HM Government

Ciberestrategia nacional 2022

Lideramos el ciberfuturo con la participación activa de la totalidad del RU

Ciberestrategia nacional 2022

Lideramos el ciberfuturo con la participación activa de la totalidad del RU

Contenido

Contenido adicional

Prólogo

El Reino Unido está formado por una sociedad abierta y democrática cuyos antecedentes en materia de colaboración e innovación fundamentan nuestro éxito como una nación global y con amplitud de miras. Esto se aprecia en nuestra respuesta frente a las emergencias sanitarias internacionales y en la difusión que hacemos de los objetivos de emisiones netas cero. Sin embargo, uno de los ámbitos donde esas ventajas se hacen más patentes es en la cibernética.

Tanto si se trata de materializar la amplia gama de beneficios que la cibernética ofrece a nuestros ciudadanos y nuestra economía a medida que subimos de nivel y unimos a todo el país como de colaborar con nuestros socios para lograr un ciberespacio que refleje nuestros valores nacionales o de utilizar plenamente nuestras capacidades cibernéticas para influir en acontecimientos globales, el Reino Unido considera la cibernética como una manera de proteger y promover nuestros intereses en un panorama que está siendo reconfigurado por la tecnología.

La nueva Ciberestrategia nacional es nuestro plan para garantizar que el Reino Unido pueda continuar confiando, siendo capaz y resiliente en un mundo digital que evoluciona rápidamente y que sigamos adaptándonos, innovando e invirtiendo con el fin de proteger y favorecer nuestros intereses en el ciberespacio.

Partiendo del punto donde termina la innovadora Estrategia de ciberseguridad nacional de 2016, este próximo capítulo nos conduce a un futuro donde el RU es aún más resiliente frente a los ciberataques. Como ministro principal, tengo claros dos de sus objetivos básicos: el primero, reforzar nuestra posición con respecto a las tecnologías que son esenciales para la cibernética y, segundo, limitar nuestra dependencia de proveedores individuales o tecnologías desarrolladas bajo regímenes que no comparten nuestros valores.

La ciencia y la tecnología del RU serán la sala de máquinas de ese cambio, y nos aseguraremos de que la cibernética continúe siendo un activo económico y estratégico nacional, y de que nuestra tecnología sea más confiable y esté mejor capacitada para protegernos de ciberadversarios cuyas capacidades eran, hasta hace poco, competencia exclusiva de los Estados nacionales.

Como Gobierno, nos hemos comprometido a gastar 22 000 millones de libras esterlinas en investigación y desarrollo, y a dar protagonismo a la tecnología en nuestros planes de seguridad nacional. Todos hemos sido testigos del potencial transformador de las tecnologías digitales, pero, al igual que ocurre con el 5G, también de su potencial de causar interrupciones. Nuestros planes de inteligencia artificial y política de datos nos permitirán mantenernos a la vanguardia de estas tecnologías, y los pasos que demos en virtud de la ciberestrategia garantizarán que podamos confiar en la seguridad y la resiliencia de proveedores y socios.

La creación de la Ciberfuerza Nacional el año pasado representa un paso hacia delante en nuestra capacidad cibernética ofensiva. No obstante, la ciberseguridad básica continúa siendo un elemento fundamental de nuestros esfuerzos a medida que endurecemos nuestra respuesta frente a aquellos que atacan al RU y a nuestros ciudadanos. Nuestro enfoque también se centra en lograr que el sector público sea más resiliente, ayudando a los ayuntamientos a proteger sus sistemas y los datos personales de los ciudadanos de *ransomware* y otros ciberataques.

Como sociedad, la cibernética es para todos. Gracias a esta estrategia, el Gobierno está haciendo más para proteger a los ciudadanos y las empresas del RU, así como a sus socios internacionales, contribuyendo a hacer realidad su visión del ciberespacio como un lugar seguro y resiliente donde las personas y los negocios pueden prosperar.

Rt Hon Steve Barclay MP Canciller del Ducado de Lancaster y Ministro del Gabinete de la Presidencia

Introducción

Las oportunidades y los desafíos de la era digital

1. Los beneficios exponenciales de la tecnología, aunados a una disminución de los costes, han hecho que el mundo esté más conectado que nunca, impulsando oportunidades extraordinarias, así como la innovación y el progreso. La pandemia de coronavirus (COVID-19) ha acelerado esa tendencia, pero probablemente aún nos encontremos en la fase inicial de un cambio estructural a largo plazo. La expansión global del ciberespacio está cambiando nuestra manera de vivir, trabajar y comunicarnos, además de transformando los sistemas críticos de los que dependemos en áreas como las finanzas, la energía, la distribución de alimentos, la asistencia sanitaria y el transporte. En resumen, ahora el ciberespacio constituye una parte integral de nuestra seguridad y prosperidad futuras. Esto presenta unas oportunidades extraordinarias para países tecnológicamente avanzados como el Reino Unido de alcanzar sus objetivos nacionales de nuevas maneras.

2. La escala y la velocidad de este cambio, que a menudo sobrepasan nuestras normas sociales, leyes e instituciones democráticas, también están desencadenando una complejidad, una inestabilidad y un riesgo sin precedentes. Durante el pasado año se produjeron ciberataques en hospitales, oleoductos, escuelas y empresas, algunos de ellos llegando incluso a quedar paralizados por el *ransomware* y *software* espía comercial utilizados para atacar a activistas, periodistas y políticos. La naturaleza transnacional del ciberespacio significa que la colaboración internacional es imprescindible para abordar esos desafíos, pero también es un escenario cada vez más importante para la competencia sistémica y el choque de intereses, valores y visiones opuestos sobre nuestro futuro global.

Nuestra visión: un ciberpoder que respalde nuestros objetivos nacionales

3. En este contexto, el ciberpoder se está convirtiendo cada vez más en un recurso esencial del poder nacional y en una fuente de ventaja estratégica. **El ciberpoder es la capacidad de proteger y promover los intereses nacionales en el ciberespacio.** Aquellos países que sean capaces de abrirse camino entre las oportunidades y los desafíos que presenta la era digital serán más seguros, más resilientes y prósperos en el futuro. El RU es una de las naciones más avanzadas del mundo a nivel digital y su Gobierno cuenta con una ambiciosa agenda tecnológica, tanto a nivel nacional como en el extranjero. Eso significa que estamos especialmente expuestos a los desafíos que plantea el ciberespacio, aunque también nos encontramos en una posición única para liderar el camino y aprovechar las oportunidades que ofrece para nuestros ciudadanos y para el bien común de la humanidad.

4. Durante los próximos diez años, Internet, la tecnología digital y la infraestructura que la sustenta se tornarán aún más fundamentales para nuestros intereses y los de nuestros aliados y adversarios. A medida que forjamos un nuevo papel para el RU en una era más competitiva, fortalecer nuestro ciberpoder nos permitirá liderar el camino para la industria y otros países, adelantarnos a los cambios futuros en la tecnología, mitigar las amenazas y obtener una ventaja estratégica sobre nuestros adversarios y competidores. Eso convertirá al RU en una de las economías digitales más seguras y atractivas donde vivir, hacer negocios e invertir.

5. Nuestra visión para **2030 es que el RU continúe siendo un importante ciberpoder democrático y responsable, capaz de proteger y promover nuestros intereses en el ciberespacio en apoyo de nuestros objetivos nacionales**:

- una nación más segura y resiliente, mejor preparada para enfrentarse a las amenazas y los riesgos en constante cambio, que utilice sus cibercapacidades para proteger a los ciudadanos frente a la delincuencia, el fraude y las amenazas de Estado
- una economía digital innovadora y próspera con oportunidades distribuidas más equitativamente a lo largo del país y de nuestra población diversa
- un superpoder de la ciencia y la tecnología que utilice con seguridad tecnologías transformadoras en pro de una sociedad más ecológica y sana
- un socio más influyente y valorado en el panorama global, que defina las futuras fronteras de un orden internacional abierto y estable, manteniendo a la vez nuestra libertad de actuación en el ciberespacio

6. Durante la última década hemos establecido al RU como un ciberpoder mediante la creación de una ciberseguridad y unas capacidades operativas de vanguardia y de un sector de la ciberseguridad líder en el mundo. Esta estrategia se basa en los importantes avances conseguidos a través de la Estrategia de ciberseguridad nacional 2016-2021 y en tres conclusiones cruciales establecidas en la Revisión Integrada de Seguridad, Defensa, Desarrollo y Política exterior del Gobierno. En primer lugar, que en la era digital, el ciberpoder del RU será un recurso cada vez más importante para lograr nuestros objetivos nacionales. En segundo lugar, que mantener nuestro ciberpoder requiere una estrategia más exhaustiva e integrada que tenga en cuenta nuestra gama completa de capacidades y objetivos cibernéticos. Y, en tercer lugar, que este enfoque debe centrarse en la totalidad de la sociedad. Lo que ocurre en las salas de reuniones o en el aula es tan importante para nuestro ciberpoder como las actuaciones de expertos técnicos y de los funcionarios del Gobierno, sin olvidar que trabajar en colaboración será fundamental para nuestro éxito.


CHELTENHAM
Science
Festival
18.2 Cyber Skills a
@CyNam

Los cinco pilares de nuestra estrategia

7. En la Revisión Integrada se establecieron cinco «actuaciones prioritarias» para esta estrategia, que utilizaremos como pilares de nuestro marco estratégico, **con el fin de guiar y organizar las actuaciones específicas que llevaremos a cabo y los resultados que tenemos previsto lograr hasta 2025**:

- **Pilar 1: fortalecer el ciberecosistema del RU**, invirtiendo en nuestras personas y habilidades e intensificando la alianza entre el Gobierno, el mundo académico y la industria.
- **Pilar 2: crear un RU digital resiliente y próspero**, reducir los riesgos cibernéticos para que las empresas puedan maximizar los beneficios económicos de la tecnología digital y los ciudadanos puedan estar más seguros y tranquilos en línea sabiendo que sus datos están protegidos.
- **Pilar 3: tomar la iniciativa en las tecnologías vitales para el ciberpoder,** desarrollar nuestras capacidades industriales y desarrollar marcos para garantizar futuras tecnologías.
- **Pilar 4: favorecer el liderazgo y la influencia globales del RU para lograr un orden internacional más seguro, próspero y abierto**, trabajar con el Gobierno y con socios de la industria y compartir la experiencia que afianza el ciberpoder del RU.
- **Pilar 5: detectar, interrumpir y disuadir a nuestros adversarios con el fin de mejorar la seguridad del RU en el ciberespacio**, realizando un uso más integrado, creativo y rutinario de la gama completa de recursos del RU.

8. En la primera parte de este documento se establece el contexto estratégico en el cual estamos operando, los objetivos de nuestra estrategia y el enfoque estratégico que adoptaremos en la próxima década. En la segunda parte se presentan las actuaciones específicas que emprenderemos para lograr nuestros objetivos para 2025 organizados bajo esos cinco pilares.

Visión

En 2030, el RU continuará siendo un ciberpoder responsable y democrático líder a nivel mundial, capaz de proteger y favorecer nuestros intereses en el ciberespacio en apoyo de nuestros objetivos nacionales.

Pilares y objetivos

Pilar 1

Fortalecer el ecosistema cibernético del RU

1. Fortalecer las estructuras, asociaciones y redes necesarias para respaldar un enfoque hacia la cibernética de toda la sociedad en general.
2. Mejorar y expandir las habilidades cibernéticas de la nación en todos los niveles, por ejemplo, a través de una profesión en el campo de la cibernética diversa y de primera clase que inspire a futuros talentos y les ofrezca las herramientas necesarias.
3. Fomentar el crecimiento de un sector de la seguridad de la información y la cibernética sostenible, innovador y competitivo a nivel internacional, que ofrezca productos y servicios de calidad y que satisfaga las necesidades del Gobierno y de la economía más amplia.

Pilar 2

Construir un RU digital resiliente y próspero

1. Mejorar el entendimiento del ciberriesgo para impulsar medidas más eficaces con respecto a la ciberseguridad y la resiliencia.
2. Evitar y resistir a los ciberataques más eficazmente mejorando la gestión del ciberriesgo en las organizaciones del RU, y ofrecer una mayor protección a los ciudadanos.
3. Fortalecer la resiliencia a nivel nacional y organizativo para prepararnos, responder y recuperarnos de los ciberataques.

Pilar 3

Tomar la iniciativa en las tecnologías que son fundamentales para el ciberpoder

1. Mejorar nuestra capacidad de anticiparnos, evaluar y actuar con respecto a los avances en ciencia y tecnología que son de vital importancia para nuestro ciberpoder.
2. Favorecer y mantener la ventaja soberana y la ventaja de nuestros aliados en la seguridad de las tecnologías críticas para el ciberespacio.

2a. Preservar una iniciativa Crypt-Key nacional robusta y resiliente que satisfaga las necesidades de los clientes del HMG, de nuestros socios y aliados, y que haya mitigado adecuadamente nuestros riesgos más importantes, incluida la amenaza de nuestros adversarios más capaces.

3. Garantizar la próxima generación de tecnologías e infraestructuras conectadas, mitigar los riesgos que la dependencia de los mercados globales supone para la ciberseguridad y garantizar que los usuarios del RU tengan acceso a un suministro fiable y diverso.
4. Colaborar con la comunidad de múltiples partes interesadas para configurar el desarrollo de estándares técnicos digitales globales en las áreas prioritarias que revisten más importancia para el mantenimiento de nuestros valores democráticos, garantizando nuestra ciberseguridad y potenciando la ventaja estratégica del RU a través de la ciencia y la tecnología.

Pilar 4

Propiciar el liderazgo y la influencia globales del RU

1. Reforzar la ciberseguridad y la resiliencia de los socios internacionales e incrementar las actuaciones colectivas para desestabilizar y disuadir a los adversarios.
2. Perfilar la gobernanza global para favorecer un ciberespacio libre, abierto, tranquilo y seguro.
3. Aprovechar y exportar las capacidades y la experiencia cibernéticas del RU para aumentar nuestra ventaja estratégica y promover nuestros intereses más amplios en la prosperidad y la política exterior.

Pilar 5

Detectar, interrumpir y disuadir a los adversarios

1. Detectar, investigar y compartir información sobre actores estatales, delictivos y otros tipos de ciberactores y actividades cibernéticas maliciosas para proteger al RU, a sus intereses y sus ciudadanos.
2. Disuadir e interrumpir a los actores estatales, delictivos y a otros ciberactores maliciosos y las actividades perpetradas contra el RU, sus intereses y sus ciudadanos.
3. Tomar medidas en el ciberespacio para respaldar nuestra seguridad nacional y la prevención y detección de delitos graves.

Apoyar los objetivos nacionales

- Seguridad y resiliencia
- Superpoder científico y técnico
- Prosperidad económica
- Dar forma al orden internacional

Primera parte: estrategia

Contexto estratégico

Una Gran Bretaña global en una era competitiva

9. La Revisión Integrada de Seguridad, Defensa, Desarrollo y Política exterior, publicada en marzo de 2021, describe la visión del gobierno sobre el papel del RU en el mundo durante la próxima década y las medidas que adoptaremos hasta 2025. La revisión reconoce que para que el RU esté mejor preparado para un mundo más competitivo debemos adoptar la innovación en la ciencia y la tecnología con el fin de impulsar nuestra prosperidad nacional y nuestra ventaja estratégica. La Estrategia de ciberseguridad nacional se basa en ese enfoque y su publicación es uno de los compromisos adoptados de acuerdo con el objetivo estratégico de la Revisión Integrada de «mantener una ventaja estratégica a través de la ciencia y la tecnología».

El panorama cibernético

10. Los retos políticos que presenta el ciberespacio no son únicamente de naturaleza tecnológica. El ámbito cibernético es un entorno creado por el ser humano y, fundamentalmente, viene determinado por el comportamiento humano. Para bien o para mal, amplifica esos comportamientos, y habitualmente sus efectos también se hacen sentir en el mundo físico. El ciberespacio está gestionado y es propiedad de empresas privadas, Gobiernos, organizaciones sin ánimo de lucro, ciudadanos individuales e incluso delincuentes. Eso significa que cualquier respuesta estratégica a ese contexto debe vincular la geoestrategia con la seguridad nacional, la justicia penal y la reglamentación civil, la política económica e industrial y requiere un entendimiento profundo de los distintos contextos culturales o sociales y de los sistemas de valores que interactúan en línea.

11. El ciberespacio también trasciende las fronteras nacionales. Las cadenas de suministro tecnológicas y las dependencias críticas son cada vez más globales, los ciberdelincuentes y los actores estatales operan desde cualquier parte del mundo, las empresas tecnológicas más potentes exportan productos y establecen sus estándares, y las reglas y normas que rigen en ciberespacio e Internet se deciden en foros internacionales. El ciberespacio también continúa evolucionando como tecnología y las maneras en que las personas lo utilizan también cambian, lo cual nos obliga a adoptar un enfoque ágil y receptivo.

Capas del ciberespacio

¿Qué es el ciberespacio?

Para muchos de nosotros, el ciberespacio es el mundo virtual que experimentamos cuando nos conectamos en línea para comunicarnos, trabajar y llevar a cabo tareas del día a día. En términos técnicos, el ciberespacio es la red interdependiente de infraestructuras de tecnologías de la información que incluye Internet, redes de telecomunicaciones, sistemas informáticos y dispositivos interconectados. Para el ámbito militar, y al considerar nuestros esfuerzos de contrarrestar las amenazas en el ciberespacio, se trata de un dominio operativo, junto con la tierra, el mar, el aire y el espacio.

¿Cómo se experimenta el ciberespacio? Por definición, el ciberespacio es un espacio «compartido» cuya escala y complejidad implican que la experiencia que cada persona tiene de él es única. Los ciudadanos acceden al ciberespacio cuando, por ejemplo, comprueban sus cuentas bancarias en línea o ven una película en casa. Las empresas utilizan el ciberespacio para conectar a sus empleados con los recursos que necesitan, tanto si se trata de acceder a la información como de controlar un proceso de fabricación. Los Gobiernos ofrecen servicios públicos a sus ciudadanos a través de portales en línea. Los ciberprofesionales exploran los entresijos de la tecnología, los estándares y los protocolos que hacen que «las cosas funcionen» para los usuarios. Todos esos grupos utilizan el ciberespacio de maneras distintas y para propósitos diferentes, y todos lo usamos cada vez con mayor frecuencia.

El ciberespacio se puede definir en relación con tres capas:

Virtual

La parte del ciberespacio que la mayoría de personas experimentan. Está formado por representaciones de personas y organizaciones a través de una identidad virtual en un espacio virtual compartido. Las representaciones virtuales podrían ser una dirección de correo electrónico, una identificación de usuario, una cuenta de redes sociales o un alias. Una persona o una organización puede tener múltiples identidades en línea. Por otro lado, múltiples personas u organizaciones también pueden crear una única identidad compartida.

Lógica

La parte del ciberespacio basada en código o datos, como los sistemas operativos, los protocolos, las aplicaciones y otros *software*. La capa lógica no puede funcionar sin la capa física y los flujos de información a través de redes por cable o del espectro electromagnético. La capa lógica, junto con la capa física, permite que las identidades virtuales se comuniquen y actúen.

Física

La capa física del ciberespacio incluye todo el *hardware* a través del cual se transmiten los datos, desde los enrutadores, cables y concentradores que tenemos en el hogar hasta los grandes y complejos sistemas de telecomunicaciones de las grandes empresas de tecnología. Además de una infraestructura física, incluye el espectro electromagnético en el cual se transmiten los datos, como el *wifi* y la radio.

Ciberpoder

12. El tema central de nuestra estrategia es el concepto del ciberpoder, que definimos como la capacidad de un Estado de proteger y promover sus intereses en el ciberespacio. Identificamos cinco amplias dimensiones del ciberpoder que se alinean con los pilares de esta estrategia:

- Las personas, conocimientos, capacidades, estructuras y asociaciones que constituyen los cimientos de nuestro ciberpoder y que sustentan todos los demás componentes y los integran en un enfoque nacional.
- La capacidad de proteger nuestros activos a través de la ciberseguridad y la resiliencia con el fin de materializar plenamente los beneficios que el ciberespacio ofrece a nuestros ciudadanos y a nuestra economía.
- Las capacidades técnicas e industriales para mantener una participación en la evolución de las cibertecnologías clave e implementar nuevos avances en pro de la sociedad.
- La influencia global, las relaciones y los estándares éticos para crear reglas y normas en el ciberespacio que estén en línea con nuestros valores e intereses y promover la seguridad y la estabilidad internacionales.
- La capacidad de adoptar medidas en el ciberespacio para apoyar la seguridad nacional, el bienestar económico y la prevención de delitos. Esto incluye las ciberoperaciones que tienen un efecto importante en el mundo real y que contribuyen a obtener una ventaja estratégica, las operaciones de las autoridades del orden público y la aplicación de cibersanciones para llevar a los delincuentes y ciberactores maliciosos ante la justicia e interrumpir sus actividades.

13. El ciberpoder es distinto de las formas más tradicionales de poder. Implica integrar sin problemas las capacidades duras y los mecanismos más blandos de influencia. Está más distribuido y los Gobiernos deben trabajar con sus socios para alcanzarlo y ejercerlo. Además, el ritmo del cambio tecnológico implica que se puede ganar y perder más rápidamente, a medida que las capacidades que anteriormente se consideraban avanzadas quedan desplazadas por nuevos avances.

14. Nuestra estrategia refleja precisamente eso, y describe cómo trabajaremos con nuestros socios siempre que podamos como parte de un esfuerzo que implica a toda la sociedad. Haremos más para abordar los problemas en las fases iniciales y corregir las causas fundamentales, anticiparnos a las tendencias futuras y establecer respuestas a largo plazo, además de ser más activos a la hora de configurar en lugar de responder al entorno geopolítico disputado.

El RU como un ciberpoder en la actualidad

15. El RU ya es un importante ciberpoder.[1] Durante la última década, el Gobierno ha liderado un esfuerzo nacional continuado con el fin de reforzar la ciberseguridad del RU, aumentar la concienciación pública sobre los riesgos cibernéticos, expandir el sector de la ciberseguridad y desarrollar una amplia gama de capacidades en el ciberespacio para responder a las amenazas de actores hostiles. Pese a haber realizado grandes avances y habernos situado en una posición consolidada, seguimos enfrentándonos a desafíos importantes a lo largo de los cinco pilares de esta estrategia.

[1] Se clasificó en el segundo puesto en el Índice Global de Ciberseguridad elaborado por la Unión Internacional de Telecomunicaciones, el tercer puesto en el Índice de Ciberpoder del Harvard Belfer Center y en el segundo nivel de la Evaluación de Capacidades de Ciberpoder del Instituto Internacional de Estudios Estratégicos.

El ecosistema cibernético y el liderazgo tecnológico del RU

16. El enfoque del RU hacia el desarrollo de su ciberpoder ha incluido esfuerzos organizados para desarrollar la base de habilidades cibernéticas y las capacidades comerciales del país, con la colaboración entre el Gobierno del RU y los Gobiernos descentralizados de Irlanda del Norte, Escocia y Gales, cuya asociación nos ha permitido aprender los unos de los otros. El sector de la ciberseguridad en el RU está creciendo rápidamente, con más de 1400 negocios que el pasado año generaron unos ingresos de 8900 millones de libras esterlinas, contribuyeron a la creación de 46 700 empleos cualificados y atrajeron unas inversiones extranjeras considerables. Este sector es esencial para nuestro ciberpoder, fomenta nuestra seguridad, nuestra influencia internacional y nuestro crecimiento económico. Hemos consolidado la reputación del RU como líder global en la investigación de la ciberseguridad, con 19 centros académicos de excelencia y 4 institutos de investigación que abordan nuestros desafíos más apremiantes para la ciberseguridad.

17. El personal del sector de la ciberseguridad ha crecido alrededor de un 50 % en los últimos cuatro años, con una demanda de habilidades que a menudo sobrepasa la oferta. Hemos colaborado ampliamente con la industria, con organizaciones profesionales, estudiantes, empleadores, profesionales actuales de la ciberseguridad y el mundo académico para entender mejor la naturaleza del desafío de las habilidades de ciberseguridad. Asimismo, hemos puesto a disposición de los jóvenes que desean emprender una carrera en la ciberseguridad una amplia gama de iniciativas extracurriculares. Entre 2019 y 2020, contamos con la participación de cerca de 57 000 jóvenes en nuestros programas de aprendizaje CyberFirst y Cyber Discovery. Hemos ampliado nuestros cursos para llegar a los estudiantes más jóvenes, y la competición CyberFirst Girls en línea atrajo a 11 900 chicas, con equipos principales que compitieron simultáneamente en 18 salas repartidas por el RU. Nuestro programa de becas CyberFirst ha atraído a estudiantes universitarios con talento y altamente motivados. El pasado año, 750 estudiantes participaron en el programa y la totalidad de los 56 graduados asumieron cargos a tiempo completo en el ámbito de la ciberseguridad.

18. A pesar de esas intervenciones, la cartera de habilidades más amplias continúa suponiendo un reto importante: del 1,32 millones de empresas que conforman la economía más amplia, alrededor de un 50 % aún registran lagunas en las habilidades de ciberseguridad técnicas básicas.[2] Y aunque el sector de la ciberseguridad en el RU ha crecido rápidamente, la mayoría de compañías son empresas de nueva creación y conseguir proveedores domésticos a larga escala continúa siendo difícil de cara a la consolidación internacional. Como ha demostrado la experiencia con el 5G, el RU y nuestros aliados no ocupan una posición de liderazgo en algunas áreas clave de la industria tecnológica en general. Los países que sean capaces de establecer un papel de liderazgo en las tecnologías críticas para el ciberpoder estarán en una mejor posición para influir en su diseño e implementación, serán más capaces de proteger su seguridad y su ventaja económica y podrán explotar más rápidamente las oportunidades de lograr importantes avances en sus capacidades cibernéticas.

La ciber resiliencia del RU

19. En la última década hemos llevado a cabo una amplia variedad de intervenciones dirigidas a fortalecer la ciberresiliencia del RU. Esto ha sido posible gracias a una inversión importante y continuada en algunas de nuestras cibercapacidades básicas, como el Centro de ciberseguridad nacional (NCSC, *por sus siglas en inglés*), los cuerpos y fuerzas de seguridad y los profesionales de la seguridad y la política que conforman nuestro Gobierno, así como nuestras asociaciones nacionales e internacionales en expansión.

[2] DCMS, Habilidades de ciberseguridad en el mercado laboral del RU 2021 (2021)

20. Nuestros esfuerzos más innovadores y pioneros consisten en haber tomado medidas a escala, como, por ejemplo, a través del desarrollo y la implementación creciente del programa de Ciberdefensa Activa (ACD, *por sus siglas en inglés*). El año pasado, este programa eliminó 2,3 millones de campañas maliciosas, incluidas 442 campañas de *phishing* que utilizaron la marca del NHS y 80 aplicaciones ilegítimas del NHS albergadas y disponibles para su descarga fuera de las tiendas de aplicaciones oficiales.[3] Asimismo, tomamos la delantera a nivel global al presionar para que los productos de consumo conectables fueran «seguros por diseño», desarrollando un código de prácticas del RU en 2018 que inspiró a otros a seguir nuestro ejemplo y que fundamentó el primer estándar de la industria aplicable a nivel global sobre dispositivos de consumo conectados a Internet.[4] [5]

21. Las nuevas normativas han tenido un efecto positivo sobre la ciberseguridad, y un 82 % de las organizaciones afirman que las mejoras que experimentaron estuvieron influenciadas por la introducción del Reglamento General de Protección de Datos del RU en 2018.[6] Y, ahora, un 77 % de las empresas consideran la ciberseguridad como una alta prioridad, lo cual supone un aumento del 12 % desde 2016.[7] La introducción de las Normativas de Redes y Sistemas de Información («normativas NIS», *por sus siglas en inglés*) en 2018 también hizo que las organizaciones designadas tomaran medidas para garantizar la seguridad de sus redes y sistemas de información, lo cual condujo a una reducción de los riesgos cibernéticos para los servicios esenciales y los servicios digitales importantes.[8] Un buen ejemplo de colaboración a lo largo de las cuatro naciones del RU han sido las mejoras realizadas a lo largo del sector sanitario, incluida la implementación de las normativas NIS.

22. Hemos ofrecido una orientación y un asesoramiento exhaustivos en materia de ciberseguridad a organizaciones de la economía más amplia, así como apoyo personalizado a sectores críticos durante la pandemia de coronavirus (COVID-19). En cuanto al público, nuestra campaña Cyber Aware ha proporcionado asesoramiento sobre las medidas que deben tomar para protegerse en línea. Cuando se han producido ciberataques, hemos utilizado nuestras capacidades de respuesta ante incidentes líderes a nivel global para ofrecer asistencia directa a los casos más graves, y nuestra inversión en especialistas de los cuerpos y fuerzas de seguridad locales significa que, ahora, todos los incidentes denunciados reciben una respuesta.

23. Hemos establecido ciberunidades de policía especializadas en todo el RU, además de la red cibernética PROTECT, la Unidad de Atención a las Víctimas de Delitos Económicos y los Centros de Ciberresiliencia regionales. Estas iniciativas significan que los ciudadanos y las pequeñas y medianas organizaciones tienen acceso a alguien cerca de ellos o pueden ponerse en contacto fácilmente con alguien que posee las habilidades y los conocimientos locales adecuados para prestar apoyo y orientación con el fin de mejorar su ciberresiliencia.

24. No obstante, tenemos pruebas cada vez más concluyentes de la presencia de lagunas en nuestra resiliencia nacional, con niveles de ciberdelincuencia y brechas en continuo crecimiento que afectan al Gobierno, a las empresas y los individuos,

[3] NCSC, Revisión Anual del NCSC 2021 (2021)
[4] DCMS, Código de prácticas para la seguridad del Internet de las cosas dirigido a consumidores (2018)
[5] DCMS, Estándar de la industria del ETSI basado en el Código de prácticas (2019)
[6] DCMS/RSM, El impacto del RGPD en los resultados de la ciberseguridad (2020). El Reglamento General de Protección de Datos (RGPD) introducido en la legislación del RU en 2018 ha sido sustituido por el RGPD del RU
[7] DCMS, Encuesta sobre violaciones de la ciberseguridad 2021 (2021)
[8] DCMS, Revisión de la posimplementación de las Normas de Redes y Sistemas de la Información 2018 (2020)

así como un aumento en la delincuencia perpetrada a través de la cibernética, como el fraude.[9] [10] Los sistemas informáticos heredados, las vulnerabilidades en la cadena de suministro y la escasez de profesionales de la ciberseguridad son áreas que suscitan una preocupación creciente. Casi cuatro de cada diez empresas (un 39 %) y una cuarta parte de las organizaciones benéficas (un 26 %) afirman haber sufrido violaciones de la ciberseguridad o ciberataques en el último año, y muchas organizaciones (especialmente las pequeñas y medianas empresas) carecen de la capacidad de protegerse y responder a los incidentes.[11] La industria nos dice que muchas empresas no entienden los riesgos cibernéticos a los cuales se enfrentan, que los incentivos comerciales para invertir en la seguridad no están claros y que, a menudo, existe poca motivación para informar sobre violaciones y ataques.

El liderazgo y la influencia internacionales del RU

25. A nivel internacional, la ciberexperiencia del Reino Unido goza de gran aceptación por parte de nuestros socios y el RU ha sido fundamental para aumentar la capacidad internacional y la determinación de afrontar las ciberactividades maliciosas. Esto ha quedado reforzado por un uso responsable de nuestras cibercapacidades ofensivas, que es coherente tanto con las leyes internacionales como con las del RU y nuestras posiciones expresadas públicamente, en contraste con las actividades indiscriminadas de algunos de nuestros adversarios.

26. Durante nuestro periodo como Presidente en ejercicio de la Commonwealth, el RU creó y lideró la implementación de la Ciberdeclaración de la Commonwealth, un compromiso compartido con nuestra seguridad, prosperidad y valores en el ciberespacio. La red internacional de la Agencia Nacional contra la Delincuencia (NCA, *por sus siglas en inglés*), ha fortalecido nuestras asociaciones de ejecución del derecho informático en el extranjero, reforzando las relaciones que hemos cultivado a lo largo de una dilatada historia de respuesta operativa colaborativa. El RU también ha desarrollado su red de funcionarios técnicos y de ciberseguridad en el extranjero en cinco continentes distintos y ha realizado labores de fomento de la capacidad en 100 países, consolidando la resiliencia, aumentando la influencia del RU y promoviendo sus valores.

27. El programa de Embajador de la Ciberseguridad ha generado relaciones a largo plazo y ayudado a las empresas del RU a conseguir importantes contratos internacionales. Las intervenciones de desarrollo internacional del RU, como el Programa de Acceso Digital, han colaborado con éxito con países aliados en África, Asia y Latinoamérica mediante la provisión de asesoramiento técnico para aumentar la capacidad de ciberseguridad de sus Gobiernos, sectores empresariales y usuarios. Esto incluye un incremento de las capacidades de ciberhigiene en comunidades con pocos recursos para lograr que los más vulnerables puedan protegerse de los riesgos y desafíos de estar conectados.

28. Sin embargo, nos enfrentamos a enfoques contrapuestos a nivel internacional a medida que competidores sistémicos como China y Rusia continúan abogando por una mayor soberanía nacional sobre el ciberespacio como respuesta a los desafíos de seguridad. La libertad en Internet va en declive a nivel global y la visión de Internet como un espacio compartido que promueve el intercambio de conocimientos y bienes entre sociedades abiertas se está viendo amenazada.

[9] Definido como delitos en virtud de la Ley de Utilización Indebida de Ordenadores
[10] ONS, Delitos en Inglaterra y Gales: año que finaliza en junio de 2021 (2021)
[11] DCMS, Encuesta sobre violaciones de la ciberseguridad 2021 (2021)

Combatir las ciberamenazas para el RU y disuadir a nuestros adversarios

29. Las amenazas a las cuales nos enfrentamos en el ciberespacio han aumentado en intensidad, complejidad y gravedad en los últimos años. Los ciberataques contra el RU corren a cargo de una amplia variedad de actores estatales, grupos delictivos (que en ocasiones actúan bajo las órdenes de Estados o con su aprobación implícita) y activistas con el propósito de espiar, obtener ganancias comerciales, sabotear y desinformar. Esos ataques provocan pérdidas financieras importantes, robos de propiedad intelectual, malestar psicológico, interrupciones en los servicios y los activos y, además, pone en riesgo nuestra infraestructura nacional crítica, las instituciones democráticas y los medios de comunicación. También pueden dañar la confianza de los inversores y consumidores y amplificar desigualdades y daños existentes. Durante la pandemia de COVID-19, la pandemia en la sombra de la violencia de género se vio agravada por los ataques en línea. Los ataques de *ransomware* son cada vez más sofisticados y dañinos. Aunque el nivel general de las ciberamenazas procedentes de actores hostiles durante la pandemia de COVID-19 ha permanecido constante, esto se ha explotado como una oportunidad y han cambiado el enfoque de sus ciberoperaciones para robar vacunas e investigaciones médicas, y para debilitar a otras naciones ya perjudicadas por la crisis. La dependencia creciente en las tecnologías digitales para el trabajo remoto y las transacciones en línea también ha aumentado la exposición a los riesgos. A esto se le suma el hecho de que las brechas digitales también han creado un acceso desigual a los servicios en línea y han expuesto a las personas a abusos y daños en Internet debido a la limitada alfabetización digital y a la falta de concienciación sobre las medidas de ciberseguridad que todos podemos adoptar para mantenernos seguros en línea.[12]

30. El Gobierno ha aplicado medidas para contrarrestar esas amenazas crecientes. La importante inversión que hemos realizado en nuestras capacidades de inteligencia ha aumentado nuestro entendimiento de la amenaza y nos ha permitido llevar a cabo contracampañas encubiertas más efectivas. Hemos desarrollado una respuesta integrada de las autoridades del orden público ante la ciberdelincuencia, liderada por la Agencia Nacional contra la Delincuencia (NCA) y por ciberequipos especializados en unidades regionales de lucha contra la delincuencia organizada y fuerzas policiales locales a lo largo de Inglaterra, Gales, Irlanda del Norte y Escocia. Esto ha mejorado nuestra capacidad operativa e investigativa de los ciberdelincuentes y otros adversarios. El Gobierno también está reforzando la seguridad de un número cada vez mayor de soluciones de identidad digital, desenvolviendo el marco de confianza de la identidad digital y atributos del RU.[13] Esto también nos ayudará a combatir delitos que implican el uso indebido de datos de identidad. Sin olvidar que el programa Cyber Choices de la NCA está ayudando a las personas a tomar decisiones más fundamentadas, alejándolas de la delincuencia para que utilicen sus habilidades cibernéticas de una manera positiva y legal.

31. Hemos realizado una gran inversión en nuestras cibercapacidades ofensivas, primero a través del Programa de Ciberofensiva Nacional (NOCP, *por sus siglas en inglés)* y, más recientemente, a través del establecimiento de la Ciberfuerza Nacional (NCF, *por sus siglas en inglés*). Por primera vez, la NCF reúne a personal de la Sede de comunicaciones del Gobierno (GCHQ, *por sus siglas en inglés*), el Ministerio de Defensa (MOD,

[12] NCSC, CyberAware
[13] DCMS, Marco de confianza de la identidad digital y atributos del RU (2021)

por sus siglas en inglés), el Servicio Secreto (SIS, *por sus siglas en inglés*, también conocido como MI6) y el Laboratorio de Defensa, Ciencia y Tecnología bajo un único mando unificado. Este grupo está operando en el ciberespacio para mantener la seguridad del país y proteger y promover los intereses del RU tanto a nivel nacional como en el extranjero.

32. En colaboración con nuestros aliados, también hemos procurado aumentar el coste de las actividades hostiles auspiciadas por Estados en el ciberespacio mediante la atribución de ataques (tal y como hicimos con las recientes violaciones de SolarWinds y Microsoft Exchange) e imponiendo consecuencias sobre los responsables. El desarrollo del régimen autónomo de cibersanciones del RU ha añadido otra herramienta disruptiva que nos ha servido para responder a incidentes como los ataques WannaCry y NotPetya. No obstante, pese a todo esto, nuestro enfoque hacia la disuasión cibernética no parece haber alterado aún en lo fundamental los cálculos de riesgo de los atacantes. A continuación se describen algunos ejemplos recientes de ciberataques importantes.

Casos prácticos recientes de ciberataques

Durante 2021, el RU prosiguió la colaboración con sus socios globales para detectar e interrumpir amenazas compartidas, las más constantes de las cuales provenían de Rusia y China. Además de las amenazas directas a la ciberseguridad planteadas por el Estado ruso, se hizo evidente que muchas de las bandas de delincuencia organizada que iniciaron ataques de *ransomware* contra objetivos occidentales estaban situadas en Rusia. China continuó siendo un actor altamente sofisticado en el ciberespacio, con una ambición creciente de proyectar su influencia más allá de sus fronteras y un interés demostrado en los secretos comerciales del RU. La manera en la cual China evolucione en la próxima década será probablemente el mayor impulsor individual de la ciberseguridad futura del RU. Aunque con un grado de sofisticación menor que el de Rusia y China, Irán y Corea del Norte continuaron recurriendo a las intrusiones digitales para lograr sus objetivos, incluidos el robo y el sabotaje.

Los ciberdelincuentes que usan el *ransomware* para atacar a los servicios públicos

El *ransomware* se convirtió en la ciberamenaza más importante a la que el RU tuvo que enfrentarse en 2021. Debido al probable impacto de un ataque exitoso sobre los servicios esenciales o la infraestructura nacional crítica, el NCSC evaluó el *ransomware* como potencialmente igual de dañino que el espionaje auspiciado por Estados.[14]

En octubre de 2020, el Ayuntamiento de Hackney sufrió un ciberataque de *ransomware* que provocó muchos meses de interrupciones y cuya rectificación tuvo un coste de millones de libras esterlinas. En un momento crítico cuando estaba lidiando con el impacto de la pandemia de COVID-19, el ayuntamiento perdió el acceso a datos importantes y se produjeron interrupciones en muchos servicios, incluidos el impuesto municipal y el pago de subsidios. Otras autoridades locales han sufrido ataques similares, al igual que distintas organizaciones del sector de la educación.

[14] NCSC, Mitigación de los ataques de *malware* y *ransomware* (2021)

En mayo de 2021, un ataque de *ransomware* perpetrado contra el Servicio Ejecutivo de Salud Irlandés (HSE, *por sus siglas en inglés*) interrumpió las redes de TI de asistencia sanitaria y afectó a los hospitales irlandeses durante más de 10 días, provocando consecuencias reales para los pacientes y sus familias. También se publicaron en línea algunos datos robados de pacientes. El HSE, que proporciona servicios sanitarios y de atención social en Irlanda, cerró las redes nacionales y regionales ese mismo día para tratar de contener el incidente. También se detectó una ciberactividad maliciosa en la red del Departamento de Salud Irlandés (DoH, *por sus siglas en inglés*). Sin embargo, gracias a la utilización de herramientas durante el proceso de investigación, fue posible detectar y detener un intento de ejecución de *ransomware*. El ataque también tuvo un impacto en Irlanda del Norte, ya que afectó a la capacidad de acceder a los datos del HSE en algunos servicios con pacientes transfronterizos.

Lo importante es que no se efectuó ningún pago de rescate en ninguno de los casos. **Los cuerpos y fuerzas de seguridad no fomentan, apoyan ni aprueban el pago de demandas de rescate. En caso de pagar un rescate:**

- **no existe ninguna garantía de que podrá acceder a sus datos o a su ordenador**
- **su ordenador continuará infectado**
- **estará realizando un pago a grupos delictivos**
- **es más probable que sea objeto de otro ataque en el futuro**

El NCSC publica directrices sobre cómo defender a las organizaciones frente a ataques de *malware* o *ransomware*, incluidos cómo prepararse para un incidente y qué medidas adoptar si su organización ya ha sido infectada.

Estados que explotan las vulnerabilidades estratégicas y las cadenas de suministro

El compromiso de la empresa de *software* SolarWinds y la explotación de Microsoft Exchange Servers puso de relieve la amenaza de los ataques a las cadenas de suministro. Estos sofisticados ataques, dirigidos a elementos menos seguros (como los proveedores de servicios gestionados o las plataformas de *software* comercial) en la cadena de suministro de instituciones económicas, gubernamentales y de seguridad nacional fueron dos de las intrusiones cibernéticas más graves jamás observadas por el NCSC.

A principios de diciembre de 2020, una empresa de ciberseguridad americana llamada FireEye descubrió que un atacante había logrado añadir una modificación maliciosa a un producto utilizado tanto por ellos como por muchas otras organizaciones del mundo. Esa modificación permitía que el atacante pudiera enviar comandos a nivel de administrador a cualquier instalación afectada de ese producto y utilizar eso para perpetrar ataques selectivos adicionales en sistemas conectados. El ataque inicial a la cadena de suministro se llevó a cabo a través de un *software* llamado Orion, una herramienta de monitorización de redes de TI desarrollada por una empresa llamada **SolarWinds**. El actor fue capaz de implantar código malicioso en un archivo de actualización del *software* en marzo de 2020. En abril de 2021, el NCSC, junto con sus homólogos de seguridad en EE. UU., revelaron por primera vez que el Servicio de Inteligencia Exterior de Rusia (el SVR) estaba detrás de este ataque, en lo que constituye una de las intrusiones cibernéticas más graves de los últimos tiempos.[15] SolarWinds confirmó que 18 000 organizaciones de todo el mundo, incluidos algunos departamentos del

[15] FCDO, Rusia: el RU y los EE. UU. exponen una campaña global de actividad maligna por parte de los servicios de inteligencia rusos (2021)

Gobierno de los EE. UU., habían quedado afectados. Este incidente formaba parte de un patrón más amplio de intrusiones cibernéticas por parte del SVR, que anteriormente había intentado obtener acceso a las redes de TI de miembros de la OTAN y de Gobiernos de toda Europa.

El 2 de marzo de 2021, Microsoft hizo público que algunos actores sofisticados habían atacado una serie de servidores de **Microsoft Exchange** , utilizados por organizaciones de todo el mundo para gestionar su correo electrónico, realizar planificaciones y organizar colaboraciones. Microsoft confirmó que las intrusiones iniciales comenzaron en enero de 2021 y que habían estado auspiciadas por China. Como respuesta a esto, se publicaron múltiples actualizaciones de seguridad dirigidas a los servidores afectados. En julio de 2021, el RU se unió a socios afines para confirmar que los actores auspiciados por China eran los responsables de los ataques que afectaron a más de un cuarto de millón de servidores en todo el mundo.[16] Era muy probable que el ataque pudiera facilitar un espionaje a larga escala, incluida la adquisición de información de identificación personal y propiedad intelectual. Al comprometer Microsoft Exchange, el autor de los hechos tuvo un punto de apoyo para saltar a las redes de TI de las víctimas. En el momento del ataque, el Gobierno facilitó asesoramiento con celeridad y recomendó medidas a tomar a los afectados. Microsoft señaló que, hasta finales de marzo, un 92 % de sus clientes había aplicado parches contra la vulnerabilidad.

[16] FCDO, el RU y sus aliados hacen responsable al Estado chino de un patrón generalizado de piratería informática (2021)

Impulsores del cambio

33. En la próxima década se producirá **una expansión rápida y continuada de los datos y la conectividad digital a prácticamente todos los aspectos de nuestras vidas**. El enorme crecimiento global del acceso a Internet y de su uso, sustentado por los datos y la infraestructura en la que se basa el uso de los datos, está creando nuevos mercados y aumentando la comodidad, la elección y la eficiencia. Pero también hace que los países dependan mucho más de los sistemas digitales interconectados, lo cual ofrece más oportunidades de que se produzcan actividades maliciosas y de que eso tenga un impacto importante en el «mundo real». A medida que las tecnologías críticas y no críticas continúan convergiendo en los distintos sectores, estos riesgos se están propagando a nuevas áreas de nuestra economía, y el traslado de datos y servicios a la nube (a menudo fuera del RU) está aumentando más si cabe nuestra exposición.

34. Cada vez más estamos viendo la interacción de empresas consolidadas en sectores regulados, como las telecomunicaciones y la energía, con nuevas empresas en su mayoría no reguladas, como las que ofrecen microgeneración, carga de vehículos eléctricos o capacidades de «espacios inteligentes». Las infraestructuras críticas se tornarán mucho más distribuidas y difusas y, fundamentalmente, eso cambia cómo la regulación afectará a la seguridad de las funciones críticas y los servicios de los que dependemos. Esta diversificación también afectará a nuestra seguridad nacional más amplia, haciendo que resulte más difícil conseguir acceso a la información, tanto a nivel de las autoridades del orden público como de la ciberseguridad. Ese cambio de escenario también afectará a los productos y servicios de una manera más generalizada fuera de nuestra infraestructura crítica nacional tradicional.

35. Este **panorama cada vez más complejo** hará que sea aún más difícil que los Estados, los negocios y la sociedad entiendan los riesgos a los cuales se enfrentan y cómo pueden y deben protegerse a sí mismos. El aumento de la dependencia con respecto a proveedores terceros de servicios gestionados, quienes a menudo tienen un acceso privilegiado a los sistemas de TI de miles de clientes, está generando nuevos riesgos que debemos abordar. Los dispositivos y redes estarán cada vez más conectados a Internet de serie, extendiendo así el ciberespacio a nuestros hogares, vehículos, entornos construidos e infraestructuras industriales. Los sensores, la tecnología ponible, los dispositivos médicos y biométricos desdibujarán los límites entre la actividad en línea y fuera de línea. Los riesgos cibernéticos se volverán generalizados, aumentando el volumen de datos personales y confidenciales generados y el impacto potencial en caso de producirse una vulneración de los sistemas.

36. En ese contexto, las **amenazas en el ciberespacio continuarán evolucionando y diversificándose** a medida que las cibercapacidades de alto nivel se vuelvan comercializables y proliferen en una amplia variedad de Estados y grupos delictivos. El número de actores con la capacidad y la intención de elegir al RU como blanco en el ciberespacio aumentará, y los Estados emplearán una extensa variedad de recursos para llevar a cabo actividades disruptivas, incluido el uso de representantes. La transición acelerada hacia el trabajo híbrido y las restricciones relativas a los viajes internacionales resultantes de la pandemia han conducido a una mayor dependencia de los servicios digitales, y han incentivado a los grupos de delincuencia organizada hacia los delitos cibernéticos. Ya se están comenzando a apreciar indicios de esta tendencia, y la última encuesta sobre delincuencia estima que los delitos cibernéticos aumentaron significativamente entre 2019 y 2021.[17]

[17] ONS, Delitos en Inglaterra y Gales: año que finaliza en junio de 2021 (2021)

Este desafío no será exclusivo del RU, sino que creará una vulnerabilidad mutua para todos aquellos que dependen del ciberespacio.

37. El ciberespacio se convertirá en un lugar más disputado a medida que los actores estatales y no estatales busquen una ventaja estratégica en el ciberespacio. Las ciberoperaciones se volverán cada vez más importantes para la proyección del poder por debajo del umbral de los conflictos armados y en situaciones previas a conflictos. También se apreciará un aumento en el uso de las cibercapacidades en los conflictos del futuro. Para que el RU pueda actuar de una manera eficaz necesitaremos incorporar unos niveles más elevados de ciberresiliencia en nuestras capacidades defensivas. Habrá que integrar las ciberoperaciones con otros elementos de fuerza para vencer las amenazas y posibilitar unas actividades defensivas más amplias. El espacio se convertirá cada vez más en un ámbito de actividad, según lo establecido por la Estrategia Espacial Nacional, abriendo nuevas áreas de riesgo, pero también creando nuevas oportunidades para que el RU pueda explotar sus cibercapacidades con el fin de lograr ventajas de nuevas maneras.[18]

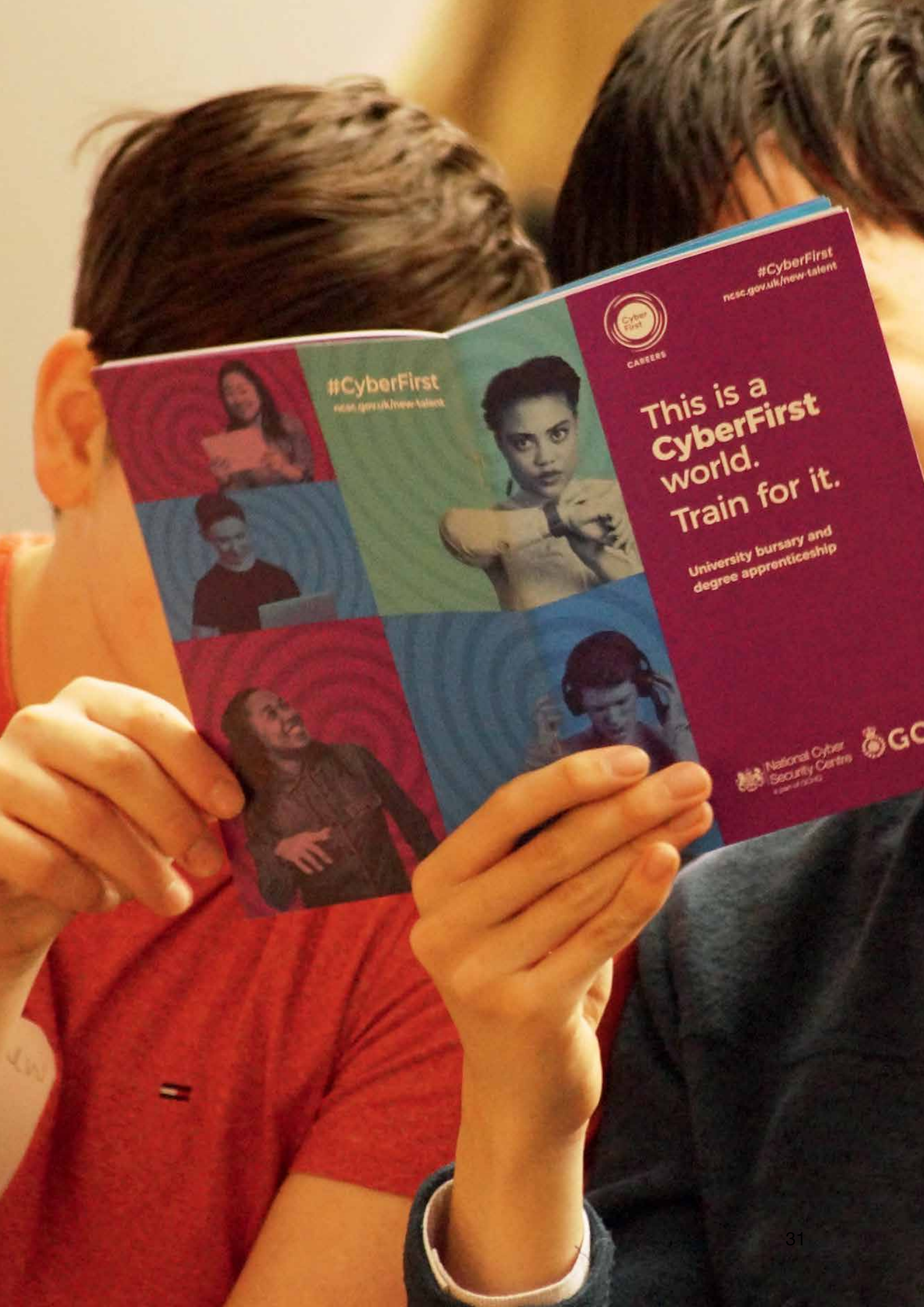
38. Los debates sobre las reglas que rigen el ciberespacio se convertirán cada vez más en un lugar **de competición sistémica entre grandes poderes,** con un choque de valores entre los países que desean conservar un sistema basado en las sociedades abiertas y los competidores sistémicos como China y Rusia, que están promoviendo un mayor control del Estado como única solución para garantizar la seguridad del ciberespacio. Esto ejercerá presión sobre un Internet libre y abierto, a medida que los Estados nacionales, las grandes empresas de tecnología y otros actores promueven enfoques contrapuestos hacia los estándares técnicos y la gobernanza de Internet.

39. Esto se verá agravado por **la competición por el control de un panorama tecnológico en rápida evolución**. A medida que la tecnología digital se integra en nuestras vidas diarias, en las empresas y las infraestructuras, algunas tecnologías se están convirtiendo en verdaderamente esenciales para el funcionamiento de la sociedad. El poder quedará cada vez más en manos de países que posean una ventaja estratégica en ciencia y tecnología y acceso a los datos que impulsan la innovación, lo cual les permitirá ejercer una influencia sobre otros y conformar los estándares globales de maneras que se adapten mejor a sus intereses económicos y políticos.

40. Las tecnologías emergentes como los gemelos digitales, la computación cuántica y los sistemas autónomos a gran escala (así como la información que estos generan) crearán nuevas oportunidades y riesgos y abrirán nuevas cibercapacidades para los atacantes y defensores, sin olvidar que las criptomonedas están siendo explotadas por bandas de *ransomware*. El liderazgo tecnológico se está volviendo más distribuido, y el RU no será capaz de desarrollar capacidades soberanas en todas las tecnologías que importan. Los Estados y las empresas utilizan los estándares técnicos para promover sus propios intereses y nos arriesgamos a que aquellos que no comparten nuestros valores sean quienes modelen las tecnologías clave.

41. Durante más de una década, el RU ha perseguido una ambiciosa estrategia de ciberseguridad nacional y ha dedicado un nivel importante de inversión, estableciendo al país como un líder mundial de la cibernética. Tal y como evidencia el análisis anterior, continúan habiendo desafíos y oportunidades. Los siguientes apartados describen nuestra respuesta nacional.

[18] HMG, Estrategia Espacial Nacional (2021)


#CyberFirst
ncsc.gov.uk/new-talent
CAREERS
This is a CyberFirst world. Train for it.
University bursary and degree apprenticeship
National Cyber Security Centre

Nuestra respuesta nacional

42. En este entorno estratégico, el RU tiene una elección que realizar. Podríamos tener el objetivo de simplemente mantener el ritmo en relación con las amenazas y los desafíos a los que nos enfrentamos en un ciberespacio cada vez más complejo, consolidando los avances de los últimos cinco años y abordando los problemas más urgentes allá donde podamos. No obstante, ese enfoque implica dos riesgos.
El primero es que no materialicemos plenamente el potencial de la fuerza del RU en la cibernética para apoyar las prioridades nacionales, y que perdamos oportunidades. El segundo riesgo más grave es que alcancemos un punto crítico a nivel tecnológico y descubramos que los cimientos de nuestra economía y sociedad futuras están siendo conformados por nuestros competidores y adversarios, y que debamos trabajar más duro para garantizar nuestra propia seguridad.

43. A nuestro parecer, a medida que el ciberespacio se torne más fundamental para nuestros intereses y los de nuestros aliados y adversarios **es imperativo que fomentemos nuestra ventaja competitiva ante ese panorama desde un punto de vista estratégico**. Eso nos permitirá no solo garantizar nuestra seguridad actual, sino también dar forma al mundo del futuro y beneficiarnos de ello.

Nuestra visión, objetivos y principios

44. Nuestra visión es que el RU en 2030 continuará siendo un **ciberpoder responsable y democrático líder en el mundo, capaz de proteger y fomentar nuestros intereses en el ciberespacio en apoyo de nuestros objetivos nacionales**.

45. Para hacer realidad esta visión perseguiremos cinco objetivos estratégicos. Cada uno de ellos tiene el objetivo de reafirmar nuestra fuerza nacional en una de las cinco dimensiones del ciberpoder, y colectivamente pretenden mejorar nuestra capacidad de mantener un ciberespacio que refleje nuestros valores e intereses. Estos cinco objetivos o pilares constituyen un marco estratégico que guiará nuestra actividad, y la segunda parte establece las actuaciones que realizaremos hasta 2025 en relación con cada uno de ellos.

- **Pilar 1: fortalecer el ciberecosistema del RU**, invirtiendo en nuestras personas y habilidades e intensificando la alianza entre el Gobierno, el mundo académico y la industria.
- **Pilar 2: crear un RU digital resiliente y próspero**, reducir los riesgos cibernéticos para que las empresas puedan maximizar los beneficios económicos de la tecnología digital y los ciudadanos puedan mantenerse seguros en línea y tener la confianza de que sus datos están protegidos.
- **Pilar 3: tomar la iniciativa en las tecnologías vitales para el ciberpoder,** desarrollar nuestras capacidades industriales y desarrollar marcos para garantizar futuras tecnologías.
- **Pilar 4: favorecer el liderazgo y la influencia globales del RU para lograr un orden internacional más seguro, próspero y abierto**, trabajar con el Gobierno y con socios de la industria y compartir la experiencia que afianza el ciberpoder del RU.
- **Pilar 5: detectar, interrumpir y disuadir a nuestros adversarios con el fin de mejorar la seguridad del RU en el ciberespacio**, realizando un uso más integrado, creativo y rutinario de la gama completa de recursos del RU.

46. La finalidad de estos objetivos es que se refuercen mutuamente. Por ejemplo, lograr unos niveles mayores de ciberseguridad y resiliencia a nivel nacional será un fundamento necesario para lograr una postura más activa a nivel internacional. A su vez, nuestras cadenas de suministro globales y las amenazas exteriores a las que nos enfrentamos significan que no seremos capaces de garantizar nuestra propia seguridad sin determinar más activamente el comportamiento de los actores internacionales. Y nuestra capacidad de influir en los debates sobre el ciberespacio, Internet y la tecnología se basará en mantener nuestra ventaja técnica y en crear un ecosistema de innovación que genere una ventaja competitiva auténtica en las tecnologías que más importan.

47. Un elemento fundamental de nuestra visión **es la promoción de un ciberespacio libre, abierto, pacífico y seguro**. Nuestro enfoque estratégico en el ciberpoder no tiene que ver con avivar los conflictos ni con que otros deban perder para que el RU gane. Según señala la revisión integrada, un mundo en el cual las sociedades y economías abiertas puedan florecer es la mejor garantía para nuestra prosperidad, soberanía y seguridad futuras. El RU trabajará con naciones afines para promover sus valores compartidos de apertura y democracia, adoptando un **enfoque responsable y democrático hacia el ciberpoder**. Eso significa que al trabajar en pro de esos cinco objetivos estratégicos aplicaremos los **principios siguientes**:

- Priorizaremos la capacidad de los ciudadanos y las empresas de operar en el ciberespacio con seguridad de modo que puedan maximizar los beneficios económicos y sociales de la tecnología digital y ejercer sus derechos legales y democráticos.

- Trabajaremos para defender un Internet abierto e interoperable como mejor modelo para fomentar la prosperidad y el bienestar globales, resistiendo la presión ejercida por Estados autoritarios hacia la fragmentación y su idea de la soberanía de Internet.

- Haremos un uso lícito, proporcionado y responsable de nuestras capacidades cibernéticas, con el apoyo de una supervisión clara y la colaboración del público y de nuestros aliados, y exigiremos que otros rindan cuentas con respecto a comportamientos imprudentes o indiscriminados en el ciberespacio.

- Tomaremos medidas contra el uso delictivo del ciberespacio utilizando todos los medios que tenemos a nuestra disposición, desafiando a todos aquellos que utilizan a representantes delictivos o que amparan a grupos delictivos en sus territorios, y trabajando para evitar la proliferación de las cibercapacidades de alto nivel entre los delincuentes.

- Abogaremos por un enfoque inclusivo con múltiples partes interesadas hacia los debates sobre el futuro del ciberespacio y la tecnología digital, defendiendo los derechos humanos en el ciberespacio y contrarrestando maniobras dirigidas hacia el autoritarismo digital y el control estatal.

Cambios clave en nuestro enfoque

48. En muchas áreas, nuestra estrategia tomará como base nuestro enfoque actual y buscará mejorar, expandir o adaptar nuestros esfuerzos allí donde sea necesario. Las principales diferencias con respecto a la Estrategia de ciberseguridad nacional 2016-2021 se establecen a continuación y reflejan nuestra ambición más amplia de afianzar la posición del RU como un ciberpoder líder a nivel mundial.

49. Un compromiso de mantener al RU en la vanguardia de la cibernética. En los próximos tres años, el Gobierno invertirá 2600 millones de libras esterlinas en cibernética y TI heredada. Esto supone una adición a una importante inversión en la Ciberfuerza Nacional anunciada en la Revisión de Gastos 2020 (SR20, *por sus siglas en inglés*). Incluye un incremento de 114 millones de libras esterlinas en el Programa de Ciberseguridad Nacional, y se cuenta entre los aumentos de las inversiones anunciados también en investigación y desarrollo (I+D), inteligencia, defensa, innovación, infraestructura y habilidades, todo lo cual contribuirá en parte al ciberpoder del RU. La inversión en cibernética anunciada en la SR20 y en la Revisión de Gastos 2021 (SR21) supera con creces los 1900 millones de libras esterlinas durante cinco años destinados a la anterior estrategia.[19]

50. Una Estrategia de ciberseguridad nacional más completa. La ciberseguridad continúa siendo un elemento fundamental de esta estrategia, pero ahora abarca el conjunto de las capacidades del RU, tanto dentro como fuera del Gobierno. Otorga una mayor importancia a las tecnologías y las infraestructuras críticas que sustentan el ciberespacio, apoya a las empresas de cibernética del RU para que puedan crecer a nivel nacional y competir a nivel internacional, intensifica la actuación internacional para dar forma al ciberespacio e influir en su futuro e integra la cibernética ofensiva como un recurso de poder. Esto requiere un enfoque estratégico nacional verdaderamente conjunto. La estrategia distribuye las responsabilidades de liderazgo y coordinación a lo largo de los Secretarios de Estado e implica más estrechamente a las administraciones descentralizadas. Todo esto se basa en nuestro éxito a la hora de coordinar los esfuerzos en todo el Gobierno, uno de los puntos fuertes clave del RU.

[19] HM Treasury, Presupuesto y Revisión de Gastos de otoño 2021 (2021)

51. Un esfuerzo de toda la sociedad. Nuestro objetivo es lograr un enfoque estratégico nacional que nos ayude a guiar y esté definido por nuestra toma de decisiones en organizaciones de todo el país, y que ofrezca la base de una colaboración más sólida con nuestros socios en el RU y en todo el mundo. Aún nos queda trabajo por hacer para convertir eso en una realidad. Las actuaciones a corto plazo incluirán: (i) establecer una nueva Junta Consultiva Nacional sobre Cibernética, invitar a los altos dirigentes de los sectores privado y terciario a que cuestionen, apoyen y orienten nuestro enfoque; (ii) reorientar nuestros programas de innovación del cibersector y alejarlos de iniciativas de gran envergadura ubicadas habitualmente en Londres para pasar a un modelo a nivel regional, creado en colaboración con la industria local, los innovadores, los cuerpos y fuerzas de seguridad y el mundo académico; y (iii) dar los pasos necesarios para aumentar la diversidad de la fuerza laboral cibernética, reconociendo que ser capaces de fomentar y aprovechar las habilidades y los talentos de toda la población es algo crucial para nuestra seguridad nacional. La propia estrategia está fundamentada en la participación de los Gobiernos descentralizados de Irlanda del Norte, Escocia y Gales, la industria, las autoridades del orden público, los reguladores, el mundo académico, la sociedad civil y los socios internacionales. Nuestra intención es mantener esos diálogos abiertos durante el periodo de implementación.

52. Un enfoque más proactivo hacia la incentivación y protección de nuestra ventaja competitiva en las tecnologías críticas para el ciberespacio. La Revisión Integrada y las estrategias subsiguientes ya han comenzado a adoptar este enfoque en áreas como la inteligencia artificial, las tecnologías cuánticas y los datos. Esta estrategia asume compromisos futuros en relación con el diseño de microprocesadores, la seguridad de las tecnologías operativas y la criptografía. Anuncia el establecimiento de un laboratorio nacional para la seguridad de la tecnología operativa, como un nuevo centro de excelencia centrado en crear el más alto nivel de ciberresiliencia en colaboración con la industria y el mundo académico. Y anuncia la expansión de las capacidades de investigación del Centro de ciberseguridad nacional (NCSC), incluido el nuevo centro de investigación aplicada de Manchester, con un enfoque en la tecnología emergente en áreas como los espacios inteligentes y el transporte. La estrategia también aprovecha nuestro trabajo de éxito para promocionar enfoques que aportan seguridad a las nuevas tecnologías, haciéndolas «seguras por diseño». Esto significará invertir y hacer un mayor uso de los recursos regulatorios y legislativos allí donde sea necesario para promover cadenas de suministro de tecnología más diversas, seguras y resilientes, tal y como hemos hecho con las telecomunicaciones.

53. Fortalecer nuestro esfuerzo principal para promover la ciberseguridad de una manera significativa, con el Gobierno a la cabeza. Invertiremos más que nunca en una reforma radical y rápida de la ciberseguridad del Gobierno, mediante el establecimiento de estándares claros para los departamentos y abordando las infraestructuras de TI heredadas. Hasta 2025, las funciones críticas del Gobierno se reforzarán significativamente ante los ciberataques y nos aseguraremos de que todas las organizaciones gubernamentales a lo largo de todo el sector público sean resilientes frente a vulnerabilidades y métodos de ataque conocidos hasta 2030. Haremos más para proteger e implicar a los ciudadanos y eliminaremos todas las cargas que les afectan dentro de lo posible. Reforzaremos el entorno digital, protegiendo a los ciudadanos de la ciberdelincuencia y el fraude y asignando una mayor responsabilidad sobre los fabricantes, minoristas, proveedores de servicios y el sector público para elevar los estándares de ciberseguridad. Favoreceremos un mayor nivel de participación por parte del sector privado y fomentaremos la inversión en la ciberresiliencia mediante una alineación de las normativas y los incentivos a lo largo

de la economía, así como facilitando un mayor apoyo. Asimismo, nos centraremos más en los riesgos de la cadena de suministro, poniendo a prueba una serie de intervenciones para ayudar a las organizaciones a gestionar los riesgos para la ciberseguridad que plantean sus proveedores, y para garantizar que las prácticas recomendadas lleguen hasta la cadena de suministro.

54. Más campañas integradas y continuadas para desestabilizar y disuadir a nuestros adversarios y proteger y promover los intereses del RU en el ciberespacio. Estas campañas tendrán su base en una gama más amplia de recursos diplomáticos, operativos y de política a lo largo del Gobierno. Contarán con el importante respaldo del establecimiento y la expansión de la Ciberfuerza Nacional (NCF), que estará situada en Samlesbury, Lancashire. Haremos un uso más rutinario de las capacidades de la NCF para interrumpir amenazas provenientes tanto de actores estatales como no estatales y apoyar los intereses de seguridad nacional más amplios del RU. Nuestras campañas también se beneficiarán de una mayor inversión en capacidades de alto nivel para los cuerpos y fuerzas de seguridad a nivel nacional, regional y local. Esto nos ayudará a abordar la importante amenaza que suponen el *ransomware* y unos ciberdelincuentes cada vez más innovadores. Asimismo, continuaremos utilizando el régimen de cibersanciones autónomo del RU y el proceso de atribuciones para imponer costes a nuestros adversarios y alertar sobre ataques malignos e irresponsables.

55. Situar el ciberpoder en el centro de la agenda de política exterior del RU y reconocer que todas las partes de la estrategia precisan de un compromiso internacional. Reforzaremos nuestras principales alianzas y buscaremos la participación de un abanico mucho más amplio de países para combatir la propagación del autoritarismo digital. Durante los próximos años, aumentaremos la inversión en programas internacionales para apoyar a países socios, ayudándolos así a desarrollar su capacidad de resiliencia y a mejorar sus capacidades para combatir las ciberamenazas. Y sacaremos un mayor partido a nuestra amplia gama de puntos fuertes nacionales, incluida nuestra experiencia en comunicaciones operativas y estratégicas, nuestro liderazgo de pensamiento y nuestras relaciones comerciales y asociaciones industriales con el fin de respaldar nuestros objetivos internacionales.

Funciones y responsabilidades a lo largo del RU

56. Un aspecto central de nuestra estrategia será un enfoque hacia la cibernética que abarque a toda la sociedad en general. Necesitamos crear una asociación duradera y equilibrada a lo largo de los sectores público, privado y terciario, donde cada uno de ellos desempeñe un papel destacado en nuestro esfuerzo nacional.

Ciudadanos

57. Esta estrategia tiene el objeto de eliminar en la mayor medida posible la carga que la ciberseguridad supone para los ciudadanos, pero todos continuaremos teniendo un papel importante que desempeñar. Pese a que el Gobierno hará todo lo posible por detener los ciberataques antes de que causen daños a las personas, algunos actores que suponen amenazas encontrarán una manera de eludir esas protecciones. Todos podemos tomar medidas para mejorar la seguridad de los activos que valoramos tanto en el mundo físico como en el virtual.[20] Eso significa asumir nuestra responsabilidad personal de adoptar todas las medidas razonables para proteger no solo nuestro *hardware* (teléfonos inteligentes y otros dispositivos), sino también los datos, *software* y sistemas que aportan libertad, flexibilidad y conveniencia en nuestras vidas privadas y profesionales. Para ello,

[20] Cyber Aware es el asesoramiento del Gobierno sobre cómo mantenerse seguro en línea

el Gobierno ofrece un asesoramiento técnicamente preciso, oportuno y práctico. Las organizaciones de la sociedad civil y los grupos de la comunidad también desempeñan un papel destacado en ayudar a las personas a entender los riesgos cibernéticos y a protegerse de ellos. Muchas organizaciones benéficas, por ejemplo, ofrecen una asistencia específica, asesoramiento y actividades de concienciación a grupos vulnerables.

Empresas y organizaciones

58. Las empresas y organizaciones tienen la responsabilidad de garantizar que estén manejando los riesgos cibernéticos de una manera eficaz, de volverse ciberresilientes y de apoyar a sus clientes y a las personas que utilizan sus servicios. Las empresas y organizaciones dependen cada vez más de las tecnologías digitales y los servicios en línea para operar, innovar y crecer. Esto mejora los servicios, pero también crea nuevos riesgos y desafíos, como el volumen cada vez mayor de datos personales y activos digitales de los que son responsables. Eso conlleva la responsabilidad de proteger esos datos y activos, manteniendo a la vez sus servicios. El incumplimiento de esa obligación puede conllevar importantes implicaciones económicas y para la reputación de las organizaciones y puede causar daños a sus clientes. Los operadores de servicios esenciales y los proveedores de servicios digitales clave (como los servicios en la nube) tienen las responsabilidades específicas de abordar los riesgos cibernéticos a los que se enfrentan y de cumplir las obligaciones establecidas en las Normas de Redes y Sistemas de la Información (las «normativas NIS»). El asesoramiento y las directrices del NCSC ayuda a proporcionar apoyo a todas las empresas y organizaciones para ayudarlas a proteger su información, activos y sistemas. La Oficina del Comisionado de Información (ICO, *por sus siglas en inglés*) también ofrece asesoramiento a organizaciones sobre sus obligaciones relativas a la ciberseguridad en virtud del Reglamento General de Protección de Datos del RU.

El sector de la ciberseguridad y las grandes empresas de tecnología

59. El sector de la ciberseguridad, que está en crecimiento en el RU, tiene un papel esencial a la hora de responder a las ciberamenazas emergentes y los desafíos a los que se enfrenta nuestro país. La rápida proliferación de productos conectables y la acelerada transformación digital de los negocios y las organizaciones están proporcionando oportunidades de crecimiento e innovación para el sector, así como ofreciendo nuevos servicios y productos. Esta estrategia describe cómo el Gobierno continuará apoyando el crecimiento del sector de la ciberseguridad en el RU y cómo se beneficiará de sus capacidades y experiencia manteniendo y fortaleciendo nuestras asociaciones. Asimismo, queremos forjar alianzas más amplias entre el mundo académico, la comunidad técnica más amplia y el sector privado, para asegurarnos de sacar el máximo partido a la experiencia y los conocimientos técnicos del RU.

60. Las principales empresas de tecnología que ofrecen servicios digitales tienen un papel fundamental que desempeñar para garantizar un entorno seguro donde las empresas y organizaciones del RU puedan operar. Esto es especialmente cierto para los proveedores de servicios gestionados y los negocios de plataformas que integran una serie de actividades. Estos deben asegurarse de que los servicios que ofrecen son «seguros por defecto» y de que no dependan demasiado de que sus clientes tomen medidas de protección. Las principales empresas de tecnología también tienen una responsabilidad específica de priorizar su propia ciberresiliencia. La dependencia cada vez mayor de empresas, Gobiernos y miembros de la sociedad con respecto a la nube y a los servicios en línea está creando vulnerabilidades nuevas y únicas, así como interdependencias.

Gobierno

61. El **Gobierno del RU** se encuentra en una posición única para reunir la inteligencia necesaria para entender las amenazas más sofisticadas, crear y hacer cumplir las leyes, establecer estándares nacionales y combatir las amenazas de actores hostiles, lo cual incluye llevar a cabo ciberoperaciones ofensivas. Mediante esta estrategia invertiremos en reforzar nuestras capacidades cibernéticas nacionales. Los departamentos del Gobierno y los organismos públicos también tienen la responsabilidad de proteger sus propias redes y sistemas. Como detentor de datos importantes y proveedor de servicios, el Gobierno toma medidas estrictas para brindar garantías en relación con sus activos de información. Por último, el Gobierno también tiene una responsabilidad importante de asesorar e informar a los ciudadanos, empresas y organizaciones sobre qué deben hacer para protegerse en línea. Y, cuando sea necesario, de establecer los estándares con los que esperamos que cumplan las empresas y organizaciones clave con el fin de protegernos a todos.

62. La mayor parte de las áreas de la ciberpolítica y la mayoría de las medidas indicadas en esta estrategia están relacionadas con asuntos reservados como la seguridad nacional, las relaciones exteriores y la defensa, las telecomunicaciones, los estándares y la seguridad de los productos y la protección de los consumidores. Pero el desarrollo y la implementación de esta estrategia aún depende de las aportaciones, las actuaciones y las inversiones de los **Gobiernos descentralizados de Irlanda del Norte, Escocia y Gales**. Esto es especialmente cierto en relación con las áreas de políticas transferidas que se sitúan principalmente en los pilares de «ecosistema» y «resiliencia» de esta estrategia, como la educación, la actuación policial y la ciberresiliencia de ciertos sectores críticos que incluyen sus propios sectores públicos. La coordinación y cooperación a lo largo de las cuatro naciones del RU es fundamental para garantizar el mayor impacto posible a lo largo de todo el país. Eso requiere un diálogo regular y temprano del *Cabinet Office* (Ministerio de la Presidencia británico) y de otros departamentos gubernamentales con sus homólogos galeses, escoceses y norirlandeses a la hora de compartir información sobre prioridades y planes. Esto también ayuda a evitar duplicaciones y a obtener el mejor valor de la financiación pública. Los Gobiernos descentralizados continuarán desarrollando sus propias ciberestrategias y planes, alineándolos con esta estrategia del Gobierno del RU.

El Centro de ciberseguridad nacional

«Contribuimos a que el RU sea el lugar más seguro donde vivir y trabajar en línea»

El Centro de ciberseguridad nacional (NCSC) se puso en marcha oficialmente en 2017 como parte de la GCHQ con el fin de convertirse en la autoridad nacional del RU en el ámbito de la ciberseguridad. Desde entonces, ha compartido conocimientos, abordado vulnerabilidades sistémicas y proporcionado liderazgo sobre temas clave de la ciberseguridad nacional.[21] La creación del NCSC simplificó las estructuras operativas del Gobierno, transformó la capacidad del RU de responder a ciberincidentes a nivel nacional e inició la implantación de servicios digitales innovadores que han contribuido a que las organizaciones y las personas estén más seguras en línea automáticamente.

Nos estamos cerciorando de que el NCSC esté preparado para enfrentarse a los desafíos de la próxima década definiendo las capacidades y los atributos perdurables que sustentan su labor, financiándolos de una manera sostenible y enfocando su uso donde la experiencia operativa hasta la fecha nos dice que tendrán el máximo impacto posible a escala nacional.

Las capacidades y los atributos duraderos que sustentan la labor del NCSC son:

- Una experiencia técnica de categoría mundial en las disciplinas y especialidades de la ciberseguridad que necesita el RU.
- Una percepción incomparable de las ciberamenazas actuales y potenciales (intención y capacidad) para los intereses del RU.
- Acceso a la amplia variedad de capacidades y autoridades de seguridad nacional del RU para los objetivos de la ciberseguridad.
- Alcance directo a las comunidades de la ciberseguridad en colaboración con socios del mundo académico, la industria y a nivel internacional.
- Habilidades y servicios criptográficos cruciales para la seguridad de los intereses del RU a nivel global.

Las principales responsabilidades del NCSC en virtud de la nueva estrategia serán:

- **Adoptar medidas directas para reducir los daños cibernéticos para el RU** ofreciendo protección a escala a través de servicios digitales (p. ej., el programa Ciberdefensa Proactiva o ACD, *por sus siglas en inglés*), impulsando cambios tecnológicos, gestionando la respuesta ante ciberincidentes de relevancia nacional y (junto con la Ciberfuerza Nacional [NCF]), combatir directamente las ciberoperaciones de nuestros adversarios.

[21] HMG, Estrategia de ciberseguridad nacional 2016 a 2021 (2016): párrafo 1.9

- **Apoyar a todos los sectores de la sociedad del RU para que se protejan a sí mismos** ofreciendo una experiencia personalizada y unos conocimientos únicos que los ciudadanos, las empresas y las organizaciones de todo el RU puedan utilizar para protegerse a sí mismos y contribuir a convertir al Reino Unido en un lugar más seguro para todo el mundo en línea.
- **Facilitar aportaciones técnicas a la política y las regulaciones del Gobierno de Su Majestad (HMG, *por sus siglas en inglés*) sobre los temas de mayor importancia para la ciberseguridad** proporcionando a los líderes de las políticas a lo largo de Whitehall datos técnicos acreditados y una evaluación de las amenazas derivados de las capacidades esenciales del NCSC, apoyando el desarrollo y la implementación de políticas y regulaciones para mantener la seguridad digital de los ciudadanos, las organizaciones y los intereses del RU.
- **Proporcionar al RU competencias soberanas** a través del National Crypt-Key Centre (Centro criptográfico nacional o NCKC, *por sus siglas en inglés*) del NCSC, que protege la información y los servicios críticos en los que se basan la comunidad militar y de seguridad nacional del RU, y que incluye la protección ante los ataques de nuestros adversarios más capaces.
- **Promover el crecimiento de las capacidades y las inversiones en la cibernética** facilitando las bases técnicas para cada nivel de educación en ciberseguridad y apoyando y haciendo partícipe a la industria, catalizando las inversiones hacia el sector de la cibernética.

El NCSC también contribuirá a la **evaluación del progreso** de los objetivos de esta estrategia de ciberseguridad nacional a través de las Evaluaciones del NCSC, la función de evaluaciones cibernéticas con independencia editorial del RU.

La Ciberfuerza Nacional

La Ciberfuerza Nacional (NCF), creada en 2020, es responsable de operar en el ciberespacio para combatir, interrumpir, degradar y defendernos de aquellos que tienen la intención de dañar al RU o a sus aliados, con el propósito de mantener al país seguro y proteger y favorecer los intereses del RU tanto a nivel nacional como en el extranjero. La NCF está formada por un porcentaje prácticamente igual de personal de defensa e inteligencia y reúne su experiencia, recursos y autoridades bajo una única estructura de mando. Estará situada en Samlesbury, Lancashire.

La NCF alcanza una amplia gama de resultados en aras de la seguridad nacional, como el apoyo a defensa, el bienestar económico del RU y la prevención de delitos graves. Las actividades de la NCF abarcan desde lo táctico hasta lo estratégico, tanto en relación con actores estatales como no estatales. Su trabajo se enmarca en tres categorías principales:

- Combatir las amenazas de los terroristas, delincuentes y Estados que utilizan Internet para operar a lo largo de las fronteras con el fin de dañar al RU y a otras sociedades democráticas.
- Combatir las amenazas que perjudican a la confidencialidad, integridad y disponibilidad de los datos y servicios en el ciberespacio (es decir, apoyar a la ciberseguridad).
- Contribuir a las operaciones de defensa del RU y ayudar a avanzar en la agenda de política exterior del RU (por ejemplo, interviniendo en una crisis humanitaria para proteger a los civiles).

Las operaciones de la NCF se pueden utilizar para influenciar a personas y grupos, causar interrupciones en los sistemas en línea y de comunicaciones y degradar las operaciones de los sistemas físicos. A menudo, se denomina a este tipo de actividad «cibernética ofensiva» (OC, *por sus siglas en inglés*).

Las operaciones de la NCF se llevan a cabo en línea con un marco legal bien consolidado, que incluye la Ley de Servicios de Inteligencia de 1994 y la Ley de Poderes de Investigación de 2016. Anteriormente, el RU ha dejado claro que desarrolla y despliega sus capacidades de conformidad con el derecho internacional, que incluye la ley de conflictos armados (en su caso). Sus actividades están sujetas a la aprobación ministerial, la supervisión judicial y la revisión parlamentaria, lo cual convierte al régimen de gobernanza del RU para las ciberoperaciones en uno de los más sólidos del mundo.

El RU no habla de manera rutinaria sobre ciberoperaciones individuales, pero los tipos de actividad operativa que podría realizar la NCF incluyen:

- Evitar que grupos terroristas lleven a cabo sus planes deshabilitando sus comunicaciones de mando y control y limitando la diseminación de medios de comunicación extremistas.
- Reducir el riesgo de daño para las fuerzas armadas del RU degradando los sistemas armamentísticos de los adversarios.
- Defender la democracia y unas elecciones libres, justas y abiertas luchando contra las campañas de desinformación organizadas por los Estados que tienen la intención de menoscabarlas.
- Impedir que los grupos delictivos se aprovechen de sus actividades causando interrupciones en su uso de las plataformas y los servicios en línea.
- Ayudar a imponer sanciones internacionales interrumpiendo los esfuerzos para evadirlas.
- Proteger al RU y a otros de los ciberataques causando interrupciones en la infraestructura que los adversarios utilizan para llevarlos a cabo.
- Proteger a los civiles durante las crisis humanitarias conservando su capacidad de acceder a información crítica.

Como centro nacional de excelencia para operaciones basadas en efectos en el ciberespacio, la NCF transformará la capacidad del RU para desarrollar, integrar y utilizar esas capacidades junto con otras y las optimizará para obtener resultados.

La Red Nacional de Ciberdelincuencia de los cuerpos y fuerzas de seguridad

La Red Nacional de Ciberdelincuencia, creada durante el transcurso de la Estrategia de ciberseguridad nacional 2016-2021, ha desarrollado una respuesta plenamente integrada frente a la ciberdelincuencia, lista para ofrecer una respuesta liderada por la inteligencia a todas las formas de ciberataques contra personas, organizaciones y sectores enteros. Se trata de un sistema nacional que opera a nivel nacional, regional y local. Ofrece atención a las víctimas, ayuda a las empresas y a las personas a protegerse y recuperarse rápidamente, y busca resultados contra los perpetradores en materia de justicia penal.

La **Unidad Nacional de Ciberdelincuencia (NCCU, por sus siglas en inglés), que se enmarca dentro de la Agencia Nacional contra la Delincuencia (NCA),** ofrece liderazgo nacional y coordinación de respuestas con el apoyo de una red de **Unidades Regionales de Ciberdelincuencia (RCCU, *por sus siglas en inglés*) especializadas** en cada una de las nueve regiones policiales de Inglaterra y Gales, en colaboración con sus contrapartes en la Policía de Escocia y el Servicio de Policía de Irlanda del Norte (PSNI, *por sus siglas en inglés*), así como la Unidad de Ciberdelincuencia de la Policía Metropolitana de Londres (MPS, *por sus siglas en inglés*).

Estos se complementan además con las **Unidades Locales de Ciberdelincuencia (LCCU, *por sus siglas en inglés*)**, que están integradas en cada una de las 43 fuerzas policiales y sincronizadas a través de un coordinador regional. Estas CCU regionales y locales tienen la autoridad para investigar y perseguir a los delincuentes, ayudar a las empresas y las víctimas a protegerse de ataques y trabajar con socios para evitar que personas vulnerables acaben siendo captadas para cometer ciberdelitos.

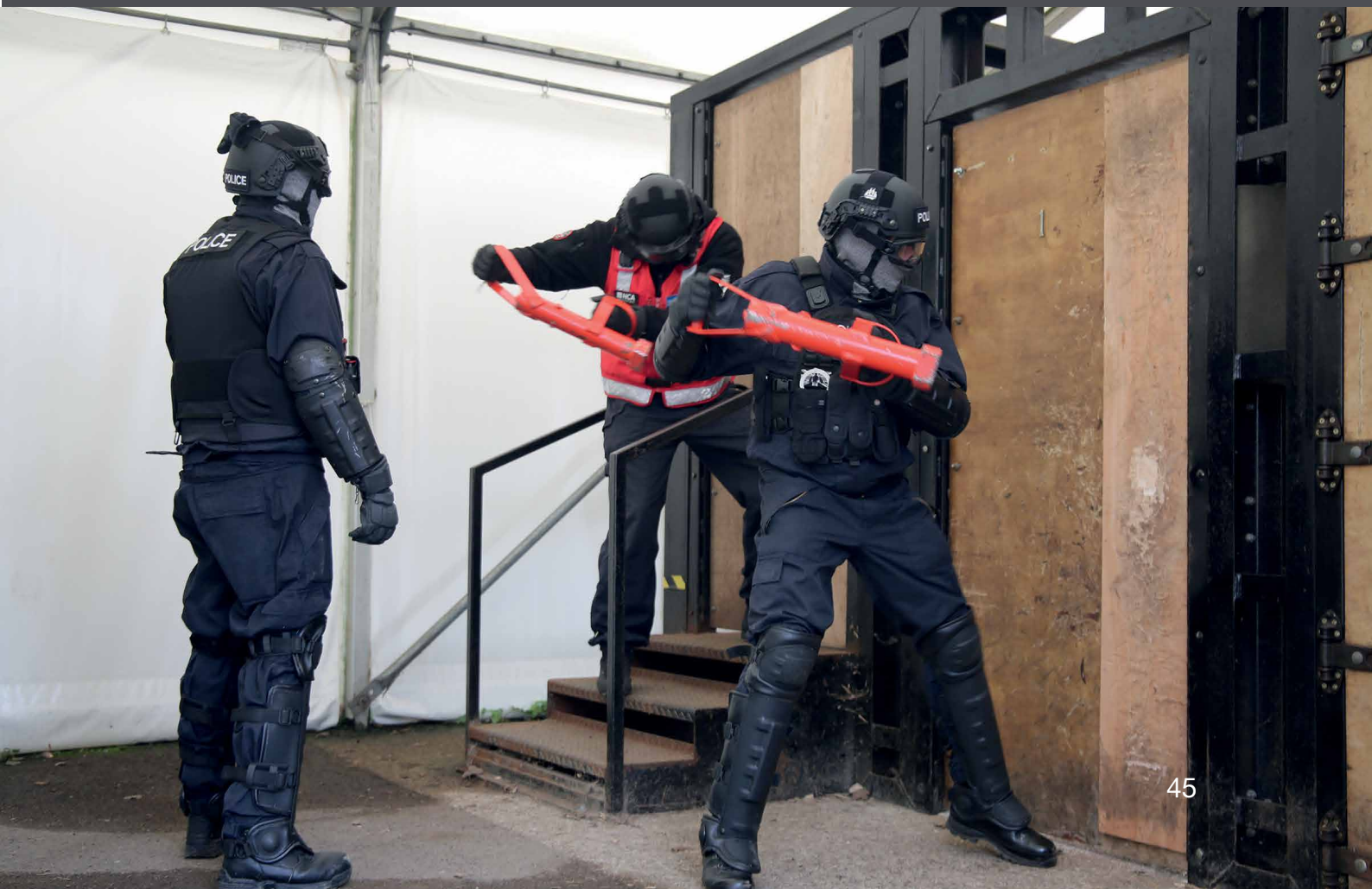
La denuncia centralizada de delitos, el triaje y el análisis corren a cargo de **Action Fraud**, que está a cargo de la **City of London Police**. Posteriormente, los casos más graves y/o complejos se derivan a la NCA y a la red regional para su resolución, mientras que otros casos se trasladan a las fuerzas del orden locales. La City of London Police también coordina la atención a las víctimas, que incluye la **Unidad de Atención a las Víctimas de Delitos Económicos.**

Los sistemas se están aunando a las capacidades forenses, de inteligencia y compartición de datos transformadas para crear una única plataforma, de manera que las unidades nacionales y regionales puedan acceder a todas las capacidades y herramientas de alto nivel que se están desarrollando. Esto incluye la capacidad de colaborar de una manera eficaz con socios de la comunidad de la seguridad y la inteligencia y, en particular,

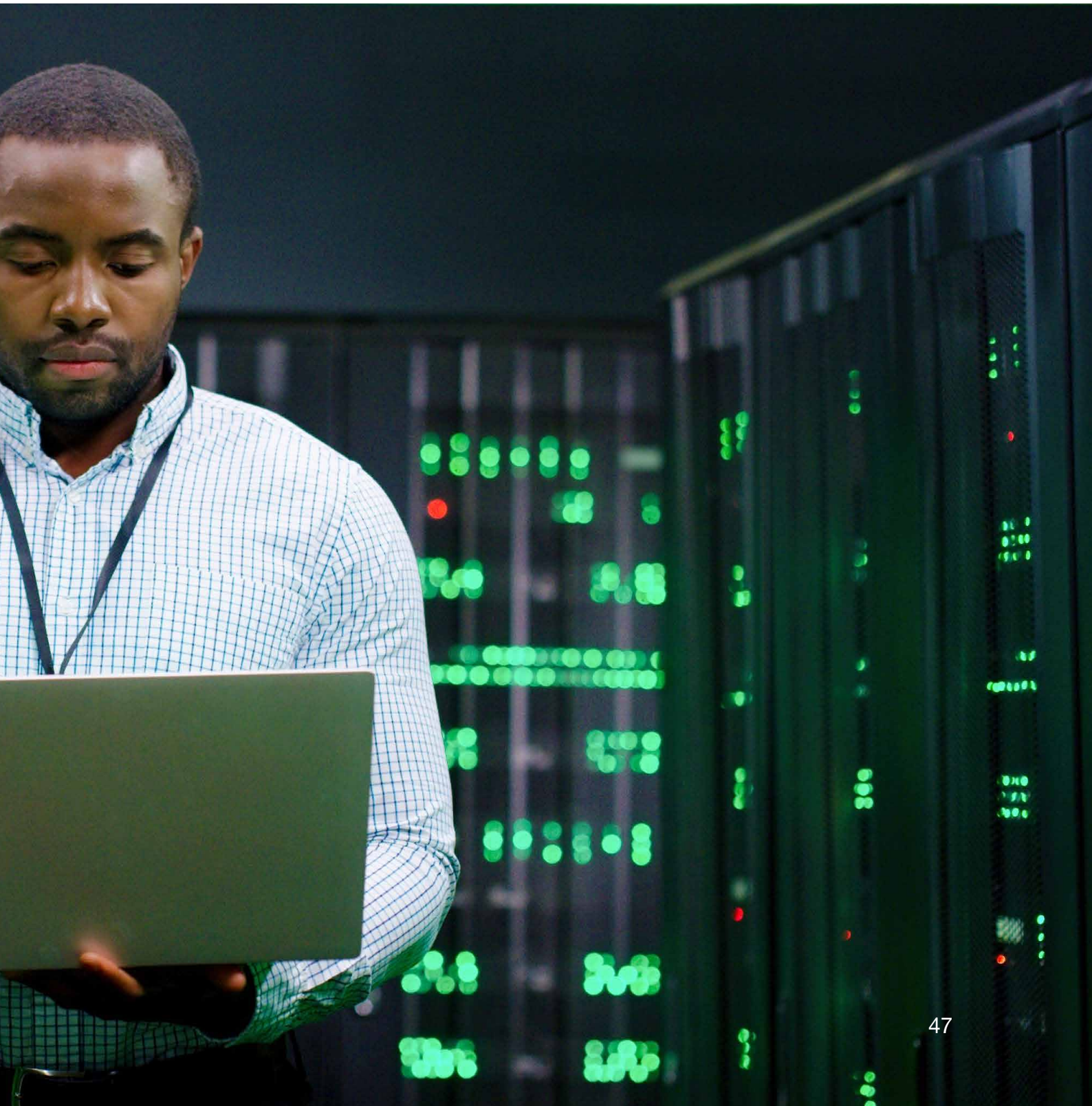
de responder a una mezcla de amenazas delictivas y de Estado. Continuando con el espíritu «construyámoslo una vez, construyámoslo a nivel nacional en beneficio de toda la red de lucha contra la ciberdelincuencia», las unidades locales de ciberdelincuencia también pueden acceder a estas capacidades a través de coordinadores regionales. Este enfoque en la totalidad del sistema ya está ofreciendo una respuesta mejorada importante a las amenazas de la ciberdelincuencia.

La Red Nacional de Ciberdelincuencia de los cuerpos y fuerzas de seguridad continuará impulsando nuestra respuesta de justicia penal hacia las actividades maliciosas del ciberespacio independientemente de que el actor de la amenaza haya actuado a nivel internacional, nacional, regional o local. Esto quedará complementado por una amplia variedad de métodos disruptivos que incluyen, sin limitación:

- Desarrollar cibercapacidades especializadas investigativas y desestabilizadoras de alto nivel.
- Utilizar la amplia red internacional de la NCA para apoyar las intervenciones de países aliados con inteligencia y pruebas.
- Evitar que los grupos delictivos se beneficien de sus actividades interrumpiendo su uso de los mercados delictivos y los servicios que los hacen posibles.
- Proteger al RU y a otros países de los delitos cibernéticos degradando y perturbando la infraestructura utilizada para llevarlos a cabo.
- Contribuir a las actividades sancionadoras y a la atribución pública contra delincuentes de alto nivel.
- Confiscar criptomoneda y otros activos en calidad de productos de la ciberdelincuencia.



Segunda parte:
implementación



Pilar 1: cibereco-sistema del RU

Fortalecer el ciberecosistema del RU

63. Para que esta estrategia funcione, debemos asegurarnos de que el RU cuente con las personas, los conocimientos y las asociaciones adecuados. Debemos tener empleados diversos y con habilidades técnicas, una comunidad investigadora dinámica, un cibersector competitivo a nivel internacional y un ecosistema regional de innovación próspero que nos permita tomar la iniciativa en las tecnologías críticas, todo ello asentado sobre asociaciones más estrechas entre el Gobierno, la industria y el mundo académico.

64. El crecimiento del ciberecosistema debe ser autosuficiente y no depender de las intervenciones del Gobierno. Durante el transcurso de esta estrategia pasaremos de financiar una variedad de programas de innovación y habilidades en gran parte personalizados y de gestión centralizada a un enfoque más sostenible, sistémico y regional. Aprovecharemos las reformas más amplias del Gobierno a los sistemas educativos y de habilidades para apoyar y animar a más personas a adquirir las habilidades que necesitan para desarrollar una carrera en la cibernética. Y priorizaremos una serie de medidas específicas para aumentar la diversidad de la fuerza laboral cibernética. No se trata únicamente de asegurarnos de que esos trabajos y carreras estén a disposición de todo el mundo, sino de que también cumplan una misión crítica para nuestra seguridad nacional, cerciorándonos de aprovechar el talento y las habilidades de toda la población. Asimismo, nos aseguraremos de que el crecimiento del sector cibernético beneficie a la totalidad del RU, no solo a Londres y al sureste, que concentran alrededor de un 45 % del empleo del sector y atraen a un 85 % de la inversión externa.[22]

65. En general, adoptaremos una posición más estratégica donde facilitaremos la unión de líderes de la industria, miembros del mundo académico, innovadores, autoridades del orden público, la comunidad de seguridad nacional y otros que deseen colaborar para hacer al RU más resiliente frente a las ciberamenazas. Alinearemos todos los recursos del Gobierno para apoyar el ciberecosistema, desde cómo se enseña la cibernética en las escuelas hasta cómo las normativas económicas impulsan los estándares, para garantizar que el RU desarrolle las capacidades esenciales necesarias para protegernos de amenazas futuras.

[22] DCMS, Análisis sectorial de la ciberseguridad 2021 (2021)

Objetivo 1: reforzar las estructuras, asociaciones y redes necesarias para apoyar un enfoque hacia la cibernética que abarque a toda la sociedad.

66. El ciberpoder requiere un enfoque centrado en la totalidad de la sociedad. Nuestra ventaja competitiva procederá de nuestra capacidad de fomentar y aprovechar el talento en todo el RU y de conseguir que las personas correctas trabajen juntas de las maneras adecuadas a lo largo de todo el sector público, la industria y el mundo académico, aunando los esfuerzos de la comunidad cibernética al completo. Para ello, necesitaremos forjar una alianza integrada y genuina con la industria capaz de ofrecer resultados y asegurarnos de contar con un enfoque geográfico extenso a lo largo de las naciones y regiones del RU, trabajando estrechamente con los Gobiernos descentralizados de Irlanda del Norte, Escocia y Gales y aprovechando la oportunidad de nivelación que presenta el ciberpoder. Lograremos los resultados siguientes hasta 2025:

67. Un diálogo cibernético nacional más inclusivo y estratégico con la industria, el mundo académico y los ciudadanos mediante el establecimiento de una nueva Junta Consultiva Nacional sobre Cibernética sénior, tomando como base las ya sólidas redes de asociaciones de crecimiento y resiliencia cibernéticos y los centros académicos de excelencia para la investigación y educación sobre ciberseguridad.

68. Unas redes cibernéticas regionales más integradas y eficaces a lo largo del RU, que permitan unas alianzas más sólidas entre el Gobierno, las empresas y el mundo académico para respaldar el crecimiento sectorial y la resiliencia empresarial. Colaboraremos con los clústeres cibernéticos regionales y con la organización UK Cyber Cluster Collaboration (UKC3) de reciente creación, un número cada vez mayor de centros de ciberinnovación regionales y Centros de Ciberresiliencia, fortaleciendo los vínculos entre las empresas locales, los centros académicos de excelencia y las autoridades del orden público.

69. Estos pasos tendrán como base las relaciones actuales entre el Centro de ciberseguridad nacional (NCSC) y sus partes interesadas, entre departamentos del Gobierno, organismos a distancia y los sectores de la economía a los cuales representan, incluidos la infraestructura nacional crítica (CNI, *por sus siglas en inglés*) y los reguladores, y el diálogo más amplio del Gobierno con la industria y los sectores digital y tecnológico.

Ciara Mitchell, Directora de Cibernética de ScotlandIS

Ciara también es la gerente del Clúster Cibernético de Escocia y miembro de la junta de UKC3.

«El Clúster Cibernético de Escocia ha desempeñado un papel clave a la hora de apoyar a la comunidad de la ciberseguridad en Escocia. Existe un entendimiento cada vez mayor de la experiencia sobre la gestión de clústeres en Escocia y la oportunidad de continuar construyendo un cibersector próspero. A medida que el valor de los clústeres ha ido recibiendo un mayor reconocimiento, estoy encantada de haber desempeñado una función clave en el nuevo UK Cyber Cluster Collaboration en calidad de Jefa de Desarrollo de Ecosistemas. A través de UKC3 habrá un enfoque mayor en la colaboración, la innovación y el desarrollo de habilidades, lo cual ofrece una plataforma para el crecimiento del sector de la ciberseguridad en el RU».

Ciberorganizaciones (representante de las ubicaciones)

Clústeres cibernéticos del RU

1. Bristol and Bath Cyber
2. Cyber North
3. Cyber Wales
4. CyNam (Cyber Cheltenham)
5. East of England Cyber Security Cluster
6. Midlands Cyber
7. ScotlandIS Cyber
8. South West Cyber Security Cluster
9. Yorkshire Cyber Security Cluster
10. NI Cyber (Irlanda del Norte)
11. North West Cyber Security Cluster
12. West of England Cyber Cluster

- Academic Centre of Excellence in Cyber Security Education
- Change Academic Centre of Excellence in Cyber Security Research*
- GCHQ/sitio NCSC
- Organizaciones de autoridades descentralizadas

*El punto rojo y la línea negra denotan los estados CSE y CSR

1. The Business Resilience Centre for the North East
2. The North West Cyber Resilience Centre
3. The Cyber Resilience Centre for the East Midlands
4. The Cyber Resilience Centre for the West Midlands
5. The Cyber Resilience Centre for the South East
6. The South West Cyber Resilience Centre
7. The Cyber Resilience Centre for Wales
8. The Eastern Cyber Resilience Centre
9. The Cyber Resilience Centre for London


Scottish Business Resilience Centre
Abertay University
CyberScotland Partnership
Edinburgh Napier University
University of Edinburgh
Queen's University Belfast
Northumbria University
Newcastle University
NI Cyber Security Centre
Lancaster University
GCHQ Scarborough
National Cyber Force
GCHQ Manchester
University of Birmingham
De Montfort University
GCHQ/NCSC Cheltenham
University of South Wales
University of Warwick
Cardiff University
University of Cambridge
University of the West of England
University of Oxford
University of Bristol
King's College London
GCHQ Bude
Imperial College London
University of Kent
University College, London
Royal Holloway
Kingston University
University of Surrey
University of Southampton

Objetivo 2: mejorar y expandir las habilidades cibernéticas de la nación en todos los niveles, incluyendo a través de una profesión en la ciberseguridad diversa y de primera clase que inspire y prepare a futuros talentos.

70. Un aspecto fundamental de las ambiciones del RU será desarrollar un suministro continuado y diversificado de personas altamente cualificadas para la fuerza laboral cibernética, capaz de proteger los elementos básicos de la economía digital, además de innovar y desarrollar nuevos enfoques. Esto respaldará nuestro objetivo de liderar con el ejemplo mediante el reconocimiento y la retención de experiencia a lo largo del sector público y el aumento de nuestra capacidad en el cumplimiento de la ley, la defensa y la seguridad, incluida la Ciberfuerza Nacional (NCF). Al igual que ocurre con otras partes de esta estrategia, trabajaremos con los Gobiernos descentralizados de Escocia, Gales e Irlanda del Norte para garantizar la adopción de un enfoque coherente a lo largo de todo el país en relación con las iniciativas del Gobierno del RU sobre las competencias transferidas, como la educación y las habilidades. Lograremos los resultados siguientes hasta 2025:

71. Un aumento significativo en el número de personas que poseen las habilidades necesarias para incorporarse a la fuerza laboral cibernética, tomando como base el trabajo que se está realizando a lo largo de las cuatro naciones del RU para garantizar que la política relativa a la educación y las habilidades satisfaga las demandas de las personas y los empleadores. Lo haremos a través de una serie de medidas que incluyen la expansión de programas de formación después de los 16 años acordes con las necesidades de la fuerza laboral cibernética, financiando una serie de campamentos de entrenamiento de habilidades en ciberseguridad, implantando a nivel nacional el programa Institutes of Technology y continuando con el programa de becas CyberFirst para estudiantes universitarios. Esto se sustenta en el trabajo del Gobierno de alinear la mayor parte de la formación y educación para jóvenes mayores de 16 años con los estándares reforzados liderados por empleadores hasta 2030. Esto se desarrollará junto con el Consejo de Ciberseguridad del RU para la cibercomunidad más amplia y se basará en prácticas, T Levels y nuevas cualificaciones técnicas superiores. Esto garantizará que los empleadores tengan un papel destacado a la hora de diseñar y desarrollar cualificaciones y formación.

72. Una profesión en ciberseguridad de mayor calidad y más consolidada, reconocida y estructurada. Establecido mediante Decreto Real, el Consejo de Ciberseguridad del RU creará estándares e itinerarios profesionales para cursar carreras en cibernética sobre la base del proyecto de clase mundial Cyber Security Body of Knowledge (CyBOK, *por sus siglas en inglés*). Asimismo, exploraremos todos los recursos del Gobierno, incluida la legislación, para integrar esos estándares a lo largo de la profesión, asegurándonos de que la excelencia y la experiencia puedan reconocerse claramente y de una manera sistemática a lo largo de la fuerza laboral cibernética.

73. Una fuerza laboral cibernética más diversa, dando un apoyo más eficaz para acceder y prosperar en una carrera en cibernética a los grupos infrarrepresentados y a las personas procedentes de comunidades desfavorecidas a lo largo del RU. Nuestro conjunto de medidas incluirá apoyar a más mujeres a participar en la fuerza laboral cibernética, así como intervenciones específicas para apoyar a grupos infrarrepresentados para que avancen hasta niveles superiores. Y aprovecharemos los éxitos de las actividades extracurriculares ofrecidas a través de nuestro programa de referencia CyberFirst, incluido el concurso CyberFirst Girls. También aumentaremos el acceso a la educación y a las oportunidades profesionales para jóvenes en riesgo a través del programa Cyber Choices de la Agencia Nacional contra la Delincuencia, con el fin de alejarlos de las ciberactividades ilegales y guiarlos hacia oportunidades más positivas de utilizar su talento y entusiasmo.

74. Mantener un flujo continuado y diverso de personas altamente cualificadas en nuestro sistema educativo. Inspiraremos y apoyaremos a más jóvenes para que sigan un itinerario tecnológico a través de la educación, lo cual incluye un aumento de la aceptación y la diversidad de candidatos que cursen GCSE en Ciencias de la Computación y cualificaciones equivalentes en Escocia, y que posteriormente pasen a una educación superior como los T Levels en Inglaterra, a prácticas y otras oportunidades de educación superior. Asimismo, mejoraremos las cualificaciones de más maestros en Inglaterra a través del Centro Nacional de Educación en Computación (NCCE, *por sus siglas en inglés*), garantizando que tengan acceso a recursos y oportunidades de desarrollo que les ayudarán a despertar el interés en más estudiantes.

75. El Gobierno puede identificar, contratar, formar y retener mejor a los profesionales que necesita. Como principales empleadores de ciberprofesionales, el Gobierno y el sector público deberán predicar con el ejemplo, apoyando y basándose en las medidas señaladas anteriormente. Adoptaremos un enfoque más coherente y eficaz a lo largo del sector público confeccionando a la vez medidas específicas para mejorar las capacidades de los funcionarios públicos y los altos dirigentes, y desarrollar nuestras capacidades en defensa y seguridad, incluidos la NCF, el NCSC y las autoridades del orden público. Esto incluirá invertir en talento precoz mediante la expansión del programa Cyber Fast Stream y ofrecer más prácticas en ciberseguridad, apoyar a los programas de habilidades especializadas dentro del NCA, incluidos puestos de prácticas y para estudiantes graduados, programas personalizados de neurodiversidad y programas de diversidad de verano. Esto se asentará en los éxitos de la Defence Cyber School (Escuela de Ciberdefensa) con su expansión a la Defence Cyber Academy (Academia de Ciberdefensa) mediante una oferta más extensa de formación cibernética defensiva y ofensiva, colaborando a la vez con socios internacionales, del mundo académico y de la industria.

El Consejo de Ciberseguridad del RU

El Consejo de Ciberseguridad del RU se puso en marcha en marzo de 2021 y es una novedad mundial para la profesión de la ciberseguridad. Su misión consiste en ser la voz de la profesión, aportando claridad y estructura a la fuerza laboral cibernética en crecimiento y la variedad de cualificaciones, certificaciones y carreras que existen en el ámbito. Reconocer que la profesión cibernética incorpora una amplia variedad de experiencia técnica y no técnica y especialidades a lo largo de toda la economía, con un alcance similar al de profesiones más consolidadas como la medicina y el derecho es un paso fundamental.

El Consejo tiene cuatro objetivos:

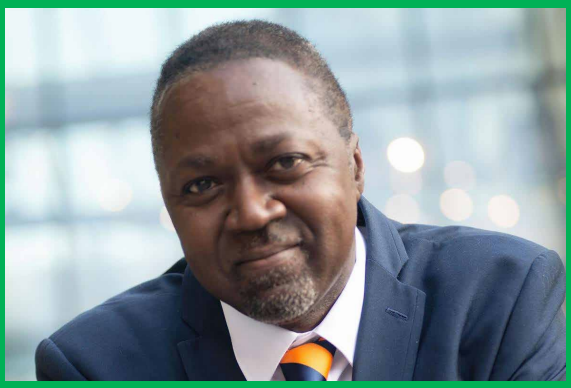
- Liderazgo intelectual y estándares profesionales: liderar el trabajo para desarrollar la ciberseguridad y acordar los estándares que la definen.
- Carreras y aprendizaje: apoyar a los empleadores y a las personas en su toma de decisiones profesionales, ofreciendo asesoramiento sobre habilidades de ciberseguridad, desarrollo profesional y reconocimiento.
- Ética profesional: ofrecer principios rectores dentro de los cuales los profesionales practicantes y las propias organizaciones puedan demostrar unas prácticas de ciberseguridad éticas.
- Diversidad e inclusión: promover la ciberseguridad como una oportunidad de carrera para personas de todas las edades y orígenes, haciendo un esfuerzo por eliminar las barreras a la entrada y la progresión dentro del campo.

El Consejo estudiará cómo desarrollar y consolidar su credibilidad y sostenibilidad como autoridad profesional a lo largo del ciclo de vida de esta estrategia. Unirá a una variedad de organismos profesionales y de certificación existentes, identificando y empoderando a organizaciones expertas que puedan aportar claridad a los requisitos de progresión y competencias para los nuevos candidatos, los practicantes actuales y los empleadores.

La Reina aprobó el otorgamiento de un Decreto Real al Consejo de Ciberseguridad del RU en noviembre de 2021. Por primera vez, esto proporciona un reconocimiento personalizado y certificado específico para la ciberseguridad que cubre la variedad de especializaciones que existen en el campo.

Somos conscientes de que queda más trabajo por hacer para integrar los estándares y los itinerarios profesionales en el ecosistema cibernético, incluido en el Gobierno, en defensa y en las autoridades del orden público. El Consejo tendrá un importante papel en ese sentido, mediante el apoyo a los jóvenes y a las personas que desean cambiar de carrera para dirigirla hacia la cibernética.

Simon Hepburn, CEO, Consejo de Ciberseguridad del RU



Mi trabajo implica promover el Consejo de Ciberseguridad del RU como «la voz de la profesión de la ciberseguridad». El Consejo es el organismo de autorregulación de la profesión de la ciberseguridad en el RU, y nuestro objetivo consiste en unir a la industria para desarrollar, promover y supervisar los estándares de la cibernética reconocidos a nivel nacional con el fin de convertir al RU en el lugar más seguro donde vivir y trabajar en línea. El Consejo se puso en marcha oficialmente en marzo de 2021 tras un exitoso proyecto de formación, y ahora está abierto a la presentación de solicitudes de admisión. La Estrategia de ciberseguridad nacional es un elemento fundamental para garantizar que las personas y las organizaciones puedan trabajar de una manera que beneficie a la profesión, con el Consejo como coordinador clave.

Objetivo 3: favorecer el crecimiento de un sector de la cibernética y la seguridad de la información sostenible, innovador y competitivo a nivel internacional, ofreciendo productos y servicios de calidad que satisfagan las necesidades del Gobierno y de la economía más amplia.

76. Para mejorar su ciberpoder e impulsar el crecimiento digital y las exportaciones, el RU precisa de un cibersector dinámico conformado por empresas de confianza y alta calidad. Las empresas del RU ofrecen tecnologías líderes en el mundo, formación y asesoramiento tanto a la industria como a Gobiernos del RU y a nivel global. Pero, para desarrollar tecnologías de vanguardia, algunas empresas necesitan ayuda y conexiones con inversiones para alcanzar una fase en la que puedan ofrecer un producto viable.

77. Las empresas también necesitan estar seguras de que están innovando de acuerdo con los parámetros aprobados por el Gobierno que otras organizaciones también están siguiendo. Y podemos hacer más para ayudar a los compradores a desenvolverse en el complejo panorama que supone la amplia variedad de productos y servicios de distinta calidad. A su vez, esto estimulará la demanda en el ecosistema y favorecerá un mayor crecimiento. Lograremos los resultados siguientes hasta 2025:

78. Un cibersector que ha alcanzado un crecimiento interanual global superior a la media, incluido a través del comercio y de las ciberexportaciones. Ayudaremos a las empresas de cibernética a acceder a nuevos mercados a nivel nacional y en el extranjero mediante el respaldo de eventos cibernéticos de referencia líderes a nivel mundial en el RU e invitando a nuestras empresas de cibernética más innovadoras a participar en misiones comerciales y ferias cibernéticas internacionales. Utilizaremos la contratación en el sector público de una manera más eficaz y estableceremos un directorio exhaustivo de proveedores autorizados por el NCSC para impulsar la demanda de productos y servicios de ciberseguridad de alta calidad.

79. Un cibersector aún más innovador que ha experimentado un aumento considerable de las inversiones iniciales y más empresas de cibernética que han podido ponerse en marcha, crecer y ampliar su escala. Nuestro nuevo programa Cyber Runway facilita a las empresas un único foco de atención para la asistencia, habiendo aprendido las lecciones de nuestros anteriores programas como el Tech Nation Cyber Programme, Cyber101 y Hut Zero. Transformaremos el Cheltenham Innovation Centre, que incluye el ciberacelerador «NCSC for Startups», en un centro de innovación verdaderamente internacional: el Centro de Ciberinnovación Nacional (National Cyber Innovation Centre). Aprovecharemos la experiencia de las organizaciones que existen para promover y permitir la cocreación, como la National Security Technology and Innovation Exchange. Y favoreceremos una inversión de alto riesgo en las empresas cibernéticas de nueva creación en sus etapas tempranas, incluido a través de la National Security Strategic Investment Fund, en asociación con el British Business Bank.

80. Una cibereconomía del RU que se ha nivelado considerablemente gracias a un aumento del crecimiento fuera del sureste que ha contribuido a la recuperación de la pandemia de coronavirus (COVID-19) y ha respaldado la actividad económica regional más amplia. Estableceremos la sede central permanente de la NCF en Samlesbury, en el noroeste de Inglaterra, con el fin de impulsar el crecimiento en los sectores tecnológico, digital y de defensa fuera de Londres y ayudar a crear nuevas asociaciones en la región. Incrementaremos nuestro apoyo a los innovadores y emprendedores situados fuera de Londres y el sureste para que desarrollen sus productos y servicios, hagan crecer sus negocios y contraten a personal cualificado. Esto incluye el campus de Golden Valley liderado por el Cheltenham Borough Council, dedicado a apoyar el crecimiento de las empresas de tecnología relacionadas con la cibernética. Y aumentaremos las capacidades de exportación de las empresas de cibernética a lo largo de más regiones del RU mediante la participación de los clústeres cibernéticos regionales y de eventos planificados para mostrar más talento de nuestra industria cibernética a los compradores internacionales.

81. Un número mayor de empresas capaces de ofrecer tecnologías, productos y servicios de ciberseguridad que satisfacen los estándares de calidad verificados de manera independiente, aumentando así la confianza del usuario. Lograremos esto en consonancia con el libro blanco «The Future of NCSC Technology Assurance» (El Futuro del Aseguramiento de la Tecnología del NCSC), publicado por el NCSC en septiembre de 2021, utilizando la marca y la experiencia del NCSC para crear un mercado confiable que ayude a los consumidores del RU a comprar servicios con confianza, mejorar su seguridad y elevar los estándares de ciberseguridad nacional.[23]

[23] NCSC, Libro blanco: The future of NCSC Technology Assurance (2021)

Berta Pappenheim, CEO y Fundadora, Cyberfish Company

CyberFish participó en un programa de acelerador cibernético del Gobierno. Nuestra misión es ayudar a las empresas y los equipos gubernamentales a prepararse para gestionar mejor las interrupciones del negocio, como los ciberincidentes. Para ello, llevamos a cabo ejercicios de simulación de incidentes durante los cuales observamos sus dinámicas de equipo bajo estrés, y los entrenamos sobre cómo realizar mejoras. A muchos asesores se les da bien el aspecto técnico de la respuesta ante los incidentes, y a otros el aspecto del comportamiento del liderazgo y la toma de decisiones. Nosotros hacemos ambas cosas juntos, recurriendo a los conocimientos expertos de ambos lados. Nuestros ejercicios han ayudado a casi 500 líderes de la industria que trabajan en equipos de misiones críticas a lo largo del planeta a cambiar perspectivas y mejorar su trabajo en equipo, lo cual conduce a una mejora en la respuesta ante las crisis y en la toma de decisiones.

¿Está interesado en unirse a la fuerza laboral cibernética o en poner en marcha su propio negocio?

82. Nuestra anterior estrategia hizo un especial hincapié en el desarrollo de la base de habilidades cibernéticas y el sector de los servicios de ciberseguridad en el RU. Tal y como se explica en el contexto estratégico, hemos avanzado considerablemente **en el desarrollo del sector y de las exportaciones**:

Ayudamos a las empresas de cibernética a encontrar mercados internacionales. El RU exportó 4200 millones de libras esterlinas en ciberservicios en 2020.

Cyber Exchange, nuestro ciberportal en línea, que reúne a las empresas de cibernética de todas las regiones del RU.

La asociación Cyber Growth Partnership ha reunido al Gobierno y a la industria para romper las barreras que impiden el crecimiento.

83. Hemos **apoyado a los innovadores para que desarrollen y amplíen sus negocios**, asegurándonos de que el ciberecosistema del RU haya prosperado en los últimos cinco años:

El programa NCSC for Startups está dirigiendo a los innovadores hacia los desafíos estratégicos más importantes, mientras sus empresas de nueva creación ya han participado en más de 160 ensayos corporativos.

LORCA ha ayudado a 72 ciberinnovadores a recaudar más de 200 millones de libras esterlinas y a obtener unos ingresos de más de 37 millones de libras esterlinas.

Cyber Runway ayuda a los innovadores a lanzar, desarrollar y ampliar sus negocios, basándose en el éxito de Hutzero y Cyber101.

84. Hemos estado trabajando para reducir el déficit anual de 10 000 profesionales **que se incorporan a la fuerza laboral cibernética**:[24]

El programa de becas CyberFirst ayuda a los estudiantes universitarios y aporta cientos de personas con experiencia laboral a la fuerza laboral cibernética todos los años.

Actualmente existen cuatro estándares de formación de aprendices en cibernética que han sido diseñados por la industria y tres ciberofertas para resultados de aprendizaje iniciales ofrecidos a través de la iniciativa «Courses for Jobs» del Departamento de Educación (DfE, *por sus siglas en inglés*).

Se han organizado nueve campamentos de entrenamiento en ciberseguridad apoyados por la National Skills Fund, que han dirigido a las personas hacia emocionantes carreras en cibernética, con planes para celebrar más campamentos de este tipo todos los años durante el periodo de gastos.

85. Hemos estado **profesionalizando la fuerza laboral cibernética**, haciendo que sea más fácil para las empresas entender qué habilidades necesitan y que a las personas les resulte más sencillo saber qué información necesitan:

El Consejo de Ciberseguridad del RU es la primera autoridad profesional en el ámbito de la ciberseguridad del mundo. Ha comenzado a establecer estándares profesionales claros y coherentes, aprovechando todo el trabajo que los organismos profesionales existentes han llevado a cabo hasta la fecha. El Consejo buscará identificar claramente las cualificaciones más eficaces de entre la amplia gama disponible actualmente.

El Cyber Security Body of Knowledge (CyBOK) fundamenta la educación y la formación profesional en el sector de la ciberseguridad.

[24] DCMS, Entender la base de contratación de la ciberseguridad (2021)

86. Hemos estado trabajando para **garantizar que todo el mundo pueda unirse a la fuerza laboral cibernética**, abordando la desigualdad en un sector donde solo un 16 % de los empleados son mujeres y únicamente un 3 % de los altos cargos están ocupados por mujeres y minorías étnicas.[25]

Los cursos de CyberFirst y el programa Discovery han hecho partícipes a casi 300 000 jóvenes de entre 11 y 17 años de edad en los últimos cinco años.

La organización UK Cyber Cluster Collaboration está forjando asociaciones entre la industria, las escuelas y los institutos para garantizar que haya oportunidades y experiencia disponibles a lo largo de todas las regiones.

El programa Cyber Choices de la NCA está ayudando a los jóvenes a tomar decisiones fundamentadas y a usar sus habilidades cibernéticas de una manera legal, aumentando la concienciación y facilitando mejores alternativas y prácticas laborales.

[25] HMG, Habilidades de ciberseguridad en el mercado laboral del RU (2021)

Pilar 2: ciberresi-liencia

Construir un RU digital resiliente y próspero

87. La ciberseguridad y la resiliencia son esenciales para nuestros objetivos estratégicos más amplios como ciberpoder: sin ellas, no podemos pretender aprovechar al máximo el potencial transformador de las tecnologías digitales para reconstruir de una manera mejor, más justa y sólida, y para proteger la ventaja estratégica del RU en el ciberespacio. Debemos continuar creando unas fuertes ciberdefensas, tomando medidas para proteger las redes digitales, la información y los activos del RU a nivel nacional, local e individual y asegurarnos de que estos sean resilientes cuando se produzcan incidentes.

88. Y pese a que en este capítulo nos centramos en la ciberresiliencia, para que esta sea plenamente eficaz deberá formar parte de un esfuerzo conjunto de toda la sociedad para mejorar la resiliencia del RU. La próxima Estrategia de Resiliencia Nacional (National Resilience Strategy), un compromiso clave de la Revisión Integrada, establecerá el enfoque global hacia la resiliencia nacional.

89. En la última década se han producido avances importantes en la mejora de nuestra ciberresiliencia, con la creación del Centro de ciberseguridad nacional (NCSC), una disponibilidad cada vez mayor de asesoramiento, orientación y otras herramientas, y la implementación de legislación, incluidas las Normas de Redes y Sistemas de la Información (las «normativas NIS»), el Reglamento General de Protección de Datos y la Ley de Protección de Datos de 2018. No obstante, continúa habiendo algunas lagunas importantes. Las violaciones cibernéticas afectan al Gobierno, a empresas, organizaciones y personas, y muchas organizaciones continúan notificando cifras elevadas de ciberataques o violaciones de la ciberseguridad.

90. Nosotros nos basamos en los fundamentos de la estrategia anterior, desarrollamos nuestro enfoque y logramos cambios en la ciberresiliencia del RU, poniendo un énfasis especial en:

- ampliar nuestro trabajo para hacer que Internet sea un lugar automáticamente más seguro, evitar ataques, desarrollar protecciones básicas en beneficio de todas las empresas, las organizaciones y los ciudadanos del RU y aumentar el apoyo disponible para aquellos menos capaces de protegerse a sí mismos en línea
- establecer la ambición de que el Gobierno actúe como un ejemplo de las prácticas recomendadas en la ciberseguridad
- integrar la ciberseguridad como una parte básica de los buenos negocios mediante un uso mejor de las regulaciones y otros incentivos, y aprovechar el poder de nuestros conocimientos sobre amenazas para construir comunidades capaces de defenderse
- fundamentar todo esto con estándares, pruebas y datos mensurables objetivamente y pasar de recabar datos a actuar sobre la base de estos

91. En esta estrategia, el concepto de ciberresiliencia tiene tres aspectos clave. En primer lugar, debemos entender cuál es la naturaleza del **riesgo**. En segundo lugar, necesitamos actuaciones que **protejan** los sistemas con el fin de evitar los ciberataques y resistir frente a ellos. Por último, debemos reconocer que continuarán produciéndose algunos ataques y que debemos prepararnos para ellos, siendo lo suficientemente **resilientes** como para minimizar su impacto y ser capaces de recuperarnos.

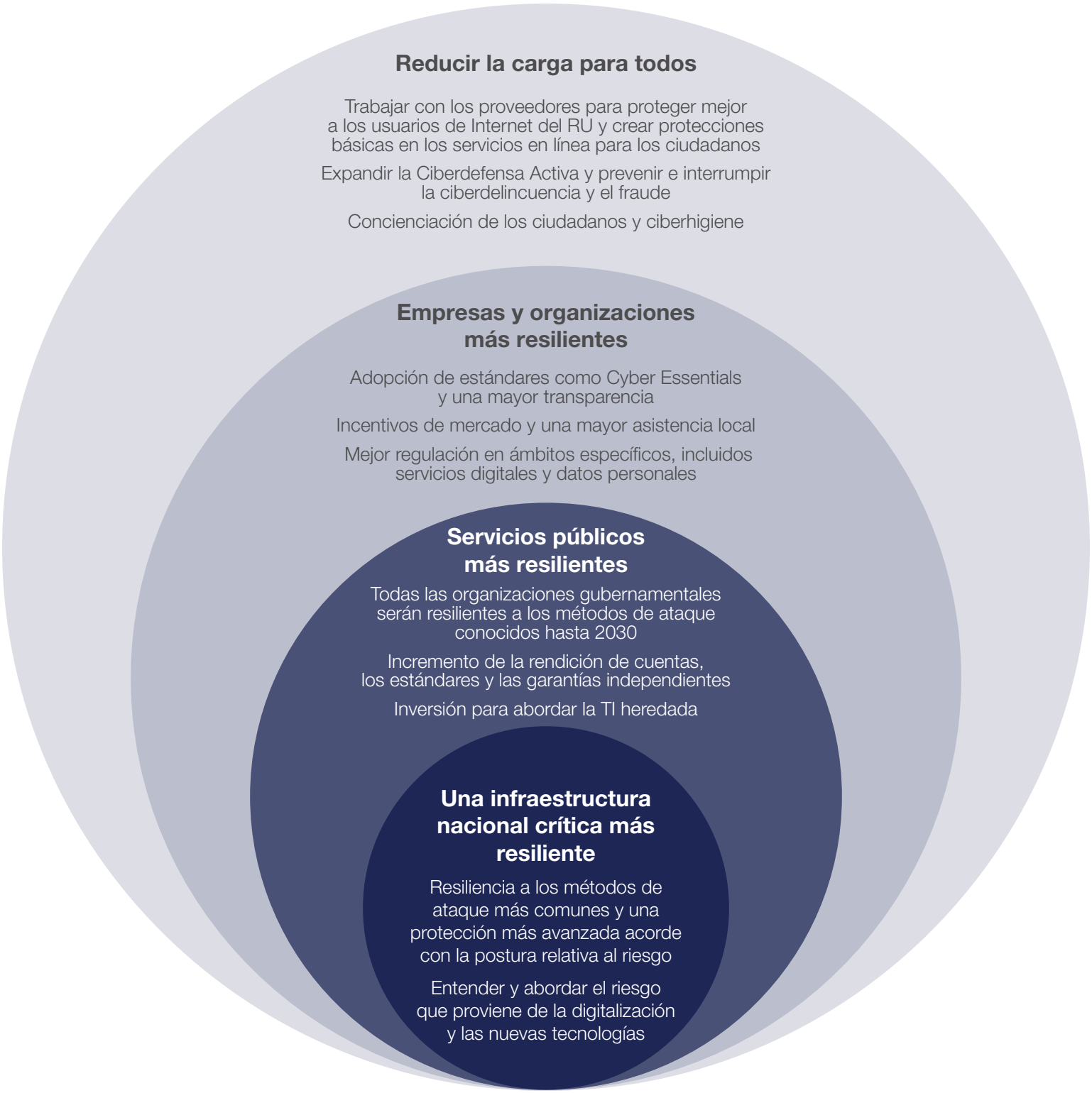
92. Nuestro enfoque estará adaptado a cada tipo de público, con el apoyo de las capacidades nacionales que nos permiten abordar riesgos sistémicos. Los públicos que tenemos la intención de proteger y sobre quienes queremos influir son ciudadanos, empresas y organizaciones del RU, el Gobierno y el sector público, y aquellos que gestionan nuestra infraestructura nacional crítica (proporcionando servicios básicos de los que todos dependemos, como agua potable, electricidad, finanzas, transporte y telecomunicaciones).

93. Primero nos centraremos en adoptar medidas para proteger el entorno digital para todos los usuarios de Internet del RU, evitar ataques, incorporar una seguridad básica a productos y servicios y ayudar a las personas y a las pequeñas empresas y organizaciones llevando a cabo actuaciones básicas para mejorar la ciberseguridad. Cuando lleguemos a aquellos con una mayor responsabilidad y capacidad de añadir capas de seguridad y resiliencia adicionales y proporcionales al riesgo, eso conducirá a un mayor nivel de protección esperado para los servicios públicos y esenciales clave de los que dependen nuestros ciudadanos y nuestra economía.

94. Este debe ser un esfuerzo conjunto entre el Gobierno y todas las partes de la economía y la sociedad. Las juntas de las empresas y organizaciones tienen la responsabilidad de gestionar su propio ciberriesgo. Nuestro propósito consiste en establecer expectativas claras sustentadas por un marco de incentivos, apoyo y regulaciones adecuado que permita mejorar y trasladar la carga que supone el riesgo para la ciberseguridad de los usuarios hacia aquellos que cuentan con las mejores herramientas para gestionarlo.

95. Necesitamos que los departamentos gubernamentales, el sector público más amplio y los operadores regulados de la infraestructura nacional crítica (CNI) eleven su nivel y gestionen sus riesgos de una manera más proactiva. Esperamos que las grandes empresas y organizaciones, incluidos los proveedores de servicios y plataformas digitales, se hagan más responsables con respecto a sus sistemas, servicios y clientes como una parte básica de la gestión de sus negocios. A cambio, el Gobierno hará más para proteger el entorno digital, abordar riesgos sistémicos y proporcionar apoyo a través de asesoramiento, herramientas y acreditación en el mercado, además de desarrollar las habilidades que hagan posible la mejora.

96. Nuestros esfuerzos por promover la ciberresiliencia en el RU también deben formar parte de nuestra implicación a nivel internacional. La intensificación de la globalización de las cadenas de suministro, las plataformas de TI, las empresas multinacionales y el propio Internet implica que no podemos mejorar la ciberseguridad del RU de manera aislada. Para responder a ese desafío deberemos comprender mejor los vínculos entre la ciberresiliencia global y la del RU, abordar áreas de alto riesgo y trabajar con socios internacionales para generar una resiliencia que facilite la transformación digital, la seguridad y el comercio para nuestro beneficio mutuo, tal y como se explica en el Pilar 4: capítulo sobre el liderazgo global.


Reducir la carga para todos
Trabajar con los proveedores para proteger mejor a los usuarios de Internet del RU y crear protecciones básicas en los servicios en línea para los ciudadanos
Expandir la Ciberdefensa Activa y prevenir e interrumpir la ciberdelincuencia y el fraude
Concienciación de los ciudadanos y ciberhigiene
Empresas y organizaciones más resilientes
Adopción de estándares como Cyber Essentials y una mayor transparencia
Incentivos de mercado y una mayor asistencia local
Mejor regulación en ámbitos específicos, incluidos servicios digitales y datos personales
Servicios públicos más resilientes
Todas las organizaciones gubernamentales serán resilientes a los métodos de ataque conocidos hasta 2030
Incremento de la rendición de cuentas, los estándares y las garantías independientes
Inversión para abordar la TI heredada
Una infraestructura nacional crítica más resiliente
Resiliencia a los métodos de ataque más comunes y una protección más avanzada acorde con la postura relativa al riesgo
Entender y abordar el riesgo que proviene de la digitalización y las nuevas tecnologías

Objetivo 1: mejorar el entendimiento del ciberriesgo para impulsar actuaciones más eficaces en relación con la ciberseguridad y la ciberresiliencia

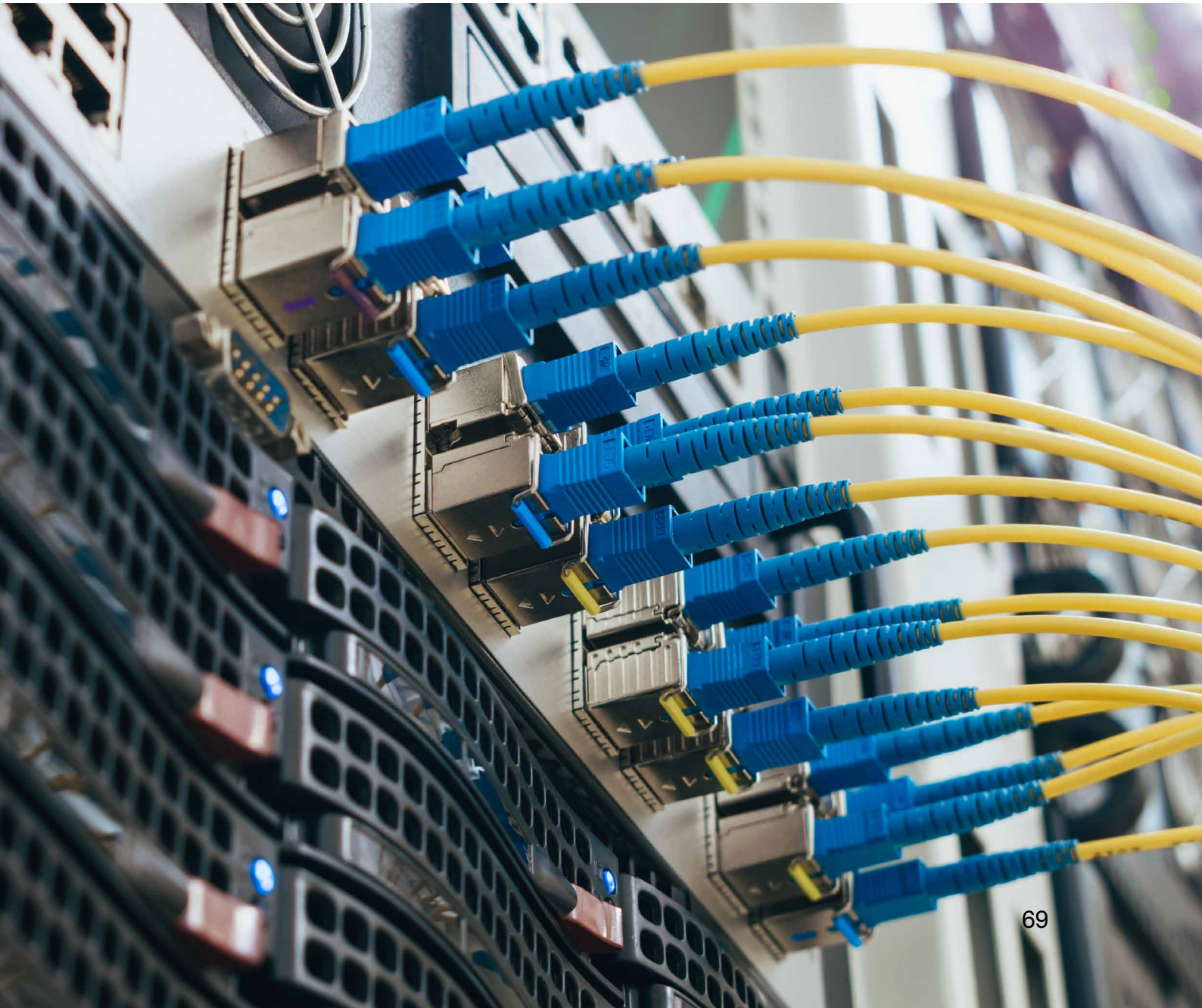
97. Ofreceremos una alianza mucho más estrecha entre Gobierno, empresas y organizaciones para impulsar el entendimiento colectivo del riesgo, guiar la priorización y justificar la adopción de medidas. Apoyaremos a los ciudadanos colaborando con empresas y organizaciones que ofrecen servicios a los consumidores; y reforzaremos aún más la capacidad del Gobierno de identificar riesgos transversales. Lograremos los resultados siguientes hasta 2025:

98. El Gobierno posee un entendimiento estratégico y actualizado del ciberriesgo al que se expone la nación y utiliza ese entendimiento para identificar riesgos sistémicos, comunicar prioridades e impulsar la estrategia y los resultados. Mantendremos y generaremos un mayor valor a partir de inversiones importantes efectuadas para «entender la amenaza» de la anterior Estrategia de Ciberseguridad Nacional y aprovecharemos los esfuerzos actuales para entender el riesgo en un mundo cada vez más interconectado. Esto incluirá identificar dónde están demasiado concentradas las cadenas de suministro digitales y trabajar con socios internacionales para gestionar los riesgos colectivos. Asimismo, mejoraremos nuestro registro de los delitos relativos a la Ley sobre el Uso Indebido de Ordenadores (CMA, *por sus siglas en inglés*), entendiendo los vínculos entre las violaciones de datos y la criminalidad asociada, y aumentando nuestros conocimientos de cómo los delitos relacionados con la CMA están facilitando otros tipos de actividades delictivas.

99. El Gobierno está dando ejemplo en su entendimiento del ciberriesgo. Adoptaremos el Marco de Evaluación Cibernético (CAF, *por sus siglas en inglés*) del NCSC como el marco de garantía para todos los departamentos gubernamentales, y mapearemos los sistemas críticos y los proveedores comunes. Estableceremos un nuevo Centro de Cibercoordinación del Gobierno (GCCC, *por sus siglas en inglés*) y un Servicio de Notificación de Vulnerabilidades Interministerial (VRS, *por sus siglas en inglés*) para que el Gobierno pueda «defenderse como uno» en el momento de gestionar incidentes, vulnerabilidades y amenazas. El objetivo del VRS será establecer relaciones valiosas y de confianza con la comunidad de la investigación de la seguridad, logrando con ello una reducción de las vulnerabilidades de todo el Estado. Continuaremos ofreciendo apoyo y coordinándonos con iniciativas similares en los Gobiernos descentralizados, como la propuesta de establecimiento de una función de coordinación central para la ciberresiliencia en Escocia.

100. A lo largo de la CNI del RU, tendremos un entendimiento más sofisticado del ciberriesgo. Incrementaremos la adopción del Marco de Evaluación Cibernético (CAF) o de equivalentes a lo largo de los sectores de la CNI, y mejoraremos la comparabilidad con otros marcos actuales de notificación y evaluación de la ciberseguridad. Llevaremos a cabo revisiones de criticidad y mapearemos las dependencias en la CNI y sus cadenas de suministro. Crearemos alianzas más sólidas con los propietarios y operadores de la CNI para mejorar el acceso a la información sobre amenazas y riesgos, y acordaremos posturas con respecto al riesgo. Y trabajaremos para entender nuevos riesgos o dónde están emergiendo nuevas CNI como consecuencia de la digitalización y las nuevas tecnologías, lo cual incluye prioridades más amplias como la transición a unas emisiones netas cero.

101. Las empresas y organizaciones del RU poseen un mejor entendimiento de los ciberriesgos y de sus responsabilidades a la hora de gestionarlos. Ayudaremos a las organizaciones a entender mejor cuál es el riesgo para sus clientes, lo cual incluye cómo podrían utilizarse los datos que conservan para facilitar delitos como el fraude, el robo de identidad o la extorsión. Y compartiremos más información de investigaciones y datos sobre la prevalencia y el impacto de los ciberataques y los avances relativos que los sectores están realizando para mejorar la ciberseguridad.



Objetivo 2: evitar y resistir frente a los ciberataques de una manera más eficaz mejorando la gestión del ciberriesgo dentro de las organizaciones del RU, y brindando una mayor protección a los ciudadanos

102. Nuestro enfoque hacia la prevención y la resistencia frente a los ciberataques da por sentado lo siguiente: (i) que las organizaciones tienen la responsabilidad de adoptar medidas para gestionar su propio ciberriesgo, pero que se necesitan marcos más sólidos de rendición de cuentas y buena gobernanza a nivel directivo para convertir eso en una prioridad; (ii) que el Gobierno tiene un papel que desempeñar trabajando con la industria para adoptar medidas que reduzcan directamente el riesgo a escala en aquellos ámbitos donde se encuentre en una posición única para hacerlo; y (iii) debemos asegurarnos de que las personas, los autónomos y las pequeñas empresas y organizaciones tengan a su disposición el apoyo y la orientación necesarios para gestionar su ciberriesgo. Lograremos los resultados siguientes hasta 2025:

103. El Gobierno ha reducido los daños al RU a escala y ha disminuido la carga sobre los ciudadanos del RU. Actuaremos cada vez más en las fases iniciales en nombre de todos los usuarios de Internet del RU ampliando nuestras medidas de Ciberdefensa Activa para respaldar a un mayor abanico de sectores, incluidas las organizaciones benéficas, el mundo académico, las pequeñas y medianas empresas y los ciudadanos. Y reforzaremos las protecciones a los servicios en línea a través de una participación y compartición de información mayores con la industria.

104. Esta labor complementa a otras prioridades del Gobierno dirigidas a proteger a los ciudadanos en línea, como el Proyecto de Ley de Seguridad en Línea y la política dirigida a combatir los delitos económicos como el fraude.

105. Eso significará colaborar más estrechamente con los sectores implicados, como los proveedores de servicios en línea, telecomunicaciones, tecnología, banca y comercio minorista para proteger mejor a los usuarios de Internet del RU. Esto incluye: hacer que sea más difícil registrar sitios web para fines ilegales, aumentar la retirada y el bloqueo de contenido malicioso en línea, mejorar la recuperación y la devolución de credenciales robadas y mejorar la seguridad de la infraestructura de telecomunicaciones del RU. Asimismo, desarrollaremos opciones para ofrecer respaldo legal a las protecciones de los ciudadanos en caso de que los acuerdos voluntarios sean insuficientes.

106. Nuestros esfuerzos por reducir el daño a escala también incluirán abordar los riesgos sistémicos de la cadena de suministro digital. Cuando sea necesario, intervendremos para fomentar la diversificación de la cadena de suministro, al igual que hacemos en las telecomunicaciones; fortaleceremos nuestra seguridad económica colectiva con enfoques robustos, predecibles y proporcionados basados en la compartición de información hacia la investigación de inversiones directas extranjeras (FDI, *por sus siglas en inglés*) en sectores esenciales, y estableceremos requisitos claros para proveedores críticos y frecuentes del Gobierno.

107. Las funciones críticas del Gobierno están considerablemente reforzadas ante los ciberataques, y todos los organismos gubernamentales (a lo largo de todo el sector público) serán resilientes frente a vulnerabilidades y métodos de ataque conocidos hasta 2030. Nuestro objetivo es que el sector

público del RU se convierta en un ejemplo de prácticas recomendadas. Para lograr ese resultado, publicaremos la primera Estrategia de Ciberseguridad del Gobierno. Esta se centrará en unos procesos de gestión del riesgo, una gobernanza y una rendición de cuentas más eficaces, unas capacidades desarrolladas y utilizadas a nivel central (incluida la Ciberdefensa Activa), una monitorización más exhaustiva de los sistemas, redes y servicios, una respuesta ante los incidentes más rápida y a escala y una inversión en habilidades, conocimientos y una cultura que promueva el cambio sostenible.

108. Los ciberriesgos para la infraestructura nacional crítica del RU están sometidos a una gestión más eficaz. Por definición, estos son los servicios de los que más depende el país. Continuaremos trabajando estrechamente con los operadores para lograr una resiliencia frente a los métodos de ataque comunes lo más rápido posible y para aplicar más protecciones avanzadas donde sea apropiado. Para los operadores de servicios esenciales nombrados en virtud de las normativas NIS, eso significa como mínimo cumplir el estándar de referencia establecido por las autoridades competentes de cada sector.

109. Para lograr ese resultado, analizaremos la capacidad del Gobierno de hacer rendir cuentas a los operadores de la CNI para garantizar que inviertan en la ciberseguridad de sistemas críticos y gestionen sus riesgos de una manera eficiente, lo cual incluye hacerlo desde sus cadenas de suministro. Reforzaremos el marco normativo para mejorar su cobertura, poderes y agilidad para adaptarse, dentro del contexto de un riesgo para la seguridad nacional más amplio y de una amenaza y una tecnología que cambian rápidamente. Esto comenzará con una consulta sobre las reformas de las normativas NIS, implementando el nuevo marco de seguridad para los proveedores de telecomunicaciones del RU y desarrollando un marco normativo proporcionado que garantice que el sistema energético inteligente y flexible que necesita el RU para alcanzar el objetivo de unas emisiones netas cero sea seguro y resiliente frente a los ciberataques.

110. Además de lo anterior, haremos lo siguiente: mejorar las capacidades de los reguladores; invertir en habilidades para mejorar la capacidad de los operadores de la CNI para atraer, desarrollar y retener a ciberprofesionales (véase el capítulo sobre el Ciberecosistema del RU); y apoyar la gestión de los riesgos para la cadena de suministro por parte de los operadores mejorando la interacción con proveedores críticos y explorando la gama completa de recursos, desde la orientación hasta las propuestas legislativas y de adquisición.

111. La infraestructura de la que depende nuestro uso de los datos es segura y resiliente. Esta infraestructura es un activo nacional crucial que respalda nuestra economía, ofrece servicios públicos e impulsa el crecimiento. Asumiremos un papel más importante para garantizar que los datos estén lo suficientemente protegidos durante su tratamiento, cuando estén en tránsito o se almacenen a escala, por ejemplo, en centros de datos externos. Crearemos un marco de gestión del riesgo más sólido para garantizar una seguridad y una resiliencia mayores a lo largo de todo el sector e implementaremos las disposiciones establecidas en la Ley de Inversiones y Seguridad Nacional de 2021 con el propósito de fortalecer el análisis de las inversiones. Consolidaremos nuestro trabajo con los socios internacionales para garantizar que el acceso cada vez mayor a los datos y los flujos globales no aumenten los riesgos de seguridad a los que se enfrenta el RU, así como para abordar los desafíos a la seguridad que plantea la recopilación masiva de datos.

112. También consideraremos la creciente criticidad de los servicios de infraestructura de datos del RU a la hora de sostener la economía y su papel en la infraestructura nacional crítica. Estas medidas se ajustan a los compromisos establecidos en la Estrategia de Datos Nacional y la Revisión Integrada.

113. Un número cada vez mayor de empresas y organizaciones del RU está manejando de manera proactiva sus ciberriesgos y tomando medidas para mejorar su ciberresiliencia. Facilitaremos apoyo e impulsaremos los cambios en el comportamiento a través del desarrollo de incentivos del mercado que fomenten una ciberseguridad eficaz. Cuando sea necesario, esto se complementará con una legislación específica que garantice que aquellos que tienen la mayor responsabilidad de gestionar el ciberriesgo lo estén haciendo de una manera eficaz, y que la legislación sobre ciberseguridad del RU siga siendo efectiva en vista de los riesgos y tecnologías en constante evolución.

114. En apoyo de esos objetivos, trabajaremos cada vez más con actores influyentes en el mercado (como responsables de adquisición, instituciones financieras, inversores, auditores y aseguradoras) para incentivar las buenas prácticas en ciberseguridad a lo largo de la economía. Propondremos mejoras para que las empresas informen sobre la resiliencia frente a los riesgos, incluidos los ciberriesgos. Esto ofrecerá a los inversores y accionistas una idea mejor sobre cómo las empresas están gestionando y mitigando los riesgos materiales para sus negocios. Y continuaremos promoviendo la adopción de acreditaciones y estándares como el programa de certificación Cyber Essentials, así como la participación a nivel directivo en la gestión del ciberriesgo.

115. La legislación específica se centrará principalmente en sectores donde el impacto potencial de un ciberataque es mayor, incluidos proveedores de ciertos servicios esenciales y digitales, la protección de datos en la economía más amplia y para empresas de mayor tamaño. Esto complementará el Plan de Normativa Digital (Plan for Digital Regulation), que inicialmente se centrará en las normativas que rigen la seguridad de las Normas de Redes y Sistemas de la Información (NIS), según lo indicado anteriormente y en el capítulo de Tecnología y en los próximos pasos para reformar el régimen del RU para la protección de los datos personales.

116. En la Revisión de la Normativa y los Incentivos en materia de Ciberseguridad se abordarán en mayor detalle las actuaciones que debemos llevar a cabo para mejorar la resiliencia y la ciberseguridad de las empresas en las compañías y organizaciones del RU.

117. Encontrar asesoramiento técnico, herramientas de autoayuda y productos y servicios garantizados resulta fácil y es algo que mejora continuamente, con un especial énfasis en ayudar a los ciudadanos, los autónomos y las pequeñas organizaciones. Continuaremos desarrollando directrices prácticas, oportunas y técnicamente precisas, así como herramientas de autoayuda, a través del NCSC. Nos aseguraremos de que los mensajes sean coherentes y claros y de que lleguen a través de los canales más eficaces, ya sea a través de la campaña Cyber Aware, el sitio web del NCSC, el Gobierno, las redes de los cuerpos y fuerzas de seguridad o nuestras asociaciones con la industria. Asimismo, ofrecemos un mayor apoyo a nivel local. A través del «Derecho Digital», continuaremos financiando plenamente las cualificaciones en habilidades digitales esenciales para los adultos que las necesitan, asegurándonos de que los estudiantes posean las habilidades digitales básicas que precisan para mantenerse seguros y ser responsables en línea. Y ayudaremos a las empresas y organizaciones a moverse en el complejo mercado de la ciberseguridad, ampliando nuestros marcos a productos y servicios garantizados y desarrollando ofertas comerciales centradas en Cyber Essentials que facilitarán el acceso de las pequeñas empresas a un asesoramiento básico.

Elis Power, Agente de Cyber Protect/Prevent, Tarian Regional Cyber Crime Unit

La Unidad de Ciberdelincuencia Regional Tarian (TARIAN-RCCU, *por sus siglas en inglés*) es un equipo multidisciplinario de agentes de policía y personal adscrito de la policía de Gales. Su misión consiste en contribuir a la creación de un ciberentorno más seguro en el sur de Gales.

El Agente Elis Power de Cyber Protect/Prevent forma parte del equipo de trabajo:

«Puede parecer un cliché, pero no hay una jornada típica en la unidad. Según el día, puedo ser responsable de realizar presentaciones con asesoramiento para departamentos de policía internos, u organizaciones externas, con el fin de garantizar que tengan un entendimiento sólido de cómo protegerse a sí mismos y a su lugar de trabajo frente a las ciberamenazas. Pero también podría estar realizando una presentación para jóvenes en escuelas sobre temas como la seguridad en Internet o la Ley sobre el Uso Indebido de Ordenadores de 1990. Con frecuencia asisto a reuniones con agencias y fuerzas colaboradoras para discutir nuevas amenazas y guías asociadas para nuestras audiencias. También me relaciono con organizaciones de las cuales hemos recibido alertas sobre vulnerabilidad, participo en operaciones nacionales, asisto a eventos y conferencias relevantes y dedico tiempo a mejorar continuamente mis habilidades y mi base de conocimientos».

Objetivo 3: reforzar la resiliencia a nivel nacional y organizativo para prepararnos frente a los ciberataques, responder y recuperarnos de ellos

118. Pese a los esfuerzos por entender el riesgo y tomar medidas preventivas, seguirán produciéndose algunos incidentes. Debemos fortalecer las capacidades de respuesta y gestión de incidentes a lo largo de todas las organizaciones para minimizar el daño causado y ofrecer un mejor apoyo a las víctimas. Lograremos los resultados siguientes hasta 2025:

119. La gestión y coordinación estratégicas de la respuesta a ciberincidentes importantes a nivel nacional por parte del RU es aún más eficaz. Aprovecharemos la experiencia del Gobierno a la hora de responder a ciberincidentes importantes, asegurándonos de utilizar las lecciones identificadas para mejorar nuestras políticas y procesos. Compartiremos nuestra experiencia de gestión de crisis con socios internacionales y con la industria y, a su vez, identificaremos las prácticas recomendadas de otros lugares a fin de mejorar nuestra preparación y nuestros procesos.
Nos aseguraremos de que el NCSC y los equipos de gestión de incidentes de las autoridades del orden público cuenten con la experiencia y las herramientas necesarias para responder a la amplia variedad de incidentes en constante cambio y de que puedan coordinar una respuesta nacional frente a amenazas prioritarias.

120. Resulta más fácil denunciar los ciberincidentes y las víctimas reciben un apoyo mejor. La denuncia de información también se utilizará para evitar futuros incidentes y ayudar a las autoridades del orden público a investigar, interrumpir y enjuiciar a los ciberdelincuentes. Para ello, ofreceremos un nuevo servicio nacional de denuncia y análisis de ciberdelitos y fraude que reemplazará a Action Fraud hasta 2025. Fomentaremos una mayor denuncia de los ciberincidentes por otros medios como, por ejemplo, a través de una nueva capacidad de notificación de empresas de la City of London Police. En los sectores regulados, habilitaremos a los reguladores para que puedan exigir la notificación de una gama más amplia de incidentes, incluidos los «conatos de incidente». La implantación de la Unidad de Atención a las Víctimas de Delitos Económicos mejorará el apoyo y la orientación disponibles para las víctimas tras lo que puede ser una experiencia estresante y nociva.

121. El Gobierno y la CNI están más preparados para responder a incidentes y recuperarse de ellos, lo cual incluye una mejor planificación de los incidentes, así como ejercicios regulares. Ayudaremos al Gobierno del RU y a los operadores de la CNI a encontrar los servicios de ciberejercicios y gestión de incidentes que necesitan del mercado mediante la ampliación del programa acreditado del NCSC de Respuesta ante Ciberincidentes y a través de un nuevo programa de ejercicios.

122. Dentro del Gobierno, se mejorarán las capacidades de monitorización y detección dentro de los departamentos y a lo largo del estado digital del Gobierno. Nos aseguraremos de identificar las lecciones y de utilizarlas para mejorar nuestras políticas y procesos, compartir la experiencia en gestión de crisis con nuestros socios internacionales y con la industria y cerciorarnos de que nuestros equipos de gestión de incidentes cuenten con la experiencia, la capacidad y las habilidades necesarias para responder a toda la gama de incidentes en constante evolución.

123. En cuanto a la CNI, estableceremos requisitos claros para ejercer y poner a prueba nuestra simulación de adversarios a lo largo de los operadores de la CNI, y estimularemos la innovación y la colaboración en los ejercicios y la respuesta ante los incidentes, considerando la aplicación de modelos como el Centro de Cibercolaboración del Sector Financiero (Financial Sector Cyber Collaboration Centre). Y como parte de nuestras ambiciones en materia de tecnología (señaladas en el próximo capítulo), crearemos un laboratorio nacional de seguridad de la tecnología operativa como centro de excelencia para ensayar, llevar a cabo ejercicios y formación sobre las tecnologías industriales críticas con el fin de aumentar nuestras capacidades en esa área, en colaboración con la industria, el mundo académico y los socios internacionales.

124. Los negocios y las organizaciones del RU tienen un entendimiento más claro de qué hacer en caso de que se produzca un incidente, a quién llamar, quién puede ayudar y cómo recuperarse. Mejoraremos el acceso a la formación y los ejercicios, con el apoyo de servicios de la industria garantizados, incluido un nuevo programa de Respuesta ante Ciberincidentes y un servicio de Ejercicios de Ciberincidentes. Nos aseguraremos de que las víctimas individuales de ciberdelitos puedan acceder a una asistencia sistemática a nivel nacional por parte de las autoridades del orden público y animaremos a las pequeñas empresas y organizaciones a sacar partido a la asistencia local, como la de los Centros de Ciberresiliencia regionales.

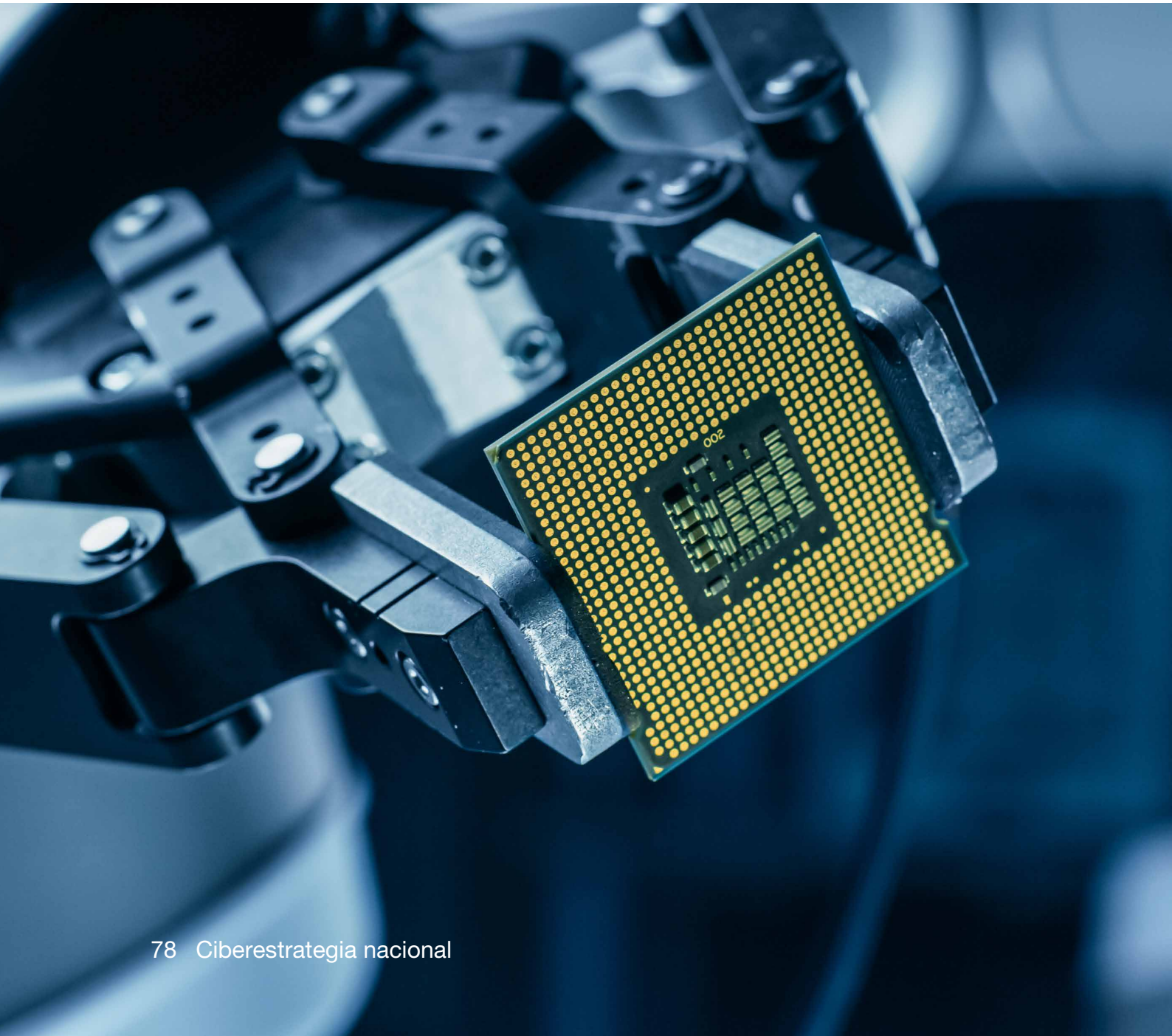
Daniel Ng, CEO, CyberOwl

CyberOwl se benefició del programa de desarrollo cibernético del Gobierno. Proporcionamos análisis y monitorización de la ciberseguridad para activos operativos en los sectores marítimo y de la CNI. El impulso hacia la sostenibilidad exige una mayor conectividad y digitalización de los activos sobre el terreno, con la consecuente exposición a los ciberriesgos. CyberOwl ayuda a los operadores a identificar y mapear sus activos, lograr una detección temprana de los ciberriesgos y demostrarse a sí mismos y a los reguladores que los han protegido. Trabajamos con los mayores operadores de activos marítimos del mundo a lo largo de la región EMEA y Asia-Pacífico con el fin de mejorar la resiliencia de la cadena de suministro logística de transporte global. En 2021, multiplicamos nuestras reservas por 14 y duplicamos las operaciones en el Reino Unido y Singapur.

Jen Ellis, Vicepresidente de Asuntos Comunitarios y Públicos, Rapid7

Mi trabajo implica hablar con los profesionales y líderes de la seguridad de organizaciones de todos los tamaños y sectores para entender los desafíos a los que se enfrentan e intentar identificar soluciones que les ayuden a mejorar su ciberseguridad. Constantemente oigo que las organizaciones están desbordadas y no saben hacia dónde dirigir sus esfuerzos, cómo comenzar o cómo lograr avances. También puede resultar difícil para el personal técnico conseguir la aceptación por parte del equipo directivo. Contar con una ciberestrategia clara, coherente y transparente por parte del Gobierno puede ayudar a abordar esto. Ofrece al personal técnico algo que destacar como parte de sus discusiones con el equipo directivo. Y también identifica áreas esenciales de enfoque, además de un camino potencial hacia la madurez. La ciberseguridad continúa siendo enormemente compleja e interminable, pero gracias a la ampliación de la ciberestrategia existe un mayor entendimiento de su importancia y una sensación de que estamos todos juntos en esto.

Pilar 3:
ventaja tecnológica



Tomar la iniciativa en las tecnologías que son fundamentales para el ciberpoder

125. Algunas tecnologías serán esenciales para conformar el futuro del ciberespacio. Los países que sean capaces de establecer un papel predominante en estas tecnologías estarán en una posición privilegiada para influir en su diseño y despliegue, serán más capaces de proteger su seguridad y su ventaja económica y también serán más rápidos a la hora de explotar oportunidades de lograr importantes avances en las cibercapacidades. A medida que la tecnología se convierta en una herramienta cada vez más importante de poder geopolítico, la competición en ese ámbito se intensificará.

126. Para el RU, buscar una ventaja estratégica a través de la ciencia y la tecnología y el acceso a los datos del cual depende, será una condición previa para alcanzar nuestros objetivos más amplios como ciberpoder. En estrategias anteriores, el Gobierno ha adoptado medidas para estimular la investigación y la innovación en las tecnologías de la ciberseguridad como, por ejemplo, a través de programas de acelerador para empresas de nueva creación y los Centros Académicos de Excelencia en la Investigación sobre la Ciberseguridad (Academic Centres of Excellence in Cyber Security Research) y para fomentar el desarrollo de dispositivos de consumo que sean «seguros por diseño». Sin embargo, ahora necesitamos un enfoque más ambicioso y proactivo hacia la participación en las tecnologías críticas y evitar depender demasiado de competidores y adversarios.

127. La Revisión Integrada establece planes para convertir al RU en un superpoder en ciencia y tecnología y utilizar esas dos disciplinas para construir y mantener nuestra ventaja estratégica. Esta estrategia respalda la labor del Consejo Nacional de Ciencia y Tecnología (National Science and Technology Council) y de la Oficina de Estrategia en Ciencia y Tecnología (Office of Science and Technology Strategy) en pro de ese objetivo, además de complementar las estrategias del RU en áreas como la inteligencia artificial, las tecnologías cuánticas y los datos.

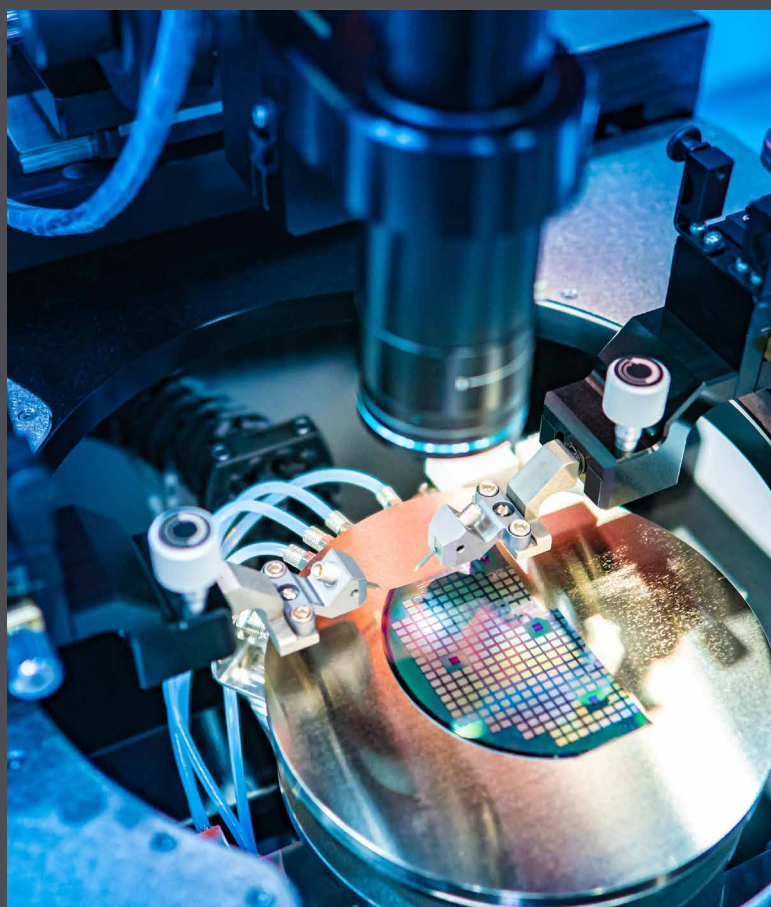
128. Fortaleceremos nuestra capacidad, liderada por la experiencia técnica del Centro de ciberseguridad nacional (NCSC) y otros actores a lo largo del Gobierno, para identificar las áreas de la tecnología que son más críticas para nuestro ciberpoder. Adoptaremos decisiones estratégicas a nivel nacional sobre las prioridades, trabajando dentro del marco de Responsabilidad-Colaboración-Acceso establecido en la Revisión Integrada. En determinadas áreas invertiremos en actividades de investigación y desarrollo, así como en las alianzas estratégicas necesarias para mejorar las capacidades nacionales del RU, y allí donde dependamos de los mercados globales trabajaremos con la industria, los reguladores y los socios internacionales para promover cadenas de suministro confiables y diversas, y para desarrollar los estándares con el fin de garantizar que las tecnologías sean seguras y abiertas. Asimismo, reforzaremos la capacidad del RU de explotar y proteger los volúmenes de datos e información cada vez más ingentes generados por la innovación y que impulsan dicha innovación en las tecnologías emergentes, utilizando como base el marco establecido en la Estrategia de Datos Nacional para maximizar los beneficios para nuestra economía y la sociedad.

Tecnologías esenciales para el ciberpoder

Una diversidad de tecnologías actuales y emergentes serán críticas para el ciberpoder del RU y debemos poder prever, evaluar y actuar en relación con esos cambios. Tenemos previsto priorizar una serie de tecnologías y aplicaciones a medida que vayamos haciendo realidad la estrategia, como las que se indican más abajo. Esta lista no tiene la intención de ser exhaustiva o fija y nuestras prioridades continuarán evolucionando en colaboración con la industria, el mundo académico y los expertos técnicos:

- Tecnología 5G y 6G, y otras formas emergentes de transmisión de datos.
- Inteligencia artificial (IA), incluida la necesidad de proteger los sistemas de IA seguros y el potencial de uso de la IA para mejorar la ciberseguridad en una amplia gama de aplicaciones, como la monitorización de redes.
- Tecnología de cadena de bloques y sus aplicaciones, como las criptomonedas y las finanzas descentralizadas.
- Semiconductores, chips microprocesadores, arquitectura de microprocesadores y su cadena de suministro, diseño y proceso de fabricación.
- Autenticación criptográfica, incluida aquella para la gestión de la identidad y el acceso y productos criptográficos altamente confiables.
- Internet de las cosas y tecnologías utilizadas en entornos de consumo, empresariales, industriales y físicos, como los espacios conectados.
- Tecnologías cuánticas, incluida la computación cuántica, la detección cuántica y la criptografía poscuántica.

Esta labor dará apoyo y se ajustará a la consecución de una serie de estrategias y resultados a lo largo del Gobierno como, por ejemplo, la Estrategia de Datos Nacional, la Estrategia de IA Nacional y la Revisión Integrada, así como los resultados centrados en la tecnología que incorpora este pilar.



Objetivo 1: mejorar nuestra capacidad de anticiparnos, evaluar y actuar con respecto a los avances en ciencia y tecnología que son de vital importancia para nuestro ciberpoder

129. Para construir y mantener una ventaja competitiva en las cibertecnologías necesitamos un enfoque coordinado, riguroso y coherente para identificar y analizar áreas críticas de la ciencia y la tecnología y priorizar los esfuerzos nacionales. Esto nos exigirá desarrollar aún más nuestra experiencia técnica y en investigación en el Gobierno y el mundo académico. Integraremos esto con nuevas estructuras del Gobierno para examinar el horizonte de la ciencia y la tecnología y la inteligencia basándonos en las ideas de los expertos de la industria y aprovechando nuestra red en el extranjero para entender las prioridades y los sistemas de socios y competidores internacionales. Lograremos los resultados siguientes hasta 2025:

130. El Gobierno está mejor preparado para analizar ciencia y tecnología nuevas y en desarrollo y entender las implicaciones para la política y la estrategia cibernéticas del RU. Ampliaremos nuestras capacidades de investigación, incluido el nuevo centro de investigación aplicada del NCSC en Manchester, con un enfoque en la tecnología emergente en áreas como los espacios conectados y el transporte, trabajando en colaboración con los expertos de la Government Office for Science (Oficina Gubernamental para la Ciencia) y de otros lugares. Aprovecharemos la experiencia externa al Gobierno, dando apoyo a los cuatro Institutos de Investigación en Ciberseguridad (Cyber Security Research Institutes) y los diecinueve Centros Académicos de Excelencia en la Investigación sobre la Ciberseguridad (Academic Centres of Excellence in Cyber Security Research), financiando los premios Pathfinder Awards para investigadores en temas prioritarios y sacando partido a nuestro impacto en el extranjero y a nuestras asociaciones internacionales de una manera más eficaz.

131. Este entendimiento mejorado está fundamentando de una manera más rápida y eficaz la exploración del horizonte más amplio, la priorización y la toma de decisiones por parte del Gobierno, lo cual nos permite adoptar un enfoque más proactivo hacia la explotación de oportunidades y la mitigación de los riesgos. Estableceremos una nueva función interna de exploración del horizonte para anticiparnos a los avances de la ciencia y la tecnología y sus implicaciones cibernéticas. Tomaremos decisiones más fundamentadas para priorizar cibertecnologías clave, dirigiendo una I+D y unas políticas de desarrollo que favorezcan la seguridad del RU. Cuando sea apropiado, esto orientará una toma de decisiones más amplia sobre las prioridades en ciencia y tecnología a través de la Oficina de Estrategia sobre Ciencia y Tecnología (Office for Science and Technology Strategy) y el Consejo Nacional de Ciencia y Tecnología (National Science and Technology Council).

Máire O'Neill, Investigadora Principal del Centro de Tecnologías Seguras de la Información (CSIT, *por sus siglas en inglés*)

El CSIT es uno de los mayores centros universitarios de investigación en tecnología centrados en la ciberseguridad del RU. Está liderado por la Profesora Máire O'Neill, Investigadora Principal, y fue seleccionado como uno de los primeros Centros de Innovación y Conocimientos en 2009. El éxito del CSIT en las áreas de la investigación, innovación y colaboración con la industria ha conducido a una importante mejora de su reputación tanto a nivel nacional como internacional durante la última década. El CSIT ha sido un factor esencial para el éxito del Northern Ireland Cyber Security Cluster gracias a su apoyo de las actividades derivadas, la expansión de los negocios nacionales y la FDI en la región. Desde su puesta en marcha en 2009, el cibersector de Irlanda del Norte ahora emplea a 2300 personas a lo largo de 104 empresas, generando 110 millones de libras esterlinas en salarios todos los años.

Objetivo 2: favorecer y mantener la ventaja soberana y la ventaja de nuestros aliados en la seguridad de las tecnologías críticas para el ciberespacio

132. Cuando el RU tenga el potencial de establecer una posición de liderazgo o de lograr una ventaja competitiva en áreas clave de la cibertecnología, o cuando confiar en fuentes de suministro no aliadas suponga riesgos inaceptables para la seguridad, buscaremos desarrollar nuestra base industrial nacional. Habrá algunas áreas en las que deberemos mantener una verdadera capacidad soberana, y otras en las que colaboraremos con socios internacionales o buscaremos una posición de liderazgo en un aspecto del mercado. Esto requerirá un enfoque coordinado hacia la estimulación de la innovación y la I+D en colaboración con la industria y el mundo académico. Lograremos los resultados siguientes hasta 2025:

133. El RU tiene un mayor éxito a la hora de traducir la investigación en innovación y nuevas empresas en las áreas de la tecnología que son más esenciales para nuestro ciberpoder. Apoyaremos a los miembros del mundo académico de todo el RU para que comercialicen y operativicen sus investigaciones adoptando un enfoque más basado en los desafíos en colaboración con los socios de la industria. Eso nos permitirá identificar las ideas con mayor potencial y favorecer la inversión por parte de financiadores. Y nos basaremos en el enfoque establecido en la Estrategia de Innovación, apoyando el desarrollo de más ecosistemas consolidados relacionados con tecnologías clave, asegurándonos de que la ventaja del RU sea más robusta y más difícil de copiar.

134. El RU se encuentra en una posición aún más fuerte como líder mundial en el diseño de microprocesadores seguros.[26] Continuaremos desarrollando el programa de Seguridad Digital por Diseño que ha desarrollado una tecnología nueva y más segura para que los chips de ordenadores puedan proteger el *software* frente a vulnerabilidades. Utilizaremos esta experiencia para influir en los procesadores de inteligencia artificial con el fin de dar a los proveedores del RU una ventaja competitiva. Y trabajaremos con el Programa Nacional de Tecnologías Cuánticas para diseñar un modelo de seguridad para los ordenadores cuánticos y para garantizar que las empresas del RU sean los líderes mundiales de referencia en esta tecnología.

135. El RU se considera un líder mundial en la investigación de la seguridad de las tecnologías operativas y los sistemas de control industrial críticos, así como en la capacidad de ponerlos a prueba y ejercerlos en el RU. Crearemos un laboratorio nacional para la seguridad de la tecnología operativa en asociación con la industria y el mundo académico. Este laboratorio organizará programas de investigación punteros y ofrecerá al Gobierno, el sector militar, la industria y los socios internacionales las instalaciones necesarias para emplear y poner a prueba esas tecnologías aquí en el RU. Y según lo confirmado por la Estrategia de Diversificación de la Cadena de Suministro de Telecomunicaciones 5G (Telecoms Supply Chain Diversification Strategy), estableceremos el UK Telecoms Lab, reuniendo al Gobierno y al regulador con la industria para apoyar el nuevo marco de seguridad de telecomunicaciones y ayudar a aumentar la diversidad de los proveedores de equipos de telecomunicaciones en la cadena de suministro del RU.[27]

136. El Gobierno es capaz de proteger mejor la innovación y la propiedad intelectual del RU en las cibertecnologías críticas contra actividades hostiles, manteniendo su ventaja competitiva.[28] Invertiremos en los recursos y la experiencia necesarios para proporcionar un liderazgo técnico en relación con la seguridad de estas tecnologías a medida que se van desarrollando, lo cual incluye asesorar sobre los riesgos de las inversiones extranjeras directas de acuerdo con los objetivos de la Ley de Seguridad Nacional e Inversiones de 2021. Y continuaremos trabajando con empresas y con el mundo académico para crear un entorno de confianza en áreas clave de la investigación y el desarrollo y para adoptar medidas robustas que eviten el robo de datos y de propiedad intelectual.

[26] Los microprocesadores son el cerebro de muchos de los dispositivos que utilizamos actualmente. Son algo omnipresente que se utiliza en áreas críticas como las telecomunicaciones, la defensa, la asistencia sanitaria y a lo largo de nuestras principales industrias. Actualmente, los avances tecnológicos en el diseño de sistemas se han visto frenados por preocupaciones relativas a la seguridad, que se ven aumentadas por una complejidad cada vez mayor de los sistemas.

[27] DCMS, Estrategia de Diversificación de la Cadena de Suministro de 5G (2020)

[28] Con un enfoque específico en los sectores identificados en la Ley de Seguridad Nacional e Inversiones de 2021: robótica avanzada, inteligencia artificial, comunicaciones, hardware de computación, autenticación criptográfica y tecnologías cuánticas.

Seguridad digital por diseño

Un 70 % de las vulnerabilidades actuales de la ciberseguridad explotan un fallo en el diseño de los microprocesadores que se conoce desde la década de 1970. Estos microprocesadores se encuentran en todos los dispositivos digitales, desde los televisores hasta las telecomunicaciones. El Gobierno ha estado trabajando con el sector tecnológico para resolver este tema y hasta 2025 habrá disponible un nuevo diseño de microprocesador para teléfonos inteligentes y una lista cada vez mayor de otros dispositivos.

Cambiar el diseño de los microprocesadores requiere asociaciones e inversiones a escala global. Gracias al liderazgo del RU y a una inversión de 70 millones de libras esterlinas por parte del Gobierno, se está diseñando la seguridad en los dispositivos del futuro, reduciendo enormemente el riesgo de que un ciberataque tenga éxito.

La investigación y el desarrollo de esta tecnología revolucionaria se llevaron a cabo en el RU. Algunos líderes tecnológicos como Microsoft, Google y otros están invirtiendo para integrar esos nuevos beneficios para la seguridad en sus productos. Los investigadores de universidades del RU están trabajando para encontrar nuevas maneras de utilizar mejor esta tecnología segura y el Gobierno está animando a las pymes a encontrar nuevos mercados para productos que incorporen ese nuevo elemento de seguridad.

Phil Wilson, Director, Investigación y Desarrollo en The Hut Group

The Hut Group es una empresa de comercio electrónico centrada en los bienes de consumo de alta rotación. Tenemos más de 200 sitios web ejecutándose en una plataforma común con más de 3000 pedidos por minuto que procesar, por lo que la seguridad de nuestra plataforma y nuestros clientes es nuestra mayor prioridad. Invertimos un gran esfuerzo en garantizar que pueda contenerse cualquier ciberataque y, por eso, estamos encantados con la posibilidad de utilizar la tecnología Seguridad Digital por Diseño (DSbD, *por sus siglas en inglés*) en nuestros sistemas. Ejecutar nuestros sistemas con esos microprocesadores, desarrollados a raíz de una asociación entre el Gobierno y la industria valorada en 180 millones de libras esterlinas, aumentaría la resiliencia de nuestros sistemas, pero administrar esa transición resulta complejo, puesto que no podemos adoptar una nueva tecnología salvo que cumpla nuestros requisitos de rendimiento. Ha sido un privilegio ser el primer proyecto piloto para el programa DSbD y esperamos poder beneficiarnos de esta nueva seguridad en todos nuestros sistemas en el futuro próximo.

Objetivo 2a: conservar una iniciativa Crypt-Key nacional robusta y resiliente que satisfaga las necesidades de los clientes del HMG, de nuestros socios y aliados, y que haya mitigado adecuadamente nuestros riesgos más importantes, incluida la amenaza de nuestros adversarios más capaces.

137. Crypt-Key es el término utilizado para describir el uso por parte del RU de la criptografía para proteger la información y los servicios esenciales de los que dependen el Gobierno, los militares y la comunidad de la seguridad nacional del RU, lo cual incluye la protección frente a los ataques de nuestros adversarios más competentes. Sustenta nuestra capacidad de elegir cómo desplegar nuestras capacidades en las áreas de seguridad nacional y defensa. Para convertirnos en una nación Crypt-Key líder en el mundo, necesitamos contar con las habilidades y tecnologías adecuadas tanto en el Gobierno como en el sector privado.

138. Continuaremos invirtiendo en nuestras capacidades en el Gobierno y trabajando con nuestra industria Crypt-Key nacional para garantizar que el RU continúe siendo una de las pocas naciones capaces de desarrollar una Crypt-Key soberana en el futuro. Asimismo, seguiremos ofreciendo un liderazgo global en Crypt-Key, lo cual incluye apoyar a la OTAN como proveedor de material clave. Este liderazgo aportará beneficios de segundo orden a la hora de mantener una industria altamente cualificada en el RU y de conservar nuestro poder en una ingeniería altamente resiliente, con el potencial de permitir capacidades nuevas y robustas para otros contextos de alta seguridad como la infraestructura nacional crítica. Lograremos los resultados siguientes hasta 2025:

139. Una iniciativa Crypt-Key del RU más resiliente y segura con una base industrial más sostenible y líder en el mundo, que proporcione la amplia gama de soluciones que el RU necesita y que nos permita exportar a socios y aliados elegidos. Combinaremos las capacidades y la experiencia del Gobierno y la industria más eficazmente, y adoptaremos un enfoque nacional más riguroso hacia la gestión de la iniciativa. Esto garantizará el desarrollo de las habilidades diferenciadas y especializadas que necesitamos.

140. El RU posee unas capacidades y unos servicios Crypt-Key más sólidos en el Gobierno, capaces de satisfacer las necesidades en constante cambio del RU y nuestros aliados y garantizando que permanezcamos a la vanguardia del desarrollo Crypt-Key. Ofreceremos un liderazgo técnico sólido para entender los requisitos de los usuarios y mejorar nuestros servicios básicos, incluida la provisión de material clave y el aseguramiento de productos y sistemas. También transformaremos los servicios Crypt-Key, aprovechando las nuevas tecnologías para que se tornen más flexibles e invisibles.

141. El RU ha avanzado su liderazgo global en Crypt-Key y ha aumentado las exportaciones a nuestros socios y aliados. Mantendremos nuestro papel de liderazgo en los Cinco Ojos, la OTAN y otras asociaciones internacionales y configuraremos el desarrollo de los estándares reconocidos a nivel internacional para permitir que las soluciones Crypt-Key del RU sean interoperables. Y trabajaremos con la industria para maximizar las oportunidades de exportación.

Objetivo 3: garantizar la próxima generación de tecnologías conectadas, mitigando los riesgos para la ciberseguridad que supone la dependencia de los mercados globales y asegurándonos de que los usuarios del RU tengan acceso a un suministro confiable y diverso

142. Durante la próxima década continuaremos viendo la integración de la potencia computacional, la conectividad a Internet y la automatización en cada vez más partes de nuestro entorno, incluidos objetos físicos e infraestructura y, a más largo plazo, en los propios humanos. Esto ampliará el alcance del ciberespacio y aumentará considerablemente el volumen de datos generados. La capacidad de gestionar datos con seguridad se convertirá en algo más crítico para el funcionamiento seguro de nuestra economía.

143. Debemos asegurarnos de que, siempre que sea posible, la próxima generación de tecnologías conectadas estén diseñadas y se implanten teniendo en cuenta la seguridad y la resiliencia como parte de un esfuerzo coordinado por adoptar un enfoque «seguro por diseño». La naturaleza global de las cadenas de suministro de tecnología implica que tendremos que usar todos los recursos a nuestro alcance para gestionar más activamente los riesgos de la dependencia tecnológica. Siempre que sea posible, intentaremos asegurarnos de que la seguridad esté ya integrada. Cuando eso no sea posible, implementaremos medidas robustas para mitigar el riesgo, como las regulaciones nacionales y la colaboración internacional con respecto a los estándares. Lograremos los resultados siguientes hasta 2025:

144. Los productos de consumo conectables vendidos en el RU cumplen los estándares básicos en ciberseguridad. Introduciremos e implementaremos el Proyecto de Ley de Seguridad de los Productos y la Infraestructura de Telecomunicaciones para permitir la ejecución de unos estándares de seguridad mínimos en todos los nuevos productos de consumo conectables vendidos en el RU. Apoyaremos una transición cibersegura hacia un sistema energético inteligente y flexible que incluya puntos de carga inteligentes para vehículos eléctricos y electrodomésticos con un consumo inteligente de la energía. Trabajaremos con organismos normativos, con la industria y con socios internacionales para influir en el consenso global sobre los estándares técnicos. Y ayudaremos a las organizaciones del RU a adquirir, desplegar y gestionar dispositivos conectados de una manera más segura, por ejemplo, a través de nuevas directrices de seguridad para los dispositivos conectados de las empresas.

145. Los principales proveedores de servicios digitales, incluidos los servicios en la nube, *software*, servicios gestionados y tiendas de aplicaciones, deberán seguir estándares de ciberseguridad mejores, y ayudar así a proteger a las organizaciones y consumidores de las ciberamenazas. Reforzaremos y ampliaremos la normativa actual de proveedores de servicios digitales y potenciaremos la capacidad de la ICO de garantizar que los proveedores digitales gestionen los riesgos asociados a sus servicios de una manera más proactiva. Continuaremos interactuando con la industria, incluidas las principales empresas de tecnología, para aprovechar la experiencia del mercado y asegurarnos de que todo el mundo desempeñe un papel a la hora de proteger las cadenas de suministro digitales del RU. Y lideraremos el desarrollo de soluciones de política internacional centradas en los proveedores digitales.

146. El RU está a la vanguardia de la adopción segura y sostenible de la tecnología de espacios conectados en beneficio de los ciudadanos y las empresas. Los espacios conectados, en ocasiones conocidos como «ciudades inteligentes», tienen el potencial de ofrecer beneficios tangibles a la sociedad como la gestión del tráfico, la reducción de la contaminación y el ahorro de dinero y recursos. Sin embargo, la interconectividad que permite que los espacios funcionen de una manera más eficiente también crea vulnerabilidades cibernéticas y el potencial de que se produzcan ciberataques. Utilizaremos como base los principios de seguridad de los espacios inteligentes del NCSC con el fin de reducir los riesgos a los que se enfrentan las empresas, la infraestructura, el sector público y los ciudadanos.[29] Reforzaremos la capacidad de las autoridades y organizaciones locales, como los puertos, universidades y hospitales, para comprar y utilizar la tecnología de espacios conectados con seguridad. Y crearemos un consenso internacional para lograr un enfoque coherente y eficaz hacia la seguridad de los espacios conectados.

147. La ciberseguridad está incorporada a otras tecnologías emergentes implantadas en el RU. Identificaremos aplicaciones tecnológicas novedosas y emergentes que tengan el potencial de crear riesgos para la ciberseguridad, y nos aseguraremos de que el RU permanezca a la vanguardia del desarrollo seguro de esas tecnologías. A medida que el Gobierno considere opciones para desarrollar una capacidad del RU en la tecnología de gemelos digitales y una «infraestructura ciberfísica» más amplia, nos cerciioraremos de que la ciberseguridad sea un aspecto clave de la toma de decisiones.[30] Y desplegaremos un sistema de garantía para asegurar que el RU se encuentre en una posición robusta para llevar a cabo una amplia variedad de implementaciones de vehículos conectados y automatizados.[31]

[29] NCSC, Principios de la Seguridad de Espacios Conectados (2021)
[30] Anunciado en la Estrategia de Innovación (2021)
[31] El Proceso de Vehículos Conectados y Automatizados para Garantizar la Seguridad (CAVPASS, *por sus siglas en inglés*)

Shadi A. Razak, CTO y Cofundador de Angoka

La publicación de directrices sobre espacios conectados seguros por parte del Gobierno y el aumento en el uso de vehículos autónomos pone de relieve la importancia de la seguridad en nuestra sociedad. Angoka es un orgulloso exalumno del programa de ciberacelerador del NCSC. Proporcionamos soluciones para una amplia variedad de aplicaciones, desde la infraestructura nacional crítica hasta la movilidad por tierra y aire y mucho más, ofreciendo una garantía de resiliencia y seguridad de extremo a extremo.

La misión de la empresa consiste en garantizar la seguridad y la resiliencia de las Ciudades Inteligentes y la movilidad, que cada vez se están tornando más complejas y dependen más de las redes de servicios conectados y de la comunicación máquina a máquina. Nuestra solución permite la creación de zonas de confianza que utilizan una seguridad descentralizada y a prueba de computación cuántica, que se actualiza de manera dinámica para ofrecer un objetivo móvil a los atacantes en todo momento. Eso significa que los propietarios de los dispositivos pueden tomar el control total de su seguridad.

El equipo de Angoka demostrando su solución

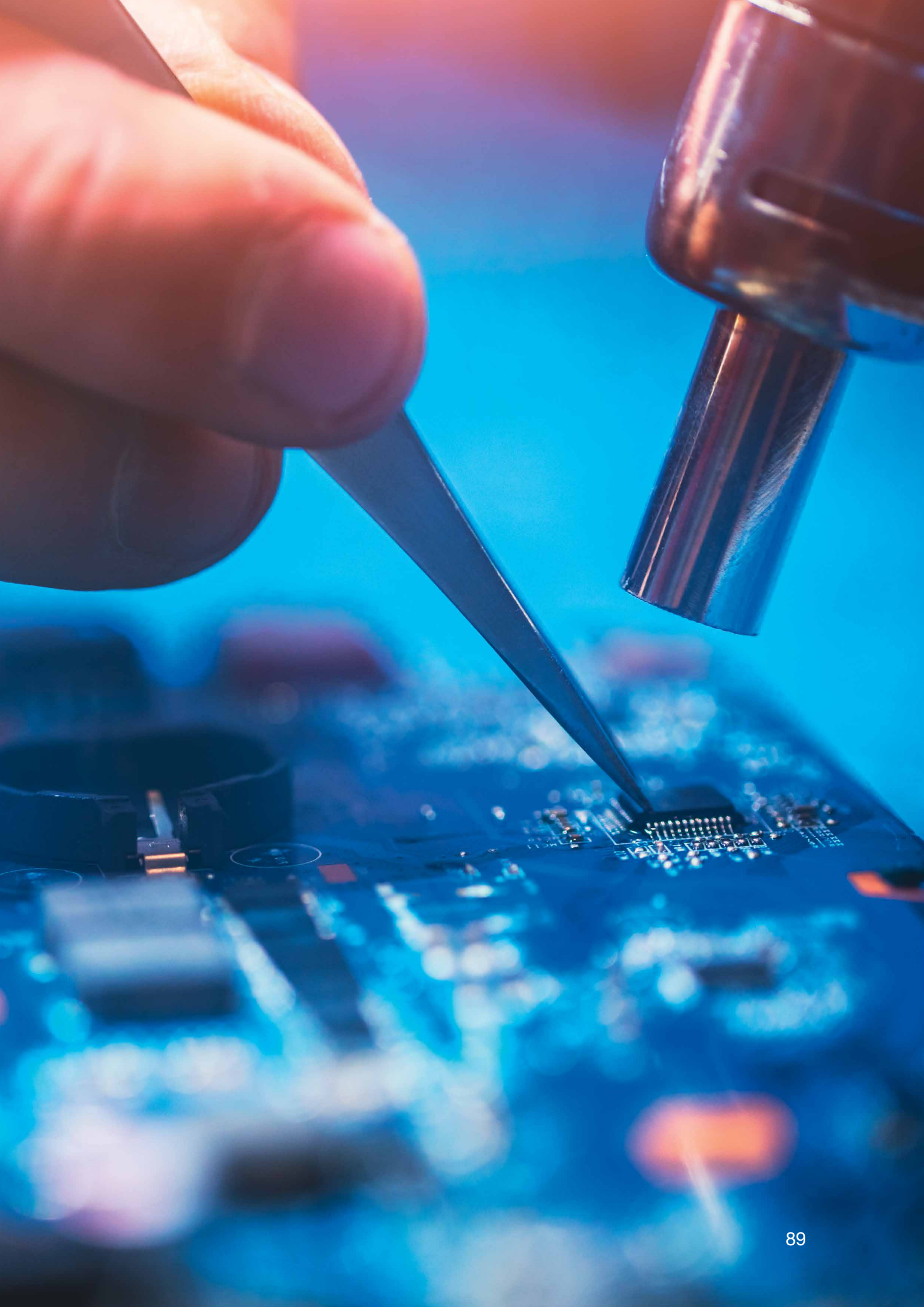
Objetivo 4: colaborar con la comunidad de múltiples partes interesadas para configurar el desarrollo de estándares técnicos digitales globales en las áreas prioritarias que revisten más importancia para el mantenimiento de nuestros valores democráticos, garantizando nuestra ciberseguridad y potenciando los intereses estratégicos del RU a través de la ciencia y la tecnología

148. Los estándares digitales globales son una parte fundamental del funcionamiento de Internet, de las redes de telecomunicaciones y las tecnologías emergentes. La manera en la cual se desarrollan e implementan puede afectar a nuestros objetivos de ciberseguridad, a nuestra prosperidad económica y a nuestras normas y valores. Históricamente, esos estándares han sido establecidos por aquellos que tenían más poder en el mercado y existen barreras materiales que impiden la participación de algunas partes interesadas importantes, incluidas las pymes, los miembros del mundo académico y otros expertos. Lograremos los resultados siguientes hasta 2025:

149. Una participación más comprometida de las múltiples partes interesadas en el ecosistema de los estándares técnicos digitales globales. Reforzaremos la participación de las múltiples partes interesadas en organizaciones de desarrollo de estándares clave y serviremos de ejemplo con nuestras delegaciones de la Unión Internacional de Telecomunicaciones (ITU, *por sus siglas en inglés*). Fomentaremos las discusiones abiertas sobre las tendencias y consideraciones clave para los formuladores de políticas a través del Foro para la Gobernanza de Internet (IGF, *por sus siglas en inglés*) de la ONU y otros foros. Y fortaleceremos la coordinación y compartición de información con socios internacionales, por ejemplo, a través del Grupo de Puntos de Contacto para los Estándares Digitales, creado durante la presidencia del G7 por parte del Reino Unido.

150. Estándares técnicos digitales globales en áreas prioritarias para el RU que están definidos más eficazmente por valores democráticos, consideraciones sobre ciberseguridad e investigación y desarrollo del RU en tecnologías emergentes. Colaboraremos con la industria, el mundo académico, los expertos técnicos y la sociedad civil en áreas como los protocolos de Internet, las redes futuras y la inteligencia artificial (IA) con el fin de aumentar la concienciación sobre las consideraciones de política pública importantes en el desarrollo de estándares técnicos. Pondremos en marcha un centro de estándares de IA para respaldar la implicación global del RU en la estandarización de la IA, según se establece en la Estrategia nacional de IA.

151. Todo esto contará con el apoyo de mecanismos de coordinación estratégicos en el RU, como la iniciativa establecida en la Estrategia Nacional de IA entre el Gobierno, la British Standards Institution (BSI, *por sus siglas en inglés*) y el Laboratorio Nacional de Física. Esta participación también fomentará la prosperidad del RU promoviendo estándares que permitan la innovación y faciliten el crecimiento y la nivelación.



Pilar 4:
liderazgo global

Propiciar el liderazgo y la influencia globales del RU para lograr un orden internacional seguro y próspero

152. Un ciberespacio libre, abierto, tranquilo y seguro sigue siendo fundamental para nuestra seguridad y prosperidad colectivas, y la participación internacional continuará siendo esencial para conseguir todos los objetivos de la ciberestrategia del RU. Sin embargo, como respuesta a una era de competición sistémica, ahora el RU adoptará un papel internacional más activista para fomentar nuestros intereses y valores en el ciberespacio. La actividad del RU en el ciberespacio y nuestra ciberexperiencia también serán protagonistas de la agenda de política exterior más amplia del Gobierno: las utilizaremos de una manera proactiva para lograr un orden internacional abierto, seguro y próspero.

153. Reforzaremos nuestras principales alianzas mientras trabajamos con una variedad más amplia de socios, incluidos la industria, los organismos de estándares técnicos globales, la sociedad civil y el mundo académico como una nación dedicada a la resolución de problemas que aboga por el reparto de responsabilidades. Invertiremos en establecer relaciones más profundas con socios de África y del Indo-Pacífico y aprovecharemos las oportunidades de forjar alianzas nuevas y más ágiles. Continuaremos mejorando nuestros instrumentos diplomáticos, conectando nuestra influencia en el extranjero con nuestros puntos fuertes nacionales, aprovechando nuestra experiencia en las comunicaciones operativas y estratégicas, los programas de habilidades y las asociaciones económicas como fuerza global para el bien. Nuestro enfoque redunda en beneficio de la seguridad y la prosperidad globales, no simplemente de nuestra seguridad y prosperidad nacionales.

Objetivo 1: reforzar la ciberseguridad y la resiliencia de los socios internacionales e incrementar las actuaciones colectivas para desestabilizar y disuadir a los adversarios

154. Las actuaciones colectivas y la resiliencia mutua son esenciales para contrarrestar las amenazas de forma ascendente, reduciendo a la vez los incentivos de los actores de las ciberamenazas para llevar a cabo ataques contra el RU y sus socios. Lograremos lo siguiente hasta 2025:

155. Los socios internacionales del RU poseen unas capacidades mayores, compromiso político y sistemas para investigar y perturbar las ciberamenazas, así como para fomentar la resiliencia. Esto dará como resultado una reducción en las amenazas extranjeras a los ciudadanos del RU. Priorizaremos nuestra asistencia en la creación de cibercapacidad en Europa del Este, África y el Indo-Pacífico, y continuaremos trabajando con aliados clave en Oriente Medio y las Américas. Desarrollaremos una oferta técnica más integrada que abarque a todo el Gobierno, con una mayor inversión en las autoridades del orden público y en la defensa, apoyándonos más en la industria y el mundo académico del RU. Nuestro enfoque se centrará en proteger la infraestructura y las cadenas de suministro críticas internacionales, avanzar en el uso seguro de las tecnologías digitales y trabajar con los socios de la industria para hacerlo a escala.

156. Asimismo, haremos más para fomentar las capacidades de las organizaciones de la sociedad civil, haciendo posible un debate sobre la tecnología y la sociedad impulsado por los valores y creando mecanismos locales de rendición de cuentas. Y continuaremos trabajando con organizaciones y asociaciones multilaterales eficaces como las Naciones Unidas, los Cinco Ojos, la OTAN, el G7, la Unión Europea, la Commonwealth, la OCDE, el Foro Global para la Ciberexperiencia (GFCE, *por sus siglas en inglés*), El Foro de la Asociación de Naciones de Asia Sudoriental (ASEAN, por sus siglas en inglés), la Unión Africana y el Banco Mundial.

157. Con el fin de mejorar nuestra protección de los intereses y ciudadanos del RU en el extranjero, también desarrollaremos y presentaremos una campaña de ciberhigiene internacional para las misiones del RU en el extranjero que se adaptará y ejecutará a nivel local. El objetivo es aumentar el coste de las actividades maliciosas, como la piratería informática, el robo de datos e IP y el *ransomware*. La campaña se ofrecerá a través de nuestros diplomáticos, del personal situado en el país, la comunidad empresarial británica local y los implementadores de los programas de desarrollo del RU.

158. Una alianza internacional más amplia que esté dispuesta y sea capaz de imponer más consecuencias significativas a los adversarios del RU. Mejoraremos la determinación y las capacidades internacionales a través de una mayor implicación diplomática, la colaboración operativa, la compartición de información y los ejercicios conjuntos. Trabajando a través de los canales políticos, operativos y de las agencias del orden público, aumentaremos el impacto de las medidas, como las cibersanciones específicas, e identificaremos nuevas herramientas para aumentar los costes para los actores de las ciberamenazas. Generaremos un mayor entendimiento mutuo a lo largo de las ciberfuerzas de los países aliados y socios clave e integraremos mejor las ciberoperaciones en operaciones aliadas en todas las áreas: tierra, mar, aire, espacio y ciberespacio.

159. Y continuaremos apoyando el desarrollo de las capacidades de ciberseguridad de la alianza de la OTAN para reforzar las actuaciones colectivas, que incluye apoyar los procesos para integrar los ciberefectos soberanos facilitados voluntariamente por el RU y otros aliados en las operaciones y misiones de la OTAN.

Objetivo 2: perfilar la gobernanza global para favorecer un ciberespacio libre, abierto, tranquilo y seguro

160. Los Estados que no comparten los valores del RU explotan los desafíos que presenta un Internet libre y abierto para promover sus visiones autoritarias del ciberespacio con el pretexto de la seguridad. El RU adoptará un enfoque más proactivo, trabajando con sus aliados y socios para garantizar que las reglas y los marcos internacionales se desarrollen en consonancia con nuestros valores democráticos. Nuestro objetivo es apoyar el crecimiento económico nacional y global, mejorar la seguridad colectiva, fomentar el uso responsable de las herramientas cibernéticas ofensivas y activar consecuencias reales para las actividades maliciosas e irresponsables. Lograremos los resultados siguientes hasta 2025:

161. Una gobernanza global del ciberespacio e Internet que protege los intereses y valores del RU y que hace que el RU y nuestros socios tengan una mayor influencia sobre el desarrollo y la implementación de los marcos normativos y de gobernanza internacionales. Adoptaremos un enfoque más progresivo y proactivo hacia la creación de los marcos que gobiernan el ciberespacio para promover el crecimiento económico y la seguridad globales. Diseñaremos y ofreceremos acciones concretas que desbloqueen el debate internacional sobre la aplicación de las reglas, normas y principios del ciberespacio para llegar a un consenso sobre las limitaciones efectivas de las actividades destructivas y desestabilizadoras. Haremos esto recurriendo a organizaciones regionales y especializadas clave, incluidas la OSCE, la ASEAN y el GFCE y colaboraremos de forma constructiva con el proceso de la ONU para elaborar un nuevo tratado internacional sobre ciberdelincuencia que coexista con el Convenio de Budapest, asegurándonos de que fortalezca la cooperación internacional y mantenga las protecciones de los derechos humanos.

162. Asimismo, continuaremos promoviendo el Convenio de Budapest sobre la ciberdelincuencia, trabajando con socios internacionales para justificar de manera convincente que continúe siendo el acuerdo internacional principal de cooperación. Y continuaremos promoviendo y mejorando los procesos de múltiples partes interesadas para la gobernanza de Internet, incluidos la Corporación de Internet para la Asignación de Nombres y Números (ICANN, *por sus siglas en inglés*) y el Foro para la Gobernanza de Internet (IGF, *por sus siglas en inglés*). Estos esfuerzos se complementarán con nuestra labor de conformar los estándares técnicos digitales globales (descritos en el capítulo «Tecnología») y nuestro trabajo de expansión de las exportaciones de ciberseguridad del RU (indicadas a continuación), lo cual también ayudará a integrar los estándares del RU en los cibersistemas de otras naciones.

163. La mayoría de países que se encuentran en una «situación intermedia» apoyan y promueven la visión del RU del ciberespacio y el futuro de Internet, contrarrestando con más éxito la influencia de los Estados autoritarios sobre el sistema de múltiples partes interesadas. Demostraremos que es posible abordar los desafíos que presenta el ciberespacio sin adoptar enfoques autoritarios, permitiendo a la vez la innovación, el desarrollo y el crecimiento. Apoyaremos a los países que tienen dificultades para lidiar con la digitalización para crear la amplia gama de experiencia legal y en comunicaciones estratégicas que necesitan para participar en el debate internacional e implementar marcos acordados. Continuaremos denunciando el uso irresponsable de las cibercapacidades, creando confianza a nivel internacional. Y continuaremos demostrando un enfoque abierto y transparente hacia nuestro uso de las cibercapacidades ofensivas siempre que podamos, reforzando la reputación del RU como una fuerza positiva.

Objetivo 3: Aprovechar y exportar las capacidades y la experiencia cibernéticas del RU para aumentar nuestra ventaja estratégica y promover nuestros intereses más amplios en la prosperidad y la política exterior.

164. En respuesta a la competición sistémica y a los rápidos cambios tecnológicos, la ciberactividad y las cibercapacidades del RU se considerarán junto con otras fuentes de poder nacional para impulsar nuestra ventaja estratégica y promocionar nuestros objetivos de política exterior y prosperidad. Nuestro objetivo consiste en lograr un orden internacional en el cual las sociedades y economías abiertas puedan prosperar y se defiendan los derechos humanos, impulsando a la vez la prosperidad a nivel nacional. Lograremos los resultados siguientes hasta 2025:

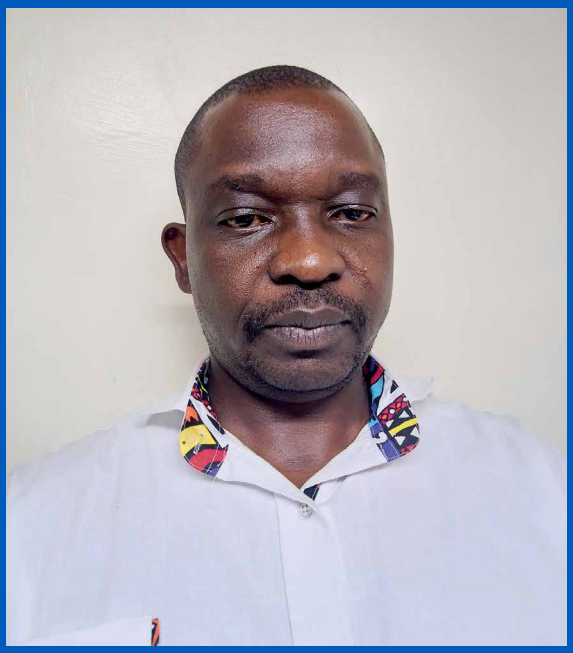
165. Nuestra actividad en relación con el ciberespacio ha mejorado la estabilidad global y protegido el sistema internacional basado en reglas, las sociedades abiertas y los sistemas democráticos en aquellos lugares donde están siendo socavados. Ofreceremos una campaña internacional basada en los valores para defender los derechos humanos, la diversidad y la igualdad de género en el diseño, el desarrollo y el uso del ciberespacio. Esto incluirá, sin limitación, abordar los cortes de Internet, los sesgos en los algoritmos de inteligencia artificial y una seguridad en línea cada vez mayor. Competiremos más eficazmente para proteger los valores, sistemas y procesos democráticos y reforzaremos el sistema internacional basado en normas (incluidas las Naciones Unidas, la Organización Mundial de la Salud y el sistema de comercio global) aumentando las inversiones en nuestra red de ciberfuncionarios que abarca a seis continentes. Mejoraremos nuestro uso de las comunicaciones estratégicas para promover la colaboración en investigación y los programas de intercambio académicos del RU y contribuiremos a asegurarnos de que las ideas del RU se traduzcan en aplicaciones prácticas.

166. El RU es uno de los 3 principales exportadores globales de cibersoluciones y ciberexperiencia, con una industria cibernética que nos convierte en el suministrador imprescindible de soluciones de ciberseguridad para gobiernos extranjeros y clientes comerciales importantes. Mostraremos lo mejor de la ciberseguridad del RU a través de una mayor participación internacional activa de Gobierno a Gobierno, bajo los auspicios del Programa de Embajador de la Ciberseguridad del RU y de nuestra red internacional. Apoyaremos a empresas de todo el RU en todas las fases, desde la innovación hasta la exportación, con el fin de que se conviertan en exportadores competentes y atraigan inversiones internas, y ofreceremos más apoyo a las pymes, por ejemplo, a través de una nueva Facultad de Exportación.[32] [33] Aparte de nuestro trabajo a través de la alianza entre la industria y el gobierno para el crecimiento (Cyber Growth Partnership) y otros esfuerzos señalados en el capítulo «Ciberecosistema del RU», también crearemos una nueva Oficina de Campaña de Cibercapacidades (Cyber Capability Campaign Office) que proporcione un apoyo más estructurado y coordinado a las principales campañas de exportación.

[32] Descrito en la Estrategia de Innovación del RU (2021)

[33] La Facultad de Exportaciones de Defensa y Seguridad del RU (UKDSE, *por sus siglas en inglés*) es un centro de aprendizaje y desarrollo en línea dirigido a las pymes en el sector de la defensa y la seguridad con módulos específicos para las empresas de ciberseguridad. El registro en la Facultad ofrece acceso a un programa de módulos de aprendizaje basados en un currículo, así como a información valiosa sobre los eventos y las actividades planeados por Exportaciones de Defensa y Seguridad del RU.

Charles Juma, Programa de Acceso Digital del RU en Nairobi



Me llamo Charles Wesonga Juma. Lidero, doy forma y ofrezco ciberseguridad, desarrollo digital, inclusión y iniciativa empresarial como parte del Programa global de Acceso Digital interministerial del RU en Kenia. También doy apoyo a proyectos complementarios que se enmarcan en la Cartera Cibernética del Fondo de Conflicto, Estabilidad y Seguridad (CSSF, *por sus siglas en inglés*). No debe subestimarse la importancia de la seguridad y la protección de datos en línea ni el uso responsable del ciberespacio. Tal y como hemos aprendido con la pandemia de COVID-19, la seguridad y la higiene en línea pueden ser tan importantes como la salud y la higiene públicas. Me apasiona garantizar que todo el mundo esté protegido de las amenazas y daños en línea como parte del ciberpoder general del Gobierno del RU.

Sara Merchant, Ciberfuncionaria de la Embajada Británica, Tbilisi

Me llamo Sara y estoy destinada a la Embajada Británica de Tbilisi en calidad de Ciberfuncionaria, trabajando estrechamente con el Gobierno de Georgia y el NCSC del RU. Mi actividad diaria incluye desde la colaboración política y el apoyo a la implementación de la nueva ciberestrategia hasta aprovechar a los especialistas del RU para aumentar las capacidades técnicas de Georgia. Me siento una privilegiada por poder proyectar la experiencia del RU y poder apoyar a Georgia para generar resiliencia contra las ciberamenazas. Como país que desafortunadamente tiene una gran experiencia estando en la línea de combate de las actividades estatales hostiles, podemos aprender mucho de Georgia. Nuestro trabajo nos hace más fuertes, resilientes y mejor informados.

Pilar 5:
contrarrestar las amenazas

Detectar, perturbar y disuadir a nuestros adversarios para mejorar la seguridad del RU en el ciberespacio

167. La naturaleza de la amenaza a la cual nos enfrentamos es compleja. Nos preocupan las amenazas que existen en el ciberespacio (por ejemplo, a nuestras actividades en línea), las amenazas al RU y a los socios que llegan a través del ciberespacio (por ejemplo, a la infraestructura nacional crítica conectada en red del RU) y las amenazas al funcionamiento de ciberinfraestructuras internacionales subyacentes. Todas esas amenazas pueden tener un impacto sobre la disponibilidad de los servicios de los que dependen las personas, o sobre la confidencialidad o integridad de los datos y la información que pasa a través de esos sistemas. Las bases de nuestro enfoque hacia contrarrestar la amenaza tienen que ver con promover la ciberresiliencia según lo indicado anteriormente en este documento. Este capítulo se centra en cómo aumentaremos los costes y riesgos de atacar al RU en el ciberespacio y en asegurarnos de conseguir nuestro pleno potencial como ciberpoder.

168. Desde la publicación de la Estrategia de Ciberseguridad Nacional 2016-2021, hemos transformado nuestro enfoque hacia la mitigación de la amenaza. Hemos establecido unas capacidades de detección y análisis de ciberamenazas de primera clase como parte del Centro de Ciberseguridad Nacional (NCSC). El NCSC trabaja con socios de los sectores público y privado, a nivel nacional y en el extranjero, para detectar y responder a amenazas e incidentes. Como parte de la comunidad de la inteligencia más amplia, el NCSC también ha podido informar a los actores políticos sobre la atribución de ataques contra intereses del RU, que es una parte fundamental de nuestro enfoque hacia la prevención de las ciberamenazas. Hemos realizado una importante inversión en nuestras cibercapacidades ofensivas a través del Ciberprograma Ofensivo Nacional (National Offensive Cyber Programme) y ahora la Ciberfuerza Nacional (NCF). También hemos desarrollado una respuesta integrada de las agencias del orden público nacionales liderada por la NCA y hemos procurado interrumpir y aumentar el coste de las actividades hostiles y delictivas en el ciberespacio. Hemos creado unas capacidades de detección y evaluación de amenazas de clase mundial con los medios necesarios para traducir la información resultante en mitigaciones de impacto a lo largo de los sectores público y privado. Y hemos diseñado un régimen de cibersanciones autónomo como recurso adicional para imponer costes sobre los actores hostiles. En combinación, nuestra participación diplomática, el NCSC, nuestras agencias de seguridad e inteligencia, la NCA, los cuerpos y fuerzas de seguridad más amplios y la NCF han reducido el impacto en el mundo real provocado por las amenazas al adoptar medidas para contrarrestar directamente a los adversarios, ayudar a evitar ataques y reducir los daños.

169. Sin embargo, las amenazas también han aumentado en sofisticación, complejidad y gravedad. En definitiva, nuestros esfuerzos aún no han alterado el cálculo de riesgo de los atacantes, quienes continúan dirigiendo con éxito sus ofensivas contra el RU y sus intereses. Los ciberataques contra el RU están motivados por el espionaje, las ganancias delictivas, comerciales, financieras y políticas, el sabotaje y la desinformación. Los atacantes desarrollan capacidades que evaden las mitigaciones; además, las ciberherramientas cada vez más sofisticadas y los aspectos facilitadores asociados se han convertido en artículos de consumo en una industria en crecimiento, reduciendo las barreras para permitir el acceso de todo tipo de actores maliciosos. Las recompensas están aumentando a medida que la capacidad de los actores de robar y cifrar datos valiosos y de extorsionar para recibir pagos de *ransomware* continúa creciendo, causando interrupciones a las empresas y los servicios públicos clave. Como resultado, los atacantes se han ido beneficiando cada vez más financieramente, han explotado la privacidad y la libertad de expresión y han intentado manipular los acontecimientos a través de la desinformación.

170. Por lo tanto, ahora el enfoque del RU será pasar a una campaña más integrada y prolongada que implicará hacer un uso rutinario, integrado y creativo de la gama completa de recursos y capacidades disponibles para imponer costes a nuestros adversarios, perseguir e interrumpir a los perpetradores y evitar futuros ataques. Los elementos de apoyo clave de este enfoque serán:

- el desarrollo continuado de la NFC como próximo paso en la capacidad del RU de llevar a cabo ciberoperaciones ofensivas contra sus adversarios

- campañas específicas interministeriales para abordar las amenazas al RU, mediante el uso de nuestras herramientas diplomáticas, militares, económicas, legales, de inteligencia, de las agencias del orden público y de comunicaciones estratégicas.

- nuevas inversiones que permitan a las agencias del orden público llevar a cabo investigaciones a escala y a un ritmo constante y mantener una ventaja técnica sobre nuestros adversarios para evitar y detectar a delincuentes peligrosos y a los servicios facilitadores de los que dependen.

- un aumento importante en la compartición de datos entre el Gobierno y la industria según lo indicado en el capítulo de «Resiliencia».

171. El ciberespacio presenta oportunidades para el RU, creando nuevas maneras de perseguir activamente nuestros intereses nacionales. Por ejemplo, las ciberoperaciones ofensivas nos ofrecen una amplia variedad de medidas flexibles, escalables y de desescalada que ayudarán al RU a mantener su ventaja estratégica y a satisfacer las prioridades nacionales, a menudo de maneras que eviten la necesidad de poner a las personas en riesgo de sufrir peligros físicos.

172. Continuaremos desarrollando e invirtiendo en nuestras cibercapacidades ofensivas a través de la NCF. La NCF transformará la capacidad del RU de defenderse contra los adversarios en el ciberespacio y en el mundo real, para proteger al país, a sus ciudadanos y su estilo de vida. Esas capacidades se utilizarán de manera responsable como una fuerza positiva junto a recursos de poder diplomáticos, económicos, militares y de justicia penal. Se emplearán para apoyar y desarrollar una amplia variedad de prioridades del Gobierno relativas a la seguridad nacional, el bienestar económico y en apoyo a la prevención y detección de los delitos graves.

Objetivo 1: detectar, investigar y compartir información sobre actores estatales, delictivos y otros tipos de ciberactores y actividades cibernéticas maliciosos para proteger al RU, a sus intereses y sus ciudadanos

173. Lograremos los resultados siguientes hasta 2025:

174. El Gobierno posee un entendimiento exhaustivo de las cibercapacidades de los actores estatales, delictivos y otros ciberactores maliciosos y de sus intenciones estratégicas hacia el RU. Mantendremos y aumentaremos las inversiones considerables que realizamos en virtud de la estrategia de 2016 en las agencias de inteligencia y en los cuerpos y fuerzas de seguridad con el fin de entender la ciberamenaza. En particular, aumentaremos la capacidad de los cuerpos y fuerzas de seguridad de entender y abordar la amenaza de la ciberdelincuencia, incluidos sus vínculos con amenazas estatales y otras amenazas internacionales y nacionales, así como sus facilitadores tecnológicos, ayudándonos a desarrollar unas respuestas políticas más eficaces. Mejoraremos nuestra manera de coordinar la detección de amenazas a lo largo del Gobierno, con una estrategia conjunta de acceso y explotación de los datos a lo largo de las agencias de inteligencia y los cuerpos y fuerzas de seguridad. Y nos centraremos aún más si cabe en entender las intenciones y los criterios de toma de decisiones de nuestros adversarios y el impacto que nuestras actividades tienen sobre ellos, lo cual incluye cómo las personas se convierten en ciberdelincuentes y qué medidas podemos tomar para evitar que eso ocurra.

175. Nuestro trabajo para permitir una denuncia más rápida y fácil de los ciberincidentes y ciberdelitos, indicado en el capítulo de «Resiliencia», también nos ayudará a lograr ese resultado.

176. Las amenazas estatales y delictivas más graves y otras amenazas se investigan de manera rutinaria y exhaustiva, recurriendo a todas las fuentes de información y reuniendo la experiencia del Gobierno, los cuerpos y fuerzas de seguridad y el sector privado. Crearemos las capacidades operativas, técnicas y de inteligencia de la red cibernética de los cuerpos y fuerzas de seguridad del RU. Invertiremos en la capacidad de ciberinteligencia de la NCA, utilizada para combatir a grupos delictivos organizados, la iniciativa regional de desarrollo de inteligencia, que mejorará el acceso a la inteligencia y su movimiento a lo largo del RU, y las habilidades y capacidades que los cuerpos y fuerzas de seguridad necesitan para investigar e interrumpir los delitos cibernéticos y digitales.

177. Las investigaciones recibirán el apoyo de la inteligencia procedente de todas las fuentes y del aprovechamiento de las habilidades y los conocimientos a lo largo del sector privado, lo cual incluye ayudar a las empresas a compartir datos más fácilmente con las agencias del orden público. Y continuaremos implementando las recomendaciones de la HMICFRS sobre la respuesta de la policía a la ciberdelincuencia para garantizar que la red de lucha contra la ciberdelincuencia a nivel nacional, regional y local continúe sobre una base sólida.[34]

[34] Inspección de Su Majestad de la Policía y de los Servicios de Bomberos y Rescate

178. La información y los datos sobre las amenazas se comparten de manera rutinaria a escala y a un ritmo constante y aquellos que los reciben tienen una mayor capacidad de tomar medidas al respecto. El NCSC ha puesto a prueba una serie de iniciativas con el fin de crear comunidades de defensores de redes más eficaces a lo largo de una amplia variedad de sectores. Estas personas no solo reciben y son capaces de compartir información sobre amenazas, sino que son cada vez más capaces de usarla para el beneficio colectivo. Ampliaremos este trabajo, con un enfoque inicial en ayudar al Gobierno a defenderse mejor, con la asistencia del Centro de Cibercoordinación del Gobierno (descrito en el capítulo de «Resiliencia»). El Centro de Cibercolaboración del Sector Financiero ya está a la cabeza en el sector privado.[35]

179. El NCSC también está investigando maneras de rastrear las amenazas emergentes y continúa trabajando con el Alan Turing Institute para explorar cómo utilizar el aprendizaje automático para detectar ciertos tipos de ciberataques. Esta investigación continuará mejorando nuestro entendimiento de cómo podemos usar la inteligencia artificial para detectar actividades maliciosas.

[35] NCSC, Centro de Cibercolaboración del Sector Financiero (FSCCC, *por sus siglas en inglés*) (2021)

Detener la ciberdelincuencia también significa combatir otros tipos de actividades delictivas

Los ciberdelitos (definidos como delitos en virtud de la Ley sobre el Uso Indebido de Ordenadores) tienen lugar cuando se produce un acceso no autorizado a ordenadores, redes, datos y otros dispositivos digitales o actos asociados que pueden provocar daños, o la creación o el suministro de herramientas para cometer esos delitos. Esto puede permitir que los ciberdelincuentes cometan otras actividades cibernéticas maliciosas, como ataques de *ransomware*, accesos no autorizados a cuentas, robos de propiedad intelectual, ataques de denegación de servicio o el robo de conjuntos de datos personales de gran tamaño, unos delitos importantes que van en aumento.

Para los ciudadanos, los ciberdelitos a menudo se manifiestan en forma de otros delitos que ellos permiten y facilitan. Por ejemplo, el uso no autorizado de un ordenador puede conducir a una amplia variedad de fraudes, robos, extorsiones sexuales y, en algunos casos, facilitar el acoso, el maltrato doméstico y el hostigamiento. Todos esos delitos provocan daños importantes a los ciudadanos del RU a diario, destruyendo empresas y arruinando vidas. Así pues, los ciberdelitos son diferentes de otros temas de seguridad en línea más amplios, como el acoso y el hostigamiento, la incitación al odio, la diseminación de desinformación, la promoción de la cultura y la violencia pandilleras o el acceso de menores a la pornografía. El Gobierno está abordando estos asuntos en el libro blanco sobre los perjuicios de Internet y el Proyecto de Ley de Seguridad en Línea.

Objetivo 2: Disuadir e interrumpir a los actores estatales, delictivos y a otros ciberactores maliciosos y las actividades perpetradas contra el RU, sus intereses y sus ciudadanos.

180. Lograremos los resultados siguientes hasta 2025:

181. Tener como objetivo al RU resulta más costoso y conlleva un mayor riesgo para los actores estatales, delictivos y otros ciberactores maliciosos. Implementaremos campañas disuasorias continuadas y personalizadas que hagan uso de la gama completa de capacidades del RU (incluidos los recursos diplomáticos, económicos, abiertos y encubiertos) para influir en el comportamiento de los ciberactores maliciosos y delictivos. En particular, mejoraremos nuestra señalización a los adversarios de nuestras capacidades y nuestra voluntad de imponer costes importantes mediante sanciones, la intervención de las agencias del orden público y las operaciones de la NCF, entre otros. Y a través del programa Cyber Choices de la NCA, apartaremos a las personas de los ciberdelitos, trabajando con la industria y el mundo académico para ofrecer a potenciales delincuentes alternativas mejores, como formación para aprendices y prácticas laborales.

182. Asimismo, facilitaremos las herramientas y las facultades que precisan los cuerpos y fuerzas de seguridad y las agencias de inteligencia a través del Proyecto de Ley para Contrarrestar las Amenazas de los Estados (Counter State Threats Bill), actualizando la legislación actual e introduciendo nuevos delitos para dar cuenta de cómo han evolucionado las amenazas estatales. Enmendaremos la Ley sobre Productos del Delito de 2002 (Proceeds of Crime Act 2002) para optimizar la capacidad de las agencias del orden público de identificar, decomisar y recuperar los productos de la ciberdelincuencia. En particular, lo haremos mediante la creación de un poder de embargo civil para mitigar los riesgos que entrañan aquellos que no pueden ser enjuiciados.

183. Los actores estatales, delictivos y otros actores maliciosos son menos capaces de tener como objetivo al RU como resultado de la interrupción y desacreditación de sus actividades y capacidades. Revisaremos la política y el enfoque operativo del Gobierno sobre cómo abordar el *ransomware*, adoptando este asunto como una de nuestras campañas prioritarias, colaborando con la industria y con nuestros socios internacionales. Maximizaremos las asociaciones entre la NCF, el NCSC y la NCA, las comunidades diplomáticas y de inteligencia más amplias y las agencias del orden público para contrarrestar las amenazas que interrumpan la confidencialidad, integridad y disponibilidad del ciberespacio o los datos y servicios en el ciberespacio. Concretamente, invertiremos en capacidades para abordar infraestructuras de ciberdelincuencia y desplegar a nuestros cuerpos y fuerzas de seguridad y nuestras capacidades cibernéticas ofensivas para interrumpir ciberactividades maliciosas. Nuestros adversarios están creando cibercapacidades y están utilizándolas cada vez más para propósitos malignos. Haremos un uso completo de la NCF cuando lo consideremos apropiado para desbaratar esos esfuerzos y defender y proteger al RU.

184. También contrarrestaremos la proliferación de las cibercapacidades de alta gama entre los Estados y los grupos de delincuencia organizada a través de los mercados comerciales y delictivos, combatiendo los foros que permiten, facilitan o ensalzan la ciberdelincuencia.

185. Un aumento en la justicia penal y otros resultados disruptivos para los ciberdelincuentes, con una mejora en la capacidad de la justicia penal de enjuiciar a los ciberdelincuentes en el RU. Revisaremos la Ley sobre el Uso Indebido de Ordenadores (CMA, *por sus siglas en inglés*) y las facultades pertinentes para garantizar que las agencias del orden público tengan la capacidad de investigar amenazas nuevas y emergentes de los delincuentes e introduciremos a más fiscales especializados para tratar el aumento en el número de casos cibernéticos. Asimismo, mejoraremos las habilidades, el ejercicio y la incorporación de cuerpos y fuerzas de seguridad especializados para garantizar un suministro continuado de agentes con los conocimientos cibernéticos especializados necesarios, a través del folleto de ciberhabilidades del Consejo Nacional de Jefes de Policía (NPCC, *por sus siglas en inglés*) y del proyecto Itinerarios Profesionales Ciberdigitales (Cyber Digital Career Pathways) del College of Policing.

Susan Moody, Agente de Prevención del Police Service of Northern Ireland (PSNI, *por sus siglas en inglés*)

De izquierda a derecha: Susan Moody (PSNI), Sarah Travers (presentadora de TV) y Joe Dolan (Director del Northern Ireland Cyber Security Centre)

Los ordenadores y los dispositivos móviles forman parte de la vida diaria de los jóvenes. Ofrecen grandes oportunidades, pero también pueden suponer peligros si no se utilizan debidamente. La función de prevención de la PSNI ofrece una intervención temprana muy necesaria para los jóvenes y les ayuda a entender las leyes relativas al uso y los usos indebidos de los ordenadores. Esto pone de relieve las señales de peligro de las actividades delictivas potenciales, así como las grandes oportunidades que existen a través de iniciativas como CyberFirst y la cibernética como carrera, que pueden ofrecer a aquellos con curiosidad o talento una alternativa a la delincuencia, y evitar los abusos de otras personas con fines delictivos. Susan ha trabajado incansablemente en el desarrollo de un programa de ciberinformación para centros educativos disponible para todas las escuelas de secundaria y ha colaborado directamente con más de 40 escuelas primarias, numerosas escuelas secundarias, organizaciones de jóvenes y grupos uniformados. Esos jóvenes podrían convertirse en nuestros ciberembajadores y en defensores del futuro.

Objetivo 3: Tomar medidas en el ciberespacio para respaldar nuestra seguridad nacional y la prevención y detección de delitos graves

186. Lograremos los resultados siguientes hasta 2025:

187. Las cibercapacidades del RU tienen un mayor impacto a la hora de disuadir e interrumpir amenazas no cibernéticas. Ampliaremos y desarrollaremos la NCF, logrando nuestra visión a largo plazo para esta capacidad clave, asegurándonos de que esté plenamente integrada con la GCHQ, el MOD, el SIS y el Laboratorio de Ciencia y Tecnología de la Defensa (Dstl, *por sus siglas en inglés*) y trabajando estrechamente con las agencias del orden público y el Gobierno más amplio. Llevaremos a cabo ciberoperaciones ofensivas legales y proporcionadas a través de la NCF, actuaremos de manera responsable en el ciberespacio y predicaremos con el ejemplo. Las ciberoperaciones ofensivas continuarán respaldando la seguridad nacional del RU, incluida nuestra política exterior y de defensa, y la prevención de delitos graves.

188. También ampliaremos y desarrollaremos las capacidades técnicas de las agencias del orden público en relación con la infraestructura y las criptomonedas, que pueden aplicarse contra otras amenazas.

189. Las cibercapacidades del RU se integran a lo largo de todas las operaciones de defensa, de conformidad con el Concepto Operativo Integrado de 2025 (Integrated Operating Concept 2025).[36] Esto nos permitirá mantener nuestra ventaja bélica competitiva sobre nuestros adversarios y hará posible una mayor colaboración con nuestros socios y aliados. Continuaremos avanzando en el Programa de Cambio de la Integración Multidominio de Defensa (Defence Multi-Domain Integration Change Programme), que unirá capacidades a lo largo de los distintos dominios, y ofrecerá una mayor integración con otros instrumentos de nuestro poder nacional, afianzando nuestra ventaja militar sobre nuestros adversarios. La cibernética será una parte fundamental del negocio de la defensa, facilitada por ciberespecialistas altamente cualificados, una concienciación cibernética general a lo largo de la fuerza laboral de defensa y cibercapacidades resilientes y de vanguardia.

[36] Ministerio de Defensa, Concepto Operativo Integrado (2020)

Investigaciones destacadas de ciberdelitos por parte de los cuerpos y fuerzas de seguridad

Operación Imperil: la Operación Imperil fue una investigación conjunta entre la Unidad de Delincuencia Organizada Regional del Sureste (SEROCU, *por sus siglas en inglés*) y el FBI sobre un sitio web que vendía información personal y bancaria de víctimas de ciberataques. Esto permitía a otras personas comprar datos personales para cometer fraudes y otros delitos relacionados con el uso indebido de los ordenadores. Una importante investigación condujo a la identificación de cuentas bancarias y pagos utilizados para la infraestructura técnica, y se descubrió que el propietario del sitio web estaba situado en Pakistán. Esto permitió que el FBI pudiera incautar el sitio web de manera encubierta y posteriormente cerrarlo. La Unidad de Delincuencia Organizada Regional del Sureste detuvo al principal sospechoso del RU, quien había abierto una cuenta bancaria situada en los EE. UU. en nombre del propietario del sitio web para el lavado de fondos procedentes de actividades delictivas. El sospechoso del RU cometió un fraude importante al utilizar algunos de los datos de las víctimas afectadas, abriendo cuentas bancarias con otros nombres, utilizando cuentas bancarias comprometidas para pagar vacaciones de lujo y presentando reclamaciones falsas al Departamento de Trabajo y Pensiones, lo cual dio como resultado una pérdida para el Estado superior a las 90 000 libras esterlinas. El sospechoso fue acusado de nueve cargos y condenado a cuatro años de cárcel, pena que quedó reducida debido a una declaración de culpabilidad temprana. El juez otorgó al equipo de investigación una mención de honor. En el momento de la publicación se está a la espera de ejecutar un decomiso y una solicitud de por vida en virtud de la Ley sobre los Productos del Delito.

Operación Nipigon: esta fue una investigación de la Met Police sobre un ciudadano búlgaro sospechoso de crear páginas de *phishing* personalizadas que habían causado unas pérdidas al RU valoradas en más de 40 millones de libras esterlinas. Fue identificado tras una investigación sobre otro ciberdelincuente conocido que anteriormente había sido condenado a 10 años de prisión en 2018 y que estaba utilizando las páginas de *phishing* creadas por el ciudadano búlgaro para llevar a cabo sus propios actos delictivos. La investigación se inició tras la identificación de una dirección de correo electrónico importante asociada con el sospechoso, la cual, tras una serie de investigaciones complejas y prolongadas, condujo a la colaboración de las autoridades búlgaras y a la detención del sospechoso, quien fue extraditado y, tras una exhaustiva revelación, se declaró culpable de todos los cargos penales y recibió una pena privativa de libertad de nueve años y medio.

Operación Leasing: En 2020, la NCA lideró una investigación sobre amenazas de bomba terroristas realizadas contra el NHS (Servicio Nacional de Salud) en el punto más álgido de la pandemia de COVID-19, que exigían pagos en Bitcoin (BTC). En colaboración con las autoridades alemanas, la NCA identificó y detuvo al sospechoso, quien recibió una condena de un tribunal alemán.

El 12 de abril de 2020, un ciudadano italiano que vivía en Alemania envió un correo electrónico a través de la red TOR indicando su intención de hacer explotar un hospital del NHS a menos que recibiera 10 millones de libras esterlinas en Bitcoin.

La NCA consideró el asunto de alta prioridad y los agentes especializados de lucha contra la ciberdelincuencia recibieron la tarea de identificar al perpetrador y evitar cualquier ataque potencial.

El perpetrador también envió correos electrónicos donde amenazaba con atacar a miembros del Parlamento y con hacer explotar una bomba contra los manifestantes de Black Lives Matter en Londres. Pese a escribir sus correos electrónicos en inglés, los investigadores utilizaron cibertécnicas especializadas, así como análisis lingüísticos y conductuales para deducir que probablemente el delincuente era un hablante nativo de alemán.

En colaboración con las autoridades alemanas, los agentes de la NCA descubrieron que los correos electrónicos estaban siendo enviados desde un ordenador situado en una dirección de Berlín. Gracias al trabajo colaborativo internacional y pese a los grandes esfuerzos por ocultar su identidad y su ubicación, se identificó al sospechoso, quien quedó bajo la vigilancia de los cuerpos y fuerzas de seguridad alemanes. El 15 de junio de 2020 se detuvo al sospechoso, quien fue acusado de intento de extorsión y permaneció en prisión preventiva. Fue sentenciado el 26 de febrero de 2021 y condenado a tres años de cárcel.

Tomar medidas a través del ciberespacio para combatir el terrorismo

Campaña contra el Dáesh: El trabajo del MOD y la GCHQ contra el Dáesh es un ejemplo de cómo hemos adoptado medidas activas para combatir las amenazas de aquellos que hacen un uso indebido del poder de Internet y las comunicaciones modernas.

El Dáesh dedicó mucho tiempo y energía a la tecnología, a crear contenido de medios utilizado para radicalizar y atraer a nuevos reclutas a sus filas e inspirar los ataques terroristas en todo el mundo. En los últimos años, hemos observado el impacto de este enfoque por toda Europa, incluidos los ataques de Londres y Manchester. El Dáesh también utilizaba los sistemas de comunicaciones modernos para ordenar y controlar sus operaciones sobre el campo de batalla. Esto les permitía operar de una manera flexible, a escala y a un ritmo constante y plantear un peligro aún mayor para las poblaciones que tenían la intención de controlar, así como maximizar su alcance a lo largo de lo que ellos denominaban «califato».

Durante la batalla de Mosul, la capital autodeclarada del Dáesh, utilizamos herramientas y técnicas cibernéticas en operaciones conjuntas con los militares en apoyo de la coalición y como parte de una campaña más amplia y de espectro completo. Los resultados de estas operaciones fueron de gran alcance. La interrupción de las comunicaciones, la degradación de la propaganda, la desconfianza creada dentro de los grupos y la denegación de equipos y redes utilizados como parte de sus operaciones fueron maneras de reducir la eficacia del Dáesh. También pudimos usar técnicas cibernéticas para promocionar los mensajes del Gobierno del RU a los objetivos, o destacar sus actividades a aquellos que sin saberlo podían estar facilitándoles ayuda. Estas operaciones realizaron una gran contribución a los esfuerzos de la coalición de suprimir la propaganda del Dáesh, dificultaron su capacidad de coordinar ataques y protegieron a las fuerzas de la coalición en el campo de batalla.

Andrew, miembro de la Ciberfuerza Nacional

Siempre me ha fascinado lo último en tecnología de vanguardia. Antes de trabajar para los servicios de inteligencia, me incorporé a la policía y fui ascendiendo en mi carrera desde agente de policía de patrulla hasta especializarme en la investigación forense digital, es decir, la investigación de dispositivos electrónicos de sospechosos en busca de pruebas. Me encantaba, pero quería ver qué otras oportunidades tenía a mi alcance.

No fui a la universidad tras dejar la escuela y, hasta ahora, el motor de mi carrera ha sido la curiosidad natural, y eso se aplica también a todos los compañeros que se incorporan a la Ciberfuerza Nacional. Provienen de todo tipo de orígenes distintos. Tenemos una base de expertos técnicos con conocimientos exhaustivos, así como a un antiguo gerente de supermercado, un profesor de primaria y un bombero. Pero lo que todos tenemos en común es una mente abierta, un gran deseo de aprender y un objetivo compartido de mantener al país seguro, detectando tanto las amenazas como las oportunidades que la tecnología emergente ofrece a seguridad nacional.

Como agente de policía, me sentí inmensamente orgulloso de poder ayudar a las personas a nivel personal. Hoy, como miembro de este exclusivo equipo de la Ciberfuerza Nacional, formo parte de una fuerza positiva a escala global.

Lograr nuestra ambición

190. Esta estrategia no significará nada sin un enfoque riguroso hacia la implementación de sus objetivos, la monitorización y la evaluación de su progreso y si no contamos con los mecanismos para cambiar de curso cuando sea necesario. En este capítulo se establece nuestro enfoque hacia la ejecución.

Funciones y responsabilidades del Gobierno

191. La Ciberestrategia Nacional será una de las subestrategias que colectivamente materializarán las ambiciones de la Revisión Integrada. El Consejo de Seguridad Nacional (NSC, *por sus siglas en inglés*) ejercerá una supervisión a nivel ministerial de estas estrategias, monitorizando la implementación y considerando el equilibrio general y la dirección de la estrategia del RU. El progreso relacionado con los objetivos de la estrategia también se evaluará a través del Marco de Planificación y Rendimiento (Planning and Performance Framework) del Gobierno y de los Planes de Entrega de Resultados (Outcome Delivery Plans).

192. Todos los ministros deben contribuir a asegurar que el RU consolide su posición como ciberpoder responsable y democrático, capaz de proteger y promover sus intereses en el ciberespacio. Esta lista incluye conjuntos de responsabilidades específicos para los ministros con funciones de liderazgo, tanto para implementar o coordinar uno o más de los cinco pilares de nuestra Ciberestrategia Nacional como para supervisar nuestras cibercapacidades y decisiones más importantes.

- **El Canciller del Ducado de Lancaster,** con el apoyo del **Tesorero General**, ofrece un liderazgo general a lo largo de los departamentos para garantizar una respuesta eficaz del Gobierno frente a las ciberamenazas, así como la consecución de nuestras ambiciones como ciberpoder. Esto incluye el desarrollo y la implementación de la Ciberestrategia Nacional, el programa de inversión que la sustenta y la coordinación de los esfuerzos gubernamentales relativos a la ciberresiliencia. También tienen una responsabilidad general de coordinación y política intersectorial relativa a la ciberseguridad y la resiliencia de la infraestructura nacional crítica del RU.

El Canciller del Ducado de Lancaster es el presidente por defecto de las reuniones ministeriales de la Sala de reuniones de la Oficina del Gabinete (COBR, *por sus siglas en inglés*) sobre los ciberincidentes, cuando estas son necesarias.

- **La Secretaria de Estado del Ministerio del Interior** tiene un papel clave en la provisión de la Ciberestrategia Nacional en su conjunto, así como en la respuesta a los ciberincidentes en línea con sus responsabilidades de seguridad nacional. Ella lidera la labor del Gobierno de detectar, interrumpir y disuadir a nuestros adversarios junto con la Secretaria de Estado de Relaciones Exteriores, Asuntos del Commonwealth y Desarrollo y el Secretario de Estado de Defensa y ofrece una coordinación general de ese trabajo. Asimismo, tiene la responsabilidad específica de combatir la ciberdelincuencia.

- **La Secretaria de Estado de Relaciones Exteriores, Asuntos del Commonwealth y Desarrollo** tiene una responsabilidad legal con respecto a la GCHQ y, por lo tanto, en relación con el Centro de Ciberseguridad Nacional. Ella lidera el trabajo del Gobierno de fomentar el liderazgo global del RU en cibernética y tiene una responsabilidad específica sobre el proceso de ciberatribución, el régimen de cibersanciones y la participación internacional en caso de ciberincidentes de gran calado. Asimismo, lidera el trabajo del Gobierno de detectar, interrumpir y disuadir a nuestros adversarios, junto con la Secretaria de Estado del Ministerio del Interior y el Secretario de Estado de Defensa.

- **El Secretario de Estado de Defensa** lidera el trabajo del Gobierno de detectar, interrumpir y disuadir a nuestros adversarios junto con la Secretaria de Estado de Relaciones Exteriores, Asuntos del Commonwealth y Desarrollo y la Secretaria de Estado del Ministerio del Interior.

- **La Secretaria de Estado de Relaciones Exteriores, Asuntos del Commonwealth y Desarrollo y el Secretario de Estado de Defensa** tienen la responsabilidad relativa a la Ciberfuerza Nacional, como un esfuerzo conjunto entre defensa e inteligencia.

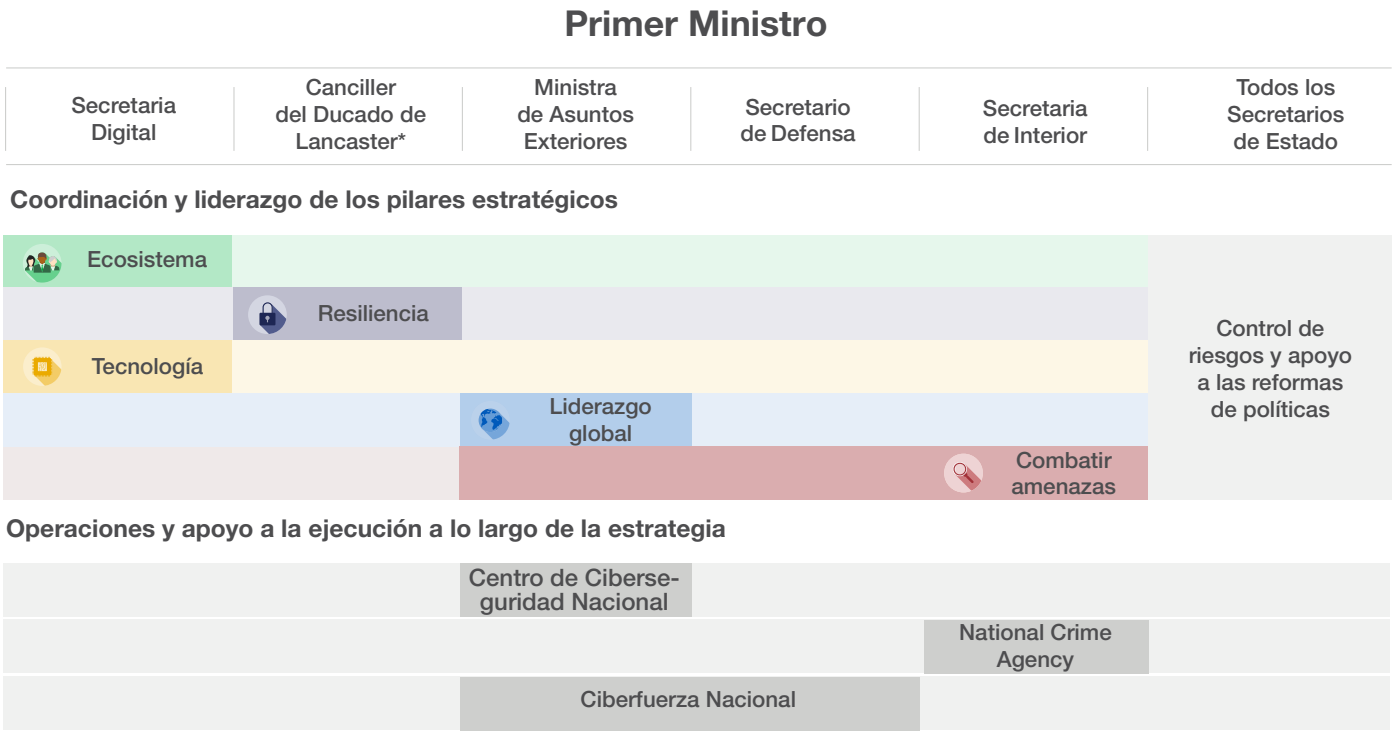
- **La Secretaria de Estado de Cultura, Medios de Comunicación y Deportes** lidera la ciberseguridad de organizaciones en la economía más amplia en lo que respecta a la política digital, y los aspectos pertinentes del crecimiento, la innovación y las habilidades de la Ciberestrategia Nacional. Lidera la labor del Gobierno de fortalecer el ciberecosistema del RU y de tomar la iniciativa en las tecnologías que son vitales para el ciberpoder.

- **Los ministros de todos los principales departamentos gubernamentales de infraestructuras nacionales esenciales** tienen responsabilidad sobre la política de ciberseguridad y resiliencia de sus respectivos sectores.

- **Todos los ministros** deberían encargarse de supervisar la ciberseguridad de sus departamentos y de implementar las mitigaciones pertinentes. Cuando un departamento supervisa un elemento del sector público o privado (por ejemplo, el DLUHC y el Gobierno local o DEFRA y las empresas de aguas) es el responsable de la ciberpolítica y de las actividades de aseguramiento relacionadas con ese sector.

193. El Viceasesor de Seguridad Nacional para Inteligencia, Seguridad y Resiliencia es el responsable principal de la estrategia y se encargará de dirigir la ejecución a lo largo del Gobierno a nivel oficial, con el respaldo de los funcionarios sénior pertinentes de los distintos departamentos.

Responsabilidades ministeriales



*ofrece un liderazgo general a lo largo de los distintos departamentos para garantizar una respuesta eficaz del Gobierno frente a las ciberamenazas, y la consecución de nuestras ambiciones como ciberpoder.

Invertir en nuestro ciberpoder

194. En los próximos tres años, el Gobierno invertirá 2600 millones de libras esterlinas en cibernética y TI heredada. Esto se suma a una inversión importante en la Ciberfuerza Nacional. Incluye un aumento de 114 millones de libras esterlinas en el Programa de Ciberseguridad Nacional, con unos gastos anuales en capacidad creada en virtud de la estrategia de 2016 que pasan a quedar bajo la gestión departamental con carácter permanente. Los programas internacionales se ejecutarán a través del Fondo de Conflicto, Estabilidad y Seguridad (CSSF, *por sus siglas en inglés*) con el fin de ayudar a países socios, desarrollar su ciberresiliencia y combatir las ciberamenazas. Esto se suma a los aumentos de financiación ya anunciados en I+D, inteligencia, defensa, innovación, infraestructura y habilidades, todos los cuales contribuirán en parte al ciberpoder del RU.[37]

Medición del éxito

195. Esta estrategia se regirá por un marco de desempeño en continuo desarrollo que rendirá cuentas ante los funcionarios sénior responsables y el Consejo de Seguridad Nacional. El marco se utilizará para fundamentar las discusiones con las instituciones parlamentarias y otros organismos que supervisan el trabajo de la comunidad de seguridad nacional. En concordancia con el enfoque de la Estrategia de Ciberseguridad Nacional 2016-2021, no será un documento público debido a la información confidencial que contiene, aunque el Gobierno publicará informes de progreso anuales.

196. Este marco de desempeño:

- Proporcionará una visión clara de cómo las actividades conducirán a los distintos objetivos indicados en la estrategia
- Garantizará la rendición de cuentas relativa a la ejecución de la estrategia
- Ofrecerá transparencia sobre los avances que está realizando el país en relación con los objetivos establecidos en la estrategia
- Ilustrará cómo debe adaptarse la actividad para situarla en línea con la estrategia
- Nos permitirá entender qué actividades son eficaces para la consecución de ambiciones estratégicas, de modo que podamos aplicar esas lecciones en el futuro
- Ofrecerá una visión integral de las actividades de los cinco pilares, reduciendo la duplicación e identificando los puntos fuertes y débiles del ciberpoder del país
- Garantizará que la estrategia proporcione apoyo cibernético a todos los sectores de la sociedad

[37] HM Treasury, Presupuesto y Revisión de Gastos de otoño 2021 (2021)

Próximos pasos

197. Esta estrategia tiene la intención de servir como guía de actuación, no solo para aquellos que están en el Gobierno y tienen responsabilidad sobre la cibernética y otras numerosas políticas asociadas (véase el Anexo A), sino también para todas las personas y organizaciones de la sociedad con un interés y responsabilidad con respecto a nuestro ciberesfuerzo nacional. También supone el inicio de una conversación que queremos continuar para garantizar que nuestros objetivos y prioridades continúen siendo relevantes durante los próximos cinco a diez años. Utilizaremos la publicación de esta estrategia como plataforma para continuar interactuando con los sectores público, privado y terciario a lo largo del RU y les invitamos a enviar sus comentarios directos a ukcyberstrategy@cabinetoffice.gov.uk. Comunicaremos de manera anual los avances que estamos realizando para implementar esa estrategia.

Anexo A: la cibernética como parte de la agenda más amplia del Gobierno

La Ciberestrategia Nacional tiene el propósito de dar apoyo y amplificar otras prioridades para el Gobierno en la agenda de seguridad, defensa, política exterior y economía. A su vez, esta estrategia dependerá de las capacidades más amplias desarrolladas a través de nuestro sistema educativo y de habilidades y de nuestro enfoque nacional hacia la política digital y la política tecnológica industrial, la investigación y el crecimiento empresarial. Las estrategias pertinentes y planes clave incluyen:

- **La Revisión Integrada**, que incluye los esfuerzos nacionales por mejorar la resiliencia, abordar las amenazas de Estados, combatir la delincuencia organizada grave y el terrorismo, mantener nuestra ventaja estratégica a través de la ciencia y la tecnología y conformar el orden internacional.
- **La Estrategia de Datos Nacional**, que establece nuestra misión de aprovechar el poder del uso responsable de los datos para aumentar la productividad, crear nuevos negocios y puestos de trabajo, mejorar los servicios públicos, apoyar a una sociedad más justa e impulsar los descubrimientos científicos, posicionando al RU como el precursor de la próxima ola de innovación. Esto incluye transformar el uso de los datos por parte del Gobierno para impulsar la eficiencia y mejorar los servicios públicos abordando las barreras a la compartición de datos entre departamentos y mejorando la calidad de los datos que almacenan. Esto será fundamental para respaldar nuestra ciberagenda, por ejemplo, para asegurarnos de que podamos recopilar y usar datos de buena calidad sobre los ciberincidentes
- **El plan de crecimiento,** que nos está ayudando a «**Build Back Better**» (Reconstruir mejor) a través de un apoyo y una inversión adicionales para la infraestructura, las habilidades y la innovación y de la «**Innovation Strategy**» (Estrategia de la innovación), que establece nuestras ambiciones para una economía liderada por la innovación
- **El Plan for Digital Regulation (Plan de Regulación Digital)**, que establece nuestro enfoque en favor de la innovación hacia la regulación de las tecnologías digitales de una manera que impulse la prosperidad y genere confianza en su uso
- **La National AI Strategy (Estrategia de IA Nacional)**, cuyo objetivo consiste en preparar al RU para la próxima década transformadora en IA mediante la inversión en las necesidades a largo plazo del ecosistema de IA, el apoyo a la transición a una economía basada en la inteligencia artificial y asegurándonos de que el RU acierte con la gobernanza nacional e internacional de las tecnologías de IA. Esto incluye medidas para apoyar la innovación cibersegura en sistemas basados en la inteligencia artificial protegiendo a la vez al público y generando confianza en su uso.
- La próxima **National Resilience Strategy (Estrategia de Resiliencia Nacional)**, que en parte se centrará en cómo el RU se mantendrá al día de las amenazas tecnológicas y conservará su resiliencia en el ciberespacio.
- La próxima **Estrategia Digital**, que establecerá una visión clara de las ambiciones del Gobierno para aprovechar el nuevo apetito por la transformación digital, acelerar el crecimiento y continuar desarrollando una economía digital más inclusiva, competitiva e innovadora para el futuro, todo lo cual se basará en las Diez Prioridades Tecnológicas del DCMS para continuar estableciendo las ambiciones del Gobierno con respecto al sector digital.
- **La Net Zero Strategy (Estrategia de Emisiones Netas Cero),** que garantizará que nuestra economía próspera e impulsada por la innovación tenga unas emisiones bajas de carbón.
- **El Beating Crime Plan (Plan para Vencer a la Delincuencia)**, que determina cómo restableceremos la confianza en el sistema de justicia penal y concretará nuestra visión compartida

de una Gran Bretaña más segura con menos delincuencia y menos víctimas.[38]

Existen otras dos publicaciones que apoyan directamente a la Ciberestrategia Nacional y que establecen cómo se lograrán partes individuales de la estrategia.

- La próxima **Estrategia de Ciberseguridad del Gobierno (Government Cyber Security Strategy)**, que establecerá planes más detallados para mejorar la seguridad del Gobierno y del sector público, en apoyo de esta estrategia nacional.
- La próxima **Revisión de Incentivos y Regulaciones de 2021 (Incentives & Regulations Review 2021)**, que indicará nuestras conclusiones sobre la eficacia de nuestro trabajo de incentivar las mejoras en la ciberseguridad dentro de la economía más amplia, y cómo proponemos implementar los elementos empresariales y organizativos del pilar de la resiliencia.

[38] Home Office, Beating Crime Plan (Plan para Vencer a la Delincuencia) (2021)

Anexo B: Normativas NIS – Estrategia Nacional

Introducción

Estrategia Nacional NIS

1. La Ciberestrategia Nacional está designada como la estrategia nacional del RU a efectos del Reglamento 2 de las Normativas de Redes y Sistemas de la Información (NIS) de 2018 del RU.

2. Este anexo ofrece información adicional que incluye:

- las funciones y responsabilidades de las autoridades clave responsables de la implementación de los NIS en el RU; y
- una lista de las autoridades clave implicadas.

Las Normativas NIS del RU

3. En 2016, la Comisión Europea acordó una Directiva con el fin de aumentar la seguridad de las redes y los sistemas de información en la Unión Europea (UE). La Directiva contó con el apoyo del Gobierno del RU.

4. El 20 de abril de 2018, el Gobierno presentó las nuevas Normativas de Redes y Sistemas de la Información (NIS) de 2018 ante el Parlamento. Esas normativas entraron en vigor el 10 de mayo de 2018.

5. Las Normativas NIS establecieron un nuevo régimen regulatorio en el RU que exige a los operadores designados de servicios esenciales (OES, *por sus siglas en inglés*) y a los proveedores de servicios digitales pertinentes (RDSP, *por sus siglas en inglés*) que tomen medidas técnicas y organizativas para garantizar la seguridad de sus redes y sistemas de información.

6. Se aplica a sectores que son esenciales para nuestra economía y sociedad y que dependen en gran medida de las redes y los sistemas de información: energía, transporte, agua potable, asistencia sanitaria e infraestructura digital.

7. Los proveedores de servicios digitales clave (motores de búsqueda, servicios de computación en la nube y mercados en línea) también quedan cubiertos por las normativas.

8. Las Normativas NIS establecen lo siguiente:

- **un marco nacional** que apoye la ejecución, incluida una estrategia nacional;
- **autoridades competentes** específicas del sector que actúen como reguladores;
- el Centro de Ciberseguridad Nacional (NCSC) como **Punto Único de Contacto** (SPOC, *por sus siglas en inglés*) y el **Equipo de Respuesta ante Incidentes de Seguridad Informática** (CSIRT, *por sus siglas en inglés*).

9. El progreso se mide a través de Revisiones Posimplementación cada 2 a 5 años.

Funciones y responsabilidades clave

Marco nacional

10. El Ministerio de la Presidencia británico es el responsable de la Ciberestrategia Nacional, que incluye la Estrategia Nacional NIS. Asimismo, el Ministerio de la Presidencia británico tiene la responsabilidad general de mejorar la seguridad y la resiliencia de la infraestructura nacional crítica.

11. El Ministerio Digital, de Cultura, Medios de Comunicación y Deportes británico (DCMS, *por sus siglas en inglés*) es responsable de la ejecución general de las Normativas NIS, incluida la coordinación de las autoridades pertinentes y el NCSC. El DCMS facilita orientación a las autoridades competentes para que apoyen una implementación de las normativas NIS más amplia a lo largo del RU.

Punto Único de Contacto (SPOC)

12. El punto de contacto nacional para la colaboración con socios internacionales [UE] en relación con las normativas NIS, encargado de coordinar las solicitudes de actuación o información y de presentar estadísticas de incidentes anuales. El Centro de Ciberseguridad Nacional es el SPOC del Reino Unido.

Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT)

13. El Centro de Ciberseguridad Nacional es el CSIRT del Reino Unido. Es el responsable de monitorear los incidentes de ciberseguridad a nivel nacional, proporcionando un análisis de amenazas a tiempo real, una defensa contra los ciberataques nacionales, asesoramiento técnico y una respuesta a ciberincidentes importantes para contribuir a minimizar los daños.

14. El NCSC mantiene el Marco de Evaluación Cibernético (CAF) basado en resultados y ofrece una orientación detallada sobre asuntos relativos a la ciberseguridad en calidad de autoridad técnica nacional.

Autoridades competentes

15. Son las responsables de supervisar y ejecutar las Normativas NIS en sus respectivos sectores, designar y evaluar el cumplimiento de los OES y RDSP con el fin de satisfacer los requisitos de las Normativas NIS. Se indican en el Apéndice 1 de las Normativas NIS y en el apartado 3 se facilita una lista.

Operadores de Servicios Esenciales (OES) y Proveedores de Servicios Digitales Pertinentes (RDSP)

16. Los OES o RDSP que cumplen los umbrales de designación de ese sector o que han sido designados por la autoridad pertinente en virtud del Reglamento 8(3) de las Normativas NIS deben cumplir los requisitos de las Normativas NIS.

17. Estas implican:

- tomar medidas técnicas y organizativas apropiadas y proporcionadas para gestionar los riesgos que afectan a la seguridad de las redes y los sistemas de información;
- tomar medidas adecuadas y proporcionadas para evitar y minimizar el impacto de los incidentes que afectan a la seguridad de las redes y los sistemas de información;
- notificar a la autoridad competente pertinente cualquier incidente que tenga una repercusión considerable en sus servicios;
- cumplir los requisitos de inspección en virtud de las Normativas NIS; y
- cumplir las notificaciones de información, ejecución y sanciones.
- Los RDSP tienen la obligación de registrarse con la ICO.

Otras autoridades pertinentes:

18. El Gobierno del RU trabaja estrechamente con las administraciones descentralizadas y otras autoridades pertinentes, incluidos los principales departamentos gubernamentales, en la implementación de las Normativas NIS.

19. El Centro para la Protección de la Infraestructura Nacional (CPNI, *por sus siglas en inglés*) proporciona asesoramiento sobre seguridad física y del personal asociada.

Lista de autoridades clave para la implementación de las NIS

Autoridades nacionales	
Las Normativas NIS del RU	Ministerio Digital, de Cultura, Medios de Comunicación y Deportes británico
Ciberestrategia Nacional del RU	Ministerio de la Presidencia británico
Punto Único de Contacto del RU (SPOC)	Centro de Ciberseguridad Nacional
Equipo de Respuesta ante Incidentes de Seguridad Informática del RU (CSIRT)	Centro de Ciberseguridad Nacional

Autoridades competentes					
Sector	**Subsector**	**Inglaterra**	**Gales**	**Escocia**	**Irlanda del Norte**
Energía	Electricidad	Conjunto: Departamento de Negocios, Energía y Estrategia Industrial y la Autoridad de Mercados del Gas y la Electricidad (Ofgem, *por sus siglas en inglés*)			Departamento de Finanzas
	Petróleo	Departamento de Negocios, Energía y Estrategia Industrial			Departamento de Finanzas
	Gas	Conjunto: Departamento de Negocios, Energía y Estrategia Industrial y la Autoridad de Mercados del Gas y la Electricidad (Ofgem, *por sus siglas en inglés*)[39]			Departamento de Finanzas
Transporte	Aire	Conjunto: Departamento de Transporte y la Autoridad de la Aviación Civil (CAA, *por sus siglas en inglés*)			
	Ferroviario	Departamento de Transporte			Departamento de Finanzas
	Agua	Departamento de Transporte			
	Carretera	Departamento de Transporte		Ministros escoceses	Departamento de Finanzas
Asistencia sanitaria	Ámbitos de asistencia sanitaria	Departamento de Salud y Atención Social	Ministros galeses	Ministros escoceses	Departamento de Finanzas
Agua potable	Agua potable	Departamento de Medio Ambiente, Alimentación y Asuntos Rurales	Ministros galeses	Regulador de la Calidad del Agua Potable de Escocia (DWQR, *por sus siglas en inglés*)	Departamento de Finanzas
Infraestructura digital	Infraestructura digital	Oficina de Comunicación (Ofcom, *por sus siglas en inglés*)			

[39] Para ciertas excepciones el Departamento de Negocios, Energía y Estrategia Industrial es la única autoridad competente. Para obtener más información, consulte los Apéndices 1 y 2 de las Normativas de Redes y Sistemas de la Información de 2018.

Anexo C: Glosario

Action Fraud: el centro de denuncias de fraude y ciberdelitos donde los ciudadanos y las organizaciones pueden presentar sus denuncias en caso de haber sido víctimas de estafas, fraudes o ciberdelitos en Inglaterra, Gales e Irlanda del Norte. En Escocia, las denuncias se dirigen a la Policía de Escocia (Police Scotland).

Autenticación: el proceso de verificación de la identidad, u otros atributos de un usuario, proceso o dispositivo.

Autoridades competentes: organismos reguladores según lo descrito en las Normativas de Redes y Sistemas de la Información (NIS) de 2018. Existen múltiples autoridades competentes responsables de distintos sectores cubiertos por las NIS.

Centro de Ciberseguridad Nacional (NCSC): la autoridad técnica del RU para las ciberamenazas que proporciona una respuesta nacional unificada frente a los ciberincidentes para minimizar los daños y que ayuda con la recuperación y las lecciones a aprender para el futuro.

Centro de Coordinación Cibernética del Gobierno (GCCC, *por sus siglas en inglés*): iniciativa conjunta propuesta entre GSG, la Oficina Central Digital y de Datos (CDDO, *por sus siglas en inglés*) y el NCSC que reúne sus respectivas funciones y áreas de experiencia para coordinar mejor los esfuerzos de ciberseguridad operativa a lo largo del Gobierno, transformar cómo se utilizan los datos sobre ciberseguridad y la inteligencia sobre amenazas en el Gobierno y mejorar verdaderamente la capacidad del Gobierno de «defenderse como uno».

Ciberamenaza: cualquier cosa capaz de poner en peligro la seguridad de, o causar daños a, los sistemas de información y dispositivos conectados a Internet (incluidos *hardware, software* e infraestructuras asociadas), los datos que hay en ellos y los servicios que ofrecen, principalmente por medios cibernéticos.

Ciberataque: explotación deliberada de sistemas informáticos, empresas y redes que dependen del mundo digital, para causar daños.

Ciberdefensa Activa (ACD, *por sus siglas en inglés*): ayuda a las organizaciones a encontrar y solucionar vulnerabilidades, gestionar incidentes o automatizar la interrupción de ciberataques. Algunos servicios están concebidos principalmente para el sector público, mientras que otros están disponibles más ampliamente para el sector privado o los ciudadanos, en función de su aplicabilidad y viabilidad.

Ciberdelincuencia: delitos que dependen del mundo cibernético (delitos que solo pueden cometerse mediante la utilización de dispositivos TIC, en los cuales el dispositivo es tanto la herramienta para cometer el delito como el blanco del delito); o delitos ciberhabilitados (delitos que pueden ser cometidos sin dispositivos TIC, como el fraude financiero, pero que han cambiado significativamente en cuanto a escala y alcance debido al uso de las TIC).

Ciberecosistema: la totalidad de la infraestructura, personas, procedimientos, datos, información y tecnologías de la comunicación interconectados, junto con el entorno y las condiciones que influyen en esas interacciones.

Ciberincidente: un incidente que presenta una amenaza real o potencial para un ordenador, un dispositivo conectado a Internet o una red —o para los datos procesados, almacenados o transmitidos en estos sistemas— que tal vez requiera una medida de respuesta para mitigar las consecuencias.

Ciberofensiva: añadir, eliminar o manipular datos en sistemas o redes para lograr un efecto físico, virtual o cognitivo. Las operaciones ciberofensivas a menudo explotan vulnerabilidades técnicas, utilizan sistemas o redes de maneras que sus propietarios y operadores no tendrían la intención de utilizar o no apoyarían, y pueden basarse en el engaño o la tergiversación.

Ciberresiliencia: la capacidad general de los sistemas y las organizaciones y ciudadanos para soportar los cibereventos y, cuando se producen perjuicios, recuperarse de estos.

Ciberriesgo: el potencial de que una determinada ciberamenaza explote las vulnerabilidades de un sistema de información y cause daños.

Ciberseguridad: la protección de sistemas conectados a Internet (incluidos *hardware, software* e infraestructuras asociadas), los datos que hay en ellos y los servicios que ofrecen frente a accesos no autorizados, daños o usos indebidos. Esto incluye los daños causados intencionalmente por el operador del sistema, o accidentalmente, como resultado de no seguir los procedimientos de seguridad o de ser manipulado para no hacerlo.

Cinco Ojos: «Cinco Ojos» es el nombre de la alianza de inteligencia entre los EE. UU., el Reino Unido, Canadá, Australia y Nueva Zelanda que contribuye a la compartición de información con el fin de mantener a sus ciudadanos lo más seguros posible frente a las amenazas.

COBR: salas de reuniones de la Oficina del Gabinete. La respuesta del Gobierno central del RU frente a las emergencias tiene como base el uso de COBR. Se trata de una ubicación física, habitualmente situada en Westminster, desde la cual se activa, monitoriza y coordina la respuesta central y que proporciona un punto focal para la respuesta del Gobierno y una fuente fidedigna de asesoramiento para los respondedores locales.

Criptografía: la ciencia o estudio que consiste en analizar y descifrar códigos y cifras; criptoanálisis.

Criptomoneda: una divisa y sistema de pago digitales como, p. ej., el Bitcoin.

Crypt-Key (CK, *por sus siglas en inglés*): el término utilizado para describir el uso de la criptografía por parte del RU para proteger la información y los servicios esenciales de los que dependen el Gobierno del RU y la comunidad militar y de la seguridad nacional, que incluye la protección frente a los ataques de nuestros adversarios más capaces.

Cyber Security Body of Knowledge (CyBOK): un recurso único que por primera vez ofrece un conjunto de conocimientos que comprende la amplitud y la profundidad de la ciberseguridad, demostrando así que la ciberseguridad abarca una amplia variedad de disciplinas.

Dominio: un nombre de dominio ubica a una organización u otra entidad en Internet y corresponde a una dirección de protocolo de Internet (IP).

Espacios conectados: una comunidad que integra tecnologías de la información y la comunicación y dispositivos IdC para recopilar y analizar datos con el fin de ofrecer nuevos servicios al entorno construido y de mejorar la calidad de vida de los ciudadanos.

GCHQ: sede de comunicaciones del Gobierno; el centro de las actividades de inteligencia de señales del Gobierno y la Autoridad Técnica Cibernética Nacional (NTA, *por su siglas en inglés*).

Gemelo digital: una réplica o representación virtual de activos, procesos, sistemas o instituciones en los entornos construidos, societarios o naturales que ofrece información sobre cómo se comportan los activos físicos complejos y los ciudadanos, ayudando a las organizaciones a mejorar la toma de decisiones y a optimizar procesos. Los cambios en el mundo real se reflejan en el gemelo, y los cambios en el gemelo se pueden replicar automáticamente en el mundo real.

Gestión de incidentes: la gestión y coordinación de actividades para investigar y remediar la ocurrencia real o potencial de un ciberevento adverso que pueda poner en peligro o dañar un sistema o red.

GFCE: Foro Global sobre Experiencia Cibernética.

Gobierno descentralizado o administración descentralizada: las legislaturas y ejecutivos independientes de Escocia, Gales e Irlanda del Norte tras la descentralización, responsable de numerosos asuntos de política nacional y con el poder de promulgar leyes para esas áreas.

ICANN: Corporación de Internet para la Asignación de Nombres y Números. Se encarga de coordinar nombres de sitios web y direcciones de IP.

Infraestructura Crítica Nacional: aquellos elementos críticos de la infraestructura (concretamente activos, instalaciones, sistemas, redes o procedimientos y los trabajadores esenciales que los operan y los facilitan) cuya pérdida podría tener como resultado:

a. un impacto perjudicial importante en la disponibilidad, integridad o prestación de servicios esenciales —incluidos los servicios cuya integridad, en caso de verse comprometida, podría derivar en una cantidad importante de fallecidos o víctimas— teniendo en cuenta los importantes impactos económicos y sociales; y/o

b. un impacto significativo en la seguridad nacional, la defensa nacional, o el funcionamiento del Estado.

Integridad: en seguridad de la información, integridad significa que la información no se ha modificado accidental o deliberadamente, que es exacta y completa.

Inteligencia artificial: una tecnología en la cual un sistema informático se codifica para que «piense por sí mismo», adaptándose y operando de manera autónoma. La IA se utiliza cada vez más en más tareas complejas, como el diagnóstico médico, el descubrimiento de medicamentos y el mantenimiento predictivo.

Internet: una red informática global que ofrece una variedad de sistemas de información y comunicación y que consiste en redes interconectadas que utilizan protocolos de comunicación estandarizados.

Internet de las cosas: la totalidad de dispositivos, vehículos, edificios y otros artículos con electrónica, *software* y sensores integrados que se comunican e intercambian información en Internet.

Marco de Ciberevaluación (CAF, *por sus siglas en inglés*): proporciona un enfoque sistemático y exhaustivo hacia la evaluación de la medida en la cual los ciberriesgos para las funciones esenciales están siendo gestionados por la organización responsable.

Microgeneración: generación de energía a pequeña escala por parte de hogares, pequeñas empresas y comunidades.

NCA: National Crime Agency (Agencia Nacional de Lucha contra la Delincuencia)

Normativas de Redes y Sistemas de la Información (NIS) de 2018: normativas del RU que establecen medidas legales para incrementar el nivel de seguridad (tanto la resiliencia física como la ciberresiliencia) de las redes y los sistemas de información para la provisión de servicios esenciales y servicios digitales.

Observación del panorama: un análisis sistemático de la información para identificar amenazas, riesgos, problemas emergentes y oportunidades potenciales que permita una mejor preparación y la incorporación de la mitigación y explotación en el proceso de elaboración de políticas.

OCDE: la Organización para la Cooperación y el Desarrollo Económicos, una organización económica intergubernamental.

Operadores de servicios esenciales: organizaciones en sectores esenciales que dependen en gran medida de las redes de información como, por ejemplo, servicios públicos, asistencia sanitaria, transporte y sectores de infraestructura digital según lo identificado por los criterios establecidos en las Normativas de Redes y Sistemas de la Información (NIS) de 2018.

OTAN: Organización del Tratado del Atlántico Norte.

Plan de regulación digital: establece el enfoque general del Gobierno hacia la gestión de las tecnologías digitales con el fin de impulsar el crecimiento y la innovación.

Proveedores de servicios gestionados: terceros que proporcionan un conjunto de servicios definidos a un cliente y asumen la responsabilidad de ejecutar, mantener y garantizar esos servicios.

***Ransomware*:** *software* malicioso que deniega al usuario el acceso a sus archivos, ordenador o dispositivo hasta que se pague un rescate.

Respuesta ante incidentes: las actividades para responder a los efectos directos y a corto plazo de un incidente, que también pueden apoyar la recuperación a corto plazo.

Revisión integrada: «Gran Bretaña Global en una Era Competitiva, la Revisión Integrada de Seguridad, Defensa, Desarrollo y Política Exterior» describe la visión del Gobierno sobre el papel del RU en el mundo durante la próxima década y las actuaciones que llevará a cabo el Gobierno hasta 2025.

Seguro por diseño: *software, hardware* y sistemas que han sido diseñados desde cero para ser seguros.

Servicio de notificación de vulnerabilidades: un mecanismo por el cual una organización puede ser alertada de fallos en la seguridad antes de que estos puedan ser explotados por atacantes.

Sistema autónomo: una colección de redes IP cuyo enrutamiento está controlado por una entidad o dominio específico.

Sistema de control industrial (ICS, *por sus siglas en inglés*): un sistema de información utilizado para controlar los procesos industriales, como la fabricación, el manejo de productos, la producción y la distribución, o el control de activos de infraestructura.

Tecnología de cadena de bloques: una manera específica de almacenar datos. Una cadena de bloques es un ejemplo de registro distribuido, un tipo de tecnología de almacenamiento para adjuntar únicamente y a prueba de manipulaciones.

Tecnologías cuánticas: la tecnología cuántica se basa en los principios de la física cuántica. El entendimiento avanzado y el control de lo que se conoce como «efectos cuánticos», como la superposición y el entrelazamiento, conducirá a una nueva ola de avances que cimentará nuestra economía y sociedad: detección, transmisión y cifrado de datos, sincronización y computación.

Tecnologías operativas (OT, *por sus siglas en inglés*): combinan el *hardware* y el *software* para monitorizar, controlar y automatizar procesos físicos, especialmente en sectores industriales como la energía, la fabricación, el agua y el transporte.

TI heredada: la TI heredada hace referencia a los sistemas y sus componentes de *software* y *hardware* que han dejado de recibir asistencia por parte del comerciante, que tienen una asistencia prolongada en el tiempo y/o que están sujetos a acuerdos de asistencia personalizados.

Violación de datos: el movimiento o la diseminación no autorizados de información en una red a una parte no autorizada para que acceda a la información o la visualice.

Vulnerabilidad: errores en programas de *software* que tienen el potencial de ser explotados por atacantes.