República de Panamá

CONSEJO NACIONAL PARA LA INNOVACIÓN GUBERNAMENTAL

Resolución No. 17
de 10 de septiembre de 2021

"Por la cual se aprueba la Estrategia Nacional de Ciberseguridad para el periodo 2021-2024".

EL CONSEJO NACIONAL PARA LA INNOVACIÓN GUBERNAMENTAL
en uso de sus facultades legales, y

CONSIDERANDO:

Que mediante la Ley 65 de 30 de octubre de 2009, publicada en la Gaceta Oficial No. 26400-C de 30 de octubre de 2009, se creó la Autoridad Nacional para la Innovación Gubernamental (AIG), anteriormente, Secretaría de la Presidencia para la Innovación Gubernamental, siendo parte de su nivel político administrativo, el Consejo Nacional para la Innovación Gubernamental, como instancia superior encargada de aprobar, entre otros temas, las propuestas de políticas y planes nacionales de desarrollo de tecnología e innovación gubernamental.

Que la Autoridad Nacional para la Innovación Gubernamental posee entre sus funciones la de establecer estándares necesarios para el desarrollo y protección de los sistemas tecnológicos del Estado panameño.

Que mediante Decreto Ejecutivo No. 709 de 26 de septiembre de 2011, publicado en la Gaceta Oficial No. 26880 de 27 de septiembre de 2011, se creó el, "CSIRT PANAMA Equipo de Respuesta a Incidentes de Seguridad de la Información del Estado Panameño", adscrito a la Autoridad Nacional para la Innovación Gubernamental, estableciéndose como parte de sus funciones la coordinación, colaboración y proposición de normas destinadas a incrementar los esfuerzos orientados a elevar los niveles de seguridad en los recursos y sistemas relacionados con las tecnologías informáticas y de comunicaciones de las entidades gubernamentales, asesorar a las entidades gubernamentales que reporten incidentes de seguridad en sus sistemas informáticos para la toma de los correctivos necesarios, así como también, entre otras funciones, la de investigar nuevas tecnologías y herramientas en materia de seguridad informática.

Que el 17 de mayo de 2013, fue publicada en la Gaceta Oficial No. 27289-A, el documento titulado "Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas", el cual fue previamente y debidamente aprobado, por el Consejo Nacional para la Innovación Gubernamental.

Que en atención a la acelerada evolución de las Tecnologías de la Información y Comunicación (TIC) se hace necesario actualizar las políticas, criterios y recomendaciones en materia de seguridad para hacer frente a las nuevas amenazas; así como también, para contrarrestar los posibles impactos que se puedan producir y en cumplimiento de lo que se establece en las normativas citadas ut supra, es por lo que la Autoridad Nacional para Innovación Gubernamental, presenta a consideración, evaluación y aprobación del Consejo Nacional para la Innovación Gubernamental, el documento contentivo de nuevas o actualizadas directrices, elementos, medidas, equipos debidamente actualizados y destinados a controlar la seguridad informática o espacio virtual (ciberseguridad) aplicables a las entidades públicas, así como también, la estrategia para la realización de las coordinaciones que resulten necesarias para su correspondiente utilización por parte de las mismas y para la interacción correspondiente de tales medidas con los ciudadanos y la sociedad en general.

Que en virtud de lo antes expuesto, y luego de la evaluación correspondiente, el Consejo.

RESUELVE:

PRIMERO: Aprobar el documento titulado "Estrategia Nacional de Ciberseguridad", para el periodo 2021-2024, el cual se adjunta como Anexo de la presente Resolución.

SEGUNDO: Dejar sin efecto la Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas, aprobada en el año 2013 y publicada en la Gaceta Oficial No. 27289-A.

TERCERO: Establecer que el presente documento podrá ser modificado cuando el Consejo Nacional para la Innovación Gubernamental lo estime conveniente, apoyándose en las recomendaciones que sean presentadas por la Autoridad Nacional para la Innovación Gubernamental.

CUARTO: Comunicar a las entidades públicas acerca de la obligatoriedad de cumplir con las directrices, recomendaciones y normativas contentivas de la nueva estrategia de ciberseguridad

QUINTO: Esta resolución empezará a regir a partir de su publicación en la Gaceta Oficial.

FUNDAMENTO DE DERECHO: Ley 65 de 30 de octubre de 2009, Decreto Ejecutivo No. 205 de 9 de marzo de 2010, Decreto Ejecutivo No. 709 de 26 de septiembre de 2011.

CÚMPLASE,

EL PRESIDENTE,

RAFAEL GONZÁLEZ
DELEGADO POR EL PRESIDENTE DE LA REPÚBLICA

LOS MIEMBROS,

ERNESTO REYES
DELEGADO POR EL MINISTRO DE LA PRESIDENCIA

ENELDA MEDRANO DE GONZÁLEZ
DELEGADA POR EL MINISTRO DE ECONOMÍA Y FINANZAS

EDUARDO ORTEGA BARRÍA
SECRETARIO NACIONAL DE CIENCIA, TECNOLOGÍA E INNOVACIÓN

EL SECRETARIO,

LUIS OLIVA
AUTORIDAD NACIONAL PARA LA INNOVACIÓN GUBERNAMENTAL

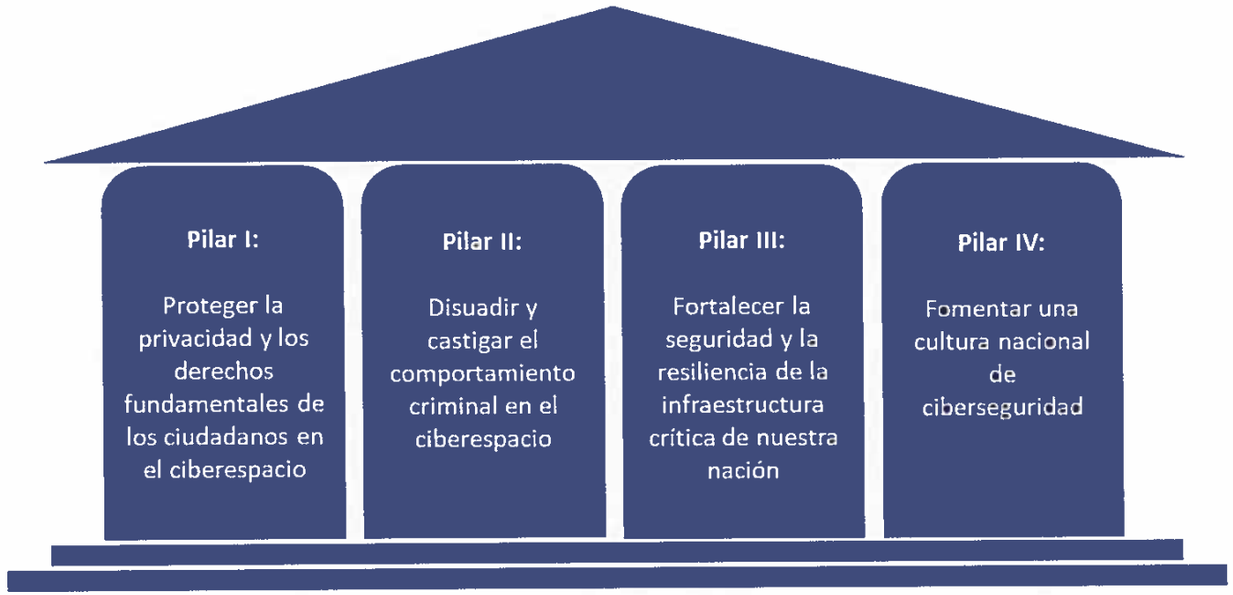
Introducción: De una estrategia hacia una hoja de ruta

En 2019, Cambridge Global Advisors (CGA) y Sistemas Aplicativos, S.A. (SISAP) fueron comisionados para redactar la Estrategia Nacional de Ciberseguridad de Panamá (ENC), un plan estratégico para proteger las Tecnologías de la Información y Comunicaciones (TIC) que son esenciales para la seguridad nacional del país, la estabilidad económica y la funcionalidad de la vida cotidiana. El trabajo de este consorcio CGA y SISAP (SIGCA) sirvió para revisar y actualizar un plan nacional de ciberseguridad inicial creado en 2013. La nueva Estrategia Nacional de Ciberseguridad es un producto de la Autoridad Nacional para la Innovación Gubernamental (AIG) y tiene la intención de ser un documento públicamente disponible que describe cómo la estrategia y los recursos, se alinearán para reforzar la postura de seguridad de las tecnologías de información y comunicaciones (TIC) y las Infraestructuras Críticas (IC) de Panamá.

La Estrategia Nacional de Ciberseguridad fue desarrollada con el conocimiento y entendimiento del entorno cibernético actual, también se realizó una revisión extensa de otras estrategias de ciberseguridad de más de 30 países. Además, datos fueron colectados en 18 ministerios y agencias de gobierno. Esta provee a la gente de Panamá, los principios y razones fundamentales que influyeron a esta estrategia integral, además de tareas que deberán llevarse a cabo para lograr su finalidad. Específicamente, nombra cuatro pilares que el gobierno de Panamá perseguirá bajo el plan: proteger la privacidad y los derechos fundamentales, disuadir y castigar la ciberdelincuencia, fortalecer la infraestructura crítica y fomentar una cultura de ciberseguridad.
O.k

Visión:

Panamá aspira a ser una nación que opera con un ciberespacio abierto, libre, seguro y resiliente que salvaguarda los derechos y libertades fundamentales de nuestro pueblo, al tiempo que permite al gobierno servir a las personas y fomentar un ambiente regulatorio favorable al crecimiento de la economía. Esto se logrará mediante la alineación de los recursos del sector público y privado, y promoviendo una conciencia universal de que la ciberseguridad es responsabilidad de todos.



Poniendo la estrategia en marcha: una hoja de ruta para la implementación

Este documento interno –"Hoja de ruta para la implementación"– es un complemento de la Estrategia Nacional de Ciberseguridad. Equipa a la AIG con una guía para coordinar con otras entidades e implementar los cuatro pilares. La Hoja de Ruta está organizada en dos componentes:

1. Una **narrativa** para ayudar a las partes interesadas a comprender claramente cada pilar y las tareas que apoyan a cada uno, respectivamente, y
2. Una **tabla** de resumen, un gráfico sumarizando cada tarea por pilar, desplegado en un formato que muestra información clave:
   - Agencia principal
   - Otras partes interesadas
   - Fecha de inicio
   - La duración estimada
   - El costo estimado

La Estrategia Nacional de Ciberseguridad es un documento "vivo", por lo que requiere que las partes interesadas lo revisen al menos cada uno o dos años para asegurar que se mantenga actualizada y reflejando el panorama mundial de ciberseguridad que se mantiene en constante evolución. En consecuencia, SIGCA recomienda a la AIG que haga una revisión anual de las acciones de esta Hoja de Ruta, y el estado de las tareas en los planes anuales de implementación al menos en forma trimestral (si es posible mensual). Este seguimiento de acciones internas es un proceso que debe ser ejecutado por la AIG, que es la Autoridad encargada de apoyar y supervisar las tareas asignadas a otras entidades. La realización de estas prácticas de revisión asegurará que el contenido de la Estrategia Nacional de Ciberseguridad sigue siendo actual y que las partes interesadas estén alcanzando los hitos establecidos y haciendo progreso hacia el logro de los objetivos críticos hacia una seguridad mejorada.

Pilar I: Proteger la privacidad y los derechos fundamentales de los ciudadanos en el ciberespacio

El primer pilar de la ENC refleja una prioridad nacional de que, aun cuando la ciberseguridad es un imperativo vital de seguridad nacional, debe respetar las libertades y derechos civiles fundamentales, incluido el derecho a la privacidad, tanto de las personas jurídicas y naturales en Panamá, siendo estos últimos residentes o visitantes temporales. Específicamente, este pilar sirve para apoyar la interpretación e implementación de la legislación nacional pasada para aprobación en 2019 (ver Ley No. 81 de 2019 sobre la Protección de los Datos Personales) para fortalecer en forma más eficaz la protección de la privacidad y de los datos personales.

Tareas a implementar:

1.1 Empoderar y brindar los recursos necesarios a la AIG para servir como el organismo de asesoría técnica y de acompañamiento en la implementación del marco regulatorio y las leyes de protección de datos personales de Panamá

1.1.1 Conceder a la Dirección Nacional de Ciberseguridad de la AIG los recursos necesarios

Mientras que la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI) es la entidad legalmente responsable por implementar la Ley No. 81 de 2019, es a la AIG a la cuál debe concedérsele la autoridad y recursos para proveer asesoría y supervisión técnica a la ANTAI. La AIG también será representada en el consejo de Protección a los Datos Personales, establecido bajo ley, para servir como el organismo de asesoría técnica, ayudando a interpretar la ley a las partes interesadas tanto en el sector público como privado.

1.1.2 Educación de las partes interesadas

Dotada de la autoridad adecuada para supervisar e interpretar la Ley No. 81, la AIG será responsable de llevar a cabo esfuerzos educativos, a través de el Instituto de Tecnología e Innovación (ITI) y la Dirección Nacional de Ciberseguridad,

para informar a las partes interesadas sobre el marco de trabajo, sus mandatos y su rol particular que jugará cada quien en la aplicación del mismo. Esto incluye el sector de gobierno, así como también las partes interesadas del sector privado, incluyendo, pero no limitándose a los Proveedores de Servicio de Internet (ISP por sus siglas en inglés).

1.1.3 Conducir revisiones con ANTAI y agencias de gobierno
Como parte de su rol de asesoría técnica y de supervisión, la AIG trabajará en estrecha coordinación y comunicación con ANTAI para asegurar la correcta implementación de la Ley No. 81. Adicionalmente, cada agencia de gobierno designará un líder de TI -con poder de toma de decisión- que servirá de punto de contacto con la AIG. La AIG conducirá revisiones periódicas con el líder de cada agencia de implementación para asegurar que se cumplan los objetivos y hacer ajustes según sea necesario. Durante el primer año de implementación se realizarán reuniones mensuales y trimestrales los años subsiguientes.

1.2 Identificar todos los conjuntos de datos de información personal

1.2.1 Llevar a cabo un proceso nacional de inventario de datos
Proteger la información personal requiere primero de saber dónde existe y después administrarla. La Ley No. 81 de 2019 requiere que todas las entidades mantengan un inventario de los sistemas de datos que contienen información personal con el fin de salvaguardarlos. La ANTAI supervisará este proceso, y la AIG en su rol de supervisión técnica, deberá hacer de esto un punto de referencia para evaluar el cumplimiento en forma trimestral junto con la ANTAI proveyendo asesoría y apoyo técnico cuando se necesite.

1.3 Promover la adopción de mejores prácticas para la privacidad de los datos y la protección de la propiedad intelectual (P.I.) a nivel de gobierno

1.3.1 Demostrar las mejores prácticas para la gestión de la información personal y la propiedad intelectual
La ley no sólo exige la adopción de buenas prácticas de protección de datos en todo el gobierno, sino que hacerlo en la práctica conducirá a un uso más ubicuo de estas prácticas en el sector comercial. Con ese fin, la Dirección Nacional de Ciberseguridad de la AIG trabajará con cada líder de TI de las agencias gubernamentales para garantizar que las protecciones de privacidad se pongan en marcha en cada oficina. La AIG también comunicará al sector privado las mejores prácticas para la gestión de datos personales y propiedad intelectual.

1.4 Promover y supervisar La Comisión Nacional de Protección de Datos de Menores

1.4.1 Apoyar las operaciones de La Comisión

La ENC hace mención explícita de la preocupación sobre la protección de los datos de los menores. Panamá reconoce que se trata de una parte de la población que es particularmente vulnerable y se requieren medidas adicionales para asegurar que los niños y adolescentes no sean explotados ni perjudicados. La AIG promoverá y supervisará a La Comisión Nacional de Protección de Datos de Menores. Trabajando en conjunto con otras agencias, incluyendo el Ministerio de Seguridad Pública y el Ministerio de Desarrollo Social, la AIG apoyará las operaciones de La Comisión, incluyendo la dotación de personal y reclutamiento, evaluación de políticas, creación e interpretación de leyes y cualquier otro apoyo técnico.

Pilar II: Disuadir y castigar la actividad criminal en el ciberespacio

El Pilar II se centra en la creciente amenaza y los costos de la ciberdelincuencia. Si bien ha habido avances hacia la aprobación de leyes más estrictas para reconocer, detener y enjuiciar más eficazmente la ciberdelincuencia –el uso ilícito de las TIC– aún no se ha aprobado un marco jurídico formal y, por lo tanto, no se está aplicando. Muchas entidades todavía no poseen la autoridad adecuada y las herramientas técnicas para luchar contra la ciberdelincuencia. Poner en movimiento el marco a través de la Asamblea Nacional de Panamá será la primera pieza crítica para disuadir y castigar más eficazmente la ciberdelincuencia.

Tareas a implementar:

2.1 Establecer un marco jurídico para proporcionar la autoridad y los recursos necesarios para combatir la actividad transnacional de ciberdelincuentes

2.1.1 Identificar defensores

Se ha desarrollado legislación y un marco jurídico que aumentaría significativamente la capacidad de Panamá para disuadir y enjuiciar la ciberdelincuencia, pero se ha estancado en la legislatura. La primera prioridad es aprobar el proyecto de ley. Es fundamental para su introducción y paso por la Asamblea Nacional de Panamá, la identificación de defensores que puedan expresar su apoyo a un marco jurídico más sólido. La Dirección Nacional de Ciberseguridad de la AIG desempeñará un papel principal en la organización de portavoces de agencias para que sirvan como validadores del marco, así como para proporcionar recursos como investigación y testimonios de expertos a la Asamblea Nacional según sea necesario.

No. 29434-A
Gaceta Oficial Digital, miércoles 15 de diciembre de 2021
7

2.1.2 Supervisar la implementación del marco jurídico

Una vez promulgada una versión de un marco jurídico sólido, la AIG será responsable de interpretarla y guiar la aplicación. La AIG dirigirá la coordinación con las partes interesadas nombradas dentro del plan, incluyendo el Fiscal Especial para Delitos contra la Propiedad Intelectual y la Seguridad de la Información y el Instituto de Medicina Legal y Ciencias Forenses (IMELCF), la investigación principal de la ciberdelincuencia, bajo la Dirección de Investigación Judicial. Se requerirá una revisión trimestral de cada entidad interesada, para informar de los progresos o impedimentos a la AIG de manera eficiente.

2.2 Dotar a los encargados de la aplicación de la ley y al sistema de justicia de las herramientas técnicas adecuadas

2.2.1 Realizar un análisis para determinar las herramientas técnicas y requerimientos adicionales para las fuerzas del orden y poder judicial

Además de otorgar autoridad jurídica más sólida en el marco jurídico aprobado por la Asamblea Nacional de Panamá, la policía y sus órganos subsidiarios, el Ministerio Público y el poder judicial también deben estar equipados con la formación adecuada, los instrumentos técnicos y las mejores prácticas para detectar actividades delictivas, llevar a cabo la vigilancia electrónica, retener datos, llevar a cabo investigaciones y presentar cargos criminales con prontitud, respetando al mismo tiempo la privacidad de los ciudadanos y las libertades civiles. La Dirección Nacional de Ciberseguridad de la AIG será responsable de entrevistar a cada uno de estos organismos para realizar un análisis que determine las herramientas técnicas y requerimientos adicionales para realizar estas funciones. La Dirección Nacional de Ciberseguridad de la AIG desarrollará un plan para su entrega oportuna.

2.2.2 Apoyar el entrenamiento y la difusión de mejores prácticas

La Dirección Nacional de Ciberseguridad de la AIG será responsable de identificar expertos que puedan impartir capacitación técnica a grupos de interesados relevante a la detección, investigación, disuasión y castigo de la ciberdelincuencia. Los proveedores externos pueden servir como formadores o desarrolladores de planes de estudio, sin embargo, la Dirección Nacional de Ciberseguridad de la AIG proveerá lineamientos a estos proveedores para asegurar que están haciendo uso de las mejores prácticas. Las agencias clave con las que hay que trabajar para impartir la capacitación incluyen agentes de las fuerzas del orden (sobre la recopilación de pruebas digitales, la retención de datos y las capacidades de gestión) y el IMELCF (para análisis forense y funcionarios legales, sobre interpretación y nuevas leyes).

2.2.3 Asegurar la protección y privacidad de los datos

Si bien este pilar se centra fundamentalmente en disuadir la ciberdelincuencia, se deben hacer consideraciones especiales para respetar los datos personales y las leyes de privacidad. Basado en el marco legal para la protección y privacidad de los datos personales aprobado en 2019, las fuerzas del orden público y los organismos judiciales deben cumplir estrictos parámetros jurídicos para la privacidad y la protección de las libertades civiles de los ciudadanos, personas jurídicas, naturales y visitantes temporales incluso cuando se están promulgando nuevos códigos penales. La Dirección Nacional de Ciberseguridad de la AIG, involucrará y educará a las partes interesadas pertinentes sobre los detalles de la ley No. 81 de 2019, descrita en el pilar anterior y lo incluirá como parte de sus revisiones mensuales y trimestrales con los líderes designados de TI en cada agencia individual. Se recomienda que AIG incluya el tema como parte de sus evaluaciones trimestrales con agencias individuales *(Véase la Tarea 1.1.3 para más detalles).*

2.3 Hacer obligatoria la notificación de ciertas violaciones graves de datos en el sector privado

2.3.1 Ordenar requisitos de notificación obligatoria por brechas de seguridad en los datos

La pronta denuncia de brechas de datos tanto en el sector gubernamental como en el privado es esencial para detener la ciberdelincuencia. A medida que se detectan brechas de seguridad en los datos, deben ser reportados a CSIRT Panamá - Equipo de Respuesta a Incidentes de Seguridad Cibernética de Panamá (en adelante CSIRT) para permitir un intercambio más efectivo y eficiente de información procesable entre el gobierno y la industria. Aunque actualmente pocas entidades están legalmente obligadas a informar, la Dirección Nacional de Ciberseguridad de la AIG desarrollará un arreglo sugerido para el reporte mandatorio de incidentes serios de brechas de datos, incluyendo aquellas que implican exposición de información personal, fugas y amenazas a las Infraestructuras Críticas.

2.3.2 Conducir una revisión legal

Es crítico entender en dónde debería ser un requerimiento legal o no, la notificación obligatoria para algunos sectores y para ciertos tipos de brechas de seguridad en los datos. A fin de efectivamente implementar un plan secuenciado para instituir los requerimientos de una notificación obligada (ver Tarea 2.3.1). La AIG conducirá una revisión legal para identificar en dónde la legislación o las leyes son deficientes en este aspecto, y dónde necesitarían cambiarse en el futuro para ayudar a su cumplimiento.

2.4 Continuar coordinando el involucramiento con entidades regionales e internacionales

2.4.1 Mejorar la coordinación entre el CSIRT de Panamá y otros CSIRT nacionales dentro de la Organización de Estados Americanos (OEA)

Como la mayoría de los crímenes cibernéticos se originan fuera del país y tienen un impacto mucho más allá de las fronteras de una nación, el intercambio de inteligencia cibernética entre Panamá y sus vecinos es vital en la detección, disuasión y procesamiento de la ciberdelincuencia. Una continua y fuerte relación entre CSIRT-Panamá y sus contrapartes en otras naciones mejorará las capacidades de todas las partes y permitirá a cada uno beneficiarse de la inteligencia de otros. La Dirección Nacional de Ciberseguridad de la AIG desarrollará un plan de implementación para encontrar nuevas formas de coordinación entre CSIRT Panamá y otros CSIRT nacionales dentro de los Estados miembros de la OEA.

2.4.2 Alinear las leyes cibernéticas de Panamá con tratados y acuerdos internacionales

En 2014, Panamá ratificó la Convención de Budapest, el primer tratado internacional que busca abordar la ciberdelincuencia armonizando las leyes nacionales, mejorando las técnicas de investigación y aumentando la cooperación entre las naciones. Panamá también ha firmado acuerdos bajo la Convención de las Naciones Unidas contra el Crimen Organizado Transnacional. Moviéndose hacia adelante, la AIG llevará la delantera en una revisión legal para asegurar que las leyes de Panamá están apropiadamente alineadas con acuerdos internacionales donde Panamá es signataria. Basado en esta revisión, la AIG hará recomendaciones a la Asamblea Nacional de Panamá sobre cualquiera de las brechas que necesiten ser abordadas a través de una futura legislación o desarrollo de un marco de trabajo legal.

2.4.3 Participar en ejercicios y foros globales para desarrollar la capacidad interna para luchar contra la ciberdelincuencia y el ciberterrorismo

En un esfuerzo por mejorar la coordinación y cooperación internacional, la Dirección Nacional de Ciberseguridad de la AIG incorporará ideas en su plan de implementación (ver Tarea 2.4.1) para aumentar la participación de Panamá en foros internacionales, debates y ejercicios de capacitación, así como con asociaciones multinacionales que promuevan el uso de las TIC y los estándares de ciberseguridad. Los órganos de participación deben incluir como una sugerencia inicial - pero no limitándose solo a estos-, a la Convención Europea sobre Ciberdelincuencia, el Foro de Equipos de Respuesta a Incidentes y Seguridad (FIRST) y el Comité Interamericano contra el Terrorismo (CICTE) de la OEA.

Pilar III: Fortalecer la seguridad y resiliencia de la infraestructura crítica de Panamá

El tercer pilar aborda los requisitos técnicos (tecnología, herramientas, protocolos y mejores prácticas) necesarios para proteger los datos y las redes vinculadas a las Tecnologías de Información y Comunicaciones (TIC) e Infraestructuras Críticas (IC) en Panamá. Al ejecutar estas tareas, el Gobierno Nacional de Panamá estará mejor posicionado para detectar amenazas y prevenir ciberataques en sus respectivos sistemas, así como para realizar procesos de respuesta y recuperación en caso de que ocurra un incidente. Estas tareas se basan en gran medida en la evaluación de alto nivel de CGA de la preparación para la ciberseguridad del gobierno nacional de Panamá medida con el Centro de Controles de Seguridad en Internet (CIS), un estándar aceptado a nivel mundial. *Véase el Apéndice A para obtener una lista de los 20 controles* del CIS.

Tareas a implementar:

3.1 Dotar de recursos y empoderar a La Dirección Nacional de Ciberseguridad dentro de la AIG, para liderar los esfuerzos de respuesta y resiliencia de las TIC del Estado, incluyendo sus Infraestructuras Críticas

3.1.1 Desarrollar una nueva estructura de gobernanza organizacional para llevar a cabo la misión de proteger las TIC y las Infraestructuras Críticas
Con el objetivo de efectivamente llevar a cabo operaciones asociadas a la protección de las Infraestructuras Críticas, es vital conceder y consolidar la autoridad adecuada a una oficina central que pueda supervisar la entera misión de proteger las TIC e Infraestructuras Críticas y servir como un punto de contacto para todas las partes interesadas. Como actualmente, esta dirección centralizada no existe, la AIG dotará de recursos y empoderará a la nueva dirección (La Dirección Nacional de Ciberseguridad), y asignarle responsabilidades dentro de sus propias funciones y las ya existentes dentro del CSIRT-Panamá que llegaría a ser parte de esta nueva dirección, La Dirección Nacional de Ciberseguridad de la AIG.

3.1.2 Desarrollar un plan nacional para las Infraestructuras Críticas
La Dirección Nacional de Ciberseguridad de la AIG asumirá el liderazgo en esculpir un plan nacional para las Infraestructuras Críticas, que deberá incluir al menos la designación o "nombramiento" de todas las Infraestructuras Críticas de la nación, evaluando la postura de seguridad de cada sector individual de estas Infraestructuras Críticas y después desarrollando planes para priorizar la seguridad de las infraestructuras de estos sectores (ver Tarea 3.2).

3.1.3 Conducir una evaluación de cada sector de Infraestructuras Críticas y agencias de gobierno relevantes
Las agencias de gobierno varían grandemente de una a otra en términos de recursos, capacidades, limitaciones y riesgo. Algunas podrían estar más evolucionadas o sofisticadas en sus capacidades, mientras que otras aún están evolucionando.

Al mismo tiempo, cada agencia encara un nivel diferente de riesgo. La protección de las Infraestructuras Críticas depende de saber estas limitaciones y priorizar acciones en las agencias en una forma que aborde de primero las necesidades más grandes y los riesgos más grandes. Con el objetivo de facilitar la planificación, la Dirección Nacional de Ciberseguridad de la AIG apoyará a los líderes designados de IT de cada agencia de gobierno a medida que estos llevan a cabo una evaluación cualitativa de su agencia para entender mejor su postura en ciberseguridad, madurez y necesidades. Este proceso cualitativo abarcará evaluar factores como recursos, personal, tecnología y otras facetas que contribuyan a la protección de las Tecnologías de Información y Comunicaciones (TIC) y de las Infraestructuras Críticas (IC). También medirá a cada agencia contra el top 20 de los controles del Centro para la Seguridad en el Internet (CIS por sus siglas en inglés - ver Apéndice A). Complementando con una evaluación cuantitativa del ciber-riesgo para ser llevada a cabo según la Tarea 3.2.1, las evaluaciones proporcionarán un mejor panorama de cómo y dónde estratégicamente, el gobierno debería enfocarse.

3.1.4 Dirigir al gobierno en materia de guía para configuraciones seguras

Actualmente, no existen estándares de configuración para todo el gobierno. Muchas organizaciones gubernamentales informaron sobre el uso de configuraciones estándar sugeridas del fabricante o que intentaron desarrollar su propia configuración -algo que debería confirmarse a través de la evaluación a llevar a cabo según la Tarea 3.1.3. Inconsistencia en el uso de esto, significará que se están incurriendo en prácticas duplicadas, y disminuyen la seguridad de la red del gobierno en general. La Dirección Nacional de Ciberseguridad de la AIG será responsable de eliminar estos puntos de preocupación mediante la implementación de directrices de configuración en todo el gobierno para todo el hardware y software. La Dirección Nacional de Ciberseguridad de la AIG realizará un esfuerzo continuo y constante en la investigación de mejores prácticas y desarrollar la orientación, en colaboración con organizaciones y expertos regionales y globales.

3.1.5 Implementar la inteligencia cibernética y el intercambio de la información de amenazas

La Dirección Nacional de Ciberseguridad de la AIG tendrá la autoridad para implementar una nueva misión de inteligencia cibernética e intercambio de información de amenazas, lo que le permitirá publicar información crítica y mitigaciones tanto para el sector público como para el privado. Actualmente, CSIRT ha sido alimentado de inteligencia e información de amenazas para el sector gubernamental panameño, pero se alentará a las entidades del sector privado a participar más activamente con CSIRT *(véase la Tarea 4.4.1),* especialmente sobre informes de incidentes, que serán obligatorios en todo el sector privado para ciertos tipos de infracciones graves en un plazo de tres años para lograr este objetivo (*véase la Tarea2.3.1*).

3.1.6 Suscribirse a *The CyberWire*

La Dirección Nacional de Ciberseguridad de la AIG fomentará la suscripción a todo el gobierno a "The CyberWire", una publicación diaria gratuita que presenta información útil como amenazas cibernéticas comunes y malware, mitigaciones y oportunidades de colaboración.

3.1.7 Identificar oportunidades de automatización de la higiene cibernética

La Dirección Nacional de Ciberseguridad de la AIG proporcionará apoyo a todas las agencias gubernamentales para identificar los procesos y procedimientos (como los de los 20 Controles del Centro para la Seguridad del Internet CIS – ver Apéndice A), que puedan ser automatizados. Trimestralmente, La Dirección Nacional de Ciberseguridad de la AIG involucrarán a los líderes de TI y ciberseguridad en las agencias gubernamentales (*véase la Tarea 1.1.3)* para discutir, entre otros puntos, el progreso en la implementación de prácticas de automatización.

3.1.8 Implementar un programa de cacería de amenazas en todo el gobierno

Estando pendiente por conducir las evaluaciones de ciberseguridad según la Tarea 3.1.2, la Dirección Nacional de Ciberseguridad de la AIG trabajará con los líderes de TI en agencias gubernamentales seleccionadas para crear un plan para implementar un programa de "cacería de amenazas" dentro de las redes y centros de datos de la agencia. Este programa está dirigido a la creación de capacidad de detección a más largo plazo a nivel de agencia y ayudará a las organizaciones gubernamentales a abordar las amenazas internas, así como al adversario sofisticado que opera en las redes.

3.1.9 Explorar la creación y/o utilización de un SOC para las agencias gubernamentales seleccionadas

Para mejorar la capacidad de defender las redes y responder a incidentes cibernéticos a nivel de agencia, la Dirección Nacional de Ciberseguridad de la AIG utilizará los hallazgos derivados de la evaluación de ciberseguridad (ver Tarea 3.1.3) y la cuantificación del ciber-riesgo (ver Tarea 3.2.1) para recomendar la selección de agencias gubernamentales para la creación de su propio Centro de Operaciones de Seguridad (SOC), definido como un complejo que opera 24x7x365 que a su vez alberga un equipo de personas de seguridad de la información responsables de monitorizar y analizar de manera continua la postura de seguridad de una organización. Para las agencias en donde un SOC independiente no es posible debido a la limitante de recursos o capacidades – o simplemente porque tienen una prioridad más baja - la Dirección Nacional de Ciberseguridad de la AIG recomendará a dichas agencias que estos servicios sean provistos por la misma Dirección Nacional de Ciberseguridad de la AIG o bien que los tercericen con un proveedor de ciberseguridad.

3.1.10 Automatizar instalación de parches

La automatización ayuda a minimizar el tiempo que los equipos de TI deben dedicar a la aplicación de parches, lo que permite a los operadores la capacidad de centrarse en las tareas críticas de supervisión y defensa de las redes. Algunas agencias gubernamentales actualmente tienen capacidades automatizadas de aplicación de parches de sistemas y aplicaciones. Para aquellos que no lo hacen, la Dirección Nacional de Ciberseguridad de la AIG proveerá guía y recomendaciones sobre cómo abordar la implementación de un sistema automatizado de parches. Tal y como las Tareas anteriores, el parchado automatizado debería ser implementado con prioridad, tomando en consideración a las

organizaciones de más alto riesgo y equilibrando las necesidades con las capacidades que estas tengan según se determine en la Tarea 3.1.3.

3.1.11 Desarrollar un programa de detección de cambios

Una de las formas más efectivas de detectar una intrusión en las redes es rastrear anomalías en la red, ya que los intrusos deben alterar archivos, elevar sus permisos, insertar ejecutables, etc. En las agencias gubernamentales con funciones en la protección de las Tecnologías de Información y Comunicaciones y las Infraestructuras Críticas, la Dirección Nacional de Ciberseguridad de la AIG desarrollará un programa de detección de cambios monitoreado que se planificará e implementará como parte de desarrollar conciencia de la situación actual y del programa de cacería de amenazas descrito en la *Tarea 3.1.8*.

3.2 Realizar análisis de riesgos y desarrollar planes de contingencia para todos los sectores de Infraestructuras Críticas

3.2.1 Realizar análisis de riesgos

De forma similar a la evaluación de ciberseguridad que se conducirá para determinar las capacidades cibernéticas de las agencias de gobierno (ver Tarea 3.1.3), la Dirección Nacional de Ciberseguridad de la AIG también será responsable de llevar a cabo un análisis cuantitativo del ciber-riesgo para todos los sectores designados como Infraestructuras Críticas (IC). Un proceso que ayuda a identificar y evaluar amenazas potenciales que podrían afectar la integridad de las IC, estos análisis cuantitativos del ciber-riesgo determinarán la asignación de prioridad y el desarrollo de los planes de contingencia con respecto a cómo medir, mitigar y controlar las amenazas cibernéticas eficazmente.

3.2.2 Desarrollar planes de contingencia

Siguiendo con la iniciativa del análisis de riesgo en la Tarea 3.2.1, la Dirección Nacional de Ciberseguridad de la AIG liderará el esfuerzo de desarrollar un plan básico de contingencia y recuperación para cada sector de las Infraestructuras Críticas (IC).

3.3 Implementar normas obligatorias de ciberseguridad e "higiene cibernética" para las agencias gubernamentales

3.3.1 Educar a las agencias gubernamentales y a las organizaciones de IC sobre los controles de CIS y las estrategias de implementación

La Dirección Nacional de Ciberseguridad de la AIG liderará un esfuerzo para educar a los líderes de TI de las agencias gubernamentales sobre la importancia de la higiene cibernética, a saber, el despliegue de los controles de CIS *(véase* el Apéndice A). Los Controles de CIS son un conjunto de acciones prioritarias reconocidas internacionalmente que constituyen colectivamente la base de la higiene cibernética básica y han demostrado poder prevenir el 80-90% de los ciberataques conocidos y más peligrosos del mundo contra las TIC. Actúan como un modelo para que los operadores de red mejoren la ciberseguridad mediante la identificación de acciones específicas que deben realizarse en un orden prioritario.

Controles de CIS (Grupos de Implementación)[1]

[1] Referencia: https://www.cisecurity.org/blog/v7-1-introduces-implementation-groups-cis-controls/

3.3.2 Ayudar a las agencias a llevar a cabo acciones del Grupo de implementación 1
Si bien el conjunto completo de controles de CIS incluye 171 subcontroles totales en 20 controles, la aplicación de un sub-control determinado debe basarse en el riesgo de la organización y sus capacidades, a saber, la sensibilidad y la criticidad de sus actividades, la experiencia de su personal y los recursos disponibles. Como mínimo, todos los organismos tendrán que implementar el Grupo de Aplicación de Controles 1, higiene cibernética básica, que consta de 43 subcontroles. En un plazo de 18 meses, todos los organismos implementarán el Grupo de Aplicación de Controles 1. La Dirección Nacional de Ciberseguridad de la AIG ayudará a los organismos en la implementación del Grupo 1 de los Controles según sea necesario.

3.3.3 Ayudar a los organismos a determinar si proceden con el Grupo de Implementación 2 y el Grupo 3
Algunas agencias mantienen datos o llevan a cabo operaciones que requerirán más que prácticas de higiene cibernética. La Dirección Nacional de Ciberseguridad de la AIG trabajará con cada agencia (es decir, el líder de TI de cada agencia que servirá de punto de contacto principal) para determinar cuáles de los tres grupos de implementación son apropiados para ellos, respectivamente. Más allá de la educación sobre los controles, La Dirección Nacional de Ciberseguridad de la AIG trabajará con cada organismo gubernamental para supervisar e implementar las medidas prescritas en los controles en su orden priorizado y secuenciado.

La siguiente explicación describe el procedimiento cronológico en el que deben completarse estos controles:

1 Inventario y control de activos de hardware
Usar el inventario actual de cada agencia gubernamental de servidores autorizados como punto de partida; los equipos de TI de cada agencia llevarán a cabo un inventario de todos los activos de hardware de cada red. A partir de ahí, habrá que determinar qué dispositivos están autorizados a estar en la red y cuáles no, posteriormente, "desconectar" aquellos que no están permitidos. Las agencias seguirán utilizando un rastreador de activos para mantener actualizado el inventario de hardware.

2 Inventario y control de activos de software
Cada agencia llevará a cabo un inventario de todo el software en sus respectivas redes. Los líderes de TI determinarán qué software está autorizado a ejecutarse en la red y desinstalará cualquier otro software que no esté autorizado. Al igual que en la Tarea 3.3.2, en el futuro, las agencias utilizarán un rastreador de activos para mantener el inventario actualizado.

3 Gestión continua de vulnerabilidades
Los líderes TI de las agencias serán responsables de crear un proceso para realizar un seguimiento y tomar medidas (al menos mensualmente) en la evaluación y remediación de vulnerabilidades publicadas para los dispositivos/software en las obras netas de cada Ministerio/Agencia.

4 Uso controlado de privilegios administrativos
Cada agencia debe identificar quién tiene privilegios de administrador en las redes. A continuación, será necesario crear una política que defina a quién se le permite tener estos privilegios, señalando que los privilegios deben limitarse a un mínimo y que la función de asignar privilegios debe centralizarse para mantener el control.

5 Configuración segura para hardware y software en dispositivos móviles, portátiles, estaciones de trabajo y servidores
Cada agencia configurará cada dispositivo, portátil, estación de trabajo y servidor y software asociado en cada red en la configuración más segura posible. Dentro de este proceso, los líderes de TI deben usar la política actual y los procedimientos aprobados para implementar estas configuraciones.

6 Mantenimiento, monitoreo y análisis de registros de auditoría
Todas las agencias gubernamentales deberán desarrollar un proceso estructurado y metódico para crear y revisar los registros de auditoría para cualquier entrada anómala. Este proceso debe aplicarse de forma continuada.

7 Protección de correo electrónico y navegador web
Muchos, y tal vez la mayoría, de ataques cibernéticos hoy en día ocurren a través de correos electrónicos de phishing y sitios web falsos. Los líderes de TI de la Agencia revisarán, crearán e implementarán políticas y procedimientos para el uso de correo electrónico y navegadores web para garantizar que estos sistemas estén protegidos.

8 Defensas de malware
CSIRT desplegará herramientas de identificación de malware en cada ministerio o agencia y evaluará cada trimestre cómo se utilizan.

9 Limitación y control de puertos de red, protocolos y servicios
La Dirección Nacional de Ciberseguridad de la AIG trabajará con cada agencia para hacer una auditoría de sus respectivos puertos de red. A continuación, la agencia cerrará cualquier puerto que no tenga una razón válida o autorizada para estar abierto.

10 Capacidades de recuperación de datos
La Dirección Nacional de Ciberseguridad de la AIG trabajará con cada agencia para revisar sus planes, procedimientos y prácticas de recuperación de datos. Cada agencia creará un cronograma y ejercerá/ensayará la recuperación de datos.

11 Configuraciones seguras para dispositivos de red, como firewalls, enrutadores y conmutadores
La Dirección Nacional de Ciberseguridad de la AIG trabajará con cada agencia inspeccionar la configuración actual de todos los firewalls, routers y switches para asegurarse de que cada dispositivo está configurado en su configuración más segura.

12 Defensa de perímetro
El "perímetro" se define como el punto donde la infraestructura de red de una agencia toca Internet. La Dirección Nacional de Ciberseguridad de la AIG trabajará con cada agencia para realizar un análisis pasivo y la revisión de sus arquitecturas actuales para comprender mejor dónde existen todos los bordes de la red para que puedan protegerse de la manera más segura posible. Si es necesario, cada agencia podrá necesitar volver a diseñar, con el fin de minimizar el número de bordes que deben ser defendidos.

13 Protección de datos
A medida que se implementan medidas de higiene cibernética, la protección de los datos críticos es un elemento esencial. La Dirección Nacional de Ciberseguridad de la AIG trabajará con cada agencia para revisar y evaluar la arquitectura de cada agencia para la gestión de datos, incluido el

cifrado. La Dirección Nacional de Ciberseguridad de la AIG entonces trabajará con la agencia para determinar si esa arquitectura es segura, puede ser segura, o si necesita hacer una nueva arquitectura – y tomará las medidas apropiadas basadas en los resultados de ese proceso de revisión.

14 Acceso controlado con base en la necesidad de conocimiento
El monitoreo y control de cuentas es un componente crucial de la higiene. Cada agencia, con el apoyo de la Dirección Nacional de Ciberseguridad de la AIG será necesaria para crear e implementar la política de acceso, incluida la autenticación basada en el usuario y multi-factor según las mejores prácticas utilizadas por la industria. Cada agencia debe evaluar el acceso que permite a los proveedores, a quienes no se les debe dar acceso ilimitado a sistemas, redes y datos.

15 Control de acceso inalámbrico
El acceso inalámbrico es una vulnerabilidad crítica, especialmente si no está diseñado, implementado, controlado, monitoreado y defendido adecuadamente. Para ello, los líderes de TI de la agencia deberán revisar la arquitectura inalámbrica de su agencia y asegurarse de que se pongan en marcha controles de red adecuados para las ubicaciones que utilizan el acceso inalámbrico.

16 Monitoreo y control de cuentas
Cada agencia administrará activamente el ciclo de vida de las cuentas de sistema y aplicación (su creación, uso, latencia y eliminación) con el fin de minimizar las oportunidades para que los atacantes las aprovechen para aprovecharlas.

17 Implementar un programa de sensibilización y capacitación en seguridad
A medida que las necesidades de ciberseguridad crezcan en todo el gobierno, será necesario incorporar a nuevo personal que entiendan la higiene cibernética, así como seguir manteniendo buenos empleados que son el guardián del conocimiento institucional. En este sentido, cada agencia deberá identificar la experiencia y los conjuntos de habilidades específicos que necesita el personal de TI y el ciber personal para implementar una buena higiene de la red. Estos conjuntos de habilidades y experiencia identificados servirán como guía de contratación para determinar qué roles deben cumplirse y con qué conjuntos de habilidades. Si no es posible contratar directamente personal con el conjunto de habilidades adecuado, entonces las agencias deben utilizar los programas de capacitación del Instituto de Tecnología e Innovación de la AIG para las nuevas contrataciones para darles los conocimientos necesarios.

18 Seguridad del software de aplicación
La Dirección Nacional de Ciberseguridad de la AIG trabajará con cada agencia para difundir información sobre las mejores prácticas de la industria para el desarrollo de software seguro. Para las agencias que desarrollan aplicaciones internamente, la Dirección Nacional de Ciberseguridad de la AIG trabajará para asegurar que el personal haya recibido la capacitación adecuada. En caso de que se externalice el desarrollo de las aplicaciones, las agencias deben dictar que las normas de desarrollo seguras formen parte del acuerdo contractual.

19 Respuesta y gestión de incidentes
Todas las agencias deben revisar sus respectivos Planes de Respuesta a Incidentes. En este proceso deben asegurarse de que las funciones y responsabilidades se delineen cuidadosamente, que se articule el papel de la administración y se explique explícitamente la coordinación (con quién, cuándo y cómo). Si esta documentación no existe, el CSIRT trabajará con la agencia para desarrollarla. El CSIRT también trabajará con las agencias para revisar sus planes actuales de respuesta a incidentes, según sea necesario. El CSIRT se asegurará de que cada agencia ejerza/practique su Plan de Respuesta a Incidentes.

20 **Pruebas de penetración y ejercicios de equipo rojo**
La Dirección Nacional de Ciberseguridad de la AIG trabajará con cada agencia gubernamental para desarrollar un plan estructurado para las pruebas de penetración ("*Pen Testing*"). Dentro de este plan, la agencia debe esbozar las metas y quién, qué, cuándo, dónde y cómo asegurarse de que las pruebas de pluma no interfieran con las operaciones y se hagan con un propósito. La frecuencia de las pruebas de penetración queda a discreción del organismo, pero debe establecerse en consulta con La Dirección Nacional de Ciberseguridad de la AIG.

3.4 Proporcionar guía y asesoría al sector privado para mejorar su postura de ciberseguridad

3.4.1 Crear intercambio de información de amenazas para entidades del sector privado
En el marco de la *Tarea 4.4.1*, la Dirección Nacional de Ciberseguridad de la AIG alentará a las entidades del sector privado que aún no están involucradas, a involucrarse más con la Dirección Nacional de Ciberseguridad de la AIG, utilizándola como centro para compartir inteligencia cibernética, intercambio de información sobre amenazas y mejores prácticas entre el gobierno y entidades similares dentro de su industria. Algunos sectores ya están realizando esto, pero es *ad hoc* (voluntariamente) y no una base formal.

3.4.2 Proporcionar estándares de higiene cibernética al sector privado
La Dirección Nacional de Ciberseguridad de la AIG difundirá información sobre higiene cibernética, específicamente sobre los Controles de CIS. Según sea necesario, también podrá proporcionar capacitación a los miembros del sector privado.

3.4.3 Exigir el incremento paulatino de las notificaciones de los ciberataques en el sector privado
Como se ha establecido, informar de un ciberataque o incidente cuando este ocurre es fundamental para proteger a otros, para detener la ciberdelincuencia y para salvaguardar las Infraestructuras Críticas (IC). En el marco de la *Tarea 2.3.1*, se requerirá la notificación de ciertos tipos de incidentes cibernéticos del sector privado en un plazo de tres años. Aunque actualmente pocas industrias del sector privado están legalmente obligadas a reportar cualquier tipo de incidente, el Gobierno de Panamá deberá comenzar a requerir informes obligatorios de ciertos tipos de incidentes, a saber, aquellos que implican compromiso de datos personales o aquellos que representan serias amenazas para las IC.

3.5 Aprovechamiento de los socios internacionales y las oportunidades para construir capacidad

3.5.1 Aumentar la participación mundial
Panamá puede desarrollar sus propias habilidades de ciberseguridad y capacidad para proteger la IC aprendiendo de socios globales y expertos de todo el mundo. A través de una mayor inteligencia cibernética y prácticas de intercambio de amenazas con aliados internacionales, Panamá también puede prepararse mejor para los ataques que se originan fuera

de sus fronteras. Para tal fin, la Dirección Nacional de Ciberseguridad de la AIG servirá como una representante nacional en eventos regionales y mundiales que mejoran la colaboración. Específicamente, esto implica identificar una lista de conferencias internacionales de ciberseguridad, ejercicios multinacionales y otras experiencias de colaboración (Tarea*2.4.3*). La Dirección Nacional de Ciberseguridad de la AIG también desarrollará un lugar formal para reforzar la coordinación con otros CSIRT nacionales dentro de la Organización de los Estados Americanos (*Tarea 2.4.1*) y explorará la participación en la ISO, la Organización Internacional de Normalización.

Pilar IV: Fomentar una cultura nacional de ciberseguridad

El pilar final abarca los componentes culturales y sociales críticos para la ENC, aquellos elementos humanos como la educación, la formación, la innovación, el trabajo y la vigilancia personal que contribuyen colectivamente a un ciberespacio más seguro para todos. Con el tiempo, los ciudadanos vienen a desarrollar un hábito de ciberseguridad en su propia vida diaria, pero inicialmente buscan a su gobierno para crear esta conciencia cultural. El pilar final de la ENC revisada aborda las tareas que el gobierno debe emprender para construir una cultura nacional de ciberseguridad, en la que todos participen tanto en la responsabilidad como en los beneficios.

Tareas a implementar:

4.1 Priorizar el desarrollo y entrenamiento de la fuerza laborar y sus habilidades

4.1.1 Crear un marco de desarrollo de la fuerza de trabajo cibernética

Una fuerza de trabajo de ciberseguridad es un activo estratégico que protege a la nación. Sin embargo, al igual que muchas otras naciones, Panamá tiene el reto de reclutar y mantener una fuerza de trabajo que pueda realizar operaciones cibernéticas cada vez más sofisticadas dentro de su propio dominio. Para aquellos con talento, el gobierno simplemente no es tan lucrativo como trabajar para una empresa del sector privado. Para hacer frente a esta escasez de capital humano, la Dirección Nacional de Ciberseguridad de la AIG será responsable de crear e implementar un plan (un "Marco de Desarrollo de la Fuerza Laboral Cibernética") para cubrir las vacantes críticas de mano de obra en todas las agencias del gobierno nacional. El plan detallará los procesos y procedimientos para todos los aspectos del desarrollo de la fuerza de trabajo: la contratación, incorporación, capacitación y certificación, retención y movilidad de los empleados. Existen varios recursos para ayudar en este proceso, incluyendo la Iniciativa Nacional para la Educación y Marco de Trabajo de Ciberseguridad de los Estados Unidos (Marco NICE).

4.1.2 Desarrollar y ampliar programas de formación acreditados en asociación con colegios y universidades

Una formación completa garantiza que un empleado pueda realizar su trabajo al más alto nivel. También ayuda con la retención, ya que da a los empleados una sensación de enriquecimiento personal y la inversión en la misión. Con el fin

de capacitar y equipar a la fuerza de trabajo cibernética del gobierno nacional, la Dirección Nacional de Ciberseguridad de la AIG liderará el desarrollo de un plan de estudios de capacitación acreditado (dentro del Marco de Desarrollo de la Fuerza Laboral Cibernética) adaptado a las habilidades necesarias para ejecutar las operaciones de ciberseguridad gubernamental. Este plan debe involucrar adecuadamente al sector privado y académico, sobre la construcción de modelos exitosos que existen en el país ahora, como, por ejemplo, el grado de maestría en seguridad informática de la Universidad Tecnológica de Panamá.

4.1.3 Desarrollar un plan de reclutamiento y retención

Encontrar y mantener el talento cibernético son dos preocupaciones distintas que un marco de desarrollo de la fuerza de trabajo debe abordar estratégicamente. Es un desafío para el gobierno atraer al talento, conscientes de que los empleos son mejor pagados en el sector privado, y es difícil mantenerlos trabajando para las instituciones de gobierno si los beneficios no coinciden con los ofrecidos por el sector privado. En este sentido, la Dirección Nacional de Ciberseguridad de la AIG debe incorporar programas de incentivos en su Marco de Desarrollo de la Fuerza Laboral Cibernética, considerando las mejores prácticas globales para reclutar y retener a la fuerza de trabajo cibernético en ideas como becas para la educación continua con cláusulas de retención para un período de tiempo específico y vías para ascensos. Debe examinar las instituciones académicas como recursos de la cartera de capital humano, así como asociaciones profesionales de ciberseguridad. Este plan de reclutamiento y retención estará dentro del marco de desarrollo de una fuerza laboral más grande, pero debe desarrollarse en consulta con otros organismos gubernamentales, académicos e intereses del sector privado.

4.1.4 Promover asociaciones profesionales de ciberseguridad en Panamá

La Dirección Nacional de Ciberseguridad de la AIG fomentará el crecimiento y la expansión de las organizaciones profesionales de ciberseguridad en el país. Los clubes y asociaciones formales e informales pueden ser una fuente de talento cibernético y pueden ayudar con la publicidad y el reclutamiento para las vacantes del gobierno.

4.2 Promover iniciativas que fomenten una cultura de ciberseguridad

4.2.1 Lanzar y ampliar un programa piloto de primaria y secundaria

La AIG, en coordinación con el Ministerio de Educación desarrollará una campaña formal a nivel nacional, "Ciber escuelas", para incorporar buenas prácticas de higiene de ciberseguridad en los planes de estudio de primaria y secundaria. El contenido del curso será desarrollado por el Ministerio de Educación, o puede ser desarrollado por proveedores externos con la supervisión de la Dirección Nacional de Ciberseguridad de la AIG. El primer año de la iniciativa puede limitarse a un pequeño programa piloto en un número selecto de escuelas. Dentro de tres años, se podría extender a todas las escuelas primarias y secundarias en todo el país.

4.3 Incentivar la innovación cibernética

4.3.1 Desarrollar un plan de Investigación y Desarrollo en ciberseguridad para aprovechar las ideas e innovación del sector privado

La capacidad de Panamá para mantenerse al día con la evolución de las amenazas cibernéticas depende en gran medida de su capacidad para innovar y mantenerse un paso adelante de los actores nefastos en el ciberespacio. En ese sentido, el gobierno desempeña un papel vital en el subsidio, la incentivación y la promoción de la investigación y el desarrollo (I+D) en todos los sectores, incluidas las TIC, para ser comisionado y supervisado por la Dirección Nacional de Ciberseguridad de la AIG, un grupo de trabajo compuesto por líderes gubernamentales, y expertos del sector privado e investigadores académicos se encargarán de desarrollar un plan de Investigación y Desarrollo de Ciberseguridad (I+D) centrado en la participación y aprovechando a las partes interesadas en la comunidad de I+D.

4.4 Promover la sensibilización, el compromiso y la acción del sector privado

4.4.1 Fomentar el compromiso del sector privado con la Dirección Nacional de Ciberseguridad de la AIG y el CSIRT

En virtud de esta nueva Estrategia Nacional de Ciberseguridad, todos los organismos de todo el gobierno nacional deberán adoptar normas y directrices básicas para la ciberseguridad dentro de su organización. La implementación será la responsabilidad primaria de los líderes de TI y Ciberseguridad en cada agencia. En el sector privado, la Dirección Nacional de Ciberseguridad de la AIG también dirigirá la divulgación para difundir y fomentar el uso de las mismas normas. A través de la Dirección Nacional de Ciberseguridad de la AIG, las entidades del sector privado también podrán comunicarse con otras entidades del sector privado sobre la inteligencia cibernética y el intercambio de información sobre amenazas. Para obtener más información, consulte *las tareas 3.4.1 y 3.4.2*.

4.4.2 Expandir la campaña "Deténgase. Piense. Conéctese."

En 2013, Panamá se unió a "Deténgase. Piense. Conéctese." (Stop. Think. Connect.), una campaña internacional de sensibilización pública destinada a aumentar la comprensión de las amenazas cibernéticas y empoderar al público para que sea más seguro y seguro en línea. Este programa está desempeñando un papel para promover buenas prácticas en línea, inculcando una noción nacional de que la ciberseguridad es responsabilidad de todos. Al mismo tiempo, la participación de Panamá es un gesto importante para unirnos en la lucha contra la ciberdelincuencia con nuestros aliados globales. La AIG impulsará la participación en este programa, para cumplir con las actividades que se derivan de este.

Pilar I: Proteger la privacidad y los derechos fundamentales de los ciudadanos en el ciberespacio

		Entidad Responsable	Otros involucrados	Año para comenzar	Duración estimada	Costo estimado
1.1	**Empoderar y brindar los recursos necesarios a la AIG para servir como el organismo de asesoría técnica y de acompañamiento en la implementación del marco regulatorio y las leyes de protección de datos personales de Panamá**					
1.1.1	Conceder a la Dirección Nacional de Ciberseguridad de la AIG los recursos necesarios	La AIG	ANTAI	2020	12 - 24 meses	40 - 75 nuevas personas para la Dirección Nacional de Ciberseguridad en la AIG $ 83,500 / $ 126,000 por mes 40 y 75 personas respectivamente

1.1.2	Educación de las partes interesadas	AIG	Direcciones y Comisiones dentro de la AIG, Instituto de Tecnología e Innovación (ITI), otras agencias y el sector privado	2020	1 año	$50,000
1.1.3	Conducir revisiones con ANTAI y agencias de gobierno	AIG	Direcciones y Comisiones dentro de la AIG, líderes de TI de otras agencias	2020	1 año	Ver 1.1.1
1.2	**Identificar todos los datos personales e información**					
1.2.1	Llevar a cabo un proceso nacional de inventario de datos	AIG, ANTAI	Todas las agencias	2021	1 año	Ver 1.1.1
1.3	**Promover la adopción de mejores prácticas para la privacidad de los datos y la protección de la propiedad intelectual (P.I.) a nivel de gobierno**					
1.3.1	Demostrar las mejores prácticas para la gestión de la información personal y la propiedad intelectual	Dirección Nacional de Ciberseguridad en la AIG	Los líderes de TI de todas las agencias	2021	En curso	Ver 1.1.1
1.4	**Promover y supervisar La Comisión Nacional de Protección de Datos de Menores**					

1.4.1	Apoyar las operaciones de La Comisión	AIG, MIDES	MINSEG, MIDES	Establecido	En curso	Ver 1.1.1

Pilar II: Disuadir y castigar el comportamiento criminal en el ciberespacio

		Entidad Responsable	Otros involucrados	Año para comenzar	Duración estimada	Costo estimado
2.1	**Establecer un marco jurídico para proporcionar las autoridades y los recursos necesarios para combatir la actividad transnacional de ciberdelincuentes**					
2.1.1	Identificar defensores	AIG	Asamblea Nacional de Panamá	2020	6 meses	$75,000
2.1.2	Supervisar la implementación	AIG	Fiscalía Especial, IMELCF	2020	En curso	Ver 1.1.1
2.2	**Dotar a las fuerzas del orden y al sistema de justicia de las herramientas técnicas adecuadas**					
2.2.1	Realizar un análisis para determinar las herramientas técnicas y requerimientos adicionales para las fuerzas del orden y poder judicial	AIG	Dirección Nacional de Ciberseguridad en la AIG, Policía, Ministerio Público, Poder Judicial	2020	1 año	Ver 1.1.1
2.2.2	Apoyar el entrenamiento y la difusión de mejores prácticas	Dirección Nacional de Ciberseguridad en la AIG	Fuerzas del orden público, IMELCF	2020	1 año	$200,000

2.2.3	Garantizar que se consideren la protección de datos y la privacidad	Dirección Nacional de Ciberseguridad en la AIG	Agencias interesadas	2020	1 año	Ver 1.1.1
2.3	**Hacer obligatoria la notificación de ciertas violaciones graves de datos en el sector privado**					
2.3.1	Ordenar requisitos de notificación obligatoria por brechas de seguridad en los datos	Dirección Nacional de Ciberseguridad en la AIG	CSIRT, Otras agencias	2020	2 años	Ver 1.1.1
2.3.2	Conducir una revisión legal	AIG	Asamblea Nacional de Panamá, organismos de justicia	2020	1 año	N/A
2.4	**Continuar el involucramiento con entidades regionales e internacionales**					
2.4.1	Mejorar la coordinación entre CSIRT Panamá y otros CSIRT nacionales	Dirección Nacional de Ciberseguridad en la AIG	CSIRT, otras naciones	2020	2 años	Ver 1.1.1
2.4.2	Conducir una revisión legal, alineando las leyes cibernéticas de Panamá con tratados y acuerdos internacionales	AIG	Asamblea Nacional de Panamá	2020	1 año	N/A
2.4.3	Participar en ejercicios y foros mundiales para desarrollar la capacidad interna para combatir la ciberdelincuencia	Dirección Nacional de Ciberseguridad en la AIG	CSIRT, otras naciones	2020	1 año	$50,000 por año

Pilar III: Fortalecer la seguridad y la resiliencia de la infraestructura crítica de nuestra nación

		Entidad Responsable	Otros involucrados	Año para comenzar	Duración estimada	Costo estimado
3.1	**Dotar de recursos y empoderar a La Dirección Nacional de Ciberseguridad dentro de la AIG, para liderar los esfuerzos de respuesta y resiliencia de las TIC del Estado, incluyendo sus Infraestructuras Críticas**					
3.1.1	Desarrollar una nueva estructura de gobernanza organizacional para llevar a cabo la misión de proteger las TIC y las Infraestructuras Críticas	AIG	Dirección Nacional de Ciberseguridad de la AIG, La Administración	2020	1 año	$25,000
3.1.2	Desarrollar un Plan Nacional para las Infraestructuras Críticas	Dirección Nacional de Ciberseguridad de la AIG	AIG, sectores de Infraestructuras Críticas	2021	6 meses	$ 250,000
3.1.3	Conducir una evaluación de ciber-riesgo para cada una las agencias relevantes de gobierno y de las que pertenecen al sector de Infraestructuras Críticas	Dirección Nacional de Ciberseguridad de la AIG	Otras agencias de gobierno, sectores de Infraestructuras Críticas	2020	18 a 24 meses	$ 50,000 por agencia
3.1.4	Dirigir al gobierno en materia de guía para configuraciones seguras	Dirección Nacional de Ciberseguridad de la AIG	Todas las agencias	2020	1 año	Ver 1.1.1
3.1.5	Implementar la inteligencia cibernética y el intercambio de información de amenazas	Dirección Nacional de Ciberseguridad de la AIG	Todas las agencias	2020	1 año	$ 15,000 a $ 150,000 por agencia, dependiendo de la herramienta y el grado de automatización

3.1.6	Suscripción al "The CyberWire"	Dirección Nacional de Ciberseguridad de la AIG	Todas las agencias	2020	1 mes	$0
3.1.7	Identificar oportunidades de automatización de la higiene cibernética	Dirección Nacional de Ciberseguridad de la AIG	Todas las agencias	2021	2 años	De $50,000 a $150,000 por agencia dependiendo de la agencia y la prioridad
3.1.8	Implementar un programa de cacería de amenazas en todo el gobierno	Dirección Nacional de Ciberseguridad de la AIG	Agencias seleccionadas	2022	2 años	$25,000 para herramientas y 3 – 5 personas por cada agencia seleccionada
3.1.9	Explorar la creación y/o utilización de un SOC para las agencias gubernamentales seleccionadas	Dirección Nacional de Ciberseguridad de la AIG	Agencias seleccionadas	2022	2 años	Hasta $100,000 y 15 personas adicionales por agencia seleccionada
3.1.10	Automatizar parches	Dirección Nacional de Ciberseguridad de la AIG	Agencias seleccionadas	2021	1 año	Hasta $50,000 por agencia seleccionada
3.1.11	Desarrollar un programa de detección de cambios	Dirección Nacional de Ciberseguridad de la AIG	Todas las agencias	2021	1-2 años	Hasta $50,000
3.2	**Realizar análisis de riesgos y desarrollar planes de contingencia para todos los sectores de las Infraestructuras Críticas**					
3.2.1	Conducir un análisis de cuantificación del ciber-riesgo para todas las Infraestructuras Críticas nombradas	Dirección Nacional de Ciberseguridad de la AIG	Todos los sectores de IC	2021	1 año	$25,000 y $50,000 según tamaño

3.2.2	Apoyar en el desarrollo de planes de contingencia y recuperación para cada Infraestructura Crítica	Dirección Nacional de Ciberseguridad de la AIG	Todos los sectores de IC	2021	1 año	Ver 1.1.1
3.3	**Implementar normas obligatorias de ciberseguridad e "higiene cibernética" para las agencias gubernamentales**					
3.3.1	Educar a las agencias de gobierno y sectores de Infraestructuras Críticas en los Controles Críticos CIS y estrategias de implementación	Dirección Nacional de Ciberseguridad de la AIG	Todas las agencias (Líderes de TI)	2020	6 meses	Ver 1.1.1
3.3.2	Asistir a las agencias con llevar a cabo la implementación de las acciones del Grupo 1 de los Controles Críticos CIS	Dirección Nacional de Ciberseguridad de la AIG	Todas las agencias (Líderes de TI)	2020	6 a 18 meses	Ver 1.1.1 / $10,000 a $25,000 por agencia
3.3.3	Asistir a las agencias para determinar de si proceder con la implementación de las acciones contenidas en los Grupos 2 y 3 de los Controles Críticos CIS	Dirección Nacional de Ciberseguridad de la AIG	Todas las agencias (Líderes de TI)	2021	6 meses	Ver 1.1.1 / Grupo 2 de $30,000 a $45,000 por agencia y Grupo 3 de $60,000 a $100,000 por agencia
3.4	**Proporcionar guía y asesoría al sector privado para mejorar su postura de ciberseguridad**					
3.4.1	Crear programas de intercambio de información sobre amenazas para entidades del sector privado	Dirección Nacional de Ciberseguridad de la AIG	Empresas seleccionadas del sector privado	2022	12 a 18 meses	$50,000
3.4.2	Proporcionar estándares de higiene cibernética al sector privado	Dirección Nacional de Ciberseguridad y Dirección Nacional de Estandarización de la AIG	Empresas seleccionadas del sector privado	2022	6 meses – 1 año	Ver 1.1.1

3.4.3	Ordenar progresivamente la notificación de ciertos incidentes en el sector privado	Dirección Nacional de Ciberseguridad de la AIG	Empresas seleccionadas del sector privado	2022	6 meses – 1 año	Ver 1.1.1
3.5	**Aprovechamiento de los socios internacionales y las oportunidades para construir capacidad**					
3.5.1	Aumentar la participación mundial	Dirección Nacional de Ciberseguridad de la AIG	CSIRT y otros CSIRT nacionales	2020	En curso	Ver 1.1.1

Pilar IV: Fomentar una cultura nacional de ciberseguridad

		Entidad Responsable	Otros involucrados	Año para comenzar	Duración estimada	Costo estimado
4.1	**Priorizar el desarrollo y entrenamiento de la fuerza laboral y sus habilidades**					
4.1.1	Crear un marco oficial de desarrollo de la fuerza de trabajo cibernética	Dirección Nacional de Ciberseguridad de la AIG	El departamento de recursos humanos de cada agencia	2021	6 meses	Ver 1.1.1 / además 1 a 2 personas por cada agencia
4.1.2	Desarrollar y ampliar programas de capacitación acreditados	Dirección Nacional de Ciberseguridad de la AIG	Sector privado, ITI, Universidades del Estado	2022	1 año	$100,000 - $250,000
4.1.3	Desarrollar un plan de reclutamiento y retención	Cada agencia	Dirección Nacional de Ciberseguridad de la AIG	2021	6 meses	Ver 1.1.1
4.1.4	Promover asociaciones profesionales de ciberseguridad en Panamá	La AIG	Asociaciones profesionales	2022	En curso	N/A
4.2	**Promover iniciativas que fomenten una cultura de ciberseguridad**					
4.2.1	Lanzar y ampliar un programa piloto de primaria y secundaria	Ministerio de Educación	Dirección Nacional de Ciberseguridad de la AIG	2021	1 año para el primer curso, luego en curso	$250,000
4.3	**Incentivar la innovación cibernética**					
4.3.1	Desarrollar un plan de investigación y desarrollo (I+D) de ciberseguridad para aprovechamiento de la innovación e ideas del sector privado	Grupo de trabajo	AIG, sector privado, sector educativo	2021	2 años	Ver 1.1.1
4.4	**Promover la sensibilización, el compromiso y la acción del sector privado**					

4.4.1	Fomentar el compromiso del sector privado con la Dirección Nacional de Ciberseguridad de la AIG y el CSIRT	AIG	Dirección Nacional de Ciberseguridad de la AIG, la administración, Sector privado	2022	En curso	N/A
4.4.2	Ampliar la campaña aclamada internacionalmente DETENGASE.PIENSE CONÉCTESE.	AIG	El Administrador de la AIG	2022	En curso	$100,000 para el primer año

Apéndice A: Controles críticos de seguridad de CIS

CONTROL CRÍTICO	DESCRIPCIÓN
1	Inventario y control de activos de hardware
2	Inventario y control de activos de software
3	Gestión continua de vulnerabilidades
4	Uso controlado de privilegios administrativos
5	Configuración segura para hardware y software en dispositivos móviles, portátiles, estaciones de trabajo y servidores
6	Mantenimiento, monitoreo y análisis de bitácoras de auditoría
7	Protecciones de correo electrónico y navegador web
8	Defensas de malware
9	Limitación y control de puertos de red, protocolos y servicios
10	Capacidades de recuperación de datos
11	Configuraciones seguras para dispositivos de red, como firewalls, enrutadores y conmutadores
12	Defensa del perímetro
13	Protección de datos
14	Acceso controlado con base en la necesidad de conocimiento
15	Control de acceso inalámbrico
16	Monitoreo y control de cuentas
17	Implementar un programa de seguridad y capacitación
18	Seguridad del software de aplicación
19	Respuesta y gestión de incidentes
20	Pruebas de penetración y ejercicios de equipo rojo

Estrategia nacional de ciberseguridad

Emitido por la Autoridad Nacional de Innovación Gubernamental (AIG) de Panamá

Octubre, 2019

PRODUCIDO POR

Autoridad Nacional para la Innovación Gubernamental

innovamos para ti

A medida que miles de millones de ciudadanos globales han llegado a confiar en el Internet en su vida diaria, los líderes gubernamentales en Panamá y en todo el mundo reconocen que con la transformación digital viene la necesidad de implementar medidas de ciberseguridad para proteger las tecnologías de información y de las comunicaciones (TIC) sabiendo que estas son esenciales para la seguridad nacional y la estabilidad económica. Con ese fin, más naciones se están moviendo para desarrollar e implementar una estrategia nacional de ciberseguridad para hacer frente a las crecientes amenazas cibernéticas. A partir de 2017, las Naciones Unidas (ONU) estiman que el 50% por ciento de los gobiernos nacionales en el mundo tienen actualmente, una estrategia en vigor de este tipo.[1]

En 2013, el Gobierno de Panamá lanzó su Estrategia Nacional para la Ciberseguridad y la Protección de Infraestructuras Críticas. Desarrollada por la Autoridad Nacional para la Innovación Gubernamental (AIG), la estrategia esbozó principios, objetivos y elementos de acción que son vitales para el bienestar de la población y el funcionamiento diario del gobierno de Panamá.

Esta revisión de la estrategia, la Estrategia Nacional de Ciberseguridad (ENC) de aquí en adelante, sirve como una actualización a la desarrollada en 2013, actualizada para reflejar la evolución y desarrollo de las amenazas en el ciberespacio. El panorama de la seguridad está evolucionando continuamente y mucho ha cambiado en el mundo, lo que requiere una mirada madura a cómo nuestra nación se está preparando para los desafíos de hoy y los que vendrán en el futuro.

Esta Estrategia Nacional de Ciberseguridad (ENC) actualizada, describe un camino a recorrer de cinco años para brindar mayor seguridad tanto al individuo, como al sector comercial y al gobierno. Desarrollada a través de una revisión intensiva realizada por expertos independientes externos, dentro y fuera de Panamá, AIG supervisó el proceso para actualizar y revisar la estrategia de 2013. Con el fin de comprender mejor el estado actual, las limitaciones y necesidades del gobierno en una manera más amplia, se entrevistó a 18 organizaciones gubernamentales nacionales. Sus evaluaciones sirvieron para esculpir este documento y reconocemos su generoso tiempo y contribuciones.

Al igual que Panamá es el centro geográfico de las Américas, con una orgullosa historia de conexión de personas y productos en todo el mundo, las políticas establecidas en nuestra nueva Estrategia Nacional de Ciberseguridad (ENC) promoverán un ciberespacio libre, abierto, seguro y resiliente en Panamá. Con una serie de actores maliciosos operando sin tener en cuenta fronteras nacionales, creemos en lo importante y crítico que es la cooperación y nos esforzamos por trabajar con nuestros vecinos regionales y otros socios globales.

Por último, pero de igual forma crítico e importante, el énfasis de esta estrategia en proteger los derechos humanos fundamentales, detener el cibercrimen y construir una cultura donde todos participen en nuestra ciberseguridad mutua servirá bien a Panamá y podrá ser un modelo a seguir para los demás en los años venideros.

Firmado,
[Representante de AIG /presidente de Panamá/otro líder gubernamental nacional] [FECHA]

---

[1] United Nations (UN), International Telecommunication Union (ITU), "Global Cybersecurity Index (GCI)" July 2017, link: http://handle.itu.int/11.1002/pub/80f875fa-en

Contenido

Resumen Ejecutivo: Una Estrategia Nacional de Ciberseguridad actualizada para Panamá

A partir de 2019, más de dos millones de personas en la República de Panamá están conectadas a Internet, utilizando las tecnologías de la información y las comunicaciones (TIC) en sus actividades diarias, la administración de servicios gubernamentales y las operaciones e innovaciones que impulsan los negocios. La prosperidad económica y cívica de Panamá depende de cómo nuestra nación en su conjunto adopta las TIC y accede el "ciberespacio" – las redes y sistemas de información públicos y privados que nos conectan entre sí –.

A medida que cada faceta de la vida se vuelve más dependiente del ciberespacio, han surgido nuevas vulnerabilidades. Del mismo modo, nuevas amenazas de una variedad de actores maliciosos están apareciendo, estas van desde los estados-nación hasta la organización de círculos criminales y hackers o "lobos" solitarios.

Por esta razón, sólidas medidas de ciberseguridad - esencialmente la protección del ciberespacio, sus redes y sistemas - deben ser una parte integral e indivisible de la transformación. Debemos proteger proactivamente las TIC, así como mejorar las políticas y procedimientos que permiten a Panamá prevenir ciberataques o estar preparados para recuperarse rápidamente si eventualmente se produce uno.

Basándose en la Estrategia Nacional de Panamá 2013 para la Ciberseguridad y la Protección de las Infraestructuras Críticas, esta nueva estrategia actualizada describe en cuatro pilares clave, cómo Panamá garantizará que las estructuras físicas y virtuales del ciberespacio estén protegidas en los próximos cinco años. Esta estrategia, que refleja nuestros principios nacionales panameños, se basa en la siguiente visión:

Declaración de Visión:

Panamá será una nación que procure un ciberespacio abierto, libre, seguro y resiliente, protegiendo los derechos y garantías fundamentales contemplados en nuestra Constitución Política, facilitando al gobierno servir a las personas y fomentar un ambiente regulatorio favorable al crecimiento de la economía. Esto se logrará mediante la alineación de los recursos del sector público y privado, y promoviendo una conciencia universal de que la ciberseguridad es responsabilidad de todos.

En un esfuerzo por mantener el plan al día en vista de los desarrollos en el panorama cibernético, esta nueva estrategia está marcada por algunos cambios:

En primer lugar, este nuevo plan hace hincapié en la necesidad de marcos de trabajo, leyes y autoridades actualizadas para desarrollar la capacidad cibernética y hacer cumplir las mejores prácticas a nivel nacional. Mientras que la estrategia de 2013 posicionó a Panamá para aumentar su capacidad de ciberseguridad, la sofisticación de los actores de amenazas también está evolucionando. A nivel regional en América Latina, el cibercrimen está en aumento, donde hubo

un 20% de incremento en los ataques de 2017 a 2018. Y cada vez más panameños están experimentando el robo de su información personal.[2]

En segundo lugar, este plan reitera la idea de que la ciberseguridad debe convertirse en una parte de la cultura y mentalidad nacional. El alcance de las TIC en la vida cotidiana de los ciudadanos ha crecido sustancialmente en los últimos años, lo que equivale a más oportunidades, pero también a más vulnerabilidades para nuestra gente y nuestras instituciones. Esta estrategia da una mayor prioridad a la educación, la sensibilización y la formación a todos los niveles, ya sea para fomentar la conciencia básica a nivel individual, implementar esfuerzos de capacitación a gran escala para construir y mantener una fuerza de trabajo cibernética de clase mundial, o promover innovaciones en el sector privado que mantendrán a Panamá por delante de la curva tecnológica.

Tercero, esta estrategia fue desarrollada teniendo en cuenta la flexibilidad, proveyendo al gobierno de capacidades para responder en forma rápida y efectiva a medida que ocurre el cambio. La ciberseguridad es un tema de constante evolución, debido a que constantemente emergen nuevas amenazas, tecnologías y normativas. Para este fin, esta estrategia nueva de ciberseguridad nacional tiene prevista una vigencia no mayor a 5 años hacia el futuro. Medidas de revisión han sido tomadas en cuenta para evaluar prioridades y progreso sobre la misma en forma recurrente.

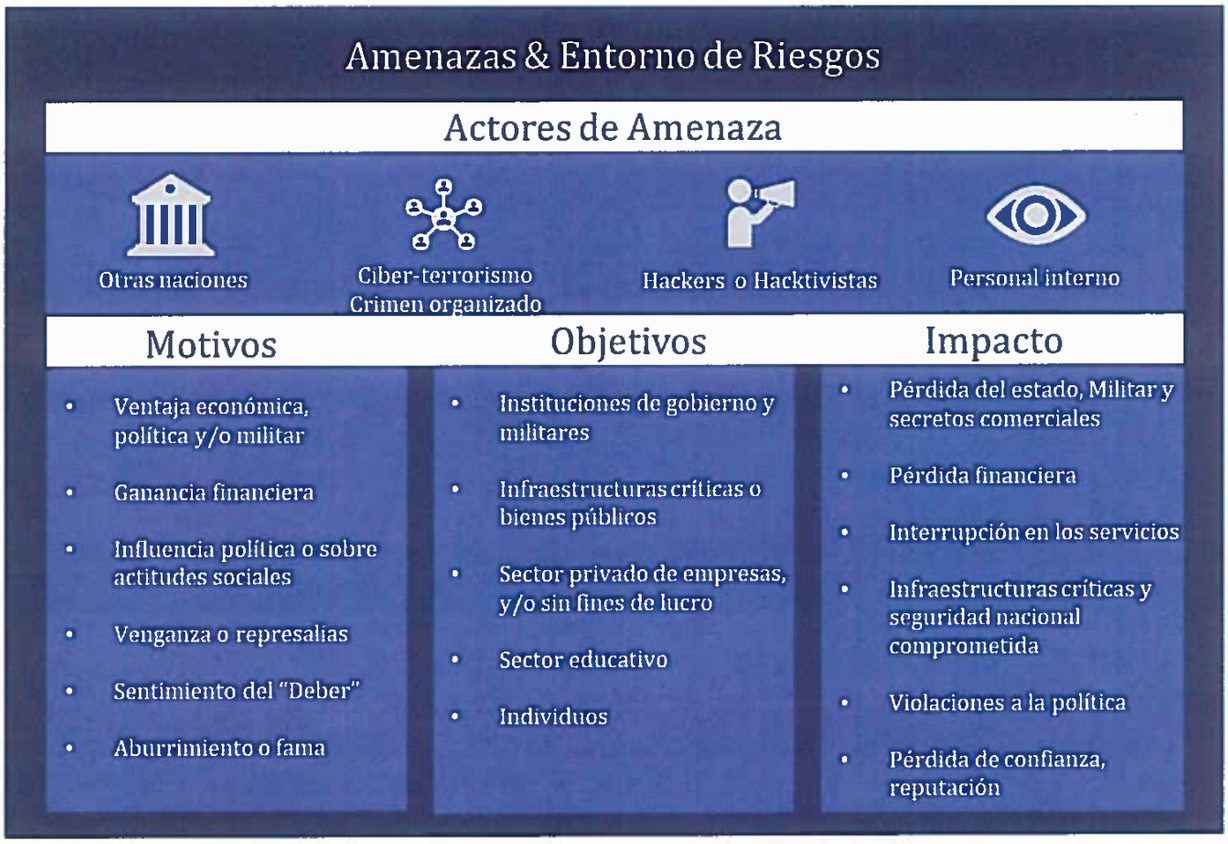
Por último, la importancia del compromiso internacional se presenta de manera más destacada. Desde 2013, las organizaciones de gobernanza internacional han puesto, con mucha razón, un mayor énfasis en las asociaciones internacionales en lo que respecta a la mejora de la ciberseguridad. En 2016, la Organización de Estados Americanos (OEA) expresó que "abordar los desafíos cibernéticos requiere esfuerzos diplomáticos y cooperación internacional. Una cosa que hemos aprendido en ciberseguridad es que ninguna nación por sí misma puede proteger adecuadamente sus redes. La cooperación es esencial". En concurrencia con esta declaración, la Estrategia Nacional de Ciberseguridad de Panamá ha incorporado más elementos de participación y cooperación cibernética internacional.

Marcada por estos cambios, esta estrategia tiene como finalidad que se tome como una guía de alto nivel para los líderes de la seguridad del gobierno a nivel nacional – así como aquellos en el sector privado que la apoyen. De esta, deben derivarse guías adicionales de implementación para abordar directamente los objetivos plasmados en este documento.

[2] LexisNexis Risk Solutions, ThreatMetrix, "Q2 2018 Cybercrime Report" October 2018, link: https://www.threatmetrix.com/info/q2-2018-cybercrime-report/

Amenazas y riesgos

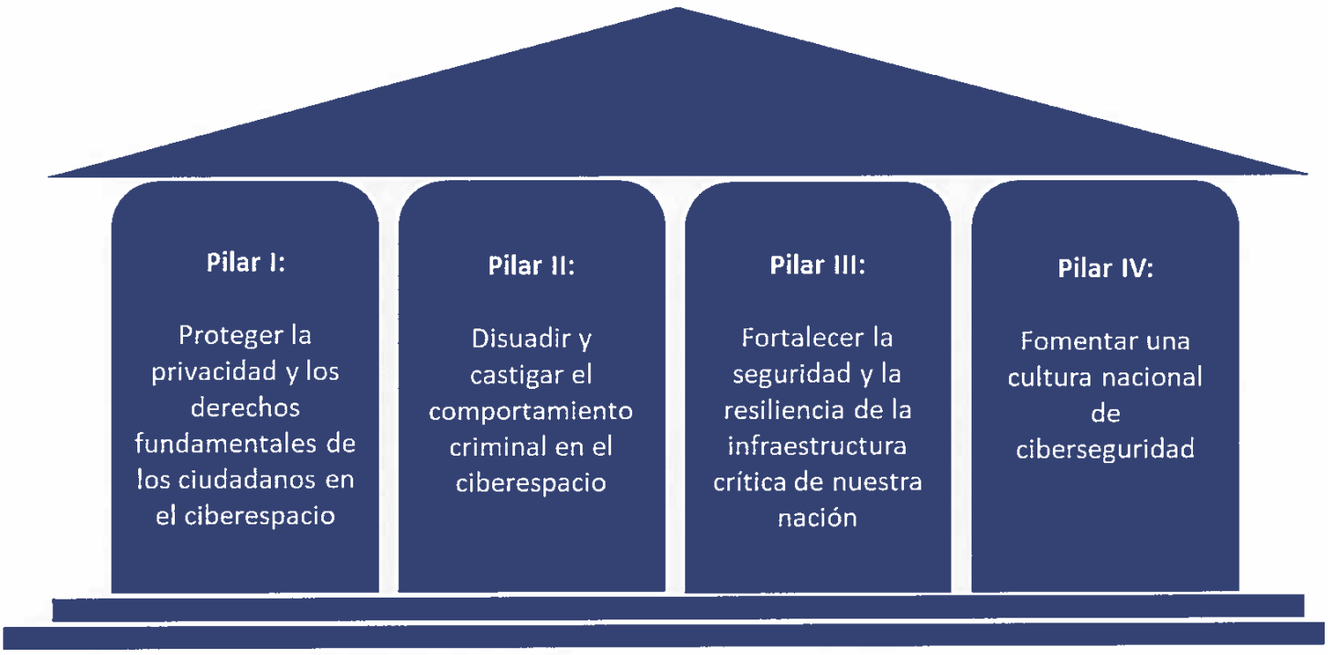
La postura de ciberseguridad de nuestra nación tiene un impacto directo y trascendente en la vida cotidiana de las personas, la vitalidad económica y la administración gubernamental. Para salvaguardar a todos estos, es necesaria una estrategia para prepararse para una variedad de amenazas cibernéticas. Los ciberataques son llevados a cabo por actores con múltiples capacidades y diversos motivos, como se muestra en el siguiente cuadro.



Los riesgos de la inacción son demasiado altos y significaría no estar debidamente preparado para afrontar incidentes cibernéticos, con amenazas que causan daños, inseguridad e inconvenientes a las personas, las empresas y el gobierno. Además, Panamá cuenta con activos únicos que deben ser protegidos. Actuando como un nodo comercial, de transporte y comunicaciones, el Canal de Panamá sirve como un centro que impulsa transacciones globales. Con una posición geográfica especial, Panamá puede encontrarse siendo un blanco atractivo para ataques cibernéticos originados dentro o fuera del país. Por lo tanto, la protección del canal y otras Infraestructuras Críticas (CI) como la energía, el agua, el transporte y los activos de salud pública adquiere una mayor importancia.

Elementos de la Estrategia Nacional de Ciberseguridad

La Estrategia Nacional de Ciberseguridad de Panamá está articulada y organizada por pilares, como se describe a continuación. La AIG coordinará con las agencias planes personalizados de los recursos para implementar estos objetivos y acciones respectivas contenidas en estos. La AIG también actuará como la entidad de supervisión clave responsable de garantizar que las agencias asignadas a objetivos o tareas específicas sean ejecutadas dentro de los plazos establecidos.



Juntos, estos cuatro pilares se perseguirán e implementarán guiados por los siguientes principios:

- La ciberseguridad afecta a todos y es responsabilidad de todos. Personas individuales, la educación, el sector comercial y el gobierno debemos trabajar juntos para mantenernos seguros.
- Sin embargo, existen responsabilidades para las que el gobierno tiene el compromiso principal de abordar, incluida la protección de la seguridad individual y las libertades fundamentales, la promoción de los intereses de seguridad nacional, el llevar a juicio el cibercrimen, y los aspectos diplomáticos de la coordinación con socios internacionales.
- Las amenazas en línea se originan en todo el mundo y Panamá debe trabajar con sus vecinos y aliados para proteger los intereses compartidos de seguridad, cívicos y económicos.
- La privacidad y los derechos fundamentales deben ser considerados y protegidos en cada momento.

- Hay poblaciones vulnerables a considerar, especialmente la población de menores, quienes deben ser protegidos.
- Los actores de amenazas están en constante evolución y las innovaciones en el campo de la defensa cibernética son esenciales para mantenerse a la vanguardia. En este sentido, los emprendedores desempeñan un papel clave.

Pilar I: Proteger la privacidad y los derechos fundamentales de los ciudadanos en el ciberespacio

Los derechos fundamentales de las personas, y especialmente el derecho a la privacidad, son primordiales en nuestra sociedad que valora la igualdad de oportunidades, las libertades civiles y la inclusión. El ciberespacio debe ser un lugar donde las personas puedan sentirse empoderadas para participar en la libertad de expresión y acceder a la información. Las TIC deben utilizarse como una herramienta que pueda mejorar y realzar la forma en que las personas interactúan entre sí, con las empresas y con su gobierno.

En cuanto a las funciones cotidianas, el sector comercial y los individuos tienen la responsabilidad de protegerse a sí mismos. Sin embargo, a nivel institucional, es vital que Panamá establezca un marco de trabajo basado en confianza y seguridad, implementando y aplicando medidas para salvaguardar la información sensible y los datos personales, que pueden ser usados en formas inapropiadas para discriminar y/o perjudicar a los ciudadanos. Los menores forman parte de una población particularmente vulnerable que se enfrenta a amenazas únicas, y se requieren iniciativas especiales para mantenerlos seguros.

Acciones prioritarias para alcanzar este objetivo:

- **1.1 Empoderar y brindar los recursos necesarios a la AIG para servir como el organismo de asesoría técnica y de acompañamiento en la implementación del marco regulatorio y las leyes de protección de datos personales de Panamá**
  En 2019, Panamá trasladó para aprobación una legislación robusta con leyes y requerimientos explícitos sobre la privacidad de los datos[3] para hacer que las regulaciones sean uniformes y estén presentes en todos los sectores. Mientras que la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI) es la entidad legalmente responsable de implementar los requerimientos de esta nueva ley, la AIG proveerá supervisión a ANTAI y será la entidad representada en el Consejo de Protección a los Datos Personales para servir como el organismo de asesoría técnica. En este rol, la AIG ayudará en la interpretación de las nuevas leyes a las partes interesadas en los sectores público y privado, incluyendo a los Proveedores de Servicio de Internet (ISP por sus siglas en inglés). La AIG también podrá emitir aclaraciones o bien, interpretación legal cuando sea necesario.

- **1.2 Identificar todos los datos personales e información**
  La protección de los datos personales requiere saber dónde existen y gestionarlos. Por lo tanto, bajo la nueva ley de privacidad de datos, esto debe ser identificado y mantener trazabilidad de las organizaciones que los poseen. La AIG y ANTAI deberán trabajar en

[3] Referencia: Ley número 81 de 2019 sobre La Protección de los Datos Personales

estrecha colaboración y comunicación para lograr este objetivo.

- **1.3 Promover la adopción de mejores prácticas para la privacidad de los datos y la protección de la propiedad intelectual (P.I.) a nivel de gobierno**
  El gobierno desempeña un papel vital en la construcción de confianza en el ciberespacio. El gobierno nacional de Panamá liderará mediante el ejemplo, asegurando que los datos personales y la propiedad intelectual que resguardan estén protegidos siguiendo mejores prácticas de protección de datos y ciberseguridad. Demostrar este éxito por parte del gobierno, servirá como modelo para futuras regulaciones y mandatos para el sector privado.

- **1.4 Promover y supervisar La Comisión Nacional de Protección de Datos de Menores**
  Dentro de la ley de protección de datos de 2019[4], existen disposiciones clave para la protección de los menores, un objetivo importante de la seguridad pública, ya que los niños y adolescentes son particularmente susceptibles al abuso y la explotación en línea. Modelado por esfuerzos similares al proyecto "Internet para todos" que lleva Internet a las escuelas de todo Panamá, la AIG promoverá y supervisará la comisión compuesta por líderes de los sectores público y privado, que ayudarán a interpretar las nuevas leyes a nivel nacional y también a informar consideraciones adicionales sobre las políticas en el futuro, abordando cualquier brecha identificada en la ley o fuera de esta.

Pilar II: Disuadir y castigar el comportamiento criminal en el ciberespacio

El cibercrimen es un riesgo para todas las sociedades modernas, y Panamá no es la excepción. Los actores de amenazas se dirigen a los ciudadanos, el sector comercial y las Infraestructuras Críticas de Panamá, socavando así, la estabilidad financiera, la seguridad personal y la confianza del público. Como gran parte de la actividad maliciosa en línea es de naturaleza criminal, el gobierno nacional – en conjunto con los organismos encargados de hacer cumplir la ley, el Instituto de Medicina Legal y Ciencias Forenses (IMELCF), los servicios de investigación, la Fiscalía y el Poder Judicial – deben trabajar juntos para detectar, disuadir y llevar a juicio el cibercrimen e imputar consecuencias apropiadas a los actores cibernéticos malintencionados.

En los últimos años, Panamá ha establecido una Fiscalía Especial para Delitos contra la Propiedad Intelectual y la Seguridad Informática, que forma parte del Ministerio Público, y una unidad de investigación para el cibercrimen dependiente de la Dirección de Investigación Judicial. Estas agencias están al mando de la averiguación y el enjuiciamiento de delitos cibernéticos. Este pilar mejorará su trabajo y apoyará a otras partes interesadas en la búsqueda de un Internet más seguro.

Las acciones principales para lograr este objetivo incluyen:

- **2.1 Establecer un marco jurídico para proporcionar las autoridades y los recursos necesarios para combatir la actividad transnacional de ciberdelincuentes**
  Desde 2013, Panamá ha trabajado para desarrollar un marco legal más sólido que proporcionará las autoridades y recursos operativos necesarios a los organismos

[4] Referencia: Ley número 81 de 2019 sobre La Protección de los Datos Personales
http://www.antai.gob.pa/wp-content/uploads/2019/04/Ley-81-de-2019-Proteccion-de-Datos-Personales.pdf

involucrados en la cadena judicial para identificar, frustrar y llevar a juicio el cibercrimen. Este marco también otorga al gobierno una mejora en la capacidad para coordinarse con las partes interesadas del sector privado. Sin embargo, este marco jurídico todavía está en estudio y aún no se ha promulgado. Su aprobación y promulgación se denominan prioritarias en esta Estrategia Nacional de Ciberseguridad.

- **2.2 Dotar a organismos de seguridad y al sistema de justicia de las herramientas técnicas adecuadas**
  Además de permitir autoridades jurídicas más sólidas, la policía y sus órganos subsidiarios, el Ministerio Público y la rama judicial también deben estar equipados con la formación adecuada, los instrumentos técnicos y las mejores prácticas para detectar actividades delictivas, llevar a cabo actividades de vigilancia electrónica, retención de datos, realizar investigaciones y presentar cargos en forma expedita, respetando al mismo tiempo la privacidad de los ciudadanos y las libertades civiles. La AIG deberá trabajar en estrecha colaboración con las entidades vinculadas a los organismos de seguridad y al sistema de justicia, como asesor técnico, para identificar los requisitos y las brechas en las agencias para cumplir con esta finalidad, y deben desarrollar en conjunto un plan para lograrlo.

  En cuanto al entrenamiento, la AIG liderará un esfuerzo para dotar a los agentes de campo -encargados de aplicar la ley- con habilidades críticas para la recopilación de evidencia digital, la retención de datos y capacidades de gestión relacionadas. La AIG también identificará capacitadores que puedan apoyar a las partes interesadas de IMELCF en el área de análisis forense. Por último, en la parte judicial la AIG supervisará la formación de los funcionarios con el fin de entender cómo se debe juzgar de acuerdo a las nuevas leyes relacionadas con el cibercrimen y la evidencia digital.

  Por último, de conformidad con la legislación nacional de seguridad de datos en 2019, la AIG trabajará en estrecha colaboración con las entidades vinculadas a los organismos de seguridad y al sistema de justicia, como asesor técnico, para desarrollar guías de orientación que enmarcan los parámetros legales para la privacidad y la protección de las libertades civiles de los ciudadanos, para las autoridades de justicia.

- **2.3 Hacer obligatoria la notificación de ciertas violaciones graves de datos en el sector privado**
  La pronta denuncia de violaciones de datos tanto en el sector gubernamental como en el privado es esencial para detener el cibercrimen. A medida que se detectan brechas de seguridad y robo de datos (como Información Personal y lo que se consideran datos sensibles), los incidentes deben ser reportados al Equipo de Respuesta a Incidentes de Seguridad Cibernética de Panamá (CSIRT-Panamá) para permitir un mejor y más rápido intercambio de información y que a su vez permitirá tomar acciones entre el gobierno y la industria. Actualmente, la notificación de brechas se ha retrasado. El Gobierno de Panamá abordará estas notificaciones obligatorias para algunas de las violaciones y el robo de datos personales o de los que afecten a las Infraestructuras Críticas. Estos requisitos se harán primero a las entidades gubernamentales, y luego al sector privado en un enfoque escalonado.

- **2.4 Continuar el involucramiento con entidades regionales e internacionales**
  En 2014, Panamá exitosamente ratificó la Convención de Budapest[5], el primer tratado internacional que busca abordar el cibercrimen armonizando las leyes nacionales, mejorando las técnicas de investigación y aumentando la cooperación entre las naciones. Panamá también ha firmado acuerdos en el marco de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. Si bien representan pasos iniciales importantes, es necesario mejorar la coordinación y la cooperación internacional. Además, es necesario incorporar al ordenamiento jurídico leyes que estén alineadas con los convenios o acuerdos internacionales, de los cuales Panamá es signataria.

  La AIG, a través de CSIRT, continuará su enfoque en una mayor coordinación entre el CSIRT de Panamá y otros CSIRT nacionales, especialmente dentro de los Estados miembros de la OEA, así como con entidades encargadas de hacer cumplir la ley, mismas que son críticas para disuadir el cibercrimen fronterizo tales como Interpol y Europol. CSIRT también participará en asociaciones multinacionales y organismos mundiales de normalización que promueven el uso de las TIC y las normas y orientaciones de ciberseguridad, como la Organización Internacional de Normalización (ISO).

Pilar III: Fortalecer la seguridad y la resiliencia de la infraestructura crítica de nuestra nación

Todas las naciones tienen infraestructura crítica que deben proteger. En Panamá, el Canal de Panamá es una infraestructura crítica única y vital, y cualquier amenaza a su operatividad puede tener consecuencias perjudiciales para el comercio global y el bienestar humano. Otros sectores como la energía, el agua, el transporte y la salud pública también tienen la necesidad de protección, debido a que no sólo se comparten los intereses del Canal, sino que, además, afectan la seguridad física y económica general de la nación.

La responsabilidad de asegurar las Infraestructuras Críticas de la nación y gestionar su riesgo de ciberseguridad es compartida por el gobierno y el sector privado por igual. Es imperativo que las entidades públicas y privadas trabajen en asociación. Cada una debe desarrollar y perfeccionar sus capacidades organizativas para detectar y defenderse de los ataques que tienen el potencial de interrumpir o inhabilitar las Infraestructuras Críticas, así como también, poner en marcha medidas de resiliencia para recuperarse rápidamente y minimizar el impacto en las operaciones en caso de ciberataques.

[5] Referencia: Convención de Budapest sobre el Cibercrimen, Tratado Número 185, Ratificación del 03 de mayo de 2014

Las acciones prioritarias para lograr este objetivo incluyen:

- **3.1 Crear, dotar de recursos y empoderar a La Dirección Nacional de Ciberseguridad dentro de la AIG, para liderar los esfuerzos de respuesta y resiliencia de las TIC del Estado, incluyendo sus Infraestructuras Críticas**
  Actualmente ninguna oficina o agencia del gobierno está dedicada exclusivamente a supervisar la protección de Infraestructuras Críticas. Para este fin, la AIG debe ser empoderada para liderar la misión de ciberseguridad para el país. La Dirección Nacional de Ciberseguridad de la AIG debe ser quien reciba la autoridad para llevar la delantera y dirigir lo relacionado a la ciberseguridad y las actividades de protección de las Infraestructuras Críticas a lo largo del gobierno, sirviendo como un ente centralizador u oficina de coordinación para alinear a las agencias, las cuales a su vez, designarán a un líder de ciberseguridad para que sea el responsable de este aspecto en la agencia para la cual trabaja y sirva de enlace hacia la Dirección Nacional de Ciberseguridad con el propósito de facilitar y hacer fluir la coordinación entre agencias. El CSIRT dentro de la Dirección Nacional de Ciberseguridad de la AIG ya cumple con algunas de las operaciones de respuesta según el Decreto ejecutivo 709 del 26 de septiembre de 2011[6]. Sin embargo, bajo la nueva designación, la Dirección Nacional de Ciberseguridad de la AIG será el ente al que se le reconocerá y se le proporcionarán los recursos para funciones que incluyen servicios preventivos, proactivos y de respuesta. Prácticamente, estos roles incluirán, entre otros, el análisis de amenazas cibernéticas, la identificación y el análisis de vulnerabilidades, el desarrollo de una capacidad de cacería de amenazas, la educación de las partes interesadas, herramientas y mejores prácticas, capacitación de la fuerza de trabajo, implementación de normas cibernéticas entre agencias gubernamentales y coordinación de las actividades de respuesta a incidentes entre el gobierno y la industria (atravesando todos los sectores).

- **3.2 Realizar análisis de riesgos y desarrollar planes de contingencia para todos los sectores de Infraestructuras Críticas**
  La Dirección Nacional de Ciberseguridad de la AIG, como nueva dirección para la protección de las Infraestructuras Críticas, asumirá la responsabilidad de identificar e inventariar todas las Infraestructuras Críticas en los sectores público y privado, realizar un análisis de riesgos en estos y luego trazar un plan básico de contingencia y recuperación para su protección. Informalmente, algunos organismos gubernamentales ya están llevando a cabo estas tareas individualmente, pero la misión de la Dirección Nacional de Ciberseguridad de la AIG será designar Infraestructuras Críticas y alinear la forma de abordar su protección en forma estratégica.

- **3.3 Implementar normas obligatorias de ciberseguridad e "higiene cibernética" para las agencias gubernamentales**
  Dado que el gobierno nacional busca liderar mediante dar ejemplo a la puesta en marcha de las mejores prácticas para proteger los datos personales alojados en sus sistemas o redes, todos los organismos gubernamentales nacionales también estarán obligados a adherirse a las normas y directrices básicas de ciberseguridad, especialmente en términos de "higiene

[6] Referencia: Decreto ejecutivo 709 del 26 de septiembre de 2011
https://www.gacetaoficial.gob.pa/pdfTemp/26880/GacetaNo_26880_20110927.pdf

cibernética". Estas normas se pondrán en marcha bajo la orientación emitida por la Dirección Nacional de Ciberseguridad de la AIG, con hitos para su aplicación en el transcurso de cinco años.

- **3.4 Proporcionar guía y asesoría al sector privado para mejorar su postura de ciberseguridad**
  El gobierno tiene un papel que desempeñar en términos de equipar a los propietarios y operadores del sector privado de Infraestructuras Críticas con orientación, guía, asesoría y canales de comunicación para prevenir, coordinar la respuesta y recuperarse de incidentes de ciberseguridad. Con el fin de mejorar la ciberseguridad de las entidades del sector comercial, la Dirección Nacional de Ciberseguridad de la AIG mejorará sus capacidades para servir como centro de respuesta del sector privado e intercambio de información, así como realizar ejercicios y simulacros para aumentar las habilidades y capacidad de los operadores cibernéticos del sector privado. La Dirección Nacional de Ciberseguridad de la AIG también proporcionará otros instrumentos, incluidas las normas y la formación, para ayudar a construir esta capacidad en el sector privado.

- **3.5 Aprovechamiento de los socios internacionales y las oportunidades para construir capacidad**
  Debido a que las amenazas cibernéticas a menudo se originan fuera del país y con efectos adversos de incidentes que se sienten más allá de nuestras fronteras, Panamá buscará desarrollar canales de comunicación más efectivos con sus vecinos. También identificará foros globales en los que pueda participar en simulacros internacionales y respuesta a incidentes.

Pillar IV: Fomentar una cultura nacional de ciberseguridad

La ciberseguridad es una responsabilidad compartida, y como imperativo de seguridad nacional, debemos buscar mejoras continuas a nivel individual, comercial y gubernamental. Crear una cultura de ciberseguridad significa que las empresas y el gobierno están invirtiendo y promoviendo la educación y puestos de trabajo de ciberseguridad, en sus estrategias. También significa que las personas consideran la ciberseguridad en el hogar, en público y mientras están en el trabajo. Lo anterior implica que cada parte interesada entiende las funciones y deberes respectivos, adoptando comportamientos y acciones que mantienen el Internet protegido, seguro, abierto y libre.

Panamá servirá como líder para promover este entendimiento fundamental a nivel nacional, enfocándose en los objetivos de entrenamiento y educación, sensibilización pública, colaboración público-privada e innovación.

Las acciones prioritarias para lograr este objetivo incluyen:

- **4.1 Priorizar el desarrollo y entrenamiento de la fuerza laboral y sus habilidades**
  Una fuerza de trabajo de ciberseguridad altamente cualificada y sostenible es esencial para la seguridad nacional y la protección de las Infraestructuras Críticas, así como para la administración de los servicios gubernamentales. Apoyada a través de alianzas con el

sector privado y académico, Panamá invertirá en programas y mejorará los ya existentes, para fortalecer y construir la cartera de talento nacional, desde la educación primaria hasta la postsecundaria. La Dirección Nacional de Ciberseguridad de la AIG deberá liderar el desarrollo de un plan de estudios acreditado adaptado a las habilidades necesarias para ejecutar las operaciones gubernamentales de ciberseguridad. Más allá de la capacitación, la AIG liderará el desarrollo de iniciativas de divulgación para supervisar el reclutamiento, la gestión y el despliegue del personal de ciberseguridad en las agencias gubernamentales nacionales. La AIG también liderará la creación de programas de incentivos tales como becas y oportunidades de desarrollo de carrera para retener eficazmente el talento crítico de ciberseguridad tomando en consideración lo competitivo del entorno en el sector comercial. La AIG también promoverá el establecimiento de asociaciones profesionales de ciberseguridad en Panamá.

- **4.2 Promover iniciativas que fomenten una cultura de ciberseguridad**
  La vigilancia a nivel individual comienza con la comprensión básica de que la "higiene cibernética" personal ayuda a la protección y privacidad de los datos y mejora la postura general de ciberseguridad de la nación. Instaurar el concepto de seguridad en línea desde el mismo principio de la educación de nuestros hijos, puede conducir a una cultura con hábitos de seguridad para toda la vida. Trabajando con el Ministerio de Educación, la AIG promoverá campañas formales a nivel nacional que fomenten una cultura de ciberseguridad, para incorporar buenas prácticas cibernéticas en los planes de estudio a nivel de primaria y secundaria.

- **4.3 Incentivar la innovación cibernética**
  A medida que el panorama de amenazas cibernéticas evoluciona, los avances en la ciencia y la ingeniería de la ciberseguridad son clave para salvaguardar los beneficios de Internet. La mayoría de estas innovaciones se generan a través de la investigación académica o del sector privado, y el gobierno desempeña un papel importante en la provisión de recursos e incentivos. Con ese fin, la AIG liderará la publicación de un plan formal de investigación y desarrollo de ciberseguridad (I&D) centrado en involucrar y aprovechar a las partes interesadas en la comunidad de I&D para proporcionarles métodos evolutivos y herramientas para protegerse contra actividades cibernéticas maliciosas y recuperarse de incidentes.

- **4.4 Promover la sensibilización, el compromiso y la acción del sector privado**
  Si bien los organismos gubernamentales deberán adoptar normas y directrices básicas para la ciberseguridad, La AIG también desempeñará un papel educativo y difundirá la orientación a los socios del sector privado y fomentará su uso. Además, Panamá considerará formas de comunicar a los ciudadanos su participación en la campaña internacional "Deténgase. Piense. Conéctese" que tiene como objetivo promover prácticas seguras en el uso del Internet.

Conclusión

Ampliando sobre la primera estrategia de ciberseguridad de la República de Panamá presentada en 2013, este documento ofrece una visión actual de cómo el gobierno buscará alcanzar los objetivos clave para mejorar la postura general de ciberseguridad de nuestra nación. Se trata de un plan a corto plazo, destinado a mirar hacia los próximos cinco años, con puntos de referencia que cumplir en áreas clave, entre ellas: La mejora de un marco de privacidad y protección de datos, la promulgación de un marco jurídico sólido para detener el cibercrimen, el objetivo de proteger nuestros activos de las TIC e Infraestructuras Críticas y el crecimiento de una mentalidad cultural donde todos los panameños participen en nuestra seguridad compartida.

La ciberseguridad es una de las áreas más dinámicas de las políticas públicas, con problemas y amenazas que evolucionan rápidamente en relación con otras áreas políticas. Con el fin de mantener el ritmo de los cambios y el desarrollo en el panorama cibernético, este plan debe ser revisado y formalmente actualizado al menos una vez al año. La AIG evaluará al menos trimestralmente el avance, trabajando con agencias individuales para garantizar la implementación oportuna y que la retroalimentación obtenida, informe adecuadamente sobre las futuras iteraciones de la estrategia nacional de ciberseguridad.

Basada en el entendimiento de que existe un vínculo inextricable entre la ciberseguridad, nuestra prosperidad económica y nuestra seguridad nacional, la estrategia desempeña un papel crítico en la protección del ciberespacio y en garantizar que los ciudadanos puedan disfrutar de oportunidades de conectividad hacia el futuro.

Apéndice A: Glosario de términos

AIG: Autoridad de Innovación Gubernamental

CAPATEC: Cámara Panameña de Tecnologías de Información, Innovación y Telecomunicaciones

CSIRT-PANAMA: Equipo de Respuesta a Incidentes de Seguridad Cibernética de Panamá

CSIRT: Computer Security Incident Response Team

I&D: Investigación y desarrollo

IMELCF: Instituto de Medicina Legal y Ciencias Forenses

PI: Propiedad Intelectual

OEA: Organización de Estados Americanos

TIC: Tecnología de la Información y las Comunicaciones

Apéndice B: Construcción de la Estrategia Nacional de Ciberseguridad

La visión de la Estrategia Nacional de Ciberseguridad de Panamá establece que la ciberseguridad es una responsabilidad de todos, lo que abarca todo. Por esta razón, la estrategia original de 2013 se construyó mediante la consulta de numerosas organizaciones y empresas encargadas de la administración de servicios públicos y la protección de infraestructuras críticas. La AIG ha sido el órgano de coordinación para el desarrollo de la Estrategia y ha contado con la colaboración de la Organización de Los Estados Americanos (OEA). En el reacondicionamiento de este documento, se volvió a consultar a varios organismos gubernamentales nacionales y socios del sector privado con el fin de comprender mejor cómo han evolucionado las necesidades, capacidades y desafíos desde 2013. Las siguientes organizaciones participaron en esta actualización más reciente:

1. Autoridad Nacional para la Innovación Gubernamental (AIG)
2. Autoridad Canal de Panamá (ACP)
3. Ministerio de Comercio e Industrias
4. Ministerio de Seguridad Pública (MINSEG)
5. Aeropuerto Internacional de Tocumen
6. Ministerio de Relaciones Exteriores (MIRE)
7. Asociación Bancaria
8. Procuraduría Nacional
9. Asamblea Nacional
10. Ministerio de la Presidencia
11. Autoridad Nacional de los Servicios Públicos (ASEP)
12. CSIRT
13. Banco Nacional
14. Superintendencia de Bancos
15. Aeronáutica Civil
16. Cable Onda
17. Naturgy Panamá
18. Empresa de Transmisión Eléctrica, S.A. (ETESA)

Esta estrategia fue actualizada y diseñada para complementar y apoyar otros planes e iniciativas de seguridad nacional del gobierno nacional de Panamá como el proyecto Internet para todos, la nube de servicios gubernamentales, la Certificación y Programa de infraestructura de firma, el Proyecto Panamá Sin Papel, el Plan Nacional de Energía 2050, el Libro Blanco del gobierno "Protección de Menores en Internet y Ciberseguridad", y la legislación marco de Datos y Privacidad aprobada en 2009. También se ha tomado como referencia el trabajo desarrollado por CAPATEC para el desarrollo de una Estrategia Nacional de TIC, que busca fortalecer la postura cibernética del sector empresarial. Por último, esta estrategia también está influenciada por la adopción de Panamá a los acuerdos internacionales para la ciberseguridad mundial, específicamente la Convención de Budapest y la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, así como la campaña mundial: "Deténgase. Piense. Conéctese".

Apéndice C: Pilares de la Estrategia Nacional de Ciberseguridad

Elementos de la ENC de Panamá Objetivos estratégicos y acciones prioritarias	
Pilar I: Proteger la privacidad y los derechos fundamentales de los ciudadanos en el ciberespacio	**1.1** Empoderar y brindar los recursos necesarios a la AIG para servir como el organismo de asesoría técnica y de acompañamiento en la implementación del marco regulatorio y las leyes de protección de datos personales de Panamá **1.2** Identificar todos los datos personales e información **1.3** Promover la adopción de mejores prácticas para la privacidad de los datos y la protección de la propiedad intelectual (P.I.) a nivel de gobierno **1.4** Promover y supervisar La Comisión Nacional de Protección de Datos de Menores
Pilar II: Disuadir y castigar el comportamiento criminal en el ciberespacio	**2.1** Establecer un marco jurídico para proporcionar las autoridades y los recursos necesarios para combatir la actividad cibercriminal transnacional **2.2** Dotar a los organismos de seguridad y al sistema de justicia de las herramientas técnicas adecuadas **2.3** Hacer obligatoria la presentación de informes de ciertas brechas graves de datos en el sector privado **2.4** Involucrar a las entidades regionales e internacionales
Pilar III: Fortalecer la seguridad y la resiliencia de la infraestructura crítica de nuestra nación	**3.1** Crear, dotar de recursos y empoderar a La Dirección Nacional de Ciberseguridad dentro de la AIG, para liderar los esfuerzos de respuesta y resiliencia de las TIC del Estado, incluyendo sus Infraestructuras Críticas **3.2** Realizar análisis de riesgos y elaborar planes de contingencia para todos los sectores de Infraestructuras Críticas **3.3** Implementar normas obligatorias de ciberseguridad e "higiene" para las agencias gubernamentales **3.4** Proporcionar guía y asesoría al sector privado para mejorar su postura de ciberseguridad **3.5** Aprovechamiento de los socios internacionales y las oportunidades para crear capacidad
Pilar IV: Fomentar una cultura nacional de ciberseguridad	**4.1** Priorizar el desarrollo de la fuerza laboral y la capacitación en habilidades **4.2** Promover iniciativas que fomenten una cultura de ciberseguridad **4.3** Incentivar la innovación cibernética **4.4** Promover la concienciación, el compromiso y la acción del sector privado