LOS CIBERATAQUES A INFRAESTRUCTURAS CRÍTICAS EN ESPAÑA

JOSÉ RAMÓN CORROCHANO PONTE

ANALISTA DE INTELIGENCIA

Fecha de recepción: 16/05/2022. Fecha de aceptación: 17/11/2022

RESUMEN

El aumento de la cibercriminalidad en todo el mundo ha experimentado un crecimiento espectacular en los últimos cinco años, y especialmente al conjunto de instalaciones cuya anulación de servicio o destrucción perjudicaría seriamente el funcionamiento del Estado o sus Administraciones Públicas o, como se conocen comúnmente, las infraestructuras críticas.

La arquitectura del sistema de ciberprotección de estos emplazamientos vitales se establece en los diversos planes (europeos, nacionales y sectoriales) y mediante la vigilancia proporcionada principalmente por cuatro entidades públicas: Centro Nacional de Protección de Infraestructuras Criticas (CNPIC), Centro Criptológico Nacional (CCN), Instituto Nacional de Ciberseguridad de España (INCIBE) y el Mando Conjunto del Ciberespacio (MCCE).

Palabras clave: ciberseguridad, infraestructuras críticas, sistemas, 5G.

ABSTRACT

The increase in cybercrime around the world has experienced a spectacular growth in the last five years, and especially to the set of facilities whose cancellation of service or destruction would seriously impair the functioning of the State or its Public Administrations or, as they are commonly known, critical infrastructures.

The architecture of the cyber protection system for these vital sites establishes in the various plans (European, national and sectoral) and through surveillance provided mainly by four public entities: National Center for the Protection of Critical Infrastructures (CNPIC), National Cryptological Center (CCN), National Institute of Cybersecurity of Spain (INCIBE) and the Joint Cyberspace Command (MCCE).

Keywords: cibersecurity, critical infrastructures, systems, 5G.

1. INTRODUCCIÓN

El pasado año 2021 se produjeron numerosos ciberataques por todo el mundo que han puesto en jaque a gobiernos y corporaciones multinacionales, tres de los más importantes han sido los de Solarwinds, el oleoducto Colonial y la vulnerabilidad Log4J.

En el mes de enero la empresa SolarWinds hizo público que, a través de una vulnerabilidad denominada `Sunburst´ o `Solorigate´, una puerta trasera que comprometió su herramienta `Orion´ y a todas las empresas que lo utilizan, unas 18.000 de todo el mundo (entre ellas Microsoft o Cisco) y 40 entidades públicas de gran importancia (como la NSA) se vieron afectadas. Fuera de Estados Unidos afectó a otros seis países: Bélgica, Canadá, España, Israel, México y Reino Unido[1].

En mayo, EE.UU. declara el estado de emergencia (en varios Estados) tras un ciberataque a la mayor red de oleoductos del país, la de la compañía Oleoducto Colonial[2], que transporta más de 2,5 millones de barriles por día, el 45% del suministro de diésel, gasolina y combustible de los aviones de la costa este. Un grupo de delincuentes informáticos (DarkSide) consiguió desconectar su sistema por completo, robando más de 100 GB de su información.

El pasado 9 de diciembre se descubrió una brecha en el código fuente de Java, conocida como Log4J, provocando una de las mayores crisis en materia de ciberseguridad del año. En palabras de Jen Easterly, directora de la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos, “esta vulnerabilidad es la más grave que he visto en todos mis años de carrera”[3].

Mediante la introducción de cadenas de código manipuladas sobre el componente Log4J, se comprometió la seguridad de aquellas herramientas que emplean este `software´, uno de los más utilizados en el mundo desde mediados de los años 90 y actualmente en los servicios de almacenamiento de la nube de algunas de las mayores empresas tecnológicas del mundo como Amazon, Google, IBM, Microsoft, Oracle o Salesforce[4].

Por último, otro de los mayores problemas en el ámbito de la ciberseguridad internacional ha sido el aumento del `ciberespionaje´ entre países y que tiene como principales objetivos de sus ataques a las Administraciones Públicas y las empresas de sectores estratégicos (aquellas con un importante número de patentes y elementos de propiedad intelectual o las industrias aeronáuticas, de defensa, energéticas, de I+D+I, etc).

En lo que respecta a España, desde 2020, quizá enmascarado por la preocupación de la pandemia, se ha producido un aumento muy considerable de los ciberataques, un 125% en el último año llegando a los 40.000 diarios, lo que nos convierte en el 3º país de Europa más atacado.

1 Bécares, B. “El ataque a SolarWinds, explicado: por qué un ataque a esta empresa desconocida trae de cabeza a grandes corporaciones y gobiernos del mundo”. Xataca. https://www.xataka.com/pro/ataque-a-solarwinds-explicado-que-ataque-a-esta-empresa-desconocida-trae-cabeza-a-grandes-corporaciones-gobiernos-mundo Fecha de consulta 19.12.2021.

2 Redacción. EE.UU. declara estado de emergencia tras un ciberataque a la mayor red de oleoductos del país. BBC Mundo https://www.bbc.com/mundo/noticias-internacional-57033536 Fecha de consulta 19.12.2021

3 Herrero, J. ¿Qué es log4j? ¿Por qué es la mayor vulnerabilidad informática de todos los tiempos? La Razón. https://www.larazon.es/tecnologia/20211221/r2t4i7flt5hy3dqm5o4nfyusvy.html Fecha de consulta: 19.12.2021.

4 Mallo, O. y Rabal, J. Log4j foto completa: Todas las vulnerabilidades de Log4Shel. Tarlogic https://www.tarlogic.com/es/blog/log4j-foto-completa-vulnerabilidades-log4shell/ Fecha de consulta 20.12.2021.

Nuestro país sufre a diario numerosos y sofisticados ciberataques de diversos sectores: denegación de servicio, espionaje industrial, phishing, etc., que en los últimos meses han afectado a las páginas webs de diversos Ministerios (Educación y Cultura, de Justicia, de Asuntos Económicos y Transformación Digital) y a instituciones públicas (Consejo de Seguridad Nuclear, Instituto Nacional de Estadística, la Red Sara, el SEPE, etc). Por esto, aunque es uno de los países con mayor fortaleza contra ciberataques, todavía tiene muchos aspectos que mejorar, como se recoge en el informede la consultora Deloitte "El estado de la ciberseguridad en España"[5].

2. LAS INFRAESTRUCTURAS CRÍTICAS: UN ELEMENTO VITAL PARA EL ESTADO

En la configuración de la Seguridad Nacional un elemento central son las infraestructuras críticas, que, según lo establecido en la Directiva europea sobre la identificación y regulación de infraestructuras críticas a nivel comunitario, la Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008, se pueden definir como "el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones".

En el ámbito comunitario, una infraestructura crítica europea (o ICE) es aquella "situada en los Estados miembro cuya perturbación, o destrucción afectaría gravemente al menos a dos Estados miembro. La magnitud de la incidencia se valorará en función de criterios horizontales, como los efectos de las dependencias intersectoriales en otros tipos de infraestructuras".

Por otra parte, en nuestro ordenamiento jurídico, se recogen, en primer lugar, en el Plan Nacional de Protección de Infraestructuras Críticas, que las establece como "aquellas instalaciones, redes, servicios y equipos de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad, el bienestar de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas".

El Real Decreto Ley 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas, que establece el Catálogo Nacional de Infraestructuras Estratégicas, "el registro de carácter administrativo que contiene información completa, actualizada y contrastada de todas las infraestructuras estratégicas ubicadas en el territorio nacional, incluyendo las críticas, así como aquellas clasificadas como críticas europeas que afecten a España, con arreglo a la Directiva 2008/114/CE".

Este catálogo tiene como principal finalidad "valorar y gestionar los datos disponibles de las diferentes infraestructuras, con el objetivo de diseñar los mecanismos de planificación, prevención, protección y reacción ante una eventual amenaza contra aquellas y, en caso de ser necesario, activar, conforme a lo previsto por el Plan Nacional de Protección de las Infraestructuras Críticas, una respuesta ágil, oportuna y proporcionada, de acuerdo con el nivel y características de la amenaza de que se trate".

5 Delloite. "El estado dela ciberseguridad en España" https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html Fecha de consulta 20.21.2021.

Todas estas instalaciones en nuestro país no son de conocimiento público debido a razones de seguridad nacional, aunque, sí que se pueden agrupar en torno a 12 sectores estratégicos[6]:

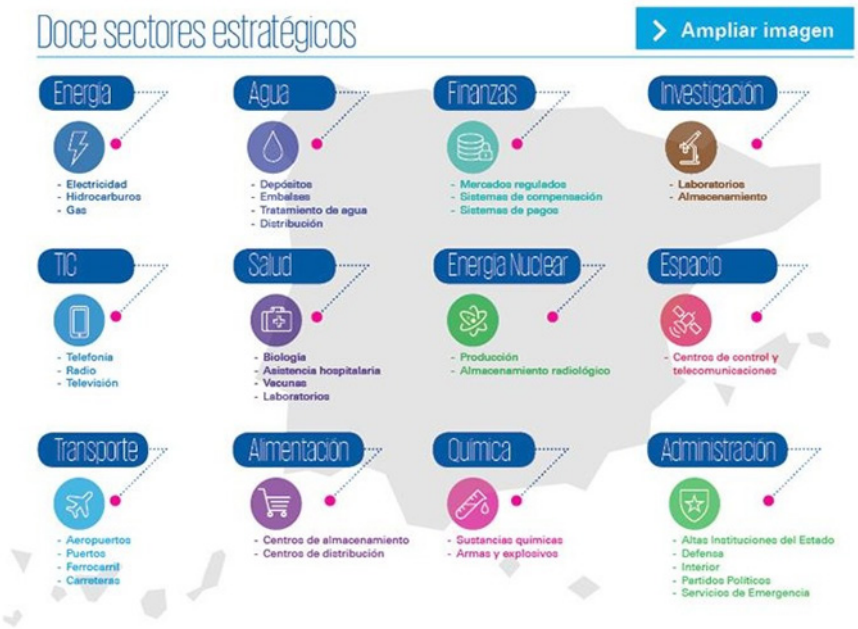

Figura 1: 12 sectores estratégicos de las infraestructuras críticas. Fuente: KPMG.

1. **Las centrales y redes de energía:** presta especial atención a la producción y distribución de todo tipo de energía, sobre todo la eléctrica.
2. **El almacenamiento, tratamiento y distribución de agua.**
3. **El sistema financiero y tributario:** focalizado en las entidades bancarias, los valores y la información en inversiones.
4. **La investigación:** se centra en los laboratorios que produzcan materiales, sustancias o elementos peligrosos.
5. **Tecnologías de la Información y las Comunicaciones (TIC):** hace referencia a las redes de telecomunicaciones e Internet.
6. **El sector sanitario:** la infraestructura sanitaria (ambulatorios y hospitales).
7. **Las centrales nucleares** pueden ser un objetivo principal por la producción, almacenamiento y transporte de materiales nucleares o radiológicos.
8. **El sector aeroespacial** y sus instalaciones.
9. **La red de transporte:** aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico.
10. **La cadena de suministros:** especialmente la producción, distribución y almacenamiento de los alimentos.

6 Calle, C. “Las empresas están muy concienciadas con la ciberseguridad; lo ven como una inversión a medio-largo plazo”. KPMG Tendencias. https://www.tendencias.kpmg.es/2018/05/entrevista-director-cnpic-ciberseguridad-infraestructuras-criticas/ Fecha de consulta 19.12.2021

11. **La industria química:** por la producción, almacenamiento y transporte de mercancías peligrosas.
12. **La Administración Pública:** por la prestación de servicios básicos, las redes de información o sus instalaciones.

Todos estos sectores poseen instalaciones que se pueden ver afectadas por 8 principales amenazas, internas o externas, físicas o cibernéticas, que entre otras son las que se recogen en la siguiente imagen.

Figura 2: Amenazas y vulnerabilidades de las infraestructuras críticas. Fuente: Lisa Institute.

La Protección de las Infraestructuras Críticas frente a las eventuales amenazas que puedan producirse requiere la configuración y ejecución de los siguientes planes de actuación:

- El Plan Nacional de Protección de las Infraestructuras Críticas.
- Los Planes Estratégicos Sectoriales.
- Los Planes de Seguridad del Operador.
- Los Planes de Protección Específicos.
- Los Planes de Apoyo Operativo.

3. LOS ORGANISMOS PÚBLICOS DE DEFENSA CONTRA LAS CIBERAMENAZAS

En España existe un conjunto de organismos públicos proveedores de servicios de ciberseguridad que protegen a los principales órganos del Estado y las Administraciones Públicas.

De todas las que conforman esta imagen, en el caso de las infraestructuras críticas, las entidades más relevantes en la configuración de su ciberseguridad son 5: Centro Nacional de Protección de Infraestructuras Criticas (CNPIC), el Centro Criptológico Nacional (CCN), el Centro de Operaciones de Ciberseguridad (SOC-AGE), el Instituto Nacional de Ciberseguridad (INCIBE), para el ámbito militar, el Mando Conjunto de Ciberdefensa (MCCD) y la Oficina de Coordinación de Ciberseguridad (OCC).

3.1. CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS (CNPIC)

Este organismo se crea en 2007, para cumplir con la Comunicación de la Comisión Europea de 20 de octubre de 2004 sobre protección de las infraestructuras críticas, que contiene propuestas para mejorar la prevención, preparación y respuesta de la UE frente a los atentados terroristas que se produzcan.

Depende de la Secretaría de Estado de Seguridad y entre sus principales funciones destacan la actualización y supervisión del Plan de Seguridad de Infraestructuras Críticas y el Catálogo Nacional de Infraestructuras Críticas.

Dentro de su organigrama, hay que resaltar tres servicios principales:

Figura 3: Estructura del CNPIC. Fuente: CNPIC.

- Servicio de Planes y Seguridad: su principal misión es desarrollar el Esquema de Planificación de IC (PIC). Además, se encarga de la gestión, organización y supervisión del Catálogo Nacional de Infraestructuras Estratégicas y de la actualización de sus bases de datos.
- Servicio de Ciberseguridad: busca compaginar todas las actuaciones de lucha contra la cibercriminalidad de la Secretaría de Estado de Seguridad, sobre todo aquellas relacionadas con las infraestructuras y servicios esenciales, tanto a nivel nacional como internacional.
- Servicio de Normativa y Coordinación: de entre sus tareas destacan varias de apoyo a las secciones anteriores en el ámbito jurídico; la recopilación, tratamiento y difusión de información; el impulso a la I+D+I; y las relaciones y coordinación con otros agentes, nacionales e internacionales.

3.2. CENTRO CRIPTOLÓGICO NACIONAL (CCN)

El Centro Criptológico Nacional es el organismo responsable de coordinar la acción de los diferentes organismos de la Administración, garantizar la seguridad de las

Tecnologías de la Información, informar sobre la adquisición del material criptológico y formar a los empleados públicos especialistas en este campo.

Fue creado en el año 2004, a través del Real Decreto 421/2004, que lo adscribe al Centro Nacional de Inteligencia (CNI), con el que comparte normativa legal, protocolos y procedimientos, así como recursos físicos y económicos; ya que, según se establece en la Ley 11/2002, de 6 de mayo, reguladora del CNI, al CCN se le conceden las tareas relativas a la seguridad de las Tecnologías de la Información y de protección de la información clasificada pertenecientes al principal servicio de inteligencia nacional.

El Centro Criptológico Nacional es el organismo responsable de dar respuesta a los incidentes que se produzcan en esta materia, y a las necesidades planteadas en el Real Decreto 421/2004, de 12 de marzo, por el que se le asignan las siguientes funciones:

- **Certificación,** establecer el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad.
- **Ciberseguridad,** contribuir a elevar el nivel de la ciberseguridad española afrontando de forma activa las amenazas que afecten a sistemas del Sector Público, a empresas y organizaciones de interés estratégico para el país, en coordinación con el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC).
- **Desarrollo,** coordinar la adquisición, desarrollo y uso de TICs.
- **Evaluación,** valorar y acreditar la capacidad de cifrado de productos y sistemas de manejo de información de forma segura.
- **Formación,** para el personal del Sector Público especialista en este ámbito.
- **Normativa,** elaborar y difundir normas, instrucciones y guías para garantizar la seguridad de los sistemas TIC (Guías CCN-STIC).
- **Relaciones,** establecer las necesarias relaciones y firmar los acuerdos pertinentes con organizaciones similares de otros países.
- **Vigilar,** velar por el cumplimiento de la normativa de protección de la información clasificada.

El CCN colabora con todos los organismos públicos y empresas de interés estratégico para el país en la detección, evaluación, notificación, respuesta y tratamiento de incidentes de seguridad de información que puedan sufrir sus sistemas. Actúa también como Nodo de Intercambio de Información de incidentes en los Sistemas de las Administraciones Públicas y como principal coordinador con los organismos adecuados del intercambio de información.

3.3. CENTRO DE OPERACIONES DE CIBERSEGURIDAD DE LA AGE (SOC)

Es el organismo más moderno, puesto en marcha en Real Decreto 63/2018, del 13 de julio. Su objetivo es “reforzar las capacidades de vigilancia, prevención, protección, detección y respuesta ante ciberincidentes. Y también las relativas al asesoramiento

y apoyo a la gestión de la ciberseguridad de un modo centralizado"[7]. Dependerá de la Secretaría General de Administración Digital (SGAD) adscrita al Ministerio de Hacienda y Función Pública.

La puesta en marcha de esta entidad se debe a dos hechos principales: que ya estaba previsto en la Estrategia Nacional de Ciberseguridad 2019, y que su inversión económica, 960 millones de euros, se establece en el reciente Plan de Recuperación, Transformación y Resiliencia[8].

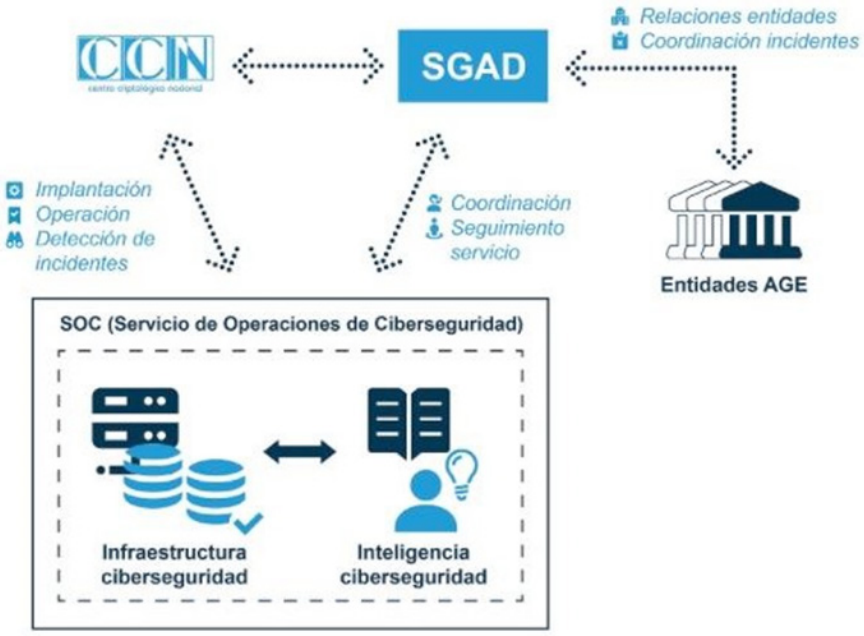

Figura 4: funcionamiento del SOC de la AGE. Fuente: CCN.

3.4. FORO NACIONAL DE CIBERSEGURIDAD

El Foro Nacional de Ciberseguridad (FNC) es una entidad público – privada (que depende orgánicamente del Consejo Nacional de Ciberseguridad) que se creó el 22 de julio 2020 y que tiene como principales objetivos: "fomentar la cultura de ciberseguridad en nuestro país, ofrecer apoyo a la Industria e I+D+i y promover la formación y el talento". Se define como "un órgano de asistencia al Consejo Nacional de Ciberseguridad Nacional en su condición de órgano de apoyo del Consejo de Seguridad Nacional"[9].

Su meta es "articular y cohesionar un entorno de colaboración público-privada que, a través de diferentes líneas de acción, genere el máximo conocimiento sobre los

7 Real Decreto 863/2018, de 13 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Política Territorial y Función Pública. https://www.boe.es/buscar/doc.php?id=BOE-A-2018-9858 Fecha de consulta: 18.12.2021.

8 Plan de Recuperación, Transformación y Resiliencia (página 39) https://www.lamoncloa.gob.es/temas/fondos-recuperacion/Documents/05052021- Componente11.pdf Fecha de consulta: 20.12.2021.

9 Redacción. "El Foro Nacional de Ciberseguridad presenta los primeros resultados de sus grupos de trabajo". Red Seguridad. Extraído de: https://www.redseguridad.com/actualidad/organismos-ciberseguridad/el-foro-nacional-de-ciberseguridad-presenta-presenta-los-primeros-resultados-de-sus-grupos-de-trabajo_20220222.html Fecha de consulta: 25.03.2022.

desafíos a la Seguridad Nacional en el ciberespacio, ya sean oportunidades o amenazas, y en colaboración con el CNC". El FNC está formado por varios organismos diferentes:

1. Presidencia: La presidencia será ejercida por el vicepresidente del Consejo Nacional de Ciberseguridad y director del Departamento de Seguridad Nacional (actualmente Miguel Ángel Ballesteros). Al menos una vez al año, y cuando se considere oportuno, el presidente del Consejo Nacional de Ciberseguridad presidirá la reunión del Foro.
2. Vicepresidencias:
   - Primera; será ejercida por el director del Instituto Nacional de Ciberseguridad.
   - Segunda; será ejercida por el subdirector del Centro Criptológico Nacional.
3. Secretaría: desempeñada por el Departamento de Seguridad Nacional.

   El secretario será designado por el presidente del Foro y asumirá funciones propias y de apoyo al presidente del Foro.
4. Vocalías Permanentes: formada por un representante de cada uno de los miembros de la Comisión Permanente de Ciberseguridad.
5. Vocalías: en la que participan los vocales representantes de cada organización.

El FNC se reunirá mínimo 2 veces al año, a iniciativa del presidente, cuando sea necesario por las incidencias que puedan afectar a la ciberprotección de las Administraciones Públicas y las infraestructuras críticas de España.

Figura 5: Composición del Foro Nacional de Ciberseguridad. Fuente: FNC.

En la estructura y organización del FNC también es importante la actividad de los Grupos de Trabajo, cuyo objetivo es fomentar la cultura de ciberseguridad en la sociedad española y, por ello, se encargan de impulsar el I+D+I en ciberseguridad, desarrollar la capacitación, formación y talento, contribuir a establecer la legislación en esta materia y analizar la industria de ciberdefensa.

Figura 6: Grupos de Trabajo. Fuente: Foro Nacional de Ciberseguridad.

Las tareas del Foro Nacional de Ciberseguridad son, entre otras:

- Proponer iniciativas al Consejo Nacional de Ciberseguridad para la creación de sinergias público-privadas (y su potenciación) en materia de ciberseguridad o ciberdefensa.
- Analizar y estudiar propuestas que permitan apoyar la toma de decisiones del Consejo Nacional de Ciberseguridad.
- Contribuir a la valoración y análisis de los riesgos y amenazas en materia de ciberseguridad, y la propuesta de acciones de mitigación y respuesta.
- Apoyar la realización y evaluación de ejercicios de gestión de crisis en el ámbito de la ciberseguridad y la ciberdefensa.
- Contribuir a la identificación de las necesidades de la industria y de los centros de investigación, en lo que se refiere a ciberseguridad.
- Impulsar la realización proactiva de estudios e informes sobre tecnologías nuevas y emergentes y analizar su impacto en la ciberseguridad nacional, a la vez que, de forma reactiva, realizarlo a petición del CNC.
- Idear iniciativas tendentes a promover la cultura Nacional de Ciberseguridad.
- Apoyar la proyección y participación de España a nivel internacional y europeo en materia de ciberseguridad y ciberdefensa.

3.5. INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA (INCIBE)

Otra de los organismos públicos más importantes en la “arquitectura” de nuestra ciberseguridad nacional es el Instituto de Ciberseguridad de España o INCIBE. Es una sociedad mercantil estatal creada en 2006, ubicada en León, y que tiene como finalidad principal “afianzar la confianza digital, elevar la ciberseguridad y la resiliencia y contribuir al mercado digital de manera que se impulse el uso seguro del ciberespacio en España”.

El Instituto Nacional de Ciberseguridad de España (INCIBE) es una entidad dependiente del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial. Se ha establecido como una de las principales entidades de referencia para el desarrollo de la ciberseguridad nacional y de concienciación a ciudadanos, empresas y profesionales, especialmente para sectores estratégicos.

La meta del INCIBE es contribuir al mercado digital de manera que se impulse el uso seguro del ciberespacio en España, a través de la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, contribuyendo a elevar nuestro estándar de ciberseguridad. Como centro de excelencia, INCIBE es un centro de excelencia de esta materia de la Administración pública para desarrollar la innovación y la transformación social.

Por todo ello, las misiones principales del INCIBE son:

- Proteger y defender a los ciudadanos y empresas nacionales.
- Impulsar la I+D+I en ciberseguridad para identificar, generar y atraer a los mejores profesionales del sector.

Actualmente entre sus proyectos más importantes destacan los programas “INCIBE Emprende”, la academia hacker, la compra pública innovadora (CPI), el programa `cibercooperante´ o proyectos europeos.

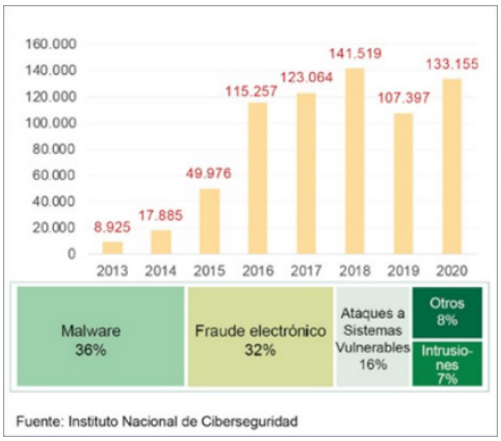

Figura 7: Evolución del número de ciberincidentes y su tipología. Fuente: Informe Anual de Seguridad Nacional 2020 (pág. 131).

El Gobierno, a través de la Agenda Digital 2025, ha establecido que el INCIBE será la piedra angular del desarrollo de este plan general de ciberseguridad; y por

ello en el Plan de Resiliencia[10] ya está programado que este organismo recibirá 183 millones de fondos europeos para impulsar a nuestro país como "nodo internacional de ciberseguridad".

3.6. MANDO CONJUNTO DEL CIBERESPACIO (MCCE)

En el ámbito militar, el órgano competente para coordinar y dirigir las actuaciones de nuestras Fuerzas Armadas en el ciberespacio es el Mando Conjunto de Ciberdefensa, dependiente del Estado Mayor de la Defensa (EMAD) y tiene como misión principal "el diseño y la ejecución de las actuaciones relativas a la ciberdefensa militar en las redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas, para contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que afecten a la Defensa Nacional".

El MCCE es el órgano responsable de la dirección, la coordinación, el control y la ejecución de las acciones conducentes a asegurar la libertad de acción de las Fuerzas Armadas en el ámbito ciberespacial.

Actualmente cuenta con 230 efectivos militares y 50 civiles pero, para poder disponer de la capacidad suficiente para los retos inminentes en ciberdefensa, este personal debería duplicarse en los próximos cinco años[11].

En el marco de la operación "Misión Baluarte" (mediante la cual las Fuerzas Armadas realizaron el rastreo de los contagiados), debido a los numerosos ciberataques contra localizaciones clave en la lucha contra la pandemia de la COVID-19 como los hospitales; el Mando Conjunto de Ciberespacio (MCCE), configuró al Ciberespacio como el quinto ámbito operativo militar.

La vital actuación de estas unidades podría suponer la creación de un cuerpo propio, una revolución en la estructura de las FAS, lo que permitiría contar con un equipo permanente especializado en la ciberdefensa para hacer frente a futuras amenazas.

La posible creación de otro cuerpo o un 4º Ejército se podría justificar sobre una serie de características especiales que posee este ámbito: no tiene un dominio territorial, un sistema dinámico y cambiante, la capacidad de producir ataques sorpresa y amenazas contras las infraestructuras críticas de la nación. De esta manera se evitaría la rotación de personal entre las diferentes organizaciones públicas de ciberdefensa, aunque los ascensos y cambios de puestos se realizarían a través de un escalafón militar[12].

10 Plan de Recuperación, Transformación y Resiliencia (página 43). https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/plan_de_recuperacion. pdf. Fecha de consulta: 20.12.2021.

11 Garrido, P. (05.11.2021). "Defensa estudia crear un cuerpo propio de militares expertos en ciberdefensa". El Confidencial Digital.https://www.elconfidencialdigital.com/articulo/defensa/defensa-estudia-crear-cuerpo-propio-militares-expertos-ciberdefensa/20211104170230299787.html

12 Senovilla, M. "El Mando Conjunto del Ciberespacio ha contenido más de 600 ataques peligrosos para la defensa de España en el último año". El Confidencial Digital. Extraído de: https://atalayar.com/content/el-mando-conjunto-del-ciberespacio-ha-contenido-m%C3%A1s-de-600-ataques-peligrosos-para-la

3.7. OFICINA DE COORDINACIÓN DE CIBERSEGURIDAD (OCC)

Creada en 2014, es el órgano técnico de coordinación de la Secretaría de Estado de Seguridad en materia de ciberseguridad. La OCC proporciona servicios técnicos de apoyo a las Fuerzas y Cuerpos de Seguridad del Estado, en concreto a la Guardia Civil y la Policía Nacional, para desarrollar las competencias propias del Ministerio del Interior en el ámbito de la ciberseguridad[13].

Entre las funciones del OCC destacan las tres siguientes:

- Asesorar a la Secretaría de Estado de Seguridad en temas de ciberseguridad, para la mejor toma de decisiones.
- Ser un medio de alerta temprana permanente en lo que respecta a las ciberamenazas, ciberataques y vulnerabilidades del Estado.
- Establecer cauces de intercambio de estrategias de actuación e información entre los diversos actores, públicos y privados, nacionales e internacionales.

4. EL PLAN NACIONAL DE CIBERSEGURIDAD Y EL PROBLEMA DE LAS REDES 5G

Para coordinar la actuación de todas las entidades y organismos protectores el Gobierno ha aprobado por Real Decreto un Plan Nacional de Ciberseguridad, con más de 130 iniciativas en la materia y con el respaldo de 1.000 millones de euros de financiación. Además, se ha acompañado con el Real Decreto 7/2022 en el que se establecen los requisitos de seguridad para implantar las redes 5G en todo el país.

Con esta normativa se busca desarrollar un entorno confiable para el despliegue de estas redes y servicios, generando la confianza necesaria entre los usuarios respecto a su funcionamiento y protección ante potenciales fugas o manipulaciones de datos.

El objetivo de esta normativa es intensificar la vigilancia y apuntalar las capacidades de planificación, preparación, detección y respuesta en el ciberespacio. Se dividió en cinco puntos: ayuda a los trabajadores, defensa del tejido económico y empresarial, medidas para el transporte, ciberseguridad y materia energética. También se prevé incrementar el número de infraestructuras de ciberseguridad en las comunidades autónomas, así como en las entidades locales, para impulsar la ciberseguridad de las pequeñas y medianas empresas (pymes) y autónomos, además de promover un mayor nivel de cultura de ciberseguridad[14].

Con este plan se quiere aumentar la seguridad de las infraestructuras críticas de los principales sectores del país (transporte, energía, agua, atención médica e instalaciones públicas) ya que, según un estudio de la consultora Gartner, en 2025 el 30%

13 Redacción. “La Oficina de Coordinación de Ciberseguridad”. Intelpage.info. Extraído de: https://intelpage.info/oficina-de-coordinacion-cibernetica-occ.html

14 Leal, J. “Los hackers frenan el plan de seguridad del Gobierno: `Combatirlos es inviable´”. La Información. Extraído de: https://www.lainformacion.com/economia-negocios-y-finanzas/los-hackers-frenan-el-plan-de-seguridad-de-sanchez-combatirlos-es-inviable/2863686/

de las organizaciones de infraestructuras críticas será víctima de una brecha de seguridad que detendrá sus operaciones[15].

La principal amenaza para España en el entorno digital, y quien desarrolla la mayoría de los intentos de agresión contra infraestructuras críticas, son otros Estados y los grupos de cibercriminales patrocinados por ellos.

El objetivo final de estos hackeos es robar información: "es una evolución del espionaje tradicional y puede tener un fondo político, como perseguir una mejora de su posición estratégica o de cara a una negociación; o bien económica, como el robo de información industrial o sobre un avance científico"[16].

Todos los organismos de ciberprotección y el plan Nacional de Ciberseguridad trabajan para evitar el ciberespionaje estatal, y por ello deben centrar una parte importante de sus esfuerzos en uno de los grandes puntos débiles: la red 5G. Su despliegue puede convertirse en una nueva "oportunidad" para la ciberdelincuencia, debido principalmente al incremento exponencial de la conexión de dispositivos.

A medida que aumenta la conectividad se añaden capas de seguridad y cifrado, pero también la interconexión y la inseguridad, ya que todos los dispositivos electrónicos que están actuando de forma conjunta podrían no estar protegidos de forma adecuada.

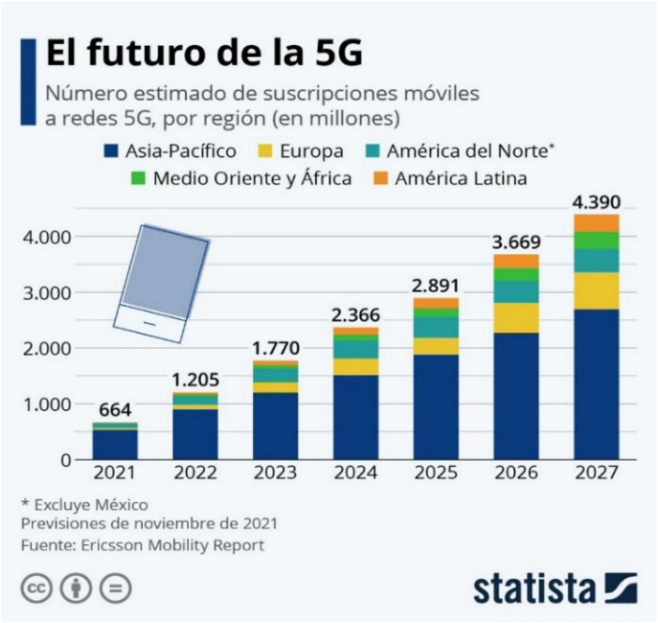

Figura 8: "El futuro de las redes 5G". Fuente: Statista.

La red 5G (o quinta generación de redes móvil) permitirá una conexión muy superior a la 4G en dos aspectos clave: la rapidez y la segmentación. En el primer caso, debido

15 Redacción. "El 30% de las organizaciones de infraestructuras críticas sufrirán brechas de seguridad a medio plazo". Digital Security. Extraído de: https://www.itdigitalsecurity.es/infraestructuras-criticas/2021/12/el-30-de-las-organizaciones-de-infraestructuras-criticas-sufriran-brechas-de-seguridad-a-medio-plazo

16 Del Castillo, C. "El CNI avisa: `Todos los ataques a infraestructuras críticas han venido de otros Estados, nunca de ciberterroristas´". El Diario.es Extraído de: https://www.eldiario.es/tecnologia/cni-ataques-infraestructuras-criticas-ciberterroristas_1_1487140.html

a las ondas de radio de mayor frecuencia, la velocidad de descarga será hasta 10 veces mayor y la latencia se reducirá a un solo milisegundo. En el segundo caso, la segmentación de la red permite que los proveedores dediquen segmentos de sus redes a usos específicos.

Figura 9: "Ciberamenazas de Estados y grupos financiados por ellos". Fuente: El Diario.es.

Diferenciar las redes por segmentos es importantes a la hora de plantear la ciberseguridad nacional, ya que los datos que se usan para el entretenimiento o la comunicación utilizarán un segmento concreto y los datos esenciales, como los que se necesitan para las instalaciones clave o los servicios de emergencia, tendrán un acceso específico y propio que no podrá ser utilizado por el resto de servicios y usuarios.

El 29 de marzo se aprobó el Real Decreto-ley 7/2022 sobre seguridad 5G, la normativa clave que establece los requisitos de seguridad para la instalación, despliegue y explotación de redes y servicios de las redes 5G en todo el territorio nacional. Con esta normativa se pretende establecer una serie de medidas para hacer frente a los riesgos que acechan a esta tecnología.

En esta Ley, tal y como han hecho otros países europeos como Francia o Reino Unido, se otorga un plazo de tres meses al Gobierno para que realice una lista de proveedores de confianza (en la que se contará previsiblemente con las europeas Ericcson y Nokia) y se impedirá a empresas extranjeras no incluidas ser licitadoras de los contratos de extensión de las redes de telecomunicaciones 5G, si se consideran una amenaza a la ciberseguridad nacional (como Huawei): "no podrán utilizar en la red de acceso de una red pública 5G equipos de telecomunicación, sistemas de transmisión, y demás recursos, que permitan el transporte de señales, hardware, software o servicios auxiliares de suministradores de alto riesgo"[17].

17 Del Castillo, C. "España podrá vetar de la red 5G a empresas `vinculadas al gobierno de terceros países´". ElDiario.es. Extraído: https://www.eldiario.es/tecnologia/espana-podra-vetar-red-5g-empresas-vinculadas-gobierno-terceros-paises_1_8873912.html

Este Real Decreto viene a concretar las ideas recogidas en el Plan España Digital 2025 -el documento que busca implantar una agenda actualizada para la Transformación Digital de España-, un proceso que relanzará el crecimiento económico, la reducción de la desigualdad y aumentará la productividad:

- Reforzar la posición de liderazgo de España en su desarrollo y despliegue.
- Desarrollar un entorno confiable para el despliegue de sus servicios.
- Apoyar su despliegue del 5G por parte de los agentes económicos[18].

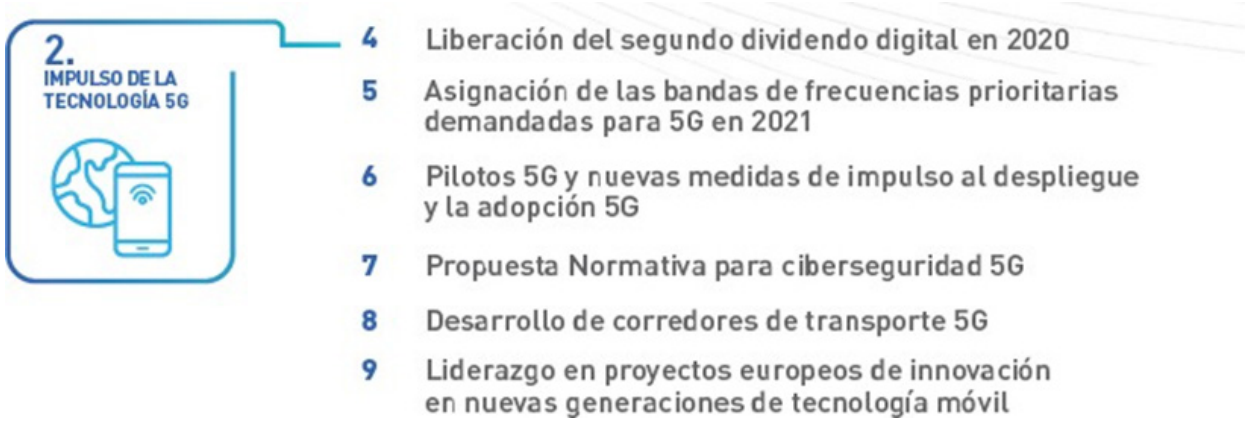

Figura 10: el impulso a la tecnología 5G. Fuente: Plan España Digital (pág. 81).

5. IDEAS PARA MEJORAR LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

España es uno de los países de la OCDE con algunos de los mejores datos en los que a ciberseguridad se refiere, entre ellos, destaca ser:

- El 3º de los países europeos con mayor penetración de fibra óptica para el hogar, solamente por detrás Francia e Italia (según datos del FTTH Council).
- El país europeo en el que más ha crecido el número de profesionales tecnológicos (un 15%) y el 4º en exportador de talento (según el informe `Startup Ecosystem Overview 2019´del Mobile World Capital Barcelona)[19].
- El 7º país más comprometido con la ciberseguridad[20]. Solamente se encuentran por delante EE.UU., Estonia, Francia, Lituania, Reino Unido y Singapur.

18 Plan España Digital 2025. Ministerio de Asuntos Económicos y Transformación Digital. Extraído de: https://portal.mineco.gob.es/RecursosArticulo/mineco/prensa/ficheros/noticias/2018/200723-np_resumen.pdf

19 `Startup Ecosystem Overview 2019´ https://gallery.mailchimp.com/9ab5c7f7f734ede362aeb83f4/files/98132712-c237-4c4c-a984-4b613b3edff5/DIGITAL_STARTUP_ECOSYSTEM_OVERVIEW_5.pdf

20 Global Cybersecurity Index 2020 https://www.itu.int/epublications/publication/global- cybersecurity-index-2020/en/

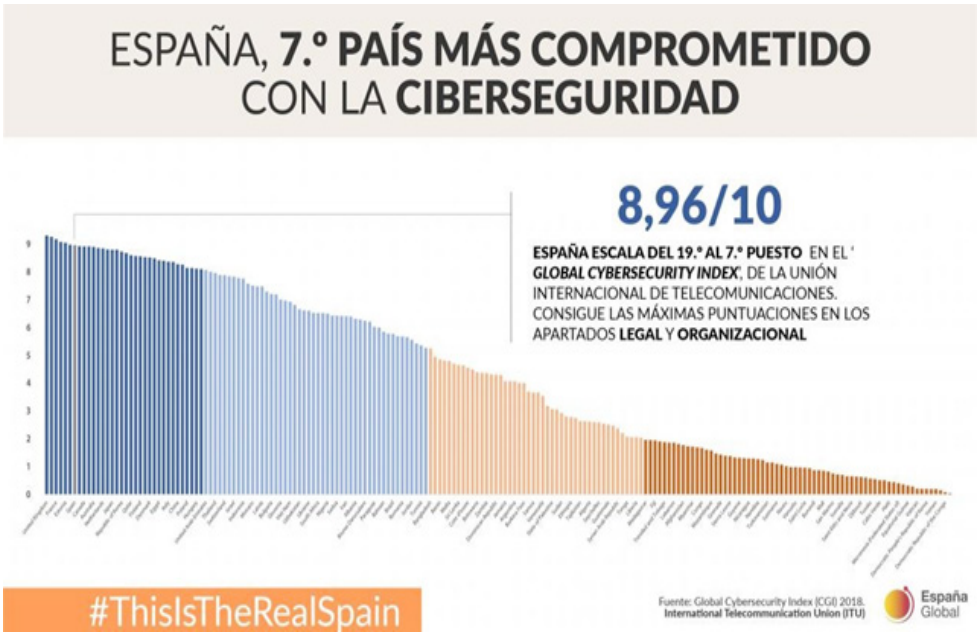

Figura 11: Ranking países comprometidos con la ciberseguridad. Fuente: España Global.

A pesar de estos resultados positivos y la confianza que aporta el conjunto de las organizaciones públicas de ciberdefensa en nuestro país, es necesario resaltar que, a la hora de evaluar la ciberprotección de las infraestructuras críticas, hay varios ámbitos en los que España tiene que mejorar:

1. Formar parte de las asociaciones internacionales en ciberseguridad.

   Nuestro país se ha quedado fuera de la alianza de 32 países para hacer frente a los problemas mundiales en el ámbito de la ciberseguridad[21]. Este foro es liderado por EE.UU. y está formado, entre otros, por: Australia, Brasil, Bulgaria, Canadá, República Checa, República Dominicana, Emiratos Árabes, Estonia, Francia, Alemania, India, Irlanda, Israel, Italia, Japón, Kenia, Lituania, México, Nueva Zelanda, Nigeria, Países Bajos, Polonia, Reino Unido, República de Corea, Rumania, Singapur, Sudáfrica, Suecia, Suiza o Ucrania.

   Este no es el único caso de falta de empuje `ciberdiplomático´ para mejorar la posición de nuestro país en las organizaciones internacionales dedicadas a esta materia. Esta falta de voluntad en nuestra acción exterior perjudicó en diciembre de 2020 la candidatura de León para ser la sede del nuevo Centro Europeo de Ciberseguridad, que recayó en favor de Bucarest (Rumanía)[22].

2. Desarrollar la `ciberreserva´.

   La Estrategia de Ciberseguridad Nacional de 2019 no consiguió uno de sus metas principales: iniciar la creación de una cultura nacional de ciberseguridad, que

21 Alandete, D. “Biden invita a 30 «estrechos aliados» a una cumbre contra los ciberataques y deja fuera a España”. ABC. Extraído de: https://www.abc.es/internacional/abci-espana-queda-fuera-gran-iniciativa-eeuu-contra-ciberataques-202110131114_noticia.html Fecha de consulta: 28.11.2021.

22 Pérez, E. “Un gigante llamado Bucarest: por qué León lo tenía difícil para albergar el Centro Europeo de Ciberseguridad”. Xataka. https://www.xataka.com/seguridad/gigante-llamado- bucarest-que-leon-tenia-dificil-para-albergar-centro-europeo-ciberseguridad Fecha de consulta: 19.12.2021

establezca un debate político sobre aspectos fundamentales en la configuración de la ciberseguridad nacional como una política estatal clave, suponga el impulso de la industria nacional de ciberseguridad, I+D+i, en esta materia, y analice las amenazas y los riesgos de no tenerla, especialmente en lo que atañe a aquellos elementos vitales del Estado y del sector privado.

Para ello es preciso contar con un conjunto de expertos en diversos campos (administrativo, empresarial, legal, militar, político, tecnológico, etc), incluyendo la aportación que pueden realizar la sociedad civil a través de la creación de la ciberreserva, a la que podríamos definir como el conjunto de profesionales del ámbito de la ciberseguridad que, en condición de reservistas de las Fuerzas Armadas, puedan ser activados en situaciones puntuales de cibercrisis que pueda sufrir España.

La ciberreserva solo será posible si, como establece Guillem Colom (experto en estudios militares y director de `Thiber´) en el especial "La necesidad de un programa nacional de ciberreserva"[23], la dotamos de mayor financiación: "sin inversión estaremos abocados a la irrelevancia cibernética, cualquier iniciativa que queramos implementar fracasará y pondremos en riesgo no solo el futuro de la soberanía nacional sino también nuestro futuro como sociedad".

3. Realizar las inversiones necesarias

El último de los grandes retos de España para la correcta configuración de un sistema de ciberprotección de infraestructuras críticas es aumentar la financiación en ciberseguridad. El proyecto de Ley de los Presupuestos Generales del Estado para 2022 muestra la reducción que se ha producido en las partidas destinadas a ciberseguridad, especialmente para el INCIBE, que depende de la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA) del Ministerio de Asuntos Económicos y Transformación Digital, de un 26,4%, desde los 253 millones de este año a los 186 millones que se otorgarán para 2022[24].

A pesar de este revés, el Plan de Recuperación, transformación y resiliencia corrige esta situación, dotando de otros 524 millones de euros extra a dicho organismo, por lo que la inversión real se incrementó un 280%, siendo el montante total de 710 millones de euros.

Para tener al día la ciberseguridad de las infraestucturas críticas no solo necesita de inversión económica para establecer el protocolo de actuación para proteger y realiza una evaluación de riesgos, el blue team, sino también el equipo de hacker ético independiente que actúa como las amenazas que intentan superar controles de seguridad de un sistema, el red team.

En el último Miami Pwn2Own, el concurso de 'hacking' más importante del mundo donde investigadores y profesionales intentan encontrar fallos críticos

23 Colom, G. "La necesidad de un programa nacional de ciber-reserva". Nº 3. Noviembre. Thiber. https://www.thiber.org/wp-content/uploads/2018/11/Numero_03_Noviembre_Comentario.pdf Fecha de consulta: 19.12.2021.

24 Sierra, Marcos. El Gobierno tarda un año en adjudicar 12 millones a contratos de ciberseguridad. Vozpópuli. https://www.vozpopuli.com/economia_y_finanzas/ciberataques-gobierno-ciberseguridad.html Fecha de consulta: 22.11.2021.

en sistemas, dos investigadores de ciberseguridad neerlandeses, Daan Keuper y Thijs Alkemade, han sido capaces de penetrar un sistema como el que se usa para controlar las redes eléctricas, reactores nucleares, sistemas de agua o los gasoductos. A pesar de que cualquier fallo en este tipo de infraestructuras podría desembocar en un desastre que puede afectar a la vida de miles de personas y costar cientos de millones de euros.

Este año los ganadores han sido los investigadores, que se han llevado 90.000 dólares por encontrar un error en la comprobación de aplicaciones confiables del protocolo de comunicaciones OPC UA (Arquitectura Unificada de Comunicaciones de Plataforma Abierta): un ‹lenguaje› que se usa en todo el mundo para que las distintas partes de un proceso industrial puedan hablar entre ellas, sobre todo las que tienen que ver con las máquinas, un componente central de las redes industriales habituales en el que se salta la autenticación que normalmente se requiere para leer o cambiar cualquier cosa[25].

Con la multitud de organismos y entidades que conforman nuestra arquitectura de ciberseguridad nacional, tenemos al CCN-CERT que sí actúa como blue team (ya que “es el centro de alerta y respuesta nacional que coopera y ayuda a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas”), aunque no tenemos uno que actúe como red team y que evalúe de forma externa la ciberprotección de nuestras infraestructuras.

6. CONCLUSIONES

El Ministerio del Interior, a través del CNPIC, envió este mes de mayo pasado varias notificaciones a algunas de las grandes empresas con riesgo sistémico para todo el país (en el sector de la energía, las telecomunicaciones, etc) ante posibles incursiones de ‹hackers›, para advertirles que deben estar en grado de alerta máxima ante incursiones en sus sistemas[26].

Esto se pudo comprobar en el reciente ejercicio de ciberdefensa Locked Shields 2022, en el que España obtuvo el último lugar, de 32 países en el que participaban más de 2.000 expertos[27].

De ambas situaciones debemos extraer la misma conclusión: el sistema de seguridad de las instituciones del Estado y las grandes empresas de nuestro país se encuentran amenazados y no estamos suficientemente protegidos. Para darle la vuelta a la situación debemos realizar un exhaustivo análisis de cómo se ha establecido la arquitectura del organigrama de ciberseguridad de nuestras infraestructuras: cómo se ha estructurado, qué entidades lo forman y su importancia en él, su presupuesto, sus objetivos y fines, etc.

25 Kardoui, O. “Atacar centrales nucleares es mucho más fácil de lo que pensábamos”. El Confidencial. Extraído de: https://www.elconfidencial.com/tecnologia/novaceno/2022-04-26/infraestructuras-clave-presa-facil-ciberdelincuentes_3414070/

26 Pastor. F. “Alerta máxima en las infraestructuras españolas por riesgo de ciberataques”. La Información. Extraído de: https://www.lainformacion.com/empresas/alerta-maxima-en-las-infraestructuras-espanolas-por-riesgo-de-ciberataques/2866557/

27 Cancio. F. “España, última en un ejercicio multinacional de ciberguerra”. La Razón. Extraído de: https://www.larazon.es/espana/20220502/fs5356ec6fav5pcqqzvnwe3wn4.html

En este sentido, también es necesario tener en cuenta algunas nuevas recomendaciones que ya se han hecho, pero que todavía, por distintas razones, no se han implantado: ser miembro de las principales asociaciones internacionales de ciberseguridad (y firmar acuerdos internacionales como el reciente el Protocolo adicional segundo al Convenio del Consejo de Europa sobre la Ciberdelincuencia[28]), dotar a nuestras entidades del imprescindible apoyo económico y de RRHH necesarios, y conseguir asegurar un refuerzo "de apoyo" a todas nuestras organizaciones con los mejores profesionales del sector privado y la sociedad civil (la ciberreserva).

Por último, es importante resaltar que las Administraciones Públicas se han dado cuenta de la necesidad de apostar por impulsar estas políticas; el último ejemplo es el acuerdo que han firmado el pasado 15 de julio la Secretaría de Estado de Digitalización e Inteligencia Artificial y la Secretaría de Estado de Seguridad[29], que actualiza y adapta los compromisos comunes presentes en su convenio de 2015. En él destacan la colaboración, la concienciación la cooperación y la formación para desarrollar acciones informativas y de concienciación dirigidas a organizaciones y ciudadanos.

Ambos organismos promoverán diversas acciones formativas conjuntas para el personal de numerosos organismos (como el INCIBE o las Fuerzas y Cuerpos de Seguridad) y la realización de ciberejercicios en los operadores críticos y de servicios esenciales privados para mejorar más su ciberseguridad.

BIBLIOGRAFÍA

Alandete, D. "Biden invita a 30 `estrechos aliados´ a una cumbre contra los ciberataques y deja fuera a España". ABC. https://www.abc.es/internacional/abci-espana-queda- fuera-gran-iniciativa-eeuu-contra-ciberataques-202110131114_noticia.html Fecha de consulta: 28.11.2021.

Bécares, B. "El ataque a SolarWinds, explicado: por qué un ataque a esta empresa desconocida trae de cabeza a grandes corporaciones y gobiernos del mundo". Xataca. https://www.xataka.com/pro/ataque-a-solarwinds-explicado-que-ataque-a-esta-empresa-desconocida-trae-cabeza-a-grandes-corporaciones-gobiernos-mundo Fecha de consulta: 19.12.2021.

Burrueco, A. El 18% de las empresas españolas cree que sufrirá alguna vulnerabilidad en 2022. Cybersecuritynews. Extraído de: https://cybersecuritynews.es/el-18-de-las-empresas-espanolas-cree-que-sufrira-alguna-vulnerabilidad-en-2022/ Fecha de consulta: 05.05.2022.

Cancio, F. "Los intentos de ciberataques contra los sistemas militares españoles se duplican". La Razón. Extraído de: https://www.larazon.es/espana/20220408/h5j5l-czz7vgs5oapk47vglvauu.html Fecha de consulta: 04.04.2022.

28 Redacción. "España firma el Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia". Red Seguridad. Extraído de: https://www.redseguridad.com/actualidad/espana-firma-el-segundo-protocolo-adicional-al-convenio-sobre-la-ciberdelincuencia_20220516.html?utm_campaign=PostEditorial

29 Redacción. "Las infraestructuras críticas y los operadores de servicios esenciales privados verán reforzada su ciberseguridad". Red Seguridad. Extraído de: https://www.redseguridad.com/actualidad/organismos-ciberseguridad/las-infraestructuras-criticas-y-los-operadores-de-servicios-esenciales-privados-veran-reforzados-su-ciberseguridad_20220718.html Fecha de consulta: 25.07.2022.

Cancio. F. “España, última en un ejercicio multinacional de ciberguerra”. La Razón. Extraído de: https://www.larazon.es/espana/20220502/fs5356ec6fav5pcqqzvnwe3wn4.html Fecha de consulta: 10.05.2022.

Calle C. “Las empresas están muy concienciadas con la ciberseguridad; lo ven como una inversión a medio-largo plazo”. KPMG Tendencias. Extraído de: https://www.tendencias.kpmg.es/2018/05/entrevista-director-cnpic-ciberseguridad-infraestructuras-criticas/ Fecha de consulta: 19.12.2021.

Colom, G. “La necesidad de un programa nacional de ciber-reserva”. Nº 3. Noviembre. Thiber. Extraído de: https://www.thiber.org/wp-content/uploads/2018/11/Numero_03_Noviembre_Comentario.pdf Fecha de consulta: 19.12.2021.

Del Castillo, C. “El CNI avisa: `Todos los ataques a infraestructuras críticas han venido de otros Estados, nunca de ciberterroristas´”. El Diario.es Extraído de: https://www.eldiario.es/tecnologia/cni-ataques-infraestructuras-criticas-ciberterroristas_1_1487140.html

Del Castillo, C. “España podrá vetar de la red 5G a empresas `vinculadas al gobierno de terceros países´”. ElDiario.es. Extraído: https://www.eldiario.es/tecnologia/espana-podra-vetar-red-5g-empresas-vinculadas-gobierno-terceros-paises_1_8873912.html

Delloite. “El estado de la ciberseguridad en España”. Extraído de: https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html Fecha de consulta: 20.21.2021.

Garrido, P. “Defensa estudia crear un cuerpo propio de militares expertos en ciberdefensa”. El Confidencial Digital. Extraído de: https://www.elconfidencialdigital.com/articulo/defensa/defensa-estudia-crear-cuerpo-propio-militares-expertos-ciberdefensa/20211104170230299787.html

Global Cybersecurity Index 2020 https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/ Fecha de consulta: 06.04.2022.

Herrero, J. ¿Qué es log4j? ¿Por qué es la mayor vulnerabilidad informática de todos los tiempos? La Razón. Extraído de: https://www.larazon.es/tecnologia/20211221/r2t4i7flt5hy3dqm5o4nfyusvy.html Fecha de consulta: 19.12.2021.

Leal, J. “Los hackers frenan el plan de seguridad del Gobierno: `Combatirlos es inviable´”. La Información. Extraído de: https://www.lainformacion.com/economia-negocios-y-finanzas/los-hackers-frenan-el-plan-de-seguridad-de-sanchez-combatirlos-es-inviable/2863686/

Mallo, O. y Rabal, J. Log4j foto completa: Todas las vulnerabilidades de Log4Shel. Tarlogic https://www.tarlogic.com/es/blog/log4j-foto-completa-vulnerabilidades-log4shell/ Fecha de consulta: 20.12.2021.

Muñoz, A. “Alerta del CNI: la sanidad pública española sufre 38 ciberataques con peligrosidad muy alta en lo que va de 2022”. Invertia. El Español. Extraído de: https://www-elespanol-com.cdn.ampproject.org/c/s/www.elespanol.com/invertia/observatorios/sanidad/20220422/alerta-cni-sanidad-publica-espanola-ciberataques-peligrosidad/666683412_0.amp.html Fecha de consulta: 24. 04.2022.

Pastor. F. “Alerta máxima en las infraestructuras españolas por riesgo de ciberataques”. La Información. Extraído de: https://www.lainformacion.com/empresas/alerta-maxima-en-las-infraestructuras-espanolas-por-riesgo-de-ciberataques/2866557/

Plan España Digital 2025. Ministerio de Asuntos Económicos y Transformación Digital. Extraído de: https://portal.mineco.gob.es/RecursosArticulo/mineco/prensa/ficheros/noticias/2018/200723-np_resumen.pdf

Plan de Recuperación, Transformación y Resiliencia (página 39). Extraído de: https://www.lamoncloa.gob.es/temas/fondos-recuperacion/Documents/05052021-Componente11.pdf Fecha de consulta: 20.12.2021.

Pérez, E. “Un gigante llamado Bucarest: por qué León lo tenía difícil para albergar el Centro Europeo de Ciberseguridad”. Xataka. https://www.xataka.com/seguridad/gigante-llamado-bucarest-que-leon-tenia-dificil-para-albergar-centro-europeo-ciberseguridad Fecha de consulta: 19.12.2021.

Real Decreto 863/2018, de 13 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Política Territorial y Función Pública. https://www.boe.es/buscar/doc.php?id=BOE-A-2018-9858 Fecha de consulta: 18.12.2021.

Redacción. EE.UU. declara estado de emergencia tras un ciberataque a la mayor red de oleoductos del país. BBC Mundo https://www.bbc.com/mundo/noticias-internacional-57033536 Fecha de consulta: 19.12.2021.

Redacción. “El 30% de las organizaciones de infraestructuras críticas sufrirán brechas de seguridad a medio plazo”. Digital Security. Extraído de: https://www.itdigitalsecurity.es/infraestructuras-criticas/2021/12/el-30-de-las-organizaciones-de-infraestructuras-criticas-sufriran-brechas-de-seguridad-a-medio-plazo Fecha de consulta: 10.05.2022.

Redacción. “El Foro Nacional de Ciberseguridad presenta los primeros resultados de sus grupos de trabajo”. Red Seguridad. Extraído de: https://www.redseguridad.com/actualidad/organismos-ciberseguridad/el-foro-nacional-de-ciberseguridad-presenta-presenta-los-primeros-resultados-de-sus-grupos-de-trabajo_20220222.html Fecha de consulta: 25. 03. 2022.

Redacción. “España firma el Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia”. Red Seguridad. Extraído de: https://www.redseguridad.com/actualidad/espana-firma-el-segundo-protocolo-adicional-al-convenio-sobre-la-ciberdelincuencia_20220516.html?utm_campaign=PostEditorial Fecha de Consulta: 16.05.2022.

Redacción. “Las infraestructuras críticas y los operadores de servicios esenciales privados verán reforzada su ciberseguridad”. Red Seguridad. Extraído de: https://www.redseguridad.com/actualidad/organismos-ciberseguridad/las-infraestructuras-criticas-y-los-operadores-de-servicios-esenciales-privados-veran-reforzados-su-ciberseguridad_20220718.html Fecha de consulta: 25.07.2022.

Redacción. “La Oficina de Coordinación de Ciberseguridad”. Intelpage.info. Extraído de: https://intelpage.info/oficina-de-coordinacion-cibernetica-occ.html Fecha de consulta: 26.07.2022.

Sierra, M. “El Gobierno tarda un año en adjudicar 12 millones a contratos de ciberseguridad pese a alertar del riesgo de ciberataques”. Vozpópuli.https://www.vozpopuli.

com/economia_y_finanzas/ciberataques-gobierno-ciberseguridad.html Fecha de consulta: 22.11.2021.

`Startup Ecosystem Overview 2019´ https://gallery.mailchimp.com/9ab5c7f7f734ede362aeb83f4/files/98132712-c237-4c4c-a984-4b613b3edff5/DIGITAL_STARTUP_ECOSYSTEM_OVERVIEW_5.pdf Fecha de consulta: 22.04.2022.