HM Government

ESTRATEGIA DE CIBERSEGURIDAD NACIONAL 2016-2021

Contenido

PREFACIO

El Reino Unido es uno de los países digitales más destacados del mundo. Gran parte de nuestra prosperidad depende de nuestra capacidad de proteger nuestra tecnología, datos y redes de las múltiples amenazas a las que nos enfrentamos.

Sin embargo, los ciberataques son cada vez más frecuentes, sofisticados y perjudiciales, cuando logran su cometido. Por lo tanto, hemos tomado medidas contundentes para proteger tanto nuestra economía como la privacidad de los ciudadanos del Reino Unido.

Nuestra Estrategia de ciberseguridad nacional presenta nuestro plan para que el Reino Unido tenga confianza, capacidad y resiliencia en un mundo digital que evoluciona rápidamente.

Durante la vida de esta estrategia a cinco años, invertiremos 1900 millones de libras esterlinas para defender nuestros sistemas e infraestructura, disuadir a nuestros adversarios y desarrollar la capacidad de toda la sociedad, desde las empresas más grandes hasta los mismos ciudadanos.

Desde la higiene cibernética más básica, hasta las estrategias de disuasión más sofisticadas, necesitamos una respuesta integral.

Nos centraremos en elevar los costos de organizar un ataque contra cualquier persona en el Reino Unido, tanto a través de defensas más fuertes como por medio de mejores pericias cibernéticas. Ya no se trata solamente de algo que atañe al departamento de informática sino a todos los equipos de trabajo. Las pericias cibernéticas tienen que tenerlas todas las profesiones.

El nuevo Centro de ciberseguridad nacional será un hub que brinde conocimientos de primera categoría, fáciles de utilizar para empresas e individuos, así como también respuesta rápida en caso de incidentes graves.

El gobierno tiene claramente el papel de líder, pero también fomentará un ecosistema comercial más amplio, que reconozca dónde puede innovar el sector de forma más rápida que nosotros. Eso incluye un impulso para atraer a los talentos jóvenes más prometedores al ámbito de la ciberseguridad.

La amenaza cibernética impacta a toda nuestra sociedad, por lo que queremos dejar muy claro que todos juegan un papel en nuestra respuesta nacional. Por eso esta estrategia es un ejercicio de transparencia sin precedente. Ya no podemos permitirnos tener este debate a puertas cerradas.

En última instancia, ésta es una amenaza que no puede eliminarse totalmente. Las tecnologías digitales funcionan porque son abiertas, y esa misma apertura conlleva el riesgo. Lo que podemos hacer es reducir la amenaza para asegurarnos que nos mantenemos a la vanguardia en la revolución digital. Esta estrategia explica cómo lograrlo.

Honorable Philip Hammond MP, Ministro de hacienda

PRÓLOGO

Nuestra responsabilidad principal es mantener el país a salvo y brindar un gobierno competente. Esta estrategia refleja estas obligaciones. Es un enfoque audaz y ambicioso para responder a las múltiples amenazas a las que se enfrenta nuestro país en el ciberespacio. Gestionar y mitigar estas amenazas es una tarea para todos nosotros, pero el gobierno reconoce su responsabilidad específica para liderar a la nación en los esfuerzos que se requieren.

El gobierno está comprometido a asegurar que los compromisos establecidos en esta estrategia se lleven a cabo y que hagamos un monitoreo adecuado e informes regulares sobre los avances para alcanzarlos. También comprobaremos que nuestro enfoque es adecuado y responderemos a cambios en el nivel de amenaza al que nos enfrentamos, así como a las evoluciones en las tecnologías de seguridad.

El gobierno también tiene una responsabilidad especial ante los ciudadanos, las empresas y las organizaciones que trabajan en el Reino Unido, y con nuestros aliados y socios internacionales. Deberíamos ser capaces de asegurarles que se hacen todos los esfuerzos necesarios para que el sistema sea seguro y para proteger nuestros datos y redes de ataques o interferencias. Por lo tanto, tenemos que establecer los estándares más elevados de ciberseguridad y asegurar que cumplamos con ellos, tanto como fundamento de la seguridad nacional del país y su bienestar económico, como ejemplo a seguir para otros. Tendremos que informar sobre los avances logrados anualmente.

Como ministro de la Oficina del gabinete, responsable de ciberseguridad y seguridad del gobierno, he decidido firmemente que quiero que esta estrategia se implemente en su totalidad. Trabajaré muy de cerca con colegas de todo el gobierno y con socios en las administraciones descentralizadas - Escocia, Gales e Irlanda del Norte -, el sector público en su totalidad, la industria y el mundo académico para asegurarnos de lograr esta ambición.

Honorable Ben Gummer MP,
Ministro de la oficina del gabinete y Tesorero general

1. RESUMEN EJECUTIVO

1.1. El futuro de la seguridad y prosperidad del Reino Unido depende de sus cimientos digitales. El desafío de nuestra generación es construir una sociedad digital floreciente que por un lado sea resiliente ante las ciberamenazas y por otro esté equipada con el conocimiento y las capacidades necesarias para maximizar las oportunidades y gestionar los riesgos.

1.2. Dependemos totalmente de Internet. Sin embargo, es intrínsecamente inseguro y siempre habrá intentos de explotar sus debilidades lanzando ciberataques. Esta amenaza no puede eliminarse totalmente, pero el riesgo puede reducirse considerablemente hasta un nivel que permita que la sociedad siga prosperando, y se beneficie de las enormes oportunidades que brindan las tecnologías digitales.

1.3. La Estrategia de ciberseguridad nacional 2011, con el respaldo del Programa de ciberseguridad nacional del gobierno británico de 860 millones de libras esterlinas, han conseguido mejoras significativas en la ciberseguridad del Reino Unido. Logró resultados importantes dependiendo del mercado para impulsar cibercomportamientos seguros. Sin embargo, su enfoque no ha conseguido la escala y la velocidad de cambio que se requieren para estar al frente de esta amenaza que avanza a un paso muy veloz. Ahora necesitamos ir más allá.

1.4. Nuestra visión para el 2021 es la de un Reino Unido seguro y resiliente a las ciberamenazas, próspero y que confía en el mundo digital.

1.5 Para lograr esta visión trabajaremos para conseguir los siguientes objetivos:

- DEFENDER Tenemos los medios para defender al Reino Unido contra las ciberamenazas que evolucionan, para responder eficazmente a los incidentes, para asegurar que las redes, los datos y los sistemas del Reino Unido estén protegidos y sean resilientes. Los ciudadanos, empresas y el sector público tienen los conocimientos y las habilidades para defenderse.
- DISUADIR El Reino Unido será un blanco difícil para toda forma de agresión en el ciberespacio. Detectamos, entendemos, investigamos e interrumpimos las acciones hostiles emprendidas contra nosotros, perseguimos y enjuiciamos a los infractores. Tenemos los medios para tomar medidas ofensivas en el ciberespacio, si decidimos tomarlas.
- DESARROLLAR Tenemos un sector de ciberseguridad innovador, cada vez más grande, respaldado por investigación y desarrollos científicos líder en el mundo. Tenemos una cartera de talentos en curso autosostenible que brinda las habilidades para responder a nuestras necesidades nacionales en los sectores público y privado. Nuestro análisis y experiencia de vanguardia permitirán al Reino Unido cumplir y superar las amenazas y desafíos futuros.

1.6. Respaldando estos objetivos, buscaremos que haya ACCIÓN INTERNACIONAL y emplearemos nuestra influencia para invertir en alianzas que den forma a la evolución global del ciberespacio de tal modo que empuje nuestros intereses económicos más amplios y de seguridad. Fortaleceremos nuestros vínculos con nuestros socios internacionales más cercanos, reconociendo que esto mejora nuestra seguridad colectiva. También desarrollaremos las relaciones con nuevos socios para fortalecer sus niveles de ciberseguridad y proteger los intereses del Reino Unido en el extranjero. Lo haremos tanto de forma bilateral como multilateral, incluidos la UE, la OTAN y las Naciones Unidas. Enviaremos mensajes claros sobre las consecuencias para los adversarios que amenazan con dañar nuestros intereses, o los de nuestros aliados, en el ciberespacio.

1.7. Para lograr estos resultados en los próximos cinco años, el gobierno del Reino Unido busca intervenir de manera más activa y realizar una mayor inversión, al seguir apoyando a las fuerzas del mercado para elevar los estándares de ciberseguridad en el Reino Unido. El gobierno del

Reino Unido, en alianza con las administraciones descentralizadas de Escocia, Gales e Irlanda del Norte, trabajará con los sectores privado y público para asegurar que las personas, las empresas y las organizaciones adopten los comportamientos necesarios para estar a salvo en Internet. Estableceremos medidas para intervenir (cuando sea necesario y dentro del ámbito de nuestras competencias) para impulsar mejoras en el interés nacional, sobre todo en relación con la ciberseguridad de nuestras infraestructuras nacionales críticas.

1.8. El gobierno del Reino Unido aprovechará sus capacidades y las del sector para desarrollar y aplicar medidas de ciberdefensa activa[1] para mejorar significativamente los niveles de ciberseguridad en las redes de todo el Reino Unido. Estas medidas incluyen minimizar las formas más comunes de ataques por phishing, filtrando las direcciones IP nocivas, y bloqueando activamente las actividades maliciosas online. Mejorar las ciberseguridad básica hará que aumente la resiliencia del Reino Unido ante las ciberamenazas que se efectúan más comúnmente.

1.9. Creamos un Centro de ciberseguridad nacional (NCSC por sus siglas en inglés) para que se convierta en la autoridad sobre el entorno de ciberseguridad del Reino Unido, para compartir conocimientos, responder a las vulnerabilidades sistémicas y brindar liderazgo sobre cuestiones clave de ciberseguridad nacional.

1.10. Nos aseguraremos de que todas nuestras fuerzas armadas sean resilientes y tengan las ciberdefensas necesarias para proteger y defender sus redes y plataformas, para seguir operando y conservando su libertad de acción global a pesar de las ciberamenazas. Nuestro Centro militar de operaciones de ciberseguridad trabajará de cerca con el NCSC y se asegurará de que las fuerzas armadas puedan prestar asistencia en caso de recibir un ciberataque nacional importante.

1.11. Contaremos con los medios para responder a los ciberataques tal y como respondemos a cualquier otro ataque, utilizando la capacidad más apropiada, incluida una cibercapacidad ofensiva.

1.12. Utilizaremos la autoridad y la influencia del gobierno británico para invertir en programas que respondan a la escasez de habilidades en ciberseguridad del Reino Unido, desde las escuelas y universidades hasta toda la fuerza laboral.

1.13. Lanzaremos dos centros de ciberinnovación para impulsar el desarrollo de ciberproductos de vanguardia y nuevas empresas de ciberseguridad dinámicas. También asignaremos una proporción del Fondo de defensa y ciberinnovación de 165 millones de libras esterlinas para apoyar adquisiciones y contratación en defensa y seguridad innovadoras.

1.14. Invertiremos un total de 1900 millones de libras esterlinas en los próximos cinco años para transformar significativamente la ciberseguridad en el Reino Unido.

[1] Entender las amenazas para las redes, e idear e implementar medidas para combatir a o defenderse contra todas esas amenazas de manera proactiva. Vea el glosario para una explicación de la terminología técnica.

2. INTRODUCCIÓN

2.1. Las tecnologías de la información y la comunicación han evolucionado en los últimos veinte años y ahora están integradas prácticamente en todos los aspectos de nuestras vidas. El Reino Unido es una sociedad digitalizada. Esto enriquece nuestra economía y nuestra vida diaria.

2.2. La transformación que aporta la digitalización crea nuevas dependencias. Nuestra economía, la administración del gobierno y la provisión de servicios esenciales ahora dependen de la integridad del ciberespacio y la infraestructura, los sistemas y los datos que la apoyan. Una pérdida de confianza en cuanto a la integridad pondría en peligro los beneficios de la revolución tecnológica.

2.3. Gran parte del software y el hardware que se crean originalmente para facilitar este entorno digital interconectado han dado prioridad a la eficiencia, el costo y la conveniencia para el usuario, pero no siempre han incluido la seguridad desde su incepción. Actores malintencionados, estados hostiles, individuos y organizaciones criminales o terroristas, pueden explotar esta brecha entre la conveniencia y la seguridad. Reducir esta brecha es una prioridad nacional.

2.4. La expansión del Internet más allá de las computadoras y los celulares, dentro de otros sistemas ciberfísicos o *smart* amplía la amenaza de explotación remota para toda una serie de nuevas tecnologías. Los sistemas y las tecnologías que respaldan nuestra vida diaria, como las redes de suministro eléctrico, los sistemas de control del tráfico aéreo, los satélites, las tecnologías médicas, las plantas industriales y los semáforos, están conectados a Internet y, por lo tanto, son potencialmente vulnerables a injerencias.

2.5. La Estrategia de seguridad nacional (NSS por sus siglas en inglés) de 2015 reiteró que las ciberamenazas son riesgos de primer nivel para los intereses del Reino Unido. La NSS establece la determinación del gobierno de abordar las ciberamenazas y “establecer medidas fuertes e innovadoras, como líder mundial en ciberseguridad”. Esta Estrategia de ciberseguridad nacional cumple con este compromiso.

2.6. Al preparar esta nueva estrategia, el gobierno está construyendo sobre los logros, objetivos y criterios de la primera Estrategia de ciberseguridad nacional a cinco años del 2011. El gobierno invirtió 860 millones de libras esterlinas durante ese período y está orgulloso de lo que se ha logrado. Las políticas, instituciones e iniciativas desarrolladas durante los últimos cinco años han ayudado a establecer al Reino Unido como protagonista global en ciberseguridad.

2.7. Estos son cimientos sólidos. Sin embargo, la persistencia e ingenuidad de los que nos pueden amenazar, la prevalencia de nuestras vulnerabilidades y las brechas en nuestras capacidades y defensas significan que necesitamos trabajar todavía más arduamente para seguirle el paso a la amenaza. Es necesario un enfoque integral si queremos resguardar eficazmente nuestros ciberintereses. Nuestra resolución de hacer más inversiones e intervenciones se basa en las evaluaciones siguientes:

- la escala y la naturaleza dinámica de las ciberamenazas, y nuestra vulnerabilidad y dependencia, significan que mantener el enfoque actual no bastará por sí mismo para mantenernos a salvo;
- un enfoque que se basa en el mercado para promover la ciberhigiene no ha producido la velocidad ni la escala de cambio que se requieren. Por lo tanto, el gobierno tiene que liderar e intervenir de manera más directa para aplicar su influencia y sus recursos para responder a las ciberamenazas;
- el gobierno por sí solo no puede responder a todos los aspectos de ciberseguridad de la nación. Se necesita un enfoque integrado y sostenible en el cual los ciudadanos, la industria y otros socios en la sociedad y el

gobierno, jueguen plenamente su papel para proteger nuestras redes, servicios y datos;
• el Reino Unido necesita un sector de ciberseguridad vibrante y una base de pericias que lo apoyen para que pueda seguirle el paso y adelantarse a la amenaza que cambia constantemente.

EL ALCANCE DE LA ESTRATEGIA

2.8. Esta estrategia fue concebida para darle forma a la política del gobierno, y ofrecer al mismo tiempo una visión coherente y convincente para compartir con el sector público y privado, la sociedad civil, el mundo académico y la población en general.

2.9. La estrategia cubre todo el Reino Unido. El gobierno del Reino Unido buscará asegurarse de que se implemente la estrategia en todo el Reino Unido, reconociendo que, en los puntos en que tenga que ver con cuestiones transferidas a las administraciones descentralizadas, trabajaremos de cerca con éstas en cuanto a su aplicación en Escocia, Gales e Irlanda del Norte (respetando las tres jurisdicciones legales separadas, y los cuatro sistemas educativos que existen en el Reino Unido). Cuando las propuestas de la estrategia se refieran a temas transferidos, conforme sea apropiado se acordará su implementación con los gobiernos de acuerdo con los acuerdos de descentralización.

2.10. La estrategia establece acciones que se sugieren o recomiendan que se dedican a todos los sectores de la economía y la sociedad, desde los departamentos del gobierno central, hasta los líderes de toda la industria y los ciudadanos. La estrategia busca aumentar la ciberseguridad en todos los niveles para nuestro beneficio colectivo y será la base a partir de la cual participará el Reino Unido a nivel internacional para promover una buena gobernanza de Internet.

2.11. En esta estrategia, la ciberseguridad se refiere a la protección de los sistemas de información (hardware, software e infraestructuras asociadas), los datos en ellos, y los servicios que brindan, ante el acceso no autorizado, daño y uso indebido. Esto incluye el daño causado de forma intencional por el operador del sistema, o accidentalmente, como resultado de no seguir los procedimientos de seguridad.

2.12. Acorde con nuestra evaluación del desafío al que nos enfrentamos y continuando con los logros de la estrategia del 2011, este documento presenta:
• nuestra evaluación actualizada del contexto estratégico, incluidas las amenazas actuales y que evolucionan: quienes presentan la amenaza más grave a nuestros intereses, y las herramientas a su disposición;
• una revisión de vulnerabilidades y cómo se han desarrollado en los últimos cinco años;
• la visión de ciberseguridad del gobierno para el 2021 y los objetivos clave para lograr la meta, incluidos los principios rectores, los roles y responsabilidades, y cómo y cuándo la intervención del gobierno marcará la diferencia;
• cómo planeamos poner en práctica nuestra políticas: estableciendo en qué áreas será líder el gobierno y cuándo esperamos trabajar asociándonos con otros, y
• cómo pretendemos evaluar nuestro avance en comparación con nuestros objetivos.

3
. CONTEXTO ESTRATÉGICO

3.1. Cuando se publicó la última Estrategia de ciberseguridad nacional en 2011, la escala del cambio tecnológico y su impacto ya eran aparentes. La tendencia y las oportunidades que se describieron en aquel entonces se han acelerado. Nuevas tecnologías y aplicaciones han salido a la luz, un mayor consumo de tecnologías que se basan en Internet a nivel mundial, sobre todo en los países en desarrollo, ha brindado cada vez más oportunidades de desarrollo económico y social. Estos desarrollos han conllevado, o conllevarán, ventajas significativas para sociedades conectadas como la nuestra. Sin embargo, nuestra dependencia de las redes en el Reino Unido y en el extranjero ha aumentado, así como las oportunidades para quienes buscan poner en peligro nuestros sistemas y datos. De igual manera, el panorama geopolítico ha cambiado. La actividad cibernética malintencionada no conoce fronteras internacionales. Los actores estatales están experimentando con cibercapacidades ofensivas. Los ciberdelincuentes están haciendo más esfuerzos para ampliar sus modus operandi estratégicos para conseguir mayores pagos de ciudadanos, organizaciones e instituciones del Reino Unido. Los terroristas, y sus simpatizantes, están llevando a cabo ataques de bajo nivel y desean llevar a cabo acciones de mayor envergadura. Este capítulo muestra nuestra evaluación de la naturaleza de estas amenazas, nuestras vulnerabilidades y cómo seguirán evolucionando.

AMENAZAS

Ciberdelincuentes

3.2. Esta estrategia trata la ciberdelincuencia en el contexto de dos formas de actividades delictivas interrelacionadas:

- delitos que dependen del ámbito cibernético – delitos que sólo pueden ser cometidos a través de dispositivos de Tecnologías de la información y la comunicación (TIC), en los cuales los dispositivos son tanto herramientas para cometer el delito, como el blanco del delito (p. ej. desarrollar y propagar malware para beneficio económico, piratería informática para robar, dañar, distorsionar y destruir datos y/o redes o actividad); y
- delitos facilitados por el ámbito cibernético – delitos tradicionales cuya escala o alcance puede aumentar por medio del uso de computadoras, redes de computadores y otras formas de TIC (como el fraude y el robo de identidad cibernéticos).

3.3. La mayoría de los ciberdelitos más graves, sobre todo el fraude, el robo y la extorsión, cometidos contra el Reino Unido siguen siendo perpetrados, principalmente, por grupos criminales organizados (GCO) de habla rusa de Europa oriental, y muchos de los servicios de mercado delictivos están basados en estos países. Sin embargo, la amenaza también viene de otros países y regiones, y de dentro del mismo Reino Unido, con amenazas emergentes que causan cada vez más preocupación del sur de Asia y el África occidental.

3.4. Incluso cuando se identifica a las personas clave responsables de las ciberactividades delictivas más perjudiciales contra el Reino Unido, a menudo es difícil para las agencias de aplicación de la ley tanto en el Reino Unido como internacionales enjuiciar a estas personas cuando están ubicadas en jurisdicciones con acuerdos de extradición limitados o inexistentes.

3.5. Estos GCO son principalmente responsables del desarrollo y despliegue del malware cada vez más avanzado que infecta a las computadoras y redes de los ciudadanos del Reino Unido, a nuestra industria y nuestro gobierno. El impacto se dispersa en todo el Reino Unido, pero el efecto acumulado es significativo. Estos ataques se vuelven cada vez más agresivos y conflictivos, como lo ilustra el uso cada vez más del ransomware, y las amenazas de denegación de servicio distribuido (DDoS) por extorsión.

3.6. Si bien GCO representan una amenaza importante para nuestra prosperidad y seguridad colectiva, también es preocupante la amenaza continua de actos de ciberdelincuencia menos sofisticados pero muy difundidos contra personas o pequeñas organizaciones.

El fraude bancario por internet, que cubre pagos fraudulentos sacados de la cuenta bancaria de un cliente del canal de banca por internet, aumentó en un 64% llegando a los 133.5 millones de libras esterlinas en 2015. La cantidad de casos aumentó a un ritmo más bajo de 23%, lo que para Financial Fraud Action UK demuestra la tendencia creciente de los delincuentes que atacan negocios o clientes de altos ingresos.

Los estados y las amenazas patrocinadas por estados

3.7. A menudo vemos intentos por parte de los estados y grupos patrocinados por el estado de penetrar las redes del Reino Unido para tener una ventaja política, diplomática, comercial y estratégica, con un enfoque particular en el gobierno, la defensa, los sectores de finanzas, energía y telecomunicaciones.

3.8. La capacidad y el impacto de estos ciberprogramas estatales varían. Las naciones más avanzadas siguen mejorando sus capacidades rápidamente, integrando a sus herramientas los servicios de encriptación y anonimización para permanecer ocultos. Aunque tienen la capacidad técnica de llevar a cabo ataques sofisticados, a menudo pueden conseguir sus objetivos utilizando herramientas y métodos básicos contra blancos vulnerables ya que las defensas de sus víctimas son deficientes.

3.9. Sólo un puñado de estados tienen las capacidades técnicas de presentar una amenaza seria para la seguridad y prosperidad generales del Reino Unido. Sin embargo, muchos otros estados están desarrollando ciberprogramas sofisticados que pueden presentar una amenaza para los intereses del Reino Unido en un futuro cercano. Muchos estados que buscan desarrollar capacidades de ciberespionaje pueden comprar herramientas de explotación de las redes informáticas listas para utilizarse y reconvertirlas para llevar a cabo espionaje.

3.10. Más allá de la amenaza de espionaje, una pequeña cantidad de actores de amenazas extranjeras hostiles han desarrollado y desarrollan capacidades ciberofensivas, incluidas las destructivas. Estas capacidades amenazan la seguridad de la infraestructura crítica nacional del Reino Unido y los sistemas de control industrial. Algunos estados pueden utilizar estas capacidades, transgrediendo el derecho internacional convencidos de que lo pueden hacer con relativa impunidad, alentando a otros para que sigan el mismo camino. Si bien los ataques destructivos en el mundo son infrecuentes, son cada vez más comunes y tienen cada vez más impacto.

Terroristas

3.11. Los grupos terroristas siguen anhelando llevar a cabo ciberactividades perjudiciales contra el Reino Unido y sus intereses. Se considera que la capacidad técnica actual de los terroristas es baja. No obstante, el impacto de la actividad incluso de baja capacidad contra el Reino Unido hasta la fecha ha sido desmesuradamente elevado: la simple desfiguración y la actividad de doxing (cuando los detalles personales pirateados se filtran por Internet) permiten a los grupos terroristas y sus seguidores que atraigan la atención de los medios e intimiden a sus víctimas.

"Los terroristas que utilizan Internet para sus fines no son lo mismo que el ciberterrorismo. Sin embargo, al participar cada vez más en el ciberespacio, y dada la disponibilidad de la ciberdelincuencia como servicio, uno puede dar por sentado que estarían a la medida de lanzar ciberataques"
Panorama de amenazas de ENISA (Agencia Europea de Seguridad de las Redes y de la Información) de 2015

3.12. La evaluación actual es que los atentados físicos, y no cibernéticos, siguen siendo la prioridad de los grupos terroristas en un futuro inmediato. Conforme una generación cada vez más competente en informática se vuelva

extremista, potencialmente intercambiando pericias técnicas mejoradas, contemplamos un mayor volumen de actividad de desarticulación de baja sofisticación (desfiguración o DDoS) contra el Reino Unido. El potencial de que surja una serie de extremistas expertos solitarios también aumentará, así como el riesgo de que una organización terrorista busque reclutar a una persona establecida con información interna privilegiada. Es probable que los terroristas utilicen cualquier cibercapacidad para lograr el mayor efecto posible. Por tanto, incluso un incremento moderado en las capacidades terroristas puede constituir una amenaza importante para el Reino Unido y sus intereses.

Hacktivistas

3.13. Los grupos hacktivistas están descentralizados y orientados a temas específicos. Forman y seleccionan a sus blancos para responder a lo que perciben como agravios, dándole un aire de sentido justiciero a muchas de sus acciones. Aunque la mayoría de la ciberactividad de los hacktivistas es de naturaleza perturbadora (desfiguración de sitios web o DDoS), los hacktivistas más capaces han sido capaces de causar daños mayores y duraderos a sus víctimas.

PERSONAS CON INFORMACIÓN PRIVILEGIADA

Las amenazas internas siguen siendo un riesgo cibernético para las organizaciones del Reino Unido. El personal interno malintencionado, que consiste de empleados de confianza de una organización y tienen acceso a sistemas y datos críticos, presentan la mayor amenaza. Pueden causar daños financieros y de reputación a través del robo de información delicada y propiedad intelectual. También pueden representar una ciberamenaza destructiva si utilizan información, o acceso, privilegiados, para facilitar o lanzar un ataque para perturbar o deteriorar los servicios críticos en la red de sus organizaciones, o borrar datos de la red.

También son muy preocupantes esas personas con información privilegiada o empleados que causan ciberdaños accidentalmente al abrir un correo de phishing, conectar a una computadora un dispositivo USB infectado, o al hacer caso omiso a los procedimientos de seguridad y descargar contenido peligroso de Internet. A pesar de que no tienen intenciones de dañar deliberadamente a la organización, su acceso privilegiado a los sistemas y la información significa que sus acciones pueden causar tanto daño como una persona con información privilegiada malintencionado. Son personas que a menudo son víctimas de ingeniería social, inadvertidamente pueden brindar acceso a las redes de su organización o seguir instrucciones con buenas intenciones que beneficien al estafador.

El riesgo cibernético general para una organización que proviene de amenazas de una persona con información privilegiada no sólo tiene que ver con acceso no autorizado a sistemas de información y su contenido. Los controles de seguridad físicos que protegen a esos sistemas del acceso inapropiado, o el retiro de datos privilegiados o información exclusiva en distintos tipos de medios, son igual de importantes. De manera similar, una cultura de seguridad de personal robusta que siempre es consciente de la amenaza que presentan los empleados descontentos, el fraude en entre los trabajadores, el espionaje industrial y de otros tipos es un elemento importante para un enfoque de seguridad integral.

Los *script kiddies*

3.14. Los denominados script kiddies , en general se trata de individuos con menos capacidad que usan guiones o programas desarrollados por otros para llevar a cabo sus ciberataques - no se considera que presenten una amenaza considerable para la economía y la sociedad en general. Pero tienen acceso a guías, recursos y herramientas de piratería informática en Internet. Teniendo en cuenta las vulnerabilidades que se encuentran en los sistemas con acceso a Internet que utilizan muchas organizaciones, las acciones de los script kiddies pueden, en algunos casos, tener un impacto desproporcionadamente perjudicial en las organizaciones afectadas.

ESTUDIO DE CASO 1: EL COMPROMISO DE TALKTALK

El 21 de octubre de 2015, el proveedor de telecomunicaciones del Reino Unido TalkTalk informó de un ciberataque exitoso y una posible violación de los datos de los clientes. La investigación subsiguiente determinó que habían accedido a una base de datos que contenía detalles de clientes, a través de servidores de Internet públicos, con los expedientes de unos 157 000 clientes en peligro, incluidos nombres, direcciones e información de cuentas bancarias.

El mismo día, varios empleados de TalkTalk recibieron un correo electrónico que exigía el pago de un rescate en bitcoins. Los atacantes detallaron la estructura de la base de datos como prueba aparente de que habían accedido a la misma.

El informe de TalkTalk sobre esta violación ayudó a la policía, con el apoyo de especialistas de la National Crime Agency, a arrestar a los principales sospechosos, todos basados en el Reino Unido, en octubre y noviembre de 2015.

Este ataque demostró que, incluso las organizaciones grandes ciberinformadas, siguen teniendo vulnerabilidades. Explotarlas puede tener un efecto desproporcionado en cuanto a daños a la reputación e interrupciones operacionales, y este incidente generó una atención de los medios importante. El hecho que TalkTalk haya informado de esta violación rápidamente permitió que las autoridades de orden público respondieran de manera oportuna, y tanto el público como el gobierno mitigaran las pérdidas potenciales de datos delicados. Se estima que este incidente le costó a TalkTalk unos 60 millones de libras esterlinas y la pérdida de 95 000 clientes, así como una caída violento del precio de sus acciones.

ESTUDIO DE CASO 2: ATAQUE CONTRA EL SISTEMA SWIFT DE BANGLADESH BANK

La Sociedad mundial de telecomunicaciones financieras interbancarias (SWIFT) brinda una red que les permite a las instituciones financieras del mundo entero mandar y recibir información sobre transacciones financieras de manera segura. Dado que SWIFT envía órdenes de pago que tienen que ser liquidadas por cuentas corresponsales que las instituciones tienen entre sí, han existido preocupaciones sobre la posibilidad de que este procedimiento se vea afectado por ciberdelincuentes y otros actores malintencionados, que busquen inyectar órdenes de pago no legítimas en el sistema o, en el peor de los casos, busquen incapacitar o alterar la funcionalidad de la misma red SWIFT.

A principios de febrero de 2016, un atacante accedió al sistema de pagos SWIFT de Bangladesh Bank y autorizó al banco de la reserva federal de Nueva York para transferir dinero de una cuenta de Bangladesh Bank a varias cuentas en las Filipinas. El intento de fraude alcanzaba 951 millones de dólares estadounidenses. El sistema bancario frenó 30 transacciones de 850 millones de dólares. Sin embargo, fueron aceptadas cinco transacciones de 101 millones de dólares. Desde entonces se han recuperado 20 millones de dólares, localizados en Sri Lanka. Los 81 millones de dólares restantes, transferidos a las Filipinas, fueron lavados en casinos y algunos fondos fueron enviados sucesivamente a Hong Kong.

La investigación forense lanzada por Bangladesh Bank descubrió que se había instalado malware en los sistemas del banco y se había utilizado para recopilar inteligencia sobre los procedimientos utilizados por el banco para pagos internacionales y transferencias de fondos. BAE Systems llevó a cabo análisis ulteriores del malware vinculado con el ataque y descubrió una funcionalidad sofisticada para interactuar con el software de la Alianza de acceso SWIFT local de la infraestructura de Bangladesh Bank. BAE concluyó “que los delincuentes están llevando a cabo cada vez más ataques sofisticados contra organizaciones víctimas, sobre todo en el área de intrusiones en la red”.

ESTUDIO DE CASO 3: ATAQUES A LA RED DE SUMINISTRO ELÉCTRICO DE UCRANIA

Un ciberataque a las empresas de distribución de energía eléctrica de Ucrania occidental, Prykarpattya Oblenergo y Kyiv Oblenergo el 23 de diciembre de 2015 causó un apagón importante, con interrupciones en 50 subestaciones en las

redes de distribución. Según se informa en la región experimentaron un apagón de varias horas y muchos otros clientes y áreas sostuvieron perturbaciones menores en su suministro de electricidad, afectando a más de 220 000 consumidores.

El ataque se ha atribuido por unos al uso del malware BlackEnergy3, tras la identificación de muestras en la red. Al menos seis meses antes del ataque, los atacantes habían enviado correos phishing a las oficinas de las empresas de suministro eléctrica en Ucrania, que contenían documentos Microsoft Office maliciosos. Sin embargo, no es muy factible que el malware haya sido culpable de abrir los interruptores que resultaron en el apagón. Es probable que el malware les haya permitido a los atacantes reunir credenciales que les hayan permitido ganar un control directo remoto de algunos aspectos de la red, que subsecuentemente les permitirían causar el apagón.

El incidente de Ucrania es la primera instancia confirmada de un ciberataque a una red eléctrica. Casos como éste demuestran claramente la necesidad de buenas prácticas en ciberseguridad en toda nuestra infraestructura nacional crítica (CNI) para prevenir que incidentes similares ocurran en el Reino Unido.

VULNERABILIDADES

Una gama cada vez mayor de dispositivos

3.15. Cuando la última estrategia de ciberseguridad nacional se publicó en 2011, la mayoría de las personas concebían la ciberseguridad a través del prisma de la protección de sus dispositivos como computadoras pc o laptops. Desde entonces el Internet se ha integrado cada vez más a nuestra vida diaria en formas que ignoramos. El Internet de la cosas crea nuevas oportunidades de explotación y hace que aumente el impacto potencial de los ataques que tienen el potencial de causar daños físicos, lesiones a personas y, en el peor de los caos, la muerte.

3.16. La rápida implementación de conectividad en los procesos de control industrial en sistemas críticos, en una gran gama de sectores como el energético, el minero, el agrícola y el de la aviación, ha creado un Internet de las cosas industrial. Esto simultáneamente empezó a abrir las posibilidades de que dispositivos y procedimientos, que en el pasado nunca eran vulnerables a dichas interferencias, fueran atacados por los piratas informáticos y falsificados, con consecuencias potencialmente desastrosas.

3.17. Por lo tanto, ya no somos únicamente vulnerables a los ciberdaños causados por la falta de ciberseguridad en nuestros dispositivos, sino por amenazas a los sistemas interconectados que son fundamentales para nuestra sociedad, salud y bienestar.

Mala ciberhigiene y cumplimiento

3.18. La consciencia de las vulnerabilidades técnicas del software y las redes y la necesidad de ciberhigiene en el Reino Unido, ha sin lugar a duda aumentado en los últimos cinco años. En parte es una consecuencia de las iniciativas como los 10 pasos de ciberseguridad del gobierno (10 Steps to Cyber Security), pero también debido al incremento en el perfil público de los ciberincidentes que afectan a los gobiernos y las corporaciones. Los ciberataques no son necesariamente sofisticados o inevitables y a menudo son el resultado de vulnerabilidades explotadas que pueden rectificarse con facilidad y, a menudo, pueden ser prevenibles. En la mayoría de los casos, el factor decisivo en el éxito de un ciberataque sigue siendo una vulnerabilidad de la víctima, más que el ingenio del atacante. Las empresas y las organizaciones deciden dónde y cómo invertir en ciberseguridad basándose en una evaluación de costo-beneficios, pero en última instancia son responsables de la seguridad de sus datos y sistemas. Sólo al equilibrar los riesgos para sus sistemas críticos y sus datos delicados de los ciberataques, con suficiente inversión en las personas, tecnología y gobernanza, las empresas lograrán reducir su exposición a ciberdaños potenciales.

"No hay sistema de seguridad de información concebible que pueda parar a una persona entre cientos a la hora de abrir un correo phishing, y puede que con eso baste."
Ciaran Martin, Director General de Cyber Security, GCHQ – Junio de 2015

Formación y pericias insuficientes

3.19. Nos faltan las pericias y conocimientos para cumplir con nuestras necesidades de ciberseguridad tanto en el sector público como en el privado. En las empresas, muchos miembros del personal no están al tanto de la ciberseguridad y no entienden sus responsabilidades en ese sentido, en parte por la falta de capacitación formal. El público tampoco es suficientemente consciente del ámbito cibernético.

"Sólo una quinta parte de los empresarios han hecho que su personal participe en una formación de ciberseguridad el último año."
Cyber Security Breaches Survey 2016.

3.20. También tenemos que desarrollar las pericias y capacidades especializadas que nos permitirán seguirle el paso a la tecnología que evoluciona y gestionar los ciberriesgos relacionados. Esta brecha de pericias representa una vulnerabilidad nacional que debe resolverse.

El legado y los sistemas sin parches

3.21. Muchas organizaciones en el Reino Unido seguirán utilizando estos sistemas de legado vulnerables hasta su próxima actualización informática. A menudo el software de estos sistemas dependerá de versiones más antiguas, sin parches. Estas versiones más antiguas a menudo sufren de las vulnerabilidades que buscan los atacantes y tienen las herramientas para explotarlas. Un problema adicional es el uso, por parte de algunas organizaciones, de software sin apoyo, para los cuales no existen sistemas de reparación.

"Analizamos recientemente 115 000 dispositivos Cisco en Internet y en entornos de clientes como forma de atraer la atención a los riesgos de seguridad que presentan las infraestructuras que envejecen y la falta de atención a las vulnerabilidades de actualización…. Notamos que 106 000 de los 115 000 dispositivos presentaban vulnerabilidades conocidas en el software que utilizaban."
Informe anual de seguridad Cisco 2016

Disponibilidad en recursos de piratería informática

3.22. La disponibilidad inmediata de información de piratería y las herramientas de piratería de fácil utilización en Internet permiten que los que quieran desarrollar una capacidad de piratería lo hagan. La información que necesitan los piratas para poner en peligro a las víctimas de manera exitosa a menudo es accesible abiertamente y puede ser recolectada rápidamente. Todos, desde la sala de la casa hasta la sala de reuniones, necesitan ser conscientes de hasta qué punto están expuestos sus detalles personales y sistemas en Internet, y el grado hasta el cual esto puede hacer que serán vulnerables a ciberexplotación malintencionada.

"99.9% de las vulnerabilidades explotadas se vieron atacadas más de un año después de que se publicara la vulnerabilidad."
Informe Verizon de investigaciones de violaciones de datos de 2015

CONCLUSIONES

3.23. El Reino Unido ha perseguido políticas y ha establecido instituciones que mejoren nuestras defensas y mitiguen algunas de las amenazas a las que nos enfrentamos en el ciberespacio.

3.24. Sin embargo, todavía no nos hemos adelantado a la amenaza. Los tipos de ciberactores malintencionados a los que tenemos que enfrentarnos, y sus motivaciones, han perdurado en gran medida, incluso conforme el volumen de malware y la cantidad de dichos

actores maliciosos ha crecido rápidamente. La capacidad de nuestros adversarios más técnicamente competentes, concretamente un número selecto de estados y ciberdelincuentes de élite, ha crecido. Nuestro desafío colectivo es asegurarnos que nuestras defensas hayan evolucionado y sean suficientemente ágiles para responder a ellos, para reducir la capacidad de atacarnos de los actores malintencionados y responder a las causas raíz de las vulnerabilidades mencionadas anteriormente.

4. NUESTRA RESPUESTA NACIONAL

4.1. Para mitigar las amenazas múltiples a las que nos enfrentamos y proteger nuestros intereses en el ciberespacio, necesitamos un enfoque estratégico que sustente todas nuestras acciones colectivas e individuales en el ámbito digital en los próximos cinco años. Esta sección establece nuestra visión y enfoque estratégico.

NUESTRA VISIÓN

4.2. Nuestra visión para 2021 es que el Reino Unido esté a salvo de y sea resiliente ante las ciberamenazas, que sea próspero y confiado en el mundo digital.

4.3. Para cumplir con esta visión, trabajaremos para lograr los siguientes objetivos:

- DEFENDER Tenemos los medios para defender al Reino Unido de las ciberamenazas que no dejan de evolucionar, para responder efectivamente a los incidentes, y asegurarse que las redes, los datos y los sistemas del Reino Unido estén protegidos y sean resilientes. Los ciudadanos, las empresas y el sector público tienen conocimientos y capacidad de defenderse a sí mismos.
- DISUADIR El Reino Unido será el blanco difícil para todas formas de agresiones en el ciberespacio. Detectamos, entendemos, investigamos e interrumpimos las acciones hostiles emprendidas contra nosotros, persiguiendo y enjuiciando a los infractores. Contamos con los medios para emprender acciones ofensivas en el ciberespacio, si decidiéramos hacerlo.
- DESARROLLAR Tenemos una industria de ciberseguridad creciente, respaldada por investigación y desarrollos científicos líder en el mundo. Tenemos una lista autosostenible de talentos que brindan las pericias para cumplir con las necesidades nacionales en los sectores públicos y privados. Nuestro análisis y experiencia de vanguardia le permitirá al Reino Unido superar amenazas y desafíos futuros.

4.4. Al respaldar estos objetivos, emprenderemos ACCIÓN INTERNACIONAL para ejercer nuestra influencia al invertir en alianzas. Le daremos forma a las evoluciones globales del ciberespacio de tal manera que fomente nuestros intereses económicos y de seguridad más amplios.

PRINCIPIOS

4.5 Al trabajar hacia estos objetivos, el gobierno aplicará los siguientes principios:

- nuestras acciones y políticas serán impulsadas por la necesidad tanto de proteger a nuestra gente como de mejorar nuestra prosperidad;
- tomaremos los ciberataques contra el Reino Unido con la misma seriedad que tomamos ataques convencionales equivalentes y nos defenderemos conforme sea necesario;
- actuaremos de acuerdo con el derecho nacional e internacional y esperaremos que los demás hagan lo mismo;
- protegeremos y promoveremos nuestros valores centrales rigurosamente. Estos incluyen la democracia, el estado de derecho, la libertad, los gobiernos e instituciones abiertos y que rinden cuentas, los derechos humanos y la libertad de expresión;
- preservaremos y protegeremos la privacidad de los ciudadanos del Reino Unido;
- trabajaremos en alianza. Solo al trabajar con las administraciones a las que se han transferido competencias, todas las partes del sector público, las empresas, las instituciones, y los ciudadanos individuales, podremos proteger el ciberespacio del Reino Unido de forma exitosa;
- el gobierno cumplirá con sus responsabilidades y liderará en la respuesta nacional, pero las empresas, las organizaciones y los ciudadanos individuales tienen la responsabilidad de tomar pasos razonables para protegerse en línea y asegurar que sean resilientes y capaces de seguir funcionando si llegara a haber un incidente;
- la responsabilidad de la seguridad de las organizaciones en todo el sector público, incluida la ciberseguridad y la protección de los datos y servicios en línea, está en manos de

los ministros, secretarios permanentes y juntas de dirección respectivas;
• no aceptaremos que se presenten riesgos significativos para el público y el país en general como resultado de los fallos por parte de las empresas y organizaciones a la hora de tomar las medidas necesarias para gestionar la ciberamenazas;
• trabajaremos de cerca con aquellos países que comparten nuestros puntos de vista y con quienes tenemos solapamientos de seguridad, reconociendo que las ciberamenazas no conocen fronteras. También trabajaremos con toda una gama de socios internacionales para influir en la comunidad más extensa, reconociendo el valor de las coaliciones amplias; y
• para asegurar que las intervenciones del gobierno están teniendo un impacto substantivo en las ciberseguridad y ciberresiliencia nacionales, buscaremos definir, analizar y presentar información que mida la situación de nuestra ciberseguridad colectiva y nuestro éxito al conseguir nuestras metas estratégicas.

PAPELES Y RESPONSABILIDADES

4.6. Proteger el ciberespacio nacional requerirá un esfuerzo colectivo. Cada uno de nosotros tiene un papel importante que jugar.

Individuos

4.7. Como ciudadanos, empleados y consumidores, tomamos pasos prácticos para proteger los activos que valoramos en el mundo físico. En el mundo virtual, tenemos que hacer lo mismo. Esto significa cumplir con nuestra responsabilidad personal de tomar los pasos razonables para proteger no sólo nuestro hardware, nuestros teléfonos smart phones y otros dispositivos, sino también los datos, software y sistemas que nos brindan libertad, flexibilidad y conveniencia en nuestras vidas privadas y profesionales.

Empresas y organizaciones

4.8. Las empresas, las organizaciones del sector público y privado y otras instituciones tienen datos personales, brindan servicios y operan sistemas en el ámbito digital. La conectividad de esta información ha revolucionado sus operaciones. Pero esta transformación tecnológica viene acompañada de la responsabilidad de proteger los activos que tienen, mantener los servicios que brindan, e incorporar el nivel de seguridad apropiado en los productos que venden. El ciudadano y el consumidor, y la sociedad en general, esperan que las empresas y organizaciones tomen todos los pasos razonables para proteger la información personal, y construir resiliencia – la capacidad de soportar y recuperarse – en los sistemas y estructuras de los que dependen. Las empresas y organizaciones también deben entender que, si son víctimas de ciberataques, son responsables de las consecuencias.

Gobierno

4.9. La responsabilidad principal del gobierno es defender al país de ataques de otros estados, proteger a los ciudadanos y a la economía de daños, y establecer un marco nacional e internacional para proteger nuestros intereses, proteger los derechos fundamentales, y llevar a los delincuentes ante la justicia.

4.10. Como detentor de datos significativos y proveedor de servicios, el gobierno toma medidas estrictas para brindar garantías para sus activos de información. El gobierno también tiene una responsabilidad importante de asesorar e informar a los ciudadanos y organizaciones sobre qué necesitan hacer para protegerse en línea, y cuando sea necesario, de establecer los estándares con los que esperamos que cumplan las empresas y organizaciones clave.

4.11. A pesar de que los sectores clave de nuestra economía están en manos privadas, en última instancia el gobierno es responsable de asegurar su resiliencia nacional y, con sus socios en la administración, por el mantenimiento de servicios y funciones esenciales en todo el gobierno.

Impulsar el cambio: el papel del mercado

4.12. La Estrategia y el Programa de ciberseguridad nacional del 2011 buscaba conseguir resultados y aumentar la capacidad tanto del sector público como privado esperando que el mercado impulsara los comportamientos adecuados. Esperamos que las presiones comerciales y los incentivos instigados por el gobierno garanticen inversiones empresariales adecuadas en ciberseguridad, al estimular el flujo de inversión hacia nuestra industria, y para alentar una lista de pericias potenciales adecuadas en el sector.

4.13. Se ha logrado mucho. En la economía y la sociedad en general, ha aumentado la conciencia del riesgo y las acciones necesarias para mitigar los ciberriesgos en los últimos cinco años. Sin embargo, la combinación de las fuerzas del mercado y el aliento del gobierno no han bastado por sí mismos para garantizar los intereses a largo plazo en el ciberespacio a la velocidad necesaria. Demasiadas redes, incluso en los sectores críticos, siguen siendo inseguras. El mercado no valora, y por lo tanto no gestiona, correctamente el ciberriesgo. Demasiadas organizaciones siguen sufriendo violaciones incluso en el nivel más básico. Muy pocos inversionistas están dispuestos a arriesgarse a apoyar a los empresarios en el sector. Muy pocos graduados y otros con las habilidades correctas salen del sistema de educación y formación.

4.14. El mercado todavía tiene que jugar un papel a más largo plazo para lograr un mayor impacto del que podrá tener el gobierno. Sin embargo, la inmediatez de la amenaza a la que se enfrenta el Reino Unido y las vulnerabilidades cada vez mayores de nuestro entorno digitalizado piden que el gobierno lleve a cabo acciones más importantes a corto plazo.

Impulsando el cambio: un papel más amplio para el gobierno

4.15. El gobierno por lo tanto debe marcar el paso al cumplir con las necesidades de ciberseguridad nacional del país. Sólo el gobierno puede recurrir a la inteligencia y otros activos necesarios para defender al país de las amenazas más sofisticadas. Sólo el gobierno puede impulsar la cooperación en los sectores público y privado y asegurar que la información se comparta entre ambos. El gobierno tiene un papel de líder, en consulta con la industria, al definir en qué consiste una buena ciberseguridad y asegurando que se implemente.

4.16. El gobierno llevará a cabo mejoras significativas en nuestra ciberseguridad nacional en los próximos cinco años. Este programa ambicioso y transformativo se centrará en las cuatro áreas siguientes:

- Medios e incentivos. El gobierno invertirá para maximizar el potencial de un cibersector del Reino Unido realmente innovador. Lo haremos apoyando los start-ups e invirtiendo en innovación. También trataremos de identificar y estimular talentos de manera temprana en el sistema educativo y desarrollar rutas más claras en una profesión que necesita definirse mejor. El gobierno también aprovechará todos los impulsores disponibles, incluida la venidera Regulación general de protección de datos (GDPR *por sus siglas en inglés*), para impulsar los estándares de ciberseguridad en toda la economía, incluso, si es necesario, a través de normativas.
- Una inteligencia ampliada y la aplicación de la ley centrada en la amenaza. Las agencias de inteligencia, el ministerio de defensa, la policía y la National Crime Agency, en coordinación con las agencias socias internacionales, aumentarán sus esfuerzos para identificar, anticipar y trastornar las actividades cibernéticas hostiles de actores extranjeros, ciberdelincuentes y ciberterroristas. Esto mejorará su recopilación y explotación de inteligencia, con el objetivo de obtener inteligencia preventiva sobre las intenciones y capacidades de nuestros adversarios.
- Desarrollo y despliegue de tecnología en alianza con la industria, incluidas las medidas de Ciberdefensa activa, para fortalecer nuestra comprensión de la amenaza, fortalecer la seguridad de los sistemas y las redes del sector público y privado del Reino Unido ante esta amenaza, e interrumpir actividades malintencionadas.

• El Centro de ciberseguridad nacional (NCSC *por sus siglas en inglés*). El gobierno estableció una entidad de ciberseguridad única, central a nivel nacional. Esta entidad gestionará los ciberincidentes nacionales, brindando una voz y un centro de especializaciones sobre ciberseguridad fidedignos, y brindando un apoyo y recomendaciones a la medida a las dependencias, las administraciones descentralizadas, los reguladores y las empresas. El NCSC analizará, detectará y entenderá las ciberamenazas, y también brindará su pericia sobre ciberseguridad para apoyar los esfuerzos del gobierno para fomentar la innovación, apoyar una industria floreciente de ciberseguridad, y estimular el desarrollo de pericias de ciberseguridad. Una característica única en una entidad que da frente al público, su entidad matriz es GCHQ y por lo tanto puede aprovechar la pericia mundial de primera categoría y las capacidades delicadas de esa organización, mejorando el apoyo que podrá brindarle a la economía y la sociedad en general. Seguirá siendo la responsabilidad de los departamentos del gobierno asegurarse que implementen de manera eficaz los consejos de ciberseguridad.

"Dada la escala industrial de robo de la propiedad intelectual de nuestras empresas y universidades, así como las estafas de phishing y malware que llevan a un desperdicio de tiempo y dinero, el Centro de ciberseguridad nacional muestra que el Reino Unido está centrando sus esfuerzos en combatir las amenazas que existen en Internet." Robert Hannigan, Director de GCHQ, marzo de 2016

4.17. Lograr estos cambios en nuestra ciberseguridad y resiliencia requerirá recursos adicionales. En la Revisión de defensa y seguridad estratégica 2015, el gobierno reservó 1900 millones de libras esterlinas en un período de cinco años a la estrategia para cumplir estos compromisos y objetivos.

EL CENTRO DE CIBERSEGURIDAD NACIONAL

El Centro de ciberseguridad nacional (NCSC) fue inaugurado el 1 de octubre de 2016. El NCSC brinda una oportunidad única de construir una alianza de ciberseguridad eficaz entre el gobierno, la industria y el público para asegurarse de que el Reino Unido esté más a salvo en línea. Brindará una respuesta a ciberincidentes y será la voz de mayor autoridad en ciberseguridad. Por primera vez, los sectores clave serán capaces de hablar directamente con el personal del NCSC para recibir los mejores consejos y apoyo sobre cómo proteger a redes y sistemas de ciberamenazas.

El NCSC brinda:

• una fuente unificada de asesoramiento para apoyar la inteligencia del gobierno y su capacidad de información sobre las amenazas de ciberseguridad;
• una cara pública fuerte de las acciones del gobierno contra las ciberamenazas, trabajando de la mano con la industria, el mundo académico y los socios internacionales para proteger al Reino Unido contra ciberataques; y
• una organización de cara al público que pueda llegar al GCHQ para obtener la inteligencia necesariamente secreta y la pericia técnica de primera categoría mundial.

Habrá un enfoque gradual para construir las capacidades del NCSC en la vida de esta estrategia. Aúna las capacidades ya desarrolladas por CESG - el brazo de seguridad de la información del GCHQ - el Centro para la protección de la infraestructura nacional (CPNI *por sus siglas en inglés*), CERT-UK (el Equipo de respuesta en caso de emergencias informáticas) y el Centro para ciberevaluación (CCA *por sus siglas en inglés*), que nos permite construir sobre lo mejor que ya tenemos, simplificando a la vez en gran medida los acuerdos anteriores. Su enfoque inicial será:

• capacidades de gestión de incidentes de primera categoría para responder a y reducir los daños de ciberincidentes, desde aquellos que afectan a una organización hasta los ataques nacionales, a gran escala;
• brindar comunicaciones sobre cómo las organizaciones en el sector público y privado pueden lidiar con temas de ciberseguridad,

facilitando el intercambio de información sobre ciberamenazas; y
• seguir brindando asesoramiento sectorial experto al gobierno y sectores críticos como las telecomunicaciones, energía y finanzas, y brindando asesoramiento sobre ciberseguridad en todo el Reino Unido.

El NSCS ofrece medios eficaces para que el gobierno logre muchos elementos de esta estrategia. Reconocemos que, conforme crece el NCSC, su enfoque y capacidades tendrán que adaptarse a nuevos desafíos y lecciones aprendidas.

PLAN DE IMPLEMENTACIÓN

Nuestras metas de ciberseguridad para el país en los próximos cinco años son apropiadamente ambiciosas. Para lograrlas necesitaremos actuar de forma consecuente y determinada en todo el panorama digital. La actividad para lograr la visión del gobierno promoverá los tres primeros objetivos de la estrategia: DEFENDER nuestro ciberespacio, DISUADIR a nuestros adversarios y DESARROLLAR nuestras capacidades, todos respaldados por una ACCION INTERNACIONAL eficaz.

5. DEFENDER

5.0.1. Los elementos que tienen que ver con DEFENDER en esta estrategia buscan asegurarse que las redes, datos y sistemas del Reino Unido en las esferas pública y privada sean resilientes y estén protegidos de los ciberataques. Nunca será posible detener todos los ciberataques, así como no es posible detener todos los delitos. Sin embargo, junto con los ciudadanos, las instituciones educativas, el mundo académico, las empresas y otros gobiernos, el Reino Unido puede construir capas de defensa que reduzcan significativamente nuestra exposición a ciberincidentes, protejan nuestros activos más valiosos, y nos permitan a todos operar de manera exitosa y próspera en el ciberespacio. Actuar para promover la cooperación entre estados y las buenas prácticas de ciberseguridad también está en el interés de nuestra seguridad colectiva.

5.0.2. El gobierno implementará medidas para asegurar que los ciudadanos, empresas, organizaciones del sector público y privado e instituciones tengan acceso a la información adecuada para defenderse. El Centro de ciberseguridad nacional provee una fuente unificada de asesoramiento en el gobierno sobre la inteligencia de amenaza y la garantía de información, asegurándose que ofrece una orientación a la medida en ciberdefensa y respuesta rápida y eficaz a incidentes significativos en el ciberespacio. El gobierno trabajará con los socios del sector e internacionales para definir en qué consiste una buena ciberseguridad para los sectores público y privado, para nuestros sistemas y servicios más importantes, y para la economía en general. Incluiremos la seguridad por defecto en todos los sistemas del gobierno y sistemas críticos. Las agencias de orden público colaborarán de cerca con el sector y el Centro de ciberseguridad nacional para dar inteligencia dinámica sobre la amenaza criminal que le permita a la industria protegerse mejor, y promover asesoramiento y estándares de seguridad de protección.

5.1. CIBERDEFENSA ACTIVA

5.1.1. La Ciberdefensa activa (ACD *por sus siglas en inglés*) es un principio de implementación de medidas de seguridad para fortalecer una red o sistema y que sea más robusto contra los ataques. En un contexto comercial, la ciberdefensa activa suele referirse a la comprensión de las amenazas a sus redes por parte de analistas de ciberseguridad, y la formulación e implementación de medidas para combatir de manera proactiva, o defenderse contra, esas amenazas. En el contexto de esta estrategia, el gobierno ha elegido aplicar el mismo principio a mayor escala: el gobierno utilizará sus competencias, capacidad e influencia únicas para lograr este cambio radical en la ciberseguridad nacional para responder a las ciberamenazas. La "red" que estamos tratando de defender ocupa todo el ciberespacio del Reino Unido. Las actividades propuestas representan un plan de acción defensivo, aprovechando la pericia del NCSC como Autoridad técnica nacional para responder a las ciberamenazas al Reino Unido a nivel macro.

Objectivos

5.1.2. Al emprender el ACD, el gobierno busca:

- hacer que el Reino Unido sea un objetivo mucho más difícil de alcanzar para los actores patrocinados por estados y los ciberdelincuentes, al aumentar la resiliencia de las redes del Reino Unido;
- derrocar la gran mayoría de actividad de malware de alto volumen/baja sofisticación en las redes del Reino Unido al bloquear las comunicaciones malware entre los piratas informáticos y sus víctimas;
- evolucionar y aumentar el alcance y la escala de las capacidades del gobierno para trastornar las amenazas graves patrocinadas por estados y de ciberdelincuentes;
- proteger nuestro tráfico de Internet y de telecomunicaciones para que no sea secuestrado por actores malintencionados;
- fortalecer ante las ciberamenazas la infraestructura crítica del Reino Unido y los servicios que dan frente al ciudadano; y
- trastornar el modelo de actividad de los atacantes de todo tipo, para desmotivarlos y

reducir el daño que sus ataques pueden causar.

Enfoque

5.1.3. Para conseguir estos objetivos, el gobierno:

- trabajará con la industria, sobre todo con los Proveedores de servicios de comunicaciones (CSPs *por sus siglas en inglés*), para hacer que sea significativamente más difícil atacar los servicios y usuarios de Internet del Reino Unido, y reducir en gran medida la posibilidad de ataques que tengan un impacto prolongado en el Reino Unido. Esto incluirá la lucha contra el phishing, el bloqueo de dominios y direcciones de IP maliciosos, y otros pasos a seguir para trastornar los ataques de malware. También incluirá medidas para proteger la infraestructura de telecomunicaciones y de enrutamiento de Internet del Reino Unido;
- aumentar la escala y el desarrollo de las capacidades del GCHQ, del Ministerio de defensa y del NCA para perturbar las ciberamenazas más significativas para el Reino Unido, incluidas las campañas de ciberdelincuentes sofisticados y actores extranjeros hostiles; y
- proteger mejor los sistemas y redes gubernamentales, ayudar a la industria a que fomente más seguridad en las cadena de suministro CNI, que haga que los ecosistemas de software en el Reino Unido sean más seguros, y brinde protecciones automatizadas en los servicios online gubernamentales para los ciudadanos.

5.1.4. Cuando sea posible, estas iniciativas tienen que cumplirse con o a través de alianzas con la industria. Para muchas, la industria diseñará y estará al frente de la implementación, con la contribución crucial del gobierno como apoyo especializado, asesoramiento y liderazgo intelectual.

5.1.5. El gobierno también se comprometerá con acciones específicas para implementar estas medidas, que incluirán:

- trabajar con CSPs para bloquear los ataques de malware. Lo haremos al limitar el acceso a dominios o sitios web específicos que se conocen como fuentes de malware. A esto se le conoce como bloqueo/filtrado del DNS (Domain Name System);
- prevenir la actividad de phishing que depende del spoofing de dominios (redireccionamiento, cuando parece que el correo electrónico viene de un remitente específico, como un banco o un departamento gubernamental, pero en realidad es fraudulento) al desplegar sistemas de verificación de correos electrónicos en las redes gubernamentales como norma y alentar a la industria a que haga lo mismo;
- promover las mejores prácticas de seguridad a través de organizaciones de gobernanza de Internet de múltiples coparticipes como la Corporación de Internet para asignar nombres y números (ICANN *por sus siglas en inglés*), el Grupo de trabajo de ingeniería de Internet (IETF *por sus siglas en inglés*) y el Registro de Internet regional europeo (RIPE *por sus siglas en inglés*) y la participación con partes implicadas del Foro de gobierno de Internet de la ONU (FGI);
- trabajar con los canales de orden público para proteger a los ciudadanos del Reino Unido y que no sean víctimas de ciberataques desde infraestructuras no protegidas en el extranjero;
- trabajar hacia la implementación de controles para proteger el enrutamiento del tráfico de Internet por departamentos del gobierno para garantizar que no pueda ser desviado de forma ilegítima por actores malintencionados; e
- invertir en programas del ministerio de defensa, el NCA y el GCHQ que mejoren las capacidades de estas organizaciones para responder a, e interrumpir las ciberactividades graves patrocinadas por estados y criminales que quieran afectar las redes del Reino Unido.

Desarrollaremos estas intervenciones técnicas conforme evolucionen las amenazas para asegurar que los ciudadanos y las empresas del Reino Unido estén protegidos por defecto de la mayoría de los ciberataques comerciales a gran escala.

Midiendo el éxito

5.1.6. El gobierno medirá su éxito al establecer un ACD eficaz mediante la evaluación de los avances para conseguir los resultados siguientes:

- Que sea más difícil hacer "phishing" contra el Reino Unido, porque tenemos defensas a gran escala contra el uso de dominios maliciosos/malintencionados, protección anti phishing más activa a escala y es mucho más difícil utilizar otras formas de comunicación, como el "vishing" o el spoofing de los mensajes de texto, para llevar a cabo ataques de ingeniería social;
- una proporción mucho mayor de las comunicaciones de malware y los artefactos técnicos asociados con los ciberataques y la explotación han sido bloqueados;
- el tráfico de Internet y de telecomunicaciones del Reino Unido es mucho menos vulnerables a la desviación por parte de actores maliciosos/malintencionados;
- las capacidades del GCHQ, de las fuerzas armadas y del NCA para responder a amenazas graves patrocinadas por los estados o criminales han aumentado significativamente.

5.2. CONSTRUYENDO UN INTERNET MÁS SEGURO

5.2.1. La tecnología cambiante nos brinda la oportunidad de reducir significativamente la capacidad de nuestros adversarios de llevar a cabo ciberdelincuencia en el Reino Unido al asegurar que los productos y servicios online futuros que se utilicen sea "seguros por defecto". Esto quiere decir que nos aseguremos que los controles de seguridad integrados en el software y el hardware que utilicemos se activen como configuración predeterminada del fabricante para garantizar que el usuario experimente una seguridad máxima, a menos que activamente elija apagarla. El desafío es efectuar un cambio transformador de tal modo que apoye al usuario final y brinde un producto o servicio que sea viable comercialmente, pero seguro. Todo esto dentro del contexto de mantener la naturaleza libre y abierta del Internet.

"Las cosas conectadas por Internet se multiplican rápidamente. Vimos muchas pruebas de concepto y ataques en el mundo real en 2015, identificando vulnerabilidades graves en los coches, dispositivos médicos y muchos otros. Los fabricantes tienen que darle prioridad a la seguridad para reducir el riesgo de consecuencias personales, económicas o sociales graves." Informe Symantec de amenazas a la seguridad del Internet de 2016

5.2.2. El gobierno está bien posicionado para tomar papel de líder en la exploración de aquellas nuevas tecnologías que protejan mejor nuestros sistemas, ayuden a la industria a construir una mayor seguridad en la cadena de suministro, protejan el ecosistema de software y brinden protecciones automatizadas a los ciudadanos que acceden a los servicios gubernamentales en línea. El gobierno tiene que poner a prueba e implementar nuevas tecnologías que den una protección automatizada para los productos y servicios del gobierno en línea. Cuando sea posible tecnologías similares deberían brindarse al sector privado y al ciudadano.

Objetivo

5.2.3. La mayoría de los productos y servicios online que se empiezan a utilizar se vuelve "seguros por defecto" para el 2021. Los consumidores estarán empoderados para elegir productos y servicios con seguridad integrada como configuración predeterminada. Las personas pueden apagar esta configuración si lo desean pero los consumidores que quieran participar en el ciberespacio de la manera más segura tendrán una protección automática.

Nuestro enfoque

5.2.4. Emprenderemos las acciones siguientes:

- el gobierno liderará por el ejemplo al ofrecer servicios seguros en Internet que no dependen de que el Internet sea seguro por sí mismo;
- el gobierno explorará opciones de colaboración con la industria para desarrollar formas de vanguardia de que el hardware y el software sean más "seguros por defecto"; y
- adoptaremos nuevas tecnologías complejas de ciberseguridad en el gobierno, alentando a las administraciones a quienes se han transferido competencias a que hagan lo mismo, para reducir lo que se percibe como

riesgo de adopción. Esto dará prueba de concepto y demostrará los beneficios de seguridad de los nuevos enfoques y tecnologías. También posicionará la seguridad en el corazón del desarrollo de nuevos productos, eliminará las oportunidades de explotación por delincuentes y por lo mismo protegerá al usuario final.

5.2.5. Para lograrlo:

- Seguiremos alentando a los proveedores de hardware y software a que vendan productos con las configuraciones de seguridad activadas por defecto, que hagan que el usuario las tenga que desactivar para estar en situación de inseguridad. Algunos proveedores ya lo están haciendo, pero otros todavía no están tomando estos pasos necesarios;
- seguiremos desarrollando un servicio de reputación de Protocolo de Internet (IP) para proteger los servicios digitales del gobierno (lo que permitiría a los servicios en línea que consigan información sobre una dirección de IP conectándose a ellos, ayudando al servicio a tomar decisiones de gestión de riesgo en tiempo real más informadas);
- buscaremos instalar productos en las redes del gobierno que den garantías de que el software funciona de forma correcta, y no sufre interferencias malintencionadas;
- veremos cómo ampliar a otros servicios digitales, más allá del dominio GOV.UK, medidas que notifiquen al usuario si el buscador que utiliza es obsoleto; y
- Invertiremos en tecnologías como Trusted Platform Modules (TPM) y estándares emergentes de la industria como Fast Identity Online (FIDO), que no dependen de contraseñas par autenticación del usuario, pero utilizan la máquina y otros dispositivos que tiene el usuario para hacer la autenticación. El gobierno pondrá a prueba estos mecanismos de autenticación innovadores para demostrar lo que pueden ofrecer, tanto en términos de seguridad como experiencia general del usuario.

5.2.6. El gobierno también explorará cómo alentar al mercado por medio de clasificaciones de seguridad de nuevos productos, para que los consumidores cuenten con información clara sobre qué productos y servicios ofrecen la mayor seguridad. El gobierno también explorará cómo vincular estas clasificaciones a organismos reguladores nuevos y existentes y cómo advertir a los consumidores cuando estén por llevar a cabo una acción en línea que ponga en peligro su seguridad.

Midiendo el éxito

5.2.7. El gobierno medirá su éxito para construir un Internet seguro al evaluar los avances para cumplir los resultados siguientes:

- la mayoría de los productos y servicios básicos disponibles en el Reino Unido en 2021 se aseguran que el Reino Unido sea más seguro con sus configuraciones de seguridad preestablecidas por defecto o con la seguridad integrada en su diseño; y
- el público del Reino Unido confía en todos los servicios gubernamentales que se brindan a nivel nacional, local y de las administraciones descentralizadas, ya que se han implementado de la manera más segura posible, y los niveles de fraude están dentro de los parámetros de riesgo aceptables.

5.3. PROTEGIENDO AL GOBIERNO

5.3.1. El gobierno del Reino Unido, las administraciones descentralizadas y el sector público en general poseen grandes cantidades de información delicada. Brindan al público servicios esenciales y operan redes que son críticas para la seguridad nacional y la resiliencia. Los sistemas del gobierno respaldan el funcionamiento de nuestra sociedad. La modernización de los servicios del sector público seguirá siendo la piedra angular de la Estrategia digital del Reino Unido – la ambición digital del gobierno es que el Reino Unido sea la nación digital líder en el mundo.

Para conservar la confianza de los ciudadanos en los servicios y sistemas online del sector público, los datos que posee el gobierno deben protegerse y todas las ramas del gobierno deben implementar los niveles adecuados de ciberseguridad para enfrentar los intentos continuos por parte de actores hostiles que

buscan acceder a las redes y datos del gobierno y del sector público.

Objetivos

5.3.2. Queremos lograr los resultados siguientes:

- los ciudadanos usan confiados los servicios online del gobierno: confían que su información delicada está a salvo y, a su vez, entienden su responsabilidad de ingresar su información delicada en línea de forma segura;
- el gobierno establecerá y respetará los estándares más adecuados de ciberseguridad, para asegurarse que las dependencias del gobierno entienden y cumplen su obligaciones de proteger sus redes, datos y servicios; y
- se protegen los activos críticos del gobierno, incluidos aquellos de más alta clasificación, de ciberataques.

Nuestro enfoque

5.3.3. El gobierno del Reino Unido seguirá pasando más de sus servicios a Internet para que el Reino Unido pueda realmente convertirse en "digital por defecto". El Servicio digital del gobierno (GDS *por sus siglas en inglés*), y el Servicio comercial de la Corona (CCS *por sus siglas en inglés*) y el NCSC se asegurarán que los nuevos servicios digitales que construya o compre el gobierno también sean "seguros por defecto".

5.3.4. Las redes del gobierno son sumamente complejas y en muchos casos siguen incorporando sistemas de legado, así como también algunos software disponibles en el comercio a los que ya no dan apoyo el proveedor. Nos aseguraremos que no haya riesgos sin gestionar en estos sistemas de legado y software sin respaldo.

5.3.5. Mejoraremos la resiliencia del gobierno y del sector público en general ante los ciberataques. Esto significa que nos aseguraremos de que sea correcto y esté actualizado el conocimiento de todos los sistemas, datos, y los que pueden acceder a ellos. La probabilidad y el impacto de un ciberincidente se serán minimizados por la implementación de la mejor práctica tal y como la establece el NCSC.

El gobierno también se asegurará de ser capaz de responder con eficacia a los ciberincidentes a través de programas de simulacros de incidentes y pruebas regulares de las redes del gobierno. Invitaremos a las administraciones descentralizadas y las autoridades locales a que participen en estos simulacros, conforme sea apropiado. A través de un análisis automático robusto lograremos saber mejor cuál es el estatus de seguridad online del gobierno.

5.3.6. La ciberseguridad no sólo tiene que ver con la tecnología. Casi todos los ciberataques exitosos tienen un factor humano que contribuye. Por lo tanto seguiremos invirtiendo en nuestra gente, para asegurar que todos los que trabajan en el gobierno tienen una comprensión cabal del riesgo cibernético.
Desarrollaremos pericia cibernética específica en áreas que están en mayor peligro y garantizaremos que contamos con los procesos adecuados instalados para gestionar con eficacia estos riesgos.

5.3.7. El NCSC desarrollará una orientación de ciberseguridad líder en el mundo que le siga el paso a la amenaza y los desarrollos de nuevas tecnologías. Tomaremos los pasos necesarios para asegurarnos de que las organizaciones gubernamentales cuentan con acceso fácil a información sobre la amenaza para que comprendan sus propios ciberriesgos y adopten medidas apropiadas.

5.3.8. Seguiremos mejorando las redes de clasificación más altas para proteger las comunicaciones más delicadas del gobierno.

5.3.9. Los sistemas de salud y atención presentan desafíos únicos en el contexto de la ciberseguridad. El sector emplea a aproximadamente 1 millón 600 mil personas en más de 40 000 entidades, con recursos y capacidades de protección de la información que difieren entre ellas. El Guardián nacional de datos para la salud y los cuidados (National Data Guardian for Health and Care) ha establecido nuevos estándares de seguridad de datos para los sistemas de salud y atención social en Inglaterra, junto con un modelo de

consentimiento/exclusión optativa para los pacientes. El gobierno trabajará con las organizaciones de salud y atención social para implementar estos estándares.

"Gran Bretaña es líder mundial en ciberseguridad, pero con las amenazas crecientes, este nuevo Centro de operaciones de ciberseguridad (Cyber Security Operations Centre) garantizará que nuestras fuerzas armadas sigan funcionando de manera segura. Nuestro presupuesto cada vez mayor en defensa significa que podemos estar al frente de nuestros adversarios en el ciberespacio mientras que a la vez invertimos en capacidades convencionales"

Honorable Michael Fallon MP,
Secretario de defensa, abril de 2016

5.3.10. La ciberseguridad es vital para nuestra defensa. Nuestras fuerzas armadas dependen de sistemas de información y comunicaciones, tanto en el Reino Unido como en sus operaciones en todo el mundo. La infraestructura y el personal del ministerio de defensa (MdD) son objetivos prominentes. Los sistemas de defensa con regularidad se ven atacados por criminales, servicios de inteligencia extranjeros y otros actores malintencionados que buscan explotar al personal, trastornar los negocios y operaciones, y corromper o robar información. Mejoraremos nuestras funciones de sensibilización, detección y reacción ante las ciberamenazas, a través del desarrollo de un Centro de operaciones de ciberseguridad (CSOC *por sus siglas en inglés*) que utilice capacidades de ciberdefensa de vanguardia para proteger el ciberespacio del MdD y lidiar con las amenazas. El CSOC trabajará de cerca con el NCSC para enfrentar los desafíos de ciberseguridad del MdD y contribuir a la ciberseguridad nacional más amplia.

Midiendo el éxito

5.3.11. El gobierno medirá su éxito para proteger las redes, sistemas y datos del gobierno al evaluar los avances comparados con los siguientes resultados:

- el gobierno tiene una comprensión profunda del nivel de riesgo de ciberseguridad en todo el gobierno y el sector público en general;
- los departamentos gubernamentales individuales y otras entidades se protegen a sí mismos en proporción a su nivel de riesgo y en relación a estándares mínimos gubernamentales acordados previamente;
- los departamentos del gobierno y el sector público en general son resilientes y pueden responder con eficacia a los ciberincidentes, manteniendo sus funciones y recuperándose con rapidez;
- las nuevas tecnologías y servicios digitales utilizados por el gobierno serán ciberseguros por defecto;
- somos conscientes de, y mitigamos activamente, todos las vulnerabilidades conocidas a las que se enfrentan los sistemas y servicios del gobierno en Internet; y
- todos los proveedores del gobierno cumplen con los estándares de ciberseguridad apropiados.

5.4. PROTEGIENDO NUESTRA INFRAESTRUCTURA CRÍTICA NACIONAL Y OTROS SECTORES PRIORITARIOS

Contexto

5.4.1 La ciberseguridad de algunas organizaciones del Reino Unido es de particular importancia ya que si se emprende contra ellas un ciberataque exitoso esto tendría un impacto muy grave para la seguridad nacional del país.

Este impacto podría influir en la vida de los ciudadanos del Reino Unido, la estabilidad y la fuerza de la economía del Reino Unido, y el lugar que ocupa y la reputación que tiene el Reino Unido en el mundo. Este grupo de empresas y organizaciones premium dentro del sector público y privado incluye la infraestructura nacional crítica (CNI *por sus siglas en inglés*), que brinda servicios esenciales a la nación. Garantizar que la CNI esté a salvo y sea resiliente ante los ciberataques será una prioridad para este gobierno. Este grupo premium también incluye a empresas y organizaciones, más allá de la CNI, que requieren de un mayor nivel de apoyo. Incluyen:

- las joyas de la corona económica – las empresas más exitosas del Reino Unido y

también las que tienen en sus manos nuestra fortaleza económica futura en el valor de sus investigaciones y propiedad intelectual;
• los detentores de datos – no sólo las organizaciones que tienen una gran cantidad de datos personales, sino también las que tienen datos sobre ciudadanos vulnerables aquí y en el extranjero, como organizaciones de beneficencia;
• los blancos de riesgo elevado – como las organizaciones de medios, donde un ataque podría dañar la reputación del Reino Unido, perjudicar la confianza pública en el gobierno, o poner en peligro la libertad de expresión;
• los referentes de nuestra economía digital – los proveedores de servicios digitales que permiten el comercio digital y nuestra economía digital, y que dependen de la confianza que tenga el consumidor en sus servicios; y
• aquellas organizaciones que, a través de las fuerzas de mercado y su autoridad, pueden ejercer una influencia en la economía en general para mejorar la ciberseguridad, como las aseguradoras, los inversionistas, los reguladores y los asesores profesionales.

5.4.2. Necesita hacerse más para proteger estas partes vitales de nuestra economía y apoyar a las organizaciones que influyen mucho en otros. Nuestra CNI, tanto en el sector público como privado, sigue siendo un blanco para atacantes. En todos estos y muchos otros sectores prioritarios no se entiende plenamente en qué consiste y cómo se gestiona el ciberriesgo, incluso cuando la amenaza sigue diversificándose y aumentando.

Objetivo

5.4.3. El gobierno del Reino Unido, trabajando con los gobiernos de Escocia, Gales e Irlanda del Norte y otras autoridades responsables donde sea apropiado, se asegurará de que las organizaciones y empresas más importantes del Reino Unido, incluida la CNI, sean lo suficientemente seguras y resilientes ante los ciberataques.
Ni el gobierno ni otras entidades públicas asumirán la responsabilidad de gestionar este riesgo por el sector privado, que cuenta con juntas, dueños y operadores que se encarguen de hacerlo. Pero el gobierno brindará apoyo y garantías proporcionales tanto a la amenaza para estas empresas y organizaciones, como a las consecuencias de que las ataquen.

"La ciberseguridad es clave para descubrir innovaciones y ampliaciones, y al adoptar un enfoque de ciberseguridad a la medida de las organizaciones, que se centre en el riesgo, las organizaciones pueden volver a enfocarse en oportunidades y exploraciones. Fomentar confianza en una empresa que opera exitosamente en el Internet de las cosas (IoT) y que apoya y protege plenamente a las personas y sus dispositivos móviles personales (desde un simple teléfono hasta un dispositivo de salud, desde aparatos Smart hasta coches Smart), es un diferenciador competitivo clave y tiene que ser una prioridad."

Encuesta global de seguridad de la información de EY de 2015

Nuestro enfoque

5.4.4. Las organizaciones y las juntas de administración de las empresas son responsables de garantizar que sus redes sean seguras. Tienen que identificar los sistemas críticos y evaluar su vulnerabilidad frente a un panorama tecnológico y una amenaza que no dejan de evolucionar. Deben invertir en tecnología y en su personal para reducir las vulnerabilidades en los sistemas actuales y futuros, y en su cadena de suministro, para mantener un nivel de ciberseguridad proporcional al riesgo. También tienen que poner a prueba las capacidades establecidas para responder en caso de que haya un ataque.
Para la CNI, tienen que hacerlo con las entidades gubernamentales y los reguladores para que puedan confiar en que el ciberriesgo se está gestionando adecuadamente y, en caso de que no sea así, intervenir en el interés de la seguridad nacional.

5.4.5. Por lo tanto, el gobierno tendrá que entender el nivel de ciberseguridad en nuestra CNI y contar con medidas establecidas que permitan intervenir cuando sea necesario para impulsar las mejoras en el interés nacional.

5.4.6. El gobierno va a:

- compartir información sobre amenazas con la industria que sólo puede obtener el gobierno para que sepan contra qué tienen que protegerse;
- producir recomendaciones y orientaciones sobre cómo gestionar los ciberriesgos y, trabajando en colaboración con el sector y el mundo académico, definir en qué consiste una buena ciberseguridad;
- estimular la introducción de seguridad de alta gama que se necesita para proteger a las CNI, como las instalaciones de formación, los laboratorios de pruebas, los estándares de seguridad y los servicios de consultoría; y
- llevar a cabo ejercicios con las empresas de CNI para asistirles en la gestión de los riesgos y vulnerabilidades cibernéticos.

5.4.7. El NCSC brindará estos servicios a las empresas y organizaciones más importantes del Reino Unido, incluida la CNI. Lo hará en alianza con los departamentos y reguladores, quienes garantizarán que el ciberriesgo se está gestionando en sus sectores hasta el nivel que lo exige el interés nacional.

5.4.8. El gobierno también se asegurará que esté establecido el marco regulatorio adecuado para la ciberseguridad, que:

- garantice que la industria emprenda acciones para protegerse de la amenaza;
- es enfocado en resultados y suficientemente flexible para que no acabe por detrás de la amenaza, o sea un cumplimiento superficial en vez de una gestión de riesgo profunda;
- es suficientemente ágil para fomentar el crecimiento e innovación, en lugar de liderarlo;
- está armonizado con los marcos en otras jurisdicciones para que las empresas del Reino Unido no sufran de un enfoque fragmentado y aparatoso; y
- cumple, cuando está combinado con el apoyo eficaz del gobierno, una ventaja competitiva para el Reino Unido.

5.4.9. Muchos de los sectores de nuestra industria ya están regulados por la ciberseguridad. No obstante, tenemos que asegurar que se tomen los pasos adecuados en toda la economía, incluida la CNI, para gestionar los ciberriesgos.

Midiendo el éxito

5.4.10. El gobierno medirá su éxito para proteger nuestra CNI y otros sectores prioritarios al evaluar el progreso ante los resultados siguientes:

- entendemos el nivel de ciberseguridad en toda la CNI, y contamos con medidas establecidas para intervenir, cuando sea necesario, para impulsar mejoras en el interés nacional; y
- nuestras empresas y organizaciones más importantes entienden el nivel de amenaza e implementan las prácticas de ciberseguridad proporcionadas.

5.5. CAMBIANDO LOS COMPORTAMIENTOS PÚBLICOS Y EMPRESARIALES

5.5.1 Una economía digital exitosa del Reino Unido depende de la confianza de las empresas y el público en los servicios online. El gobierno del Reino Unido ha trabajado con la industria y otras partes del sector público para aumentar la concientización y el entendimiento de la amenaza. El gobierno también ha brindado al público y a las empresas acceso a algunas de las herramientas que necesitan para protegerse. Aunque hay muchas organizaciones que hacen un trabajo excelente - en algunos casos siendo líderes mundiales – para protegerse, y brindar servicios a otros en línea, la mayoría de las empresas y los individuos siguen sin gestionar adecuadamente el ciberriesgo.

“El año pasado, el costo promedio de las violaciones a las grandes empresas que las sufrieron era de 36 500 libras esterlinas. Para las pequeñas empresas el costo promedio de las violaciones era de 3100 libras esterlinas. Un 65% de las grandes organizaciones explicaron que habían sufrido un violación de seguridad de la información durante el año pasado, y un 25% de ellas experimentaron una violación por lo menos

una vez al mes. Casi siete de cada diez ataques tenían que ver con virus, spyware o malware que podrían haberse evitado utilizando el programa de puntos esenciales cibernéticos del gobierno (Cyber Essentials Scheme)."
2016 Encuesta de visión de la cibersalud del gobierno y de violaciones de ciberseguridad

Objetivo

5.5.2. Nuestro objetivo es asegurar que los individuos y las organizaciones, independientemente del tamaño o sector, emprenden los pasos apropiados para protegerse a sí mismos, y a sus clientes, de los daños causados por los ciberataques.

Nuestro enfoque

5.5.3. El gobierno brindará asesoramiento que necesita la economía para protegerse. Mejoraremos la forma en que se presenta esta recomendación para maximizar su efecto. Para el público, el gobierno aprovechará las "voces de confianza" para incrementar el alcance, credibilidad y relevancia de nuestros mensajes. Brindaremos asesoramiento que sea fácil de llevar a los hechos y relevante para los individuos, en el punto en el que acceden a los servicios y se exponen al riesgo. Participarán las administraciones de Escocia, Gales e Irlanda del Norte y otras autoridades conforme sea apropiado.

5.5.4. Para las empresas, trabajaremos a través de organizaciones como las aseguradoras, reguladores e inversionistas que pueden influir en las empresas para asegurarse que se gestionen los ciberriesgos. Al hacerlo, haremos hincapié en los beneficios claros para las empresas y el precio de los ciberriesgos para los que influencian los mercados. Buscaremos entender mejor cómo muchas organizaciones siguen fracasando a la hora de protegerse adecuadamente y después trabajaremos en alianza con organizaciones como las entidades que establecen estándares profesionales, para ir más allá de la concientización para persuadir a las empresas de que actúen. También nos aseguraremos de que contamos con el marco regulatorio adecuado establecido para gestionar los ciberriesgos a los que el mercado no logra responder. Como parte de esto, buscaremos usar levas, como el GDPR, que hagan subir los estándares de ciberseguridad y protejan a los ciudadanos.

5.5.5. Los individuos y las organizaciones del Reino Unido necesitan tener acceso a la información, la educación y las herramientas que necesiten para protegerse. Para asegurarnos de que cumplimos con este cambio radical en el comportamiento público, mantendremos una serie de mensajes coherentes y consecuentes sobre orientación de ciberseguridad tanto del gobierno como de nuestros socios. El NSCS brindará asesoría técnica para respaldar esta orientación. Reflejará las prioridades y prácticas de las empresas y las públicas, y será clara, de fácil acceso y coherente, siguiéndole siempre el paso a la amenaza. El orden público trabajará de cerca con la industria y el NCSC para compartir inteligencia sobre las últimas amenazas criminales, para apoyar a la industria para que se defienda contra estas amenazas, y para mitigar el impacto de los ataques en las víctimas del Reino Unido.

Midiendo el éxito

5.5.6. El gobierno medirá su éxito al proteger nuestra CNI y otros sectores prioritarios, evaluando los avances ante los siguientes resultados:

- el nivel de ciberseguridad de la economía del Reino Unido es tan alto como, o más alto que, lo de economías avanzadas comparables;
- la cantidad, la gravedad y el impacto de ciberataques exitosos contra negocios en el Reino Unido se ha reducido, porque los estándares de ciberhigiene han mejorado; y
- hay una cultura de ciberseguridad mejorada en todo el Reino Unido porque las organizaciones y el público entienden mejor sus niveles de riesgo cibernético y entienden qué pasos de ciberhigiene tienen que emprender para gestionar estos riesgos.

CONSCIENTIZACIÓN CIBERNÉTICA

La campaña Cyber Aware, antes conocida como Cyber Streetwise, otorga al público las recomendaciones que necesita para protegerse de los ciberdelincuentes. Los mensajes dirigidos

que se dan a través de los medios sociales y la publicidad y en colaboración con empresas promueven:

- la utilización de tres palabras aleatorias para crear una contraseña fuerte; y
- siempre descargar las últimas actualizaciones del software.

Los expertos están de acuerdo en que adoptar estos comportamientos le brindará a las pequeñas empresas y las personas protección contra la ciberdelincuencia. Cyber Aware recibe el apoyo ahora mismo de 128 socios multisectoriales, incluida la policía y las empresas minoristas, de ocio, viajes y sectores de servicios profesionales. En 2015/16 se estima que 10 millones de adultos y 1 millón de pequeñas empresas declararon que era más factible que mantuvieran o adoptaran comportamientos de seguridad cibernética claves como resultado de la campaña Cyber Aware.

Para saber más visite cyberaware.gov.uk

LOS ELEMENTOS FUNDAMENTALES CIBERNÉTICOS

El programa de elementos fundamentales cibernéticos (Cyber Essentials Scheme) fue desarrollado para mostrar a las organizaciones cómo protegerse de “amenazas comerciales” de bajo nivel. Contiene una lista de cinco controles técnicos (control de acceso; los firewalls divisorios y los portales de Internet; la protección de malware; la gestión de parches y la configuración segura) que tendrían que tener en marcha las organizaciones. La gran mayoría de los ciberataques utilizan métodos relativamente sencillos para explotar las vulnerabilidades básicas en el software y los sistemas informáticos. Hay herramientas y técnicas disponibles abiertamente en Internet que les permiten a actores con pocas pericias que exploten estas vulnerabilidades. La implementación adecuada del esquema Cyber Essentials protegerá contra la gran mayoría de las amenazas comunes en Internet.

5.6. GESTIONAR LOS INCIDENTES Y ENTENDER LA AMENAZA

5.6.1. Es probable que aumente la cantidad y la gravedad de ciberincidentes que afectan a organizaciones en los sectores públicos y privados. Por lo tanto tendremos que definir cómo, tanto el sector privado como el público, participan con el gobierno durante un ciberincidente. Daremos por sentado que el nivel de apoyo del gobierno del Reino Unido a cada sector, teniendo en cuenta su cibermadurez, quede claramente definido y entendido. La recolección y diseminación de la información sobre la amenaza por parte del gobierno tiene que llevarse a cabo de tal modo y a una velocidad adecuada para todo tipo de organizaciones. El sector privado, el gobierno y el público pueden acceder en la actualidad a fuentes múltiples de información, orientación y asistencia sobre ciberseguridad.
Esto tiene que simplificarse.

5.6.2. Tenemos que lograr que lo que el gobierno brinde, tanto en respuesta a incidentes, y como disposición de orientación, no exista de manera aislada, sino en alianza con el sector privado. Nuestros procesos de gestión de incidentes deberían reflejar un enfoque integral a los incidentes, conforme el cual aprendamos de nuestros socios y compartamos técnicas de mitigación. También seguiremos utilizando nuestra relación con otros Equipos de respuesta ante emergencias informáticas (CERTs *por sus siglas en inglés*) y nuestros aliados como parte íntegra de nuestra función de gestión de incidentes.

5.6.3. La gestión de incidentes actual sigue estando hasta cierto punto fragmentada a través de varios departamentos gubernamentales y esta estrategia creará un enfoque unificado. El NCSC brindará una función de respuesta a incidentes encabezada por el gobierno que sea eficaz y racionalizada.
En caso de un ciberincidente grave, nos aseguraremos de que las fuerzas armadas sean capaces de prestar asistencia, ya sea por medios convencionales respondiendo al impacto físico de un incidente, o por medio de apoyo especializado brindado por ciberpersonal activo o de reserva. Así como brindaremos todo el apoyo que nuestros recursos permitan, el gobierno seguirá

haciendo hincapié en la importancia de que la industria, la sociedad y el público actúen para proteger su ciberseguridad básica.

Objetivos

5.6.4. Nuestros objetivos son los siguientes:

- el gobierno seguirá brindando un enfoque único, unido en la gestión de incidentes, basado en una mejor comprensión y concienciación de la amenaza y las acciones que se están emprendiendo contra nosotros. El NCSC será el capacitador, así como lo será la alianza con el sector privado, el orden público y otros departamentos, autoridades y agencias del gobierno.
- el NCSC define procedimientos claros para informar de incidentes, a la medida de los perfiles de la víctima; y
- prevendremos los incidentes cibernéticos más comunes, y contaremos con estructuras establecidas eficaces para compartir información que ayuden a la planificación "pre incidente".

Nuestro enfoque

5.6.5. Es la responsabilidad de la dirección de la organización y de la empresa, tanto en el sector público como privado, asegurarse de que las redes sean seguras y poner en marcha planes de respuesta a incidentes. En caso de un incidente de gran envergadura, el proceso de gestión de incidentes del gobierno reflejará los tres elementos distintivos de un ciberincidente: las causas precursoras, el incidente en sí y la respuesta posterior al incidente.

5.6.6. Para brindar una gestión del incidente que sea eficaz tanto para el gobierno como para el sector privado, trabajaremos de cerca para revisar y definir el alcance de la respuesta del gobierno para garantizar que refuerza la cooperación. Construiremos nuestro plan nacional de cibersimulacros, utilizando nuestra mejor comprensión y concientización de la amenaza, para mejorar nuestra oferta de apoyo a los socios del sector público y privado.

5.6.7. Crearemos una entidad gubernamental fiable y creíble que dé asesoramiento, asistencia y garantías en caso de incidentes. Esto aumentará la concientización en ciberseguridad en toda la comunidad digital del Reino Unido y nos permitirá identificar tendencias, tomar medidas proactivas y, en última instancia, prevenir incidentes.

5.6.8. Conforme avanzamos hacia un intercambio de información automatizado (a saber, sistemas de ciberseguridad que se alertan automáticamente unos a otros ante incidentes y ataques), brindaremos un servicio más eficaz. Esto permitirá que las organizaciones actúen rápidamente ante información sobre amenazas relevante.

Midiendo el éxito

5.6.9. El gobierno medirá su éxito en la gestión de incidentes al evaluar sus avances comparados con los resultados siguientes:

- se denuncia ante las autoridades una proporción más alta de incidentes, lo que lleva a entender mejor el tamaño y la escala de la amenaza;
- los ciberincidentes se gestionan de manera más eficaz, eficiente y completa, como resultado de la creación del NCSC como mecanismo centralizado de informes de incidentes y respuesta; y
- abordaremos la causa raíz de los ataques a nivel nacional, reduciendo la incidencia de explotaciones repetidas entre víctimas y sectores múltiples.

6. DISUADIR

6.0.1. La Estrategia de seguridad nacional indica que la defensa y la protección empiezan con la disuasión. Esto es cierto en el ciberespacio como en cualquier otro ámbito. Para cumplir nuestra visión de una nación que es segura y resiliente ante las ciberamenazas, y que es próspera y actúa con seguridad en el mundo digital, tenemos que disuadir e impedir a aquellos que nos lastimarían o dañarían nuestros intereses. Para lograr esto todos necesitamos seguir elevando los niveles de ciberseguridad para que atacarnos en el ciberespacio, ya sea para robarnos o dañarnos, no sea ni barato ni fácil. Nuestros adversarios deben saber que no pueden actuar con impunidad: que podemos identificarlos y lo haremos, y que podemos actuar contra ellos, utilizando la respuesta más apropiada de entre las herramientas que tenemos a nuestra disposición. Seguiremos construyendo alianzas globales y promoviendo la aplicación del derecho internacional en el ciberespacio. También trastornaremos más activamente la actividad de todos aquellos que nos amenazan en el ciberespacio y la infraestructura de la que dependen. Cumplir esta ambición requiere capacidades soberanas de primera clase mundial.

6.1. EL PAPEL CIBERNÉTICO EN LA DISUASIÓN

6.1.1. El ciberespacio es únicamente un ámbito en el que debemos defender nuestros intereses y nuestra soberanía. De la misma manera en que nuestras acciones en el ámbito físico son relevantes para nuestra seguridad y disuasión en la esfera cibernética, nuestras acciones y postura en el ciberespacio deben contribuir a nuestra seguridad nacional más amplia.

6.1.2. Los principios de disuasión son tan aplicables en el ciberespacio como lo son en el ámbito físico. El Reino Unido deja claro que el espectro completo de nuestras capacidades se utilizará para disuadir a los adversarios y denegarles las oportunidades de atacarnos. Sin embargo, reconocemos que la ciberseguridad y la resiliencia son en sí medios de disuasión de ataques que dependen de la explotación de vulnerabilidades.

6.1.3. Seguiremos un enfoque integral nacional de ciberseguridad y disuasión que haga que el Reino Unido sea un blanco más difícil, reduciendo los beneficios y elevando los costos para un adversario – ya sea político, diplomático, económico o estratégico. Tenemos que asegurarnos de que los adversarios potenciales entiendan la capacidad y la intención de responder para influir en la toma de decisiones. Tenemos que tener las herramientas y capacidades necesarias: para denegarles a nuestros adversarios las oportunidades fáciles de poner en peligro nuestras redes y sistemas; para entender su intención y capacidades; para derrocar las amenazas a escala del malware comercial; y para responder y proteger a la nación en el ciberespacio.

6.2. REDUCIENDO LA CIBERDELINCUENCIA

6.2.1. Necesitamos elevar el costo, elevar el riesgo, y reducir las recompensas de las actividades cibercriminales. A la vez que fortalecemos al Reino Unido contra los ciberataques y reducimos las vulnerabilidades, tenemos que centrarnos sin descanso en perseguir a los delincuentes que siguen atacando al Reino Unido.

6.2.2. Las agencias de orden público centrarán sus esfuerzos en enjuiciar a los criminales que mantienen sus ataques contra los ciudadanos y empresas del Reino Unido. Seguiremos trabajando con los socios nacionales e internacionales que hacen frente a los criminales donde sea que se encuentren, y buscan desmantelar su infraestructura y redes de facilitación. Las agencias de orden público también seguirán ayudando a concientizar y elevar los estándares de ciberseguridad, en colaboración con el NSCS.

6.2.3. Esta estrategia complementa la Estrategia de crimen grave y organizado de 2013 (Serious and Organised Crime Strategy), que establece la respuesta estratégica a la ciberdelincuencia del

gobierno del Reino Unido, junto con otros tipos de crimen grave y organizado. La Unidad de ciberdelincuencia (NCCU *por sus siglas en inglés*), que se enmarca dentro de la Agencia nacional contra la delincuencia (NCA *por sus siglas en inglés*), fue establecida para liderar y coordinar la respuesta nacional a la ciberdelincuencia. Action Fraud brinda un centro de informes nacionales para fraude y ciberdelitos. Una red de unidades contra la ciberdelincuencia dentro de las Unidades de crimen organizado regionales (ROCUs *por sus siglas en inglés*) ofrecen acceso a capacidades de ciberespecialistas a nivel regional, apoyando al NCCU y las fuerzas locales.

Objetivo

6.2.4. Reduciremos el impacto de la ciberdelincuencia en el Reino Unido y sus intereses al disuadir a los ciberdelincuentes de que ataquen al Reino Unido y perseguiremos sin descanso a aquellos que insistan en atacarnos.

Nuestro enfoque

6.2.5. Para reducir el impacto de la ciberdelincuencia, vamos a:

- realzar las capacidades de orden público del Reino Unido y las pericias a nivel nacional, regional y local para identificar, perseguir, enjuiciar y disuadir a los cibercriminales dentro del Reino Unido y en el extranjero;
- entender mejor cómo funciona el modelo de negocios de la ciberdelincuencia, para que sepamos hacia dónde dirigir nuestras intervenciones para que tengan el efecto más desestabilizador en las actividades delictivas. Utilizaremos este conocimiento para:
    - hacer que el Reino Unido se convierta en un entorno de alto costo y alto riesgo donde operar al atacar el nexo de criminalidad del Reino Unido, y al trabajar con la industria para reducir la capacidad de los criminales de explotar la infraestructura del Reino Unido; y
    - combatir a la ciberdelincuencia de forma ascendente, añadiendo fricción al modelo de negocios criminal al desmantelar su infraestructura y redes financieras, y cuando sea posible, al llevar a los infractores ante la justicia.
- construir alianzas internacionales para poner fin a la impunidad percibida de los cibercriminales que actúan en contra del Reino Unido, administrando la justicia para criminales de jurisdicciones extranjeras;
- disuadir a los individuos para que no se vean atraídos por, o se involucren en, ciberdelincuencia al construir nuestras propias medidas de intervenciones tempranas;
- mejorar las colaboraciones con la industria para brindarles inteligencia proactiva sobre la amenaza, y brindarnos la inteligencia ascendente que poseen, para poder asistir con nuestros esfuerzos de interrupción ascendente;
- desarrollar una nueva capacidad de informes 24/7 y clasificación en Action Fraud, vinculada con el NCSC, la unidad del ciberdelincuencia del NCA y la comunidad de orden público más amplia, para mejorar el apoyo a las víctimas de ciberdelincuencia, para brindar una respuesta más rápida a los delitos denunciados y mejorar el asesoramiento de seguridad protectiva. Un nuevo sistema de denuncias se establecerá para compartir información en tiempo real de orden público en la ciberdelincuencia y las ciberamenazas;
- trabajar con el NSCS y el sector privado para reducir las vulnerabilidades en la infraestructura del Reino Unido que puedan explotarse a escala por ciberdelincuentes; y
- trabajar con el sector financiero para hacer que el entorno del Reino Unido sea más hostil para aquellos que buscan ganar dinero de credenciales robadas, incluido mediante la perturbación de las redes.

Midiendo el éxito

6.2.6. El gobierno medirá su éxito en la reducción de la ciberdelincuencia mediante la evaluación de los avances comparados con los resultados siguientes:

- tenemos un efecto de perturbación más amplio en los ciberdelincuentes que atacan al Reino Unido, con una mayor cantidad de arrestos y condenas, y una mayor cantidad de redes criminales desmanteladas como resultado de las intervenciones de aplicación de la ley;

• existen capacidades de orden público mejoradas, incluida una mayor capacidad y pericia de especialistas dedicados y agentes convencionales y una mayor capacidad de aplicación de la ley entre nuestros socios en el extranjero;
• ha mejorado la eficacia y la escala aumentada de medidas de intervención temprana disuade y rehabilita a los perpetradores; y
• existen menos ciberdelitos de bajo nivel dado que es más difícil acceder a los servicios de los ciberdelincuentes y son menos eficaces.

QUÉ HACER SI ES VÍCTIMA DE UN CIBERDELITO

Si es miembro del público y cree que está siendo víctima de un ciberdelito, o fraude cibernético, tiene que contactar a Action Fraud.

Puede denunciar el incidente utilizando la herramienta de denuncias de delitos de Action Fraud en cualquier momento del día o de la noche, o llamando al 0300 123 2040. Para mayores informes vaya a http://www.actionfraud.police.uk/

La City of London Police está a cargo de Action Fraud.

6.3. COMBATIR A ACTORES EXTRANJEROS HOSTILES

6.3.1. Tenemos que aunar toda la gama de capacidades gubernamentales para contrarrestar la amenaza que presentan los actores extranjeros hostiles que cada vez amenazan más nuestra seguridad política, económica y militar. Trabajar con los socios internacionales será clave en nuestro éxito, y se hará mayor hincapié en su participación y en trabajar con ellos para combatir la amenaza. Gran parte de esta acción no se llevará a cabo en el dominio público. Nuestra inversión en capacidades soberanas y alianzas con la industria y el sector privado seguirán respaldando nuestra capacidad de detectar, observar e identificar esta actividad que evoluciona constantemente contra nosotros.

Objetivo

6.3.2. Tendremos estrategias, políticas y prioridades establecidas para cada adversario, para asegurar que se tome un enfoque proactivo, bien calibrado y eficaz para contrarrestar la amenaza y hacer que disminuyan la cantidad y la gravedad de los ciberincidentes en el futuro.

Nuestro enfoque

6.3.3. Para reducir las ciberamenazas de actores extranjeros hostiles, vamos a:
• reforzar la aplicación del derecho internacional en el ciberespacio además de promover el acuerdo voluntario de normas no vinculantes de comportamiento estatal responsable y el desarrollo e implementación de medidas de fomento de confianza;
• trabajar con socios internacionales, sobre todo a través de defensa colectiva, seguridad de cooperación, y una mayor disuasión según lo permite nuestra pertenencia a la OTAN.
• identificar tanto los aspectos únicos como genéricos de la ciberactividad de nuestros adversarios;
• generar y explorar todas las opciones disponibles para disuadir y enfrentarse a esta amenaza, aprovechando toda la gama de capacidades del gobierno. Tendremos en cuenta plenamente otros factores relacionados, incluidas estrategias específicas por país, prioridades cibernéticas internacionales, y objetivos de ciberdelincuencia y prosperidad;
• utilizar las redes existentes y las relaciones con nuestros socios clave internacionales para compartir información sobre amenazas actuales y nacientes, añadiendo valor a las ideas y conocimientos existentes; y
• atribuir identidades cibernéticas específicas públicamente cuando juzguemos que está en el interés nacional hacerlo.

Midiendo el éxito

6.3.4. El gobierno medirá su éxito para contrarrestar las acciones de los actores extranjeros hostiles evaluando sus avances comparados con los resultados siguientes:
• las redes fortalecidas que hemos establecido para compartir información con nuestros socios internacionales, y los acuerdos multilaterales más amplios para apoyar un

comportamiento legal y responsable por parte de los estados, contribuyen sustancialmente a nuestra capacidad de entender y responder a la amenaza, resultando en una mejor defensa del Reino Unido; y

• nuestras medidas de defensa y disuasión, junto con nuestras estrategias específicas por país, están haciendo que el Reino Unido sea un objetivo más difícil para que los actores extranjeros hostiles actúen en su contra.

6.4. PREVENIR EL TERRORISMO

6.4.1. La capacidad técnica de los terroristas sigue siendo limitada pero siguen aspirando a llevar a cabo operaciones dañinas de redes informáticas contra el Reino Unido, con la publicidad e interrupciones como objetivo principal de su ciberactividad. El gobierno identificará y detendrá a los terroristas utilizando y pretendiendo utilizar la cibernética para este propósito. Al hacerlo, minimizará su impacto y prevendrá un fortalecimiento de la cibercapacidad terrorista que amenazaría aún más a las redes y la seguridad nacional del Reino Unido.

Objetivo

6.4.2. Mitigar la amenaza del uso de la cibernética por terroristas, a través de la identificación e interrupciones a los actores ciberterroristas que ahora misma, cuentan, o aspiran a construir, capacidades que podrían amenazar la seguridad nacional del Reino Unido.

Nuestro enfoque

6.4.3. Para asegurar que la amenaza que presentan los ciberterroristas siga siendo baja, vamos a:

• detectar las amenazas ciberterroristas, identificar a los actores que buscan llevar a cabo operaciones perjudiciales de redes contra el Reino Unido y nuestros aliados;

• investigar e interrumpir a estos actores ciberterroristas para prevenir que utilicen capacidades cibernéticas contra el Reino Unido y sus aliados; y

• trabajar de cerca con los socios internacionales para permitirnos afrontar mejor la amenaza del ciberterrorismo.

Midiendo el éxito

6.4.4. El gobierno medirá su éxito para prevenir el terrorismo al evaluar los avances comparados con los siguientes resultados:

• una comprensión completa del riesgo que presentan los ciberterroristas, a través de la identificación e investigación de amenazas ciberterroristas para el Reino Unido; y

•un monitoreo cercano, y una interrupción de las cibercapacidades terroristas a la primera oportunidad, con el objetivo de prevenir un incremento de dichas capacidades a largo plazo.

6.5. MEJORA DE LAS CAPACIDADES SOBERANAS – CIBEROFENSIVAS

6.5.1. Las capacidades ciberofensivas implican intrusiones deliberadas en los sistemas o redes de los oponentes, con la intención de causar daños, interrupciones/trastornos o destrucción. Las ciberofensivas forman parte del espectro completo de capacidades que desarrollamos para disuadir a los adversarios y denegarles las oportunidades de atacarnos, tanto en el ciberespacio como en el ámbito físico. A través del Programa de ciberofensiva nacional (NOCP *por sus siglas en inglés*), hemos dedicado capacidades a actuar en el ciberespacio y vamos a comprometer recursos para desarrollar y mejorar esta capacidad.

Objetivo

6.5.2. Nos aseguraremos de que tenemos a nuestra disposición capacidades ciberofensivas apropiadas que pueden desplegarse en el momento y el lugar que decidamos, tanto para propósitos de disuasión como de operación, de acuerdo con el derecho nacional e internacional.

Nuestro enfoque

6.5.3. Para lograrlo, vamos a:

• invertir en nuestro NOCP, la alianza entre el Ministerio de defensa y GCHQ que capta las habilidades y talentos de ambas organizaciones para brindar las herramientas, técnicas y pericia del oficio requeridas;

• desarrollar nuestra capacidad de utilizar las herramientas ciberofensivas; y

• desarrollar las habilidades de nuestras fuerzas armadas para que desplieguen sus capacidades ciberofensivas como parte integrada de sus operaciones, mejorando así el impacto general que pueden lograr mediante su acción militar.

Midiendo el éxito

6.5.4. El gobierno medirá nuestro éxito para establecer capacidades ciberofensivas al evaluar los avances comparados con los resultados siguientes:

• el Reino Unido es líder mundial en las capacidades ciberofensivas; y
• el Reino Unido ha establecido una cartera de habilidades y conocimientos para desarrollar y desplegar nuestras capacidades ciberofensivas soberanas.

6.6. MEJORAR LAS CAPACIDADES SOBERANAS – CRIPTOGRAFÍA

6.6.1. Las capacidades criptográficas son fundamentales para proteger nuestra información más delicada y elegir cómo desplegar las capacidades de nuestras fuerzas armadas y seguridad nacional. Para mantener esta capacidad, necesitaremos que las habilidades y las tecnologías del sector privado estén garantizadas por GCHQ. Es muy probable que este trabajo tenga que hacerse en el Reino Unido, por ciudadanos británicos con la habilitación de seguridad necesaria, trabajando para empresas que están dispuestas a ser completamente abiertas con GCHQ debatiendo en detalle el diseño e implementación. El MdD y GCHQ están trabajando para establecer una comprensión cabal de las implicaciones de costos a largo plazo para el mantenimiento de dichas capacidades criptográficas soberanas, basado en las condiciones de mercado reinantes y en cooperación con aquellas empresas que ahora son capaces de brindar dichas soluciones.

Objetivo

6.6.2. Confiamos que el Reino Unido siempre tendrá control político de las capacidades criptográficas vitales para nuestra seguridad nacional y, por lo tanto, los medios para proteger los secretos del Reino Unido.

Nuestro enfoque

6.6.3. Seleccionaremos los medios que nos permitan compartir información de forma eficaz con nuestros aliados, y asegurar que la información y los sistemas de información disponibles sean fiables, cuando y donde se requieran. Trabajando de cerca con otros departamentos y agencias gubernamentales, GCHQ y el MdD definirán juntos los requisitos soberanos, y cuál es la mejor manera de cumplir con estos requisitos cuando tengan que ser nacionales los proveedores. Esto se llevará a cabo a través de un marco conjunto para determinar los requisitos para una ventaja operativa y libertad de acción.

Midiendo el éxito

6.6.4. El gobierno medirá su éxito para mantener las capacidades criptográficas al evaluar los avances comparados con los resultados siguientes:

• nuestras capacidades criptográficas soberanas son eficaces para mantener nuestra información secreta y delicada a salvo de divulgaciones no autorizadas.

ENCRIPTACIÓN

La encriptación es un proceso de codificación de datos o información para prevenir un acceso no autorizado a los mismos.

El gobierno está a favor de la encriptación. Es el fundamento de una economía fuerte, basada en Internet: mantiene a salvo los datos personales y la propiedad intelectual de las personas, y garantiza un comercio en línea seguro.

Sin embargo, conforme sigue evolucionando la tecnología, tenemos que asegurarnos que no hay “espacios seguros” garantizados para que los terroristas y criminales operen más allá del alcance de la ley.

El gobierno quiere trabajar con la industria conforme se desarrolla la tecnología para asegurarse que, con un marco legal robusto y una vigilancia clara, la policía y las agencias de inteligencia pueden acceder al contenido de las

comunicaciones de terroristas y criminales. La legislación existente permite que las comunicaciones de los criminales y los terroristas sean interceptadas cuando hay una orden judicial. Las empresas tienen la obligación de responder a dicha orden, brindando las comunicaciones solicitadas a las autoridades relevantes. Cuando reciben esta orden se les pide a las empresas que retiren la encriptación que han aplicado las mismas empresas, u otros en su nombre, para que éste sea material en formato legible. La ley estipula que las empresas tienen que tomar los pasos necesarios para responder a la orden, y cualquier evaluación prudencial incluirá una evaluación de los pasos que tienen que tomar la empresa para quitar la encriptación.

7. DESARROLLAR

7.0.1. La parte de DESARROLLAR de la estrategia establece cómo conseguiremos y fortaleceremos las herramientas y capacidades que necesita el Reino Unido para protegerse de una ciberamenaza.

7.0.2. El Reino Unido necesita profesionales de ciberseguridad más talentosos y cualificados. El gobierno actuará ahora para estrechar la brecha creciente entre demanda y oferta en los puestos de ciberseguridad claves, e inyectará nueva vitalidad en esta área de educación y formación. Se trata de un objetivo transformador, a largo plazo, y esta estrategia impulsará este importante trabajo, que necesariamente continuará más allá del 2021. Una plantilla con habilidades es el sustento de un ecosistema comercial de ciberseguridad líder en el mundo. Este ecosistema asegurará que los start-ups cibernéticos prosperen y reciban la inversión y apoyo que necesitan. Esta innovación y vigor sólo puede brindarlos el sector privado, pero el gobierno actuará para apoyar su desarrollo, y promover activamente el sector de ciberseguridad más amplio en el mercado mundial. Se necesita un sector de investigación científica dinámico y floreciente para apoyar tanto el desarrollo de personas muy cualificadas, como para garantizar que nuevas ideas se conviertan en productos de vanguardia.

7.1. FORTALECIENDO NUESTRA PERICIAS DE CIBERSEGURIDAD

7.1.1. El Reino Unido necesita resolver los problemas sistémicos que están al centro de la escasez de ciberpericias: la falta de jóvenes que entran a la profesión; la escasez actual de especialistas en ciberseguridad; la falta de exposición a conceptos de ciberseguridad y seguridad de la información en los cursos de informática; una falta de profesores cualificados adecuadamente; y la ausencia de una carrera establecida y rutas de formación en la profesión.

7.1.2. Esto necesita una intervención rápida del gobierno para dar respuesta a la escasez actual y desarrollar una estrategia coherente a largo plazo que pueda construir a partir de estas intervenciones para cerrar la brecha de capacidades. Sin embargo, tiene que reconocerse que para tener un impacto profundo, este esfuerzo tiene que ser colaborativo, con los insumos de toda una gama de participantes y personas influyentes en Escocia, Gales e Irlanda del Norte, el sector público, los que brindan servicios educativos, las entidades académicas y la industria.

Objetivo

7.1.3. La ambición del gobierno es asegurar que existe el mejor suministro sostenible posible de los mejores cibertalentos nacionales, financiando a la vez intervenciones específicas a corto plazo para ayudar a colmar las brechas de capacidades que se conocen. También definiremos y desarrollaremos pericias de ciberseguridad que se necesitan entre la población y las plantillas de trabajo para que operen de manera segura y a salvo online.

7.1.4. Esto requiere acciones en los próximos veinte años, no sólo en los próximos cinco. Definiremos series de acciones a largo plazo, coordinadas, que el gobierno, la industria, los proveedores de educación y el mundo académico necesitan para un suministro sostenible de profesionales de ciberseguridad competentes, que realmente cumplan con los estándares y la certificación para hacer su trabajo de con confianza y seguridad.

7.1.5. Cerraremos la brecha de pericias en defensa. Atraeremos a ciberespecialistas al gobierno, que no sólo reciban la formación eficaz pero también estén listos a proteger nuestra seguridad nacional. Esto incluye una comprensión del impacto que tiene el ciberespacio en las operaciones militares.

Nuestro enfoque

7.1.6. Desarrollaremos e implementaremos una estrategia de pericias autónomas que siga construyendo sobre el trabajo ya existente para integrar la ciberseguridad en el sistema educativo.

Esto seguirá mejorando la situación de la enseñanza e las ciencias de la computación en general e incorporará la ciberseguridad en el programa. Todos los que estudien ciencia de la computación, tecnología o pericias digitales aprenderán los fundamentos de la ciberseguridad y serán capaces de llevar todas esas habilidades al lugar de trabajo. Como parte de este esfuerzo, responderemos al desequilibrio de género en las profesiones que se centran en el ámbito cibernético, y llegaremos a personas de ámbitos más diversos, para asegurarnos de atraer a la mayor cantidad de talentos disponibles. Trabajaremos muy de cerca con Escocia, Gales e Irlanda del Norte para alentar un enfoque coherente en todo el Reino Unido.

7.1.7. Estableceremos con mayor claridad los roles respectivos del gobierno y la industria, incluido cómo evolucionarán con el paso del tiempo. El gobierno del Reino Unido y las administraciones de Escocia, Gales e Irlanda del Norte tienen un papel clave a jugar en la creación del entorno propicio para que se desarrollen las pericias de ciberseguridad y para que se actualice el sistema educativo para reflejar las necesidades cambiantes de la industria y el gobierno. Pero los que dan empleo también tienen una responsabilidad importante de articular claramente sus necesidades, así como formar y capacitar a los empleados y los jóvenes que llegan a la profesión. La industria tiene que jugar un papel importante en construir una carrera y rutas de formación diversas y atractivas en alianza con las instituciones académicas, los cuerpos profesionales y las asociaciones comerciales.

7.1.8. En reconocimiento al desafío colectivo al que nos enfrentamos al cerrar la brecha de capacidades, estableceremos un grupo perito asesor conformado por el gobierno, empleadores, organismos profesionales, organismos de fomento de capacidades, proveedores de educación y el mundo académico, que fortalecerá la coherencia entre estos sectores clave. El grupo apoyará el desarrollo de una estrategia a largo plazo que tomará en cuenta los desarrollos en el amplio ámbito de las habilidades digitales, asegurándose de que las consideraciones de ciberseguridad estén alineadas e incorporadas de punta a punta. Este grupo trabajará con entidades similares en todo el Reino Unido.

7.1.9. Junto con este trabajo, el gobierno invertirá en toda una gama de iniciativas que traigan mejoras inmediatas y apoyará el desarrollo de la estrategia de pericias a largo plazo. Estas incluyen:

- el establecimiento de un programa escolar para crear un cambio radical en la educación y formación especializada en ciberseguridad para talentos de 14-18 años (con actividades basadas en el aula, sesiones extraescolares con mentores expertos, proyectos desafiantes y escuelas de verano);
- crear prácticas de nivel superior y de grado con los sectores de energía, finanzas y transporte para colmar las brechas de capacidades en áreas esenciales;
- establecer un fondo para reciclar a candidatos que ya forman parte de la plantilla y presentan un gran potencial para la profesión de ciberseguridad;
- identificar y apoyar la cibereducación de licenciatura y posgrado de calidad, e identificar y rellenar cualquier brecha de capacidades especializadas, reconociendo el papel clave que juegan las universidades en el desarrollo de capacidades;
- apoyar la acreditación del desarrollo profesional de profesores en ciberseguridad. Este trabajo ayudará a los profesores, y otros que apoyan el aprendizaje, a que entiendan la educación en ciberseguridad y proporcionará métodos para acreditar externamente a dichos individuos;
- desarrollar la profesión de la ciberseguridad, incluso a través del estatus de Royal Chartered (Academia Real) para el 2020, reforzando la excelencia del reconocido cuerpo de ciberseguridad en el sector y brindando un punto focal por medio del cual pueda asesorarse, diseñarse e informar a las políticas nacionales;
- crear una Academía de ciberdefensa como centro de excelencia para la formación y el ejercicio cibérnetico en el Ministerio de defensa y el gobierno en general,

respondiendo a capacidades especializadas y la educación más amplia;
•desarrollar oportunidades de colaboración en la formación y la educación entre el gobierno, las fuerzas armadas, la industria y el mundo académico, junto con las instalaciones para mantener y ejercitar capacidades; y
• trabajaremos con la industria para ampliar el programa CyberFirst para identificar y alimentar al diverso grupo de talentos jóvenes que defenderá nuestra seguridad nacional; y
• incorporar la ciberseguridad y las pericias digitales como parte íntegra de los cursos relevantes dentro del sistema educativo, desde la primaria hasta los posgrados, estableciendo los estándares, mejorando la calidad y brindando un cimiento fuerte para la progresión hacia adelante en la profesión.

Como la educación es responsabilidad de las administraciones descentralizadas, algunas de estas iniciativas se aplicarán sobre todo a Inglaterra. Sin embargo, trabajaremos con Escocia, Gales e Irlanda del Norte para alentar a que se adopte un enfoque coherente en todos los sistemas educativos del Reino Unido.

Midiendo el éxito
7.1.10. El gobierno medirá nuestro éxito en el fortalecimiento de las capacidades de ciberseguridad comparando nuestros avances con los resultados siguientes:
• existen rutas de entrada a las profesiones de ciberseguridad eficaces y claras, que son atractivas para una gama diversa de personas;
• para el 2021 la ciberseguridad se enseña con eficacia como parte íntegra de los cursos relevantes desde el nivel de primaria hasta el de posgrado;
• se reconoce a la ciberseguridad como una profesión establecida con vías de carrera claras, y ha logrado el Royal Chartered Status;
• el conocimiento en ciberseguiridad apropiado es parte íntegra del desarrollo profesional continuo para los profesionales relevantes en ámbito que no sean de ciberseguridad, en toda la economía; y
• el gobierno y las fuerzas armadas tienen acceso a ciberespecialistas que logran mantener la seguridad y la resiliencia del Reino Unido.

7.2. ESTIMULAR EL CRECIMIENTO DEL SECTOR DE LA CIBERSEGURIDAD

7.2.1. Un sector de ciberseguirdad floreciente e innovador es una necesidad de nuestra economía moderna y digital. Las empresas de ciberseguridad del Reino Unido brindan tecnologías, capacitaciones y asesoramiento de primera categoría para la industria y los gobiernos. Pero a pesar de que el Reino Unido es protagonista, tiene que luchar contra una competencia feroz para mantenerse al frente. También existen barreras que el gobierno tiene que superar. Las empresas y los académicos del Reino Unido desarrollan tecnologías de punta, pero algunos necesitan el apoyo para desarrollar las habilidades comerciales y empresariales que necesitan para prosperar. Hay brechas de financiación que impiden que las PYMES crezcan y lleguen a otros mercados y territorios nuevos. Los productos y servicios más novedosos, que brindan el potencial para mantenerse al frente de la amenaza, luchan por encontrar clientes que estén dispuestos a ser primeros adoptadores. Para superar estos desafíos el gobierno, la industria y el mundo académico tienen que trabajar juntos de forma eficaz.

Objetivo
7.2.2. El gobierno apoyará la creación de un sector de ciberseguridad creciente, innovador y próspero en el Reino Unido para crear un ecosistema en el cual:
• las empresas de seguridad prosperan, y consiguen la inversión que necesitan para crecer;
• las mentes más brillantes del gobierno, el mundo académico y el sector privado colaboran de cerca para estimular la innovación; y
• los clientes del gobierno y la industria tienen suficiente confianza y preparación para adoptar servicios de vanguardia.

Nuestro enfoque
7.2.3. Para crear este ecosistema, vamos a:

• comercializar la innovación en el mundo académico, brindando formación y apoyo de mentores a los académicos;
• establecer dos centros de innovación, para impulsar el desarrollo de ciberproductos de punta y de nuevas empresas de ciberseguridad dinámicas, que estén al centro del programa de iniciativas para darles el apoyo que necesitan a los start-ups para que consigan a sus primeros clientes y atraigan más inversiones;
• asignar una proporción de los 165 millones de libras esterlinas del Fondo de defensa y ciberinnovación para apoyar la contratación y compra innovadora en defensa y seguridad;
• brindar instalaciones para las pruebas de las empresas que desarrollan sus productos, junto con una forma de evaluación acelerada para la próxima generación de productos y servicios de ciberseguridad conforme vayan surgiendo, permitiéndoles a los clientes que confíen en su utilización;
• aprovechar los conocimientos colectivos de la alianza entre la industria y el gobierno para el crecimiento (Cyber Growth Partnership) para ayudar a darle forma y enfoque a mayor crecimiento e intervenciones de innovación:
• ayudar a las empresas de todos tamaños a ampliarse y acceder a los mercados internacionales; y
• promover los estándares internacionales acordados para apoyar el acceso al mercado del Reino Unido.

7.2.4. También aprovecharemos el peso de contratación y adquisiciones del gobierno para estimular la innovación. El gobierno se enfrenta a algunos de sus peores desafíos en ciberseguridad y algunas de sus mayores amenazas. Podemos y debemos seguir las soluciones más eficaces a estos problemas. Esto significa que tenemos que facilitarles a las pequeñas empresas a que hagan negocios con el gobierno. Esto también significa que el gobierno tiene que tener menos aversión a los riesgos de poner a prueba y utilizar nuevos productos. Esta es una solución en la que todos salen ganando: el gobierno conseguirá los mejores servicios, y las tecnologías innovadoras conseguirán un adoptador anticipado, haciendo que sean más atractivas para la inversión y una base de clientes amplia. Alentaremos a todas las partes del gobierno, incluidas las administraciones de Escocia, Gales e Irlanda del Norte a que tomen enfoques similares.

"Queremos crear un ciberecosistema en el que haya una proliferación de ciber start-ups, que consigan la inversión y el apoyo que necesiten para conseguir negocio en el mundo entero, y brinden una cartera de innovaciones que canalice las ideas entre el sector privado, el gobierno y el mundo académico."

Honorable Matt Hancock MP,
Ministro de estado para las áreas digitales y de cultura

Midiendo el éxito

7.2.5. El gobierno medirá su éxito para estimular el desarrollo del sector de la ciberseguridad al evaluar sus avances comparados con los resultados siguientes:
• un crecimiento interanual global mayor del promedio en el tamaño del sector cibernético en el Reino Unido;
• un incremento significativo en la inversión en las empresas que están en sus primeras fases:
• la adopción de tecnologías de ciberseguridad más innovadoras y eficaces por parte del gobierno.

7.3. PROMOVER LA CIBERCIENCIA Y CIBERTECNOLOGÍA

7.3.1. El Reino Unido cuenta con sectores de ciencia y tecnología prósperos y con su investigación de vanguardia, que respaldan nuestras capacidades en ciberseguridad que son líder en el mundo. Para mantener y mejorar la reputación del Reino Unido como líder global en investigación de punta, necesitamos que nuestras instituciones de investigación académica sigan atrayendo a las mentes mejores y más brillantes del ámbito de la ciberseguridad.
Esto requiere que nosotros fomentemos los centros de excelencia para atraer a los científicos y los investigadores más capaces y dinámicos, y

fortalezcamos la alianza activa entre el mundo académico, el gobierno y el sector.
Esto representará un papel de relacionador para el gobierno, para que incentive dichas colaboraciones. El éxito haría que establezcamos un ecosistema autosostenible que permita que las ideas, y las personas, circulen entre los tres sectores de manera que todos salgan beneficiados.

Objetivo
7.3.2. Para el 2021, el Reino Unido habrá fortalecido su posición como líder mundial en ciberciencia y cibertecnología. Las alianzas flexibles entre las universidades y la industria traducirán la investigación en productos y servicios con éxito comercial. El Reino Unido mantendrá su reputación de excelencia innovadora, incluso en las áreas de fortaleza nacional excepcional, como el sector financiero.

Nuestro enfoque
7.3.3. Para lograr esto, el gobierno alentará modelos de financiación que se basen en colaboración y sean innovadores y flexibles para la investigación, y la comercialización de la investigación. El gobierno garantizará que se le preste suficiente atención a los aspectos humanos y de comportamiento del ámbito cibernético, y que los sistemas, más allá de lo técnico, como los procesos de negocios y las estructuras organizativas, se incluyan en la ciberciencia y la cibertecnología.

7.3.4. Esto respaldará la creación de productos, sistemas y servicios que sean “seguros por defecto”, teniéndose en consideración la seguridad adecuada desde el inicio y que la seguridad se convierta en un opción de desactivación consciente para los usuarios.

7.3.5. Publicaremos los detalles de la Estrategia de ciberciencia y cibertecnología después de una amplia consulta con socios y partes implicadas. Esto incluirá la identificación de áreas de ciencia y tecnología que el gobierno, la industria y el mundo académico consideran importante e identificar brechas en la capacidad actual del Reino Unido para responder a las mismas.

7.3.6. El gobierno seguirá proporcionando financiación y apoyo para los Centros de excelencia académica, los institutos de investigación y los centros para formación doctoral. Además, crearemos un nuevo Instituto de investigación en un área temática de importancia estratégica. También financiaremos más investigación en aquellas áreas en que la futura estrategia de ciberciencia y cibertecnología identifique las brechas de capacidades. Las áreas importantes a las que se les prestará consideración incluyen: el análisis de big data; los sistemas autónomos; los sistemas de control industrial fiables; los sistemas ciberfísicos y el Internet de las cosas; las ciudades Smart; la verificación de sistemas automatizada; y la ciberciencia y ciberseguridad.

7.3.7. Seguiremos patrocinando a estudiantes de doctorado nacionales del Reino Unido en los Centros de excelencia académica para hacer que aumente la cantidad de ciudadanos del Reino Unido con cibercompetencias.

7.3.8. El gobierno trabajará con entidades, incluida Innovate UK y los Consejos de investigación (Research Councils) para alentar a que haya colaboraciones entre la industria, el gobierno y el mundo académico. Para apoyar esta colaboración revisaremos las mejores prácticas de clasificación de seguridad e identificaremos a los expertos con habilitación de seguridad, incluidos los académicos. Esto nos permitirá que el trabajo desde espacios no clasificados hasta los que están más allá de la confidencialidad se lleve a cabo de la manera más colaborativa posible.

7.3.9. El gobierno financiará un “gran desafío” para identificar y brindar soluciones innovadoras para algunos de los problemas de ciberseguridad más apremiantes. CyberInvest, una nueva alianza entre el gobierno y la industria para apoyar investigación en ciberseguridad y proteger al Reino Unido en el ciberespacio, formará parte de nuestro enfoque para construir una alianza mundo académico-gobierno-industria.

Midiendo el éxito
7.3.10. El gobierno medirá su éxito en la promoción de la ciencia y la tecnología de la

ciberseguridad evaluando los avances comparados con los resultados siguientes:

- una cantidad mucho mayor de empresas del Reino Unido comercializan con éxito investigación cibernética académica y existen menos brechas, acordadas e identificadas, en la capacidad de investigación en ciberseguridad del Reino Unido con acciones eficaces para colmarlas; y
- se considera al Reino Unido como líder mundial en investigación e innovación en ciberseguridad.

7.4. UNA OBSERVACIÓN DEL HORIZONTE EFICAZ

7.4.1. El gobierno debe asegurarse que la elaboración de políticas tiene en cuenta los cambios en el panorama cibernético, geopolítico y tecnológico. Para hacerlo, necesitamos utilizar con eficacia la observación del horizonte y el trabajo de valoración. Necesitamos invertir en protegernos ante las amenazas futuras y anticipar los cambios del mercado que puedan afectar nuestra ciberresiliencia en cinco o diez años. Necesitamos programas de observación del horizonte que generen recomendaciones para informar las políticas y programas de planificación actuales y futuros del gobierno.

Objetivo

7.4.2. El gobierno garantizará que hagamos una evaluación rigurosa del ciberriesgo, y que ésta esté integrada en las áreas de desarrollo de políticas de ciberseguridad y de otras tecnologías, junto con la evaluación de todas las fuentes y otra evidencia disponible. Nos uniremos a la observación del horizonte entre la seguridad nacional y otras áreas de políticas para garantizar una evaluación integral de los desafíos y las oportunidades emergentes.

Nuestro enfoque

7.4.3. Vamos a:

- identificar brechas en el trabajo actual, y coordinar el trabajo entre las fronteras de las distintas disciplinas para desarrollar un enfoque integral a la observación del horizonte en el ámbito de la ciberseguridad;
- promover una mayor integración de los aspectos técnicos en la ciberseguridad con las ciencias del comportamiento;
- apoyar un monitoreo riguroso del mercado de cibercriminales para detectar nuevas herramientas y servicios que puedan permitir una transferencia de tecnologías a estados hostiles, terroristas o criminales;
- analizar tecnologías emergentes de control de procesos conectados a internet
- anticipar las vulnerabilidades entorno a las divisas digitales; y
- monitorear las tendencias de mercado en tecnologías de las telecomunicaciones para desarrollar defensas tempranas contra ataques futuros anticipados.

7.4.4. Reconocemos que la observación del horizonte va más allá de la parte técnica, incluye las dimensiones política, económica, legislativa, social y medioambiental. La ciberseguridad es sólo un aspecto de estos temas que una observación del horizonte eficaz puede ayudar a abordar. Por lo tanto, nos aseguraremos de cuando llevemos a cabo una observación del horizonte de estas otras áreas de políticas, tengamos en cuenta cualquier implicación de ciberseguridad.

7.4.5. También garantizaremos que la elaboración de ciberpolíticas siga un enfoque basado en la evidencia, teniendo en cuenta las evaluaciones de todas las fuentes disponibles. Esto incluirá, por ejemplo:

- evidencia técnica específica, por ejemplo en el Internet de las cosas, o el papel futuro de los materiales avanzados; y
- las tendencias estratégicas y societales internacionales y su impacto en el mundo cibernético.

7.4.6. Nos aseguraremos de que la ciberseguridad se considere dentro del alcance de la Celda de análisis e innovación y tecnologías emergentes interministerial (ETIAC *por su siglas en inglés*), que se establecerá para identificar las amenazas y las oportunidades de tecnología relevantes para la seguridad nacional y que el ámbito cibernético sea tomado en cuenta por las estructuras de

observación del horizonte actuales, incluido el Grupo de futuros del gobierno (GFG *por sus siglas en inglés*), y el Grupo asesor de secretario del gabinete en su observación del horizonte (CSAG *por sus siglas en inglés*).

Midiendo el éxito

7.4.7. El gobierno medirá nuestro éxito al establecer una buena capacidad de observación del horizonte al comparar los avances con los resultados siguientes:

- la observación de horizonte interministerial y la evaluación de todas las fuentes disponibles se integran en la elaboración de ciberpolíticas; y
- el impacto de la ciberseguridad se tiene en cuenta en todas las observaciones del horizonte interministeriales.

8. ACCIÓN INTERNACIONAL

8.1. Nuestra prosperidad económica y bienestar social dependen cada vez más de la apertura y seguridad de las redes que van más allá de nuestras fronteras. Es esencial que trabajemos de cerca con los socios internacionales para asegurar que siga habiendo un ciberespacio libre, abierto, pacífico y seguro que brinde estos beneficios. Esto será cada vez más importante conforme los próximos mil millones de usuarios se conecten a Internet en el mundo.

8.2. La cooperación internacional en temas cibernéticos se ha vuelto esencial para los debates de la economía y seguridad globales más amplios. Es un área de políticas que no deja de evolucionar, sin una visión única internacional acordada. El Reino Unido y sus aliados tienen éxito al garantizar que se establezcan algunos elementos del sistema internacional basado en normas: se ha llegado al acuerdo de que el derecho internacional se aplica al ciberespacio; que los derechos humanos se aplican tanto online como offline; y hay un amplio consenso en que el enfoque de partes interesadas múltiples es la mejor manera de gestionar las complejidades de gobernanza de Internet. Sin embargo, con una división creciente en cuanto a cómo responder al desafío común de reconciliación de la seguridad nacional con los derechos y libertades individuales, cualquier consenso seguirá siendo frágil.

"Debemos trabajar a nivel internacional para acordar reglas de circulación que garanticen la seguridad y prosperidad futuras del Reino Unido en el ciberespacio."
Honorable Boris Johnson, MP,
Ministro de asuntos exteriores

Objetivos
8.3. El Reino Unido busca proteger el futuro a largo plazo de un ciberespacio libre, abierto, pacífico y seguro, que impulsa el crecimiento económico y respalda la seguridad nacional del Reino Unido. Sobre esta base, el Reino Unido seguirá: promoviendo el modelo de gobernanza de Internet de partes interesadas múltiples; oponiéndose a la localización de datos; y trabajando para construir la capacidad de nuestros socios para mejorar su propia ciberseguridad. Para reducir la amenaza para el Reino Unido y nuestros intereses, gran parte de la cual tiene su origen en el extranjero, buscaremos influir en la toma de decisiones de aquellos que participan en el ciberdelitos, ciberespionaje, y actividades cibernéticas perturbadoras o destructivas y seguiremos construyendo marcos para apoyar la cooperación internacional.

Nuestro enfoque
8.4. Para lograr esto vamos a:
- fortalecer e incorporar una comprensión común de lo que es el comportamiento de un estado responsable en el ciberespacio;
- seguir adelante sobre el acuerdo de que el derecho internacional se aplica en el ciberespacio;
- seguir promoviendo un acuerdo de normas de comportamiento de un estado responsable voluntarias y no vinculantes;
- apoyar el desarrollo y la implementación de medidas de fomento de confianza;
- aumentar nuestra capacidad de perturbar y enjuiciar a los cibercriminales basados en el extranjero, sobre todo en las jurisdicciones de difícil alcance;
- ayudar a fomentar un entorno que permita a nuestras agencias de orden público que trabajen juntas para asegurarse que existan menos lugares en los cuales los ciberdelincuentes puedan actuar sin miedo a que los investiguen o los enjuicien;
- promover la resiliencia en el ciberespacio dando forma a estándares técnicos que gobiernen las tecnologías emergentes internacionales (incluida la encriptación), haciendo que el ciberespacio sea "seguro por diseño" y promoviendo las mejores prácticas;
- trabajar para construir enfoques comunes entre países afines para capacidades como una encriptación fuerte, que tienen implicaciones transfronterizas;
- fomentar la capacidad de otros para responder a amenazas al Reino Unido, y nuestros intereses en el extranjero;

• seguir ayudando a nuestros socios para que desarrollen su propia ciberseguridad – ya que compartimos un ciberespacio único, nos fortalecemos colectivamente cuando cada país mejora sus propias defensas;
• asegurar que la OTAN esté preparada para los conflictos del siglo XXI, que se llevarán a cabo tanto en el ciberespacio como en el campo de batalla;

• trabajar con nuestros aliados para permitir que la OTAN opere con la misma eficacia en el ciberespacio con la que funciona en la tierra, el aire y los mares; y
• asegurarse de que el "Proceso de Londres" de las Conferencias globales sobre el ciberespacio siga promoviendo un consenso global hacia un ciberespacio libre, abierto, pacífico y seguro.

8.5. Existe una gama de relaciones y herramientas en las que seguiremos invirtiendo para lograr y respaldar todos nuestros ciberobjetivos internacionales; no podemos lograr nuestros objetivos de forma aislada. Estos incluyen:
• trabajar de manera conjunta con los aliados tradicionales y socios nuevos para establecer y mantener una relación política y operativa activa fuerte, creando las condiciones políticas para construir alianzas mundiales robustas;
• utilizar nuestra influencia con organizaciones multilaterales como las Naciones Unidas, el G20, la Unión Europea, la OTAN, la OSCE, el Consejo de Europa, la Commonwealth y dentro de la comunidad de desarrollo global; y
• construir relaciones más fuertes con actores no gubernamentales, como la industria, la sociedad civil, el mundo académico y la comunidad técnica. Estos actores son cruciales para la información y formulación de políticas internacionales, y el fortalecimiento de mensajes políticos sobre una gran gama de problemas cibernéticos. Nuestros vínculos académicos de primera categoría mundial nos brindan una plataforma neutral y colaborativa con socios internacionales.

Midiendo el éxito

8.6 El gobierno medirá sus éxitos para fomentar nuestros intereses internacionales en el ámbito cibernético al comparar los avances con los resultados siguientes:
• una colaboración internacional potenciada reduce las ciberamenaza para el Reino Unido y nuestros intereses en el extranjero;
• una comprensión común de la responsabilidad estatal en el comportamiento en el ciberespacio;
• los socios internacionales han aumentado sus capacidades de ciberseguridad; y
• fortalecer el consenso internacional sobre los beneficios de una ciberespacio libre, abierto, pacífico y seguro.

9. PARÁMETROS

9.1. La ciberseguridad sigue siendo un área relativamente inmadura cuando se trata de medir los resultados e impactos, a los que suele llamarse parámetros. La ciencia de la ciberseguridad ya se ha obscurecido por hipérbole y se ha obstruido por la falta total de datos calibrados. Es fuente de frustración de los elaboradores de políticas así como de los negocios, que han luchado por medir su inversión comparada con sus resultados. El gobierno valora que el uso eficaz de parámetros es esencial para cumplir la estrategia y centrarse en los recursos que la respaldan.

9.2. Nos aseguraremos de que esta estrategia esté fundamentada en una serie de parámetros de medición rigurosos y completos mediante los cuales se puedan medir los avances hacia los objetivos que queremos lograr. Además de ser una parte muy importante del producto de la Estrategia por sí mismo, el NSCS juega un papel crucial al propiciar que otras partes del gobierno, la industria y la sociedad cumplan con los resultados estratégicos de esta estrategia.

9.3. El anexo 3 presenta de qué manera las medidas de éxito establecidas en la estrategia contribuirán a los resultados estratégicos, que se revisarán anualmente para garantizar que reflejen correctamente nuestras metas y requisitos nacionales. Los resultados estratégicos, titulares, son los siguientes:

1. El Reino Unido tiene la capacidad de detectar, investigar y combatir eficazmente las amenazas de las ciberactividades de nuestros adversarios.
2. El impacto de la ciberdeliencuencia en el Reino Unido y sus intereses se reduce significativamente y se logra disuadir a los cibercriminales de atacar al Reino Unido.
3. El Reino Unido tiene la capacidad de gestionar y responder eficazmente a los ciberincidentes para reducir el daño que causan al Reino Unido y combatir a los ciberadversarios.
4. Nuestras alianzas con la industria en una ciberdefensa activa hacen que el phishing y los ataques de malware a gran escala ya no sean eficaces.
5. El Reino Unido es más seguro como resultado de los productos y servicios de tecnología que han sido diseñados con la ciberseguridad integrada y activada por defecto.
6. Las redes y los servicios del gobierno serán lo más seguros que puedan ser desde el momento de su primera implementación. El público será capaz de utilizar los servicios digitales con confianza y seguridad de que su información está a salvo.
7. Todas las organizaciones del Reino Unido, grandes y pequeñas, gestionan eficazmente su ciberriesgo y cuentan con el apoyo de asesoramiento de alta calidad diseñado por el NCSC, respaldado por la combinación adecuada de regulaciones e incentivos.
8. Existe el ecosistema adecuado en el Reino Unido para desarrollar y sostener un sector de ciberseguridad que cumpla con nuestras exigencias de seguridad nacionales.

9. El Reino Unido tiene un suministro sostenible de profesionales en cibercapacidades nacionales para cumplir con la demanda cada vez mayor de una economía cada vez más digital, tanto en el sector público como en el privado, como en defensa.

10. El Reino Unido cuenta con el reconocimiento universal como líder global en investigación y desarrollo de ciberseguridad, con el respaldo de altos niveles de conocimiento en la industria y el mundo académico del Reino Unido.

11. El Reino Unido ya está planeando y preparándose para implementaciones de políticas por adelantado para las tecnologías y amenazas futuras y está “preparado para el futuro.”

12. La amenaza para el Reino Unido y nuestros intereses en el extranjero se reduce gracias a un mayor consenso internacional y capacidad hacia

un comportamiento de estado responsable en un ciberespacio libre, abierto, pacífico y seguro.

13. Las políticas, organizaciones y estructuras del gobierno se simplifican para maximizar la coherencia y la efectividad de la respuesta del Reino Unido a las ciberamenazas.

9.4. Reconocemos que algunas de nuestras ambiciones en esta estrategia van más allá del calendario a cinco años. Para que cualquier inversión futura en el ámbito cibernético más allá del 2021 siga brindando el mayor efecto transformador, buscamos que estos resultados a más largo plazo se asignen a después del 2021 para la industria, los reguladores, los auditores, los aseguradores y otras partes del sector público y privado, conforme una gestión eficaz de los riesgos de ciberseguridad se integre en la actividad de gestión estándar para todos.

CONCLUSIÓN CIBERSEGURIDAD MÁS ALLÁ DEL 2021

10.1. La rápida evolución del panorama cibernético no dejará de presentar nuevos desafíos conforme evolucione la tecnología y nuestros adversarios actúen para explotarlos. Sin embargo, esta estrategia busca presentar una gama de políticas, herramientas y capacidades que garanticen que podamos responder rápidamente a cada nuevo desafío que se presente.

10.2. Si no logramos actuar con eficacia, la amenaza seguirá por delante de nuestra capacidad de protegernos de ella. Podemos esperar una explosión de la capacidad de amenaza a todos los niveles.

10.3. En cambio, si logramos estas ambiciones, todas las partes del gobierno del Reino Unido, las empresas y la sociedad jugarán su papel al garantizar una ciberseguridad general para todo el país. Si logramos garantizar que la seguridad se diseñe y se integre, por defecto, en las tecnologías de productos comerciales, los consumidores y los negocios tendrán menos causas de preocupación en cuanto a ciberseguridad. Si el Reino Unido consigue consolidar su reputación como un entorno seguro donde llevar a cabo negocios online, más empresas e inversionistas globales querrán establecerse aquí. La seguridad de las redes CNI y los sectores prioritarios serían más eficaces. A su vez los atacantes potenciales que buscan desarrollar herramientas y métodos de ataque contra sistemas que cuentan con funciones y datos clave tendrán que trabajar más arduamente para superar las capas de seguridad que los rodean. Esto cambiaría la ecuación riesgo recompense para los cibercriminales y actores malintencionados, que tendrían que prever la misma amenaza de enjuiciamiento internacional que existe para los crímenes tradicionales. Si logramos tener éxito al integrar la ciberseguridad en todas las partes de nuestra sociedad, podría significar que el mismo gobierno puede retroceder en ese papel prominente, permitiendo al mercado y la tecnología que lleven las riendas de la evolución de la ciberseguridad en la economía y la sociedad.

10.4. Incluso en el escenario más optimista, para enfrentarse a algunos desafíos que atañen el Reino Unido en el ámbito cibernético, ya sea por su escala o su complejidad, tal vez se necesite más de cinco años. No obstante, esta estrategia nos brinda los medios para transformar nuestra seguridad futura y proteger nuestra prosperidad en la era digital.

ANEXOS

ANEXO 1: ACRÓNIMOS

CCA – el Centro de evaluación cibernética. Basado en el NCSC, brinda valoraciones de la ciberamenaza para que los departamentos gubernamentales del Reino Unido informen sus políticas.

CERT – Equipo de respuesta de emergencia informática

CERT – UK – Equipo de respuesta de emergencia informática nacional en el Reino Unido

CESG – La autoridad técnica nacional para la garantía de la información dentro del Reino Unido.
Brinda un servicio experto e independiente, basado en investigación e inteligencia de confianza sobre seguridad de la información, en nombre del gobierno del Reino Unido.

CNI – Infraestructura nacional crítica. Aquellos elementos críticos de infraestructura (concretamente activos, instalaciones, sistemas, redes o procedimientos y los trabajadores esenciales que los operan y los facilitan), que si se pierden o se ponen en peligro podrían resultar en:

a. un impacto prejudicial importante en la disponibilidad, integridad o prestación de servicios esenciales – incluidos los servicios cuya integridad, si corren peligro, podría resultar en una cantidad importante de muertos o lesionados – 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.

CPNI – El Centro para la protección de la infraestructura nacional. Brinda asesoramiento que busca reducir la vulnerabilidad de las organizaciones en la infraestructura nacional ante el terrorismo y el espionaje. También trabajará en alianza con NCSC para brindar asesoramiento integral sobre seguridad protectiva ante las amenazas en el ciberespacio.

CPNI ha construido una alianza fuerte con las organizaciones del sector privado en la infraestructura nacional, creando un entorno de confianza donde pueda compartirse la información para beneficio mutuo. Las relaciones directas aumentan por medio de la red extendida, que incluye a otros departamentos de gobierno y organizaciones de servicio profesional.

DDoS – Ataque de denegación de servicio. Inundar un sistema de información con más peticiones de información de las que puede gestionar, resultado en que los usuarios autorizados no puedan acceder a él.

GCHQ – Sede de comunicaciones del gobierno; el centro de las actividades de inteligencia y autoridad técnica cibernética nacional (NTA *por su siglas en inglés*).

TIC – Tecnologías de la información y las comunicaciones.

MdD – Ministerio de Defensa

OTAN – Organización del tratado del Atlántico del Norte

NCA – Agencia nacional de crimen; un departamento gubernamental no ministerial.

NCSC – Centro de ciberseguridad nacional.

OSCE – Organización para la Seguridad y la Cooperación en Europa.

PYMES – Pequeñas y medianas empresas.

ANEXO 2: GLOSARIO

Action Fraud – el centro nacional del Reino Unido de denuncias de fraude y delitos por Internet, brinda un punto central de contacto para el público y los negocios.

Ciberdefensa activa (ACD *por sus siglas en inglés*) – el principio de la implementación de medidas de seguridad que fortalezcan la seguridad de una red o sistema para hacer que sea más robusto contra ataques.

Anonimización – el uso de herramientas de anonimidad criptográfica para esconder u ocultar la identidad de uno en Internet.

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

Verificación de sistema automatizado – medidas que garantizan que el software y el hardware funcionen como se espera, y sin errores.

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

Big data – conjuntos de datos que son demasiado grandes para ser procesados y gestionados por herramientas de software comerciales de manera oportuna, y requiere de capacidades de procesamiento a la medida para gestionar su volumen, velocidad de entrega y multiplicidad de fuentes.

Bitcoin - Una divisa digital y sistema de pago.

Malware comercial – el malware que está disponible para comprarse o descargarse gratuitamente, de forma generalizada, que no puede personalizarse y se utiliza por una gran gama de actores de amenaza distintos.

Explotación de la red informática (CNE *por sus siglas en inglés*) – ciberespionaje; el uso de una red informática para infiltrar a la red informática que es el blanco y recolectar inteligencia.

Mercado de ciberdelincuencia – la totalidad de los productos y servicios que apoyan al ecosistema de la ciberdelincuencia.

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

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

Ciberdelincuencia – delitos que dependen del mundo cibernético (delitos que sólo pueden cometerse mediante la utilización de dispositivos TIC, en los cuales el dispositivo es tanto la herramienta para cometer el delito y 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 por el 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 estas interacciones.

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

CyberInvest – un programa de la industria y el gobierno de 6 millones 500 mil libras esterlinas para apoyar la investigación de vanguardia en ciberseguridad y proteger al Reino Unido en el ciberespacio.

Sistema ciberfísico – sistemas con componentes computacionales y físicos integrados; sistemas “smart”.

Ciberresiliencia – la capacidad general de los sistemas y las organizaciones para soportar los cibereventos y, cuando se causa prejuicio, recuperarse de estos.

Ciberseguridad – la protección de sistemas interconectados (para incluir hardware, software y la infraestructura asociada), los datos en ellos, y los servicios que brindan, de acceso no autorizado, daños o uso indebido. Esto incluye los daños causados intencionalmente por el operador del sistema, o accidentalmente, como resultado de no seguir los procedimientos de seguridad o ser manipulado para no hacerlo.

Desafío de ciberseguridad – concursos que alientan a las personas a poner a prueba sus habilidades y plantearse una carrera en el ámbito cibernético.

Ciberespacio – la red interdependiente de redes de infraestructuras de tecnologías de la información que incluye a Internet, las redes de telecomunicaciones, los sistemas informáticos, los dispositivos interconectados y los procesadores y controles integrados. También puede referirse al mundo virtual o dominio como un fenómeno experimentado, o concepto abstracto.

Ciberamenaza – cualquier cosa capaz de arriesgar la seguridad de, o causar daño a, los sistemas de información y dispositivos interconectados (para incluir el hardware, software e infraestructura asociada), los datos en ellos y los servicios que brindan, ante todo por medios cibernéticos.

Violación de datos – el movimiento o diseminación no autorizada de información en una red a una parte no autorizada para que acceda a, o vea, la información.

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

Domain Name System (DNS) – un sistema de identificación de computadoras o servicios de red basado en una jerarquía de dominios.

Documentar o Doxing – la práctica de investigar, o piratear, la información identificable personalmente de un individuo en Internet, después publicarla.

Comercio electrónico – comercio efectuado en, o facilitado por, Internet.

Encriptación – transformación criptográfica de datos (llamado “texto en claro”) a una forma (llamada “texto cifrado”) que oculta el significado de los datos originales, para evitar que se conozca o utilice.

Observación de horizontes – una exploración sistemática de información para identificar las amenazas, riesgos, problemas emergentes y oportunidades potenciales que permitan estar mejor preparados e incorporar la mitigación y la explotación al proceso de elaboración de políticas.

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

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

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

Internet de las cosas industrial (IIoT *por sus siglas en inglés*) – el uso de tecnologías del Internet de las cosas en la fabricación y la industria.

Personal interno – alguien que tiene acceso de confianza a datos y sistemas de información de una organización y que presenta una ciberamenaza intencional, accidental o inconsciente.

Integridad – la propiedad de la que goza la información que no ha sido cambiada

accidentalmente, o deliberadamente, y es exacta y completa.

Internet – una red informática global, que brinda una variedad de facilidades de información y comunicación, que consiste en redes interconectadas utilizando protocolos de comunicación estandarizados.

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

Proceso de Londres – medidas que resultaron de la Conferencia de Londres sobre el ciberespacio de 2011.

Malware – software o código malicioso. El malware incluye virus, gusanos, troyanos y spyware.

Red (informática) – una colección de computadoras centrales, junto con la subred o inter red, a través de las cuales pueden intercambiar datos.

Cibernética ofensiva – el uso de las cibercapacidades para interrumpir, denegar, degradar o destruir redes de computadores o dispositivos interconectados.

Parcheado – parchear es el proceso de actualizar el software para reparar los errores y vulnerabilidades del sistema.

Pruebas de penetración – actividades diseñadas para poner a prueba la resiliencia de una red o instalación contra la piratería informática, autorizadas y patrocinadas por la organización puesta a prueba.

Phishing – el uso de correos electrónicos que parecen originarse de una fuente fiable, que engañan a los destinatarios para que pulsen enlaces o documentos adjuntos maliciosos o armados de malware, o compartan información delicada, con un tercero desconocido.

Ransomware – un software malicioso que le deniega al usuario acceso a sus archivos, computadora o dispositivo hasta que se pague un rescate.

Reconocimiento – la fase de un ataque en la cual el atacante recolecta información sobre, o hace un mapeo de redes, así como explorarlas para encontrar sus vulnerabilidades que puedan explotarse para haquearlos.

Riesgo – el potencial de que un determinado ciberataque explotará las vulnerabilidades de un sistema de información y causará daños.

Router – dispositivos que interconectan redes lógicas al reenviar información a otras redes basado en las direcciones IP.

Script kiddie – un individuo con menos capacidades que utiliza guiones predefinidos, o programas, que pueden encontrarse en Internet para llevar a cabo ciberataques, como la desfiguración de sitios web.

Seguro por defecto – el desbloqueo del uso seguro de las tecnologías comerciales mediante la cual la seguridad se aplica por defecto para los usuarios.

Seguro por diseño – software, hardware y sistemas que han sido diseñados desde su incepción para ser seguros.

Spoofing de SMS – una técnica que enmascara el origen de un mensaje de texto SMS sustituyendo el número de celular de origen (ID del remitente) con texto alfanumérico. Lo puede utilizar legítimamente el remitente para sustituir su número de celular por su propio nombre, o nombre de la empresa, por ejemplo. O puede ser utilizado ilegítimamente, por ejemplo, para hacerse pasar por otra persona de forma fraudulenta.

Ingeniería social – los métodos que utilizan los atacantes para engañar y manipular víctimas para que lleven a cabo acciones o divulguen información confidencial. Típicamente, dichas

acciones incluyen abrir páginas web maliciosas o ejecutar un archivo adjunto no deseado.

Trusted Platform Module (TPM) – un estándar internacional para un criptoprocesador seguro, que es un microprocesador dedicado, diseñado para proteger el hardware al integrar llaves criptográficas en dispositivos.

Usuario – una persona, entidad organizativa, o proceso automatizado, que accede a un sistema, ya sea con autorización, o sin ella.

Virus – los virus son programas informáticos maliciosos que pueden propagarse a otros archivos.

Vishing – vishing o “engaño por voz” es el uso de tecnologías de voz (teléfonos fijos, celulares, correo de voz, etc.) para engañar a las personas para que develen información delicada o información personal a entidades no autorizadas, usualmente para facilitar el fraude.

Vulnerabilidad – errores en programas del software que tienen el potencial de ser explotados por los atacantes.

ANEXO 3: PROGRAMA DE IMPLEMENTACIÓN TITULAR

ESTRATEGIA NACIONAL DE CIBERSEGURIDAD 2016-2021

Visión: que el Reino Unido sea seguro y resiliente ante las ciberamenazas; que sea próspero y confíe en el mundo digital.

Resultados estratégicos	Medidas que indican éxito (para 2021)	Contribuye a
1. El Reino Unido tiene la capacidad de detectar, investigar y combatir eficazmente la amenaza de las ciberactividades de nuestros ciberadversarios.	• Las redes de intercambio de información más fuertes que hemos establecido con nuestros socios internacionales y acuerdos multilaterales más amplios para apoyar un comportamiento legal y responsable de los estados, contribuyen sustancialmente a nuestra capacidad de entender y responder a la amenaza, que tiene como resultado un Reino Unido mejor defendido. • Nuestras medidas de defensa y disuasión, junto con nuestras estrategias específicas en cada país, están haciendo que el Reino Unido sea un blanco más difícil para que puedan tener éxito los actores extranjeros hostiles y los ciberterroristas. • Una comprensión mejorada de la ciberamenaza de actores extranjeros hostiles y terroristas, a través de la identificación y la investigación de ciberamenazas terroristas contra el Reino Unido. • Garantizar que las cibercapacidades terroristas sigan siendo bajas a largo plazo, a través de un monitoreo detallado de la capacidad, y de perturbación del potencial y actividad ciberterrorista a la primera oportunidad. • El Reino Unido es líder mundial en capacidades ciberofensivas. • El Reino Unido ha establecido una cartera de habilidades y pericias para desarrollar y desplegar sus capacidades ciberofensivas soberanas. • Nuestras capacidades criptográficas soberanas son eficaces para mantener nuestros secretos e información delicada a salvo de diseminación no autorizada.	DISUADIR
2. El impacto de la ciberdelincuencia en el Reino Unido y sus intereses se reduce significativamente y los ciberdelincuentes se ven disuadidos de atacar al Reino Unido.	• Contamos con un efecto de interferencia mayor en los ciberdelincuentes que atacan al Reino Unido, con una mayor cantidad de arrestos y condenas, y más redes delictivas desmanteladas como resultado de las intervenciones de orden público. • Capacidades de orden público mejoradas, incluida: la capacidad y las pericias tanto para los especialistas dedicados como para los agentes convencionales; y una mayor capacidad de aplicación de la ley en el extranjero. • Una eficacia mejorada, y mayor escala, de las medidas de intervención temprana (“PREVENIR”) consiste en disuadir y rehabilitar a los infractores. • Una reducción en la cantidad de ciberdelitos de bajo	DISUADIR

Resultados estratégicos		Medidas que indican éxito (para 2021)	Contribuye a
		nivel como resultado de que los servicios de los ciberdelincuentes sean más difíciles de acceder y menos efectivos.	
3.	**El Reino Unido tiene la capacidad de gestionar y responder eficazmente a los ciberincidentes para reducir los daños que causan al Reino Unido y combatir a sus ciberadversarios.**	• Se denuncia una mayor cantidad de incidentes ante las autoridades, lo que lleva a una mayor comprensión del tamaño y la escala de la amenaza. • Los ciberincidentes se gestionan de forma más efectiva, eficiente y completa, como resultado de la creación del Centro de ciberseguridad nacional como mecanismo centralizado de denuncias de y respuesta a incidentes. • Responderemos a las causas raíz de los ataques a nivel nacional, reduciendo las veces que se den explotaciones repetidas entre víctimas y sectores múltiples	DEFENDER
4.	**Nuestras alianzas con la industria en ciberdefensa activa significa que los ataques de phishing y malware a gran escala ya no serán eficaces**	• Es más difícil engañar por medio de “phishing” en el Reino Unido, ya que tenemos defensas a gran escala contra el uso de dominios maliciosos, protección anti phishing más activa a escala y es mucho más difícil utilizar otras formas de comunicación, como el “vishing” y el spoofing por SMS, para llevar a cabo ataques de ingeniería social. • Una proporción más amplia de comunicaciones de malware y artefactos técnicos asociados con ciberataques y explotación se bloquean. • El tráfico de Internet y telecomunicaciones del Reino Unido es significativamente menos vulnerable ante actores maliciosos que buscan desviarlos. • Las capacidades del GCHQ, de la Defensa y del NCA para responder a amenazas graves patrocinadas por estados y amenazas criminales han aumentado significativamente.	DEFENDER
5.	**El Reino Unido es más seguro como resultado de productos y servicios de tecnología que tienen las consideraciones de ciberseguridad en su diseño y activada por defecto.**	• La mayoría de los productos y servicios comerciales disponibles en el Reino Unido en 2021 hacen que el Reino Unido sea más seguro, ya que tienen configuraciones de seguridad habilitadas por defecto o tienen la seguridad integrada desde su diseño. • El público del Reino Unido confía en los servicios del gobierno, ya que se han implementado, de la manera más segura posible, y los niveles de fraude contra ellos entran en los parámetros de riesgo aceptables.	DEFENDER
6.	**Las redes y servicios del gobierno serán lo más seguros posibles desde el momento de su primera implementación. El público será capaz de utilizar servicios gubernamentales digitales con seguridad y confiando en que su información está a salvo.**	• El gobierno entiende en profundidad el nivel de ciberriesgo en todo el gobierno y el sector público en general. • Los departamentos de gobierno individuales y otras entidades se protegen a sí mismas de manera proporcionada a su nivel de riesgo y cumpliendo con estándares mínimos acordados por el gobierno. • Los departamentos del gobierno y el sector público en general son resilientes y pueden responder de forma eficaz a los ciberincidentes, manteniendo funciones y recuperándose rápidamente.	DEFENDER

Resultados estratégicos	Medidas que indican éxito (para 2021)	Contribuye a
	• Las nuevas tecnologías y los servicios digitales desplegados por el gobierno serán ciberseguros por defecto. • Estamos al tanto de, y mitigando activamente, todas las vulnerabilidades conectadas a Internet en los sistemas y servicios del gobierno. • Todos los proveedores del gobierno cumplen con los estándares de ciberseguridad apropiados.	
7. Todas las organizaciones del Reino Unido, grandes y pequeñas, gestionan con eficacia su ciberriesgo, reciben asesoramiento de alta calidad diseñado por el NCSC, respaldado por la combinación adecuada de reglamentación e incentivos.	• Entendemos el nivel de ciberseguridad en el CNI, y contamos con medidas establecidas para intervenir, cuando sea necesario, para impulsar mejoras en el interés nacional. • Nuestras empresas y organizaciones más importantes entienden el nivel de amenaza e implementan prácticas de ciberseguridad proporcionadas. • El nivel de ciberseguridad de la economía del Reino Unido es tan elevado como, o más elevado que, las economías avanzadas comparables. • La cantidad, gravedad e impacto de los ciberataques exitosos contra negocios en el Reino Unido se ha reducido, ya que los estándares de ciberhigiene se han aplicado. • El Reino Unido ha mejorado su cultura de ciberseguridad, ya que las organizaciones y el público entienden sus niveles de ciberriesgo, y entienden los pasos de ciberhigiene que necesitan emprender para gestionar estos riesgos.	DEFENDER
8. Existe el ecosistema adecuado en el Reino Unido para desarrollar y mantener un sector de ciberseguridad que pueda cumplir con nuestras exigencias de seguridad nacional.	• Un crecimiento global más elevado que el promedio en el tamaño del cibersector en el Reino Unido en términos interanuales. • Un incremento significativo en la inversión en las empresas que están en sus primeras etapas.	DESARROLLAR
9. El Reino Unido cuenta con un suministro sostenible de profesionales nacionales con cibercapacidades para cumplir con las demandas crecientes de una economía cada vez más digital, tanto el en sector público como privado, y en defensa.	• Hay rutas de entrada efectivas y claras en la profesión de ciberseguridad, que son atractivas para una gama muy diversa de personas. • Para 2021 la seguridad se enseña de forma efectiva como parte íntegra de los cursos relevantes dentro del sistema educativo, desde el nivel de primaria hasta el de posgrado. • Se reconoce a la ciberseguridad ampliamente como profesión establecida con vías de carrera claras, y ha logrado el estatus de Royal Chartered. • Un conocimiento adecuado de ciberseguridad es parte íntegra del desarrollo profesional continuo para los que no son profesionales de ciberseguridad relevantes, en toda la economía.	DESARROLLAR

Resultados estratégicos	Medidas que indican éxito (para 2021)	Contribuye a
	• El gobierno y las fuerzas armadas tienen acceso a ciberespecialistas capaces de mantener la seguridad y resiliencia del Reino Unido.	
10. El Reino Unido es reconocido universalmente como líder global en investigación y desarrollo en ciberseguridad, respaldado por altos niveles de conocimientos en la industria y el mundo académico del Reino Unido.	• La cantidad de empresas del Reino Unido que comercializan exitosamente investigación cibernética académica ha aumentado significativamente. Hay menos brechas acordadas e identificadas en las capacidades de investigación en ciberseguridad del Reino Unido, y acciones eficaces se han emprendido para reducirlas. • Se considera al Reino Unido líder global en investigación e innovación en ciberseguridad.	DESARROLLAR
11. El gobierno del Reino Unido ya está planificando y se está preparando para implementación de políticas adelantándose a las tecnologías y amenazas futuras y está "a prueba del futuro".	• El trabajo de observación del horizonte interministerial y las valoraciones de todas las fuentes están integrados en la elaboración de ciberpolíticas. • El impacto de la ciberseguridad se tiene en cuenta en todo el trabajo de observación del horizonte interministerial.	DESARROLLAR
12. La amenaza para el Reino Unido y nuestros intereses en el extranjero se reduce debido a un mayor consenso internacional y capacidades favorables a un comportamiento responsable del estado en un ciberespacio libre, abierto, pacífico y seguro.	• Una colaboración internacional mejorada reduce las ciberamenazas para el Reino Unido y nuestros intereses en el extranjero; • Una comprensión común de un comportamiento responsable por parte del estado en el ciberespacio; • Los socios internacionales incrementan sus capacidades de ciberseguridad; y • Un consenso internacional más fuerte sobre los beneficios de un ciberespacio libre, abierto, pacífico y seguro.	ACCION E INFLUENCIA INTERNACIONALES
13. Las políticas, las organizaciones y las estructuras del gobierno del Reino Unido se simplifican para maximizar la coherencia y la efectividad de la respuesta del Reino Unido a las ciberamenazas.	• Las responsabilidades de ciberseguridad del gobierno se entienden y sus servicios son accesibles. • Nuestros socios entienden cuál es la mejor manera de interactuar con el gobierno en temas de ciberseguridad.	TRANSVERSAL