La seguridad digital debería ser una responsabilidad fundamentalmente del Estado.

Alex Javier Porras Palma (Líder)
Cristina Díaz García (Relatora)
Juan Antonio Jiménez Pedraza

18 de mayo de 2018

Índice

1. Introducción

Vivimos en una sociedad en la cada vez más, la tecnología está presente en nuestras actividades cotidianas, incluso en nuestra vida personal. Desde realizar transacciones bancarias, hasta ver la televisión. La rápida evolución de las **Tecnologías de la información y la Comunicación** han contribuido indiscutiblemente al bienestar y progreso de las sociedades. Sin embargo, también ha aparecido un número cada vez mayor de riesgos y amenazas, dando lugar a un ciberespacio cada vez más hostil. Es por esto que se hace imprescindible gestionar eficazmente la seguridad de las tecnologías digitales, ayudando a los ciudadanos a que hagan uso de servicios avanzados y se relacionen a través de medios electrónicos con confianza. La seguridad digital nace para solventar este problema.

La seguridad digital es el área de la informática dedicada a la protección de información confidencial. Esto incluye software (bases de datos, metadatos, archivos) y hardware.

También tenemos que tener en cuenta en manos de quién apoyamos la responsabilidad de proteger esos datos, ya que les estaríamos dando la llave de la privacidad. En las manos equivocadas podrían usar los datos para motivos diferentes. Por eso en este trabajo se propone que el Estado sea quien tenga la responsabilidad de proteger dichos datos.

2. El Estado como entidad de protección digital

Actualmente existen varios países que cuentan con un equipo especializado en seguridad digital. En China, el **Ejército de Liberación Popular** cuenta con 15.000 hackers. En Corea del Norte **entrenan** a sus jóvenes más hábiles en tácticas de pirateo informático con el propósito de que entren en el *Bureau 121*, su ejército de miles de hackers que combaten en la guerra digital.

El año pasado, un ransomware malicioso llamado *WannaCry*, el virus más destructivo que se ha visto jamás, **infectó** a 1.200 empresas en España.

El gobierno español está convencido de impulsar un equipo de seguridad digital estatal. Ya se han destinado 400.000 euros para becas de formación.

3. Seguridad digital en España

Este año el Gobierno ha anunciado que destinará 20 millones de euros más para reforzar la ciberseguridad nacional. Además, se ha creado un nuevo organismo, el Centro de Operaciones de Ciberseguridad de la Administración General del Estado, que estará operativo el próximo verano.Este organismo funcionará como

un mando único de ciberseguridad para la Administración del Estado, coordinará las acciones de ciberseguridad en ministerios y entidades públicas, pero no en las comunidades autónomas ni en los ayuntamientos.

El nuevo organismo público ha sido anunciado por la vicepresidenta del Gobierno, Soraya Sáenz de Santamaría, en la inauguración de las XI Jornadas STIC CCN-CERT, celebradas en Madrid. El encuentro, que concentró a administraciones, empresas y a algunos de los grandes especialistas de la ciberseguridad en España, pretendía detectar a los mejores talentos y soluciones para mejorar la defensa nacional, también a nivel digital, con programas creados desde la Administración.

El futuro Centro de Operaciones de Ciberseguridad de la Administración General del Estado centralizará recursos que hasta ahora dependían de cada ministerio y estará coordinado con otros organismos ya existentes, como el Centro Nacional de Inteligencia (CNI), el Centro Nacional de Ciberseguridad (Incibe) y la entidad que coordina la respuesta ante incidentes tecnológicos, el CCN-CERT.

4. Seguridad digital en Andalucía

El plan de seguridad y confianza digital Andalucía 2020 persigue los siguientes objetivos:

1. Potenciar la adopción de buenas prácticas en materia de seguridad digital en la administración autonómica y local de Andalucía.
2. Extender la cultura de confianza y seguridad digital, mediante programas de sensibilización, asistencia y formación, con especial atención a los menores.
3. Impulsar el mercado de la seguridad digital y la creación de empleo, mediante el estímulo de la oferta y la demanda de productos, servicios y profesionales de la seguridad digital.
4. Reforzar las capacidades de prevención, detección y respuesta a incidentes de seguridad en Andalucía (AndalucíaCERT).

Las líneas de trabajo del plan son:

1. Coordinación de la seguridad TIC en la Administración autonómica, potenciando la adopción de buenas prácticas y ofreciendo servicios de asesoramiento, apoyo y coordinación.
2. Formación y concienciación de los trabajadores del sector público, la ciudadanía y las empresas, y extensión de la cultura de confianza y seguridad digital.

3. Impulso de la industria de la seguridad digital, mediante el estímulo de la oferta y la demanda de productos, servicios y profesionales de la seguridad digital, y promoción de la adopción de buenas prácticas y de la cultura de seguridad en el tejido empresarial andaluz.

4. Coordinación con otras Administraciones y Organismos Públicos en materia de seguridad TIC.

5. Protección frente a ciberamenazas, mediante la mejora de las capacidades de prevención, detección y respuesta a incidentes de seguridad en Andalucía (a través del centro AndalucíaCERT).

5. El sector privado y la seguridad digital

No hace mucho tiempo pudimos ver como el CEO de facebook estaba declarando ante un tribunal por comerciar con los datos privados de sus usuarios.

En 2014, la compañía **Cambridge Analytica** se había metido en el bolsillo quince millones de dólares invertidos por un donante republicano, con el propósito de encontrar una manera de identificar las personalidades de los votantes americanos e influenciar su comportamiento. Lo único que les faltaba eran los datos para hacer que su producto funcionase.

Así que la firma decidió recaudar información privada de perfiles de facebook de más de **cincuenta millones** de usuarios sin su consentimiento, convirtiéndose en la mayor filtración de datos en la historia de las redes sociales. La brecha permitió que la compañía explotase los datos privados de gran parte de la población votante, desarrollando técnicas que apoyaban a la campaña del presidente Trump.

Los datos incluían detalles de las identidades de los usuarios, amigos y likes. La idea era asociar rasgos de personalidad basados en lo que la gente hizo "me gusta" para luego usar esa información para enviar publicidad especializada.

Este tipo de herramientas pone en mercado a la firma y a los ricos inversores de los partidos conservadores el poder de cambiar la política.

6. Responsabilidades del Estado

El equipo responsable de la seguridad digital no debe ser ligado a ningún partido político y debe entenderse como un poder aparte, como lo son el judicial y el ejecutivo. De esta manera intentaremos que las políticas de protección de datos no caigan en manos de intereses políticos ni campañas electorales.

El equipo debe estar dirigido y formado por expertos en el sector. Los puestos deben conseguirse en base a los méritos de los interesados.

Los datos no pueden ser accesibles, para ningún otro objetivo que no fuese para el que fue destinado. La única excepción sería si éstos fuese necesarios para aportar pruebas de un delito, como es el propio Estado el que tendría acceso a los datos en caso de ser necesario, sería más fácil detener a criminales que se aprovechan de las encriptaciones de las comunicación para organizar sus crímenes, y por lo tanto, disminuiría la tasa de criminalidad.

7. Conclusiones

En definitiva, las razones principales por las cuales el Estado debería ser responsable de la seguridad digital son:

1. Los intereses del estado no van más allá de la mera protección de los datos, no tienen intenciones económicas.
2. El estado goza de mayores recursos para mejorar la seguridad.
3. El estado potenciaría la creación de empleo en el campo de la seguridad digital y promovería la educación en este campo.
4. Reducción de la tasa de criminalidad.

8. Bibliografía

Noriega, Samuel (2014 - 2015). Seguridad Digital. Certsuperior.
https://www.certsuperior.com/Blog/seguridad-digital

De la Cal, Lucas; Negre Javier (21/05/2017). Casting de 'hackers' para defender a España. El Mundo.
http://www.elmundo.es/cronica/2017/05/21/5920208be5fdea60568b45aa.html

Granville, Kevin (19/03/2018). Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens. NY Times.
https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

Rosenberg, Matthew; Confessore, Nicholas; Carwalladr, Carole (17/03/2018). How Trump Consultants Exploited the Facebook Data of Millions.
https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

Jané, Carmen (13/12/2017). España refuerza con 20 millones más la protección ante ciberataques. Madrid. elPeriódico.

https://www.elperiodico.com/es/sociedad/20171213/el-gobierno-crea-un-mando-unico-de-ciberseguridad-6491802

Junta de Andalucía. (2018) Seguridad y Confianza Digital. http://www.juntadeandalucia.es/organismos/empleoempresaycomercio/areas/tic-telecomunicaciones/seguridadyconfianzadigital.html