*República de Panamá*

**CONSEJO NACIONAL PARA LA INNOVACION GUBERNAMENTAL**

Resolución No.21 Panamá, 12 de marzo de 2013.

"Por la cual se aprueba el documento titulado: Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas."

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

**CONSIDERANDO:**

Que mediante Ley No. 65 de 30 de octubre de 2009, se creó la Autoridad Nacional para la Innovación Gubernamental (AIG), incluyéndose como parte del nivel directivo de su estructura, al Consejo Nacional para la Innovación Gubernamental, en adelante el Consejo;

Que entre las funciones del Consejo está aprobar las políticas y planes nacionales de desarrollo de tecnología e innovación;

Que debido a la rápida evolución de las Tecnologías de la Información y Comunicación (TIC) se ha incrementado la velocidad, capacidad, agilidad, eficiencia y utilidad de las redes y sistemas actuales en todos los ámbitos del País. Estas tecnologías están cambiando el modo en el que los panameños interactúan entre sí y con el entorno;

Que esta continua y acelerada evolución hace también que puedan realizarse de forma más sencilla ataques cada vez más sofisticados y numerosos, a los sistemas tecnológicos existentes, dando lugar a un nuevo espacio de actuación delictiva, obligando a los responsables nacionales de la seguridad cibernética a disponer de medios técnicos y humanos adaptados para poder hacer frente a las amenazas y sus posibles impactos;

Que la Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas ha sido consensuada con diversos sectores públicos y privados, lo que ha resultado en un documento que será de fortalecimiento para todas las instituciones del País;

Que esta Estrategia Nacional contempla el desarrollo de acciones orientadas a mejorar la Seguridad Cibernética Nacional y hace especial énfasis en la protección de aquellas infraestructuras que son vitales para el bienestar de la población, los servicios básicos, el buen funcionamiento del gobierno y las organizaciones privadas, el bienestar económico y la calidad de vida de las personas;

Que la Autoridad Nacional para la Innovación Gubernamental ha presentado al Consejo Nacional para la Innovación Gubernamental esta Propuesta denominada Estrategia Nacional de Seguridad Cibernética para la protección de infraestructuras críticas;

Que en virtud de lo antes expuesto, el Consejo,

Este documento es fiel copia del original, que reposa en custodia de la Oficina de Asesoría Legal de la Autoridad Nacional para la Innovación Gubernamental.
Olga Maribel Cortez
Jefa de la Oficina de Asesoría Legal

**RESUELVE:**

**PRIMERO:** Aprobar el documento titulado: "Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas", el cual se incluye como Anexo de la presente Resolución.

**SEGUNDO:** Ordenar la publicación de la presente Resolución en la Gaceta Oficial.

**TERCERO:** Esta Resolución regirá a partir de su promulgación.

**FUNDAMENTO DE DERECHO:** Ley 65 de 30 de octubre de 2009. Decreto Ejecutivo No. 205 de 9 de marzo de 2010.

**PÚBLIQUESE Y CÚMPLASE,**

**EL PRESIDENTE**

**ROBERTO C. HENRIQUEZ**
**DELEGADO POR EL PRESIDENTE DE LA REPÚBLICA**

**LOS MIEMBROS,**

**SYGRID BARRAGÁN GUARDIA**
**DELEGADA POR EL MINISTRO DE LA PRESIDENCIA**

**OMAR CASTILLO**
**DELEGADO POR EL MINISTRO DE ECONOMÍA Y FINANZAS**

**CLARA E. DIAZ**
**DESIGNADA PARA LA REPRESENTACION DEL SECRETARIO NACIONAL DE CIENCIA, TECNOLOGÍA E INNOVACIÓN**

**EL SECRETARIO,**

**EDUARDO E. JAÉN**
**AUTORIDAD NACIONAL PARA LA INNOVACIÓN GUBERNAMENTAL**

Este documento es fiel copia del original, que reposa en custodia de la Oficina de Asesoría Legal de la Autoridad Nacional para la Innovación Gubernamental.
Olga Maribel Cortez
Jefa de la Oficina de Asesoría Legal

GOBIERNO NACIONAL
REPÚBLICA DE PANAMÁ

Autoridad Nacional para
la Innovación Gubernamental

**Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas**

## INTRODUCCIÓN

El ciberespacio, que comprende las redes y sistemas de información públicos y privados, son sin duda alguna elementos claves para la prosperidad del País, la fortaleza de nuestra economía e instituciones y el bienestar de los ciudadanos, además de convertirse cada día en una fuente de nuevas oportunidades de innovación y mejora de la calidad de vida de nuestros ciudadanos. Estas infraestructuras soportan el funcionamiento de actividades cotidianas de los ciudadanos, la gestión de las empresas y cada vez más de los servicios públicos. Debido a esta presencia en todos los ámbitos del País y su carácter crítico, se hace necesaria su protección, así como su capacidad de resistencia y funcionamiento ante eventos adversos (resilencia).

Para la protección de estas infraestructuras físicas y virtuales, que forman el ciberespacio, el Estado Panameño ha desarrollado **una Estrategia Nacional de Seguridad cibernética, con el objetivo de:**

> ***"aunar los esfuerzos de sus ciudadanos, empresas e instituciones públicas para redundar en un incremento de la seguridad cibernética que permita el uso confiable de las tecnologías de la información en todos los ámbitos nacionales, todo esto salvaguardando los derechos y libertades fundamentales de los ciudadanos y un entorno económico y regulatorio favorable al crecimiento y desarrollo de las empresas y permitiendo el buen funcionamiento del Estado."***

Para lograr estos objetivos hay que desarrollar acciones que permitan minimizar los factores que hacen vulnerables los sistemas o más aún, que facilitan que las amenazas cibernéticas se materialicen. Estos factores pueden concentrarse en 4 ejes: cultural, legal, tecnológico y organizativo, cada uno de estos factores requiere acciones específicas y la participación de todos los ámbitos del Estado.

Panamá es un nodo importante de comunicaciones y logística a nivel regional y mundial, por lo que garantizar la seguridad en este ámbito es de especial importancia para nuestro país, esto incluye la protección de los sistemas y redes informáticos (seguridad cibernética), lo que hace necesario impulsar la sensibilización de las personas y la formación sobre los riesgos, reforzando las políticas específicas y los procedimientos de seguridad cibernética en los sistemas de información y comunicaciones de ciudadanos, empresas e instituciones, y fortaleciendo el tejido empresarial local especializado en seguridad cibernética.

Esta estrategia además, complementa y fortalece otras iniciativas en desarrollo por parte del Estado como son los proyectos de Internet para Todos, la nube de servicios gubernamentales, la infraestructura de Certificación y Firma Electrónica y el proyecto Panamá sin Papel. También se han tomado como referencia los trabajos desarrollados por CAPATEC para el desarrollo de una Estrategia TIC Nacional, que busca fortalecer el tejido empresarial en el sector.

## LOS RIESGOS ACTUALES DEL CIBERESPACIO

La rápida evolución de las Tecnologías de la Información y Comunicación (TIC) ha incrementado la velocidad, capacidad, agilidad, eficiencia y utilidad de las redes y sistemas actuales en todos los ámbitos

GOBIERNO NACIONAL
REPÚBLICA DE PANAMÁ

Autoridad Nacional para
la Innovación Gubernamental

del País. Estas tecnologías están cambiando el modo en el que los panameños interactúan entre sí y con el entorno.

Esta continua y acelerada evolución hace también que puedan realizarse de forma más sencilla ataques cada vez más sofisticados y numerosos, dando lugar a un nuevo espacio de actuación delictiva, obligando a los responsables nacionales de la seguridad cibernética a disponer de medios técnicos y humanos adaptados para poder hacer frente a las amenazas y sus posibles impactos.

Los diferentes riesgos que afronta Panamá en el uso de las TICs se pueden clasificar de acuerdo a su origen y a los objetivos a quienes puede dirigirse, en particular son relevantes los siguientes:

| Origen | OBJETIVOS | | |
|---|---|---|---|
| | Estado | Sector Privado | Ciudadanos |
| Ataques patrocinados por Estados | Espionaje, ataques contra infraestructuras críticas, APT (Advanced Persistent Threats) | Espionaje, ataques contra infraestructuras críticas, APT | |
| Ataques patrocinados por Sector Privado | Espionaje | Espionaje | |
| Terroristas, extremismo político e ideológico | Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros | Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicio de terceros | |
| "Hacktivistas" | Robo y publicación de información clasificada o sensible, ataque contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicio de terceros | Robo y publicación de información clasificada o sensible, ataque contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicio de terceros | Robo y publicación de datos personales |
| Crimen Organizado | Espionaje | Robo de identidad digital y fraude | Robo de identidad digital y fraude |
| Ataques de perfil bajo | Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicio de terceros | Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicio de terceros | |
| Ataques de personal con accesos privilegiados (Insiders) | Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicio de terceros, robo y publicación de información sensible y clasificada, infección con malware, APT | Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicio de terceros, robo y publicación de información sensible y clasificada, APT | |

Este documento es copia de la copia autenticada, que reposa en la Oficina Institucional de Recursos Humanos de la Autoridad Nacional para la Innovación Gubernamental.

Olga Maribel Cortez
Jefa de la Oficina de Asesoría Legal

GOBIERNO NACIONAL
REPÚBLICA DE PANAMÁ

Autoridad Nacional para
la Innovación Gubernamental

Panamá no es ajena a estos riesgos, es por ello que el Estado, de forma decidida, y en conjunto con la sociedad civil y el sector privado ha venido desarrollando acciones para proteger los intereses nacionales ante estas nuevas amenazas. Estos proyectos toman ahora una nueva importancia al confluir en una Estrategia Nacional que articule las políticas públicas e integre las actuaciones de todos los sectores para incrementar la Seguridad Cibernética Nacional.

## SEGURIDAD CIBERNETICA Y PROTECCIÓN DE INFRAESTRUCTURAS CRITICAS

Esta Estrategia Nacional contempla el desarrollo de acciones orientadas a mejorar la Seguridad Cibernética Nacional y hace especial énfasis en la protección de aquellas infraestructuras que son vitales para el bienestar de la población, los servicios básicos, el buen funcionamiento del gobierno y las organizaciones privadas, el bienestar económico y la calidad de vida de las personas.

Todas estas infraestructuras están ampliamente soportadas en las TIC y tienen un componente marcado, cada vez mayor, de exposición a los riesgos y amenazas del ciberespacio. Además, estas infraestructuras son ampliamente interdependientes, lo que hace extremadamente importante el adoptar una estrategia unificada de protección, que vaya más allá del impacto individual de un incidente de seguridad cibernética en un operador o una infraestructura particular, sino que valore el impacto según los intereses nacionales y cómo puedan verse afectados de forma global.

## ¿POR QUÉ UNA ESTRATEGIA NACIONAL DE SEGURIDAD CIBERNÉTICA PARA PANAMÁ?

La estrategia nacional de Seguridad Cibernética es un instrumento que refleja un acuerdo de Estado y sirve como guía para la ejecución de políticas públicas en Seguridad Cibernética y Protección de Infraestructuras Críticas, y refleja el compromiso máximo del Estado Panameño para la protección de su ciberespacio y la colaboración con otras instituciones nacionales y regionales para alcanzar este mismo fin a nivel mundial.

Esta Estrategia Nacional de Seguridad Cibernética compromete acciones del Estado Panameño identificando los riegos y amenazas, responsables y políticas públicas necesarias.

Los ámbitos de actuación de las políticas públicas van dirigidas a fomentar:

- La protección de los derechos fundamentales de las personas y la lucha contra el uso de las TIC para fines delictivos o terroristas
- La protección de los menores en la red
- El combate a todo tipo de discriminación racial, por credo u orientación sexual.
- la resistencia de las infraestructuras críticas ante incidentes o ataques;
- la integración del Gobierno con la Sociedad Civil y la corresponsabilidad;
- la educación y concienciación de las personas y organizaciones;
- el incremento de la colaboración nacional e internacional.
- El desarrollo de prácticas aceptables para el sector de las TICs
- Desarrollo de campañas de sensibilización y buenas prácticas de prevención.
- Promoción de una cultura de ciberseguridad

GOBIERNO NACIONAL
REPÚBLICA DE PANAMÁ

Autoridad Nacional para la Innovación Gubernamental

## ELEMENTOS DE LA ESTRATEGIA NACIONAL DE SEGURIDAD CIBERNÉTICA Y PROTECCIÓN DE INFRAESTRUCTURA CRÍTICA

**Visión**

**Panamá confiable en el ciberespacio, una labor de todos**

**Premisas**

- Participación amplia de toda la sociedad y corresponsabilidad en el desarrollo de la estrategia y las acciones que derivan de ella.
- Garantizar la libertad y protección de la privacidad de las personas en el ciberespacio.
- Protección de los menores en el ciberespacio.
- Favorecer el desarrollo y crecimiento empresarial en el país y la adopción de la TIC por parte de las empresas en un entorno confiable.
- Establecer mecanismo de colaboración público-privada para el desarrollo de las acciones.
- Incorporar a organismos internacionales relevantes para el asesoramiento en el desarrollo.

**Pilares**

- Proteger la privacidad y los derechos fundamentales de los ciudadanos en el ciberespacio
- Prevenir y detener las conductas delictivas en el ciberespacio o el uso de éste para cualquier tipo de delitos o actos ilícitos.
- Fortalecer la seguridad cibernética de las infraestructuras críticas nacionales.
- Fomentar el desarrollo de un tejido empresarial nacional fuerte en seguridad cibernética, como referencia para la región.
- Desarrollar una cultura de seguridad cibernética a través de la formación, innovación y la adopción de estándares.
- Mejorar la seguridad cibernética y capacidad de respuesta ante incidentes de los organismos públicos.

## DESARROLLO DE LA ESTRATEGIA NACIONAL DE SEGURIDAD CIBERNÉTICA Y PROTECCIÓN DE INFRAESTRCUTURAS CRÍTICAS

**Los ciudadanos panameños seguros en el ciberespacio: Privacidad y Confianza en el uso de las TIC.**

Los derechos fundamentales de las personas y en especial el derecho a la intimidad y privacidad son la prioridad máxima para el Estado. La adopción de las Tecnologías de la Información y las Comunicaciones y su uso en la vida cotidiana para la relación entre personas y con las empresas a través de transacciones de comercio electrónico y los servicios de gobierno electrónico apalancarán la inclusión y la igualdad de oportunidades, sólo si se construyen en un marco de confianza y seguridad para los ciudadanos.

Uno de los principales elementos a tener en cuenta es la protección de la información sensible de las personas, entre ellas sus datos personales, los cuales pueden utilizarse de forma inadecuada para

Este documento es copia de la copia autenticada, que reposa en la Oficina Institucional de Recursos Humanos de la Autoridad Nacional para la Innovación Gubernamental.

Olga Maribel Cortez
Jefa de la Oficina de Asesoría Legal

GOBIERNO NACIONAL
REPÚBLICA DE PANAMÁ

Autoridad Nacional para la Innovación Gubernamental

discriminar personas, además, las características propias de estas BBDD de información de personas, hacen posible que su utilización, transmisión, copia, reproducción y procesamiento sea realizado de forma muy rápida y sencilla, requiriendo que el Estado asuma medidas para prevenir usos que puedan atentar contra la intimidad y privacidad de los ciudadanos.

Actualmente existen diferentes regulaciones e iniciativas para la protección de datos personales en diferentes ámbitos como el entorno bancario y los servicios públicos, sin embargo, dado el compromiso que en el Estado Panameño se le ha dado a este tema, es necesario reforzar y unificar estas acciones para lograr como objetivo que Panamá cuente con un marco regulatorio e institucionalidad con capacidades operativas de vanguardia que garanticen la intimidad y privacidad de las personas en el Ciberespacio y la protección de los derechos fundamentales.

Con especial interés se desarrollarán acciones específicas para la protección de los menores contra amenazas o usos indebidos de las TIC que puedan ponerlos en riesgo.

**Lucha contra el Delito Cibernético y el uso delictivo de las TIC**

La rápida evolución de los delitos cibernéticos requiere una lucha eficaz con el fin de mantener la confianza en el uso de las TIC. Para lograr esto, todos los organismos encargados de hacer cumplir la ley en la cadena delictiva incluyendo la Policía, el Ministerio Público, el Instituto de Medicina Legal y otros servicios de investigación, y el Poder Judicial, que se encargan de la lucha contra la delincuencia cibernética, se están reforzando para lograr incorporar un número mayor de especialistas.

El objetivo es reforzar a los organismos participantes en la cadena judicial, con un marco regulatorio actualizado y unas capacidades operativas que incrementen la voluntad de denunciar un delito de alta tecnología y aumenten la posibilidad de alcanzar a los responsables y que sean tratados con mayor severidad.

La cooperación internacional también permite abordar mejor el problema transfronterizo de los delitos cibernéticos, en este ámbito se intensificarán las acciones de colaboración con otros Estados y se impulsará la adopción de normativa internacional en la materia, como es la Convención de Delito Cibernético del Consejo de Europa.

Dentro de las acciones identificadas, hay que destacar la necesidad constante de dos elementos clave:

- La continua actualización tecnológica de los elementos de captura, preservación, manipulación y análisis de evidencia digital, para mantenerse al día de los últimos avances tecnológicos y contar con la capacidad de responder a las nuevas modalidades delictivas. En este ámbito se reforzarán las capacidades actuales del IMEL.
- La formación de todos los actores del proceso en estas nuevas tecnologías y modalidades delictivas, sus formas procesales y características que permitan que tanto la Policía y sus órganos auxiliares, el Ministerio Público y el Poder Judicial (Jueces, Secretarios, Magistrados, etc) cuenten con los conocimientos necesarios y con mecanismos de actualización.

GOBIERNO NACIONAL
REPÚBLICA DE PANAMÁ

Autoridad Nacional para la Innovación Gubernamental

**Continuidad operativa de las infraestructuras críticas**

Las Infraestructuras Críticas Panameñas requieren, debido a su situación geopolítica, una protección integral. Las repercusiones de un posible incidente sobre muchas de ellas podrían afectar el intercambio económico y bienestar tanto de Panamá como de Latinoamérica y el Caribe. Aquí, destaca de forma especial el Canal de Panamá, como eje de intercambio comercial, así como todas las instalaciones de logística que alimente estas transacciones.

El modelo que ha seguido en la administración del Canal de Panamá, debe extenderse ahora a todo el entramado de infraestructuras críticas nacionales que prestan servicios en el país, en especial los sectores que representan un elemento importante de la economía panameña y los servicios a los ciudadanos.

Para lograr la protección de estas infraestructuras críticas se requiere una estrecha colaboración entre el gobierno y el sector privado para identificar las vías más efectivas de alcanzar las cotas de protección necesarias sin impactando mínimamente las operaciones.

El primer paso para desarrollar este ámbito es la revisión del estado actual de protección de las infraestructuras críticas y el desarrollo de unas buenas prácticas nacionales con requisitos mínimos de protección, aquí una vez más, la vasta experiencia del Canal de Panamá en la materia será una de las principales fuentes a consultar.

También deberán incorporarse dentro de los planes de protección integrales, la realización de ejercicios y simulacros de emergencias para validar los planes de protección y asegurar que los canales de comunicación, la activación de emergencias y las propias medidas de contingencias funcionan apropiadamente.

**Desarrollo empresarial en Seguridad Cibernética**

Panamá no puede abordar la seguridad cibernética como un elemento más de la seguridad nacional sin contar con un tejido empresarial fuerte y con capacidades locales para abordar los grandes proyectos de protección nacional e incorporar soluciones innovadoras, adaptadas tanto a la idiosincrasia de las organizaciones Panameñas, como a la dimensión país.

Es por esto que el Estado asume una decidida apuesta por la innovación en seguridad cibernética y articulará acciones para alinear las capacidades de las empresas nacionales con las prioridades del Estado en seguridad cibernética.

De igual manera, se propiciará la participación de las empresas nacionales en la definición y desarrollo de las acciones derivadas de esta Estrategia Nacional, fomentando la creación de asociaciones o clúster de Empresas que permitan abordar los grandes proyectos.

Para apoyar el desarrollo de conocimiento local, el Estado apoyará soluciones tecnológicas basadas en estándares abiertos que permitan la apropiación tecnológica y el desarrollo e innovación local, también se fomentará el desarrollo colaborativo de proyectos.

Este documento es copia de la copia autenticada, que reposa en la Oficina Institucional de Recursos Humanos de la Autoridad Nacional para la Innovación Gubernamental.

Olga Maribel Cortez
Jefa de la Oficina de Asesoría Legal

GOBIERNO NACIONAL
REPÚBLICA DE PANAMÁ

Autoridad Nacional para
la Innovación Gubernamental

**Desarrollo de una cultura de seguridad cibernética**

Uno de los elementos más importantes a abordar para el fortalecimiento de la Seguridad Cibernética en el País es el desarrollo de una cultura de seguridad cibernética, esto se logra a través de la incorporación progresiva de elementos, conductas y acciones en las personas que permitan evaluar correctamente los riesgos a los que se enfrentan en el uso de los sistemas y las redes de información y tomar decisiones acertadas en pro de su seguridad y la de su entorno.

Este proceso de desarrollo de una cultura de seguridad cibernética requiere desarrollar labores de difusión, sensibilización y formación tanto a los ciudadanos como las organizaciones, este cambio cultural debe originarse desde las bases, por eso uno de los pilares más importantes es la incorporación de estos conceptos en los primeros niveles educativos, que es donde los menores de edad son más vulnerables y actualmente se encuentra expuestos continuamente a numerosos riesgos.

La adopción de esta cultura de seguridad cibernética debe también reflejarse a través de la oferta de educación formal en el área, donde tanto carreras o programas educativos relacionados, como la formación en sistemas, la carrera judicial o derecho, deben siempre incluir aspectos de seguridad cibernética, lo es también necesario para el buen desenvolvimiento de los profesionales en general. Adicionalmente se debe incrementar la oferta de educación formal y programas especializados en seguridad cibernética, incluyendo certificaciones profesionales, estándares y buenas prácticas internacionales y asociaciones civiles y profesionales relacionadas con la seguridad.

Para articular estos cambios, el Estado a través de los organismos de Educación, Desarrollo Humano y Profesional, desarrollará actuaciones con las instituciones educativas, medios de comunicación y otras organizaciones civiles para incluir contenidos formativos en seguridad cibernética en todos los niveles.

**Continuidad operativa de las redes y sistemas de información gubernamentales**

El Gobierno Panameño también ha desarrollado y sigue desarrollando programas para mejorar su eficiencia, agilizar los trámites a los ciudadanos y ofrecer, a través de medios electrónicos más transparencia en su gestión. Dentro de los grandes proyectos nacionales de desarrollo del Gobierno Electrónico destacan la Nube Computacional Gubernamental, la Red Nacional Multiservicios, la Red Nacional de Internet, Panamá sin Papel, y el proyecto de Firma Electrónica Nacional, entre otros.

Todos estos proyectos de adopción de las TIC por parte del Estado, requieren un componente importante de Seguridad Cibernética para asegurar que la incorporación de estas tecnologías no suponga un incremento en los riesgos de los organismos públicos ni atente contra la información de los ciudadanos y organizaciones que estos manejan.

Para garantizar que se están incorporando las medidas mínimas de seguridad cibernética el Estado fomentará el desarrollo de tres programas:

- Esquema de clasificación de la información de los organismos públicos, en función de la criticidad de la misma y el posible impacto que podría tener su destrucción, difusión, robo o revelación no autorizada.
- Adopción de estándares mínimos con controles de seguridad requeridos de acuerdo al nivel de la información gestionada, donde además se proporcionarán soluciones técnicas tipo.

Este documento es copia de la copia autenticada, que reposa en la Oficina Institucional de Recursos Humanos de la Autoridad Nacional para la Innovación Gubernamental.

Olga Maribel Cortez
Jefa de la Oficina de Asesoría Legal

GOBIERNO NACIONAL
REPÚBLICA DE PANAMÁ

Autoridad Nacional para la Innovación Gubernamental

- Incremento de las capacidades de respuesta ante eventos e incidentes de seguridad

Dentro de estas labores el trabajo desarrollado actualmente por la Autoridad de Innovación Gubernamental y específicamente el CSIRT-Panamá es un punto de partida para el desarrollo del Esquema Nacional de Seguridad Cibernética, que contenga las medidas de protección específicas y criterios de clasificación de la información. Igualmente, para el incremento de las capacidades en respuesta ante incidentes, es necesario extender sus capacidades de coordinación y fomentar el desarrollo de equipos locales de respuesta ante incidentes en los organismos del Estado, siempre bajo la coordinación y tutela del CSIRT Panamá.

Este documento es copia de la copia autenticada, que reposa en la Oficina Institucional de Recursos Humanos de la Autoridad Nacional para la Innovación Gubernamental.

Olga Maribel Cortez
Jefa de la Oficina de Asesoría Legal