EL PRESIDENTE
COMITÉ ASESOR DE TELECOMUNICACIONES DE SEGURIDAD NACIONAL

Informe de la NSTAC al Presidente sobre una toma lunar de seguridad cibernética

14 de noviembre de 2018

TABLA DE CONTENIDO

RESUMEN EJECUTIVOYE-1

1.0 INTRODUCCIÓN1

2.0¿POR QUÉ LA SEGURIDAD CIBERNÉTICA REQUIERE UN TIRO A LA LUNA? 2

3.0 PLAN DE ACCIÓN DE LA INICIATIVA "MOONSHOT" DE SEGURIDAD CIBERNÉTICA 3

3.1 Entregar la declaración de aspiraciones4
3.2 Establecer la gobernanza para el enfoque de toda la nación6
3.2.1 Todo el Gobierno7
3.2.2 Toda la industria y la academia9
3.3 Otras consideraciones clave de la Iniciativa sobre Seguridad Cibernética en la Luna10
3.3.1 Consideraciones presupuestarias10
3.3.2 Medir el éxito, definir los hitos del progreso y construir el impulso11
3.4 Definir el marco estratégico y los pilares 12
3.4.1 Pilar de la tecnología 15
3.4.2 Pilar del comportamiento humano18
3.4.3 Pilar de la educación..... 21
3.4.4 Pilar del Ecosistema..... 23
3.4.5 Pilar de la privacidad26
3.4.6 Pilar de la política28
3.5 La Iniciativa de Seguridad Cibernética Moonshot Initiative Grandes Retos30
3.5.1 Criterios de identificación y evaluación31
3.5.2 El papel del gobierno de EE.UU. en el fomento de la acción a través de la seguridad cibernética Gran Desafíos 32

4.0 CONCLUSIÓN33

APÉNDICE A:METODOLOGÍA.....ESTUDIO DEL SUBCOMITÉ A-1 APÉNDICEB: COMPOSICIÓ.....N DEL SUBCOMITÉ B-1 APÉNDICE C: ACRÓNIMOSC-1

APÉNDICE D: GLOSARIO D-1

APÉNDICE E: BIBLIOGRAFÍA E-1

RESUMEN EJECUTIVO

"Hacer que Internet sea segura para el funcionamiento del Gobierno y los servicios críticos para el pueblo americano para el año 2028".

Los Estados Unidos se encuentran en un punto de inflexión: simultáneamente se enfrentan a un entorno de amenazas a la seguridad cibernética que empeora progresivamente y a una dependencia cada vez mayor de las tecnologías de Internet fundamentales para la seguridad pública, la prosperidad económica y el modo de vida en general. Nuestra seguridad nacional está ahora inexorablemente ligada a la ciberseguridad. Por lo tanto, la nación debe basarse en los esfuerzos pasados y las estrategias actuales para aprovechar la oportunidad de reorientarse estratégicamente de una postura de seguridad cibernética incremental y en gran medida reactiva a un enfoque proactivo que garantice audazmente la confianza, la seguridad y la capacidad de recuperación digital para todos los estadounidenses. El logro de este audaz resultado requerirá un fuerte liderazgo nacional, voluntad política y una inversión sostenida de toda la nación durante un período prolongado.
El Gobierno de los Estados Unidos puede adoptar medidas inmediatas que sienten las bases de esta visión compartida de la seguridad cibernética a largo plazo para la nación, al tiempo que produce beneficios a corto plazo que aseguran un liderazgo tecnológico mundial continuo.

El liderazgo debe comenzar con una audaz declaración de aspiraciones de intención estratégica, como los Estados Unidos han hecho sólo unas pocas veces históricamente al enfrentar desafíos existenciales. El Comité Asesor de Telecomunicaciones de Seguridad Nacional del Presidente (NSTAC) cree que la seguridad cibernética representa uno de los mayores desafíos del siglo XXI, y uno que los Estados Unidos simplemente deben abordar de forma duradera como un asunto de imperativo estratégico nacional. Para comunicar esto, el
La administración, en sus niveles más altos, debe ofrecer una clara visión aspirante e inspiradora como fuerza catalizadora de las actividades nacionales. Debe declarar una intención estratégica nacional de: *Hacer que Internet sea segura para el funcionamiento del Gobierno y los servicios críticos para el pueblo estadounidense para 2028.* Esa búsqueda aseguraría la confianza de la sociedad en la infraestructura digital, promovería la vitalidad económica y reforzaría el liderazgo de la innovación estadounidense.

El NSTAC adoptó el término "Ciberseguridad". "Toma de la Luna" para describir este enfoque, llamado así por la Aeronáutica y el Espacio Nacional
El esfuerzo del programa Apolo de la Administración (NASA) para enviar a un hombre a la Luna después del discurso del Presidente John F. Kennedy en mayo de 1961 en una sesión conjunta del Congreso. El disparo original a la luna orientó la acción nacional colectiva hacia una ambiciosa meta de poner a un hombre en la luna y devolverlo sano y salvo a la Tierra para el final de la década. Es importante que el presidente Kennedy claramente articuló este objetivo final sin ser prescriptivo de las muchas innovaciones y acciones individuales necesarias para lograr ese resultado.

> "Creo que poseemos todos los recursos y talentos necesarios. Pero la realidad es que nunca hemos tomado las decisiones nacionales ni reunido los recursos nacionales necesarios para tal liderazgo. Nunca hemos especificado objetivos a largo plazo en un calendario urgente o administrado nuestros recursos y nuestro tiempo para asegurar su cumplimiento".
>
> - El Presidente John F. Kennedy en su discurso ante una sesión conjunta del Congreso el 25 de mayo de 1961

Sin embargo, son numerosas las diferencias entre las características de la visión de un disparo a la luna del presidente Kennedy y las que se prevén de un disparo a la luna para la ciberseguridad. Principalmente, los criterios de éxito de una iniciativa de tiro a la luna para la seguridad cibernética serán menos precisos y mensurables porque su logro será una transformación social más que un triunfo visual singular. El NSTAC reconoce estas limitaciones de la analogía, pero cree firmemente que la Iniciativa Moonshot representa un

un modelo poderoso y altamente aplicable para el establecimiento de prioridades nacionales, la acción colectiva y la innovación acelerada necesarias para la ciberseguridad.

Para lograr su objetivo, la Iniciativa de Ciberseguridad Lunar debe buscar respuestas a varias preguntas complejas. Para empezar: ¿Qué significa "seguro y protegido" en la sociedad digital moderna?
¿Qué "servicios críticos" son más fundamentales para la seguridad nacional y la seguridad pública y deben tener prioridad a nivel nacional para lograr una Internet mensurable y segura? Empezar a lidiar públicamente con estas complejas cuestiones a nivel nacional y con una comunidad de interesados mucho más inclusiva es fundamental para hacer realidad este futuro más audaz y sostenible. En algunos casos, el NSTAC trata de responder a este tipo de preguntas en este informe. En otros, estas respuestas deben ser fruto de la Iniciativa nacional de seguridad cibernética a largo plazo "Moonshot" que este informe propone poner en marcha.

Entregar una declaración de intenciones con aspiraciones no es suficiente, por supuesto. La Iniciativa sobre la seguridad cibernética debe estar profundamente arraigada en un marco estratégico claro y en principios compartidos que trasciendan las estrategias individuales y hagan hincapié en un verdadero cambio generacional. Debe contar con una estructura de gobernanza que permita a los grupos distribuidos de interesados de todo el Gobierno, la industria privada, el mundo académico y la sociedad civil centrar sus energías y actividades colectivas en los objetivos nacionales definidos y de orden superior de la Iniciativa "Moonshot" sobre seguridad cibernética.

A lo largo de este informe, el NSTAC se esfuerza por responder a varias preguntas fundamentales, entre ellas qué es una Iniciativa de Seguridad Cibernética en la Luna, por qué es necesaria y cómo la Nación puede ponerla en práctica de manera efectiva. La Sección 1.0, *Introducción*, y la Sección 2.0, *¿Por qué la ciberseguridad requiere una "toma de luna"?* se centran en por qué es necesaria una Iniciativa "toma de luna" para la ciberseguridad, por qué la actual trayectoria de mejora incremental de la ciberseguridad es inadecuada, y por qué este reto es digno de una persecución que defina la generación.

La Sección 3.0, *Plan de Acción de la Iniciativa sobre Seguridad Cibernética en la Luna*, ofrece recomendaciones estratégicas y medidas prácticas que el Gobierno de los Estados Unidos puede adoptar para dirigir esta iniciativa y utilizar sus autoridades únicas para promover, organizar, dirigir, dotar de recursos y potenciar estratégicamente las actividades de toda la nación en consonancia con sus objetivos. En la sección 3.0 se definen los elementos iniciales de un libro de jugadas de la Iniciativa sobre la Ciberseguridad en la Luna, en el que se esbozan las recomendaciones relacionadas con la organización práctica y la puesta en marcha de la iniciativa. Esto incluye consideraciones clave relacionadas con la gobernanza, los objetivos, los hitos, la financiación y un marco de organización denominado Pilares Estratégicos. Un resumen de las recomendaciones clave contenidas en este informe incluye:

Recomendaciones clave: Gobernanza de la Iniciativa sobre la Seguridad Cibernética (*Sección 3.1-3.3*)

- El Presidente o el Vicepresidente deben presentar y defender estratégicamente una Iniciativa de Seguridad Cibernética para señalar claramente que abordar los retos de la seguridad cibernética de manera duradera es un imperativo estratégico fundamental para el futuro de la nación. Esta proclamación debería hacerse en un foro de importancia histórica, como el Estado de la Unión o un discurso especial en una sesión conjunta del Congreso, para hacer hincapié en este nivel de prioridades nacionales.

- La Iniciativa Moonshot de Ciberseguridad debe generar un enfoque de toda la nación, incluido un modelo de gobernanza de varios niveles que abarque al gobierno, la industria y el mundo académico y que adapte sus capacidades y actividades inherentes a la realización de una Internet segura y protegida. Este modelo podría incluir una estructura empresarial de tipo consorcial que facilite la cooperación, los recursosy recompensar el reparto cuando sea apropiado y no perjudicial para la dinámica competitiva del mercado que promete el camino más eficaz hacia los objetivos. También deberían existir mecanismos oficiales de colaboración con los gobiernos y los asociados académicos para lograr objetivos comunes.

- Dentro del Gobierno de los Estados Unidos, un Consejo de Seguridad Cibernética dirigido por la Administración debería dirigir y gestionar la iniciativa. El Consejo debería encargarse y estar facultado para: aumentar la visibilidad nacional, promover una financiación sostenida, elaborar estrategias a nivel nacional y crear políticas y procesos que faculten e incentiven a las partes interesadas no gubernamentales a impulsar una innovación acelerada en los ámbitos propicios definidos por la Iniciativa sobre la Ciberseguridad Operativa. El mandato del Consejo debería orientarse exclusivamente al logro de resultados a largo plazo, distintos pero complementarios de la dirección de la seguridad cibernética existente en los gobiernos, que a menudo se orienta naturalmente hacia requisitos a más corto plazo y de actualidad.

- El Presidente o Vicepresidente debe presidir oficialmente el Consejo, que debe estar compuesto por funcionarios de nivel de gabinete de los departamentos y organismos pertinentes. El Consejo de Seguridad Cibernética de la Luna debe contar con mecanismos oficiales para que las entidades no gubernamentales designadas contribuyan directamente a la estrategia y al proceso de desarrollo de políticas de la Iniciativa sobre Seguridad Cibernética de la Luna. Un Director Ejecutivo nombrado por el Presidente debería dirigir operacionalmente la iniciativa y ser responsable y estar facultado para mantener la visibilidad de todas las actividades nacionales de la Iniciativa sobre Seguridad Cibernética y elevar las actividades que proporcionen el mayor impacto estratégico hacia la realización de un entorno de Internet seguro y protegido.

- El Consejo de la Iniciativa sobre la Seguridad Cibernética en la Luna debería articular públicamente un Marco Estratégico, tras un período de consultas internas y externas, para proporcionar una estructura común que ayude a organizar las actividades distribuidas de la Iniciativa sobre la Seguridad Cibernética en la Luna en toda la nación. Como punto de partida recomendado, el NSTAC propone seis pilares estratégicos, reconociendo que para lograr una Internet más duradera y segura en los próximos 10 años se requerirá un enfoque holístico y multidisciplinario.

Recomendaciones clave: Pilares estratégicos de la Iniciativa de Seguridad Cibernética de la Luna (*Sección 3.4*)

La realización de progresos significativos hacia una Internet más duradera y segura en los próximos 10 años no será el resultado de una solución singularmente transformadora. La complejidad del desafío de la ciberseguridad requerirá una atención estratégica y un ritmo acelerado de innovación en materia de tecnología, personas, procesos y políticas, tal como lo representa el Plan Estratégico de Seguridad de la Internet.
Pilares. Para lograr un progreso significativo será necesario incentivar las soluciones existentes y conocidas y buscar la realización de nuevas soluciones de transformación.

El NSTAC recomienda seis pilares estratégicos para guiar esta actividad distribuida en toda la nación:
(1) *Tecnología*; (2) *Comportamiento humano; (*3) *Educación; (*4) *Ecosistema; (*5) *Privacidad*; y (6) *Política*. Estos pilares no deben ser considerados como corrientes de trabajo independientes. Deben considerarse como elementos interdependientes fundamentales de la Iniciativa sobre la seguridad cibernética, que incluye actividades que complementan y refuerzan el resultado deseado de una Internet segura y protegida.

1. Tecnología

Los dramáticos avances tecnológicos siguen ampliando el panorama digital y creando nuevos riesgos de seguridad cibernética que los agentes maliciosos tratan de explotar activamente. Sin embargo, estas mismas tecnologías nuevas y rápidamente emergentes, si se aprovechan estratégicamente, pueden permitir una capacidad de seguridad defensiva más automatizada y eficaz. Muchos de estos fundamentos tecnológicos fundamentales existen o están en desarrollo, pero requerirán una estrategia nacional concertada de investigación y desarrollo de productos para hacerlos frente al desafío nacional de la ciberseguridad. Entre los principales resultados que se desean obtener dentro del pilar estratégico de la tecnología se incluyen:

- Se identifican las tecnologías estratégicas que se consideran fundamentales para la seguridad general del entorno de Internet, se les da prioridad y se invierte en ellas para acelerar su disponibilidad. A título ilustrativo, entre las esferas tecnológicas que se consideran críticas sobre la base de las conclusiones del Comité Nacional de Ciencia y Tecnología, cabe mencionar las siguientes:
    - Inteligencia aumentada que asiste a los humanos en lugar de reemplazarlos, para la prevención automatizada de amenazas que puede adelantarse al ritmo de los atacantes;
    - Comunicaciones cuánticas y criptografía cuántica resistente que puede proteger los actuales métodos criptográficos utilizados para la defensa de la ciberseguridad;
    - Biometría del comportamiento para proporcionar puntuaciones de identidad que reduzcan la dependencia de las contraseñas tradicionales y la identificación de identificación personal frecuentemente comprometida para la autenticación; y
    - 5G Comunicaciones y otras redes de próxima generación diseñadas y proyectadas desde el principio con mayor seguridad, conectividad y disponibilidad.
- Se aplican planes estratégicos nacionales para acelerar el crecimiento en esas esferas

tecnológicas fundamentales, incluso mediante grandes desafíos de seguridad cibernética selectivos, cuando proceda, para superar los esfuerzos internacionales competitivos.

- Se elabora un marco normativo y se racionalizan los obstáculos reglamentarios para incentivar y recompensar la inversión y la innovación del sector privado en las tecnologías en que se basa la Iniciativa sobre la seguridad cibernética.

2. El comportamiento humano

La tecnología por sí sola no puede hacer frente a los principales desafíos de seguridad cibernética de la nación. Estos retos exigirán el ingenio de una comunidad de innovación mucho más amplia de expertos multidisciplinarios inspirados para dedicar sus conocimientos a objetivos de transformación de la ciberseguridad. Los ciudadanos y las empresas también deben comprender su responsabilidad en la prevención de los ataques cibernéticos con éxito y estar dotados de información y herramientas que les incentiven a tomar las decisiones correctas en materia de seguridad, por defecto. Las campañas eficaces de cambio de comportamiento, como "Smokey the Bear" y las iniciativas contra la conducción bajo los efectos del alcohol, destinadas a aumentar la presión social contra los comportamientos arriesgados y perjudiciales para la sociedad, son una de esas herramientas.

1. Educación

La Iniciativa sobre la seguridad cibernética en la Luna debe abordar la importante escasez de conocimientos especializados y de financiación para las principales disciplinas de investigación estratégica, incluidas las tecnologías críticas previamente identificadas. La iniciativa debe promover herramientas educativas altamente distribuidas y de escala exponencial y ampliar el uso de la tutoría y el aprendizaje como multiplicadores de fuerza en áreas críticas. En la planificación de la educación en materia de seguridad cibernética estratégica también se debe tener en cuenta la forma en que las tecnologías emergentes, como la inteligencia aumentada, alterarán las necesidades tradicionales de la fuerza de trabajo en materia de seguridad cibernética.

2. Funciones y responsabilidades de los ecosistemas

Ninguna entidad gubernamental, empresa o grupo industrial es capaz, por sí solo, de diseñar, conceptualizar, construir o poner en funcionamiento los fundamentos de un entorno de Internet seguro. El esfuerzo debe ser el resultado de un enfoque coordinado en el que los interesados tengan una comprensión común de sus respectivas funciones y responsabilidades y adopten medidas que promuevan la integración de las capacidades complementarias del ecosistema. La Internet está compuesta por miles de millones de dispositivos, programas informáticos, servicios y usuarios. Para hacer posible un entorno de Internet fundamentalmente seguro para el gobierno y los servicios críticos, manteniendo al mismo tiempo la ubicuidad del acceso a la Internet, se requerirá un esfuerzo consciente y coordinado para trabajar con una amplia variedad de participantes en diversos niveles de confianza.

3. Privacidad

La privacidad es un principio básico que debe impregnar todos los aspectos de la Ciberseguridad Lunar.
El desarrollo de la Iniciativa y será primordial para generar la confianza del pueblo americano. Los ciudadanos americanos deben ser capaces de confiar en los sistemas de información que proporcionan servicios críticos y tener la certeza práctica de que la Iniciativa de Seguridad Cibernética Moonshot no creará privacidad
vulnerables, sino que en su lugar mejoran la garantía de privacidad y aseguran que sus datos y transacciones personales permanecerán protegidos y bajo su control.

4. Política

El Gobierno debe evaluar y aplicar cuidadosamente políticas que faculten e incentiven a los principales interesados responsables de la Iniciativa sobre la seguridad cibernética de la luna, permitiendo las innovaciones y la aplicación. Será necesario crear, reformar o poner fin a las políticas para fomentar la creación de un entorno de Internet fundamentalmente seguro. Por ejemplo, el requisito de una identidad de confianza y de interacciones plenamente autenticadas para garantizar un entorno de Internet seguro requerirá una infraestructura de políticas de mayor seguridad, atribución y responsabilidad. La estrecha coordinación con los legisladores, la comunidad nacional e internacional y los asociados del sector privado en lo que respecta a las normas mundiales de comportamiento en el ciberespacio también será fundamental para el éxito.

Recomendaciones clave: Iniciativa de seguridad cibernética Moonshot - Grandes desafíos (*Sección 3.5*)

Cuando se propone algo tan a largo plazo y complejo como la Iniciativa Moonshot de seguridad cibernética, el NSTAC cree que es fundamental identificar un número discreto de esferas de interés específicas a corto plazo que sirvan de modelos representativos de los principios más amplios de la visión general de la seguridad cibernética Moonshot. Los principios representados por la comunidad bien establecida de los "Grandes Retos": pensamiento audaz, incentivos basados en los resultados, innovación abierta, solución de crowdsourcing encajan perfectamente en este molde. Este enfoque de "Gran Reto" debe ser adoptado con más fuerza por la comunidad de ciberseguridad. El Gobierno de los EE.UU. puede liderar esta transformación mediante el lanzamiento de una serie de Grandes Retos de la Ciberseguridad que producen avances más inmediatos y de mayor impulso hacia la realización de un entorno de Internet seguro y protegido.

- Como catalizador de la Iniciativa sobre la seguridad cibernética en general, el Consejo de Seguridad Cibernética debería dirigir la identificación y el lanzamiento de uno o más grandes desafíos mediante un proceso de colaboración de seis meses de duración en el que participen oficialmente las partes interesadas de todo el país. Esos Grandes Retos deberían organizarse en torno a esferas críticas del desarrollo tecnológico en las que la intransigencia sistémica y los fallos del mercado han obstaculizado anteriormente el progreso. El Gobierno de los Estados Unidos puede aprovechar diversas herramientas para incentivar y acelerar la adopción en toda la nación de estas actividades alineadas con el Gran Reto a través de los seis pilares estratégicos.

- Al evaluar los posibles candidatos al Gran Reto, el Gobierno debe sopesar varias consideraciones y preguntas clave, entre ellas: 1) ¿Tiene el Gobierno una función clara en la catalización de actividades alineadas con el Gran Reto en los casos en que los anteriores impulsores basados en el mercado han demostrado ser insuficientes? 2) ¿Requiere el Gran Reto actividades que van más allá del alcance de las autoridades gubernamentales y/o de los puntos fuertes y se beneficiaría de una colaboración más amplia?
  3) ¿Comprendería la sociedad, en particular los expertos en materia de no ciberseguridad, el valor estratégico y la importancia del Gran Reto? 4) ¿Es el Gran Reto mensurable y alcanzable? 5) ¿Produciría la realización de los objetivos del Gran Reto un resultado altamente escalable? y 6) ¿Tiene el Gran Reto un alcance lo suficientemente amplio como para incluir actividades a través de múltiples pilares estratégicos?

La Administración tiene una oportunidad única en la historia. Decenios de actividades bien intencionadas pero inconexas han hecho que Internet sea cada vez menos segura para los servicios críticos que dependen de ella. El NSTAC cree que debemos ser más audaces y proclamar, como imperativo estratégico nacional, que nuestro objetivo a 10 años es hacer que la Internet sea segura para las interacciones de los estadounidenses con el Gobierno y los servicios críticos. El NSTAC tiene una visión clara de la enormidad de este objetivo y formula esta recomendación teniendo plenamente en cuenta tanto la urgencia del éxito como las cuestiones críticas que han hecho que los esfuerzos anteriores y bien intencionados se quedaran cortos.

La historia proporciona un precedente real para que la nación supere desafíos aparentemente imposibles. En estas instancias históricas, los líderes declararon una intención estratégica sin una clara comprensión de los medios para el fin. En estos ejemplos históricos, como ahora, había un objetivo claro, primeros pasos tangibles y un enfoque de toda la nación que los líderes del gobierno de los Estados Unidos utilizaron para dirigir el esfuerzo e inspirar el éxito. Una oportunidad igualmente imperativa existe para el siglo XXI. Nuestra futura prosperidad y éxito como nación depende ahora intrínsecamente de nuestro éxito en la ciberseguridad, y un inspirador esfuerzo como el de Moonshot es necesario para abordarlo.

1.0INTRODUCCIÓN

La Internet, y la actual era digital que ha inaugurado, ha sido fuente de inconmensurables beneficios económicos y sociales. La posibilidad de utilizar la Internet abierta y la libertad de utilizar las tecnologías conectadas a ella se ha convertido simplemente en un derecho básico y fundamental. Los Estados Unidos deben preservar esta libertad asegurándose de que los estadounidenses puedan utilizar esas tecnologías con seguridad, como cuestión de imperativo estratégico nacional, y al mismo tiempo dar el ejemplo a nivel internacional.

> Tal vez más que cualquier otro desafío económico y de seguridad nacional del siglo XXI, la seguridad cibernética exige un mayor sentido de responsabilidad compartida y de acción colectiva.

En su actual trayectoria, los Estados Unidos se enfrentan a riesgos inequívocos para hacer realidad este imperativo nacional e internacional. Las amenazas a la seguridad cibernética son cada vez más frecuentes, más sofisticadas,
y más destructiva, erosionando gradualmente la confianza de la sociedad en la infraestructura digital. A medida que la tecnología continúa avanzando y cada faceta de la vida diaria se interconecta cada vez más, tanto la
la probabilidad y el costo de la falla aumentan dramáticamente. Los tecnólogos y expertos en seguridad cibernética de todo el mundo reconocen esta tendencia preocupante, pero muchos dirigentes gubernamentales, ejecutivos de empresas o el público en general todavía no la comprenden ampliamente. Tal vez más que cualquier otro desafío económico y de seguridad nacional del siglo XXI, la ciberseguridad exige un mayor sentido de responsabilidad compartida y de acción colectiva. Nuestra era de hiperconectividad significa ahora que su riesgo es mi riesgo, ya que los ataques a los eslabones más débiles pueden ahora tener consecuencias para el entorno digital más amplio. *1*

La compleja naturaleza de la ciberseguridad ha creado una multitud de desafíos que abarcan cuestiones de tecnología, personas y procesos. Esta complejidad ha dado lugar a una tendencia a compartimentar el desafío en sus componentes individuales, más fáciles de entender. Otra complicación para la identificación de soluciones duraderas es el hecho de que las capacidades, autoridades y responsabilidades de la ciberseguridad están muy distribuidas en todo el ecosistema. Ninguna de las partes interesadas puede hacer frente al desafío de manera unilateral. A menudo, los principales costos de un ataque a la ciberseguridad no son
que soporta la víctima inicial, lo que conduce a externalidades negativas e incentivos mal alineados para mejorar los comportamientos de riesgo de la ciberseguridad. Estas características nos han llevado con demasiada frecuencia a conceptualizar soluciones de forma demasiado fragmentada, reactiva o incremental. En consecuencia, los desafíos discretos en materia de ciberseguridad tienden a abordarse a expensas de la prevención proactiva de los ataques cibernéticos y la reducción del riesgo sistémico de la ciberseguridad sobre una base holística.

La escala, gravedad y complejidad de la amenaza a la seguridad cibernética plantea ahora un riesgo existencial para el futuro de la nación, lo que exige la exploración de un enfoque fundamentalmente nuevo para identificar soluciones más audaces para una Internet más duradera y segura. El Comité Asesor de Telecomunicaciones para la Seguridad Nacional (NSTAC) del Presidente reconoce que hay muchas prácticas óptimas conocidas y que las políticas, si se siguen con mayor sensatez, mejorarán de manera apreciable la seguridad de Internet. Sin embargo, el presente informe se centra en la búsqueda de esfuerzos más transformadores que alteren fundamentalmente el nivel por defecto de la seguridad de Internet. Esta búsqueda será un desafío

que definirá la generación y, al igual que la carrera espacial que la precedió, puede servir para inspirar y sentar las bases de un liderazgo tecnológico mundial continuo de los Estados Unidos en los decenios venideros. Mientras que los Estados Unidos aún no han experimentado un evento singular, como el Sputnik, para galvanizer ciberseguridad, la Nación debe demostrar la fortaleza y la previsión para tomar medidas audaces y proactivas antes de que ocurra un evento tan catastrófico y que obligue a tomar medidas.

[1] Kirstjen M. Nielsen, "Observaciones de la Secretaria Kirstjen M. Nielsen en la Conferencia RSA" (observaciones, San Francisco, CA, 17 de abril de 2018) Discursos, https://www.dhs.gov/news/2018/04/17/secretary-kirstjen-m-nielsen-remarks-rsa-conference.

2.0¿POR QUÉ LA CIBERSEGURIDAD REQUIERE UN TIRO A LA LUNA?

La primera fase de la investigación del NSTAC para este estudio se centró intencionadamente en disciplinas distintas de la seguridad cibernética, en las que la nación, y en algunos casos el mundo, organizó actividades contra la realización de un resultado muy ambicioso. En el examen de estos esfuerzos históricos "a la luna", surgió un consenso común: Los esfuerzos de tipo lunar tienen un tiempo y un lugar distintos en la historia. Requieren una convergencia singular de fuerzas políticas, sociales, tecnológicas y de otra índole para crear el entorno propicio necesario para el éxito. [2] En última instancia, estas fuerzas se unen de forma que conducen a un consenso social en torno a dos amplios principios: 1) el desafío es de tal importancia que el fracaso no es un resultado aceptable; y 2) la creencia de que el fracaso es una fatalidad en la trayectoria actual, en ausencia de un enfoque fundamentalmente nuevo. Estos principios se aplican directa y completamente al entorno actual y futuro de la ciberseguridad.

Pero queda mucho por hacer para fomentar un entendimiento nacional compartido sobre la naturaleza y la gravedad del problema de la seguridad cibernética. Esto comienza por articular una respuesta clara y convincente a la pregunta "¿Por qué?" para justificar las importantes inversiones nacionales, los reajustes de prioridades e incluso los sacrificios personales que se necesitarán para lograr un progreso real y duradero frente a este desafío particularmente complejo. Ayudar a catalizar un plan de acción nacional que reencuadre y eleve la ciberseguridad como un desafío económico y de seguridad nacional casi singular es uno de los objetivos fundamentales de este informe.

Como nación, los Estados Unidos han fracasado fundamentalmente en articular el desafío de la seguridad cibernética de manera que incentive y asegure este nivel de acción colectiva. Debido a la complejidad de la ciberseguridad, la nación ha compartimentado con demasiada frecuencia todo el alcance del desafío y lo ha caracterizado en términos predominantemente técnicos. Este enfoque ha excluido a menudo a los principales interesados del debate, dejándolos desinformados y creyendo que no tienen ninguna responsabilidad o capacidad para ayudar a hacer frente al desafío. El Gobierno de los Estados Unidos debe enmarcar el reto de la ciberseguridad de manera más amplia, dejando claro que los factores políticos, educativos y de comportamiento humano son tan importantes como la innovación tecnológica para lograr una solución a largo plazo y que debe recurrirse a una gama más amplia de expertos.

La ciberseguridad como desafío nacional también tiene una respuesta clara y convincente a la pregunta "¿Por qué ahora?". El pueblo americano parece haber aceptado las violaciones de datos que comprometen su información personal como el precio de la conveniencia de la tecnología. Sin embargo, no es probable que toleren futuros ataques cibernéticos con un impacto directo y físico en sus vidas. En un entorno digital en el que la información existe cada vez más sólo como bits y bytes, hay una línea cada vez más estrecha que separa una sociedad digital que funciona sin problemas y que está construida sobre una base digital de confianza, y la ruptura caótica de la sociedad que resultaría de la erosión de esa confianza.

En la trayectoria actual, es muy probable que en los próximos 10 años, los Estados Unidos experimenten ataques cibernéticos más severos y físicamente destructivos que los experimentados hasta la fecha. Prevenirlos requerirá un enfoque proactivo, estratégico y sistemático de defensa que

[2] Lisa Goldman y Kate Purmal, "How to Launch a Successful Moonshot", (Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, February 20, 2018).

galvaniza la acción colectiva del pueblo americano. Este enfoque debe comenzar con una declaración de los dirigentes nacionales, apoyada por los más altos niveles del Gobierno, la industria y el mundo académico de los Estados Unidos, que enmarque el desafío de la seguridad cibernética como un riesgo que ya no es aceptable, sino una amenaza existencial para el modo de vida fundamental del pueblo estadounidense.

Los líderes de la nación deben articular este "Por qué y por qué ahora" de una manera aspirante y optimista. Si bien es importante ser franco sobre las consecuencias negativas de la inacción, los dirigentes nacionales también deben propugnar los efectos positivos y en cascada de una acción centrada y acelerada de toda la nación hacia una Internet fundamentalmente segura. Estos efectos positivos y en cascada podrían ser similares a los resultados de la movilización nacional en torno al programa espacial. Durante el disparo original a la luna, las inversiones masivas en investigación y desarrollo (I+D) distribuidas por el Gobierno de los Estados Unidos, la industria privada y el sistema académico dieron lugar a espectaculares avances de ingeniería e innovaciones inesperadas en la medicina, la ciencia de los materiales y las tecnologías del GPS que constituyeron los cimientos del liderazgo tecnológico mundial de los Estados Unidos en los decenios siguientes.

Los Estados Unidos poseen gran parte de la base tecnológica en materia de seguridad cibernética para hacer de esta actividad algo más que un ejercicio académico. Los avances tecnológicos recientes y a corto plazo (explorados en profundidad en el *Informe de la* NSTAC *al Presidente sobre la visión estratégica de las tecnologías emergentes3)* en áreas como la informática cuántica, la inteligencia artificial y el aprendizaje automático, la informática en nube y las comunicaciones 5G crean el potencial para unas defensas de la ciberseguridad más simplificadas y automatizadas, trasladando más influencia y el equilibrio general de poder a los defensores de la ciberseguridad.

El gobierno y la industria deben considerar estas cuestiones tecnológicas y las cuestiones interdependientes de política, proceso y comportamiento, de modo que puedan evaluar, priorizar e incentivar eficazmente la acción hacia aquellas innovaciones que proporcionen la mayor cantidad de apalancamiento, y en última instancia, de ventaja, contra los actores cibernéticos maliciosos. Esto comienza con una declaración de intención estratégica enfocada en los resultados, con aspiraciones e inspiración.

3.0 PLAN DE ACCIÓN DE LA INICIATIVA "MOONSHOT" DE SEGURIDAD CIBERNÉTICA

Los Estados Unidos se han afianzado en una trayectoria de incremento de su enfoque para abordar la seguridad cibernética. Forjar una trayectoria de progreso fundamentalmente nueva es desalentador para conceptualizar, pero la nación simplemente debe cambiar su mentalidad insostenible y costosa en torno a la seguridad cibernética. Esto exigirá el más alto nivel de liderazgo nacional para galvanizar los recursos y las energías hacia una búsqueda más audaz. Para tener éxito, la iniciativa debe convertirse en una verdadera "nación entera", impulsada por un liderazgo carismático, un plan de ejecución integral impulsado por hitos y una coalición comprometida de expertos del gobierno, la industria y el mundo académico.

En esta sección, el *Plan de Acción de la Iniciativa sobre la Seguridad Cibernética en la Luna*, se detallan las recomendaciones estratégicas relacionadas con la ejecución práctica y la puesta en marcha de la Iniciativa sobre la Seguridad Cibernética en la Luna. Detalla las medidas prácticas que el Gobierno de los Estados Unidos puede adoptar para dirigir esta

iniciativa utilizando sus autoridades y capacidades únicas para defender y organizar estratégicamente,

[3] NSTAC. *Informe de la NSTAC al Presidente sobre la Visión Estratégica de las Tecnologías Emergentes*. (Washington, DC: NSTAC, 14 de julio de 2017) Publicaciones de la NSTAC 2017, https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Emerging%20Technologies%20Strategic%20Vision.pdf.

Dirigir, dotar de recursos y potenciar las actividades de toda la nación alineadas con los objetivos definidos. El mensaje general aquí es simple: Aunque puede ser difícil de visualizar e imposible predecir todas las medidas a largo plazo necesarias para lograr un entorno de Internet fundamentalmente "seguro y protegido" en los próximos 10 años, esta Administración puede demostrar su liderazgo adoptando medidas específicas a corto plazo que produzcan beneficios inmediatos y sienten las bases de una visión a largo plazo más audaz de la ciberseguridad.

Debido a que el NSTAC está contratado para asesorar al Presidente, el resto de las recomendaciones contenidas en este informe están orientadas a las medidas específicas que el Gobierno de los Estados Unidos puede tomar para hacer avanzar esta iniciativa. El NSTAC reconoce y celebra la naturaleza interconectada de Internet a nivel mundial. Será esencial establecer una estrecha colaboración con asociaciones de ideas afines. Sin embargo, dado el alcance de la carta del NSTAC, nuestras recomendaciones se centran en las medidas que el Gobierno de los Estados Unidos puede adoptar para servir de modelo a las naciones con ideas afines. Sin embargo, estas recomendaciones no deben interpretarse como acciones que el Gobierno de los Estados Unidos debe tomar unilateralmente, sino más bien como acciones que el NSTAC recomienda que el Gobierno de los Estados Unidos tome para potenciar el ecosistema más amplio. A menudo, esto requerirá una consulta estrecha y directa con los interesados no gubernamentales durante el proceso de desarrollo de políticas e iniciativas. Por consiguiente, en muchas recomendaciones de esta sección se hace referencia directa a que el Gobierno de los Estados Unidos ejerza su capacidad de convocatoria y movilización para dirigir este proceso de colaboración.

Iniciativa de seguridad cibernética Moonshot
Acciones recomendadas: Línea de tiempo

- Anunciar la Iniciativa de Seguridad Cibernética de la Luna/Declaración de aspiraciones (*Sección 3.1*) en el lanzamiento
- Establecer el Consejo de Seguridad Cibernética de la Luna (*Sección 3.2.1*) En el lanzamiento
- Establecer el componente no gubernamental del Consejo (*Sección 3.2.2*) . Lanzamiento + 60 días
- Definir el marco estratégico y las prioridades nacionales de I+D para la ciberseguridad (*Sección 3.4) Lanzamiento* + 120 días
- Lanzar el proceso de múltiples partes interesadas para definir los grandes desafíos (*Sección 3.5*) Lanzar +180 días
- Lanzamiento del primer Gran Reto de Ciberseguridad (*Sección 3.5*) Lanzamiento +1 año

3.1 Entregar la declaración de aspiraciones

Recomendación clave: El Presidente o el Vicepresidente deberían presentar y defender estratégicamente una Iniciativa de Seguridad Cibernética para señalar claramente que abordar de forma duradera los problemas de seguridad cibernética de la nación es un imperativo estratégico singular. Esta proclamación debería hacerse en un foro de importancia histórica, como el Estado de la Unión o un discurso conjunto especial ante el Congreso, para hacer hincapié en esta prioridad nacional.

Al revisar los mensajes históricos sobre iniciativas a gran escala, incluido el discurso original del Presidente Kennedy "moonshot", la NSTAC identificó varias características comunes que deben estar arraigadas en una proclamación de seguridad cibernética a nivel presidencial o vicepresidencial. Entre las principales características se incluyen:

- **Un objetivo claro y convincente:** La declaración presentaba un objetivo sucinto, basado en los resultados, articulado de forma que se redujera la complejidad a algo que se pudiera entender ampliamente en toda la sociedad.

- **Un tono de aspiración:** La declaración enmarcó el reto y su solución esperada en términos optimistas que promovían los objetivos nacionales, en lugar de "vender el miedo" o las consecuencias negativas de la inacción.

- **Una línea de tiempo comprimida:** La declaración presentaba una línea de tiempo claramente articulada y establecida, subrayando la urgencia de la resolución.

- **Un enfoque audaz y no prescriptivo:** La declaración fue intencionalmente audaz por naturaleza para generar escepticismo y un diálogo productivo sobre su viabilidad. [4]

 Recomendación clave: Con estas características en mente, el NSTAC recomienda que el Presidente o el Vicepresidente entregue una declaración de intenciones aspirante a: *"Hacer que Internet sea segura para el funcionamiento del gobierno y los servicios críticos para el pueblo americano para el año 2028".*

El NSTAC consideró que esta declaración de aspiraciones era efectiva en el sentido de que se consideraba específica en su intención pero flexible en su interpretación. El término "seguro" fue elegido específicamente porque se determinó que las concepciones sociales de seguridad eran más universales, instintivas y
identificables, especialmente cuando se comparan con los términos técnicos más ambiguos que se asocian comúnmente con la ciberseguridad. También se consideró que "seguro" era instructivo en el sentido de que reconocía adecuadamente que las amenazas a la seguridad cibernética trascienden ahora el ámbito digital y plantean verdaderas amenazas físicas a la seguridad pública a medida que la sociedad se adentra cada vez más en un mundo de automóviles conectados y sistemas de infraestructura crítica dependientes de Internet.

También se determinó que el término "seguro" conllevaba un grado productivo de ambigüedad, fundamental para catalizar una conversación nacional más sólida. Por ejemplo, para lograr una Internet "segura", ¿qué tecnologías básicas debe priorizar la nación para la inversión en I+D a largo plazo? ¿Cómo deben reformar los Estados Unidos su sistema educativo para contar con expertos en seguridad cibernética bien preparados e incentivar mejores prácticas de seguridad cibernética entre los ciudadanos? ¿Cómo deben adaptarse las políticas de la cadena de suministro de la tecnología de la información para garantizar más fundamentalmente la seguridad?

El NSTAC no afirma tener todas las respuestas a estas difíciles cuestiones, muchas de las cuales serán compensaciones de gestión de riesgos y no de naturaleza binaria. Con sus conclusiones, el NSTAC espera catalizar un diálogo nacional más amplio que abarque estas conversaciones complejas y, a veces, difíciles, porque son desafíos que simplemente deben superarse para el futuro de la nación. La sección 3.4, *Definir el marco estratégico y los pilares,* explora más a fondo este tipo de cuestiones.
Tal vez incluso más crítico que la sustancia de la declaración de aspiraciones, es quién entrega el primer mensaje y dónde lo entrega el individuo. Este individuo debe ser un fuerte y

[4] Lisa Goldman y Kate Purmal *El efecto de la luna: Interrumpiendo los negocios como de costumbre* (San Carlos, CA: Wynnefield Business Press, 2016).

líder carismático, alguien visto con legitimidad a través de múltiples conjuntos de interesados y motivado por el interés nacional más amplio. El individuo debe articular la visión para hacer hincapié en el compromiso de continuidad y en la inversión sostenida en la Iniciativa Moonshot de Ciberseguridad a largo plazo, lo que es imposible para las transiciones de la Administración y el partidismo político. Esto requerirá un nivel de aspiración y unidad de esfuerzo entre los poderes Ejecutivo y Legislativo que no se ha visto en algún tiempo.

La evaluación del NSTAC es que sólo un nivel de énfasis presidencial o vicepresidencial puede generar la movilización nacional apropiada en torno a este desafío con una urgencia similar a la de la guerra. Cuando el Presidente o el Vicepresidente articula por primera vez la iniciativa, debe hacerlo en estrecha coordinación con los funcionarios pertinentes del Gabinete, los dirigentes del Congreso, los jefes ejecutivos y los dirigentes académicos para demostrar una unidad de esfuerzo real y simbólica que se extienda a los elementos de la sociedad mucho más allá de la comunidad tradicional de la ciberseguridad. El lugar y el foro de entrega también deben ser de elevada estatura histórica; el Capitolio de los Estados Unidos para un discurso sobre el Estado de la Unión o un discurso especial conjunto ante el Congreso son ejemplos representativos apropiados que transmitirían la importancia estratégica e histórica de esta iniciativa nacional.

3.2 Establecer la gobernanza para el enfoque de toda la nación

Sin embargo, la mera entrega de una declaración de intenciones no es suficiente. La declaración debe estar profundamente arraigada en un marco estratégico claro y en principios compartidos. Debe estar respaldada por una estructura de gobernanza clara que permita a los grupos distribuidos de interesados de todo el Gobierno, la industria privada, el mundo académico y la sociedad civil contribuir y centrar sus energías y actividades colectivas en los objetivos nacionales definidos y de orden superior de la Iniciativa sobre la Ciberseguridad Operacional.
Antes de que la iniciativa sea presentada formalmente al público por el Presidente o el Vicepresidente, la Casa Blanca debería dirigir un proceso interno para establecer una estructura de gobierno para la Iniciativa sobre la Seguridad Cibernética. En términos generales, la NSTAC define la gobernanza como la forma en que la Iniciativa Moonshot sobre Seguridad Cibernética organiza a los participantes, autoriza a las autoridades encargadas de la adopción de decisiones, establece objetivos e impone medidas de rendición de cuentas para garantizar el progreso. Una evaluación sólida y exhaustiva de los modelos de gobernanza y organización apropiados será fundamental para la viabilidad y eficacia a largo plazo de una Iniciativa Nacional de Seguridad Cibernética distribuida.

Encontrar la llave: La Iniciativa sobre la seguridad cibernética en la luna sólo tendrá éxito mediante una unidad de esfuerzo que aproveche tanto las autoridades y capacidades únicas de todo el Gobierno como los esfuerzos armonizados de toda la industria y el mundo académico.

La ciberseguridad es un desafío inherentemente distribuido, con autoridades, funciones y responsabilidades únicas que se comparten en todo el ecosistema público, privado y académico. Todas estas capacidades deben aprovecharse eficazmente en un modelo de seguridad colectiva para hacer
un progreso significativo. La aplicación y el éxito de la Iniciativa sobre la seguridad cibernética dependerá de un sistema muy distribuido de grupos de interesados que estén efectivamente facultados, dotados de recursos y movilizados.

Sobre la base de una recopilación de las conclusiones de múltiples reuniones informativas, el Comité Nacional de Ciencia y Tecnología desarrolló el gráfico que figura a continuación para visualizar conceptualmente la forma en que se comparte la comprensión de las funciones y responsabilidades distribuidas,

y la visión estratégica pueden ayudar a centrar -no a limitar o a sofocar- la innovación dirigida hacia áreas definidas que pueden conducir a una Internet más fundamentalmente segura y protegida. Desde el punto de vista conceptual, esto incluye la presión descendente de los niveles más altos del Gobierno de los Estados Unidos para definir la intención estratégica, y la presión ascendente de los motores operativos del sector privado y el mundo académico que están definiendo activamente las prioridades de innovación y liderando el progreso.

Figura 1: Modelo conceptual *de enfoque de toda la nación hacia los objetivos definidos de la Iniciativa de Seguridad Cibernética de la Luna.*

3.2.1 Todo el Gobierno

Recomendación clave: Dentro del Gobierno de los Estados Unidos, la Casa Blanca debería establecer un Consejo de Seguridad Cibernética de la Luna ("Consejo") para dirigir y supervisar estratégicamente la iniciativa. El Consejo se encargará de: establecer la intención estratégica, aumentar la visibilidad nacional, abogar por una financiación sostenida, desarrollar en colaboración estrategias a nivel nacional, convocar a las partes interesadas y crear políticas y procesos que faculten e incentiven a las entidades no gubernamentales para impulsar la innovación acelerada en los ámbitos definidos de la ciberseguridad que permitan la captura lunar.

El Consejo debe estar presidido oficialmente por el Presidente o el Vicepresidente y compuesto por funcionarios de nivel de gabinete de los departamentos y organismos pertinentes. Deberían crearse nuevas oficinas dentro de los departamentos y organismos existentes con la responsabilidad y la autoridad de aplicar y ejecutar las directrices de política interinstitucional del Consejo. Esto debe incluir el departamento
entidades de nivel superior con responsabilidad y autoridad designadas para dirigir el sector privado y la participación académica en las Iniciativas de Seguridad Cibernética de la Luna, como se indica en las recomendaciones del informe. Basándose en la capacidad demostrada y la autoridad del Congreso para dirigir la colaboración con la comunidad de infraestructuras críticas, el NSTAC recomienda que se otorgue al Departamento de Seguridad Nacional (DHS) la responsabilidad principal de este tipo de participación de los interesados.

Además, el Consejo debería contar con mecanismos oficiales para designar a las entidades no gubernamentales que contribuirán directamente al proceso de elaboración de estrategias y políticas de la Iniciativa en el marco de la estructura oficial del Consejo. El Consejo debería tener un componente no gubernamental oficial, integrado por representantes de entidades fundamentales de todo el sector privado y el mundo académico. El Presidente debería determinar la estructura y las autoridades que rigen la participación de las entidades no gubernamentales y el nivel de autoridad que tienen esos representantes con respecto a la adopción de decisiones generales del Consejo. Sin embargo, el Comité Nacional de Ciencia y Tecnología cree firmemente que las responsabilidades y las autoridades de los participantes no gubernamentales dentro de la estructura de dirección del Consejo deben superar las responsabilidades que tradicionalmente se otorgan a los participantes no gubernamentales en los órganos consultivos gubernamentales.

Modelo ilustrativo: Consejo Nacional del Espacio de todo el Gobierno

En junio de 2017, el Presidente Trump firmó la Orden Ejecutiva 13803, Reviviendo *el Espacio Nacional* Council„, que restablece el Consejo Nacional del Espacio como un foro de múltiples interesados dirigido por el Gobierno de los Estados Unidos para coordinar el desarrollo y la aplicación de las políticas espaciales nacionales. El Consejo Nacional del Espacio constituye un modelo de gobernanza útil, con muchos atributos organizativos que el NSTAC recomienda que el Consejo de Seguridad Cibernética en la Luna debe encarnar, entre otros:

- Presidido por el Vicepresidente con representantes de nivel de gabinete que forman el Consejo.
- Entidades no gubernamentales que participan oficialmente en el proceso de adopción de decisiones por conducto del Grupo Consultivo de Usuarios del Consejo Nacional del Espacio, integrado por expertos de alto nivel de la industria privada y el mundo académico.
- Oficinas correspondientes a nivel de departamento/agencia con responsabilidad en la implementación de las políticas del Consejo Nacional del Espacio (incluyendo el Departamento de Defensa, el Departamento de Comercio y la NASA)
- Capacidad de elaborar y emitir eficazmente políticas del Poder Ejecutivo destinadas a reducir los obstáculos y potenciar el ecosistema nacional más amplio de la industria espacial. El Consejo Nacional del Espacio emitió tres directivas de política espacial nacional en su primer año.

Un Director Ejecutivo nombrado por el Presidente debe dirigir operacionalmente la iniciativa y ser responsable y estar facultado para mantener la visibilidad de todas las actividades nacionales de la Iniciativa sobre la seguridad cibernética en la luna. El Director Ejecutivo debe ser responsable de:

- Actividades de elevación determinadas para proporcionar la mayor influencia estratégica hacia el resultado de un entorno de Internet seguro;
- Comunicar los objetivos estratégicos a largo plazo de la iniciativa, desglosar el esfuerzo en sus componentes básicos, comunicar a las partes interesadas cómo encaja cada componente en la iniciativa general y dirigir su aplicación;
- Reconocer y coordinar el valor que cada grupo de interesados puede aportar al objetivo general y la forma en que los grupos pueden crear sinergias para optimizar aún más el valor; y

- Identificar a las partes interesadas y formular recomendaciones sobre la forma de incentivarlas para que actúen en apoyo de los objetivos compartidos de la Iniciativa sobre Seguridad Cibernética.

3.2.2 Toda la industria y la academia

La función de liderazgo del sector privado y de los círculos académicos en la Iniciativa sobre la Seguridad Cibernética no puede limitarse a las personas nombradas oficialmente para prestar servicios en el Consejo oficial
construir. Las entidades gubernamentales no pueden únicamente iniciar, gestionar o mantener la Iniciativa de Seguridad Cibernética en la Luna. La estructura de la iniciativa debe reflejar la naturaleza altamente distribuida de Internet y generar activamente el compromiso entusiasta y la participación sostenida en el Consejo de un grupo diverso de interesados con funciones, responsabilidades y autoridades complementarias en materia de seguridad cibernética.

Al hacerlo, la gobernanza de la Iniciativa Moonshot de Ciberseguridad debe reconocer que el centro de gravedad de la innovación en este país ha evolucionado desde una financiación predominantemente del Gobierno de los Estados Unidos a una I+D financiada por el sector privado. En el tiro a la luna original, el Presidente Kennedy presentó su aspiración como un mandato nacional, invocando la batalla entre la libertad y la tiranía y, al hacerlo, consiguió una notable participación de contratistas y empresas privadas. La Iniciativa sobre la seguridad cibernética del tiro lunar debe depender aún más de diversos grupos de interesados del sector privado y del mundo académico.

Recomendación clave: La Iniciativa Moonshot de Ciberseguridad debe generar un enfoque de toda la nación, incluido un modelo de gobernanza cooperativa que sirva de puente entre el gobierno, la industria y el mundo académico para alinear sus capacidades y actividades inherentes a la realización de los objetivos de seguridad de Internet. Esto debería incluir una estructura empresarial de tipo consorcial que facilite la cooperación, comparta recursos y recompensas y trabaje en estrecha colaboración con los asociados del gobierno y los círculos académicos para lograr objetivos comunes.

El liderazgo de la Iniciativa de Seguridad Cibernética Moonshot surgirá, por necesidad, en muchos foros distribuidos. Si se galvaniza efectivamente a nivel presidencial o vicepresidencial, un estado ideal sería la puesta en marcha voluntaria de una miríada de consorcios independientes sin fines de lucro, asociaciones educativas y otros esfuerzos conjuntos para ejecutarlos en función de los objetivos definidos de la Iniciativa. La función del Gobierno de los Estados Unidos, a través del Consejo de Seguridad Cibernética para la Captura de Imágenes Lunares, consistiría en incentivar, dar a conocer o incluso financiar de forma selectiva los logros de estas entidades independientes si están en consonancia con los objetivos estratégicos de la Iniciativa para la Captura de Imágenes Lunares de Seguridad Cibernética.

Varios ejemplos históricos ilustran este modelo. Por ejemplo, a finales del decenio de 1990, el Gobierno de los Estados Unidos -a través de la Casa Blanca, el Instituto Nacional de Salud y el Congreso- proporcionó una importante financiación y defendió estratégicamente grandes porciones del Proyecto del Genoma Humano. Sin embargo, el logro final del proyecto fue el producto de actividades en gran medida independientes de entidades como la Celera Corporation y más de 20 universidades y entidades de investigación de todo el mundo que formaban parte del Consorcio Internacional de Secuenciación del Genoma Humano. [5]

En los decenios de 1980 y 1990 se pusieron en marcha varias iniciativas de múltiples interesados para defender la ventaja tecnológica de los Estados Unidos frente a las empresas extranjeras fuertemente subvencionadas por su gobiernos. El resultado fue la creación de consorcios empresariales como el Consorcio de Tecnología de Fabricación de Semiconductores (SEMATECH)[6] y la Corporación de Microelectrónica y Tecnología Informática (MCC). Estos consorcios eran corporaciones sin fines de lucro, de propiedad privada y constituidas por el Congreso, diseñadas específicamente para ayudar a la nación en áreas específicas de investigación y desarrollo comercial. En última instancia, más de 100 empresas trabajaron juntas para resolver los problemas tecnológicos de gran escala de la época, lo que dio lugar a importantes avances en esferas como los microchips y la infraestructura de la Internet.

5 "La finalización del Proyecto del Genoma Humano: Frequently Asked Questions", 30 de octubre de 2010, Instituto Nacional de Investigación del Genoma Humano, https://www.genome.gov/11006943/.

Modelo ilustrativo: Toda la industria/academia
La Corporación de Microelectrónica y Tecnología Informática

Ante la pérdida de la superioridad tecnológica de los Estados Unidos frente a las empresas japonesas debido a su mayor nivel de asistencia gubernamental, en 1982 se fundó la Corporación de Microelectrónica y Tecnología Informática (MCC). Patrocinada por la Administración Reagan, diseñada por antiguos miembros de la Comunidad de Inteligencia de los Estados Unidos, promulgada por el Congreso, y dirigida por recientes luminarias del Gobierno, la MCC reclutó a los principales fabricantes de computadoras y semiconductores, representantes de escuelas tecnológicas de élite y grupos afines para fomentar el crecimiento tecnológico.

En virtud de la *Ley Nacional de Investigación Cooperativa de 1984*, la MCC fue vital para el desarrollo de las tecnologías de la IA, las tácticas de ingeniería inversa y la creación de funciones fundamentales de búsqueda en Internet. Fue una de las primeras empresas en registrar una dirección de correo electrónico ".com". La MCC reunió a organizaciones dispares para compartir el escaso personal de investigación y los fondos de inversión, colaborar en objetivos comunes y desarrollar soluciones para beneficiar a toda la nación.

* Fuente: La Corporación de Microelectrónica y Tecnología Informática[7]

3.3 Otras consideraciones clave de la Iniciativa sobre Seguridad Cibernética en la Luna

La puesta en marcha de una iniciativa oficial de seguridad cibernética requiere decisiones sobre complejas consideraciones relacionadas con la gobernanza, la política, el presupuesto y muchos otros factores para que el esfuerzo sea inclusivo, duradero y viable. Esta sección se centra en el esbozo de algunas consideraciones iniciales, así como en recomendaciones específicas para fundamentar las decisiones organizativas clave que el Director Ejecutivo debe tomar antes de la puesta en marcha de la Iniciativa sobre Seguridad Cibernética.

3.3.1 Consideraciones presupuestarias

La historia ofrece innumerables ejemplos de comisiones y comités asesores que *asesoraban* al Presidente sobre la asignación de recursos pero no controlaban ningún recurso presupuestario. En este caso, es fundamental que el Director Ejecutivo desempeñe un papel oficial en la planificación y ejecución del presupuesto en apoyo del proceso y las recomendaciones de la Iniciativa sobre la seguridad cibernética, incluidas las actividades relativas a las entidades no gubernamentales. El Presidente y el Director Ejecutivo deben articular las necesidades de recursos del presupuesto federal, hacer coincidir los recursos con los objetivos específicos de la Iniciativa sobre la seguridad cibernética y garantizar que los resultados justifiquen las inversiones. El nivel de financiación e inversión del Gobierno de los Estados Unidos en materia de seguridad cibernética debe superar los niveles actuales en órdenes de magnitud y debe mantenerse en niveles similares a los de una guerra durante el decenio de vigencia de la iniciativa.

6 Robert Hof, "Lessons from Sematech", *MIT Technology Review*, 25 de julio de 2011, https://www.technologyreview.com/s/424786/lessons-from-sematech/.

7 David V. Gibson y Everett M. Rogers, *R&D Collaborations on Trial (*Boston: Harvard Business School Press, 1994), , Introducción, 15.

Recommendación clave: El Director Ejecutivo de la Iniciativa sobre la seguridad cibernética en la luna debería desempeñar un papel importante en la planificación, formulación y ejecución del presupuesto. El Presidente debería considerar la posibilidad de designar al Director Ejecutivo como codirector del Director de la Oficina de Gestión y Presupuesto en la elaboración del proyecto de presupuesto anual de la Administración. El Presidente también debe considerar la posibilidad de exigir al Director Ejecutivo que certifique que el presupuesto anual apoya plenamente los objetivos de la Iniciativa sobre la seguridad cibernética en la Luna. Por último, el Director Ejecutivo debe tener una línea de comunicación regular y directa con los Comités de Apropiación y los comités de autorización pertinentes del Senado y la Cámara de Representantes de los Estados Unidos

3.3.2 Medir el éxito, definir los hitos del progreso y crear un impulso

Encontrar la llave: El éxito general de la Iniciativa Moonshot de Ciberseguridad dependerá de la capacidad del Consejo para articular claramente el objetivo final estratégico, identificar los hitos de progreso significativos y desarrollar métricas para demostrar el éxito. La forma en que el Gobierno articule y mida el éxito de la Iniciativa Moonshot de Seguridad Cibernética es fundamental para su eventual impacto y la forma en que los estadounidenses recuerden y sientan la Iniciativa.

Al igual que en el disparo original a la luna espacial, el Gobierno debe identificar hitos concretos que el público pueda comprender fácilmente, aunque los detalles subyacentes sean complejos. El discurso del presidente Kennedy, transmitido públicamente en mayo de 1961, implícitamente estableció un camino firme y visible hacia adelante: El vuelo suborbital, los vuelos multiorbitales del programa Mercurio, las maniobras de atraque de ingeniería y las actividades extravagantes durante el programa Géminis, el desarrollo de la cápsula Apolo para tres personas, los vuelos orbitales tripulados más largos, los vuelos lunares no tripulados y, por último, el alunizaje de julio de 1969.

Debajo de estos importantes eventos transmitidos públicamente, los ingenieros lograron un flujo constante de triunfos en el desarrollo: mayores impulsores, más potencia, desarrollo de nuevos combustibles, mayores
fiabilidad, y mejores sistemas de nutrición y eliminación de desechos. Del mismo modo, la comunicación de los progresos de la Iniciativa de Seguridad Cibernética Moonshot es esencial para mantener al público centrado en el esfuerzo y servir como recordatorio intermitente, si no continuo, de su importancia nacional.

La dificultad y complejidad del objetivo general y la intensidad y el ritmo de la acción exigen que el Gobierno observe, mida y, en cierta medida, haga cumplir tanto los progresos como la finalización de la Iniciativa sobre la seguridad cibernética en la Luna. El Consejo rector de la Iniciativa sobre la seguridad cibernética en la luna, en coordinación con las partes interesadas identificadas, debería encargarse de desarrollar los hitos y la métrica de la Iniciativa sobre la seguridad cibernética en la luna. Hay varios parámetros teóricos que ilustran la forma en que la Iniciativa sobre la Seguridad Cibernética en la Luna podría medir el logro de subobjetivos en un horizonte de 10 años, entre ellos:

- La seguridad cibernética ya no es la principal amenaza de la Oficina del Director de Inteligencia Nacional de Evaluación de Amenazas Mundiales;

- Demostración repetida y mensurable por parte de los operadores de infraestructuras

críticas, tanto grandes como pequeñas, de la capacidad de mantener la continuidad del servicio durante los ataques cibernéticos;

- Las medidas del Departamento de Trabajo o de las asociaciones de la industria sobre las vacantes y los déficits de la fuerza de trabajo cibernética disminuyen;

- Mejoras en las encuestas públicas sobre la percepción de seguridad y confianza en la infraestructura de Internet y las tecnologías conectadas a Internet;
- Una notable disminución del número de incidentes de seguridad cibernética material notificados a los órganos reguladores estatales y federales, incluida la Comisión de Valores y Bolsa; y

- Una disminución del tiempo para remediar las vulnerabilidades conocidas ("tiempo de parcheo") por parte de los proveedores de infraestructura crítica que deben informar sobre esos datos.

3.4 Definir el marco estratégico y los pilares

Recomendación clave: Como una de sus primeras medidas, tras un período de consultas internas y externas, el Consejo de la Iniciativa sobre la Seguridad de la Ciberdelincuencia debería articular públicamente un Marco Estratégico para proporcionar una estructura común que ayude a organizar las actividades distribuidas de la Iniciativa sobre la Seguridad de la Ciberdelincuencia en toda la nación. Como punto de partida recomendado, el
La NSTAC propone seis pilares estratégicos: *Tecnología, Comportamiento Humano, Educación, Ecosistema, Privacidad y Política*; reconociendo que para lograr una Internet más duradera y segura en los próximos 10 años se requiere un enfoque holístico y multidisciplinario.

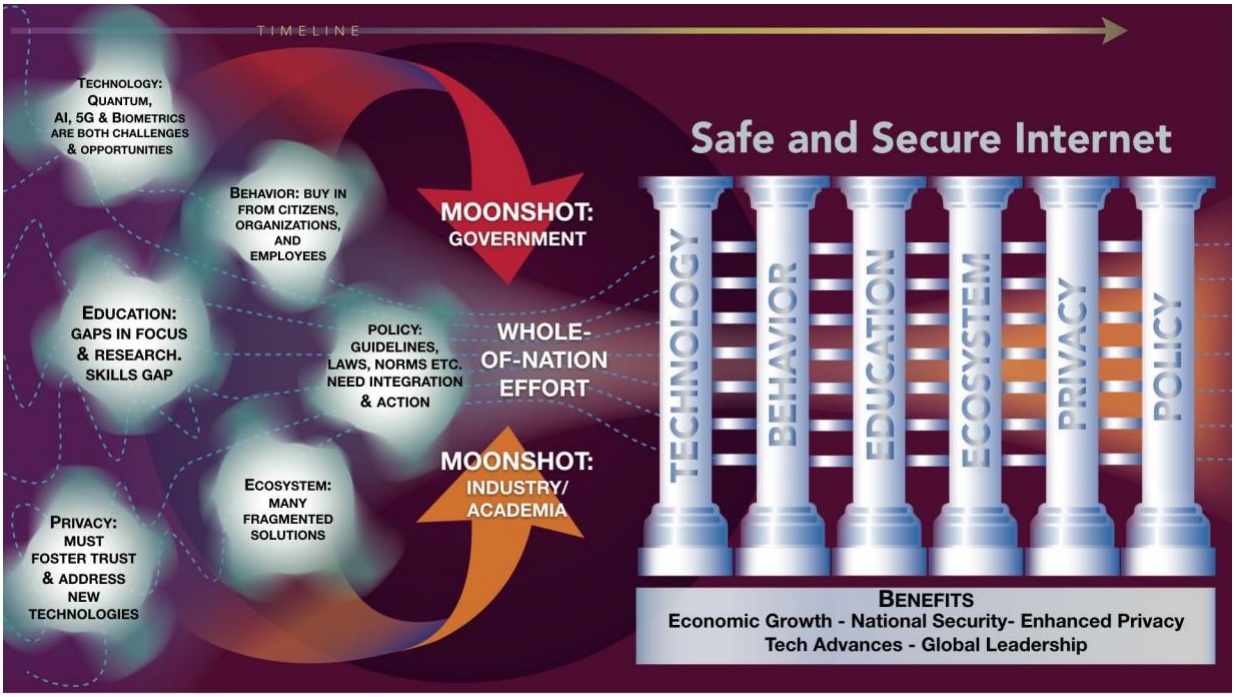

Figura 2: *La recomendación del NSTAC para los pilares estratégicos de la Iniciativa sobre la Seguridad Cibernética en la Luna, una propuesta de estructura organizativa para las amplias pero interdependientes categorías de actividades necesarias.*

El NSTAC utilizó la estructura de los Pilares Estratégicos para describir amplias categorías de actividad en las que se deben organizar acciones multidisciplinarias en toda la nación con el fin de lograr un entorno de Internet fundamentalmente seguro y protegido que garantice la confianza y la capacidad de recuperación de los gobiernos conectados digitalmente y los servicios críticos a un nivel fundamentalmente superior en relación con el statu quo. Los Pilares Estratégicos deben interpretarse como un refuerzo y una interdependencia en lugar de como una corriente de trabajo separada independiente. De hecho, algunos pilares estratégicos
Los pilares, como el pilar de la política, se centran principalmente en la habilitación directa de otros objetivos del pilar. Estas relaciones de habilitación interdependientes se exploran en la sección de dependencias entre pilares.

El NSTAC recomienda la búsqueda de un entorno de Internet seguro y protegido en el actual, abierto Internet para asegurar una interacción segura con los servicios críticos de una manera más resistente y fuerte. Las características clave para lograr este resultado incluyen:

- Los puntos finales y las medidas serán atribuibles;
- El comportamiento malicioso tendrá consecuencias;
- Las identidades se moverán más allá de las contraseñas y el PII;
- La privacidad y la confianza se mejorarán y se harán cumplir; y
- Un proceso voluntario y de participación voluntaria para obtener todo el espectro de beneficios.

El NSTAC cree que esto debe lograrse para 2028, como un esfuerzo de toda la nación, antes de que los desafíos se vuelvan más difíciles y complejos.

e

Este es el momento óptimo para que el país aproveche de manera más efectiva las capacidades tecnológicas emergentes para lograr un entorno de Internet fundamentalmente seguro, con los próximos avances en la tecnología de comunicaciones de quinta generación (5G) para una conectividad enormemente mayor y una
infraestructura defendible, avances en inteligencia artificial y aumentada para una prevención de ciberamenazas más automatizada, biometría del comportamiento que puede ofrecer una forma completamente nueva de identificar a las personas, y nuevas capacidades de encriptación cuántica que pueden resistir ataques avanzados en un futuro lejano. Mientras que todos estos avances están llegando -tanto a los Estados Unidos como a nuestros adversarios- sin un marco nacional para dirigir su investigación, desarrollo y despliegue hacia el bien común, nos arriesgamos a perder esta oportunidad generacional.

Para ser claros, el NSTAC no aboga por la balcanización de Internet, la creación de una infraestructura de Internet totalmente separada, ni prescribe ningún tipo específico de arquitectura técnica. El NSTAC aboga por una Internet fundamentalmente segura y protegida para los servicios críticos, caracterizada por el aprovechamiento de importantes avances tecnológicos, incentivos y consecuencias más ajustados para el comportamiento de los usuarios que promuevan opciones seguras, una política de ciberseguridad y reformas educativas, y una comprensión más clara de las funciones y responsabilidades del ecosistema en la creación y el funcionamiento de este entorno fundamentalmente seguro para determinados servicios críticos. Otros elementos deseados que se identificaron fueron

- Resistencia a los ataques;
- Disponibilidad garantizada de los servicios;

- Acciones totalmente atribuibles de los usuarios, para funciones de servicio críticas específicas;
- Consecuencias de las acciones maliciosas;
- Protección asegurada de la información privada;

- La confianza de los consumidores y las empresas en los sistemas;
- Canal primario de entrega de servicios vitales; y
- Accesible para todos los que lo necesiten.

Al referirse a los servicios "críticos" y "vitales" a lo largo de este informe, el NSTAC utiliza una definición informada por la política bien establecida del Gobierno de los Estados Unidos. A través de una serie de políticas que abarcan la actual y las tres anteriores Administraciones, el Gobierno de los Estados Unidos se ha unido en torno a una estrategia de gestión de riesgos de seguridad cibernética que da prioridad a la protección de la infraestructura crítica conectada a Internet. En cumplimiento de la Orden Ejecutiva 13636, *Mejora de la Infraestructura Crítica de la Ciberseguridad*, el Departamento de Seguridad Nacional y los organismos sectoriales pertinentes identifican y mantienen anualmente una lista de entidades de la "Sección 9", que se definen como "las infraestructuras *críticas en las que un incidente de ciberseguridad podría tener razonablemente como resultado efectos catastróficos a nivel regional o nacional en la salud o la seguridad pública, la seguridad económica o la seguridad nacional*"."[8] En la *Estrategia Nacional de Ciberseguridad* publicada en septiembre de 2018, la Administración definió además siete áreas prioritarias para identificar las funciones críticas y centrar las actividades de reducción de riesgos en torno a: seguridad nacional, energía y potencia, banca y finanzas, salud y seguridad, comunicaciones, tecnología de la información y transporte. Pero la concepción del NSTAC de los servicios vitales no está definida de forma puramente
base de sectores específicos. El NSTAC apoya plenamente los nuevos esfuerzos de priorización de la gestión de riesgos de la infraestructura crítica, incluidos los propugnados por el Centro Nacional de Gestión de Riesgos del DHS, que tratan de identificar y priorizar la protección de las funciones intersectoriales consideradas más críticas para una Internet segura y protegida.

Marco de alcanzabilidad

El NSTAC consideró valioso examinar y clasificar ampliamente las iniciativas sobre la base de la evaluación de sus probabilidades de éxito en el marco del plazo de 10 años de la Iniciativa sobre la seguridad cibernética en la luna. En el presente informe se han clasificado algunas iniciativas a modo de ejemplo. Estas categorías se basan en sesiones informativas directas de expertos y en investigaciones, son subjetivas y se utilizan únicamente como orientación general. Ese marco resultaría valioso para que el Consejo de la Iniciativa sobre la seguridad cibernética en la Luna lo utilizara al evaluar las iniciativas propuestas. Estas categorías incluyen

R: Se espera que se aborde sobre la base de la trayectoria actual, incluido el ritmo previsto de innovación y desarrollo tecnológico.

B: Se prevé que se abordará con una mayor inversión, un enfoque a nivel nacional y la colaboración hacia los principales avances tecnológicos y las aplicaciones innovadoras de los otros cinco pilares estratégicos.

C: No se espera que se aborde sin un Gran Reto específico que utilice diversas herramientas de incentivo para acelerar drásticamente la innovación en toda la nación.

D: No se conoce ningún enfoque razonable (Nota: El NSTAC no incluyó ninguna iniciativa "D", por lo que lo

[8] Exec. Orden. No. 13800, 82 FR 22391 (11 de mayo de 2017), https://www.dhs.gov/sites/default/files/publications/EO-13800-Section- 9-Report-Summary-20180508-508.pdf.

3.4.1 Pilar de la tecnología

Objetivo del pilar estratégico: Aprovechar estratégicamente los avances de las tecnologías emergentes para crear un entorno de Internet seguro y protegido, accesible para el ciudadano medio, las empresas y las entidades gubernamentales federales, estatales y locales, a fin de realizar transacciones de servicios críticos sin temor a comprometerse.

Introducción y antecedentes

Los Estados Unidos dependen cada vez más de la Internet y de las tecnologías conectadas digitalmente para su seguridad nacional, su seguridad pública y su prosperidad económica. La Iniciativa Moonshot de Ciberseguridad aspira a identificar, priorizar, coordinar y acelerar el desarrollo de tecnologías que conduzcan a la creación de un entorno de Internet más fiable y capaz de satisfacer las necesidades de seguridad, protección y privacidad de un entorno de infraestructura crítica moderno e hiperconectado.

Entre los ejemplos representativos de estas tecnologías figuran la inteligencia aumentada, las comunicaciones cuánticas y la criptografía de resistencia cuántica, la biometría, las comunicaciones 5G y las tecnologías de autenticación. Estas tecnologías proporcionarán la base tecnológica para lograr una Internet más segura y protegida.

El NSTAC entiende que los adversarios están persiguiendo estas mismas tecnologías hacia sus propios objetivos. Por lo tanto, la Iniciativa de Seguridad Cibernética Moonshot debe incluir fuertes implementaciones defensivas de estas nuevas tecnologías, incluyendo protegerse contra el envenenamiento de los datos de entrenamiento en inteligencia aumentada, basado en el hardware vulnerabilidades introducidas dentro de las cadenas de suministro de los ecosistemas, y computadoras cuánticas de propósito general capaces de descifrar los datos existentes.

Cambio de paradigma de identidad

Para las identidades en línea, necesitamos ir más allá de las identificaciones, las contraseñas y la información personal identificable - todo lo cual puede ser comprometido - para lograr un medio más seguro para identificar a los usuarios. El NSTAC recomienda aprovechar los avances tecnológicos en biometría del comportamiento, inteligencia aumentada, y nuevos datos de sensores disponibles con el despliegue de las comunicaciones 5G, para proporcionar un puntaje de identidad en tiempo real (de 1 por ciento a 99 por ciento) cuando se requiere una credencial de identidad. Este método proporciona transparencia para las transacciones sin fricción, una garantía de identidad mucho mayor basada en
muchos puntos de datos, y reduce significativamente el riesgo de identidad en línea.

Historia del NSTAC: Estudios previos y futuros relacionados con las tecnologías emergentes

El *Informe de* 2017 del *NSTAC al Presidente sobre la resistencia de Internet y las comunicaciones se centró* principalmente en recomendaciones a corto plazo relacionadas con las mejores prácticas y tecnologías existentes y conocidas que, si se aplicaran de manera más amplia, podrían tener un efecto tangible inmediato en la reducción de la amenaza de los ataques cibernéticos automatizados y distribuidos. En el informe también se reforzaban las conclusiones y recomendaciones del *Informe de la NSTAC al Presidente sobre la visión estratégica de las tecnologías emergentes* (2017) y se llegaba a la conclusión de que el panorama tecnológico emergente, incluidos los importantes avances en materia de inteligencia artificial, computación en nube, computación cuántica, biometría y autenticación, proporcionaba la base necesaria para lograr una transformación drástica de la seguridad cibernética. La NSTAC está elaborando actualmente un informe sobre el fomento de la capacidad de recuperación y la promoción de la innovación en el ecosistema de la tecnología de la información y las comunicaciones (TIC), en el que se examinarán las capacidades tecnológicas que son fundamentales para la seguridad nacional y la preparación para casos de emergencia de los Estados Unidos (NS/EP) y la forma en que el Gobierno puede gestionar los riesgos a corto plazo, apoyar la innovación y mejorar la diversidad de proveedores de capacidades fundamentales NS/EP. El NSTAC tiene la intención de completar este informe en la primavera de 2019.

En este informe, el papel del NSTAC no es prescribir tecnología específica relacionada con como soluciones singulares para lograr los resultados deseados de la Iniciativa sobre la seguridad cibernética en la luna. La identificación de las esferas de interés de mayor prioridad -aquellas que proporcionan la mayor cantidad de influencia estratégica para lograr un entorno de ciberseguridad seguro y protegido para los servicios críticos- tendrá que nacer de un proceso más distribuido. Sin embargo, hay amplias categorías de tecnologías que son fundamentales para la realización de un entorno de seguridad cibernética seguro en el futuro. Los siguientes son sólo ejemplos ilustrativos. A medida que se pone en marcha la Iniciativa Moonshot de seguridad cibernética, los dirigentes del Gobierno de los Estados Unidos pueden utilizar una serie de palancas de política para incentivar y habilitar al sector privado y a los círculos académicos a fin de acelerar la investigación y el desarrollo de estas tecnologías fundamentales que cambian de paradigma:

- **Comunicaciones 5G y redes de próxima generación:** Proporcionar una red de comunicaciones 5G (inalámbrica y por cable) diseñada con mayor seguridad, interconectividad, privacidad y disponibilidad. Esto proporcionará una infraestructura mucho más resistente, ampliará la conectividad segura para la Internet de las Cosas (IO), los sistemas de control industrial, los móviles, la atención de la salud, y más, con un ancho de banda dramáticamente mayor y una latencia casi en tiempo real. [9]

- **Inteligencia Artificial**: Asegurar el desarrollo del aprendizaje por máquina y la IA para aumentar (en lugar de reemplazar) a los humanos, mientras se minimizan los riesgos como el envenenamiento de los datos de los sistemas de IA. Permitir una respuesta casi autónoma a las amenazas cibernéticas a velocidad de máquina para lograr entornos informáticos autocurativos que identifiquen los fallos, eviten la explotación de esos fallos y mitiguen los efectos de los mismos.

- **Biometría del comportamiento para la identidad:** La biometría del comportamiento combinada con las capacidades de la inteligencia artificial puede reducir la dependencia de la identificación personal fácilmente comprometida, permitiendo la creación de puntuaciones de identidad que convierten las contraseñas en obsoletas y dan mayor transparencia y confianza en la identificación de los usuarios. [10]

- **Comunicaciones Cuánticas y Criptografía Cuántica Resistente:** Proporcionar una plataforma de comunicaciones y cifrado de confianza, aprovechando las tecnologías cuánticas, que sea resistente a las computadoras de propósito general cuántico (QGP), a prueba de manipulaciones y disponible para todos los servicios. Esto debe estar en funcionamiento antes de la llegada de las computadoras QGP que pueden descifrar los datos sensibles existentes.

- Resistencia **común:** Asegurar el acceso y la disponibilidad de la funcionalidad requerida de los servicios críticos mediante la automatización y simplificación del modelo de consumo de herramientas y capacidades de ciberseguridad orientadas a la prevención de amenazas. [11]

- **Microsegmentación: La implementación** de microsegmentos criptográficamente asegurados dentro de las redes distribuidas puede reducir las superficies de ataque, limitar el reconocimiento lateral y disminuir drásticamente los impactos del malware, para ayudar a apoyar tanto la resistencia operativa como las metodologías de confianza cero.

[9] William O'Hern, "AT&T NSTAC Moonshot Briefing", (Briefing al Subcomité de Ciberseguridad Lunar de la NSTAC, Arlington, VA, 18 de septiembre de 2018).

[10] John M. Poindexter, "Internet Accountability", (Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, March 22, 2018).

[11] Samuel Visner, "Cybersecurity Moonshots" (Sesión informativa para el Subcomité de Ciberseguridad Lunar de la NSTAC, Arlington, VA, 29 de marzo de 2018).

Resultados esperados

Si bien el NSTAC no trata de prescribir soluciones tecnológicas específicas, sí define los estados finales deseados como un desafío organizativo para los innovadores que aprovecharán las tecnologías previamente esbozadas. La nación debe desarrollar un modelo de mayor confianza que permita una autenticación más fuerte y otros mecanismos de seguridad y garantice una reacción oportuna a los nuevos desafíos de seguridad y privacidad. Los resultados previstos incluyen:

- Aumento de la confianza de los propietarios y operadores de infraestructuras críticas;
- Asegurar la resistencia de los sistemas de infraestructura crítica; [12]
- Asegurar la privacidad de los usuarios mediante controles de datos que refuercen la confianza a través de la transparencia, reconociendo al mismo tiempo las complejidades de la propiedad de la información compartida y la información derivada;
- Asegurar que los usuarios puedan contar con dispositivos e infraestructura que funcionen adecuadamente; y
- Asegurar que la información y los dispositivos estén razonablemente protegidos contra las amenazas en evolución.

Se necesitarán requisitos más específicos para aprovechar plenamente los posibles avances de la tecnología para proporcionar una seguridad fundamental. Estos requisitos incluyen:

- Promoviendo las puntuaciones de identidad basadas en la biometría del comportamiento (Categoría B);
- Desarrollar una red basada en la inteligencia artificial y defensas informáticas (Categoría B);
- Proporcionar la gestión de datos de IO con 5G (Categoría C);
- Fomentar la investigación y el desarrollo de la codificación resistente al quantum y la gestión de claves, que se mejoran para que coincidan con los avances de la informática cuántica (Categoría C);
- Promover las operaciones en línea centradas en el ciudadano y seguras, como la votación y la declaración de impuestos, seguidas de otras funciones de infraestructura críticas (Categoría C);
- Permitir la capacidad de realizar una o varias transacciones entre dos entidades con confidencialidad, integridad y resistencia (Categoría B);
- Gestión de las relaciones de los dispositivos físicos y virtuales conectados a Internet (Categoría B);
- Permitir la capacidad de prevenir, defenderse, operar con éxito a pesar de la incursión y

eliminar el código malicioso de forma autónoma (Categoría B); y

- Prevenir, identificar, rastrear y remediar la corrupción y el compromiso de los datos en todos los aspectos de una infraestructura crítica (Categoría C).

[12] Ibid.

Dependencias entre pilares

En esta sección se incluyen referencias a los resultados, iniciativas y actividades de otros Pilares Estratégicos que afectan a la tecnología, incluidos aquellos en los que el ritmo del desarrollo tecnológico puede acelerarse con el apoyo adecuado. Por ejemplo

- Si la educación fuera más accesible y se centrara estratégicamente en áreas críticas de la informática, se podrían acelerar los avances en las tecnologías habilitantes críticas;

- La educación de los poderes ejecutivo, legislativo y judicial del Gobierno en materia de tecnología podría ayudar a garantizar que el Gobierno proporcione el marco normativo adecuado para permitir avances rápidos y asegurar el liderazgo de los Estados Unidos en los avances tecnológicos necesarios;

- Garantizar un marco normativo y racionalizar los obstáculos reglamentarios para incentivar y recompensar la inversión y la innovación del sector privado en las tecnologías que sustentan la Iniciativa sobre la seguridad cibernética;

- Elaborar un marco en el que se incentive a los interesados en el ecosistema a trabajar juntos para cumplir los objetivos tecnológicos; y

- Desarrollar tecnologías que abstraigan la complejidad de la seguridad del usuario final y permitan a los humanos actuar con mayor seguridad, por defecto.

3.4.2 Pilar del comportamiento humano

Objetivo del **pilar estratégico:** Lograr y mantener una Internet segura y protegida requerirá cambios de comportamiento significativos en todos los componentes del ecosistema de la ciberseguridad, incluidos los usuarios, los proveedores y sus empleados. Todas las partes deberán comprender sus funciones específicas y su relación con el éxito, así como la fuerte conexión entre la ciberseguridad y nuestra seguridad nacional. El progreso hacia este resultado requerirá la adopción de medidas por varios caminos:

- Aprovechar la comunidad de innovación intrínseca de los Estados Unidos para dinamizar y ampliar el interés por la seguridad cibernética como una actividad socialmente admirable que va más allá de los tecnólogos especializados y se extiende a la corriente principal;

- Proporcionar incentivos tangibles a los usuarios de Internet para que tomen decisiones más seguras a través de toda la gama de herramientas que refuerzan la selección adecuada de seguridad y autenticación en lugar de la selección más barata; [13]

- Demostrar a los ciudadanos que las buenas prácticas de seguridad cibernética forman parte de la seguridad nacional ofreciendo mensajes claros, convincentes y mínimamente técnicos a los ciudadanos; y

- Asegurar que un conjunto adecuado de herramientas, opciones y tecnologías de seguridad sea accesible a una amplia gama del público estadounidense, independientemente de la perspicacia técnica.

[13] Grupo de Tareas Cibernético de Nueva York, *Construyendo un Ciberespacio Defensible* (Nueva York: Escuela de Asuntos Internacionales y Públicos de la Universidad de Columbia, 28 de septiembre de 2017), https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF.

Introducción y antecedentes

Los anteriores esfuerzos nacionales de seguridad cibernética no han logrado un éxito generalizado, en parte porque carecían de un componente de comportamiento humano integrado. Esos esfuerzos anteriores, si bien ofrecían importantes beneficios al país, a menudo estaban demasiado aislados o compartimentados para ofrecer el enfoque holístico que requiere el desafío de la seguridad cibernética.

De manera similar al esfuerzo original de los "disparos a la luna", el "colectivo de ciudadanos" debe ser reconocido como una parte interesada clave para la Iniciativa de Seguridad Cibernética de los "disparos a la luna". El público en general suele estar aislado de las graves amenazas a la seguridad cibernética a las que se enfrenta la nación y no considera que el problema afecte al bienestar nacional, y mucho menos a la seguridad nacional. [14,15] Aprovechar la energía y el enfoque del "colectivo de ciudadanos" será vital para afrontar y resolver no sólo los retos técnicos, sino también para navegar por el panorama político que es primordial para el éxito de la Iniciativa Moonshot sobre seguridad cibernética.

Además, esta iniciativa, al igual que el disparo a la luna original, puede impulsar innovaciones en otros ámbitos y dejar un legado duradero que va mucho más allá de un entorno fiable y resistente para los servicios críticos. La estabilidad, la seguridad y la protección de Internet es un factor clave para las innovaciones en otras industrias vitales y críticas, como la atención sanitaria, la energía y el transporte. Se ha demostrado que es imposible encontrar una salida a los desafíos que enfrentamos en Internet hoy en día: no existe una solución tecnológica para nuestros principales desafíos de seguridad cibernética. Además, no ha habido un progreso significativo hacia la toma de decisiones difíciles que resulten en un entorno más simplificado, seguro y protegido. Los cambios en el comportamiento de los ciudadanos, los desarrolladores y operadores de tecnología, los funcionarios del gobierno y los usuarios de Internet han sido demostrable y frustrantemente difíciles de alcanzar.

Resultados esperados

Las actividades de toda la nación relacionadas con el Pilar del Comportamiento Humano deben centrarse en los siguientes resultados ideales:

- **Comprometiendo la imaginación y la energía del público americano:** Una base tecnológica segura para la prestación de servicios críticos requerirá el compromiso de más que sólo proveedores de tecnología, operadores de redes y profesionales de la seguridad que tradicionalmente se han centrado en estos desafíos. Se requerirán cambios fundamentales en la forma en que funciona el entorno, la forma en que los usuarios se comprometen, la idea de la identidad en línea y las funciones de cada individuo para apoyar el logro de este ambicioso paso adelante. Estos cambios sólo pueden tener éxito si tenemos una población dedicada, informada y comprometida.

- **Dinamizar la comunidad de la innovación:** La innovación debe ser reconocida como un componente cultural clave de la vida americana. El monto de la financiación general para la investigación avanzada sigue siendo un porcentaje decreciente del producto interno bruto general, lo que hace que cada

[14] Michael Daniel, Necessary Policy Foundations for a Cyber Moonshot," (Briefing to the NSTAC Cybersecurity Moonshot

Subcommittee, Arlington, VA, March 27, 2018).

15 Dov S. Zakheim, "Structuring Government to Address the Cyber Challenge," (Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, September 27, 2018).

de investigación aplicada aún más crítica. [16] Las universidades tienen más que ofrecer en esta área ya que tradicionalmente son un participante clave en la comunidad de la innovación. El establecimiento y el cultivo de una comunidad alineada con objetivos de investigación comunes ha dado lugar a importantes hallazgos en las esferas de la física y los materiales; este modelo debe adaptarse y acelerarse en el ámbito de la ciberseguridad.

- **Haciendo que la decisión más segura sea la elección por defecto:** Todos los usuarios, incluidos los empleados, estudiantes, consumidores y ciudadanos, deben considerar la seguridad cibernética como algo importante para el bien de la sociedad y comprender su papel en la ayuda a los Estados Unidos a través de prácticas de seguridad cibernética mejoradas. Al mismo tiempo, las opciones de seguridad deben ser lo más transparentes posible para no añadir cargas significativas o requerir conocimientos técnicos avanzados o sofisticación para que los usuarios finales tomen las decisiones de seguridad correctas. Por ejemplo, los estudios han demostrado que algunos de los cambios más impactantes en apoyo de la seguridad se han producido cuando las características de seguridad se activan por defecto y no requieren ninguna acción por parte del usuario. [17, 18]

- **Los incentivos refuerzan la selección apropiada de los requisitos de seguridad y autentificación en lugar de sólo la selección más barata:** El Gobierno de los Estados Unidos, a través del DHS, el Departamento de Comercio y las agencias de sectores específicos, ha apoyado y proporcionado durante mucho tiempo recomendaciones y directrices voluntarias en el área de la promoción de resultados seguros. Un elemento necesario para el éxito de la Iniciativa Moonshot de Ciberseguridad incluirá la influencia direccional sobre los actores privados que incentiven la acción. El Gobierno puede incentivar los comportamientos a través de incentivos financieros, como directrices de adquisición centradas en los resultados, la realización de grandes desafíos o la organización de concursos con premios. [19] Al mismo tiempo, las campañas de relaciones públicas, con un fuerte alcance organizativo, pueden ayudar a los consumidores a tomar las decisiones correctas en materia de seguridad. Por último, el gobierno puede promover la seguridad estableciendo requisitos de seguridad para las interacciones entre el público y el gobierno en Internet.

A fin de convertir el compromiso en acción, se debe proporcionar a los usuarios métodos sencillos y de bajo costo para aumentar su seguridad. Estos mecanismos deben ser fácilmente comprensibles y accesibles para una amplia gama del público estadounidense. El aprovechamiento de las innovaciones en el aprendizaje automático, la autonomía y la informática establecerá y reforzará la elección de vías seguras para las transacciones críticas, así como la gestión de la hiperconectividad que 5G ayudará a establecer. [20,21]

---

16 Jeffrey Mervis, "Comprobación de datos: La participación del gobierno de EE.UU. en la financiación de la investigación básica cae por debajo del 50%". Revista *Science*, 9 de marzo de 2017, http://www.sciencemag.org/news/2017/03/data-check-us-government-share-basic-research-funding-falls- por debajo del 50.

17 Grupo de Tareas Cibernético de Nueva York, Construyendo un Ciberespacio Defensible, https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF.

18 Randy Sabett, "The Role of Incentive-Based Policies in a Whole-Of-Nation Cybersecurity Strategy", (Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, September 26, 2018).

19 Paul Afonso, "Regulación y coordinación de los servicios públicos con los organismos estatales en relación con una iniciativa de seguridad cibernética en la luna" (Sesión informativa para el Subcomité de Seguridad Cibernética en la Luna de la NSTAC, Arlington, VA, 26 de septiembre de 2018).

20 Bruce McConnell, "Make the [Global] Internet Safe and Secure . . . by 2028," (Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, August 22, 2018).

21 O'Hern, "AT&T NSTAC Moonshot Briefing".

Dependencias entre pilares

El ingenio y la voluntad del pueblo americano serán un elemento definitorio del éxito de la Iniciativa de Seguridad Cibernética Moonshot. El establecimiento, sostenimiento y aplicación de este ingenio y voluntad humana se mide a través de la atención, la acción y los recursos y se verá impactado significativamente por los otros Pilares Estratégicos. Por ejemplo, las reformas educativas, la protección de los derechos de privacidad, la evolución y adopción de la tecnología, y las políticas que incentivan los comportamientos para impulsar una mejora exponencial de la seguridad en Internet requerirán coordinación y desarrollo conjunto en todos los Pilares Estratégicos.

3.4.3 Pilar de la educación

Objetivo del pilar estratégico: La nación debe aumentar drásticamente la disponibilidad, la calidad y la diversidad de los talentos en materia de ciberseguridad para las esferas de interés estratégico de la Iniciativa Moonshot de Ciberseguridad, y al mismo tiempo educar a todos los ciudadanos en sus responsabilidades compartidas en la creación de un entorno de Internet seguro y protegido. Esto incluye una comprensión fundamental de los riesgos e incentivos positivos para cumplir sus responsabilidades de forma segura y protegida.

Introducción y antecedentes

El desarrollo y la aplicación de tecnologías habilitadoras de un entorno seguro impulsarán una mayor demanda de profesionales cualificados para desarrollar y operar su infraestructura de seguridad cibernética subyacente. Abordar esta necesidad requerirá un aumento en la amplitud y profundidad de los programas de Ciencia, Tecnología, Ingeniería y Matemáticas (STEM) del K-12 que alimentan las áreas de enfoque estratégico alineadas con la Iniciativa de Seguridad Cibernética. La nación debe desarrollar una estrategia nacional concertada para aumentar rápidamente el número de investigadores y profesionales cibernéticos cualificados. Estos profesionales de la ciberseguridad deben ser capaces de fomentar los avances tecnológicos transformadores más críticos para desarrollar y mantener el entorno seguro de Internet. Estos avances deben lograrse a tiempo para apoyar el desarrollo, el despliegue y la el cultivo de las mejores prácticas, especialmente en las áreas clave identificadas como la computación cuántica, la IA y la 5G.

Se deben exigir nuevos incentivos para aumentar los mecanismos normales de oferta y demanda del mercado a fin de retener a los graduados de STEM en el mundo académico y en las funciones de seguridad nacional e infraestructura del gobierno. Esos incentivos pueden ayudar a atraer y retener a personas en la fuerza de trabajo de la seguridad cibernética del Gobierno que, de otro modo, podrían entrar en el sector privado. [22] Para ello se necesitarán fondos adicionales y colaboraciones innovadoras entre el gobierno, las organizaciones sin fines de lucro y la industria privada para desarrollar nuevas iniciativas de educación en materia de ciberseguridad. [23]

Una sólida educación en materia de STEM a todas las edades también será un elemento fundamental para la educación en materia de seguridad cibernética y las iniciativas de desarrollo de la fuerza de trabajo. La tecnología innovadora basada en la nube debe ser aprovechada para mejorar la velocidad y la calidad de la educación STEM. Por ejemplo, la IA, los grandes datos y la realidad aumentada ofrecen el potencial para ayudar a abordar los obstáculos en la educación primaria y secundaria y en la educación superior. Estos programas pueden aprovechar la gamificación, los medios de comunicación y las plataformas distribuidas para el aprendizaje.

Esfuerzos

[22] Richard Heimann, "Estado de la Disciplina: Inteligencia Artificial", (Sesión informativa para el Subcomité de Seguridad Cibernética de la NSTAC, Arlington, VA, 6 de septiembre de 2018).

[23] Maughan, "Sesión informativa para el Subcomité de Seguridad Cibernética de la NSTAC".

también se debe hacer para retener a los mejores y más brillantes graduados de los colegios y universidades de EE.UU., muchos de los cuales no son residentes de EE.UU., para permanecer en los EE.UU. y unirse a la fuerza de trabajo de EE.UU. Además, los miembros del ecosistema deben considerar un sistema de rotación o intercambio, en el que los empleados del Gobierno se asignen, de forma voluntaria, a proveedores comerciales clave y viceversa. [24] Aunque se están llevando a cabo varias iniciativas de educación en materia de ciberseguridad y desarrollo de la fuerza laboral, la nación se enfrenta a una escasez de mano de obra crítica y bien documentada. [25,26] Los estudios varían pero indican que para 2021 habrá al menos 350.000 puestos de seguridad cibernética sin cubrir en los Estados Unidos y hasta 3,5 millones de vacantes relacionadas con la seguridad cibernética en todo el mundo. [27,28] Este enorme déficit sigue persistiendo en un entorno en el que los salarios de la seguridad cibernética triplican en promedio los ingresos medios nacionales, y en el que la industria privada paga mucho más que las compensaciones gubernamentales. [29]

Por último, operar en un entorno de ciberseguridad fundamentalmente seguro puede implicar cierto nivel de inconvenientes personales: un cambio de paradigma para el usuario medio. Los usuarios finales suelen ser el eslabón más débil de la seguridad de un sistema, ya sea como resultado de una intención maliciosa, de la falta de formación o de la negligencia. [30] El gobierno, el mundo académico y el sector privado deben comprometerse a ayudar a educar sobre esta transformación cultural. [31]

Resultados esperados

Las actividades de toda la nación relacionadas con el pilar de la educación deberían centrarse en los siguientes resultados ideales:

- El énfasis nacional en los imperativos de la educación puede dividirse en dos grandes categorías: 1) para las carreras profesionales de la ciencia y la tecnología relacionadas con la ciberseguridad; y 2) para la población general de usuarios de la infraestructura de seguridad cibernética;

- Más fondos de la comunidad de investigación universitaria -tanto de investigación pura como aplicada- para crear y expandir programas de ciberseguridad alineados con el desarrollo a corto plazo de los campos habilitantes identificados en el Pilar de la Tecnología;

- Creación de estructuras basadas en consorcios para la educación, con rotación de puestos de trabajo y polinización cruzada entre el gobierno, la industria y el mundo académico; [32]

- Dramática expansión de becas, becas de investigación y subvenciones para hacer la educación STEM más accesible; pasantías, aprendizajes y colocación de posgrado para ayudar a llenar el trabajo crítico

24 Zakheim "Estructurando el gobierno para enfrentar el desafío cibernético".

25 "Meet the Millennials", 2017, Centro de Seguridad y Educación Cibernética, https://iamcybersafe.org/research_millennials/. 26 Centro de Estudios Estratégicos e Internacionales, *Hacking the Skills Shortage*, (Washington, DC: McAfee, 2016), https://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf.

27 Ibid.

28 Douglas Maughan, "Briefing to the NSTAC Cybersecurity Moonshot Subcommittee", Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, August 28, 2018.

[29] Kenneth Corbin, "Cybersecurity Pros in High Demand, Highly Paid, and Highly Selective", 8 de agosto de 2013, CIO, https://www.cio.com/article/2383451/careers-staffing/cybersecurity-pros-in-high-demand--highly-paid-and-highly-selective.html.

[30] Robert Hinden y Russell Housley, "Challenges to Deploying Security on the Internet", (Briefing to the NSTAC Cybersecurity Moonshot Subcommittee, Arlington, VA, September 25, 2018).

[31] Sabett, "El papel de las políticas basadas en incentivos en una estrategia de ciberseguridad de toda la nación".[32] *Ibídem.*

necesidades; tutoría temprana y sostenida, especialmente para las poblaciones tradicionalmente subrepresentadas en STEM;

- Evolución de los planes de estudios de educación STEM para introducir temas de informática en la educación de la primera infancia a través de la escuela secundaria (incluso mediante cursos de colocación avanzada de seguridad cibernética), de modo que la seguridad cibernética se considera una carrera profesional claramente definida y socialmente admirable;

- Para 2028, cada estudiante de K-12 debe tener una conciencia básica de las mejores prácticas de higiene cibernética y conocer los fundamentos de los sistemas de computación según lo establecido por el Instituto Nacional de Estándares y Tecnología (NIST); y

- Oportunidades de ciudadanía a través de cuotas de visado específicas e incentivos financieros para retener en la
  La fuerza de trabajo de EE.UU. canaliza el talento de seguridad cibernética nacido en el extranjero del sistema educativo de EE.UU.

Dependencias entre pilares

Los resultados de la educación tienen importantes interdependencias con otros Pilares Estratégicos. Algunos ejemplos representativos son

- Comportamiento **humano:** Se necesitarán incentivos del tipo "zanahoria" y "palo" para lograr resultados educativos clave, incluyendo campañas de concienciación pública para (1) llevar a los estudiantes a campos académicos alineados con la Iniciativa de Ciberseguridad de la Luna; y (2) mejorar significativamente los comportamientos de ciberseguridad de la población en general. [33]

- **Ecosistema:** Será necesario capacitar a un número incontable de profesionales de la seguridad cibernética de los sectores público y privado para que construyan y operen la infraestructura subyacente de un entorno de Internet fundamentalmente seguro.

- **Privacidad:** Informar a los estadounidenses sobre el papel de la privacidad de los datos, sus responsabilidades relacionadas necesarias para mantener esa privacidad, y los impactos que las políticas nacionales tienen en sus acciones es un resultado educativo esencial.

3.4.4 Pilar del Ecosistema

Meta del **pilar estratégico:** Para 2028, los Estados Unidos necesitan un ecosistema integrado de interesados voluntarios que trabajen en colaboración para diseñar, desarrollar y operar un ambiente seguro para servicios críticos y vitales. Tal ecosistema no es algo que una sola entidad, incluso el Gobierno Federal por sí solo, pueda simplemente ordenar. En cambio, requiere un conjunto de organizaciones representativas que tengan tanto un incentivo comercial como de seguridad nacional, abiertas a todas las partes en diversos niveles de confianza y que operen con un enfoque de toda la nación, que adopten una mentalidad de "seguridad en el mercado" por encima de la de "primero en el mercado".

33 Craig Fields, "Una Iniciativa Cibernética Nacional". (Sesión informativa para el Subcomité de Seguridad Cibernética de la NSTAC, Arlington, VA, 21 de agosto de 2018).

Introducción y antecedentes

Hoy en día, las empresas de tecnología ofrecen en gran parte productos y servicios competitivos disponibles comercialmente que son generalmente confiables, resistentes, accesibles y que se espera que evolucionen continuamente. Individualmente, estas entidades pueden efectuar pocos cambios, pero al trabajar como parte de un ecosistema cohesivo, el colectivo puede proporcionar las soluciones de seguridad más integradas que se requieren. Este ecosistema de seguridad cibernética incluye componentes de los gobiernos (federal, estatal y local), el mundo académico y el sector privado, con inclinaciones inherentes tanto a la competencia como a la cooperación. [34]

Los participantes en el ecosistema incluyen a todos los que proveen o utilizan la infraestructura de servicios críticos. Además de los investigadores, los fabricantes, los operadores y los usuarios, también se incluyen las cadenas de suministro de los fabricantes y los operadores. El ecosistema incluye a los actores de las entidades del sector privado, todos los niveles de gobierno, los ciudadanos, las organizaciones de normalización, las entidades extranjeras, las organizaciones sin fines de lucro, la comunidad de código abierto y otros. Los componentes físicos y lógicos del ecosistema abarcan dispositivos, componentes, redes, servicios y tecnologías aplicadas que funcionan conjuntamente para crear la Internet, sistemas de infraestructura crítica y servicios gubernamentales.

En el contexto de la Iniciativa sobre la seguridad cibernética, los servicios gubernamentales y la infraestructura crítica necesitan mayores garantías de autenticación, integridad, seguridad, privacidad, accesibilidad, resistencia y atribución. Si bien la Iniciativa Moonshot de Seguridad Cibernética encomienda al Gobierno el liderazgo estratégico definitivo, el sector privado comercializará la tecnología, así como preverá, creará y habilitará capacidades que garanticen un entorno seguro en Internet de manera permanente. Si bien la Iniciativa Moonshot de Seguridad Cibernética se propone como una iniciativa de los Estados Unidos, la
El Gobierno de los Estados Unidos debe seguir coordinando estrechamente con los aliados de "Cinco Ojos" y otras naciones de ideas afines.

El ecosistema de hoy en día ofrece productos y servicios que producen una inmensa comodidad, una mayor utilización de los recursos y un sinnúmero de otros beneficios. A través de estas soluciones hay diversos niveles de seguridad, resistencia y durabilidad en una base instalada de legado en constante expansión. El mercado estadounidense de productos de TIC lucha perpetuamente por equilibrar el coste, la facilidad de uso y las características visibles para el cliente con la seguridad (a menudo) invisible y las capacidades de resistencia. Las empresas que intentan proporcionar una seguridad superior a la media son desplazadas por aquellas que llevan los productos primero al mercado o proporcionan una funcionalidad equivalente a un coste inferior al de los productos existentes.

Las soluciones comerciales ya existentes y de amplia adopción permiten economías de escala que hacen inviable el intento de crear soluciones personalizadas más seguras. En el mejor de los casos, las empresas con marcas fuertes tratan de reducir el riesgo asignando recursos para la gestión del riesgo, la seguridad, la resistencia o la respuesta a incidentes. Las normas o tecnologías que requieren un despliegue generalizado para mejorar la seguridad pero que no están intrínsecamente entrelazadas con el valor localizado, suelen estar subempleadas. [35]

En todos los sectores, los informadores del NSTAC anticiparon una aplicación transformadora sin

precedentes de las nuevas tecnologías. Se espera que las soluciones crezcan implacablemente más integradas, interconectadas y

34 Ibid.

35 Hinden y Housely, "Desafíos al despliegue de la seguridad en Internet".

complejo. Algunos ejemplos citados por los informantes fueron las aplicaciones 5G para la infraestructura de transporte36 y la adición de recursos energéticos distribuidos37 a la red; el aumento de las amenazas a los protocolos de cifrado heredados de la informática cuántica; y la naturaleza dual de la IA, que puede utilizarse como herramienta de seguridad preventiva o como arma cibernética.

Resultados esperados

En última instancia, el Gobierno necesita comprometerse con todos los participantes en el ecosistema para dar prioridad a la reducción de los riesgos de la ciberseguridad y lograr un entorno seguro y protegido para los servicios esenciales para 2028. Hay tres resultados ideales fundamentales que el Gobierno de los Estados Unidos debe cumplir para potenciar las actividades de toda la nación relacionadas con el pilar del ecosistema:

- Dirigir y organizar el ecosistema a través de los sectores que unen a los interesados voluntarios para lograr los objetivos comunes necesarios para un entorno seguro y protegido, sobre la base de una importante mitigación de los riesgos, normas, tecnologías defensivas, infraestructura y servicios compartidos. Una organización de beneficio público, siguiendo los pasos exitosos de SEMATECH y MCC desde el decenio de 1980 (explorados en mayor profundidad en la sección 3.2.2, *Toda la industria y la academia*) es un modelo útil para este tipo de estructura de consorcios voluntarios.

- Participar en la transición entre las fases de diseño y ejecución de la habilitación de un entorno seguro y protegido, dedicado a abarcar los servicios gubernamentales y críticos, en un plazo de 10 años. Los elementos básicos de seguridad, resistencia y accesibilidad necesarios para una infraestructura de entorno seguro y protegido deben identificarse en todos los servicios gubernamentales, la infraestructura crítica y otros sectores que participen voluntariamente. Los obstáculos a la aplicación -ya sean financieros, técnicos, reglamentarios o de transparencia- deben abordarse colectivamente a través del liderazgo del Gobierno de los Estados Unidos. *38*

- Poner a disposición de otras aplicaciones y soluciones comerciales todos los elementos necesarios para prestar servicios gubernamentales y críticos de manera segura. Entre esos elementos figuran una infraestructura resistente y fundamental, servicios compartidos, autenticación de usuarios con biometría, proveedores de identidades de confianza que puedan sustituir las contraseñas tradicionales, una identidad sólida de los dispositivos y servicios, atribución, respuesta a incidentes y parches de los fabricantes, prácticas óptimas de ciberseguridad, mecanismos de recuperación a distancia, garantía de software, organizaciones de respuesta cibernética y autoridades para investigar y remediar las actividades ilegales.

Dependencias entre pilares

Por definición, el pilar del ecosistema incluirá actividades con interdependencias en todos los demás pilares, ya que representa la recopilación, la agregación, la integración y la ejecución de la Iniciativa sobre la seguridad cibernética en la luna. Este enfoque fundamental, según el cual cada pilar es vital para la finalización con éxito del proyecto, no puede ser exagerado.

36 Terry Halvorsen, "Tecnología y capacidades de la red 5G", (Sesión informativa para el Subcomité de Seguridad Cibernética de la NSTAC, Arlington, VA, 5 de septiembre de 2018).

[37] Afonso, "Regulación de servicios públicos y coordinación con los organismos estatales en relación con una iniciativa de seguridad cibernética en la luna".[38] Jennifer Gustetic, "Diseñando e implementando grandes desafíos: Learning from NASA's Experience," (Briefing to the
NSTAC Cybersecurity Moonshot Subcomité, Arlington, VA, 23 de agosto de 2018).

3.4.5 Pilar de la privacidad

Objetivo del pilar estratégico: La privacidad es un componente clave para proporcionar la confianza necesaria para proporcionar servicios críticos a la Nación. [39] Para 2028, los ciudadanos estadounidenses deben poder confiar en los sistemas de información que proporcionan servicios críticos y exigirán con certeza práctica que las actividades de la Iniciativa de Seguridad Cibernética Moonshot no creen vulnerabilidades en la privacidad, sino que mejoren la garantía de la privacidad y aseguren que los datos personales y las transacciones sean seguros, permanezcan protegidos y estén bajo su control. La privacidad es un principio básico que está fundamentalmente entrelazado con los objetivos de seguridad y protección y debe impregnar todos los aspectos de la Iniciativa Cibernética Moonshot.

Introducción y antecedentes

La privacidad en un ambiente seguro de Internet debería ser un derecho, haciendo eco de los derechos de la [4ta. Enmienda de] que los americanos estarán "seguros *en sus personas, casas, papeles y efectos, contra registros e incautaciones irrazonables". "*La definición pionera de Alan Westin de que *"la privacidad es el reclamo de los individuos, grupos o instituciones para determinar por sí mismos cuándo, cómo y hasta qué punto la información sobre ellos se comunica a los demás*", proporciona otra base fundamental. [40] El diseño y las directrices de la Iniciativa sobre la seguridad cibernética en la luna deben incorporar principios de privacidad que se extiendan a todas las interacciones dentro del entorno seguro. Un elemento fundamental del pilar de la privacidad es que los individuos, grupos e instituciones determinarán cómo y cuándo se comunicará la información personal. [41,] Por último, la arquitectura de un entorno seguro de Internet debe tener en cuenta la importante exposición de los datos personales debido al aumento de la IO y la conectividad de los sensores impulsada por la aplicación de los 5G. [42]

La privacidad en el mundo digital se ha debilitado en parte debido a los continuos compromisos de información y la proliferación de prácticas comerciales basadas en la información que, en algunos casos, no han ido acompañadas de prácticas de seguridad adecuadas. Casi todos los estadounidenses se han visto afectados por una violación de datos que afecta negativamente a su privacidad personal. En nuestro actual curso inalterado, a medida que aumenta el número de dispositivos conectados y los intercambios de datos, la probabilidad y el impacto de futuras violaciones de la privacidad aumentan exponencialmente. Dados estos desafíos, la Iniciativa Moonshot de Ciberseguridad debe establecer un nivel de confianza, transparencia y privacidad para asegurar una adopción óptima dentro de los entornos seguros de Internet.

Cuando se trata de la privacidad, es importante entender la interacción entre el anonimato y la atribución. Todos los usuarios, independientemente de su nivel de atribución o anonimato en las actividades en línea, tienen una expectativa válida de privacidad y opciones sobre cómo se utilizarán sus datos. Si bien el anonimato protege la privacidad, ello no significa que toda comunicación por Internet, incluido el acceso a una infraestructura esencial, deba ser anónima; de hecho, ese anonimato a menudo ha dado lugar a una falta de disuasión con respecto a las actividades perjudiciales. Al mismo tiempo, debe protegerse el anonimato, en particular en las zonas en que el temor o la incapacidad de ejercer los derechos humanos básicos y fundamentales están en peligro. En el actual entorno en línea hay poco temor a las consecuencias cuando se emprende una actividad maliciosa; el entorno seguro debe hacer frente a esta realidad y trabajar para

[39] Poindexter, "Responsabilidad en Internet".

[40] Westin, Alan, *Privacidad y Libertad*, Nueva York: IG Publishing, 1967.

[41] "Crítica de libros": Privacy and Freedom", 24 de noviembre de 2004, Privacilla.org, http://www.privacilla.org/fundamentals/privacyandfreedom.html.

[42] O'Hern, "AT&T NSTAC Moonshot B r i e f i n g ".

asegurar que la atribución es absoluta para servicios críticos específicos y, por lo tanto, las consecuencias para un individuo no sólo son posibles sino probables.

Resultados esperados

El pilar de la privacidad aboga por soluciones que ayuden a resolver los desafíos en muchas áreas fundamentales de la privacidad. Las áreas específicas que deben ser abordadas incluyen: atribución y responsabilidad, transparencia, identidad, encriptación, datos de sensores e inteligencia aumentada. El éxito se demostrará con transparencia y se basará en resultados objetivos y subjetivos, tales como:

- Todas las transacciones que se realicen en entornos seguros de Internet serán plenamente responsables con identidad positiva y atribución completa; [43]
- En toda la Iniciativa sobre la seguridad cibernética se ha integrado una sólida gobernanza de la privacidad, que incluye las aportaciones y la supervisión de los principales grupos de defensa de la privacidad junto con el Gobierno y las partes interesadas del sector;

- La percepción medida del público en general será que las transacciones de servicios críticos son seguras, protegidas y dignas de confianza.

La atribución y la rendición de cuentas deben poder aplicarse dentro de entornos seguros, lo cual ha sido casi imposible de lograr hoy en día. Fuera del entorno seguro, la falta de atribución y responsabilidad es un imperativo moral (por ejemplo, apoyar la libertad de expresión sin temor a represalias); sin embargo, este mismo entorno ha permitido cada vez más actividades y comportamientos que son una amenaza para nuestra sociedad. La asimetría del riesgo y la recompensa favorece al usuario malicioso.

Para asegurar la privacidad, debe haber cambios en la gestión de la identidad, la codificación, el uso de los datos de los sensores y el despliegue de la inteligencia aumentada. Por ejemplo, la identidad debe ser sensible al contexto, extrayendo los atributos necesarios para confirmar positivamente la identidad de una entidad en función de la necesidad específica de conocerla; los protocolos de cifrado deben ser resistentes al quantum; deben existir protecciones para evitar que la privacidad infrinja el uso de la inteligencia artificial; y los datos de los dispositivos y sensores de IO deben ser gestionados y protegidos. El establecimiento y el suministro de puntuaciones de identidad, en lugar de contraseñas, derivadas de
Los datos biométricos y de sensores en tiempo real devaluarán la información de identificación personal, al tiempo que aumentarán la privacidad dentro del entorno seguro y se extenderán a otros aspectos del uso de Internet.

Dependencias entre pilares

Si bien la privacidad depende de la interacción satisfactoria de los otros cinco pilares, tres de ellos tienen una codependencia especialmente fuerte: una comprensión profunda del *comportamiento humano* es fundamental para aplicar con éxito las protecciones de la privacidad, debe promulgarse una *política* que apoye e incentive las innovaciones en materia de privacidad, y la *tecnología*, especialmente con la aparición de la 5G y la maduración de la IA para aplicaciones de ciberseguridad.

[43] Poindexter, "Responsabilidad en Internet".

3.4.6 Pilar de la política

Objetivo del pilar estratégico: La nación debe hacer cambios significativos y centrados en la política, incluyendo leyes, regulaciones, normas, reglas y estándares para permitir grandes avances en los otros pilares estratégicos. Estos cambios pueden ser impulsados por incentivos, la creación de normas nacionales e internacionales, las nuevas amenazas y las nuevas tecnologías, todo ello con el objetivo común de facilitar una Internet más duradera y segura. Las políticas deberán reconocer, incentivar y recompensar a los actores de este espacio por su comportamiento positivo, así como hacer cumplir la rendición de cuentas, la atribución y la consecuencia de los comportamientos negativos. [44] Las políticas tendrán que evolucionar, según sea necesario, para que la Iniciativa de la Ciberseguridad en la Luna tenga éxito y sea consciente de la escala internacional del reto.

Introducción y antecedentes

Hoy en día, la Nación está luchando por mantenerse al día con las sofisticadas y crecientes amenazas cibernéticas, que fundamentalmente ponen en peligro el estilo de vida americano. La firme resolución de la nación de preservar y respetar la apertura de la sociedad y la libertad de todas las personas crea oportunidades para que los criminales y adversarios nos exploten y dañen a través de los ataques cibernéticos. Al igual que el reto de las fuerzas del orden de detener el terrorismo dirigido a objetivos fáciles, las políticas de Internet han dejado a los sistemas críticos vulnerables al robo de datos privados y sensibles y a una posible interrupción o destrucción. Tal vez más que cualquier otra transformación en la historia de la nación, la política de seguridad cibernética debe adaptarse para superar los desafíos actuales y futuros que plantea nuestro mundo conectado digitalmente.

Estudio de caso: Política y seguridad del automóvil

En este esfuerzo deben tenerse en cuenta las lecciones del pasado en relación con el uso de una amplia reforma de las políticas para impulsar el cambio. A finales del decenio de 1960, el Gobierno se asoció con la industria del automóvil para hacer frente al desafío de crear condiciones más seguras para el número cada vez mayor de personas y vehículos que circulan por las carreteras. El Gobierno instituyó estrictas normas de seguridad, comenzando con los cinturones de seguridad obligatorios en el regazo en 1968. En 1989, los airbags simples para el conductor pasaron a ser obligatorios, pero hoy en día el mercado exige múltiples sistemas de airbags frontales, laterales y traseros para aumentar la probabilidad de supervivencia de los pasajeros en un accidente. El Gobierno también abordó el problema mediante reglamentos sobre el diseño de las carreteras, los controles de tráfico y los límites de velocidad obligatorios, así como directrices estrictas para los conductores, como licencias específicas para cada categoría de vehículos y fuertes consecuencias para el incumplimiento de las leyes de tráfico. Hoy en día, la industria está introduciendo nuevas tecnologías como el auto-frenado para reducir aún más la probabilidad de un accidente. Todos estos cambios se hicieron para el bien mayor percibido de una sociedad cada vez más dependiente del automóvil. Aunque el número de accidentes de tráfico, lesiones y muertes sigue siendo demasiado elevado, los vehículos y la infraestructura que utilizan los conductores hoy en día son significativamente más seguros que hace 20 años.

Resultados esperados

Ni el gobierno, ni la industria, ni el mundo académico pueden resolver los problemas de seguridad cibernética de manera holística sin una reforma de las políticas. Como se desprende del enfoque multidisciplinario adoptado para que los viajes en automóvil sean más seguros para todos los estadounidenses, encontrar el equilibrio adecuado entre la promoción de un entorno de seguridad cibernética que sea seguro para las empresas, los consumidores y el Gobierno -sin sofocar la innovación y la competencia- requerirá una aplicación delicada de diversos instrumentos de política.

44 Visner, "Cybersecurity Moonshots".

Las políticas nacionales e internacionales, que incluirán leyes, normas y orientación derivadas de diversos órganos, entre ellos el Congreso, normas gubernamentales, normas de la industria y la tecnología, así como normas internacionales de Internet, podrían incluir lo siguiente:

- Definir e invertir en la infraestructura necesaria para diseñar y operar la Internet de una manera fundamentalmente más segura y protegida;

- Definir las responsabilidades y autoridades de los interesados en los ecosistemas de seguridad cibernética que incentiven la adopción de medidas proactivas y voluntarias acordes con sus funciones específicas y responsabilidades; [45]

- Definir los límites de las normas de seguridad cibernética dentro del entorno seguro y promover la comprensión pública y privada del papel que sus decisiones desempeñan en nuestra seguridad nacional;

- Definir vías de decisión para los interesados (incluido el fomento de los impulsores del mercado o el desarrollo de nuevos recursos no tecnológicos) para fomentar incentivos positivos y evitar las consecuencias de la violación de las normas de comportamiento establecidas para las actividades dentro del entorno seguro. Por ejemplo, definir certificaciones del tipo "Underwriters Laboratory" para los productos y servicios de ciberseguridad;

- Elaborar políticas que fomenten la definición de la capacidad de recuperación de las infraestructuras críticas mediante el uso de tecnología de alta disponibilidad y redundante, así como la responsabilidad de los proveedores de servicios para prestar los servicios prometidos; y

- Definir recompensas para la investigación sobre ciberseguridad y asociaciones de innovación entre la industria, el gobierno y el mundo académico para dirigir el desarrollo de la tecnología de la ciberseguridad hacia los requisitos definidos en la Iniciativa Moonshot de Ciberseguridad y aumentar el volumen y la calidad tanto de la tecnología cibernética estadounidense como de los profesionales cibernéticos en nuestra futura fuerza laboral.

Dependencias entre pilares

La política es el habilitador y la principal herramienta del gobierno de los Estados Unidos para asegurar el éxito de la Iniciativa Moonshot de Ciberseguridad. Para ello, el pilar de la *política* apoya el pilar de la *tecnología*, específicamente cuando se definen hojas de ruta tecnológicas que abordan la seguridad; *el comportamiento*, en el que políticas impulsarán y, en algunos casos, regularán la actividad de los usuarios; *la privacidad*, a medida que se introduzcan nuevas leyes y reglamentos que garanticen el derecho del público a determinar el uso de su información personal; y *la educación*, en la que los esfuerzos gubernamentales por aumentar el número de ciberprofesionales afectan a las políticas educativas de los grados K-12. Estos pilares ayudan a determinar la dirección general de la gobernanza de la Iniciativa para crear un entorno seguro fiable, resistente y accesible. En apoyo de la Iniciativa de Seguridad Cibernética en general, la reforma de las políticas debería ser:

- Basado en incentivos positivos y en la evitación de consecuencias negativas;

[45] Por ejemplo, tanto los usuarios de las empresas como los proveedores de infraestructuras esenciales deben tener la expectativa de aplicar un marco de seguridad cibernética aceptado, como el NIST o el Instituto SANS, que se pueda hacer cumplir a través de los canales de rendición de cuentas existentes en el sector.

- Considerado desde el principio y a lo largo de las iniciativas en otros pilares estratégicos de la Iniciativa de Seguridad Cibernética de la Luna, no al final como una idea o consecuencia posterior; y

- Justo y equitativo para el bien común americano, siendo al mismo tiempo el ejemplo para el mundo y promoviendo, cuando sea posible, resultados internacionales positivos y la libertad de Internet.

3.5 La Iniciativa de Seguridad Cibernética Moonshot Initiative Grandes Retos

Recomendación clave: Tras definir el Marco Estratégico de la Iniciativa Moonshot sobre Ciberseguridad y las prioridades nacionales de I+D en materia de ciberseguridad, el Consejo Moonshot sobre Ciberseguridad y las entidades asociadas a nivel de departamento deberían liderar un proceso nacional de múltiples partes interesadas para definir, identificar y lanzar uno o más Grandes Retos de la Ciberseguridad. El Consejo de la Ciberseguridad de la Cámara de Comercio también puede desempeñar un papel fundamental en el aumento de la visibilidad y incentivando la acción distribuida alineada con sus objetivos.

A lo largo del estudio, los expertos destacaron repetidamente la importancia de determinar una o dos esferas iniciales específicas en las que un enfoque acelerado de toda la nación podría producir progresos demostrables en un horizonte temporal de tres a cinco años. Esos expertos subrayaron la importancia de ese enfoque para producir avances más inmediatos, ayudar a crear impulso y establecer un modelo fundamental para la visión a más largo plazo (10 años) de la Iniciativa sobre la seguridad cibernética en general. El NSTAC ha adoptado el modelo bien establecido de "Grandes Retos" para describir este enfoque para un enfoque específico. Los ponentes presentaron una variedad de definiciones de lo que constituye un Gran Reto, incluyendo las siguientes:

- Objetivos audaces pero alcanzables en materia de ciencia, tecnología e innovación que exigen un amplio número de actividades en todas las disciplinas técnicas y no técnicas;

- Una "Estrella del Norte" para colaboraciones multidisciplinarias de alto impacto entre el gobierno, la industria, las universidades, las organizaciones sin fines de lucro y la élite de científicos, ingenieros y ciudadanos de la nación;

- Un mecanismo para que las organizaciones aprovechen sus singulares aptitudes y capacidad para resolver problemas de mayor envergadura que los que pueden abordar con éxito por sí mismas; y

- Un medio para abordar muchos de los problemas más difíciles del siglo, especialmente aquellos que capturan la imaginación de la sociedad, y por lo tanto el apoyo político.

El NSTAC escuchó a expertos con experiencia directa en la ejecución de iniciativas de "Gran Reto" dentro del Gobierno, la industria privada y la comunidad sin fines de lucro. Estas actividades abarcaban numerosas disciplinas, y eran más frecuentes en áreas como el espacio, la biomedicina y la salud pública. Nuestra investigación también reveló una importante comunidad de interés de Grand Challenges en todo el Gobierno Federal, con importantes recursos de mejores prácticas agnósticas de la disciplina proporcionados centralmente a través de recursos como

Innovation.gov y Challenge.gov, gestionados administrativamente por la Administración de Servicios Generales. [46,47] Sin embargo, la ciberseguridad como disciplina no ha

46 "Challenges of Challenge", 2018, Challenge.gov, https://challenge.gov/list.

47 "The Better Government Toolkit provides resources to build a better government through innovation", 2018, Innovation.gov, https://innovation.gov/toolkit/.

desarrolló una cultura igualmente robusta de innovación abierta y de pensamiento "como la luna" representada por la comunidad de los Grandes Retos. El NSTAC cree que esto debe cambiar.

Con este fin, el NSTAC recomienda al Consejo de Seguridad Cibernética Moonshot liderar la identificación y el lanzamiento de uno o más Grandes Retos de la Ciberseguridad. Para identificar los candidatos apropiados para el Gran Reto, el Consejo y las entidades departamentales asociadas deberían llevar a cabo un proceso de colaboración de seis meses de duración en el que participen oficialmente los interesados del sector privado y del mundo académico de todo el país. Es fundamental que este proceso incluya a ciudadanos sin asociación profesional ni conocimientos especializados en materia de ciberseguridad para inyectar nuevas ideas en este diálogo.

3.5.1 Criterios de identificación y evaluación

La designación de "Gran Reto" es apropiada para un área específica de desarrollo prioritario en la que el progreso de toda la nación tiene una trayectoria inadecuada y se beneficiaría de una atención nacional específica y un enfoque estratégico (Categoría "C" en la rúbrica del Marco de Alcance, introducida por primera vez al principio de la Sección 3.4, *Definir el Marco Estratégico y los Pilares*). Al evaluar a los posibles candidatos al Gran Reto durante este proceso de múltiples interesados, el Consejo debería proponer y sopesar varios criterios de evaluación y preguntas clave, entre ellos

- **Un claro papel del gobierno:** ¿Tiene el Gobierno un papel claro en la catalización de las actividades de toda la nación alineadas con la iniciativa? ¿Puede la atención estratégica del Gobierno, la reducción de barreras, la dotación de recursos o los requisitos incentivar la acción cuando los anteriores impulsores basados en el mercado han demostrado ser insuficientes?

- **Beneficios de la colaboración:** ¿Requiere la iniciativa de actividades que no están al alcance de las autoridades gubernamentales o de los puntos fuertes? ¿Se beneficiaría la iniciativa de un esfuerzo más distribuido y de mayor escala que aproveche una variedad de fuentes de asociación y colaboración?

- **Socialmente resonante:** ¿Puede articularse la iniciativa de manera que sea ampliamente comprendida por la sociedad, especialmente por los expertos no especialistas en ciberseguridad, como algo fundamentalmente importante y estratégico a nivel nacional?

- **Medible y alcanzable:** ¿Hay hitos y objetivos demostrables que puedan alcanzarse en el plazo de 10 años de la Iniciativa sobre la seguridad cibernética en general?

- **Altamente escalable:** ¿La realización de los objetivos de la iniciativa produciría un resultado capaz de ser fácilmente, incluso automáticamente, aprovechado en los entornos de defensa de la ciberseguridad?

- **Multidimensional:** ¿Tiene la iniciativa un alcance amplio, lo suficientemente extenso como para incluir actividades a través de múltiples Pilares Estratégicos?

Un examen cuidadoso de estos criterios y otros, aunque una diversidad de aportaciones del proceso de seis meses de múltiples interesados, debería culminar en la identificación de una declaración específica basada en los resultados, junto con actividades alineadas para el logro de

ese resultado en los seis Pilares Estratégicos.

Ejemplo ilustrativo de las iniciativas del Gran Reto: IA para la Ciberseguridad

- La Casa Blanca anunció el premio para lograr que la tecnología de la IA cibernética sea el "Santo Grial" en 5 años.
- Concursos para el desarrollo de algoritmos para la prevención automatizada de amenazas
- Innovaciones políticas/campañas de comunicación para hacer que la disciplina "IA para el ciberespacio" sea tan prestigiosa como la "IA para vehículos autónomos".
- Consorcios Educativos Modelos que tienden un puente entre el mundo académico y la industria privada para inculcar, desarrollar y retener los conocimientos técnicos de la IA para las aplicaciones de la ciberseguridad

3.5.2 El papel del gobierno de EE.UU. en el fomento de la acción a través de la seguridad cibernética Grandes retos

Una vez completada la fase de identificación, el Gobierno de los Estados Unidos puede desempeñar un papel fundamental para aumentar y mantener la visibilidad de los Grandes Retos de la Ciberseguridad a lo largo de su ciclo de vida.
Entre los ejemplos representativos cabe citar el anuncio a nivel presidencial o vicepresidencial del lanzamiento del Gran Reto o las celebraciones de alto nivel de los principales avances relacionados con el Gran Reto. El Gobierno de los Estados Unidos también puede suscitar y mantener el interés de manera permanente utilizando diversos instrumentos para incentivar y acelerar las actividades de toda la nación en consonancia con el logro del Gran Desafío. Entre ellas figuran herramientas que recompensan predominantemente la demostración y el logro de resultados, de manera coherente con los principios de un enfoque de "tiro a la luna".

Para que quede claro, el NSTAC no propone que el Gobierno de los Estados Unidos dirija unilateralmente el desarrollo y lanzamiento de estos Grandes Retos de la Ciberseguridad y lleve a cabo todas las actividades asociadas. Numerosas entidades no gubernamentales, como XPrize y la Fundación Gates, tienen una sólida experiencia en la ejecución con éxito de los Grandes Retos y los concursos de premios asociados para lograr objetivos ambiciosos y centrados en los resultados. Sin embargo, el Gobierno de los Estados Unidos puede desempeñar un papel fundamental en la puesta en marcha del interés, la determinación del alcance del desafío y la creación de una vía que permita una posible democratización y futuras oportunidades comerciales. Al emparejar una visión inspiradora e impactante con tecnologías orgánicamente emergentes, como la fabricación de aditivos de bajo costo, aplicaciones de nube y la IA, estos Grandes Retos de la Ciberseguridad pueden ser naturalmente reforzados por recursos corporativos, académicos y sin fines de lucro que sirvan a sus propias prioridades.

Category	Types
1. Pay-for-Performance	A. **Incentive Prizes**: Results-based market incentives that are designed to overcome market failures and catalyze innovation. Unlike "recognition" prizes that honor past achievements, "inducement" or "incentive" prizes encourage participants in the competition to achieve a particular goal.
	B. **Pay-for-Success Bonds**: Also known as a social impact bonds. The financing organization and the Federal, state, or local government enter into a contract that specifies the population to be served, the outcomes to be achieved, the measurement methodology to be used, and the schedule of payments to be made. The financing organization works with philanthropic and other investors to invest in innovative, data-driven service providers that can achieve results.
	C. Mi**lestone-Based Payments**: Terms in a contract in which the payment for each performance milestone established in the statement of work is not made until the prior milestone is proven to have been achieved. Risk is placed on the performer or vendor, unlike other contracts in which payment is either guaranteed with limited protections for quality of performance or in which payments are designed to support in advance the performer's effort to complete the next milestone.
	D. **Challenge Based Acquisitions**: A Federal Acquisition Regulation (FAR)-based acquisition approach that uses challenges to communicate the needed capability, encourage innovation in a minimally prescriptive environment, assess candidate offerings, and, ultimately, purchase the proven solution(s).
2. Purchase Commitments	A. **Advance Market Commitments (AMCs)**: Binding commitments to purchase, or to subsidize purchase, of a certain volume of a product at a fixed prize, if the product meets pre-defined performance characteristics
	B. **Non-Binding Purchase Commitments**: Non-binding commitments to purchase products can provide market pull, if there is both a clearly defined performance specification and a strong expression of interest from potential buyers.
	C. **Buyer's Consortia**: Cooperative agreements between purchasers of products that leverage the combined buying power of those purchasers to drive down the price of products
3. Accelerated Review or Exclusive Access	A. **Priority Review Vouchers**: An accelerated regulatory review offered to products that meet certain performance or cost criteria
	B. **Exclusive Access**: Unique or accelerated access to training, partnership, or procurement opportunities
	C. **Pilot and Third-Party Evaluation Opportunities**: Dedicated opportunities to deploy a pilot implementation a solution/intervention, potentially with resources for third-party evaluation 8

Figura 3: Hay *una amplia gama de "mecanismos de atracción" a disposición del Gobierno de los Estados Unidos como herramientas para inculcar una acción centrada en los resultados y alineada con los Grandes Retos definidos.* [48]

4.0 CONCLUSIÓN

En este informe de la NSTAC se presentó el caso para establecer una Iniciativa de Seguridad Cibernética en toda la nación con el objetivo fundamental de hacer que la Internet sea segura y protegida para 2028. Este caso se basa en un sólido precedente histórico de logros colectivos al enfrentarse a un reto con importantes riesgos nacionales.

En el presente informe se expone el camino para un futuro estado de la Internet que sea resistente y fuerte, que valore la privacidad y la responsabilidad personal, que esté disponible y sea accesible, y que aproveche para bien las capacidades tecnológicas emergentes. Este camino requerirá cambios drásticos en la educación y la política, el establecimiento de grandes desafíos que los estadounidenses puedan afrontar, incentivos más alineados para comportamientos seguros y consecuencias para los maliciosos, y una comprensión fundamental de la naturaleza global e interconectada de Internet. El informe presenta un camino en el que los Estados Unidos pueden liderar el mundo con el ejemplo y debe servir tanto como guía como advertencia, que cuando se trata de la preservación de la confianza y la seguridad de Internet y nuestra forma digital de
la vida que depende de ella, el fracaso no es una opción.

[48] Jennifer Gustetic, "Diseñando e implementando grandes desafíos": Learning from NASA's Experience," (Sesión informativa para el Subcomité de Seguridad Cibernética en la Luna de la NSTAC, Arlington, VA, 23 de agosto de 2018).

APÉNDICE A: METODOLOGÍA DE ESTUDIO DEL SUBCOMITÉ

El Subcomité de tiro lunar de seguridad cibernética del Comité Asesor de Telecomunicaciones de Seguridad Nacional del Presidente (NSTAC) estaba compuesto por representantes de más de 20 entidades gubernamentales, académicas y de la industria privada de todo el ecosistema de la tecnología de la información, las telecomunicaciones y la seguridad cibernética. Además de la representación de las empresas miembros del NSTAC, el subcomité nombró a miembros del mundo académico para asegurarse de que el grupo representara perspectivas importantes del enfoque de toda la nación que defendía la Iniciativa de la Ciberseguridad Lunar. El NSTAC utilizó varios métodos para reunir información, entre ellos, reuniones informativas de expertos en la materia, el examen de numerosos informes y artículos sobre seguridad cibernética y la realización de exámenes de políticas. En concreto, el NSTAC:

- Recibió 27 sesiones informativas oficiales de expertos de la industria, el mundo académico y el sector público (Apéndice E), además de numerosas otras entrevistas no oficiales con expertos externos; y

- Realizó un examen de las políticas, reglamentos, informes y documentos sobre prácticas óptimas en materia de seguridad cibernética del sector privado y del Gobierno Federal.

> "Cada vez que me encuentro con un problema que no puedo resolver, siempre lo hago más grande. Nunca puedo resolverlo tratando de hacerlo más pequeño, pero si lo hago lo suficientemente grande, puedo empezar a ver los contornos de una solución."
>
> - El presidente Dwight D. Eisenhower

Durante el período de estudio que comenzó en febrero de 2018, el Subcomité de Seguridad Cibernética en la Luna celebró aproximadamente 50 reuniones. En la primera fase del estudio, el subcomité se centró intencionadamente en recibir información de expertos con experiencia directa o conocimientos en esfuerzos de "tiro a la luna" fuera del ámbito de la ciberseguridad. La intención de este enfoque era identificar a los mejores agnósticos del dominio modelos de práctica y metodologías sobre la forma en que se han aprovechado eficazmente los recursos de toda la nación en el pasado para lograr resultados ambiciosos. El NSTAC creía que esto era fundamental para liberar el pensamiento más allá de los límites normales que, en nuestra opinión, a menudo han limitado nuestro diálogo nacional en torno a la seguridad cibernética. Entre los ejemplos representativos cabe citar las reuniones informativas sobre el Proyecto del Genoma Humano, la creación de la Red del Organismo de Proyectos de Investigación Avanzada /Internet, los Grandes Retos de la Agencia de Desarrollo Internacional de EE.UU. para la Salud Pública Mundial, y el programa Apolo.

En la segunda fase del estudio, el subcomité escuchó a destacados expertos en seguridad cibernética para comenzar a identificar los principios organizativos comunes y los resultados deseados para lograr un entorno de seguridad cibernética fundamentalmente seguro. Entre los ejemplos representativos cabe citar las reuniones informativas de expertos en tecnologías críticas, educación, investigación y desarrollo, grandes desafíos y política de innovación, y modelos de gobernanza para informar a la estructura de la Iniciativa sobre Seguridad Cibernética.

MIEMBROS DEL SUBCOMITÉ

Sr. Peter Altabef, Unisys Corporation y Copresidente del Subcomité Sr. Mark McLaughlin, Palo Alto Networks y Copresidente del Subcomité

El Sr. Sean Morgan, codirector del Grupo de Trabajo sobre redes y seguridad cibernética de Palo Alto
El Sr. Thomas Patterson, de la Corporación Unisys y el Grupo de Trabajo de Seguridad Cibernética de la Luna, codirige

Nombre	Compañía
El Sr. Mark Bentley	Unisys Corp.
El Sr. Christopher BoyerAT&T	, Inc.
La Sra. Cherilyn Caddy	Agencia de Seguridad Nacional
El Sr. John Campbell	Iridium Communications, Inc.
El Sr. James Carnes	Ciena Corp.
La Sra. Terri Claffey	Neustar, Inc.
El Sr. Mark Cohn	Unisys Corp.
La Sra. Kathryn Condello	CenturyLink, Inc.
Sra. Amanda Craig-Deckard-Microsoft Corp.	
El Sr. Michael Daly	Raytheon Co.
El Sr. Darrell Durst	Lockheed Martin Corp.
El Sr. Victor EinfeldtIridium Communications, Inc.	
El Sr. Patrick Flynn	McAfee, Inc.
El Dr. Boaz Gelbord	Dun & Bradstreet, Inc.
El Sr. William Gravell	Diogenes Group, LLC
La Sra. Katherine GronbergForeScout	Technologies, Inc.
El Sr. Dean Hullings	ForeScout Technologies, Inc.
El Sr. Rodney JoffeNeustar	, Inc.
La Sra. Ilana JohnsonNeustar	, Inc.
El Sr. Kent LandfieldMcAfee	, Inc.
El Sr. Gregory Lebovitz	Equinix, Inc.
Sr. William RyanDepartamento de Seguridad Nacional	

El Sr. Jerry Scarborough	Raytheon Co.
El Sr. John Scimone	Dell, Inc.
El Sr. Robert Spiger	Microsoft Corp.
La Sra. Roberta Stempfley	Instituto de Ingeniería de Software
El Sr. Kent Varney	Lockheed Martin Corp.
El Sr. Milan Vlajnic	Communication Technologies, Inc.
La Dra. Prescott Winter	Oracle Corp.

GESTIÓN DEL SUBCOMITÉ

La Sra. Helen Jackson	El Comité Asesor de Telecomunicaciones de Seguridad Nacional del Presidente (NSTAC) Oficial Federal Designado (DFO)
La Sra. Sandra Benevides	Alternativa NSTAC DFO
La Sra. DeShelle Cleghorn	Alternativa NSTAC DFO
La Sra. Kayla Lord	Departamento de Seguridad Nacional NSTAC Apoyo
La Sra. Stephanie Curry	Booz Allen Hamilton, Inc.
La Sra. Laura Karnas	Booz Allen Hamilton, Inc.
El Sr. Barry Skidmore	Total Systems Technologies Corp.

APÉNDICE C: ACRÓNIMOS

AI Inteligencia Artificial

DHSD Departamento de Seguridad Nacional

DOJDepartamento de Justicia

DSB La Junta Científica de Defensa

FDA Administración de Alimentos y Medicamentos

GPS Sistema de posicionamiento global

ICT Tecnología de la Información y la

Comunicación IO Internet de las cosas

MCC Corporación de Microelectrónica y Tecnología

Informática NASA Administración Nacional de Aeronáutica y del

Espacio

NIST Instituto Nacional de Normas y Tecnología

NS/EP Seguridad Nacional/Preparación para

emergencias

NSTAC Comité Consultivo de Telecomunicaciones de Seguridad

Nacional NTIA Administración Nacional de Telecomunicaciones e

Información QGP Propósito general cuántico

I+D Investigación y desarrollo

SEMATECH Consorcio de Tecnología de Fabricación de

Semiconductores STEMCiencia , Tecnología, Ingeniería y

Matemáticas

APÉNDICE D: GLOSARIO

5G - Una futura red móvil de quinta generación, cuya especificación la Unión Internacional de Telecomunicaciones (UIT) no ha definido completamente. Se espera que soporte velocidades de datos de 10 gigabits por segundo y superiores. Los despliegues comerciales de 5G no se esperan hasta alrededor de 2020. (Diccionario de Telecomunicaciones de Newton)

Fabricación aditiva - Se define como el proceso de unir materiales para hacer objetos a partir de datos de modelos tridimensionales (3D), normalmente capa sobre capa, en contraposición a las metodologías de fabricación sustractiva como el mecanizado. (Un artefacto de prueba de fabricación aditiva, Shawn Moylan, John Slotwinski, April Cooke, Kevin Jurrens, y M. Alkan Donmez, Revista de Investigación del Instituto Nacional de Estándares y Tecnología, Volumen 119 (2014) http://dx.doi.org/10.6028/jres.119.017)

Inteligencia **Artificial** - La inteligencia exhibida por las máquinas o el software. Un término popularizado por Alan Turing, describe históricamente una máquina que podía engañar a la gente para que pensara que era un ser humano a través de la Prueba de Turing. Recientemente, los científicos de este campo han abandonado en gran medida este objetivo para centrarse en la singularidad de la inteligencia de las máquinas y aprender a trabajar con ella de forma inteligente y útil. (Diccionario de Telecomunicaciones de Newton)

Inteligencia **Aumentada** - Una conceptualización alternativa de la inteligencia artificial que se centra en el papel de asistencia de la IA, enfatizando el hecho de que está diseñada para mejorar la inteligencia humana en lugar de reemplazarla. (whatis.techtarget.com/definition/augmented-intelligence)

Autenticación - El proceso mediante el cual un usuario, fuente de información o simplemente información demuestra que es quien dice ser; el proceso de determinar la identidad de un usuario que intenta acceder a una red y/o sistema informático. (Diccionario de telecomunicaciones de Newton)

Biometría del comportamiento - Rasgos de comportamiento que se aprenden o adquieren, como la verificación de la firma dinámica y la dinámica de las teclas. (Programa de Estándares Biométricos y Centro de Recursos del NIST)

Biometría - El uso de características biológicas mensurables, como el reconocimiento de huellas dactilares, el reconocimiento de voz y los escáneres de retina e iris para proporcionar autenticación. (Diccionario de Telecomunicaciones de Newton)

Computación en nube - Modelo para permitir el acceso a la red a petición a un conjunto compartido de capacidades/recursos de tecnología de la información configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios), que se pueden aprovisionar y liberar rápidamente con un mínimo de esfuerzo de gestión o de interacción con el proveedor de servicios. Permite a los usuarios acceder a servicios basados en la tecnología desde la nube de la red sin conocimiento, experiencia o control de la infraestructura tecnológica que los sustenta. Tanto los datos del usuario como los servicios de seguridad esenciales pueden residir y gestionarse dentro de la nube de red. (Comité de Instrucción de Sistemas de Seguridad Nacional (CNSSI) 4009, adaptado) (Informe NSTAC 2016)

Infraestructura crítica - Sistemas y activos, ya sean físicos o virtuales, tan vitales para los

Estados Unidos que la incapacidad o destrucción de dichos sistemas y activos tendría un impacto debilitante en la seguridad, la seguridad económica nacional, la salud o la seguridad pública nacional, o cualquier combinación de esos asuntos. La infraestructura crítica puede ser propiedad de los sectores público y privado y ser explotada por ellos. *Ley de protección de la infraestructura crítica de 2001,* 42 U.S.C.519c(e)] (CNSSI 4009, adaptado)

Ataque cibernético - Un ataque, a través del ciberespacio, dirigido al uso del ciberespacio por parte de una empresa con el propósito de interrumpir, inutilizar, destruir o controlar maliciosamente un entorno/infraestructura informática; o destruir la integridad de los datos o robar la información controlada. (CNSSI 4009)

Ciberseguridad - La capacidad de proteger o defender el uso del ciberespacio de los ataques cibernéticos. (CNSSI 4009)

Sistemas de Control Industrial - Un sistema de información utilizado para controlar los procesos industriales como la fabricación, el manejo de productos, la producción y la distribución. Los sistemas de control industrial incluyen sistemas de control de supervisión y adquisición de datos utilizados para controlar activos geográficamente dispersos, así como sistemas de control distribuidos y sistemas de control más pequeños que utilizan controladores lógicos programables para controlar procesos localizados. (NIST SP 800-53A, Revisión 4)

Tecnología de la información - Equipo, procesos, procedimientos y sistemas utilizados para proporcionar y apoyar los sistemas de información (computarizados y manuales) dentro de una organización y los que llegan a los clientes y proveedores. (Diccionario de Telecomunicaciones de Newton)

Internet de las cosas - La colección total interconectada de redes de dispositivos. (Diccionario de Telecomunicaciones de Newton)

Aprendizaje automático - Un tipo de inteligencia artificial en la que los ordenadores utilizan enormes cantidades de datos para aprender a hacer tareas en lugar de ser programados para hacerlas. (Diccionario del estudiante de Oxford)

Incidente material de ciberseguridad - un suceso que real o potencialmente tiene consecuencias adversas para los sistemas de información o los datos de una empresa que razonablemente se esperaría que afectara al valor de los valores (de la empresa) o que influyera en las decisiones de los inversores. (ARTÍCULO 33-10459).

Ciencia de los materiales - El estudio científico de las propiedades y aplicaciones de los materiales de construcción o fabricación (como cerámicas, metales, polímeros y compuestos). (Diccionario Merriam- Webster)

Comunicaciones de seguridad nacional/preparación para emergencias (NS/EP) - Servicios de telecomunicaciones que se utilizan para mantener un estado de preparación o para responder y gestionar cualquier evento o crisis (local, nacional o internacional) que cause o pueda causar lesiones o daños a la población, daños o pérdidas de propiedad, o que degrade o amenace la postura NS/EP de los Estados Unidos (47 Código de Regulaciones Federales Capítulo II, § 201.2(g)). Las comunicaciones del NS/EP incluyen principalmente las capacidades técnicas respaldadas por políticas y programas que permiten al Poder Ejecutivo comunicarse en todo momento y en toda circunstancia para llevar a cabo las funciones esenciales de su misión y responder a cualquier evento o crisis (local, nacional o internacional), lo que incluye la comunicación consigo mismo; con los poderes Legislativo y Judicial; con los gobiernos estatales,

territoriales, tribales y locales; con las entidades del sector privado; así como con el público, los aliados y otras naciones. Las comunicaciones NS/EP incluyen además esos sistemas y capacidades a todos los niveles del gobierno y del sector privado que son necesarias para garantizar la seguridad nacional y para gestionar eficazmente los incidentes y las emergencias. (Comité Ejecutivo de Comunicaciones NS/EP basado en el Decreto (EO) 13618, *Asignación de las funciones de comunicaciones de seguridad nacional y preparación para emergencias* [2012])

Redes - Sistema(s) de información implementado con un conjunto de componentes interconectados, que pueden incluir enrutadores, concentradores, cableado, controladores de telecomunicaciones, centros de distribución clave y dispositivos de control técnico. (Glosario de términos de seguridad de la información del NIST - NIST IR 7298 - Revisión 2)

Protocolo - Un conjunto de reglas y formatos, semánticos y sintácticos, que permiten a los sistemas de información intercambiar información. (Glosario de términos de seguridad de la información del NIST - NISTIR 7298 - Revisión 2)

Comunicaciones cuánticas - Un campo de la física cuántica aplicada estrechamente relacionado con el procesamiento de la información cuántica y la teletransportación cuántica. Su aplicación más interesante es la protección de los canales de información contra las escuchas por medio de la criptografía cuántica. (www.picoquant.com/applications/category/quantum-optics/quantum-communication)

Computación Cuántica - Una tecnología de computación en desarrollo que explota las propiedades de los átomos para crear un tipo de arquitectura de computación radicalmente diferente a través de la física cuántica. La computación cuántica se basa en los rasgos básicos de un átomo, como la dirección de su giro (de izquierda a derecha, de derecha a izquierda) para crear un estado, como el "1" o el "0", tanto como los ordenadores convencionales utilizan las variaciones de la energía eléctrica (polaridad positiva y negativa). (Diccionario de Telecomunicaciones de Newton)

Criptografía Cuántica Resistente - La encriptación cuántica resistente es un conjunto de algoritmos de encriptación de clave pública desplegados que son resistentes a ser rotos por una computadora cuántica en pleno funcionamiento (Informe del NSTAC al Presidente sobre la Visión Estratégica de las Tecnologías Emergentes, 2017)

Garantía de software - El nivel de confianza de que el software está libre de vulnerabilidades, ya sea diseñado intencionadamente en el software o insertado accidentalmente en cualquier momento de su ciclo de vida y que el software funciona de la manera prevista. (NIST SP 800-163)

Amenaza - Cualquier circunstancia o evento con el potencial de impactar adversamente las operaciones de la agencia (incluyendo la misión, funciones, imagen o reputación), los activos de la agencia o los individuos a través de un sistema de información por medio de acceso no autorizado, destrucción, divulgación, modificación de información y/o negación de servicio. (NIST SP 800-53, CNSSI 4009, adaptado)

APÉNDICE E: BIBLIOGRAFÍA

Afonso, Paul. "Regulación de servicios y coordinación con agencias estatales en relación con una iniciativa de seguridad cibernética en la luna". Sesión informativa para el Subcomité de Seguridad Nacional de Telecomunicaciones del Presidente (NSTAC) sobre Seguridad Cibernética en la Luna, Arlington, VA, 13 de septiembre de 2018.

"El Programa Apolo (1963-1972)". 16 de septiembre de 2013. Administración Nacional de Aeronáutica y del Espacio (NASA). https://nssdc.gsfc.nasa.gov/planetary/lunar/apollo.html.

Bade, Gavin. "'Darknet' y las comunicaciones cuánticas podrían mejorar la ciberseguridad de la red, dicen los científicos al Senado." Inmersión de *utilidad*. 27 de octubre de 2017. https://www.utilitydive.com/news/darknet-and-quantum-communications-could-enhance-grid-cybersecurity-scie/508357/.

Bauer, Lujo. "Ciberseguridad, IA y ML: Oportunidades y desafíos". Sesión informativa para el Subcomité de Ciberseguridad Lunar de la NSTAC Arlington, VA, 18 de septiembre de 2018.

"El conjunto de herramientas para un mejor gobierno proporciona recursos para construir un mejor gobierno a través de la innovación". 2018. Innovation.gov. https://innovation.gov/toolkit/.

"Crítica de libros": Privacidad y Libertad". 24 de noviembre de 2004. Privacilla.org. http://www.privacilla.org/fundamentals/privacyandfreedom.html.

Braga, Matthew. "En el futuro, dejaremos la búsqueda de errores de software a las máquinas". *Placa madre.* 16 de junio de 2016. https://motherboard.vice.com/en_us/article/mg73a8/cyber- gran reto.

Calvert, Kenneth y Gianchandani, Erwin. "NSF/CISE": Una visión general y 'Moonshots'." Sesión informativa para el Subcomité de Ciberseguridad Lunar de la NSTAC, Arlington, VA, 15 de marzo de 2018.

Centro de Estudios Estratégicos e Internacionales. Hacking the Skills Shortage. (Washington, DC: Patrocinado por McAfee, 2016). https://www.mcafee.com/us/resources/reports/rp-hacking- skills-shortage.pdf.

Cerf, Vinton. "El futuro de la Internet de las cosas". Sesión informativa para el Subcomité de Ciberseguridad Lunar de la NSTAC, Arlington, VA, 5 de abril de 2018.

"Desafíos del desafío". 2018. Challenge.gov. https://challenge.gov/list.

El Consejo de Coordinación del Sector de las Comunicaciones. *Libro Blanco Técnico de la Industria*. Washington, DC: NTIA, 17 de julio de 2017. https://www.ntia.doc.gov/files/ntia/publications/cscc_industrywhitepaper_cover_letter.pdf.

El Consejo de Seguridad, Fiabilidad e Interoperabilidad de las Comunicaciones. *Grupo de Trabajo 2A: Informe final de las mejores prácticas de ciberseguridad*. Washington, DC: Comunicaciones Federales

Comisión, marzo de 2011. https://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf.

Corbin, Kenneth. "Profesionales de la seguridad cibernética en alta demanda, altamente pagados y altamente selectivos". 8 de agosto de 2013. CIO. https://www.cio.com/article/2383451/careers-staffing/cybersecurity- pros-in-high-demand--highly-paid-and-highly-selective.html.

"Sectores de infraestructura crítica". 22 de agosto de 2018. Departamento de Seguridad Nacional (DHS). https://www.dhs.gov/critical-infrastructure-sectors.

Daniel, Michael. "Fundamentos políticos necesarios para una ciberfotográfica". Sesión informativa para el Subcomité de Seguridad Cibernética de la NSTAC, Arlington, VA, 27 de marzo de 2018.

Diamandis, Peter. "Una masiva interrupción viene con la computación cuántica". 10 de octubre de 2016. SingularityHub. https://singularityhub.com/2016/10/10/massive-disruption-quantum- computering/.

DHS. *Carta del Consejo Asesor de la Asociación de Infraestructuras Críticas.* Washington, DC: DHS, 30 de noviembre de 2016. https://www.dhs.gov/sites/default/files/publications/cipac-charter-11- 30-16-508.pdf.

"Iniciativas de seguridad cibernética del DHS". 06 de febrero de 2013. Equipo de Preparación para Emergencias Informáticas de los Estados Unidos. https://www.us-cert.gov/security-publications/dhs-cyber-security-iniciativas.

Departamento de Justicia (DoJ). "El Departamento de Justicia es el anfitrión de la mesa redonda de la industria de la ciberseguridad". 28 de septiembre de 2018. https://www.justice.gov/opa/pr/justice-department-hosts-cybersecurity- mesa redonda de la industria.

DOJ. "Sesiones del Fiscal General anuncia la publicación del informe del Grupo de Tareas Cibernético-Digital". 19 de julio de 2018. https://www.justice.gov/opa/pr/attorney-general-sessions-announces- publication-cyber-digital-task-force-report.

Consejo Científico de Defensa (DSB). *Ciber como una Capacidad Estratégica - Resumen Ejecutivo.* Washington, DC: Oficina del Subsecretario de Defensa para la Investigación y la Ingeniería (USD-R&E), junio de 2018. https://www.acq.osd.mil/dsb/reports/2010s/DSB_CSC_Report_ExecSumm_Final_Web.pdf.

DSB. Disuasión *Cibernética*. Washington, DC: USD-R&E, Febrero, 2017. https://www.acq.osd.mil/dsb/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.

DSB. *Cyber Supply Chain-Executive Summary.* Washington, DC: USD-R&E, Abril, 2017.

https://www.acq.osd.mil/dsb/reports/2010s/1028953.pdf.

The Economist. "La gran brecha de datos sufrida por Equifax tiene implicaciones alarmantes". 16 de septiembre de 2017. https://www.economist.com/finance-and-economics/2017/09/16/the- La gran brecha de datos sufrida por el Equifax tiene implicaciones alarmantes.

"Habilitando la seguridad distribuida en el ciberespacio". 4 de octubre de 2016. DHS. https://www.dhs.gov/enabling-distributed-security-cyberspace.

Ferguson, David y Kavanaugh-Ulku, Lorin. "Los grandes desafíos de la USAID para el desarrollo". Sesión informativa para el Subcomité de Seguridad Cibernética de la NSTAC, Arlington, VA, 1 de marzo de 2018.

Fields, Craig. "Una iniciativa cibernética nacional". Sesión informativa para el Subcomité de Seguridad Cibernética de la NSTAC, Arlington, VA, 21 de agosto de 2018.

Administración de Alimentos y Medicamentos (FDA). *Gestión post-mercadeo de la ciberseguridad de los dispositivos médicos: Guía para el personal de la industria y de la Administración de Alimentos y Medicamentos.* Washington, DC: FDA, 28 de diciembre de 2016. https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

Frontera, Michael. "Corporación de Microelectrónica y Tecnología Informática". *Estado de Texas Asociación Histórica.* 15 de junio de 2010. https://tshaonline.org/handbook/online/articles/dnm01.

Gallagher, Patrick. "Programas de educación e investigación relacionados con el desarrollo de tecnología de ciberseguridad crítica". Sesión informativa para el Subcomité de Seguridad Cibernética de la NSTAC, Arlington, VA, 11 de septiembre de 2018.

Gibson, David V. y Everett M. Rogers. Colaboraciones de *I+D en el ensayo.* Boston: Harvard Business School Press, 1994.

"Estudio sobre la fuerza laboral de la seguridad de la información mundial". 2017. Centro de Seguridad Cibernética y Educación. https://iamcybersafe.org/GISWS.

Goldman, Lisa y Purmal, Kate. "Cómo lanzar una toma de la luna con éxito", Sesión informativa para el Subcomité de Seguridad Lunar de la NSTAC, Arlington, VA, 20 de febrero de 2018.

Goldman, Lisa y Kate Purmal. *El efecto de la luna: Interrumpir el negocio como de costumbre*. San Carlos, CA: Wynnefield Business Press, 2017.

Greatwood, Duncan. "Facilitar el cumplimiento de las normas de ciberseguridad para las infraestructuras críticas". Revista *CPO*. 3 de octubre de 2018. https://www.cpomagazine.com/2018/10/03/making-compliance-with-cybersecurity-regulations-easy-for-critical-infrastructure/.

Greenburg, Andrew. "La historia no contada de NOTPETYA, el ciberataque más devastador de la historia". *Conectado.* 22 de agosto de 2018. https://www.wired.com/story/notpetya-cyberattack- ukraine-russia-code-crashed-the-world.

Gustetic, Jennifer. "Diseñando e implementando grandes desafíos: Aprender de la experiencia de la NASA". Sesión informativa para el Subcomité de Ciberseguridad Lunar de la NSTAC, Arlington, VA, 23 de agosto de 2018.

Gustetic, Jennifer, y otros: "El gran desafío de los asteroides de la NASA: Estrategia, resultados y lecciones aprendidas". Política espacial (2018). 10.1016/j.spacepol.2018.02.003.

Halvorsen, Terry. "Tecnología y capacidades de la red 5G". Sesión informativa para el Subcomité de Ciberseguridad Lunar de la NSTAC, Arlington, VA, 5 de septiembre de 2018.

Halvorsen, Terry. "Entrando": Debemos anticipar las consecuencias de 5G ahora". *Señal.* 1 de marzo de 2018. https://www.afcea.org/content/incoming-we-must-anticipate-5g-consequences-now.

Hawkins, Derek. "La Ciberseguridad 202": El Congreso está listo para permitir que el DHS tome la delantera en la ciberseguridad federal." *The Washington Post*. 25 de septiembre de 2018.
https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/09/25/the-cybersecurity-202-congress-poised-to-allow-dhs-to-take-the-lead-on-federal-cybersecurity/5ba915ba1b326b7c8a8d162c/?utm_term=.706f4fe7dca5.
.

Heimann, Richard. "Estado de la Disciplina": Inteligencia Artificial." Sesión informativa para el Subcomité de Seguridad Cibernética de la NSTAC, Arlington, VA, 6 de septiembre de 2018.

Hinden, Robert y Russell Housley. "Desafíos al despliegue de la seguridad en Internet". Sesión informativa para el Subcomité de Ciberseguridad de la NSTAC, Arlington, VA, 25 de septiembre de 2018.

Hof, Robert. "Lecciones de Sematech". *Revista de Tecnología del MIT*. 25 de julio de 2011. https://www.technologyreview.com/s/424786/lessons-from-sematech/.

"La finalización del Proyecto del Genoma Humano: Preguntas frecuentes". 30 de octubre de 2010. Instituto Nacional de Investigación del Genoma Humano. https://www.genome.gov/11006943/.

Isaacson, Walter. "Construyendo el próximo Internet: Un tiro de luna para hacer un sistema de identificación seguro y verificado para las comunicaciones en línea" Sesión informativa para el Subcomité de Ciberseguridad Lunar de la NSTAC, Arlington, VA, 6 de marzo de 2018.

Kalil, Thomas. "Lecciones aprendidas de la Casa Blanca y del sector privado". Sesión informativa para el Subcomité de Seguridad Cibernética de la NSTAC, Arlington, VA, 27 de febrero de 2018.

Lewis, James. "Problemas de seguridad cibernética en la luna". Sesión informativa para el

Subcomité de Seguridad Cibernética de la NSTAC, Arlington, VA, 30 de agosto de 2018.

Markoff, John. "Matar la computadora para salvarla". *El New York Times.* 29 de octubre de 2012. https://nyti.ms/S91QbY.

Maughan, Douglas. "Esfuerzos de aceleración relacionados con el desarrollo de tecnología de ciberseguridad crítica". Sesión informativa para el Subcomité de Seguridad Cibernética de la NSTAC, Arlington, VA, 28 de agosto de 2018.

McConnell, Bruce. "Hacer que la Internet [global] sea segura y protegida... para el 2028." Sesión informativa para el Subcomité de Ciberseguridad de la NSTAC, Arlington, VA, 22 de agosto de 2018.

Mervis, Jeffrey. "Comprobación de datos": La participación del gobierno de EE.UU. en la financiación de la investigación básica cae por debajo del 50%". *La ciencia*. 9 de marzo de 2017. http://www.sciencemag.org/news/2017/03/data-check-us- La participación del gobierno en la financiación de la investigación básica cae por debajo del 50%.

NASA. *Datos de la NASA: Beneficios de Apolo: Saltos gigantescos en la tecnología.* Houston, TX: NASA. Julio de 2004. https://www.nasa.gov/sites/default/files/80660main_ApolloFS.pdf.

"Metas del Plan Nacional de Comunicaciones de Emergencia". 17 de mayo de 2018. DHS. https://www.dhs.gov/national-emergency-communications-plan-necp-goals.

NSTAC. *Informe de la NSTAC al Presidente sobre la Visión Estratégica de las Tecnologías Emergentes.* Washington, DC: NSTAC, 14 de julio de 2017. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Emerging%20Technologies%20Strategic%20Vision.pdf.

NSTAC. *Informe de la NSTAC al Presidente sobre la movilización de la tecnología de la información y las comunicaciones.* Washington, DC: NSTAC, 19 de noviembre de 2014. https://www.dhs.gov/sites/default/files/publications/NSTAC%20-%20Información%20y%20Comunicaciones%20Tecnología%20Movilización%20Informe%2011-19-2014.pdf.

NSTAC. *Informe de la NSTAC al Presidente sobre la resistencia de Internet y las comunicaciones.* Washington, DC: NSTAC, 16 de noviembre de 2017. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20ICR%20FINAL%20%2810-12-17%29%20%281%29-%20508%20compliant_0.pdf.

NSTAC. *Informe de la NSTAC al Presidente sobre el Internet de las cosas.* Washington, DC: NSTAC, 19 de noviembre de 2014. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf.

Administración Nacional de Telecomunicaciones e Información (NTIA). Catalogo *de Normas de Seguridad Existentes de IO Versión Borrador 0.01*, Washington, DC: NTIA, Julio 2017. https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog.pdf.

NTIA. *Fomentando el avance del Internet de las cosas*. Washington, DC: NTIA, enero de 2017. https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.

NTIA. *Proceso de múltiples interesados: Vulnerabilidades de la ciberseguridad*. Washington, DC: NTIA, 15 de diciembre de 2016. https://www.ntia.doc.gov/other-publication/2016/multistakeholder- proceso-ciber-seguridad-vulnerabilidades.

Grupo de Tareas Cibernético de Nueva York. *Construyendo un ciberespacio defendible.* Nueva York: Escuela de Asuntos Internacionales y Públicos de la Universidad de Columbia, 28 de septiembre de 2017.

https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF.

Nielsen, Kirstjen M. "Observaciones de la Secretaria Kirstjen M. Nielsen en la Conferencia de la RSA". Observaciones, San Francisco, CA, 17 de abril de 2018. Discursos. https://www.dhs.gov/news/2018/04/17/secretary-kirstjen-m-nielsen-remarks-rsa-conference.

O'Hern, William. "Sesión informativa para el Subcomité de Ciberseguridad Lunar de la NSTAC sobre redes y estándares 5G". Sesión informativa para el Subcomité de Ciberseguridad Lunar de la NSTAC. Arlington, VA, 18 de septiembre de 2018.

Oficina de Gestión y Presupuesto (OMB). Orientación sobre el uso de los retos y premios para promover el gobierno abierto. Marzo de 2010. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2010/m10-11.pdf.

Pence, Michael. Palabras del Vicepresidente Pence en la Cumbre de Ciberseguridad del DHS. 31 de julio de 2018. https://www.whitehouse.gov/briefings-statements/remarks-vice-president- pence-dhs-cybersecurity-summit/.

Perullo, Jerry. "Intercambio Intercontinental / NYSE" Sesión informativa para el Subcomité de Seguridad Cibernética de la NSTAC. Arlington, VA, 27 de septiembre de 2018.

Poindexter, John M. "Responsabilidad en Internet". Informe para el Subcomité de Ciberseguridad Lunar de la NSTAC. Arlington, VA, 22 de marzo de 2018.

Rosenblum, Todd. "Ciberseguridad": Un enfoque de poder nacional completo". *El resumen del cifrado.* 11 de enero de 2017. https://www.thecipherbrief.com/column_article/cybersecurity-a-whole-of- national-power-approach.

Rung, Anne E. y Tony Scott. "Laboratorios de Innovación en Adquisición y Piloto para el Laboratorio de Innovación en Adquisición Digital". Memorándum de Anne E. Rung y Tony Scott a los Oficiales Jefes de Adquisiciones, Ejecutivos Superiores de Adquisiciones y Jefes de Información. 9 de marzo de 2016. https://www.dhs.gov/sites/default/files/publications/March%202016%20Memo.pdf.

Rutkowski, Kenneth. "Sesión facilitada". Sesión informativa para el Subcomité de Seguridad Cibernética de la NSTAC, Arlington, VA, 10 de abril de 2018.

Sabett, Randy. "El papel de las políticas basadas en incentivos en una estrategia de ciberseguridad de toda la nación". Sesión informativa para el Subcomité de Seguridad Cibernética de la NSTAC, Arlington, VA, 26 de septiembre de 2018.

"Entrenamiento de Seguridad de la Información de la SANS". 2018. Instituto SANS. https://www.sans.org/.

Seffers, George. "AFCEA: Se necesita un enfoque de seguridad cibernética en toda la nación". *Señal.* https://www.afcea.org/content/afcea-whole-nation-cybersecurity-approach-needed.

Serbu, Jared. "Las ciberarmas extranjeras 'superan con creces' la capacidad de los EE.UU. para defender la infraestructura crítica, según el panel de Defensa". Red *Federal de Noticias*. 17 de marzo de 2017. https://federalnewsnetwork.com/dod-reporters-notebook-jared-serbu/2017/03/foreign-cyber- weapons-far-exceed-u-s-ability-defend-critical-infrastructure-defense-panel dice/.

La Chispa. "Cómo nuestro gobierno puede adaptarse a la evolución de la ciberseguridad y las necesidades de infraestructura de TI". Julio de 2017. https://www.icf.com/blog/cybersecurity/how-government-can-adapt-to- Evolución de las necesidades de ciberseguridad.

"Participación de los interesados y resistencia de la infraestructura cibernética". 22 de agosto de 2018. DHS. https://www.dhs.gov/stakeholder-engagement-and-cyber-infrastructure-resilience.

Estudiante, William. "Diálogo con el Subcomité de Ciberseguridad Lunar de la NSTAC". Sesión informativa para el Subcomité de Seguridad Cibernética de la NSTAC, Arlington, VA, 22 de marzo de 2018.

Comisión de Asistencia Electoral de los Estados Unidos (EAC). *PUNTO DE INICIO: Los sistemas electorales de EE.UU. como infraestructura crítica.* Silver Spring, MD: EAC https://www.eac.gov/assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf.

Visner, Samuel. "Lunas de seguridad cibernética". Sesión informativa para el Subcomité de Seguridad Cibernética de la NSTAC, Arlington, VA, 29 de marzo de 2018.

Waldrop, M. Mitchell. "La Gran Transición". Sesión informativa para el Subcomité de Seguridad Cibernética de la NSTAC, Arlington, VA, 8 de marzo de 2017.

Westin, Alan. *Privacidad y Libertad.* Nueva York: IG Publishing, 1967.

Zakheim, Dov S. "Estructurando el gobierno para enfrentar el desafío cibernético". Sesión informativa para el Subcomité de Seguridad Cibernética de la NSTAC, Arlington, VA, 27 de septiembre de 2018.