República Democrática Popular de Corea, que cierra la clasificación.

CONCLUSIONES

Cada vez existe una consciencia más generalizada de la necesidad de abordar los problemas de ciberseguridad de forma conjunta. Prueba de ello es la creciente participación de los estados en las diversas iniciativas internacionales que contribuyen a la compartición de información sobre los riesgos y amenazas y que proporcionan los medios con los que alcanzar un mayor grado de ciberseguridad, como puede ser la realización de ejercicios, la impartición de cursos de formación y la creación de puntos de contacto entre expertos.

Frente a esta tendencia a la colaboración, también están surgiendo disensiones debido a la

8 Cyber maturity in the Asia-Pacific region 2014, ASPI International Cyber Policy Centre https://www.aspi.org.au/publications/cyber-maturity-in-the-asia-pacific-region-2014/ASPI_cyber_maturity_2014.pdf

importancia que la protección de la información está tomando en la actual sociedad del conocimiento. Así, pese a la creciente compartición de la información, también se está incrementando el interés de las naciones por contar con herramientas propias con las que salvaguardar la independencia y la seguridad.

El avance de las iniciativas contrasta en su velocidad con el rápido desarrollo que se está produciendo en el campo de las tecnologías de la información y, especialmente, en el de los ataques y amenazas a los sistemas. Resulta destacable a este respecto que aquellos países que han sido objeto de ataques dirigidos a su territorio o su información, como es el caso de EEUU, Brasil, Corea del Sur, etc. son los que actualmente cuentan con un mayor grado de compromiso y presentan una evolución más rápida en la implantación de normas y políticas.

Por último, queda patente la necesidad de contar con mecanismos de evaluación con los que determinar el grado de compromiso con la ciberseguridad así como las líneas que se deben potenciar para mejorarlo. Al igual que son necesarios estos mecanismos de evaluación, destaca la variabilidad que puede producirse en función de los criterios utilizados para determinar los indicadores y las calificaciones asignadas a cada aspecto considerado.

David Ramírez Morán
Analista del IEEE