# *Euskadi 2025 - Sin ciberseguridad no hay futuro*

## *Basque Country 2025. Without cybersecurity, there is not future*

**La profunda digitalización que se está produciendo en la economía y en la sociedad ha hecho que sea actualmente una de las palancas de crecimiento y competitividad. Para ello se necesita mantener una seguridad de los datos y en las comunicaciones. El objetivo del artículo es describir la ciberseguridad como elemento estratégico de competitividad, señalar la importancia de la seguridad digital en la economía y en la sociedad del siglo XXI, esencialmente en la fase de prevención, analizar su evolución y desarrollo a nivel mundial y en particular en Euskadi. Asimismo, detallar las tendencias y amenazas, y la necesaria y prioritaria labor de las Administraciones públicas para crear y fomentar un entorno de ciberseguridad global, en un escenario digital de confianza. Por último, el trabajo se centra en la situación de la ciberseguridad en Euskadi, y las estrategias público-privadas que se siguen desde el nivel europeo hasta el desplegado en Euskadi junto a sus perspectivas y retos futuros**

*Ekonomia eta gizartearen digitalizazio sakona hazkunderako eta lehiakortasunerako palanketako bat da gaur egun. Aldaketa horretan, datuen eta komunikazioen segurtasuna bermatzea ezinbestekoa da. Artikuluaren helburua honako hau da: zibersegurtasuna lehiakortasunerako elementu estrategiko gisa deskribatzea; segurtasun digitalak XXI. mendeko ekonomian eta gizartean duen garrantzia azpimarratzea, batez ere prebentzio-fasean; eta mundu-mailako bilakaera eta garapena aztertzea, bereziki EAEkoa. Era berean, hainbat zehaztapen egitea: joerak eta mehatxuak, eta administrazioei dagokien lehentasunezko protagonismoa zibersegurtasun globaleko ingurua sortu eta sustatzerakoan, egoera digital konfiantzazko batean. Azkenik, lanak EAEko segurtasun digitalaren egoera jasotzen du, eta indarrean diren estrategia publiko-pribatuak, Europa-mailatik EAEraino, etorkizuneko ikuspegiekin eta erronkekin batera.*

The current far-reaching digitisation of the economy and of society has become a major force for growth and competitiveness. Accordingly, there is a need to keep data and communications secure. The article describes cybersecurity as a strategic element for competitiveness, highlights the importance of digital security to the economy and to society in the 21st century, especially at the prevention stage, and analyses its evolution and development globally and with particular reference to the Basque Country. It also details trends and threats and the important, necessary efforts made by public administrations to create and foster a secure cyber environment globally, in a context of trust in things digital. The article thus focuses on the cybersecurity situation in the Basque Country and on the public and private sector strategies employed, ranging from the EU level to the Basque Country itself. It also outlines prospects and challenges for the future.

**Xabier Mitxelena**
*Accenture Limited*



## *Índice*



**Palabras clave:** ciberseguridad, *hacker,* ciberataque, cibercrimen, transformación digital, Euskadi, programas malignos.

**Keywords**: cybersecurity, hacker, cyber attack, cyber crime, digital transformation, Basque Country, malware.

**Nº de clasificación JEL:** D83, H56, O31

Fecha de entrada: 04/10/2020 Fecha de aceptación: 03/11/2020

## 1. INTRODUCCIÓN

«*Nadie me hubiera dicho en mayo de 1999 que aquella idea del bueno –y visionario– de Mikel Fernández (socio fundador de S21sec) se había adelantado varios años a un escenario que hoy ya forma parte de nuestras vidas. Cuando Mikel, junto a su 'junior' favorito, Igor Unanue, hoy convertido en excelente profesional y emprendedor, me contaron la idea de crear una empresa de ciberseguridad con un grupo de jóvenes expertos en hacking, pensé que me enfrentaba a un guion de ciencia-ficción*». Durante estos años he revisado películas que nos «advertían» de los riesgos derivados de los grandes cambios digitales y la comunicación masiva entre personas y dispositivos. Desde *Juegos de Guerra* (1983), *La Red* (1995), *Firewall* (2006), *La Jungla de Cristal 4* (2007), y otras muchas que han nacido en plenas pandemias digitales, como *Fast&Furious 8* (2019), donde se manipula remotamente un coche, no han hecho más que confirmar que, cuando pusimos en marcha la empresa S21sec en enero del año 2000 estábamos en el camino adecuado de un futuro próximo, cuya realidad nos ha superado. Hoy, en el año 2020, en plena crisis sanitaria y económica derivada de la aparición y propagación del COVID-19, según diferentes fuentes, el mundo requiere entre 2,5 y 3,5 millones de nue-

vos profesionales en el ámbito de la ciberseguridad. Una brecha a nivel global que, si trabajamos en la línea adecuada, nos ofrece una gran oportunidad.

La ciberseguridad es, en la actualidad, uno de los sectores donde mayor proyección profesional se puede encontrar y una práctica que evoluciona de forma constante. El cibercrimen innova todos los días y para construir una sociedad digital de confianza hay que anticiparse a sus objetivos y a sus formas de pensar y actuar. Sin duda, la evolución sufrida desde finales del siglo XX, donde la penetración de Internet en los ámbitos personal y profesional se ha incrementado exponencialmente, ha generado una mayor consciencia sobre los continuos riesgos existentes en redes cada vez más interconectadas.

Como ejemplo, y sin entrar en los grandes incidentes de todo tipo que han sido actualidad en entornos más reducidos, diariamente la sociedad se enfrenta a noticias que cada vez generan mayor preocupación[1]. A ello se añaden los incidentes que, entre otros, vienen sufriendo las compañías aseguradoras y energéticas de primera línea y cuyo impacto es difícil de valorar. A nivel global, se ha dado un incremento del 60% en el pago medio por *ransomware* en el primer cuatrimestre de este año 2020 (US$ 178.250), especialmente en compañías del entorno pyme.

Si bien la seguridad estaba en el origen de las comunicaciones militares en la era previa a Internet –red Arpanet–, la (in)seguridad de las conexiones compartidas ha sido y está siendo uno de los elementos claves a los que nos venimos enfrentando en este cambio de paradigma.

Nos enfrentamos a una de las claves del futuro de la competitividad: la seguridad de los datos, la seguridad de las comunicaciones. Transportar los nuevos productos y servicios, en este caso a través de las redes y las telecomunicaciones, es de vital importancia, y debe aportar garantías de seguridad y privacidad para poder mantener los negocios de cara a competir en este mercado global que es el ciberespacio.

A medida que el índice de penetración de Internet en empresas y hogares ha ido creciendo, los riesgos asociados a la colaboración y la confianza por defecto han subido como la espuma. Desde los primeros hackers que intentaban demostrar esos riesgos que estábamos generando al «abrir» las puertas de nuestras casas, de nuestra

---

[1] 14 de mayo de 2020: «El 51% de las empresas han sido atacadas por *ransomware* durante el último año» (Fuente: IT Reseller) https://www.itreseller.es/seguridad/2020/05/el-51-de-las-empresas-han-sido-atacadas-por-ransomware-en-el-ultimo-ano

16 de septiembre de 2020: «Detectan una estafa a través de Bizum, haciéndose pasar por la Seguridad Social» (Fuente: EITB) https://www.eitb.eus/es/noticias/sociedad/detalle/7492120/detectan-estafa-traves-bizum-haciendose-pasar-seguridad-social/

16 de septiembre de 2020: «Ciberataque contra GAM, firma asturiana especializada en industria 4.0 y maquinaria» (Fuente: Business Insider)

https://www-businessinsider-.es.cdn.ampproject.org/c/s/www.businessinsider.es/reivindican-ciberataque-gam-firma-asturiana-industria-40-717705?amp)

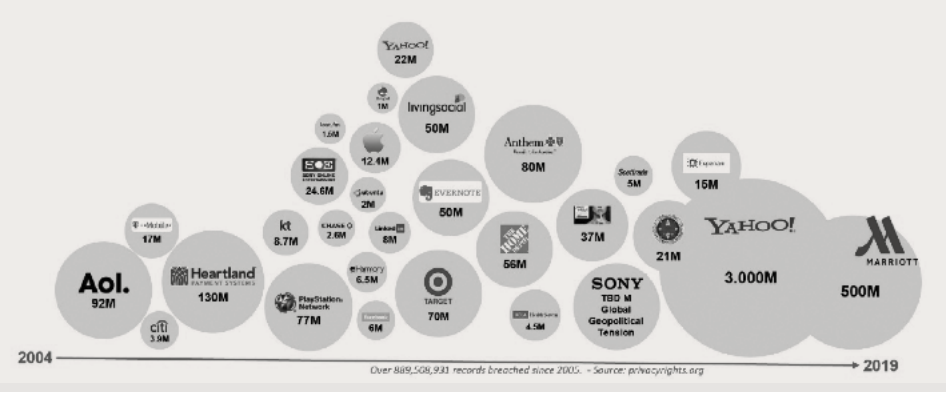
17 de septiembre de 2020: «Muere un paciente de un hospital en Alemania debido a un ataque de hackers que bloqueó los servidores» (Fuente: RT)

https://actualidad.rt.com/actualidad/366851-paciente-muere-hospital-alemania-ataque-hackers

información, a terceros de confianza, la ciberdelincuencia ha evolucionado de forma exponencial a una industria donde el cibercrimen y los ciberdelincuentes (los crackers) son capaces de transformar sus negocios a entornos de máximo lucro. Se ha pasado del factor humano en el ámbito más físico –crimen, espionaje, fraude…– al entorno cibernético –cibercrimen, ciberespionaje, ciberfraude…–. Y siempre amparándose en los elementos que hacen del ser humano un ser vulnerable: sus emociones. La capacidad de engañar(nos) al ser humano sigue siendo la misma que hace cientos, miles de años. La diferencia está en los medios que se utilizan. Hoy la tecnología aporta elementos únicos capaces de anular la capacidad de reflexión humana, dando lugar a errores similares a los que cometieron nuestros antepasados.

Pero no hay que olvidar que, además, hay un cambio de paradigma que afecta a la sostenibilidad como sociedad y que debe ser objeto prioritario de los retos más inmediatos: el trabajo. Estamos en una nueva era donde la robotización, la automatización y los nuevos perfiles profesionales suponen un reto colectivo que sin duda dará lugar a un nuevo «status» y modelo económico. «Gracias» a esta REVOLUCIÓN, en mayúsculas, millones de empleos tradicionales van a seguir desapareciendo y habrá que evitar que haya una parte de la sociedad que sea excluida de este nuevo escenario. La educación va a ser un eje prioritario en esta estrategia, eso sí, empezando por la propia transformación de los modelos educativos.

*Gráfico nº 1.* **NOTIFICACIONES DE BRECHAS DE SEGURIDAD**
(millones de datos expuestos-grandes empresas. 2004-2019)




*Fuente:* privacyrights.org

Finalmente, hay que destacar la importancia que la información tiene para el devenir del futuro más próximo. La propia evolución de los incidentes, de las brechas de seguridad y de la fuga y robo de datos, ha acelerado la puesta en marcha de un entorno legal que proteja la privacidad y los derechos que nos deben asistir en este nuevo mundo digital, hasta el punto de que los líderes de empresas y organizaciones que gestionan datos sensibles tienen hoy responsabilidad penal en caso de brechas de seguridad. En el

gráfico nº 1 se puede constatar esta realidad con un simple repaso a la historia más reciente de ataques y fugas de datos que han afectado a grandes actores de la economía.

Desde la implantación de la directiva europea de protección de datos (General Data Protection Regulation-GDPR) en mayo de 2018, la aplicación de sanciones de hasta 250 MM de euros a diferentes entidades por no haber implantado los modelos de seguridad digital adecuados y haber expuesto datos de terceros, han comenzado a ser comunes.



Sin embargo, no hay que olvidar la situación de las pymes, cuyo peso específico en la economía es fundamental, y que operan en las mismas redes sufriendo de forma silenciosa esta misma «pandemia digital». Por ello la estadística que más preocupa es que el 70% de las empresas afectadas por un ciberataque son pymes, que el coste medio de los mismos oscila, según fuentes, entre 50.000 y 90.000 euros de media, y que nadie se atreve a aventurar cuántas han tenido que cerrar sus negocios por esta causa. España y Euskadi son territorios Pyme, por lo que se necesita que la transformación digital llegue a todas ellas para ser competitivos. Sin duda, la ciberseguridad es y será imprescindible para garantizar su sostenibilidad.

El objetivo del artículo es definir la ciberseguridad como elemento estratégico de competitividad, señalar la importancia de la seguridad digital en la economía y en la sociedad del siglo XXI, esencialmente en la fase de prevención, analizar su evolución y desarrollo a nivel mundial y a nivel más local, en particular en Euskadi. Asimismo, detallar las tendencias y amenazas, y la necesaria y prioritaria labor de las Administraciones públicas para crear y fomentar un entorno de ciberseguridad global, en un escenario digital de confianza. Por último, el trabajo se centra en la situación de la ciberseguridad en Euskadi, y las estrategias que se siguen desde el nivel europeo hasta el desplegado en nuestra región junto a sus perspectivas y retos futuros. Convertir los nuevos riesgos en grandes oportunidades desde la colaboración público-privada es el camino.

Tras esta introducción, la estructura del artículo tiene la siguiente secuencia: se describe los antecedentes de las redes e Internet y el impacto de la ciberseguridad en su crecimiento y consolidación, y continúa señalando los riesgos actuales y futuros donde la ciber(in)seguridad puede impactar negativamente en el devenir de la nueva economía y sociedad digitales. Después se hace una inmersión en el ecosistema de ciberseguridad de Euskadi, junto a un viaje posterior a través de la estrategia de Europa y su modelo de relación y gobernanza con los países miembros, con foco en una estrategia público-privada que ofrezca seguridad en las redes a empresas y ciudadanos europeos, pasando por el Gobierno central y Autonomías, y con foco final en la Estrategia de Ciberseguridad Euskadi 2025. Las conclusiones finales resumen el necesario compromiso de toda la sociedad para, desde una verdadera cultura de seguridad, dotar a Euskadi de las mejores capacidades para competir en este nuevo escenario digital.

## 2. ANTECEDENTES DE LA CIBERSEGURIDAD

Si bien los orígenes de la protección de la información datan de 1965, a los que siguen los primeros desarrollos legislativos en 1970-1977 y 1977-1981, la madurez se inicia con la Ley Orgánica 5/1992 de 29 de octubre, de regulación del tratamiento

automatizado de los datos de carácter personal, la LORTAD. Posteriormente, la Ley Orgánica de Protección de Datos 15/1999, la LOPD, y el Reglamente de Seguridad RD994/199, supusieron la uniformización del modelo, convirtiéndose posteriormente en un derecho fundamental.

Estos aspectos, junto a la necesidad de verificar y dar carácter legal a los trámites administrativos, dieron lugar al desarrollo de procedimientos y herramientas de soporte que tuvieran validez oficial. El reto era trabajar con entidades y personas de confianza, actuar con aplicaciones y portales de Internet seguros, desarrollar modelos de evidencias digitales…. Todo, dentro de marcos legales y jurídicos necesitados de una transformación absoluta.

Entidades como la Fábrica Nacional de Moneda y Timbre (FNMT) pusieron en marcha la emisión de certificados digitales que permitieran garantizar transacciones, la interoperabilidad con las empresas y administraciones, a la vez que aportaran una identidad digital reconocida. Por su parte las Cámaras de Comercio crearon Camerfirma con el mismo objetivo. Operaciones como el pago de impuestos, la solicitud de un expediente, la firma y aceptación de liquidaciones, daban lugar a múltiples aplicaciones donde los certificados daban soporte a la persona/entidad con sus datos y responsabilidades (poderes) acreditados de cara a refrendar las transacciones.

Muchos de los incidentes de ciberseguridad se deben a suplantación de identidades, a robo de credenciales por diferentes caminos que posteriormente permiten el acceso a información privada. Los certificados, con sus entidades de autorización al frente, son una ayuda para tratar de evitar este tipo de situaciones. El problema ha sido la velocidad de adopción, la incompatibilidad de sistemas y software en el tiempo, y la necesidad de que sea universal y sencillo de adoptar. Y, sobre todo, la necesidad de alfabetizar digitalmente a la sociedad y mejorar los conocimientos al nivel adecuado para evitar brechas sociales.[2]

### 2.1. **Antecedentes de la ciberseguridad en Euskadi**

Las primeras empresas de Internet vieron la luz en Euskadi en torno a 1994-1996 (Facilnet, ATE Internet, Hispavista…, y muchas otras) y ayudaron a dar los primeros pasos a empresas y organizaciones en este nuevo medio, pero también es cierto que la (in)seguridad pronto empezó a ser una fuente de problemas con necesidad de búsqueda de soluciones. En este sentido, con anterioridad se pueden encontrar empresas vascas, como Panda Security, que desde sus inicios en 1990 desarrollaron soluciones que ayudaran a evitar problemas de seguridad –inicialmente virus– en los entornos de los nuevos puestos de trabajo –cuyo carácter gráfico y

[2] ¿De qué nos vale comprar un coche si nunca nos hemos puesto delante de un volante ni conocemos las reglas de circulación? El coche autónomo es un reto en la actualidad y viene a suplir diferentes problemas derivados de los riesgos que asumimos día a día en las carreteras. Tal vez los sistemas biométricos, la voz, los sistemas inteligentes, nos puedan simplificar la dificultad de seguir y asimilar los cambios a la velocidad necesaria.

abierto dieron lugar a los primeros problemas de esta índole–. Eso supone que, antes de desarrollar Internet de forma comunitaria y global, ya se empezaron a desarrollar redes de ordenadores empresariales que trabajaban en modelos de colaboración. En su concepto de globalidad, Internet abría una puerta a la globalización digital activa, a la RED GLOBAL.

En esa época, la Administración vasca ya era consciente de la necesidad de aplicar la tecnología para mejorar sus servicios a ciudadanos y empresas y fue pionera en su puesta en marcha buscando la compatibilidad con estamentos nacionales e internacionales[3]. Los procesos de informatización de los años 80 y 90 se convirtieron en planes de desarrollo de la Administración Electrónica. La Administración vasca ha fomentado e impulsado procesos de transformación de sus servicios públicos, aplicando las nuevas tecnologías como modelo de democratización de los mismos. En 25 años, se han desarrollado diferentes planes estratégicos y, si bien la satisfacción no es plena en todos los ámbitos, no hay duda de que ser innovadores genera resultados y modelos que posteriormente se han tomado como referentes.

Desafortunadamente, la vida de las tecnologías y su diferenciación son efímeras, y esto obliga a las organizaciones a establecer planes plurianuales que den lugar a servicios y productos concretos que lleguen de forma sencilla y eficiente a sus clientes. He aquí uno de los grandes dilemas a los que las administraciones se han ido enfrentando. No es sencillo sincronizar los cambios tecnológicos con las capacidades del ecosistema para beneficiarse de aquellos. Además, formar a los usuarios de la propia Administración y a los ciudadanos y empresas en el uso correcto de las nuevas plataformas no es cuestión de magia, sino de planes concretos e intensos de cuyas métricas y resultados se puedan ir sacando conclusiones.

## 3. RIESGOS GLOBALES, IMPACTOS ECONÓMICOS Y AMENAZAS MUNDIALES

En este apartado es de destacar la profunda reflexión que se viene haciendo durante los últimos años en el World Economic Forum (WEF), donde a los aspectos fundamentales como la estrategia para luchar contra la crisis climática se han sumado los riesgos de ciber(in)seguridad como uno de los mayores peligros para la humanidad.

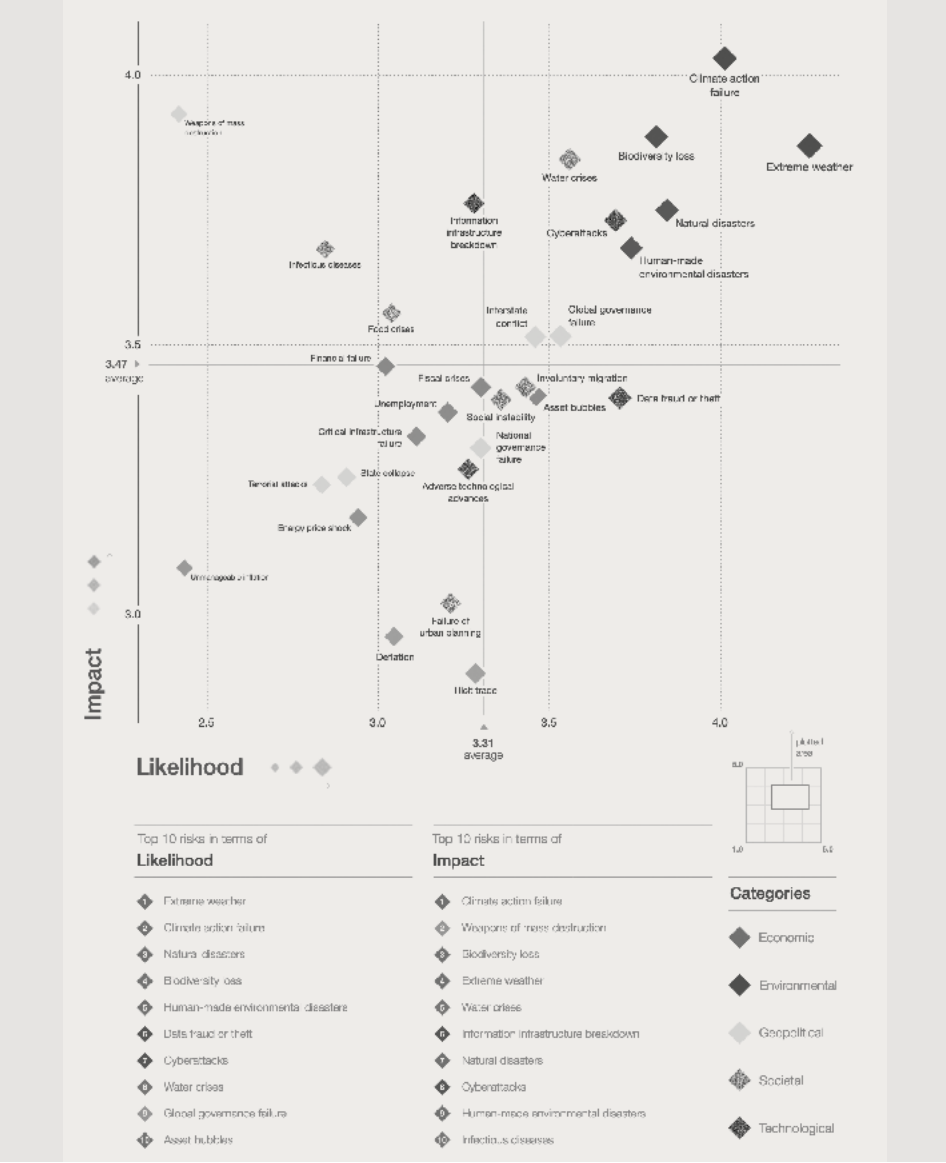
### 3.1. Riesgos e impactos económicos de la ciberseguridad

Durante el WEF de 2019, uno de los debates más relevantes vino a refrendar que la transformación digital de la economía y de la sociedad era un camino sin retorno en el que los riesgos son cada vez más un compañero de viaje que tenemos que considerar. Por primera vez los ciberataques aparecían entre los TOP 5 de riesgos globa-

[3] En Euskadi surgió IZENPE, en 2002, como entidad certificadora para dar soporte al ciudadano y a las empresas en sus relaciones directas con la Administración.

les más probables (ver gráfico nº 3) cuyo impacto, en caso de un ataque globalizado, generaría una gran catástrofe[4].

*Gráfico nº 2.* **PROBABILIDAD E IMPACTOS DE RIESGOS GLOBALES 2019**




*Fuente:* WORLD ECONOMIC FORUM.

[4] Afirmaciones como «Un ciberataque serio podría costar más de 120 billones de dólares, similar a catástrofes naturales como el huracán Katrina» (Fuente: LLoyds), sirven para reforzar estudios como el de Cybersecurity Ventures, que en 2017 auguraba que el coste de los ciberataques supondrá un coste total de 6 trillones de dólares en el año 2021, un 6% del PIB mundial.

Claramente, después de *Wannacry*[5], la sensibilidad de todos los actores económicos y políticos respecto a la importancia de tener una ciberseguridad adecuada en todas las infraestructuras esenciales que dan soporte a la actividad económico-social, ha crecido de forma relevante. En este sentido, es muy interesante el estudio que se presentó en dicho congreso sobre la confianza digital. Con la participación de más de 2700 directivos de las empresas más grandes del mundo, pertenecientes a 11 países y 16 sectores, los resultados no dejan la menor duda sobre el impacto que los ciberataques pueden tener en el futuro de la economía.

*Gráfico nº 3.* **IMPACTO ECONÓMICO DE LOS CIBERATAQUES 2019-2023**

(Valor en riesgo: periodo 2019-2023, por sectores y por países)


*Fuente:* Accenture Research.

A este impacto económico, 5,2 trillones de dólares, se podrían sumar otros impactos potenciales, como los impactos dirigidos a infraestructuras críticas que dan soporte a servicios esenciales, que pueden causar víctimas humanas de forma directa o indirecta[6].

[5] También conocido como WanaCrypt0r 2.0,1 es un programa dañino de tipo *ransomware*. El 12 de mayo de 2017 se registró un ataque a escala mundial que afectó a numerosas empresas, así como al servicio de salud británico. La prensa digital informó aquel día que al menos 141.000 ordenadores habían sido atacados en todo el mundo.

[6] Si la telemedicina es parte de la transformación digital del sector salud, los riesgos asociados al nuevo modelo deben ser parte de su diseño. Basta con echar una mirada al efecto del *ransomware* en los centros clínicos y sus resultados potencialmente catastróficos en situaciones como las que hoy vivimos debido al COVID-19. Y qué decir de la Administración pública, que tiene en los datos su mejor activo para dar soporte a la ciudadanía y gestionar la «empresa» más grande de cada país.

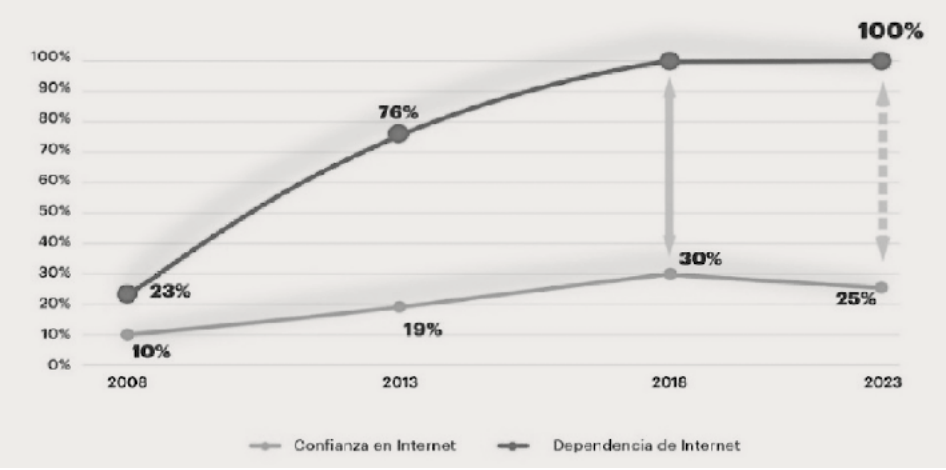
Pero no se queda aquí esta importante reflexión derivada de la encuesta anterior[7]. La más profunda y relevante es la «falta de confianza» de los máximos responsables de las empresas en el mundo digital:

- En 2018 el 100% de los encuestados señalan que sus organizaciones dependen de internet, y de ellos el 75% afirman que dicha dependencia continúa creciendo y que, como resultado, la exposición a riesgos de ciberseguridad aumenta de forma notable.
- Para el 56%, la inestabilidad de Internet es cada vez mayor por problemas de ciberseguridad y no saben cómo reaccionar.
- El 52% reconoce que su futuro crecimiento se puede ver frenado por no poder crecer de forma segura en la economía digital.

Si bien el 100% tiene en Internet su canal de crecimiento, la confianza digital es inferior al 30%, y con tendencia descendente. Y es aquí donde sentencian sobre cómo construir el futuro:

- El 90% reconoce que una Internet digital de confianza es imprescindible para su modelo de crecimiento.
- Para el 69%, sin una mejora dramática de la seguridad en Internet, el avance de la economía digital se verá frenado severamente.

*Gráfico nº 4.* **GRADO DE CONFIANZA Y DEPENDENCIA DE INTERNET**
(encuesta a CEOs) (2008-2019)



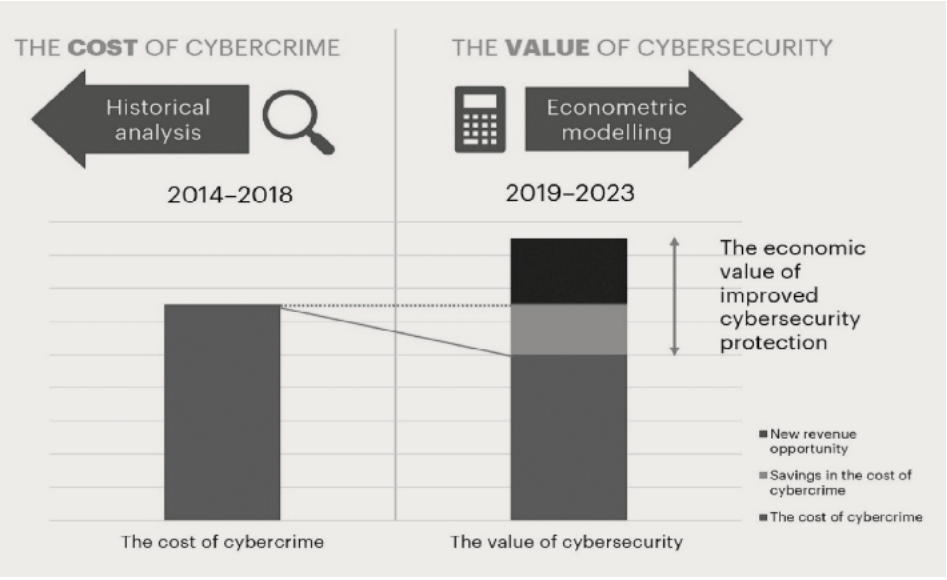

*Fuente:* Accenture Research.

[7] https://www.accenture.com/_acnmedia/thought-leadership-assets/pdf/accenture-securing-the-digital-economy-reinventing-the-internet-for-trust.pdf

Es importante resaltar que, después de muchos años, una de las conclusiones más esperadas es la opinión generalizada de que la ciberseguridad es una inversión y no un coste (ver comparación del coste al que asciende el cibercrimen con el valor que nos da la ciberseguridad en el gráfico nº 4). Al igual que la calidad ha sido un valor distintivo y diferencial a la hora de competir en los mercados, las inversiones en ciberseguridad harán a las empresas más competitivas.



*Gráfico nº 5.* **EL COSTE DEL CIBERCRIMEN Y EL VALOR DE LA CIBERSEGURIDAD (2014-2023)**




*Fuente:* Accenture Research.

Probablemente esta visión supone un antes y un después, pero sobre todo viene a dar la razón a todos aquellos profesionales que con decisión y confianza han seguido impulsando en todos los estamentos públicos y privados un modelo de calidad en el que la seguridad sea también una parte del proceso. Nos encaminamos, sin duda, hacia un escenario de seguridad concertada donde la confianza y la responsabilidad van a estar claramente definidas en la cadena de suministro. Partiendo del coste de la ciberdelincuencia y el potencial de los negocios dentro de una economía digital segura, el gráfico nos acerca al verdadero valor de la Ciberseguridad como elemento de competitividad.[8]

[8] https://www.accenture.com/_acnmedia/thought-leadership-assets/pdf/accenture-securing-the-digital-economy-reinventing-the-internet-for-trust.pdf

### 3.2. **Las amenazas**

La evolución del cibercrimen no ha hecho más que «transformar» actividades delictivas y/o de dudosa legalidad, habituales a lo largo de la historia, en una gran industria cuyo crecimiento económico no para de crecer. Sin duda, cuando se afirma que el futuro es el de aquellas empresas o entidades que mejor aplican la innovación, se puede asegurar que la industria del cibercrimen ha asumido de forma íntegra el modelo.

El gran cambio digital viene avalado por los grandes cambios tecnológicos y su aplicación a modelos de futuro. Las nuevas tecnologías, como la Inteligencia Artificial, Cloud, IoT (Internet of Things), Blockchain, Quantum Computing…, abren un océano de posibilidades para transformar y mejorar nuestras economía y modelo social. Sin embargo, llevan aparejados riesgos que si no se consideran desde el inicio pueden resultar fatídicos. Las nuevas redes industriales conectadas ofrecen grandes ventajas a la hora de competir y, a la vez, generan nuevos riesgos que se deben gestionar y mitigar. Si Stuxnet fue un *malware* dirigido a «paralizar» procesos de enriquecimiento de uranio en Irán, cualquier infraestructura crítica podrá (ya lo son) ser «víctima» de este tipo de ataques. Con la conectividad, seguiremos aumentando la superficie potencial de ataque y, por ende, las consecuencias negativas seguirán en crecimiento si no se abordan modelos diferentes a los aplicados hasta la fecha.

Desde hace más de un lustro la evolución de las amenazas se ha caracterizado por la automatización de los ataques. Si se acude a los mapas que representan los ataques en tiempo real a través de la red[9] se visualiza una realidad que según las últimas estadísticas refleja una automatización de más del 80% de los ataques de forma global y aleatoria, frente a un 20% de ataques dirigidos.

Las amenazas que se esperan tanto a nivel global, como en Euskadi, de cara al próximo lustro 2025, van a seguir incidiendo en el eslabón más débil de la cadena, el usuario, y tendrán su mayor exponente en:

- Los ataques de programas maliciosos (*malware*), con el *ransomware* como modelo de negocio más rentable en estos momentos, seguirán siendo parte del ecosistema digital, y la sofisticación del mismo hará cada vez más difícil su detección y eliminación. El *ransomware* es y será la «pandemia digital» por excelencia. Su capacidad de inutilizar sistemas y robar-cifrar información aprovechando vulnerabilidades y exigiendo rescates está poniendo en juicio de valor las capacidades de detección y defensa de las infraestructuras de empresas y organizaciones.

---

[9] El mapa más reconocido en su momento fue el de la empresa NORSE –ver en Youtube https://www.youtube.com/watch?v=bWXIJSiagBY–. Hoy, compañías como Arbor Networks –https://www.digitalattackmap– o como Fire Eye –https://www.fireeye.com/cyber-map/threat-map.htm–, entre otras, ofrecen esta información en tiempo real.

- *Phishing*: la ingeniería social como modelo de engaño seguirá poniendo a prueba la sensibilización y concienciación de la sociedad. Nuestros datos son una fuente de beneficios para los atacantes y su objetivo es y seguirá siendo la suplantación de identidad.
- *Ataques DDOS*: ataques de denegación de servicio. Estarán a la orden del día. Motivaciones comerciales, económicas, políticas, religiosas…, seguirán siendo la base de este perfil de ataques que pueden dejar sin servicio infraestructuras empresariales, críticas y de otra índole. ¿Qué sucedería si un ataque de grandes dimensiones paralizara Internet?
- Desinformación, *Fake News*: cada vez más frecuente (aunque siempre ha acompañado al ser humano). Su impacto puede ser devastador debido a la viralidad de las redes sociales y la falta de capacidad crítica para eliminarlo o reducirlo a causa de la velocidad con la que se transmite. Puede cambiar el rumbo de la humanidad y, sobre todo, nos debe hacer reflexionar sobre los riesgos reales de Internet[10].
- *Aplicación de Tecnologías de Última Generación:* la Inteligencia Artificial, a falta de un código ético, ofrece grandes ventajas a la hora de llegar a los objetivos definidos. Su aplicación por parte de los atacantes es cada vez más común, y será mucho más sofisticada en el futuro. Llegar a los objetivos definidos en base a algoritmos de nuevo cuño estará asociado a la nueva generación de incidentes. Asimismo, la hiperconectividad derivada del desarrollo e implantación de tecnologías 5G e IoT darán lugar a nuevos puntos de intrusión si no se garantiza su seguridad desde el diseño. El robo de más de 10 millones de credenciales a través de un ciberataque al termómetro conectado a Internet de la pecera de un casino de New York es un claro ejemplo de estos nuevos riesgos[11].

Además, en línea con las necesidades globales de futuro, una buena educación digital, la concienciación permanente, trabajar en una identidad digital única que evite la suplantación de identidades y el engaño automático, junto al futuro de la computación cuántica como elemento de seguridad de nueva generación, serán el complemento ideal a los modelos de colaboración en la prevención y respuesta a estos riesgos permanentes.

Llegados a este punto, es fundamental trasladar las mismas preguntas a los líderes políticos y sociales. Los presupuestos públicos son uno de los motores esenciales de la economía a la hora de generar la demanda adecuada y aumentar y fortalecer el bienestar de los ciudadanos.

---

[10] El video «El dilema de las Redes Sociales» de Netflix puede ayudar a entender cómo asistimos al cambio del comportamiento humano anulando sus ideas y valores. Los gobiernos, las multinacionales, el cibercrimen…, todos quieren gobernar Internet.

[11] https://computerhoy.com/noticias/software/roban-datos-casino-traves-del-termometro-del-acuario-79195

Estas conclusiones tuvieron una propuesta de Plan de Acción por parte de dichos responsables (más de 1700 CEOs del G2000 dieron respuesta a esta reflexión) para mejorar la percepción y la «postura» de seguridad en Internet, en la que los líderes mundiales terminaron afirmando que, para poder construir una vida digital de confianza, donde hacer crecer la economía sin frenos no deseados, necesitamos implementar 3 elementos-acciones fundamentales:

- Gobernanza: ninguna empresa puede resolver de forma individual los problemas y riesgos de Internet. Solo con un esfuerzo colectivo se podrá conseguir un escenario de confianza. La colaboración público-privada es un factor prioritario y esencial en este aspecto.
- Arquitecturas de negocio: no es suficiente con securizar las infraestructuras. El ecosistema de los negocios, con la cadena de suministro en el mismo, requiere un modelo de confianza conjunto[12].
- Tecnología: «Security by Design": incluir la ciberseguridad en el diseño y producción de productos y servicios para ganar en competitividad.

## 4. EL ECOSISTEMA DE CIBERSEGURIDAD EN EUSKADI

### 4.1. Iniciativa privada

En el momento del nacimiento de Internet, Euskadi empezaba a tener empresas especializadas en el ámbito de la seguridad en redes y, gracias a ciertos entornos universitarios, junto a personas con inquietudes en la realidad de la ciber(in)seguridad, nacieron otras entidades que, en algunos casos, son referente nacional e internacional –Panda, S21sec, Nextel–.

Las universidades en Euskadi han tardado en evolucionar también. El Plan Bolonia era una excelente oportunidad para hacer de la seguridad una línea estratégica, y no hubo ninguna excepción que pudiera confirmar la regla. Durante la primera parte de los años 2000, el crecimiento de las empresas y expertos de ciberseguridad en Euskadi fue limitado, de acuerdo a la propia estrategia de las empresas y sus propios planes de atracción y formación de nuevos profesionales. Se puede afirmar que, además de técnicos expertos en integrar tecnologías de seguridad comerciales con bases de conocimiento en redes y sistemas, las empresas vascas pioneras en modelos de ciberseguridad se han ido nutriendo de personas inquietas y autodidactas, cuyo mejor escenario de desarrollo y aprendizaje han sido los foros de Internet. Es como crear una nueva profesión a partir de grupos reducidos con un interés común que se puede transformar de «hobby» a profesión.

Aquellas empresas, *start-ups* entre la era Internet y su burbuja, se enfrentaron a un mercado reactivo e inmaduro. Y poner en marcha un equipo joven (muy joven,

[12] «¿De qué nos sirve asegurar nuestros sistemas si en la relación con clientes o proveedores, ellos pueden ser una fuente de riesgos que aprovechen con éxito los atacantes para llegar a nuestra información?» (Comentario del autor).

en general) con un modelo de empresa y de servicios avanzado y diferencial tampoco es baladí; si bien existían en el mercado empresas que habían desarrollado sus negocios en base a la adopción y desarrollo de plataformas Internet/Intranet que añadían la seguridad de las redes[13].

Entender cómo actúan los atacantes, valorar cómo se puede evitar la efectividad de los mismos y construir modelos de seguridad orientados a la prevención, eran las claves esenciales de su propuesta, con una base sólida en el I+D+i. Y es aquí donde tampoco la Red Vasca de Ciencia y Tecnología tenía una estrategia definida de cara a innovar en ciberseguridad y a embeber la misma en todos sus modelos de innovación. Curiosamente, tanto las universidades como los centros de I+D+i, han tenido en estas compañías sus mejores fuentes de inspiración para incluir en sus respectivas estrategias estos perfiles y planes de desarrollo de ideas y talento. Y hoy, algunas de ellas son referentes a nivel nacional y europeo (Tecnalia, Vicomtech, Ikerlan).

De la necesidad se hace virtud, y esas empresas vascas tuvieron que acelerar su salida a otros mercados nacionales e internacionales para poder generar y atraer talento, llegar con sus productos y servicios a empresas relevantes y tractoras, invertir e innovar en nuevas líneas. La ciber(in)seguridad se genera por la constante investigación e innovación a la hora de buscar brechas de seguridad por parte de los ciberdelincuentes, y la situación exige un modelo de inversión y adaptación continua[14].

Además, a la hora de desarrollar sector y mercado, las empresas nacidas en Euskadi han sido palanca del desarrollo legal y regulatorio de modelos de confianza digital, siendo parte activa en foros nacionales e internacionales, trabajando con la Administración pública para la definición, desarrollo y aprobación de una Estrategia Nacional de Ciberseguridad, a la par que su participación y liderazgo en el ecosistema de la Industria Nacional de Ciberseguridad es único[15]. Curiosamente, esas iniciativas fueron llevadas a otras administraciones, dando lugar a diferentes planes de carácter parcial que, poco a poco, se han ido consolidando. Entidades, como INCIBE (antigua INTECO), han sido y siguen siendo referentes en los que plasmar esas ideas a nivel nacional, con una participación muy activa del ecosistema vasco. Si hoy se

---

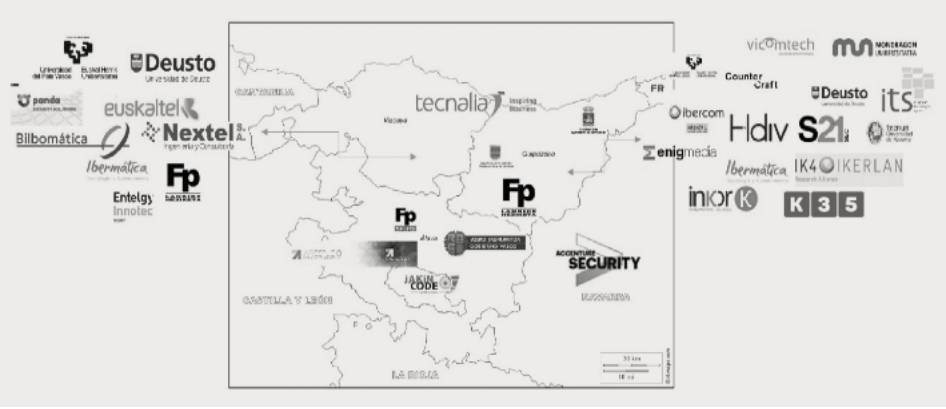
[13] «Recuerdo que poner en marcha S21sec con un equipo de expertos/hackers venidos de diferentes comunidades, al que se unió un equipo local que venía de experimentar en los laboratorios de la UPV –Facultad de Informática de Donostia–, supuso un cambio diferencial a la hora de valorar los riesgos tecnológicos» (Comentario del autor).

[14] «Si miramos la foto actual, podemos comprobar que el talento inicial se ha ido desarrollando profesionalmente y ha terminado, en muchos casos, dando un paso adelante, convirtiéndose en emprendedores cuyos productos y servicios son reconocidos allende nuestras fronteras. Hoy en día forman parte de nuestro excelente Ecosistema Vasco de Ciberseguridad» (Comentario del autor).

[15] «Ya en el año 2005 se propuso a la Administración Pública Vasca poner en marcha un Centro Vasco de Ciberseguridad en formato de colaboración público-privada para desarrollar la nueva Sociedad Digital –Euskadi Digital Segura– y crear un ecosistema de Empleo e Innovación que posicionara a Euskadi en el mapa global de esta materia. Tras insistir durante las siguientes 3 legislaturas, nuestra región ya tiene en marcha su modelo» (Comentario del autor).

analiza el mapa de empresas a nivel nacional y a nivel de Euskadi, se puede afirmar que es la comunidad líder[16].

*Gráfico nº 6.* **EL ECOSISTEMA DE LA CIBERSEGURIDAD EN EUSKADI (2017-18)**




*Fuente:* Proyecto Cyber-Range- BIC Berrilan- Igor Unanue-Xabier Mitxelena.

El mapa del ecosistema de ciberseguridad de Euskadi 2017-18 (gráfico nº 6) es una amplia muestra del sector y evidencia el grado de especialización del mismo que se ha ido construyendo en el entorno del País Vasco, líder a nivel nacional, con amplia presencia a nivel internacional, y cuya consolidación es un reto permanente. La necesidad de establecer un modelo industrial siempre ha estado latente en el propio desarrollo del sector, y hoy en día es relevante establecer las líneas estratégicas adecuadas.

Según apunta el último Global Cybersecurity Index de la Unión Internacional de Telecomunicaciones (ITU, 2019)[17] referente al compromiso de sus países miembros con la Ciberseguridad[18], España se sitúa en el séptimo lugar a nivel mundial de los 193 Estados miembros de la ITU con una puntuación de 8,96, escalando 12 posiciones respecto a 2017. A la cabeza de este ranking se encuentra Reino Unido (9,31), Estados Unidos (9,26) y Francia (9,18). En el caso de Euskadi, sin tener datos oficia-

16 En la actualidad, Euskadi tiene catalogados 153 agentes, con 125 empresas privadas, de las cuales 29 son *start ups –2ª Edición Libro Blanco Ciberseguridad en Euskadi–*, 4 empresas están en el TOP10 a nivel nacional, los centros tecnológicos son líderes y referentes en Europa. Además https://www.businessinsider.es/14-startups-espanolas-sector-ciberseguridad-nacional-665619, hay 6 *Start-Ups* entre las más prometedoras del momento. *Business Insider*.

17 El índice de la ITU se basa en 25 indicadores de 5 bloques obtenidos a través de encuestas a los países participantes, expertos, instituciones colaboradoras y stakeholders. Se divide en legal, técnico, organizacional, de construcción de capacidad y de cooperación, e incluyen aspectos como estándares de seguridad, protección de la infancia o campañas públicas de advertencia, entre otras.

18 https://cuadernosdeseguridad.com/2019/11/espana-ciberseguridad-ranking/

les, un estudio de Cybersecurity Ventures reflejado en el *Libro Blanco de la Ciberseguridad en Euskadi* (2ª edición), aporta algunos datos acerca a la dimensión del sector y la adopción de la ciberseguridad por parte de la industria como elemento de competitividad:

- ≈ 29 *start-ups* enfocadas en la ciberseguridad establecidas en Euskadi.
- ≈ €2M de Ayudas Programa de ayudas público específico para proyectos vascos de ciberseguridad en 2019.
- 38% incremento de demanda de empleo en ámbito informática e ingeniería industrial vs 2016.
- > 2.000 profesionales en el ámbito de la ciberseguridad establecidas en Euskadi (≈ 200 en *start-ups*).
- 5.200 empleos titulados universitarios o de FP necesarios en el ámbito de informática e ingeniería industrial.
- 18% de empresas industriales tienen planes formales de ciberseguridad.
- 80% de empresas vascas contempla realizar acciones de ciberseguridad en sus presupuestos.
- 85% de empresas vascas consideran que la inversión en ciberseguridad industrial se incrementará en los próximos años.

Asimismo según el estudio *Advice Strategic Consultants* en base a una encuesta a más de 2.400 empresarios, tres empresas vascas figuran entre las diez principales del Estado: Panda Security (2ª), S21SEC (5ª) y Counter Craft (8ª)[19].

En general, hasta la fecha, a nivel de Comunidades Autónomas se carece de una estimación fidedigna, si bien, respecto a las incidencias reportadas en el entorno de los ciberataques, Euskadi no aparece entre las más afectadas. Cataluña, Madrid, Andalucía y la Comunidad Valenciana lideran el ranking de Ciberdelitos[20].

### 4.2. **Impulso público**

Inicialmente la Administración Pública Vasca, al igual que muchas otras, siguió las mismas pautas a la hora de incluir la ciberseguridad en sus planes, si bien con el tiempo se dieron actuaciones que supusieron un antes y un después en el compromiso con la Agenda digital(Nota al pie)[21] y sus recursos esenciales. Actualmente, la

---

[19] https://escudodigital.com/ciberseguridad/2019/11/04/ranking-del-estudio-advice-sobre-las-primeras-empresas-de-ciberseguridad-espanolas/

[20] https://www.redseguridad.com/actualidad/los-ciberdelitos-crecen-en-espana-un-35-en-2019_20200608.html

[21] Los distintos planes del Gobierno vasco en sus diversas etapas asociados a la Agenda Digital son: Euskadi 2000tres (2000-2003), Plan Euskadi en la Sociedad de la Información (2002-2005 PESI), Plan Euskadi en la Sociedad de la Información 2010 (PESI 2.0), Agenda Digital Euskadi 2015 (AD@15) y la actual Agenda Digital de Euskadi 2020 (AD@2020).

Agenda Digital de Euskadi 2020 (AD@2020) articula y despliega las medidas concretas que expresa dicho compromiso.

Así, siguiendo iniciativas que países como Alemania habían ya iniciado, en Euskadi, con su Gobierno a la cabeza, se puso en marcha la transformación de la industria a través de la conectividad y la digitalización de su operativa. Se empezaba a ser muy consciente de la relevancia de transformar productos en servicios, de aprovechar las tecnologías de comunicación y la conectividad para competir más y mejor en los mercados. Euskadi forma parte del proyecto Vanguard desde el año 2013, proyecto en el que 15 regiones europeas comparten el objetivo de alcanzar un nuevo modelo de crecimiento de forma inteligente (Gobierno Vasco, 2017).

En paralelo, el Plan de Ciencia , Tecnología e Innovación 2020 «*PCTI Euskadi 2020*»[22] que el Gobierno Vasco aprobó e implementó está alineado con la estrategia de crecimiento que planteaba la Unión Europea para esta década, Estrategia Europa 2020, con la doble finalidad de superar la crisis reciente y crear las condiciones propicias para un crecimiento distinto con tres prioridades: que sea inteligente, sostenible e integrador.

*Gráfico nº 7.* **PRIORIDADES ESTRATÉGICAS DE ESPECIALIZACIÓN INTELIGENTE (RIS3) DE EUSKADI GOBIERNO VASCO**


*Fuente:* Documento RIS3 Euskadi.

El Plan de Ciencia, Tecnología e Innovación Euskadi 2020 (PCTI) aúna todos los esfuerzos y los agentes que trabajan en la estrategia de especialización inteligente, y por tanto en el RIS3 Euskadi. La estrategia RIS3 de Euskadi[23], diseñada como herramienta para poder acceder a los fondos estructurales europeos y alineada con esas

[22] https://www.euskadi.eus/contenidos/enlace/pcti2020_resumen/es_def/adjuntos/pcti_resumen_es.pdf

[23] La Estrategia de investigación e innovación para la especialización inteligente de Euskadi.

tres prioridades, tenía como objetivo fundamental generar modelos de colaboración y transformación en el ecosistema, tanto de empresas como de centros educativos e innovación, poniendo el foco en 3 áreas fundamentales en el tejido económico vasco: biociencias/salud, energía y fabricación avanzada.

Si bien en el ámbito del RIS3 la ciberseguridad no tenía un papel primordial –*la respuesta inicial ante la pregunta sobre su encaje fue que esas capacidades eran comunes y no específicas*–, hoy en día no se plantea su exclusión[24]. El nuevo enfoque supone un antes y un después a la hora de diseñar la economía digital y la sociedad conectada con igualdad de oportunidades para la ciudadanía.

Al igual que el liderazgo y compromiso de las Administraciones públicas es esencial para dinamizar este nuevo escenario, generando la demanda adecuada y reconvirtiendo los soportes fundamentales –I+D+i, educación, internacionalización, infraestructuras– ese liderazgo en el ámbito de la confianza en el ciberespacio, que se debe compartir globalmente, supone también un añadido más para lograr un futuro sostenible.

Uno de los elementos clave a la hora de dar cobertura a los servicios digitales y a la consolidación de un nuevo modelo económico es la identidad digital. La velocidad de los cambios tecnológicos, la presión de los mercados desde la oferta y la adopción de tecnologías como solución a riesgos y problemas, ha sido parte de la inmersión –*reactiva*– en la seguridad digital. Se ha pasado de los virus de finales de los 80 y los 90 a ataques automatizados y/o dirigidos mucho más sofisticados y efectivos.

Las administraciones, al igual que la mayoría del resto de empresas y organizaciones, han hecho inversiones muy relevantes en crear redes conectadas y generar servicios que pudieran ser consumidos de forma remota y sencilla. Una de las claves que dieron lugar a la primera burbuja de Internet (año 2000) es que las ideas se valoraban a niveles nunca vistos y la proliferación de las mismas impulsaron a las empresas a su rápida adopción: portales de servicios, plataformas eCommerce. La clave era ser el primero y dar con la fórmula mágica de la sencillez y la operatividad. Eso sí, la seguridad, entonces, estaba más en los equipos de TI –Tecnologías de la Información– añadiendo tecnologías de protección a redes, servidores y puestos de trabajo –antivirus, firewall, IDS–. Básicamente, era «pasar de la máquina de escribir a un procesador de textos», de redes privadas sin acceso a Internet a redes con «tecnologías de seguridad» que generaran confianza ante un nuevo servicio. No es momento de entrar en los resultados, lo que sí está claro es que las versiones 1.0 de cualquier modelo tienen mucho margen de mejora. La experiencia prueba/error, considerada como proceso de mejora, siempre ayuda a avanzar, eso sí de forma reactiva en años pasados.

---

[24] El último Congreso de 2019 del Basque Industry 4.0 así lo ha reflejado, integrando el Congreso de Industry con el de Ciberseguridad, que tuvo su bautizo en 2018 –más de 1000 asistentes en esa primera edición dan fe de la sensibilidad actual en la sociedad vasca–. Se ha pasado de declaraciones en las que se afirmaba que las empresas que no aborden un proceso de transformación Industry 4.0, industria conectada, no tendrían futuro, a afirmar que sin ciberseguridad no hay Industria 4.0.

## 5. LAS ESTRATEGIAS DE CIBERSEGURIDAD

Si bien la historia de la ciberseguridad es muy reciente, no es menos cierto que la velocidad de los cambios y la evolución «innovadora» de la ciberdelincuencia, con todos sus «colores y sabores», ha terminado por hacernos reaccionar y entender de primera mano qué necesitan las empresas, la Administración y los ciudadanos.



### 5.1. La Estrategia europea

Cuando los programas electorales en Europa incluyen estrategias de transformación económica y social, con foco en la generación de empleo de calidad y en generar oportunidades que lleguen de forma adecuada a todos los ciudadanos, la ciberseguridad pasa a ser un elemento esencial: sin ciberseguridad no hay futuro, no hay confianza digital. Si llevamos estas ideas al entorno más cercano, podemos afirmar que estamos 100% alineados.

En un ciberespacio en el que las grandes empresas tecnológicas dominan las infraestructuras y la información, en el que hay países que aprovechan la falta de gobernanza para ganar en influencia y control sobre el resto del mundo, Europa decidió hace ya unos años dar un paso adelante y puso en marcha una Estrategia de digitalización y competitividad con un área específica de creación de un ecosistema de confianza. Los actores e hitos especiales en esta línea se pueden resumir en:

- European Network Information Security Agency (ENISA) (marzo de 2004): Agencia de Ciberseguridad de la Unión Europea cuyo objetivo fundamental es ayudar a elaborar las políticas y la legislación de la UE sobre seguridad de las redes y de la información. Esto también contribuye al crecimiento económico en el mercado interior europeo (Cybersecurity Industry).
- European Cybersecurity Organization (ECSO): Asociación sin ánimo de lucro que nace en junio de 2016 como parte de la iniciativa público-privada de ciberseguridad europea (cPPP), conjuntamente con la Comisión Europea. Sus objetivos están orientados a crear redes digitales de confianza para empresas y ciudadanos europeos en base al desarrollo de la industria de la ciberseguridad (talento, certificaciones, tecnologías, empresas, servicios).
- Directiva NIS (6 de julio de 2016): Identificación de los sectores de servicios esenciales en los que se debe garantizar la seguridad de las redes y sistemas de información y establecer las exigencias para la gestión de las crisis y notificación de incidentes de forma coordinada.
- Reglamento General de Protección de Datos (RGPD_GDPR) (14 de abril de 2016): El Reglamento General de Protección de Datos es el reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de los mismos. Su fecha definitiva de aplicación y puesta en marcha fue el 25 de mayo de 2018.

Tal y como refleja el artículo publicado por el Real Instituto Elcano (Alonso Lecuit, J., 2018), la agenda de ciberseguridad de la UE ha evolucionado significativamente desde el primer Plan Estratégico de Ciberseguridad en 2013 para incorporar nuevas medidas en defensa de la seguridad, prosperidad y libertades de los ciudadanos frente a las amenazas y vulnerabilidades disruptivas del ciberespacio.

Este plan inicial ha dado lugar a sucesivos planes quinquenales donde el impulso más relevante se ha venido desarrollando dentro del marco de la Estrategia Europea de Seguridad 2015-2020.

Sin duda esta Estrategia, cuya continuación ha sido revisada y aprobada para el periodo 2020-2025.- COMISIÓN EUROPEA (2020d), tiene sus mimbres en los aspectos de la seguridad integral, pero por la propia evolución de la sociedad se trasciende a un ámbito digital, en el que se han instalado y transformado muchos de los riesgos y delitos más tradicionales.

Un aspecto a considerar son los 4 pilares estratégicos que, sin duda, debemos trasladar a cada rincón de la UE: 1) un entorno de seguridad con garantías; 2) hacer frente a las amenazas cambiantes; 3) proteger a los ciudadanos europeos del terrorismo y la delincuencia organizada; y 4) un ecosistema de seguridad robusto.

En definitiva, crear un espacio de seguridad y confianza que proteja a los ciudadanos y empresas europeas dotándoles de las herramientas necesarias para construir la economía del futuro desde la innovación y la competitividad.

Europa tiene en ENISA su instrumento para la puesta en marcha de las políticas de desarrollo del sector, de la innovación, de los modelos de gobernanza. Recientemente, la Agencia ha realizado un estudio dirigido a identificar los obstáculos para una mayor seguridad de la información y ha dado una serie de recomendaciones a Europa y a sus países miembros para garantizar los niveles de confianza necesarios. Las conclusiones principales de este estudio son las siguientes:

- La Unión Europea debería presentar una ley que obligue a notificar las brechas de seguridad.
- Debería garantizarse la publicación de estadísticas fiables sobre el delito electrónico.
- Es necesario recoger y publicar datos sobre la cantidad de spam y otro tráfico indeseable que emiten los proveedores de servicio de internet (ISP) europeos.
- Instauración de una escala de sanciones para los ISP que no respondan con prontitud a peticiones de retirada de máquinas comprometidas y que se recoja el derecho de los usuarios a que sus máquinas sean reconectadas, siempre y cuando ellos asuman la total responsabilidad.
- Desarrollo e implantación de estándares para que el equipo que se conecte a las redes sea seguro por defecto.

- Debería adoptarse una revelación temprana y responsable de vulnerabilidades, junto a la responsabilidad del fabricante sobre el software no parcheado, de forma que se acelere el ciclo de desarrollo de parches.
- Los parches de seguridad deben ser gratis y mantenerse separados de los que representan actualizaciones de funcionalidades.
- Debería armonizarse el proceso de resolución de disputas entre clientes y proveedores de servicios de pago con respecto a las transacciones electrónicas.
- Establecer un régimen de sanciones efectivas y proporcionadas contra las prácticas abusivas del comercio on-line.
- Estudiar los cambios a realizar en las leyes de protección de los consumidores para adaptarlas al progreso del comercio on-line.
- Las autoridades encargadas de velar por la competencia deberían ser asesoradas, siempre que la diversidad tenga consecuencias sobre la seguridad.
- Investigar los efectos de los fallos en los nodos de intercambio de Internet (IXP).
- Impulsar la ratificación por parte de los estados miembros de la Convención sobre Ciberdelito.
- Establecimiento de un cuerpo de ámbito europeo encargado de facilitar la cooperación internacional sobre ciberdelitos, usando la OTAN como modelo.
- Garantizar ante la Comisión Europea que las regulaciones presentadas con otros propósitos no dañen inadvertidamente a los investigadores y las empresas de seguridad.

Sin duda, se trata de democratizar la ciberseguridad y los riesgos digitales para crear una verdadera cultura que nos permita competir y navegar en las redes de confianza, generando un ecosistema donde la responsabilidad compartida sea parte de la solución.

### 5.2. **El despliegue de la Estrategia europea en España y comunidades autónomas**

A nivel nacional, la proliferación y transformación de centros de ciberseguridad públicos ha tenido en los últimos años una evolución desigual, hasta llegar a los modelos de colaboración y complementariedad (CCN-CERT, INCIBE, CNPIC, MCCD, DSN).

El Centro Criptológico Nacional (CCN), adscrito al Centro Nacional de Inteligencia (CNI), nace al amparo de la Ley 11/2002 para garantizar la seguridad de las tecnologías de la información y de protección de la información clasificada. Sin embargo, el auge llega algunos años después. Desde el nacimiento de INTECO, hoy Instituto Nacional para la Ciberseguridad (INCIBE), en 2006, y al mismo tiempo de crearse en ese mismo año el Centro Criptológico Nacional-Computer Emergency

Response Team (CCN-CERT), se puso en marcha el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), por acuerdo del Consejo de Ministros del 2 de noviembre de 2007, y el Mando Conjunto de Ciberdefensa (MCCD) (Orden Ministerial 10/2013, de 19 de febrero de 2013).

En el camino, en virtud del Real Decreto 1119/2012 de 20 de julio, se puso en marcha el Departamento de Seguridad Nacional (DSN) como órgano de asesoramiento al Presidente del Gobierno en materia de Seguridad Nacional.

Recientemente (julio de 2020), se ha creado el Foro Nacional de Ciberseguridad, un espacio de colaboración público-privada impulsado por el Consejo de Seguridad Nacional. Sus líneas de trabajo están centradas en generar una cultura de ciberseguridad, ofrecer apoyo a la industria e I+D+i y una oportunidad para la formación y el talento en ciberseguridad; todas ellas alineadas con las medidas recogidas en la Estrategia Nacional de Ciberseguridad 2019 (Consejo Nacional de Seguridad, 2019).

Si bien en principio la Ciberseguridad era motivo de reflexión general, con un mayor foco y prioridad en algunos de estos centros, hoy es la línea esencial de todas las estrategias conjuntas. Afortunadamente, la «competencia» en el ámbito público, consciente de la importancia del liderazgo ante los riesgos digitales, ha dado lugar a una estrategia a nivel nacional donde la coordinación y la identificación de funciones dan respuesta a un único modelo de gobernanza. Alineados con las líneas maestras que se han diseñado desde la Comisión Europea, los principios rectores de la Estrategia Nacional de Ciberseguridad se sustentan en 4 principios fundamentales:

- Unidad de acción: la eficacia y rapidez de respuesta frente a los ciberincidentes que involucren a diferentes agentes estatales se lograrán en coordinación con la Unidad de Acción del Estado.
- Anticipación: las acciones estatales para reducir los alcances de las amenazas críticas demandan mecanismos preventivos ideados por organismos especializados. El sector privado también debe participar con su conocimiento.
- Eficiencia: la Estrategia Nacional de Ciberseguridad requiere sistemas multipropósito, como tácticas tecnológicas, económicas, socialmente responsables, que optimicen los recursos y encaucen la acción del Estado.
- Resiliencia: el Estado debe disponer de elementos que mejoren la capacidad de reacción contra las ciberamenazas.

Estos principios vienen avalados por un modelo de organización y gobernanza que dé respuesta eficiente a todos los riesgos digitales que amenazan de forma constante la continuidad de los servicios e infraestructuras digitales, así como mantener la privacidad e integridad de la información. Y se definen para dar respuesta a los modelos de colaboración y gestión de crisis establecidos en Europa, y que deben tener un entorno de coordinación único. Su relación con las CC.AA. es parte de las nuevas revisiones de cara a la Estrategia Nacional de Ciberseguridad 2021.

Llegados a este punto hay que afirmar que todos los países miembros de la Unión Europea han ido definiendo su modelo de gobernanza incluido dentro del modelo europeo de comunicación, compartición y gestión unificada de ciberincidentes de carácter crítico. La proliferación de los CSIRT/CERT (Computer Security Incident Response Team) ha hecho que se quieran regular a nivel público y privado dentro de este entorno de colaboración. Por último, de cara a conseguir los objetivos de confianza y percepción de ciberseguridad en la sociedad, se ha puesto en marcha un Plan de Acción en España, en la Estrategia Nacional de Seguridad 2019, con 5 objetivos fundamentales:

- Reforzar las capacidades ante las amenazas provenientes del ciberespacio y garantizar la seguridad y ciberresiliencia de las infraestructuras críticas.
- Incrementar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad de los ciudadanos y proteger los derechos y libertades en el ciberespacio.
- Desarrollar e impulsar los niveles de ciberseguridad de ciudadanos y empresas.
- Obtener una autonomía digital única desarrollando la industria de ciberseguridad, generando, atrayendo y reteniendo al mejor talento.
- Contribuir a la seguridad del ciberespacio a nivel internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable en apoyo a los intereses nacionales.

Sin duda, esta Estrategia que nace desde Europa para alinear a sus países miembros tiene en las regiones un elemento adicional de desarrollo económico y social. A nivel de gobernanza, las Comunidades Autónomas son un elemento complementario en esta cadena de valor dentro del ciberespacio, donde, además de coordinarse a diferentes niveles en los ámbitos de gestión de riesgos y respuesta ante crisis conjuntas, deben establecer políticas y estrategias que den cobertura y respuesta local a estos nuevos retos que nos ofrece el ciberespacio. En este sentido la función del Departamento de Seguridad del Gobierno Vasco en el ámbito de protección de infraestructuras críticas, dando cobertura a aquellas que se han identificado a nivel nacional que «residen» en Euskadi, y aquellas que pueden afectar al futuro y sostenibilidad dentro de la Comunidad, se ha venido desarrollando en el ámbito de colaboración con la Estrategia Europea y su implantación en el Estado. La respuesta ante incidentes y su prevención como objetivo son una de las líneas de acción que, de forma más o menos coordinada, se han puesto en marcha durante la última década.

Así comunidades autónomas como Cataluña han creado sus propios centros de ciberseguridad (CESICAT-2009), basándose en estos pilares que hoy son comunes en Europa, como el CERT de Andalucía, que vio la luz en el Plan Director de Servicios de Información y Telecomunicaciones 2010-2013, o el CSIRT de la Comunidad Valenciana, que lleva años trabajando en los modelos de ciberseguridad y respuesta impulsados desde su Gobierno.

### 5.3. El despliegue presente y futuro de la Estrategia público-privada de ciberseguridad en Euskadi. Sus fortalezas

A la par de los riesgos y las amenazas globales señaladas anteriormente es necesario evaluar y revisar las fortalezas que existen, en este caso en Euskadi, en el marco de la Estrategia europea y estatal en materia de ciberseguridad a la hora de «combatir» estos riesgos y amenazas.

Aunque las estadísticas no han llegado hasta el último trienio, como se ha comentado con anterioridad, Euskadi aparece como una de las comunidades autónomas con menos delitos informáticos denunciados a nivel nacional, si bien Bizkaia aparece en el TOP6 a nivel de provincias. No es menos cierto que los ataques de ransomware han impactado en algunas empresas y en diferentes ámbitos de la Administración pública, sin un resultado grave o irreparable hasta la fecha. Por eso hay que destacar las fortalezas que ofrece Euskadi en este mundo digital, siendo claves los planes estratégicos que desde 2018 forman parte de la hoja de ruta pública. Los aspectos más destacables son:

- Estrategia Ciberseguridad Industrial 2025 Gobierno Vasco, con un plan de inversiones ambicioso alineado con la transformación digital de la sociedad y su economía. El liderazgo público, con el BCSC y ZIUR como centros de apoyo y dinamización, junto al clúster de empresas de ciberseguridad Cybasque, serán elementos críticos a la hora de consolidar una Euskadi digital de confianza.
- Ecosistema robusto de empresas de ciberseguridad: con más de 25 años de historia, hoy hay más de 150 actores que refuerzan una industria cuyo desarrollo y globalización deben hacer que en Euskadi exista una «autonomía digital».
- Educación: siendo pioneros en el desarrollo de profesionales, la ciberseguridad es parte de la Formación Dual (FP y Universidad) desde hace varios años, ejemplo que posteriormente se ha seguido a nivel nacional. Un plan ambicioso de concienciación, capacitación y desarrollo del talento seguirá siendo la base fundamental de la resiliencia de los negocios y actividades digitales.
- Ecosistema de innovación: el más avanzado del sur de Europa, cuenta con aceleradores que se han ido incorporando en los últimos años. Programas como Bind 4.0[25] y diferentes iniciativas público-privadas con un creciente volumen de inversores en este eje estratégico.
- Participación en la Estrategia Europea: desde la colaboración y el liderazgo en los programas de I+D+i y certificaciones, el mapa innovador de los próximos 5 años tendrá en Euskadi uno de sus nodos de referencia.

---

[25] Es un programa del Gobierno vasco de aceleración de ideas y proyectos empresariales de 24 semanas donde las *start-ups*, además de desarrollar un proyecto remunerado con una de las empresas industriales colaboradoras, disponen de un programa intensivo de servicios de apoyo y actividades. Este año 2020 en su 5ª edición se han inscrito 750 *start-ups* de todo el mundo y 57 empresas colaboradoras. https://www.spri.eus/es/basque-industry-comunicacion/bind-4-0/750-startups-de-todo-el-mundo-se-inscriben-al-programa-de-innovacion-abierta-bind-4-0/

En Euskadi se han hecho avances importantes en los últimos 4 años. Con un sector privado fuerte y unos centros de investigación cada vez más activos en los ámbitos de la securización de productos y servicios, la última legislatura ha supuesto un antes y un después en los retos de confianza que nos plantea el mundo digital.

***El Centro Vasco de Ciberseguridad (BCSC)***

La inauguración del Centro Vasco de Ciberseguridad, el 18 de julio de 2018, supuso la puesta de largo de una iniciativa que vio su luz en octubre de 2017 como resultado de la Estrategia del Gobierno Vasco en materia de seguridad en el ciberespacio. De carácter 100% público y dependiente de la SPRI, su objetivo esencial es «promover la ciberseguridad en Euskadi».

La importancia de este compromiso queda reflejada en sus órganos de gobierno, del que forman parte diferentes Departamentos del Gobierno Vasco: Desarrollo Económico, Sostenibilidad y Medio Ambiente, Seguridad, Gobernanza Pública y Autogobierno, y Educación; así como centros tecnológicos con líneas especializadas en ciberseguridad: Basque Center for Applied Mathematics (BCAM), Ikerlan, Tecnalia y Vicomtech.

Sería conveniente resaltar la gran visibilidad que actualmente tienen estos centros tecnológicos tanto a nivel nacional como internacional, liderando proyectos estratégicos en materia de seguridad. Sin duda, a ello ha contribuido el amplio y potente tejido empresarial de ciberseguridad que existe en Euskadi desde finales del siglo XX. Esta característica se une al espíritu emprendedor que ha sido reforzado con la proliferación de núcleos inversores en tecnología y programas públicos, como BIND 4.0, que han acercado la innovación, en este caso en materia de ciberseguridad, al tejido empresarial vasco.

El Centro Vasco de Ciberseguridad (BCSC) ha sido clave a la hora de poner en marcha iniciativas que, por su dimensión y alcance, no hubieran sido sencillas de elevar al nivel del Congreso de Ciberseguridad celebrado en el Palacio Euskalduna en 2018, con asistencia e interés masivos, y a un evento con participación del Gobierno Vasco y de las empresas vascas en el Congreso de Ciberseguridad más relevante del mundo (RSA Conference-San Francisco-2019) dando visibilidad a una estrategia que en la nueva legislatura será diferencial y única.

***Centro de Ciberseguridad Industrial (ZIUR)***

En paralelo, dentro de la propia idiosincrasia y paradojas de Euskadi, Gipuzkoa puso en marcha la Fundación ZIUR[26] con el objetivo de llevar la ciberseguridad al tejido empresarial de la provincia. La amplia participación y compromiso de los lí-

[26] La Diputación Foral de Gipuzkoa y el Ayuntamiento de Donostia inauguraron las instalaciones de este Centro de Ciberseguridad Industrial en el Parque Empresarial de Zuatzu, en noviembre de 2019.

deres políticos y empresariales en impulsar ambos centros da fe de la relevancia que ha adquirido la ciberseguridad como activo de la sociedad vasca, y la razón de ser de ZIUR en el ámbito de la industria de Gipuzkoa es un valor añadido que solo puede acelerar la adopción de las buenas prácticas de forma generalizada.

Viendo los objetivos de ambas entidades y entendiendo que la colaboración es el elemento crítico de cara a optimizar recursos, acciones y resultados, se puede asegurar que en Euskadi el futuro pasa por generar un modelo digital que dé soporte a la Nueva Economía. BCSC y ZIUR son dos excelentes palancas para demostrar el liderazgo.



Palancas que se antojan claves en medio de una pandemia global que está haciendo revisar las agendas, obligando a tomar decisiones valientes y exigiendo modelos y planes en el entorno social, económico y laboral que den paso a una Euskadi digital competitiva, igualitaria y única. Hace falta un liderazgo mucho más acusado que el mantenido hasta ahora y una unidad de acción sin precedentes en la democracia. Y es aquí, en esta necesaria y urgente transformación, donde llevar la seguridad aplicada al diseño de las soluciones, de los servicios y de los productos, a las infraestructuras y a la cultura de la sociedad y ciudadanos, debe conducir que Euskadi se convierta en un referente y ejemplo de cómo afrontar los retos de futuro de forma inteligente y decidida.

### *Cybasque*

Aunque este proyecto comenzó antes de la emergencia sanitaria decretada por la pandemia de coronavirus COVID-19, Euskadi, con el Gobierno Vasco, el BCSC y sus empresas de ciberseguridad a la cabeza, anunció en San Francisco (febrero de 2020), en su segunda puesta de largo en la RSA Conference, la puesta en marcha de Cybasque[27], asociación de empresas vascas de ciberseguridad que, al amparo de la experiencia y éxito del clúster GAIA, nace con el objetivo fundamental de alinear la estrategia público-privada en materia de ciberseguridad, dotando a la región de autonomía digital y creando un ecosistema que sea referente en Europa.

La pandemia no ha hecho más que inyectar velocidad adicional a la necesidad de trabajar juntos para poner las bases de Euskadi de cara a 2050. Y, curiosamente, la propia experiencia en el ámbito digital durante el confinamiento[28] puede permitir entender mejor cómo reforzar la confianza digital.

---

[27] Agrupa actualmente a diez empresas, que se han visto ampliadas a 44 antes de la Asamblea General del 14 de octubre de 2020, y nace con el reto de posicionar al ecosistema vasco como *hub* de referencia a nivel internacional, aunando el potencial empresarial para responder de manera efectiva a las necesidades de la industria vasca.

[28] Durante este confinamiento, derivado del estado de alarma decretado por el Gobierno español el 14 de marzo de 2020 para hacer frente a la expansión de coronavirus COVID-19, hemos descubierto que hay elementos que debemos revisar de forma urgente. El teletrabajo tenía un índice de ejecución entre el 6-7%, cuando en realidad estamos preparados para que al menos un 20% del trabajo se pueda ejecutar de forma remota. Meses después del inicio del estado de alarma, parece que el teletrabajo ha

La puesta en marcha de un Plan Estratégico de Ciberseguridad 2020-2025 por parte del Gobierno Vasco al final de la reciente legislatura, viene a reforzar la ambición de dotar a la economía y a la sociedad vasca de una solvencia digital que se acompañe de elementos de diferenciación que permitan seguir siendo competitivos en este mundo globalizado.

Por su impacto en las vidas, en las actividades económicas, y por su relevancia en la resiliencia de los negocios y actividades presentes y futuros, la estrategia que debe desarrollar Euskadi en un modelo claro de colaboración público- privada es embeber la ciberseguridad en la cultura laboral y cotidiana.

Se necesita una Administración de nueva generación que sea palanca de la transformación de la economía. Cuando se presentó en el Departamento de Industria, (actual Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente) el proyecto «Euskadi Digital Segura», el alcance de dicho modelo no estaba tan claro como ahora. Hoy, las industrias, empresas de servicios, los productos y sus derivados que serán la base del futuro, no solo se deben transformar –si no lo han hecho ya–, sino que deben certificar que cumplen con los mejores estándares de seguridad.

Una vez que los centros de ciberseguridad forman parte, de forma activa, de la Estrategia Europea de Ciberseguridad, especialmente participando en los grupos de trabajo de ECSO, visionar los retos e inversiones que desde Europa se están desarrollando debe ser una de las palancas claves para diferenciarnos. Si el WEF ha puesto en marcha el Center for Cybersecurity (C4C), un centro ubicado en Ginebra con el objetivo de industrializar los modelos y requisitos de ciberseguridad en cada sector, Euskadi se debe postular en la misma línea para convertirse en un *hub* de referencia europea y mundial en el ámbito de las capacidades y soluciones de ciberseguridad industrial.

Europa, a través de la Agencia Europea de Ciberseguridad (ENISA), está decidiendo dónde ubicar su Centro Europeo de Ciberseguridad para gestionar la innovación en este campo, con un presupuesto de más de 2.000 millones de euros hasta el año 2027. Hay varias candidaturas optando a ser la sede oficial, entre ellas León a través de INCIBE y el ecosistema de la AEI de ciberseguridad, donde hay una amplia

---

sido un éxito que hemos descubierto «gracias» a la situación que estamos viviendo. Pues bien, a mi modesto entender, nada más lejos de la realidad. Hemos gestionado una crisis sin tener realmente un plan, de forma improvisada y, eso sí, con el voluntarismo y el compromiso de una sociedad que siempre está dispuesta a sacar lo mejor de sí misma en momentos críticos. El «éxito» real es que nos hemos conectado mucho más y que lo hemos podido hacer de forma remota, sin tener un conocimiento mínimo sobre qué supone el teletrabajo y cómo debemos gestionar su aplicación. Y no hablo desde el entorno legal y laboral –para eso hay grandes expertos–, sino desde el balance físico y psíquico que requiere este nuevo formato. Las consecuencias de ese hipotético «éxito» están todavía por llegar y, sumado a las situaciones personales que se han vivido (hijos en casa, pérdidas irreparables…), en este nuevo modelo necesitamos afrontar también la transformación del puesto de trabajo junto a medidas de contingencia que impidan un nuevo caos futuro.

representación de empresas vascas, así como de centros de innovación y universidades. Sin duda, independientemente de su ubicación final, la estrategia de ciberseguridad de Euskadi como región y dada su especialización en el ámbito industrial debería ser partícipe de dichos fondos.

Esa importancia que Europa da a las regiones ofrece una oportunidad única para convertir nichos inconexos de conocimiento y soluciones en una verdadera industria de la ciberseguridad. Construir plataformas y servicios de seguridad y certificación de confianza que se puedan globalizar con modelos de servicios remotos, es un complemento a una estrategia integral que va desde los ciudadanos a la Administración y las empresas.



## 6. RETOS DE FUTURO

Es necesario colaborar entre regiones y países dentro de Europa, y analizar los factores que rigen la estrategia de ciberseguridad de cara al futuro, y que debe ser refrendada en la nueva legislatura del Gobierno Vasco en colaboración con el sector privado, tiene como retos esenciales:

- Cultura de ciberseguridad: crear una verdadera cultura de seguridad educando a la sociedad en el correcto uso de la tecnología y en el conocimiento de sus riesgos asociados. Dotando a la autoridad pública de los recursos humanos y técnicos adecuados para prevenir y perseguir los delitos digitales, ayudando en colaboración con la ciudadanía a mejorar la ciberseguridad percibida. Superar las brechas digitales y consolidar la confianza digital como factor diferenciador para atraer proyectos, empresas e inversores, serán retos prioritarios.
- Talento: desarrollar programas de formación, capacitación, atracción y retención de talento que sean la base de un sector que puede ser generador de empleo de diferentes capacidades para dar soporte a la transformación digital de las industrias y los servicios de Euskadi. Añadir a la calidad de vida del entorno vasco, reconocida con un amplio consenso, alicientes de empleo estable y de calidad, será la base fundamental del crecimiento.
- Industria de ciberseguridad: colaborar, planificar y poner en valor el tejido vasco de ciberseguridad, dando paso a la generación de la demanda junto a modelos de internacionalización que no solo ayuden a dar recorrido y crecimiento al sector, sino que sean atractivos para otras empresas que decidan desarrollar su actividad en Euskadi.
- Productos y servicios seguros: participando de los modelos y estándares que se están concretando en Europa, e incluyendo la ciberseguridad y las certificaciones oficiales en los productos y servicios que generan las empresas. Dotar a los productos industriales de una seguridad por diseño, ofrecer servicios que lleven la seguridad por defecto y aportar el reconocimiento del

ecosistema, aseguran poder competir en las mejores condiciones. Hay un gran avance en el camino de las homologaciones y de la convivencia digital de confianza en la cadena de suministro. Ser pioneros es el reto. Si en calidad, la iniciativa Euskalit –referente en Europa– llevó las buenas prácticas al ecosistema de las pymes, en ciberseguridad urge un Plan de Acción que simplifique el acceso a plataformas seguras para todas.

- I+D+i: reforzar las actividades de innovación haciendo hincapié en incluir la ciberseguridad en todas las iniciativas y aprovechar las iniciativas de innovación específica en la materia para seguir generando nuevos productos y servicios disruptivos. La Red Vasca de Ciencia y Tecnología es clave en este camino, junto a las universidades y sus equipos de investigación.
- Emprendimiento: Euskadi es líder a nivel nacional y uno de los polos europeos donde más y mejor se innova en el ámbito de la ciberseguridad desde su ecosistema de Start-Up. Urge reforzar la colaboración inter- e intra- compañías, difundir la diferenciación del emprendizaje dentro de la ciberseguridad y dotar al territorio de las herramientas económicas y de inversión para acompañar al sector en su crecimiento global. La velocidad es la clave.
- Inversión público-privada: hoy más que nunca, esta es la clave para salir adelante. Y con el impacto de la pandemia del COVID-19 es fundamental dotar a los planes de acción de los recursos necesarios. Con especial hincapié en los 4 sectores estratégicos dentro de Europa. Hacer de la ciberseguridad un elemento común a todos ellos y al resto de las actividades económicas del país requiere de un modelo de riesgo que no se debe poner en duda. Invertir es crear el futuro y no se puede ni se debe esperar a que llegue.

Sin la apuesta por la calidad de los años ochenta y noventa, la economía vasca no hubiera sido ejemplar. La apuesta por la ciberseguridad es la que dará el liderazgo del futuro. Construir herramientas de inversión, aprovechar los Fondos Europeos presentando un proyecto sólido, colaborando con otras regiones y compartiendo el conocimiento de forma bidireccional para ser elegidos. Estas y otras acciones están en marcha y requieren de un modelo de coordinación y gobernanza dentro de Euskadi. Conociendo otras regiones referentes en ámbitos de tecnología, como Lisboa, Dublín, Helsinki, Barcelona, Tel Aviv, algunos de ellos emblema en la innovación y colaboración público-privada, el reto en Euskadi pasa por hacer una apuesta única por esta materia transversal, que, al igual que la calidad en su momento, debe dotar de las herramientas adecuadas al tejido empresarial vasco para abordar sus cambios y sus nuevas apuestas con las máximas garantías.

Estamos empezando una nueva etapa, después de haber cubierto un camino que aporta mimbres y activos muy potentes para ponerse en marcha. En la segunda edición del Libro Blanco de Ciberseguridad de Euskadi «*se han catalogado 153 agentes, con 125 empresas privadas, de las cuales 29 son startups, frente a las 109 empresas y 18 startups de*

*la 1ª edición. Se aspira al reconocimiento de la imagen de marca del sector vasco de ciberseguridad industrial como un ecosistema especializado y referente en Europa*». [29]

La puesta en marcha de Cybasque como motor del desarrollo privado del sector, en colaboración con el Basque Cybersecurity Center (BCSC), viene a iniciar una nueva etapa para posicionar a Euskadi como región, y a sus empresas de ciberseguridad como polo de referencia en Europa. Y la ambición va más allá de los especialistas: se trata de construir un nuevo ecosistema digital que tenga en la seguridad uno de sus activos esenciales, desde las empresas TI de desarrollo y sistemas hasta las empresas industriales en el desarrollo de sus productos y servicios. El software embebido seguro, las máquinas conectadas a través de comunicaciones seguras, serán parte de la competitividad colectiva. Y sin duda, la Administración pública debe ser el mejor de los ejemplos, en un momento donde debe abordar retos trascendentales con cambios generacionales en diferentes departamentos y una necesidad de construir la Administración electrónica de confianza de nueva generación. Proyectos como el Plan Estratégico para el Diseño de un Polo de Ciberseguridad Industrial 2025 en Euskadi, serán la base de este plan conjunto. Pero, sin duda, en unos momentos tan decisivos, el nuevo Plan Estratégico TIC del Gobierno Vasco 2020-2024 deberá contemplar esta apuesta conjunta. Hacer de la ciberseguridad un modelo cultural en el ámbito público será el complemento ideal con ciudadanía y empresas.

## 7. CONCLUSIONES

Actualmente la seguridad digital y la lucha contra los virus informáticos forman parte de las preocupaciones y prioridades de las personas, empresas y de la sociedad en general. El desarrollo y grado de internacionalización de las empresas y las cadenas de valor global establecidas, junto al aumento del soporte digital en los procesos productivos y administrativos, han hecho que la economía real dependa totalmente de los sistemas de seguridad informáticos, pero también han creado un incentivo y caldo de cultivo para acceder a los datos privados, mediante ataques informáticos, para su explotación con fines ilícitos.

Hoy, en plena pandemia y crisis sanitaria y económica, los ataques se han incrementado cerca del 100%, y servicios esenciales como la Sanidad son objeto de la locura y falta de ética absoluta del cibercrimen. El hecho de estar hiperconectados les ha permitido aumentar su «público objetivo» y el éxito de sus actividades delictivas.

Por ello, a la par de la iniciativa privada, necesitamos una Administración de nueva generación que sea la palanca de la transformación de la economía que procure sistemas seguros donde los ciudadanos puedan conectarse confiadamente entre ellos, con las empresas y con las distintas administraciones.

---

[29] https://www.basquecybersecurity.eus/es/actualidad-bcsc/segunda-edicion-libro-blanco-ciberseguridad-euskadi.html

En Euskadi ya existe una ventaja competitiva en base a una industria de ciberseguridad incipiente que tiene más de 25 años de historias de éxito en el ámbito tecnológico y de los servicios, si bien necesita un impulso para su consolidación y liderazgo a nivel de Europa, de cara a competir en los mercados globales. Innovar con una red público-privada alineada y colaborativa y embeber la ciberseguridad en la nueva economía vasca deben ser factores diferenciales de nuestras empresas y organizaciones, y la palanca clave para una sociedad de confianza.

El Gobierno Vasco y los Departamentos que lo integran: Educación, Sanidad, Seguridad, Justicia, Gobernanza, Industria..., la Administración en general, tiene un reto esencial en el que la colaboración intra-Departamentos es vital. Diputaciones, Ayuntamientos y otros estamentos son parte del mismo ecosistema y, por tanto, deben ser partícipes de esta nueva estrategia. Ninguna transformación ha sido tan radical como la que ahora tenemos por delante, y solo invirtiendo en generar un ADN común, una verdadera cultura de ciberseguridad en la sociedad vasca, dará lugar a un entorno de futuro que siga siendo el ejemplo a seguir. El liderazgo de la confianza es suyo y la estrategia debe ser única.

Alinear los planes de transformación de entidades públicas y privadas optimizando las inversiones y los recursos disponibles, redundará en una industria de ciberseguridad de referencia que, junto a la creación de talento y empleos de calidad, hará de Euskadi un país competitivo y atractivo para las inversiones. Las inversiones, las líneas estratégicas y la historia deben avalar este camino, avanzando con convencimiento hacia un futuro apasionante.

Sin olvidar que se debe seguir priorizando innovación, cultura, talento y emprendizaje como acciones esenciales en la hoja de ruta que la sociedad y las empresas vascas requieren. Un futuro mejor es posible, un futuro digital de confianza es necesario.

*«¡Quién le iba a decir a Mikel Fernández que aquel sueño de profesionalizar la ciberseguridad desde el ámbito de la Investigación y la Innovación terminaría siendo el eje fundamental de una nueva era! A veces, los emprendedores anónimos son los que mejor definen la verdadera hoja de ruta del futuro. Como él nos decía, nunca tendremos la seguridad necesaria en las redes hasta lograr que la seguridad 'extremo a extremo' sea real. Una identidad digital única es el reto. Al igual que hace 20 años, cuando su luz se apagaba y nos daba fuerzas para seguir, nuestro lema seguirá siendo: KEEP ON MOVING ON/SEGI AURRERA».*

## REFERENCIAS BIBLIOGRÁFICAS


### LIBROS

Caballero Velasco, M.A. (2019): *Ciberseguridad y Transformación Digital.* Ed. Anaya.

Ellis, R.; Mohan, V. (2019): *Rewired: Cybersecurity Governance*. Editorial John Wiley & Sons.

Harari, Y.N. (2019): *21 lecciones para el Siglo XXI- Parte 1.- El desafío tecnológico.* Penguin Random House Grupo Editorial.

Mitnick, K.; Vamosi, R. (2018): *El arte de la Invisibilidad*. Editorial Anaya.

Suárez, A. (2015): *El Quinto Elemento.* Editorial Deusto.

### DOCUMENTOS Y PÁGINAS WEB

Agencia de la Unión Europea para la Ciberseguridad (ENISA) (2020): *https://www.enisa.europa.eu/news/enisa-news/prs-in-es/enisa-la-agencia-de-ciberseguridad-de-la-ue-apuesta-por-una-mayor-proteccion-de-los-sistemas-scada/view*

*https://europa.eu/european-union/about-eu/agencies/enisa_es*

Accenture (2019): *9º Estudio Anual del Coste del Cibercrimen.* Accenture. *https://www.accenture.com/es-es/insights/security/cost-cybercrime-study*

— (2020a): *State of Cybersecurity Report 2020. https://www.accenture.com/es-es/insights/security/invest-cyber-resilience*

*https://www.accenture.com/_acnmedia/PDF-130/Accenture-3rdAnnual-State-of-CyberResilience-Infographic-Utilities.pdf*

— (2020b): *Accenture 2020 cyber threatscape report https://www.accenture.com/us-en/insights/security/cyber-threatscape-report*

Alonso Lecuit., J. (2018): Evolución de la agenda de ciberseguridad de la Unión Europea. Disponible en: *http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari121-2018-lecuit-evolucion-agenda-ciberseguridad-union-europea* REAL INSTITUTO ELCANO

Basque Cybersecurity Center - Centro Vasco de Ciberseguridad (2020: *https://www.basquecybersecurity.eus/es/*

Centro Criptológico Nacional. Computer Emergency Response Team (CCN-CERT) (2020): *https://www.ccn-cert.cni.es/*

Centro de Ciberseguridad Industrial de Gipuzkoa - ZIUR (2020): *https://www.ziur.eus/es/*

Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) (2020): *http://www.cnpic.es/*

Centro Vasco de Ciberseguridad (2020): *Libro Blanco Ciberseguridad Euskadi*. 2ª Edición. *https://www.basquecybersecurity.eus/es/actualidad-bcsc/segunda-edicion-libro-blanco-ciberseguridad-euskadi.html*

Comisión Europea (2010): *Europa 2020: la estrategia de la Unión Europea para el crecimiento y la ocupación. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=LEGISSUM:em0028&from=ES*

— (2015): *Agenda Europea de Seguridad (2015-2020). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52015DC0185&from=GA*

*https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3A230801_2*

— (2016): *La Directiva sobre seguridad de redes y sistemas de información (Directiva NIS). https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive*

— (2020a): *La seguridad cibernética. Dar forma al futuro digital de Europa. https://ec.europa.eu/digital-single-market/en/cyber-security*

— (2020b): *Implementación de la Directiva NIS en España. https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-spain*

— (2020c): *Protección de datos-Normas sobre protección de datos personales dentro y fuera de la UE. https://ec.europa.eu/info/law/law-topic/data-protection_es*

*https://eur-lex.europa.eu/eli/reg/2016/679/*

— (2020d): Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la Estrategia de la UE para una Unión de la Seguridad. Disponible en: *https://eur-lex.europa.eu/legal-con-*

*tent/ES/TXT/PDF/?uri=CELEX:52020DC0605&from=EN*

Comunicado de prensa: Estrategia de la UE para una Unión de la Seguridad: integrar las medidas individuales en un nuevo ecosistema de seguridad. Disponible en *:https://ec.europa.eu/commission/presscorner/detail/es/ip_20_1379*

Consejo Nacional de Seguridad (2019): Estrategia Nacional de Seguridad. Disponible en: *https://www.boe.es/boe/dias/2019/04/30/pdfs/BOE-A-2019-6347.pdf*

Cybersecurity Ventures (2016): *Cybercrime Damages $6 Trillion By 2021. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/*

Departamento de Seguridad Nacional (DSN) (2020): *https://www.dsn.gob.es/es/sistema-seguridad-nacional/departamento-seguridad-nacional*

Europol (2020): *Computer Emergency Response Team for the EU institutions, agencies and bodies (CERT-EU). https://www.europol.europa.eu/organisations/computer-emergency-response-team-for-eu-institutions-agencies-and-bodies-cert-eu*

forrester (2020a): *Top Recommendations For Your Security Program, 2020. https://www.forrester.com/report/Top+Recommendations+For+Your+Security+Program+2020/-/E-RES159378#*

— (2020b): *The S&R Practice Playbook For 2020. https://www.forrester.com/playbook/The+S-R+Practice+Playbook+For+2020/-/E-PLA113*

Gartner (2020a): Rethink the Security & Risk Strategy. *https://www.gartner.com/en/publications/rethink-security-risk-strategy-ebook-pd.html?utm_source=google&utm_medium=cpc&utm_campaign=RM_EMEA_2020_ITTRND_CPC_LG1_H2-GTS-AOC&utm_adgroup=113671253711&utm_term=%2Bgartner%20%2Bcyber%20%2Bsecurity&ad=471122732556&gclid=Cj0KCQjw2or8BRCNARIsAC_ppyZnG-bxxqHORzriixMdxolK-C79EJnT9hRXXdUX-T0B05y652UJy6oQaAuLAEALw_wcB*

— (2020b): *The Urgency to Treat Cybersecurity as a Business Decision. https://www.gartner.com/en/documents/3980891/the-urgency-to-treat-cybersecurity-as-a-business-decisio*

Gobierno Vasco (2014a): *RIS3-Prioridades estratégicas de especialización inteligente de Euskadi. https://www.irekia.euskadi.eus/uploads/attachments/4633/prioridades_estrategicas201404_ris3_gobierno_vasco.pdf?1400573225*

— (2014b): *Plan de Ciencia Tecnología e Innovación Euskadi PCTI 2020. https://www.euskadi.eus/contenidos/enlace/pcti2020_resumen/es_def/adjuntos/pcti_resumen_es.pdf*

— (2016): *Agenda Digital Vasca 2020. https://www.euskadi.eus/contenidos/plan_departamental/14_plandep_xileg/es_def/adjuntos/Agenda%20Digital%20de%20Euskadi%202020%20-%20Anexo%202017.pdf*

— (2017): *Irekia. https://www.irekia.euskadi.eus/es/news/37557-euskadi-formara-parte-nueva-asociacion-vanguard-initiative-que-agrupa-regiones-europeas-consejo-gobierno-2017*

Infosecinstitute (2016): *Evolution in the World of Cyber Crime.*
*https://resources.infosecinstitute.com/evolution-in-the-world-of-cyber-crime/*

Instituto Nacional de Ciberseguridad (INCIBE) (2020): *https://www.incibe.es/*

Organización Europea de Seguridad Cibernética (ECSO) (2020): *https://ecs-org.eu/*

World Economic Forum (WEF) (2020a): *The Global Risks Report 2020. https://www.weforum.org/reports/the-global-risks-report-2020*

— (2020b): *Dar forma al futuro de la ciberseguridad y la confianza digital https://www.weforum.org/platforms/shaping-the-future-of-cybersecurity-and-digital-trust*