Gobierno de la República de

Trinidad y Tobago

Estrategia Nacional de Seguridad Cibernética

Preparada por el Comité Interministerial para la Seguridad Cibernética

Diciembre de 2012

Índice

1.0 Resumen ejecutivo

Los gobiernos, las empresas y los ciudadanos se están convirtiendo, en creciente medida, en grandes consumidores de las tecnologías de la información y la comunicación (TIC) y de servicios electrónicos, y recurren más a ellas en las esferas de la gestión, la comunicación, la educación, el comercio, las compras y la prestación de servicios. La realidad de este entorno es que todas las oportunidades que traen consigo las TIC se ven acompañadas, asimismo, por riesgos a la seguridad. A falta de medidas de mitigación y gestión, estos riesgos pueden dañar la reputación del Gobierno de Trinidad y Tobago, tanto en la esfera interna como en la internacional.

Con la presente Estrategia se procura orientar todas las operaciones e iniciativas relacionadas con la seguridad cibernética en Trinidad y Tobago. La estrategia se basa en el Marco de Política de Mediano Plazo 2011-2014 del Gobierno, en el que se destaca el papel de las TIC en la promoción del desarrollo del país. Sus principales objetivos son los siguientes:

i. Crear un entorno digital seguro que permita a todos los usuarios gozar plenamente de los beneficios que ofrece la Internet.

ii. Proporcionar un marco de gobernanza en relación con todos los asuntos de seguridad cibernética mediante la identificación de las estructuras institucionales y administrativas necesarias, incluidas las de recursos humanos, capacitación y desarrollo de capacidades, y las relativas a las necesidades presupuestarias.

iii. Proteger los activos físicos, virtuales e intelectuales de los ciudadanos, las instituciones y el Estado a través de la creación de un mecanismo eficaz para responder a las amenazas cibernéticas, sea cual fuere su origen.

iv. Facilitar la seguridad de todos los ciudadanos promoviendo la sensibilización frente a los riesgos cibernéticos y elaborando medidas de protección eficaces y apropiadas para mitigar riesgos y ataques.

v. Ayudar a prevenir ataques cibernéticos contra la infraestructura crítica y redes de información segura generando competencias entre los principales interesados y el público en general.

vi. Reducir al mínimo los perjuicios y los tiempos de recuperación frente a ataques cibernéticos a través de eficaces medidas de gestión de incidentes.

vii. Crear un marco legal y regulatorio para mantener el orden, proteger la privacidad de los usuarios y penalizar los ataques perpetrados en el ciberespacio.

A fin de alcanzar esos objetivos se han identificado cinco principales áreas de interés:

1. **Gobernanza:** La meta fundamental consiste en el establecimiento de una agencia de seguridad cibernética en Trinidad y Tobago (TTCSA por su sigla en inglés), que sería el principal organismo responsable de todos los asuntos relativos a la seguridad cibernética y el centro de coordinación de todas las operaciones relacionadas con esta materia.
2. **Gestión de incidentes**: Establecimiento de un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT-TT, por su sigla en inglés), como punto focal nacional en materia de información, gestión y respuesta frente a incidentes.
3. **Colaboración**: El establecimiento de alianzas entre los sectores público y privado y la sociedad civil para proteger la infraestructura cibernética del país y promover la cooperación con organismos internacionales.
4. **Cultura:** Sensibilización, capacitación y educación en materia de seguridad cibernética en todas partes del país.
5. **Legislación:** Redacción y promulgación de leyes pertinentes sobre delitos cibernéticos para penalizar las transgresiones pertinentes, procesar a los transgresores y proteger a los ciudadanos.

Con esta estrategia, el Gobierno pretende crear un entorno cibernético seguro y sólido, basado en la mutua colaboración de todos los interesados clave, que permita aprovechar las TIC en beneficio de todos y para la prosperidad de todos.

2.0 Introducción

Las TIC constituyen la base para el desarrollo de toda sociedad moderna y progresista y hace posible su incorporación en la economía mundial de la información.

Los Gobiernos, las empresas y los ciudadanos se están convirtiendo, cada vez en mayor medida, en consumidores de TIC y de servicios electrónicos. La creciente utilización de estos bienes y servicios queda demostrada, entre otras cosas, por su influencia en la educación, el continuo mejoramiento de las redes de comunicación, la mayor facilidad del comercio internacional, los cambios en los sistemas de gestión y compras y los avances en materia de prestación de servicios del cuidado de la salud. En los últimos doce años el uso de TIC se incrementó un 1.310,8% en América Latina y el Caribe[1]/. En el Informe Mundial sobre Tecnología de la Información del Foro Económico Mundial se demuestra que el grado de preparación de Trinidad y Tobago para aprovechar las TIC a fin de incrementar la competitividad y el desarrollo hizo saltar al país del puesto 79 entre 133 países en 2010[2]/ al puesto 60 entre 142 países en 2012[3]/.

El potencial transformador de las TIC y de la Internet ha sido reconocido por el Gobierno de Trinidad y Tobago, que identificó las TIC y el establecimiento de una economía del conocimiento diversificada como pilares independientes del desarrollo dentro de su Marco para el Desarrollo Sostenible[4]/. Lo que se pretende es promover un acceso universal y equitativo a las TIC y a la Internet y su utilización para cerrar la brecha digital y dar lugar a la inclusión de las comunidades subatendidas o carentes de estos servicios.

1 World Internet Usage and Population Statistics, junio de 2012, http://www.internetworldstats.com/stats.htm

2 Foro Económico Mundial, "The Global Information Technology Report 2009-2010: ICT for sustainability, 2010". pág. xvii. http://www3.weforum.org/docs/WEF_GITR_Report_2010.pdf

3 Foro Económico Mundial. "Global Information Technology Report: Living in a hyperconnected world": 2012, pág. xxiii. http://www3.weforum.org/docs/Global_IT_Report_2012.pdf

4 Gobierno de Trinidad y Tobago, "Innovation for Lasting Prosperity: Medium Term Policy Framework, 2011-2014", octubre de 2011.

No obstante, un corolario de las numerosas oportunidades que ofrecen las TIC es la presencia de diversos riesgos en el ciberespacio. Esto hace que la respuesta del país a las amenazas internas y externas deba incluir el despliegue de tecnologías que haga posible el seguimiento y el análisis de los desastres naturales y antropogénicos, la protección física de la infraestructura de información que respalda la economía basada en el conocimiento y la mitigación de las amenazas que puede generar el uso impropio de sistemas de informática. Al tratar de hacer frente a estas amenazas se hace necesario asegurar el mantenimiento de una efectiva comunicación entre los interesados pertinentes. Éste es un componente clave de la realización y el mantenimiento de los objetivos generales de seguridad de las TIC consistentes en **disponibilidad, confidencialidad e integridad.**

A través de esta estrategia se pretende orientar todas las operaciones e iniciativas relacionadas con la seguridad cibernética en Trinidad y Tobago. En ella se reconoce la crítica necesidad de un marco global de gobernanza, una apropiada legislación sobre delitos cibernéticos y el establecimiento de un equipo CSIRT. También se reconoce la importancia de sensibilizar a todos los interesados (el Gobierno, las empresas, las instituciones académicas, la sociedad civil y los ciudadanos) sobre sus funciones y responsabilidades en el establecimiento de un entorno de TIC seguro.

2.1 ¿Qué es seguridad cibernética?

Si bien no existe consenso internacional sobre la definición de seguridad cibernética (o "ciberseguridad" como nombra a este concepto la Unión Internacional de Telecomunicaciones), Trinidad y Tobago se suscribe a la Recomendación UIT-T X.1205 (X.cso) del Sector de Normalización de las Telecomunicaciones del mencionado organismo, en la que se establece lo siguiente:

> "*La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el*

ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno[5]/."

Una seguridad cibernética eficaz garantizaría la disponibilidad, integridad, autenticidad y confidencialidad de un sistema, y evitaría que fuera rechazado; tendría en cuenta la privacidad del usuario y aumentaría la confianza que inspiren los sistemas conexos.

3.0 Razonamiento

La red mundial interdependiente de infraestructuras digitales de TIC conocida como "ciberespacio" constituye la fuerza que impulsa el crecimiento de la economía mundial del conocimiento. El impacto de las TIC se sigue haciendo sentir en todos los sectores de la sociedad en países de todo el mundo, haciendo posibles nuevas prácticas operativas, nuevas modalidades de actuación conjunta entre el Gobierno y los ciudadanos, así como cambios en las relaciones interpersonales. Todo ello, en consecuencia, modifica, entre otras cosas, las estructuras y actividades económicas, sociales y políticas, la infraestructura pública, los servicios públicos, la educación y la seguridad nacional. El propio sector de las TIC también crece continuamente. En la última década las tecnologías se han vuelto aún más poderosas. El acceso al ciberespacio se ha visto facilitado por la aparición de nuevos mecanismos, tales como los dispositivos móviles y la banda ancha móvil, a través de los cuales los contenidos digitales pueden ser generados y compartidos en cuestión de minutos en las redes sociales.

5. Unión Internacional de Telecomunicaciones, http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Las amenazas al ciberespacio constituyen un motivo de gran preocupación para todos los países. Según la Unión Internacional de Telecomunicaciones (UIT) existen pruebas de que los ataques cibernéticos son cada vez más sofisticados, frecuentes y serios. Se estima, por ejemplo, que debido a la automatización de los procesos operativos la cifra diaria de actos de piratería informática puede llegar a los 80 millones[6]. La empresa de seguridad Symantec informa que las pérdidas provocadas en el mundo por los delitos cibernéticos llegan a US$388.000 millones por año. En un estudio llevado a cabo en veinticuatro países por dicha empresa, el 69% de los encuestados declararon haber sido víctimas de tales delitos. Se constató que 431 millones de adultos por año –más de un millón por día– son víctimas de ese tipo de actos[7].

El ciberespacio proporciona el entorno que facilita ataques virtuales organizados contra activos de información y contra la infraestructura física, que incluso pueden llevarse a cabo mediante la utilización de tecnologías de consumo de fácil acceso.

Los delincuentes cibernéticos altamente capacitados pueden ocultar su identidad, su ubicación y sus vías de acceso. Pueden aprovechar el ciberespacio para perturbar comunicaciones y ocultar o demorar una respuesta defensiva, ofensiva o de emergencia. Un ejemplo es el del virus Stuxnet[8], descubierto en 2010, diseñado para atacar sistemas utilizados para controlar y operar instalaciones industriales tales como centrales eléctricas, refinerías petroleras y gasoductos[9].

En Trinidad y Tobago las esferas siguientes se cuentan entre las que pueden ser comprometidas por elementos criminales o terroristas:

---

6 Unión Internacional de Telecomunicaciones, "El ciberdelito: guía para los países en desarrollo", abril de 2009, pág. 72

7 Symantec, "Norton Cybercrime Report 2011", http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/

8 El objetivo final de Stuxnet era manipular el equipo físico adjunto a sistemas de control industrial específicos para que operara en una forma programada por el atacante, contraria a la finalidad a la que estaba destinado.

9 Symantec, "Duqu: the Precursor to the Next Stuxnet", http://www.symantec.com/outbreak/?id=stuxnet

- redes bancarias y financieras en línea
- servicios gubernamentales en línea, tales como TTBizLink
- sistemas de información en tiempo real tales como los de control industrial SCADA (supervisory control and data acquisition), que se usan para manejar las estaciones de bombeo de la Dirección de Agua y Alcantarillado y de la Comisión de Electricidad de Trinidad y Tobago
- la infraestructura de petróleo, gas y petroquímica
- los servicios públicos de transporte aéreo y transporte terrestre

Las experiencias habidas en Trinidad y Tobago, como las registradas en el resto del mundo, no han hecho más que confirmar lo ya sabido: el uso creciente del ciberespacio genera tanto oportunidades como riesgos. La acelerada integración de la Internet en casi todos los aspectos de la actividad social y económica, así como la ubicuidad de las TIC ha aumentado la vulnerabilidad de todas las esferas de la sociedad. El país ha experimentado un incremento en varios incidentes cibernéticos, incluidos la pornografía infantil en línea, el hostigamiento en línea, las tentativas de apropiación indebida de dominios y el pirateo de sitios web. El pirateo de sitios web del Ministerio de Finanzas y del Parlamento ocurrido en abril de 2012, y el saqueo de cajeros automáticos que tuvo lugar en julio de 2012, en que un grupo de ladrones utilizó cámaras hábilmente escondidas para captar los números de identificación personal de las tarjeas de débito y de crédito de algunos clientes de unas cuantas instituciones bancarias importantes son ejemplos locales recientes de un creciente número de incidentes cibernéticos[10].

En respuesta a preguntas de la revista en línea *ICT Pulse*, un experto en seguridad de tecnologías de la información y de redes indicó que lo que está cada vez más de moda en materia de amenazas e intrusiones en Trinidad y Tobago es la "presencia de BOT de comando y control, los intentos de apropiación indebida de dominios y los antivirus falsos, así como los constantes escaneos de puertos"[11].

10 "Cyber Unit and Fraud Squad probe ATM scam". *Trinidad Guardian*, 10 de julio de 2012. http://www.guardian.co.tt/news/2012-07-09/cyber-unit-and-fraud-squad-probe-atm-scam

11 Expert insights 3: Cyber threats and security in the Caribbean. *ICT Pulse*: ICT issues from a Caribbean perspective. 1 de abril de 2012. Entrevista a Aaron Manzano, de HMP Consulting en

El Gobierno de Trinidad y Tobago ha emprendido una serie de programas destinados a ampliar el acceso a las TIC y la asequibilidad económica de las mismas y a reducir la brecha digital. Entre estos se incluye el Programa eConnect and Learn (conocido como eCAL), a través del cual todos los alumnos que ingresen en el primer nivel de educación secundaria reciben laptops, y la flota de autobuses que facilita la capacitación y el desarrollo de capacidades en TIC en zonas rurales insuficientemente atendidas o no atendidas. Estos programas ponen de manifiesto la importancia que se ha dado a las TIC y a la Internet como componente crítico para lograr el crecimiento económico, la competitividad mundial y mejores condiciones de vida para los ciudadanos.

Un enfoque como el referido permite realizar en la máxima medida posible los beneficios que puede brindar la revolución digital. Sin embargo, es necesario que al mismo tiempo se apliquen estrategias que permitan hacer frente a los riesgos vinculados con el uso de la Internet, en especial para nuestros niños y jóvenes.

Trinidad y Tobago debe pues definir y aplicar las políticas, estrategias y planes necesarios para garantizar una continua confianza y certidumbre en la confiablidad de la Internet, la seguridad de los sistemas conectados a la misma, y la seguridad, protección y solidez de la infraestructura digital de las TIC del país.

4.0 Fundamento estratégico

En el MTPF[12]/ del Gobierno de Trinidad y Tobago se hace hincapié en el papel de las TIC como promotoras del desarrollo nacional. En dicho documento se señala:

Trinidad and Tobago. http://www.ict-pulse.com/2012/03/expert-insights-3-cyber-threats-and-security-in-the-caribbean/

12. Gobierno de Trinidad y Tobago, "Innovation for Lasting Prosperity: Medium Term Policy Framework, 2011-2014", octubre de 2011.

1. "El uso de las TIC es un elemento esencial de la infraestructura en que se basa la creación de una economía moderna y competitiva, en un mundo rico en información, impulsado por el saber y la tecnología.
2. La creación de una economía diversificada y en que se utilice el saber en forma intensiva es un factor medular para generar competitividad internacional, estimular nuevas esferas de crecimiento económico y ascender en la cadena de valor[13]/."

El MTPF tiene como premisa el Marco para el Desarrollo Sostenible que se basa en siete pilares de desarrollo interconectados. En el cuarto de ellos *(Tecnologías de la información y la comunicación para conectar a Trinidad y Tobago y crear una nueva economía)* se reconoce la medida en que la adopción y utilización de las TIC es un factor decisivo para el éxito en la consecución de un desarrollo sostenible. La seguridad cibernética es una de las piedras angulares de ese nuevo paradigma de las TIC, pues se considera fundamental establecer el marco legislativo apropiado y la maquinaria de aplicación de normas para la detección, lucha y protección contra los delitos cibernéticos.

4.1 Visión

El Gobierno de Trinidad y Tobago creará un entorno cibernético seguro y sólido, basado en la colaboración entre todos los interesados clave, que haga posible el aprovechamiento de las TIC en beneficio y para la prosperidad de todos.

4.2 Consideraciones de política nacional

Las siguientes son posiciones de política clave que se han adoptado para definir la estrategia de seguridad cibernética para la protección de los activos e intereses nacionales de Trinidad y Tobago:

13. Ídem

- La entidad responsable de la coordinación, la aplicación, el seguimiento, el continuo mejoramiento y la adecuada gestión de las iniciativas de seguridad cibernética será la Agencia de Seguridad Cibernética de Trinidad y Tobago (TTCSA, por su sigla en inglés);

- La seguridad cibernética es un componente de la estrategia de seguridad nacional y del plan nacional de TIC, que a su vez son subconjuntos del Marco para el Desarrollo Sostenible. Como tales, todas las políticas y estrategias pertinentes están sujetas al marco general de políticas.

- En la estrategia de seguridad se tienen en cuenta la protección de datos y de privacidad.

- Se promulgarán y aplicarán leyes generales de alcance nacional sobre delitos cibernéticos que sean aplicables y puedan armonizarse en los ámbitos regional e internacional.

- En la medida de lo posible la estrategia de seguridad cibernética será orientada por acuerdos y estándares internacionales.

- Se promoverá una cultura de seguridad cibernética para sensibilizar y generar confianza en el entorno de las TIC.

- Se promoverá y fortalecerá la coordinación y la colaboración en las esferas nacional, regional e internacional.

- Se promoverá la labor de investigación y desarrollo en la esfera de la seguridad cibernética para desarrollar capacidades y mantener una sólida base de conocimientos.

5.0 Marco de referencia

La creación y aplicación de un plan nacional de seguridad cibernética requiere una estrategia general que incluya un amplio examen de la suficiencia de las actuales prácticas nacionales y la consideración del papel que han de cumplir en este proceso todos los interesados (las autoridades gubernamentales, la sociedad civil, las instituciones académicas, las empresas y los ciudadanos).

Se han identificado los siguientes **objetivos estratégicos** en consonancia con marcos de referencia internacionales:

i. Crear un entorno digital seguro que ponga a todos los usuarios en condiciones de gozar plenamente de los beneficios que ofrece la Internet.

ii. Proporcionar un marco de gobernanza en relación con todas las cuestiones de seguridad cibernética mediante la identificación de las estructuras institucionales y administrativas necesarias que hayan de exigirse, incluidas las necesidades de recursos humanos, capacitación y desarrollo de capacidades y recursos presupuestarios.

iii. Proteger los activos físicos, virtuales e intelectuales de los ciudadanos, las instituciones y el Estado a través de la creación de un mecanismo que permita hacer frente eficazmente a las amenazas cibernéticas, sea cual fuere su origen.

iv. Facilitar la seguridad de todos los ciudadanos haciéndolos conscientes de los riesgos cibernéticos y elaborando eficaces y adecuadas medidas de protección para mitigar riesgos y ataques.

v. Ayudar a prevenir ataques cibernéticos contra la infraestructura crítica y las redes de información segura generando las aptitudes pertinentes entre los principales interesados y el público en general.

vi. Reducir al mínimo los perjuicios causados por ataques cibernéticos y los tiempos de recuperación, a través de eficaces medidas de gestión de incidentes.

vii. Crear un marco jurídico y reglamentario para mantener el orden, proteger la privacidad de los usuarios y penalizar los ataques perpetrados en el ciberespacio.

Para alcanzar esos objetivos se han identificado y se describen a continuación cinco áreas clave:

1. Gobernanza
2. Gestión de incidentes
3. Colaboración
4. Cultura
5. Legislación

5.1 Gobernanza

Los esfuerzos que realice Trinidad y Tobago en materia de seguridad cibernética deben estar orientados a hacer frente eficazmente a las amenazas, dinámicas y graves, de que es objeto el ciberespacio. Ello requiere un marco general de gobernanza para coordinar y administrar eficazmente una estrategia general de seguridad cibernética.

Es preciso identificar y hacer frente a las vulnerabilidades existentes que podrían generar las más graves perturbaciones en los sistemas y la infraestructura críticos de Trinidad y Tobago. El Gobierno promoverá la creación de nuevos sistemas con menos vulnerabilidades y, simultáneamente, realizará una continua evaluación de tecnologías emergentes para detectar imperfecciones. Se elaborarán y harán cumplir normas comunes para dotar de seguridad a la infraestructura de TIC, los servicios y los repositorios de datos en todo el territorio de Trinidad y Tobago. Asimismo, se llevarán a cabo exámenes periódicos de normas, políticas y reglamentos, y se promoverá la comunicación bilateral y multilateral entre los ministerios y otros organismos gubernamentales.

Es preciso lograr cohesión entre el sector público, el sector privado y todos los interesados clave para administrar la respuesta del país a las amenazas cibernéticas, cuya evolución es incesante, y para coordinar la labor de la amplia gama de entidades cuyos cometidos en materia de gestión de estos problemas parezcan superponerse. A este respecto debe aplicarse un Marco de Gobernanza para proporcionar la infraestructura necesaria para la gestión y coordinación de todas las actividades relacionadas con esta respuesta.

Por vía de una ley, el Gobierno de Trinidad y Tobago establecerá la Agencia de Seguridad Cibernética de Trinidad y Tobago que proporcionará los servicios necesarios para cumplir las siguientes funciones clave:

1. Asesoría e implementación de la estrategia nacional de seguridad cibernética.
2. Suministro de información para crear conciencia sobre la situación, y recopilación y análisis de datos sobre temas de seguridad cibernética.
3. Promoción de una eficiente gestión de seguridad de redes y seguridad de la información.
4. Sensibilización y promoción de la cooperación local e internacional.

La TTCSA se encargará de coordinar o realizar la gestión de las siguientes áreas funcionales clave de la seguridad cibernética:

1. Elaboración y aplicación de marcos de gestión para todas las áreas funcionales.
2. Gestión y respuesta ante incidentes.
3. Estudios forenses e investigaciones en materia cibernética (función que desempeñará la Unidad de Delitos Cibernéticos del Servicio de Policía de Trinidad y Tobago).
4. Promoción de una cultura, educación, capacitación e investigación en materia de seguridad cibernética.
5. Comunicaciones, colaboración internacional y alianzas públicas y privadas;
6. Aspectos jurídicos en materia de seguridad cibernética (continuo examen y recomendación de enmiendas a la legislación);

7. Interdependencia de la Protección de la Infraestructura de Información Crítica (CIIP) y de la Protección de la Infraestructura Crítica (CIP).

Ese marco de gobernanza proporcionará una estructura sostenible que puede evolucionar para atender la realidad de la seguridad cibernética en Trinidad y Tobago.

Se ha elaborado ya la estructura orgánica que se propone para la TTCSA y se presenta como anexo I.

5.2 Gestión de incidentes

A fin de dar seguridad y fortalecer la infraestructura de información crítica del país se deben realizar esfuerzos coordinados tendientes a mitigar o controlar incidentes del modo más rápido y eficiente posible. En consecuencia, se necesita una institución que pueda fungir como punto focal nacional en materia de información, gestión y respuesta frente a incidentes.

El Gobierno de Trinidad y Tobago establecerá un equipo CSIRT que se encargará de:

- difundir información sobre seguridad cibernética;
- proporcionar orientación y respaldo técnicos en caso de incidentes cibernéticos, y
- promover la colaboración bilateral y multilateral entre entidades gubernamentales nacionales, el sector privado, las instituciones académicas y la comunidad internacional de equipos CSIRT.

El equipo CSIRT de Trinidad y Tobago estaría en condiciones de:

- alertar sobre potenciales amenazas, incidentes y ataques;
- facilitar el intercambio de información entre las entidades representadas en el equipo CSIRT con respecto a prácticas óptimas, información para investigaciones, coordinación de la respuesta frente a incidentes y procedimientos y procesos de gestión de incidentes;
- analizar vulnerabilidades, incidentes y metodologías de ataques cibernéticos;
- proporcionar asistencia técnica al Gobierno de Trinidad y Tobago y a otros interesados dentro del marco nacional;
- realizar investigaciones y análisis forenses;
- realizar actividades de defensa frente a ataques, centradas especialmente en la infraestructura de información crítica, y
- orientar programas nacionales de recuperación en caso de incidentes cibernéticos.

La creación y puesta en marcha del equipo CSIRT se basarán en estándares del sector y prácticas óptimas internacionales, y harán que la comunidad nacional tenga conocimiento de los protocolos de información de incidentes cibernéticos.

El equipo CSIRT tendrá su sede en la TTCSA.

5.3 Colaboración

Proteger el ciberespacio es una responsabilidad compartida, en que cada uno de los protagonistas cumple un papel clave en la cadena de seguridad. Para que se logre realmente la seguridad cibernética, la estrategia que se adopte debe ser pertinente para el contexto local y al mismo tiempo compatible e interoperable con la que adopten otros países, de ahí que se subraye la decisiva importancia de la cooperación y colaboración nacional e internacional.

5.3.1 Colaboración nacional

La existencia de una alianza entre los sectores público y privado y la sociedad civil es esencial para proporcionar seguridad a la infraestructura cibernética de Trinidad y Tobago, cuyo gobierno también formará parte de dicha alianza para la aplicación de su estrategia de seguridad cibernética.

Se facilitará la cooperación a través de intercambio de información, participación en foros de tecnología e investigaciones y análisis, a fin de proporcionar insumos para la elaboración y difusión de prácticas óptimas para la seguridad cibernética.

Las empresas privadas, incluidas las proveedoras de servicios de Internet, tienen que cumplir un papel importante en la labor de dar seguridad al ciberespacio, ya que son propietarias de grandes redes y sistemas de informática. Se instará a estas entidades a evaluar la seguridad de las redes que influyen en la seguridad de la infraestructura crítica de Trinidad y Tobago. Esto incluiría:

- La realización de estimaciones y auditorías de riesgos.
- La elaboración de planes de continuidad en que se tengan en cuenta las necesidades de personal y equipos.

- La participación en actividades de intercambio de información y la difusión de prácticas óptimas en todo el sector.

El ministerio responsable de la seguridad nacional promoverá asimismo la elaboración de otros programas de certificación en seguridad cibernética que serán reconocidos en el país y aceptados por los sectores público y privado.

5.3.2 Colaboración internacional

Dada la interconectividad de las infraestructuras de las TIC y el carácter mundial de las amenazas cibernéticas, se requiere cooperación y colaboración internacionales para darles seguridad. Esa colaboración tendría por objeto crear sensibilidad en materia de seguridad cibernética, mejorar el intercambio de información sobre datos recíprocos, participar en la formulación de normas y estándares internacionales, adoptar y adaptar tales normas y buenas prácticas en todas las dimensiones de la seguridad cibernética; proporcionar asistencia jurídica mutua y participación en investigaciones coordinadas y en el procesamiento penal de los perpetradores de delitos cibernéticos.

Un aspecto clave de esa cooperación internacional es la promoción de debates desde la perspectiva de un pequeño Estado insular en desarrollo, en especial en cuanto a su relación con convenciones internacionales sobre delitos cibernéticos que puedan afectar económicamente a Trinidad y Tobago y a otros pequeños Estados. Ello requerirá una participación más intensa en organismos normativos regionales, hemisféricos e internacionales.

A la fecha, las principales fuentes de asistencia internacional para Trinidad y Tobago en la esfera de la seguridad cibernética han sido la Organización de los Estados Americanos (OEA), la Unión Europea (UE), la Unión de Telecomunicaciones del Caribe (CTU por sus siglas en inglés) y la Unión Internacional de Telecomunicaciones (UIT). No obstante, se reforzará el intercambio de información y la cooperación con otros organismos multilaterales, como la Comunidad del Caribe (CARICOM), la Secretaría

del Commonwealth y el Consejo de Europa. También se explorarán vías para el fortalecimiento de la cooperación bilateral.

5.4 Cultura

Se admite que la sensibilización sobre el tema en todo el país constituye un requisito previo para lograr una protección eficaz del ciberespacio. El Gobierno de Trinidad y Tobago guiará la creación de una cultura de seguridad cibernética, para lo cual será necesario adoptar un enfoque multidisciplinario y coparticipativo que incluya actividades de sensibilización, inserción de la seguridad cibernética en los más amplios aspectos de la formulación de políticas y educación de los usuarios de las TIC y de la Internet acerca de sus respectivos papeles en el ciberespacio.

Además, el Gobierno de Trinidad y Tobago, en coordinación con el sector privado, se ocupará de educar al público en general y a las pequeñas, medianas y grandes empresas en temas básicos de seguridad y protección del ciberespacio. Inicialmente, se centrará la atención en la elaboración de directrices y la creación de programas en la esfera de la seguridad cibernética para alumnos de escuelas de enseñanza primaria y secundaria.

También se alentará a las instituciones de educación superior a que adopten políticas y medidas necesarias para mejorar la seguridad de los sistemas.

La investigación y la innovación científicas revisten también decisiva importancia como garantía de la seguridad cibernética y el desarrollo de la economía digital nacional. Por lo tanto, se realizarán actividades de capacitación e investigación continua tendientes a mantener sistemas confiables y al mismo tiempo generar resistencia a amenazas actuales y futuras. El Gobierno de Trinidad y Tobago asignará

recursos para capacitación y educación de personas que puedan desarrollar estos instrumentos y especializarse en dar seguridad a la estructura de información crítica.

Los ministerios competentes en materia de seguridad nacional y ciencia y tecnología promoverán también la capacitación avanzada de profesionales de seguridad cibernética en instituciones educativas públicas y privadas, y el establecimiento de estándares de certificación de profesionales calificados en seguridad de las TIC.

El ministerio competente en materia de seguridad nacional alentará a organismos y compañías privados a proporcionar suficientes oportunidades de educación continua y capacitación avanzada en el lugar de trabajo para mantener altos niveles de aptitudes y la capacidad de innovar. También abogará por la coordinación de programas de capacitación entre el Gobierno y el sector privado.

5.5 Legislación

Uno de los objetivos del marco nacional de política en la materia es la ampliación de las capacidades de conexión del país a la Internet, para que todos los interesados estén en condiciones de realizar negocios y obtener acceso a una amplia gama de servicios gubernamentales. Como corolario, se reconoce el hecho de que el Gobierno debe cumplir un papel importante en el establecimiento de una política clara, dotada de un marco reglamentario y jurídico en relación con los delitos cibernéticos. Por lo tanto, el Gobierno de Trinidad y Tobago elaborará una política nacional sobre delitos cibernéticos y adoptará una legislación nacional en la materia.

Reconociendo el hecho de que una firme vigilancia en materia de delitos cibernéticos es necesaria para el goce de los beneficios digitales, el Gobierno de Trinidad y Tobago elaborará un marco jurídico adecuadamente definido para establecer y mantener el orden y la seguridad de los usuarios del entorno electrónico y sancionar a quienes deliberadamente dañen computadoras y redes electrónicas.

El marco legislativo:

- adoptará un enfoque integral para hacer frente a los delitos cibernéticos y otros delitos conexos para tener en cuenta la acelerada evolución de las TIC en el mundo;
- tipificará delitos tales como el acceso ilegal, la interceptación ilegal y la violación de derechos de propiedad intelectual, los delitos relacionados con la identidad, el correo electrónico basura, el hostigamiento cibernético, así como actos de instigación y complicidad;
- facilitará la recopilación y admisibilidad de pruebas electrónicas;
- promoverá investigaciones transfronterizas con Gobiernos regionales e internacionales y con los organismos encargados de aplicar las leyes, y
- creará un conjunto de expertos judiciales de los sectores público y privado con fines de intercambio de experiencia técnica y conocimientos.

6.0 Metas operativas y actividades conexas

La Estrategia Nacional de Seguridad Cibernética, definida por las cinco metas operativas arriba referidas, puede representarse en forma tabular, como a continuación se expone:

Metas operativas		**Actividades**	
1.0	Crear un marco apropiado de gobernanza para la seguridad cibernética	1.1	Establecer la Agencia de Seguridad Cibernética de Trinidad y Tobago.
		1.2	Elaborar y aplicar estándares comunes de seguridad de las TIC en todos los ámbitos gubernamentales.
		1.3	Proporcionar un mecanismo de examen y evaluación periódicos de las políticas y

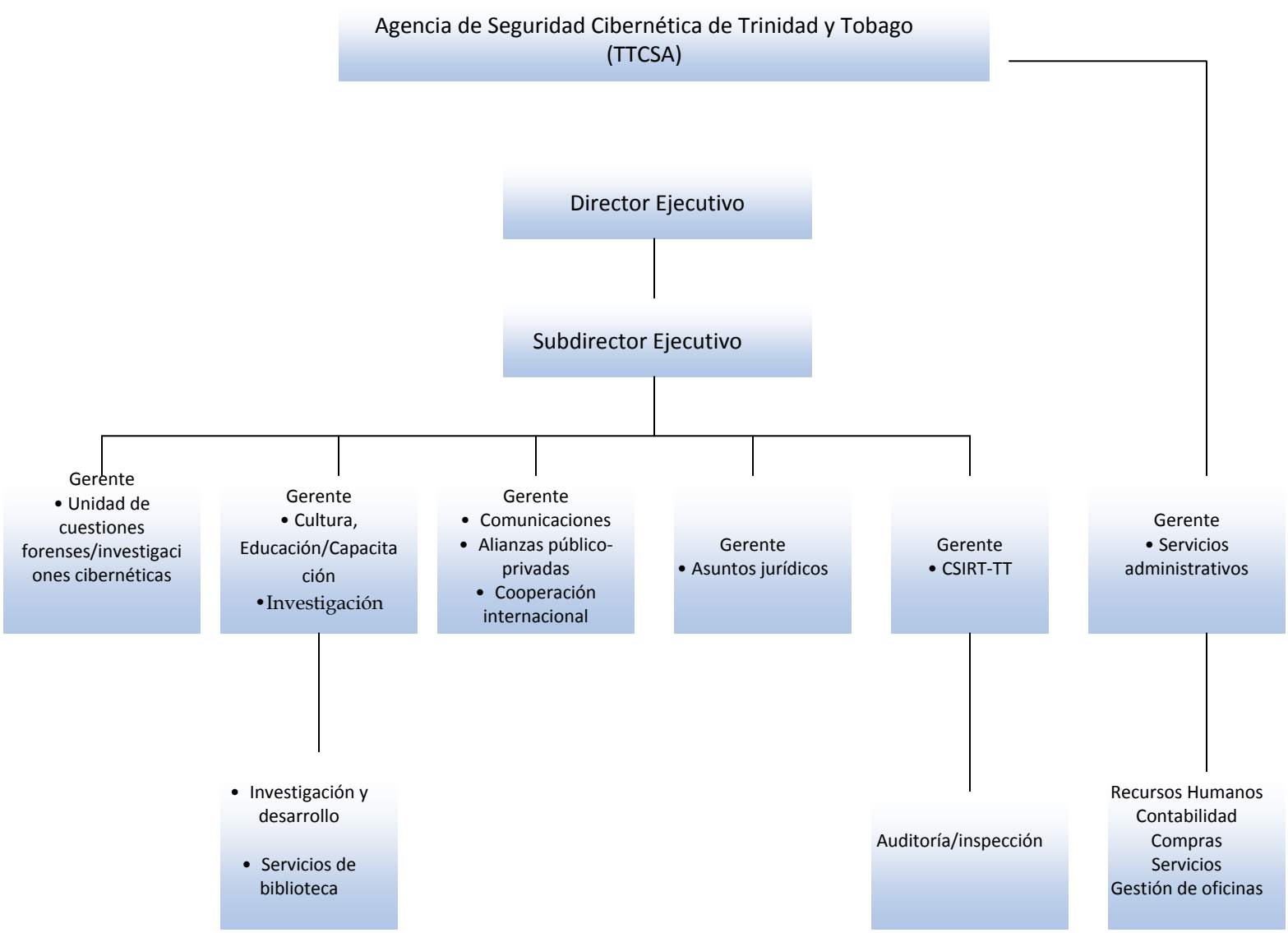
			reglamentos nacionales sobre seguridad cibernética.
2.0	Desarrollar capacidades nacionales de gestión de incidentes	2.1	Establecer un mecanismo centralizado de respuesta ante incidentes de seguridad informática (CSIRT-TT).
		2.2	Lograr que exista conciencia de la situación en todos los ámbitos de la red GovNeTT.
		2.3	Crear un sistema nacional coordinado de respuesta en materia de seguridad cibernética para prevenir, detectar y responder frente a incidentes cibernéticos y facilitar las tareas de recuperación.
		2.4	Establecer puntos focales para la gestión de incidentes cibernéticos, en que converjan elementos críticos del sector público (incluidas las entidades encargadas de la aplicación de las leyes), operadores y proveedores de infraestructura para reducir el riesgo y la gravedad de los incidentes.
		2.5	Participar en mecanismos de vigilancia, alerta e intercambio de información en materia de respuesta frente a incidentes.
		2.6	Elaborar, poner a prueba y aplicar planes, procedimientos y protocolos de respuesta frente a emergencias para tener la certeza de que los colaboradores del sector público y de los demás sectores puedan generar confianza y coordinar eficazmente sus actividades si sobreviene una crisis.

3.0	Establecer relaciones de colaboración entre el sector público, la sociedad civil y la empresa privada que procuren realizar una eficaz gestión del riesgo cibernético y proteger el ciberespacio.	3.1	Proporcionar un mecanismo que reúna diversas perspectivas, experiencia técnica y conocimientos para lograr consenso con el fin de conseguir mejoras en materia de seguridad en el país.
		3.2	Incluir perspectivas empresariales en las más tempranas etapas de elaboración y aplicación de la política de seguridad y programas conexos.
		3.3	Alentar el desarrollo de entidades privadas de diferentes sectores de infraestructura esencial para hacer frente a intereses de seguridad comunes en un espíritu de mutua colaboración con el gobierno.
		3.4	Reunir a los sectores privado, civil y público en foros que gocen de confianza para hacer frente a problemas comunes de seguridad cibernética.
		3.5	Alentar la mutua colaboración entre grupos pertenecientes a organismos y entidades interdependientes.
		3.6	Establecer mecanismos de cooperación entre el Gobierno y diversas entidades en materia de gestión de incidentes.
4.0	Promover una cultura nacional de seguridad congruente con las resoluciones de la Asamblea General de las Naciones Unidas 57/239 y 58/199, tituladas, respectivamente, "Creación de una cultura mundial de seguridad cibernética" y "Creación de una cultura mundial de seguridad cibernética y	4.1	Implementar un plan de seguridad cibernética para sistemas operados por el sector público.
		4.2	Implementar programas e iniciativas de sensibilización en materia de seguridad para usuarios de sistemas y redes.
		4.3	Alentar la creación de una cultura de seguridad cibernética en las empresas.
		4.4	Respaldar las labores de extensión a la

protección de las infraestructuras de información esenciales".	sociedad civil, prestando especial atención a las necesidades de los niños y los usuarios individuales. 4.5 Promover un amplio programa nacional de sensibilización para que todos los interesados –las empresas, los trabajadores y la población en general– den seguridad a sus lugares en el ciberespacio. 4.6 Crear conciencia sobre los riesgos cibernéticos y las soluciones disponibles. 4.7 Reforzar las iniciativas sobre ciencia y tecnología y sobre investigación y desarrollo. 4.8 Revisar el régimen de privacidad existente para que sea congruente con el entorno digital. 4.9 Hacer de la seguridad de las tecnologías de la información una prioridad en la educación superior. 4.10 Revisar la política de seguridad institucional y mejorar la utilización de las herramientas de seguridad existentes. 4.11 Integrar la labor realizada en la educación superior con el programa nacional de fortalecimiento de la infraestructura crítica. 4.12 Lograr una mejor colaboración entre el sector de la educación superior, las empresas y el gobierno.

5.0 Impedir el delito cibernético	5.1 Promulgar y hacer cumplir la legislación relativa a la seguridad cibernética y el delito cibernético. 5.2 Desarrollar las capacidades locales de las entidades encargadas de la aplicación de las leyes. 5.3 Desarrollar capacidades judiciales locales.

7.0 Anexo: Estructura orgánica de la Agencia de Seguridad Cibernética de Trinidad y Tobago



8.0 Glosario

Apropiación indebida de dominios: el hecho de obtener acceso a una computadora sin autorización o rebasando el acceso autorizado.

BOT de control y comando: un grupo de computadoras comprometidas que ejecutan programas informáticos sujetos a control externo.

Ciberespacio: conjunto de capacidades, tales como sensores, señales, conexiones, transmisiones, procesadores y controladores que generan una experiencia virtual interactiva a la que se accede con fines de comunicación y control, sea cual fuere la ubicación geográfica. El ciberespacio permite a la red interdependiente de infraestructuras de tecnologías de la información, redes de telecomunicaciones tales como la Internet, sistemas de informática, sensores integrados, redes de control de sistemas y procesadores y controladores integrados comunes realizar actividades de control y de comunicaciones globales.

Correo basura: El envío masivo de mensajes de correo electrónico no solicitados, así como los mensajes mismos.

Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT, por su sigla en inglés): un órgano de servicio encargado de recibir, examinar y responder a informes y actividades en materia de incidentes de seguridad informática. Generalmente este equipo proporciona sus servicios a determinadas entidades, que podrían consistir en una entidad matriz, tal como una compañía, un organismo gubernamental o una institución educativa, una región o un país, una red de investigación o un cliente que pague por el servicio.

GovNeTT: la red de área amplia del Gobierno de Trinidad y Tobago es la columna vertebral de la red de comunicación y colaboración entre los ministerios y otras dependencias gubernamentales que proporciona una plataforma global para la prestación de servicios de TIC relacionados con el sector público, incluida la capacidad de prestar servicios de correo electrónico, acceso a la Internet, transmisión de mensajes, etc.

Hostigamiento cibernético: el hecho de que una persona esté siendo atormentada, amenazada, acosada, humillada, puesta en situación embarazosa o sea objeto de actos hostiles por parte de otra persona mediante el uso de la Internet, tecnologías interactivas y digitales o teléfonos móviles.

Infraestructura crítica: sistemas, dispositivos, redes y programas de informática, así como datos informáticos tan vitales para el país que la incapacitación o destrucción de los mismos, o el hecho de que tales sistemas y activos sufran interferencias iría en detrimento de la seguridad, la defensa o las relaciones internacionales del Estado, la prestación de servicios directamente relacionados con la seguridad nacional o económica, los servicios bancarios y financieros, la infraestructura de comunicaciones, la salud y la seguridad pública nacional, el trasporte público, la infraestructura pública clave o cualquier combinación de estas.

Pirateo: penetración no autorizada en una computadora, una red o un sitio web.

Programa eConnect and Learn (eCal): constituye el principal de los programas gubernamentales destinados a aumentar la accesibilidad a tecnologías de la información y la comunicación entre los estudiantes e infundir dicha tecnología en la educación a través del suministro de computadoras portátiles a todos los alumnos que ingresan en el primer nivel de enseñanza secundaria. Está destinado a lograr que los estudiantes obtengan la capacidad y las aptitudes necesarias para el siglo XXI.

Saqueo de cajeros automáticos: un tipo de fraude consistente en la grabación de los números de una tarjeta de crédito o de débito y su ulterior transferencia a un duplicado de la misma, sin conocimiento del tenedor de la tarjeta original.

Tecnologías de la información y la comunicación: las tecnologías utilizadas por las personas para dar a conocer, distribuir y recopilar información y para comunicarse a través de computadoras y redes de computadoras.

TTBizLink: denominación dada a la ventanilla electrónica única de facilitación del comercio y los negocios, destinada a mejorar la competitividad en general de Trinidad y Tobago a través de la aplicación de las TIC.

ttconnect: Conjunto de servicios electrónicos suministrados por varios canales a través de la cual se puede obtener acceso a información y servicios. Comprende los cinco canales de entrega siguientes:

» *ttconnect* Online: portal de gobierno electrónico
» *ttconnect* Service Centers: centros de servicio ubicados estratégicamente en diferentes partes del territorio de Trinidad y Tobago
» *ttconnect* Self-serve: quioscos de autoservicio automatizados
» *ttconnect* Mobile: sistema de acceso a información y servicios del Gobierno a través de teléfonos inteligentes portátiles
» *ttconnect* Express: autobuses adaptados para las TIC que funcionan como centros de servicio móviles

9.0 Referencias

1. Cyber Unit and Fraud Squad probe ATM scam. *Trinidad Guardian*, 10 de julio de 2012. http://www.guardian.co.tt/news/2012-07-09/cyber-unit-and-fraud-squad-probe-atm-scam

2. Expert insights 3: Cyber threats and security in the Caribbean. ICT Pulse: ICT issues from a Caribbean perspective. Entrevista realizada el 1 de abril de 2012 a Aaron Manzano, de HMP Consulting en Trinidad y Tobago. http://www.ict-pulse.com/2012/03/expert-insights-3-cyber-threats-and-security-in-the-caribbean/

3. Gobierno de Trinidad y Tobago, "Innovation for Lasting Prosperity: Medium Term Policy Framework, 2011-2014", octubre de 2011.

4. Unión Internacional de Telecomunicaciones, "El ciberdelito: guía para los países en desarrollo", abril de 2009.

5. Unión Internacional de Telecomunicaciones, "National Cybersecurity Strategy Guide", septiembre de 2011. People's Partnership, "Prosperity for All- 2010 Manifesto of the People's Partnership for a United People to Achieve Sustainable Development for Trinidad and Tobago"

6. Symantec, "Duqu: The Precursor to the Next Stuxnet", http://www.symantec.com/outbreak/?id=stuxnet

7. Symantec, "Norton Cybercrime Report 2011", http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/

8. Foro Económico Mundial, "The Global Information Technology Report 2009-2010: ICT for sustainability", pág. xvii. http://www3.weforum.org/docs/WEF_GITR_Report_2010.pdf.

9. Foro Económico Mundial. "Global Information Technology Report: Living in a hyperconnected world", 2012, pág. xxiii. http://www3.weforum.org/docs/Global_IT_Report_2012.pdf

10. World Internet Usage and Population Statistics, junio de 2012, http://www.internetworldstats.com/stats.htm