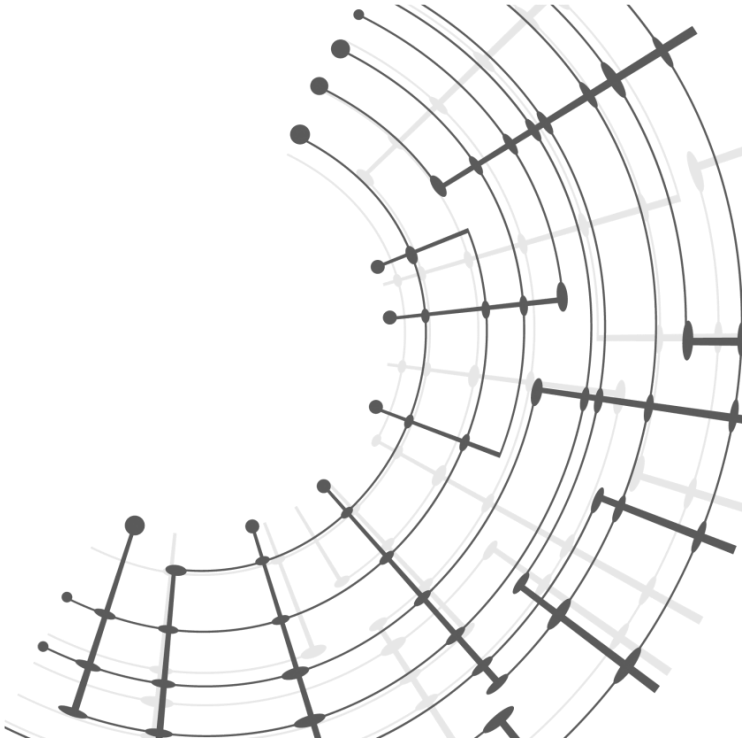
Universidad de Málaga

E.T.S. DE INGENIERÍA INFORMÁTICA



La seguridad digital es responsabilidad fundamentalmente del sector privado

Proyectos y Legislación - Grupo A

Integrantes:

Marcos Hidalgo Baños	marcos_hidalgo_banos@uma.es
Juan Cubo Bravo (líder)	juancubo@uma.es
Carlos Marfil Barranco (relator)	carlosmarfilbarranco@uma.es
Alejandro Bermúdez Aviñón	alejandroba@uma.es

Índice de contenidos

1. Introducción al tema

Definimos la **seguridad digital** como las diferentes formas de protección de datos e información en línea para que no sean robados, dañados o comprometidos.

En las últimas décadas ha cobrado mayor relevancia en el proceso de creación de los proyectos tecnológicos y ha logrado introducirse en la mayoría de los planes estatales de las principales potencias mundiales. En ellos, se destaca principalmente la importancia de la **colaboración público-privada**, donde el Estado establece los estándares generales que las propias empresas deben cumplir.

En los países occidentales suele ser el sector privado el que regula la seguridad en entornos digitales, pero a medida que nos desplazamos a Oriente, el control que los Estados ejercen sobre los datos de los ciudadanos es mayor.

Entonces… ¿Qué situación es la correcta? ¿Debería tener el **Estado** un papel más activo en el proceso? ¿O bien están en lo cierto los países occidentales dejando la seguridad digital fundamentalmente en manos de las **empresas**? Nosotros creemos en esta última postura basándonos en una serie de argumentos que expondremos a continuación.

2. Desarrollo de los argumentos

2.1. El principal motor de la innovación es el sector privado

El sector privado suele estar impulsado por la **competencia** y la **búsqueda de beneficios económicos**, por lo que las principales ventajas de que la seguridad digital esté en manos de estas empresas son la innovación, la agilidad, la eficiencia y otro punto a favor es que tienen la capacidad de invertir en **tecnologías de vanguardia** como el análisis de big data, las inteligencias artificiales o la encriptación avanzada, entre otras, con el objetivo de proteger los datos de sus clientes.

Con respecto a la **innovación** este tipo de empresas al buscar beneficio económico como hemos mencionado anteriormente invierte en diversas tecnologías y soluciones de seguridad que pueden llevar a avances más rápidos y eficientes en la **protección de los datos** o en la prevención de **ciberataques** a diferencia del Estado que para llegar a conseguir los mismos objetivos tendrían que destinar muchos recursos al tema de la seguridad lo que conllevaría a recortes en diversos sectores como el económico o el médico.

Con el tema de la **eficiencia** en el sector privado se llevan a cabo la implementación de soluciones de seguridad digital en términos de costo, las empresas **optimizan los recursos** y encuentran formas innovadoras de ofrecer servicios para la seguridad a un costo razonable, con las distintas soluciones lo que se intenta conseguir es mantener una **ventaja competitiva** en el mercado.

2.2. El sector privado atrae un talento que el Estado es incapaz de captar

Faltan profesionales de ciberseguridad. Esa es la realidad que vive a día de hoy un sector que parece no parar de crecer. Las empresas de nuestro país se "**pelean**" entre ellas para poder conseguir estos **preciados profesionales**, y gracias al teletrabajo, también contra empresas extranjeras, cuyas ofertas son muy difíciles de igualar por los superiores sueldos que ofrecen.

En este escenario tan tensionado, el Estado también ha de ser capaz de captar parte de ese talento, y no puede obligarles a trabajar para él, puesto que aludiendo al **principio de justicia**, estos profesionales tienen todo el derecho a elegir la oferta que más les beneficie, para compensar los años de formación y el valor que aportan en su trabajo. Sabiendo esto, el Estado **ha de convencerles**, y no lo tiene nada fácil por varias razones.

En primer lugar, las empresas privadas cuentan con la ventaja de poder ofrecer **mejores sueldos** que el Estado, dado que éste tiene que financiar multitud de necesidades ciudadanas más allá de la ciberseguridad. Además, las empresas dan mayor facilidad para el **teletrabajo**, el **escalado de puestos** y la propia **contratación**, pues en las ofertas públicas es necesario, además de la carrera universitaria, aprobar unas oposiciones y tener la nacionalidad española, algo que es especialmente grave, ya que anula la posibilidad de captar talento extranjero. Finalmente, el principal atractivo de ser funcionario (tener un **empleo estable**) no es relevante para estos profesionales pues saben que están muy demandados.

Por todo ello, relegar la seguridad digital fundamentalmente al Estado sería un **error**, pues no sería capaz de captar los suficientes profesionales como para sustituir la labor del sector privado, llevándonos a un escenario de **mayor inseguridad**. Por lo que, en aras del **bien común** y la **seguridad** de nuestra sociedad, debemos mantener al sector privado como el principal responsable de la seguridad digital.

2.3. El sector privado tiene mayor capacidad de reacción y recursos

La seguridad digital es un aspecto crítico para la protección de datos personales y financieros en la era digital actual. Si bien tanto el sector privado como el gobierno tienen un papel que desempeñar en la protección contra amenazas cibernéticas, la empresa privada **puede responder más rápido** ante cualquier problema de seguridad digital.

Una de las principales ventajas que tiene el sector privado en la protección de la seguridad digital es su capacidad para responder rápidamente ante cualquier problema. Las empresas privadas tienen recursos y personal dedicado a la seguridad digital, lo que les permite detectar y remediar problemas de seguridad de manera rápida y eficiente. Además, las empresas privadas tienen **incentivos financieros** para responder rápidamente a las amenazas de seguridad digital, ya que cualquier interrupción en los servicios en línea puede tener un impacto significativo en la confianza del cliente y en los ingresos de la empresa.

El Estado como tal **no tiene clientes** de los que dependa, sino ciudadanos contribuyentes que lo seguirán haciendo a pesar de que ocurran brechas de seguridad. Un ejemplo de esto fue el sonado ciberataque que sufrió el SEPE, dejando la página web bloqueada durante días y provocando el retraso del cobro del paro. Una empresa privada no puede permitir esto. Aunque estas **no son infalibles**, sufren brechas y ataques. La diferencia radica en la **reacción** ante estos ataques. Todos alguna vez hemos experimentado una caída de alguna red social (WhatsApp, Twitter, Instagram…), pero estas duran horas gracias a la labor de sus técnicos de ciberseguridad. Es imposible que ocurra un evento similar a lo del SEPE.

También muchas empresas ofrecen **programas de recompensas por vulnerabilidades** para incentivar a los investigadores de seguridad a identificar y reportar posibles vulnerabilidades en su software o sistemas. Un ejemplo de esto es Microsoft Bug Bounty Program. En este programa se recompensa el reporte de vulnerabilidades de productos Microsoft con cuantías de hasta cien mil dólares. Estas prácticas sólo las llevan a cabo las empresas, no el Estado, por lo que podemos afirmar que su **capacidad de reacción y recursos es mucho mayor** al de cualquier gobierno.

2.4. ¿Es centralizar la solución para garantizar la seguridad digital?

A lo largo de la historia, el papel de los Estados como principal dirigente de aspectos comunes a sus ciudadanos como pueden ser el económico, con la administración de la moneda, o el social mediante la legislación ha logrado establecer un **orden centralizado** en el que el ciudadano delega en sus dirigentes la responsabilidad de proteger sus derechos.

Con el progreso tecnológico, destacando principalmente la **digitalización** de numerosos sectores, surgen nuevas alternativas para gestionar de manera **descentralizada** dichos aspectos, como pueden ser las criptomonedas o las redes sociales.

Sin embargo, estas herramientas pueden ser empleadas para fines completamente opuestos. El mejor ejemplo para definir este caso tal vez sea **China**, dónde el Estado es capaz de inmiscuirse en la vida cotidiana de sus ciudadanos para defender **"el bien común"** aunque ello suponga perder derechos fundamentales por el camino, situación que parecen aceptar.

En el artículo de EL PAÍS citado en las referencias bibliográficas, se comenta cómo la región china de Xinjiang "es el primer gran modelo en la era de la vigilancia digital masiva" y que en China "no se podía consultar el Gmail de la universidad o algunas redes sociales".

En este contexto, la **seguridad digital** no es más que un aspecto más de la larga lista de derechos que el Estado chino administra en nombre de sus ciudadanos, ejerciendo de protector y reprimidor de las posibles amenazas que se generen.

En este caso, no existe ninguna entidad superior que controle el buen hacer del Estado.

En los países occidentales, gracias a la separación de poderes este tipo de situaciones autoritarias son mayormente evitadas y se relega en el sector privado para que se garanticen los derechos designados por documentación oficial como pueden ser los Planes Estatales.

Una **colaboración público-privada** efectiva, donde el Estado legisla para guiar a las empresas en la implementación de sus propios sistemas de seguridad digital de los cuales son responsables ellos mismos, dota al ciudadano de capacidad para elegir cuál es el proveedor que más se ajusta a sus necesidades, evitando la imposición o falta de libertad de elección.

3. Conclusiones del estudio realizado

I. **Las empresas privadas pueden obtener grandes ventajas frente al Estado gracias a la innovación y al desarrollo de tecnologías de vanguardia.**

II. **El sector privado blinda nuestra seguridad digital, pues es capaz de captar un talento para el cual el modelo de contratación público no resulta atractivo.**

III. **El sector privado tiene mayor capacidad para reaccionar ante ciberataques debido a que invierte más recursos en seguridad digital que el Estado.**

IV. **Otorgar al Estado capacidades para controlar la seguridad digital reduce las libertades de los ciudadanos, con la justificación de proteger sus derechos.**

4. Bibliografía

- *https://www.cope.es/actualidad/tecnologia/noticias/falta-profesionales-ciberseguridad-20220129_1719822*
- *https://www.incibe.es/empleo*
- *https://www.infojobs.net/ofertas-trabajo/ciberseguridad*
- *https://www.microsoft.com/en-us/msrc/bounty*
- *https://www.lasprovincias.es/economia/trabajo/sepe-caida-20211010141117-nt.html?ref=https%3A%2F%2Fwww.google.com%2F*
- *https://elpais.com/tecnologia/2022-05-05/xinjiang-es-el-primer-gran-modelo-en-la-era-de-la-vigilancia-digital-masiva-nunca-se-ha-visto-nada-igual.html*