*Fernando Ballestero**

LA CIBERSEGURIDAD EN TIEMPOS DIFÍCILES
¿Nos ocupamos de ella o nos preocupamos por ella?

La crisis del COVID-19 ha puesto en evidencia la vulnerabilidad de nuestras sociedades y nuestras economías. Pero el gran aumento del teletrabajo y las ventas *online*, sin la adecuada protección ante los virus informáticos o *malwares*, ponen sobre la mesa otro tipo de vulnerabilidad existente, el posible gran aumento de los ciberdelitos en los próximos meses. De ahí que sea necesario sensibilizarse más ante esta vulnerabilidad. Para ello se hace un repaso de la evolución de la ciberseguridad, sus tendencias y principales amenazas y el marco institucional que regula esta actividad. Aunque tenemos un ecosistema bien desarrollado, sigue siendo insuficiente el nivel de concienciación, en especial entre pymes, muchas instituciones y ciudadanos.

Palabras clave: ciberseguridad, riesgos digitales, ecosistema de ciberseguridad, crisis, vulnerabilidad.
Clasificación JEL: A19, D83, L86, M14, O30.

1. Introducción. Virus biológicos y virus digitales

La crisis por el COVID-19 ha puesto de manifiesto la vulnerabilidad de nuestras sociedades y de nuestra economía. Un virus transmitido de un animal a humanos en una ciudad del interior de China ha provocado, en menos de tres meses, medidas de aislamiento de ciudades y regiones en varios países, cierre de fronteras al movimiento de personas y un fuerte impacto negativo en muchos sectores de la economía.

Pero, con independencia de las lecciones que todos saquemos, cuando se supere esta crisis, sobre la necesidad de prevenir y de protegerse ante futuras posibles epidemias y pandemias, no estaría de más, ahora que se intensifica el teletrabajo, que pensáramos también en las vulnerabilidades ligadas a otro tipo de virus: los llamados virus digitales.

Realmente no debería hablarse de virus digitales; lo correcto sería utilizar los términos *malware* o *software* malicioso. Pero así se les llamó inicialmente por su analogía con los biológicos a la hora de infectar un cuerpo, en este caso el *software* de un ordenador, tableta o teléfono, sin que el cuerpo invadido haya detectado esa intrusión, si bien el proceso de infección o propagación es muy diferente. También se llamaron antivirus a los programas para detectarlos y anularlos. ▷

* Doctor en Economía, Técnico Comercial y Economista del Estado. Miembro de la Junta Directiva de la World Compliance Association. Exmiembro del Consejo de la OCDE.

Versión de marzo de 2020.
DOI: https://doi.org/10.32796/bice.2020.3122.6993

El hecho es que cada vez más va siendo muy cierta la afirmación que hiciera el CEO de una gran compañía, hace ya unos años, cuando dijo que hay dos tipos de empresas: las que han sufrido un ataque informático en el último año y las que no son conscientes de que lo han sufrido.

Por ello, resulta imprescindible saber hoy ante qué ciberamenazas nos encontramos y qué actitud y qué estrategia debemos de adoptar para reducir nuestra vulnerabilidad y la de la sociedad en su conjunto. Y, más aún, en unos tiempos difíciles como los que estamos viviendo en que los ciberdelincuentes, aprovechando el *boom* del teletrabajo, las compras *online* y el envío masivo de mensajes, sin contar en muchos casos con sistemas y procedimientos de protección adecuada, pueden estar ganando un espacio muy importante que después explotarán.

2. Las ciberamenazas a las que nos enfrentamos

2.1. Las amenazas informáticas y la ciberseguridad

El término «ciberseguridad» se ha generalizado hoy día en nuestra sociedad y, junto a él, algunos otros como ciberdelincuencia, ciberterrorismo, ciberataque, ciberdefensa, etcétera.

Podemos decir que la ciberseguridad es la capacidad de resistir, con un nivel determinado de fiabilidad, a toda acción que comprometa la disponibilidad, autenticidad, integridad, o confidencialidad de los datos almacenados o transmitidos, o de los servicios ofrecidos[1].

[1] Definición tomada del art. 3.3b del RDL 12/2018, de 7 de septiembre, que transpone la Directiva NIS de la UE, de redes y sistemas de información. BOE del 8 de septiembre de 2018.

Es evidente que tanto en el mundo físico como en el virtual la seguridad al cien por cien no existe, pero se trata de reducir al máximo posible los riesgos de que una amenaza o un evento potencial negativo se materialice y cause un daño.

En este sentido, se llama «amenaza» a cualquier circunstancia o evento que puede explotar, intencionadamente o no, una vulnerabilidad específica de un sistema u organización. Puede ser un incendio, un corte en el suministro eléctrico, un bloqueo de acceso provocado a una página web, un robo de información, la suplantación del titular de una cuenta de correo electrónico, etcétera. Por su parte, «vulnerabilidad» es la debilidad, la falta de protección o la falta de control que puede permitir que una amenaza se materialice provocando ese impacto negativo. Por ejemplo, no tener adecuada protección contra incendios o tener un deficiente sistema de claves de acceso restringido a la información. A su vez, la probabilidad de que esto suceda, esto es, de que una amenaza concreta se materialice, es lo que se llama «riesgo». La ciberseguridad, por tanto, busca reducir los riesgos en el ámbito digital.

Pero ¿quién puede provocar ese tipo de hechos o incidencias? Se considera que los diferentes tipos de agentes que pueden provocar un problema de ciberseguridad son:

- *Agentes naturales* sin intencionalidad ni motivación. Por ejemplo, un desastre natural o un error humano.
- *Agentes de perfil bajo*. Individuos aislados o poco organizados que actúan normalmente con fines exclusivamente personales.
- *Cibercriminales*. Organizaciones mafiosas o de crimen organizado que pretenden obtener un beneficio económico ▷

o provocar daños de acuerdo con sus intereses.
- *Ciberterroristas*. Organizaciones terroristas en acciones de propaganda, reclutamiento y atentados contra sistemas de información.
- *Ciberactivistas*. Grupos antisistema, de extremismo radical político o ideológico, que actúan principalmente para desacreditar o dañar a las instituciones.
- *Estados*. Cuando estos dan continuidad a los conflictos físicos extendiéndolos al mundo virtual, pudiendo ir desde las simples campañas de desprestigio, la intromisión en procesos electorales o, de modo más amplio, hasta la ciberguerra.

En este contexto, y relacionados con ellos, hay que añadir una categoría específica, los *hackers*, que son aquellas personas que realizan actividades ilícitas para vulnerar la seguridad de equipos y sistemas por cuenta propia siguiendo una motivación o por cuenta ajena a cambio de una retribución.

Pero estos no deben confundirse con los llamados *hackers éticos*, o *white hat hackers*, surgidos en los últimos años y que se dedican a encontrar vulnerabilidades en el *software* para que puedan ser corregidos o «parcheados», aumentando así su seguridad. Pueden actuar de modo independiente cobrando por su trabajo, y de hecho muchas empresas de *software* acuden a ellos para mejorar la seguridad de productos que desarrollan o que están ya en el mercado. Muchas veces, los comunicados de que debemos actualizar una versión responden a ello. Y es que no hay que olvidar que, en general, y sobre todo hasta hace pocos años, los programas de *software* se elaboraban pensando en dar soluciones operativas lo más sencillas posibles, sin profundizar mucho en sus posibles vulnerabilidades.

Por último, hay una última categoría a tener en cuenta: los *insiders*, esto es, personas dentro de la organización o institución, sean trabajadores o proveedores, que, por negligencia, porque les han robado o suplantado la identidad o por motivaciones de venganza o hacer daño, se convierten en un elemento interno de robo de datos o información o de entrada de intrusiones. Según el *think tank* Ponemon Institute, en su Informe publicado en enero, *2020 Cost of Insider Threats: Global*, la frecuencia de estos ataques internos ha aumentado un 47 % en los últimos dos años[2].

2.2. La evolución de la seguridad informática

Pero no siempre ha sido así. Desde su origen, la evolución de la seguridad de los programas de *software* ha seguido distintas etapas:

- Una primera, de *respuesta a un reto tecnológico*. El primer programa creado para ser introducido en un ordenador con la finalidad de modificar sus instrucciones o funciones desde dentro fue el *creaper* (enredadera que aparecía en pantalla con el mensaje «soy una enredadera; si puedes controlarme, hazlo») y el consiguiente antivirus *reaper* (podadora). Fue diseñado en un laboratorio en 1972. No obstante, el primero que fue calificado como tal, dando origen al nombre de virus, apareció diez años más tarde, por iniciativa de un adolescente ▷

[2] Ver *www.ponemon.org*. Un resumen puede encontrarse también en *www.pandasecurity.com*

norteamericano que consiguió elaborar un programa que le permitía vencer a los juegos de su consola.

– Una segunda etapa, de *respuesta a retos personales.* En los años noventa, cuando el uso de los ordenadores e internet se hizo masivo, empezaron a surgir los primeros *hackers*, pero siempre con la característica de que lo hacían como resultado de un reto personal y tecnológico. Se trataba, en general, de jóvenes con un alto conocimiento práctico de la informática que buscaban desafíos personales, introduciéndose en computadoras y sistemas complejos e importantes sin su conocimiento. El primer virus que tuvo una gran expansión internacional, «Brain», fue creado por dos hermanos en Pakistán con el fin de contaminar copias ilegales de *software*. Sus datos, el nombre, el teléfono y la dirección aparecían en el programa ofreciendo una solución para su eliminación. Era un virus que se replicaba pero que no pretendía modificar archivos.
– Una tercera etapa, con el objetivo de *hacer negocios ilícitos y ganar dinero*, en la que nos encontramos. En los primeros años de la década de 2000, los delincuentes comenzaron a encontrar un filón de hacer dinero en el robo de datos, la suplantación de identidades o el robo de información. Empezaron a surgir nuevas formas más sofisticadas de virus como los gusanos, los troyanos, los *spyware*, el *ransonware*, etcétera. Desde entonces la evolución fue creciente e imparable, siendo los incidentes y los «ataques» cada vez más sofisticados y eficaces. Dada la sofisticación, dejó de hablarse de virus, como categoría, para hablarse de códigos maliciosos o *malware*.

Hoy día la ciberdelincuencia es, fundamentalmente, una actividad organizada muy lucrativa, existiendo un altísimo número de códigos maliciosos que constituyen una importante amenaza a las comunicaciones, a las operaciones comerciales, al archivo de datos e información y al propio funcionamiento de los sistemas.

Pero al mismo tiempo, en el lado de los usuarios, se ha producido un cambio fundamental: el cambio del perímetro de seguridad. En el ámbito físico, la seguridad se centraba en proteger los accesos dentro de un perímetro físico (puertas, ventanas, vallas…); en el mundo virtual ya no hay un perímetro limitado. Todos nos trasladamos y viajamos con algún dispositivo con acceso al correo e información personal y al de la empresa o institución en la que trabajamos.

2.3. Tendencias actuales. Los principales riesgos

En este contexto es importante conocer cuáles son, actualmente, las principales amenazas y sus tendencias. Los informes elaborados por expertos de diferentes empresas e instituciones coinciden, en general, en destacar entre los ciberdelitos más comunes los siguientes:

– *Ransomware*
  Se trata de una forma de secuestro. Se bloquea o cifra el contenido de un ordenador o dispositivo, exigiendo el pago de una recompensa para volver a ser disponible. ▷

Aunque empezó afectando a grandes empresas e instituciones, como son los casos conocidos de UBER en 2016, o los ataques WannaCry y NotPetya en mayo de 2018, actualmente lo están sufriendo pymes, instituciones públicas y privadas, y particulares.

– *Ataques a dispositivos IoT*
Es una intrusión en un dispositivo que está conectado a internet para robar datos u otra información, pudiendo incluso utilizarse también con fines de chantaje. Así, en electrodomésticos, vehículos…, habiendo casos reportados[3] en equipos médicos y en flotas de transporte de camiones o autobuses, o el caso conocido de la identificación de ubicaciones secretas del ejército de EE UU por los datos de recorrido de las pulseras de fitness de algunos soldados que, imprudentemente, las tenían conectadas.

– *Phishing e ingeniería social*
Son técnicas para suplantar la identidad de una web, y actuar a través de ella, o acceder a claves de acceso en sistemas a través de comunicaciones falsas para engañar a la víctima. A veces los delincuentes se hacen pasar por policías u otra autoridad administrativa. Hace unos años llegó a haber muchos casos con falsas webs bancarias para hacer transacciones, llegando a ser España uno de los países de la UE con más porcentaje de suplantación o robos de identidad registrados, un 7 % de los cibernautas. Actualmente se utiliza menos, salvo en pymes, ya que, de hecho, en el mercado negro es posible poder comprar registros ya robados, pero como se recoge en la nota a pie de página número 10, está de nuevo creciendo en esta crisis.

– *Fraude del CEO o whaling attack* (caza de la ballena)
Partiendo de suplantar la identidad del CEO de una empresa, utilizando como refuerzo de credibilidad informaciones sobre sus rutinas que previamente han sido ilegalmente conocidas accediendo a sus redes sociales y correos, se cursan instrucciones a un empleado con responsabilidades para que pague una cantidad o transfiera una información sensible. En los tres últimos años se han producido fraudes en cien países, creciendo su número, y solo se recuperó un 4 % del dinero estafado.

– *Ataque de denegación de servicio (DOS)*
Se impide la prestación de un servicio, en la mayoría de los casos, por bloqueo de la web. Se utiliza también a veces para pedir un rescate. Para ejecutarlo, se hacen previamente con el control de una red de ordenadores en los cuales han introducido «troyanos» sin conocimiento del propietario. Estos virus esperan una orden para actuar y, cuando se produce, intentan acceder simultáneamente todos a la dirección de destino objetivo, bloqueándola. La red se llama Botnet o red zombie, y se estima que hay millones de ordenadores infectados en el mundo. De hecho, en el mercado negro se alquilan redes de este tipo. ▷

[3] Un problema para conocer la importancia y magnitud real de los casos de ataque es la no publicidad de la información. El que sufre un ataque, por cuestión de imagen y no quebrar la confianza de sus clientes y socios, no lo cuenta salvo a los profesionales que trabajan para corregir y solucionar el problema. Salvo que por imperativo legal tenga que hacerlo y haya filtraciones.

A ellos habría que añadir los robos directos de información y la simple suplantación de identidades. También podríamos mencionar las ATP o amenazas persistentes avanzadas, que es un tipo de amenazas dirigidas a las grandes empresas u organizaciones que incluye la intrusión y la expansión para lograr un objetivo concreto. Un ejemplo fue el ataque Carbabank para robar cantidades de billetes que salían de cajeros automáticos concretos respondiendo a una orden dada por los ciberdelincuentes.

En definitiva, la sofisticación ha ido aumentando, si bien, afortunadamente, las empresas que trabajan en ofrecer soluciones han ido también desarrollando técnicas innovadoras para combatir las intrusiones y los ataques. De los simples antivirus y *firewall* de protección se ha pasado ya a herramientas basadas en inteligencia artificial, con técnicas como Machine Learning y Deep Learning, entre otras, y a sistemas de autentificación basados en biometría u otras técnicas.

3. ¿Cómo debemos protegernos?

Decíamos que la ciberseguridad trata de minimizar los riesgos. Pero cada empresa o institución tiene sus características y, por tanto, sus vulnerabilidades, en función de la actividad que desarrolla y su tamaño. Por tanto, lo primero que debe hacerse es definir el mapa de riesgos, esto es, identificar las amenazas potenciales concretas con criterios objetivos, su probabilidad, su posible impacto negativo en función del grado de vulnerabilidad que tenga (existencia o no de sistemas de protección, controles, etc.), y a partir de ahí hacer el listado de riesgos ordenándolos según su importancia para la actividad.

Hecho esto, para garantizar un nivel alto de ciberseguridad es necesario actuar en los tres frentes o fases del ciclo que se recogen en la Figura1.

Para hacer frente a la fase de prevención, hay que actuar instalando o estableciendo:

- Aplicaciones y procedimientos *anti-malware*.
- Sistemas y procedimientos antifraude.
- Procedimientos para evitar fuga de información.
- Protección de las comunicaciones.
- Seguridad en dispositivos.

Para hacer frente a la fase de control, hay que implementar y llevar a cabo:

- Auditorías técnicas.
- Soluciones de certificación.
- *Compliance* o cumplimiento legal.
- Controles de acceso y trazabilidad. ▷

FIGURA 1
CICLO OPERATIVO DE LA CIBERSEGURIDAD

Fuente: elaboración propia a partir del esquema muy utilizado en el sector.

Para mitigar los daños tras una incidencia y recuperar la actividad, disponer de:

– Un plan de contingencia.
– Un plan de continuidad en la actividad.

4. El marco institucional de la ciberseguridad

4.1. La obligación legal de mantener un nivel de ciberseguridad

Las primeras empresas e instituciones que se vieron obligadas por la legislación a mantener un nivel de ciberseguridad fueron las consideradas como parte de las infraestructuras críticas de un país. Ya en 2002, tras los atentados del 11 de septiembre de 2001, la OCDE estableció unos principios y unos criterios de actuación para proteger las infraestructuras informáticas y de comunicaciones, con el apoyo explícito de todos los Gobiernos, y una cooperación mutua[4]. Dos años después, tras el impacto de los atentados en Madrid, el Consejo Europeo de la UE aprobó el lanzamiento de un Programa Europeo para la Protección de las Infraestructuras Críticas, que podrían ser afectadas por ataques terroristas, iniciativa que culminaría con la aprobación de la Directiva 114/2008 sobre Protección de Infraestructuras Críticas.

Nuevos acontecimientos, como el ciberataque del que fue víctima Estonia en 2007, que afectó a sus ministerios, bancos, periódicos…, paralizando el país, y otros no menos importantes que tuvieron lugar entre 2008 y 2012 (ataque a la planta nuclear en Irán, a Sony, a Saudi Aramco…) impulsaron de nuevo los trabajos y, en 2013, fue aprobada una Estrategia de Ciberseguridad, integrándola como un elemento importante y crítico para la implementación del Mercado Único Digital, lanzado como proyecto en 2015.

Adicionalmente, se extendieron las obligaciones legales a la prestación de servicios digitales. En 2016 se aprobó la Directiva 1148/2016, más conocida como Directiva NIS, por sus siglas inglesas (Network and Information Security), relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información. En ella, se establecen mecanismos de notificación de incidentes (CSIRT o Computer Security Incidence Response Team). Pero el gran cambio cualitativo se produjo con la aprobación del Reglamento 2016/679 de Protección de Datos o GDPR. Dentro de las obligaciones que toda empresa e institución debe cumplir, en relación a la custodia de los datos personales que mantiene, está la de adoptar las medidas técnicas y organizativas adecuadas para proteger los datos.

En consecuencia, todos los Estados miembros de la UE han ido estableciendo normas legales y procedimientos, existiendo hoy un marco legal claramente definido.

Por ello, la ciberseguridad, además de ser fundamental para garantizar la buena marcha de un negocio o el buen funcionamiento de una institución, se ha convertido hoy en una exigencia que hay que cumplir, un elemento más del *compliance*[5]. ▷

[4] *Recommendations of the Council concerning the Guidelines for the Security of Information Systems and Networks: Towards a culture of Security*, aprobadas en la Reunión Ministerial anual de 2002. Ver: *www.oecd.org*

[5] *Compliance* es «el conjunto de procedimientos y buenas prácticas adoptados por las organizaciones para identificar y clasificar los riesgos operativos y legales a los que se enfrentan y establecer mecanismos internos de prevención, gestión, control y reacción frente a los mismos». La definición está tomada de la World Compliance Association. Ver: *www.worldcomplianceassociation.com*

La extensión de la responsabilidad penal a las personas jurídicas en todos los países de la OCDE y muchos otros más, haciendo que los directivos y administradores puedan ser penalmente responsables de los delitos que cometa la empresa, hace que se haya generalizado la implementación de un «programa de *compliance*» o cumplimiento normativo que, entre otras cosas, puede eximir o atenuar esa responsabilidad.

4.2. Las políticas de ciberseguridad en la UE

Además de la legislación y de los programas de apoyo a la I+D, la UE creó también en 2004 ENISA, la Agencia de seguridad de las redes y la información, con el objetivo de apoyar a los Estados miembros y crear una mayor cultura de seguridad en relación con las redes de comunicación. Impulsada por la propia Comisión de la UE, en junio de 2016 se constituyó ECSO (European Cyber Security Organization) como organización sin ánimo de lucro que agrupa al sector privado y a instituciones públicas nacionales y locales para facilitar la implantación de una colaboración público-privada en Europa en este campo.

A ello hay que sumar una cooperación mutua en materia de ciberdefensa y en la propia gestión de las infraestructuras críticas.

4.3. El marco de la ciberseguridad en España

Si dejamos aparte el ámbito de la ciberdefensa y seguridad nacional por no ser objeto de este artículo, así como el de las infraestructuras críticas, que tienen una regulación específica y unos procedimientos de actuación muy definidos ante incidencias de ciberseguridad[6], y nos centramos en el ámbito de las empresas e instituciones, el marco de la ciberseguridad en España se articula con base en varios ejes:

- Las exigencias establecidas en la normativa legal. Esta es la derivada de la normativa europea antes mencionada, y fundamentalmente la Directiva NIS transpuesta por RDL 12/2018, el Reglamento 679/2016 de Protección de Datos y la Ley Orgánica 3/2018 de Protección de datos y garantía de los derechos digitales.
- El apoyo del INCIBE (Instituto de Ciberseguridad), dependiente de la SE de Digitalización e Inteligencia Artificial, que es el organismo especializado de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos[7].

  El INCIBE-CERT es el centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España[8].
- Los productos y servicios que ofrecen las empresas especializadas del sector de ciberseguridad, que en España cuentan con un nivel muy alto. Muchas de ellas, aparte de proveer aplicaciones *antimalware*, hacen test de penetración, auditorías de seguridad, etcétera, o prestan servicios externos con un SOC (Security Operations Center) que gestiona la protección, monitorización y respuesta ante ataques informáticos. ▷

[6] La regulación en materia de infraestructuras críticas es básicamente la Ley 8/2011, por la que se establecen medidas para la protección de infraestructuras críticas; el RD 704/2011, que aprueba el Reglamento de protección de infraestructuras críticas; y la Resolución de 8 de septiembre de 2015 de la SE de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos. A partir de ahí, están los planes desarrollados.

Aunque la información puntual sobre las infraestructuras críticas es secreta, en España existen más de 3.500, incluidas en los siguientes doce sectores recogidos en la ley: Administración pública, Espacio, Industria nuclear, Industria química, Instalaciones de investigación, Agua, Energía, Salud, Tecnologías de la información y las comunicaciones (TIC), Transporte, Alimentación y Sector financiero y tributario.

El CNPIC, Centro Nacional de Protección de las Infraestructuras Críticas, dependiente de la SE de Seguridad, es el órgano responsable de la gestión y coordinación, incluidas las crisis.

[7] Ver: *www.incibe.es*

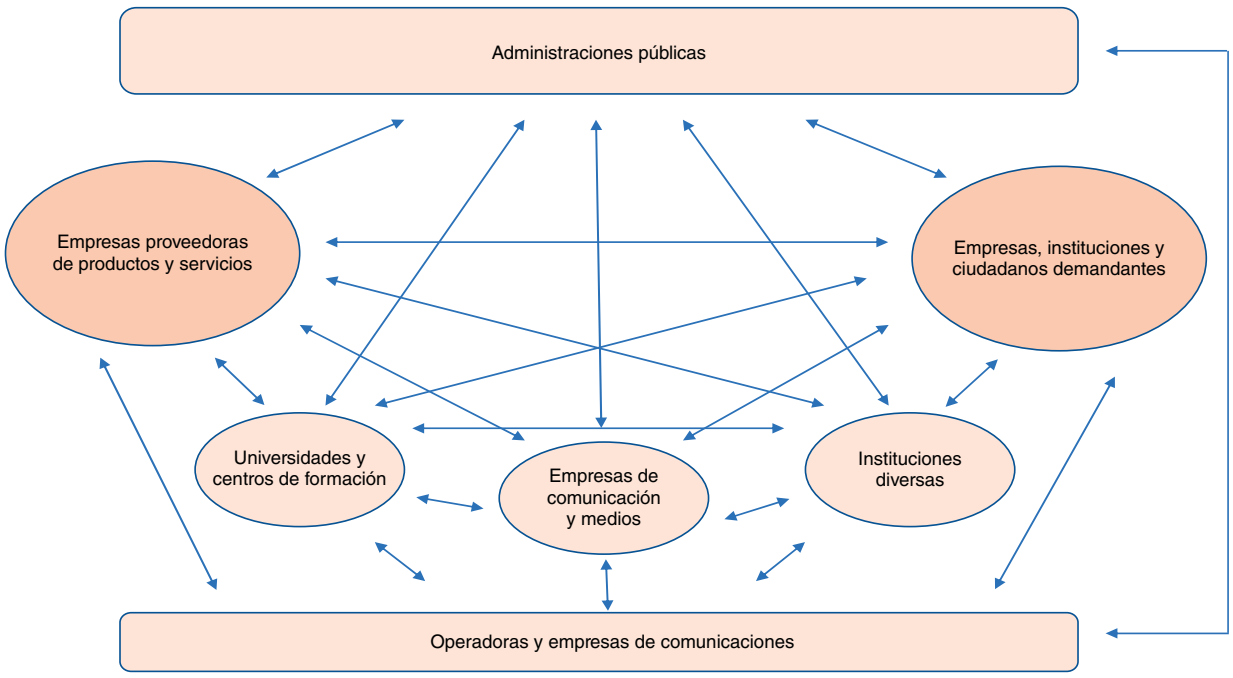
[8] CERT, o Computer Emergency Response Team, es el Equipo de Respuesta para Emergencias inmediatas al que se deben de comunicar las incidencias que se produzcan, dando éste apoyo y respuesta.

– Las operadoras de telecomunicaciones, las empresas proveedoras de servicios *cloud*, empresas proveedoras de servicios web, de pagos *online*, etcétera, que prestan cobertura de ciberseguridad a sus clientes.
– Las instituciones públicas e instituciones privadas que impulsan la ciberseguridad, dando apoyo directo a proyectos o iniciativas empresariales. Dentro de este grupo hay que destacar las iniciativas de potenciar el desarrollo de *clusters* que hay en marcha con el objetivo de reforzar el desarrollo de empresas y atraer talento y formar profesionales, elemento crítico para el sector. Así, la AEI Ciberseguridad, asociación sin fines de lucro nacida con el apoyo del INCIBE para crear un *cluster* nacional; el *cluster* que se está formando en el País Vasco con el apoyo del Gobierno autónomo; o la iniciativa en marcha de consolidar un *cluster* en la región de Madrid, surgida a iniciativa del ayuntamiento, que cuenta con el apoyo de la Comunidad de Madrid, en colaboración con el propio INCIBE y la AEI de Ciberseguridad.
– Por último, los centros de formación, tanto universidades como escuelas de negocio, u otros centros dirigidos a colectivos diferentes, que ayudan a desarrollar el sector y la cultura de ciberseguridad.

Estos ejes configuran el ecosistema de ciberseguridad que existe en España y que esquemáticamente queda recogido en la Figura 2.

Se trata de un ecosistema con gran potencial, si bien contrasta con el aún bajo nivel de concienciación que existe en buena parte ▷

FIGURA 2
EL ECOSISTEMA DE LA CIBERSEGURIDAD



Fuente: elaboración propia.

de las pymes, empresarios autónomos y ciudadanos españoles. Lo que, como apuntábamos en la introducción, es un problema en el momento actual.

5. Reflexión final

En plena crisis del COVID-19, en que el teletrabajo, las compras *online* y el intercambio de correos y mensajes se han generalizado con gran rapidez, es muy importante ser conscientes de los riesgos de ciberseguridad a los que vamos a tener que hacer frente en los próximos meses, muy probablemente con gran intensidad en la fase de recuperación de la actividad económica. No es exagerado pensar que, dadas las vulnerabilidades actuales en este ámbito de muchas empresas e instituciones, los ciberdelincuentes van a aprovechar las circunstancias para tomar posiciones haciendo intrusiones y robando información y datos[9].

Esto lleva a una primera reflexión. Es necesario plantearse seriamente, si no lo hemos hecho ya, el tema de la ciberseguridad en nuestra empresa, organización e incluso actividad, y aprender las lecciones del pasado[10].

De ahí que sea necesario, para bien de todos, dedicar un tiempo y un esfuerzo para analizar el mapa de riesgos propio, establecer unos protocolos mínimos adicionales de seguridad, reforzar esta, bien internamente o bien con un apoyo externo, y, sobre todo, incorporar la ciberseguridad como una parte importante de la cultura de la gestión empresarial.

Como veíamos en el apartado 2.1, ya no solo hay que preocuparse de protegerse ante ataques de agentes externos; hoy día los *insiders,* de modo voluntario o involuntario, pueden hacer mucho daño. No olvidemos que un porcentaje muy alto de las intrusiones se producen por una mala práctica o un error humano de alguien que trabaja en nuestro sistema. Simplemente reforzando la formación, la cultura y los procedimientos internos ganamos mucha protección. En esta línea, una consulta a la página web del INCIBE puede ser de gran utilidad.

Bibliografía

OECD (2002). *Recommendations of the Council concerning the Guidelines for the Security of Information Systems and Networks: Towards a culture of Security*. www.oecd.org

Páginas web

www.incibe.es
www.ponemon.org
www.pandasecurity.com
www.worldcomplianceassociation.com

[9] Un ejemplo ilustrativo puede leerse en el artículo aparecido en el diario digital *El País* el 23 de marzo pasado de los periodistas O. López Fonseca y J. Pérez Colomé, «Interior alerta de una quincena de ciberestafas que utilizan como señuelo el coronavirus. Los expertos policiales destacan la peligrosidad de una web que ofrece falsos diagnósticos de la enfermedad». Señala que, según el Ministerio del Interior, se ha incrementado en un mes un 70 % el *phishing*, está circulando el *randsonwere* Covidlock y hay aplicaciones falsas con el nombre de la OMS para que el lector descargue, accediendo entonces el *malware.*

[10] Ver en este sentido la reflexión tras el caso WannaCry, en Fernando Davara, «WannaCry: ¿Nos asustamos y lloramos? Mejor nos concienciamos». Blog «Reflexiones sobre la Sociedad Digital» publicado el 3 de mayo de 2017. Recuperado en *www.fernandodavara.com*