

ESTRATEGIA NACIONAL DE
**SEGURIDAD
CIBERNÉTICA**



Por el Ministerio de Gobernación:

Licenciado Enrique Antonio Degenhart Asturias
Ingeniero Gabriel Juárez Lucas
Ph. D. Lic. Román Estuardo Cancinos Arbizú
Luis Fernando Ruíz Ordoñez

Diseño Gráfico:

Stephanie Lara
Haroldo García

ISBN: 978-9929-764-89-7

**MINGOB. 2018. Estrategia Nacional de Seguridad Cibernética.
Ministerio de Gobernación. Documento Técnico No. 1 (1-2018)**

Guatemala de la Asunción, Marzo de 2018. Edición Digital

Ministerio de Gobernación

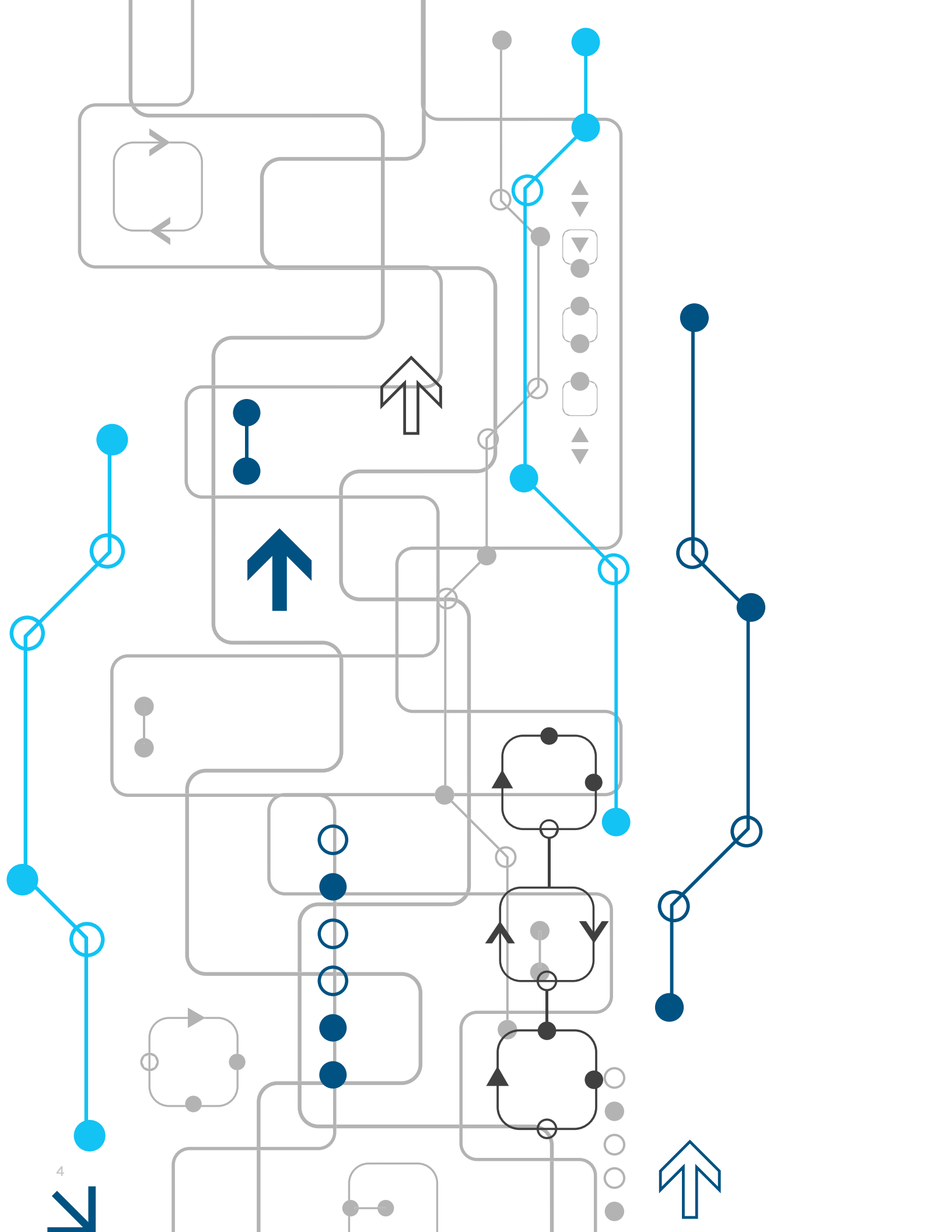
6a. Avenida, 13-71 Zona 1, Guatemala, Guatemala
PBX: (502) 2413 8888
Código Postal: 01001

www.mingob.gob.gt



ÍNDICE

Palabras Preliminares	5
Introducción	9
Antecedentes	13
I. Diagnóstico Nacional de la Seguridad Cibernética	14
I. 1 Infraestructuras Críticas	14
I. 2 Las Tecnologías de Información y Comunicaciones	16
I. 3 La Investigación y Respuesta a Incidentes Cibernéticos	21
I. 4 La Administración Pública	23
I. 5 El Sector Privado y Financiero	24
I. 6 Sensibilización y Educación	25
II. Construcción de la Estrategia	27
III. Visión y Principios Generales	31
IV. Ejes, Objetivos y Acciones	32
Eje 1. Marcos Legales	34
Eje 2. Educación	38
Eje 3. Cultura y Sociedad	42
Eje 4. Tecnologías de Información	46
V. Gobernanza de la Seguridad Cibernética	50
Acrónimos	57
Glosario	58
ANEXO	63
Madurez de la Seguridad Cibernética en Guatemala	64
Estrategia Nacional Oficial	65
Cultura y Sociedad	65
Educación	67
Marcos Legales	67
Tecnologías	69
Agradecimientos	73





El mundo cibernético afronta cambios sustanciales, especialmente en las tecnologías de la información y las comunicaciones, las cuales juegan un papel preponderante en los lineamientos de seguridad y desarrollo establecidos en la Política General de Gobierno 2016-2020, en donde se fomenta la educación, la innovación y la competitividad dentro de sus planes de acción.

El crecimiento acelerado del acceso, uso y dependencia de los sistemas de información digital es evidente en todos los ámbitos de la sociedad guatemalteca, reflejándose en la capacidad de compartir información de manera casi instantánea, provocando como fenómeno asociado acciones que amenazan la seguridad de las personas y vulneran la disponibilidad, integridad y confidencialidad de los sistemas de información multisectoriales en el país,

por lo que se hace inminente contar con una Estrategia Nacional de Seguridad Cibernética que proporcione respuestas a los requerimientos provenientes de la gestión de incidentes cibernéticos.

Lo anterior implica grandes desafíos a nivel de Nación, como una visión clara en la protección de bienes, activos y servicios en el ecosistema digital, aunado a la responsabilidad compartida y acciones coordinadas con otros Estados, en tanto que la cooperación internacional constituye un pilar en la seguridad cibernética.

La participación de todos los sectores responsables e involucrados en el tema hace posible construir las bases para la creación de una cultura de seguridad cibernética. Esto representa el primer paso para elevar el nivel de conciencia de las amenazas y vulnerabilidades en el uso de las tecnologías de la información, permitiendo que se generen los espacios de articulación al más alto nivel para fortalecer las capacidades de resiliencia ante incidentes de esta naturaleza.

La Estrategia Nacional de Seguridad Cibernética presenta objetivos y acciones que se implementarán en el marco de los mecanismos de colaboración, cooperación y coordinación del Sistema Nacional de Seguridad; y que a la vez contribuirán un mayor desarrollo al fortalecimiento de la cooperación interinstitucional y público-privada, facilitando las condiciones para lograr la participación, el desarrollo y el ejercicio de los derechos de los guatemaltecos en el ciberespacio.

Jimmy Morales Cabrera

Presidente de la República de Guatemala



El internet ha evolucionado de ser una herramienta convencional a un medio fundamental para intercambiar datos e información de distinta naturaleza; esto ha permitido el desarrollo de varios sectores fundamentales como la educación, salud, comercio, seguridad, entre otros. El impacto de su uso creciente constituye al internet como una pieza importante para el desarrollo integral de las naciones.

La tendencia a un mundo cada vez más interconectado, trae consigo una serie de riesgos y amenazas en un ambiente virtual que concluyen lamentablemente en ilícitos que repercuten en los derechos, el patrimonio y algunas veces en la integridad de las personas, tales como el secuestro, la pornografía infantil, extorsión, trata de personas, entre otros.

De lo anterior, y acorde a los instrumentos legales y técnicos existentes en el país, el Ministerio de Gobernación presenta la Estrategia Nacional de Seguridad Cibernética, donde se proponen líneas de acción que contribuyen al cumplimiento del Plan Nacional de Desarrollo a través de la incorporación de las tecnologías digitales en un entorno seguro para alcanzar el desarrollo sostenible del país.

La Estrategia Nacional de Seguridad Cibernética, ha sido diseñada en coherencia a los instrumentos de Seguridad de la Nación, aportando al desarrollo de los programas estratégicos de la Política Nacional de Seguridad, así como a la implementación del Plan Estratégico de Seguridad de la Nación 2016–2020. Orientada por la Agenda Nacional de Riesgos y Amenazas y la Agenda Estratégica de Seguridad de la Nación, presenta un análisis del escenario deseado que permita mitigar los riesgos y amenazas provenientes del ciberespacio, estableciendo acciones estratégicas para alcanzar las metas y objetivos propuestos.

A partir de los distintos foros se formularon los ejes, objetivos y acciones, que constituyen los marcos del trabajo a realizar en los planes de acción de los Comités de Seguridad Cibernética con una visión compartida. Desde estos espacios de articulación se definirán los actores, acciones, instituciones, y alineaciones a los planes estratégicos institucionales, y en el caso de instancias gubernamentales, la inclusión del componente de la Estrategia de Seguridad Cibernética en los planes operativos anuales, así como la formulación y monitoreo de convenios con la iniciativa privada.

De esta forma, se presenta a la ciudadanía guatemalteca la Estrategia Nacional de Seguridad Cibernética, que constituye un instrumento de dirección y articulación de los diferentes actores en un marco de gestión del riesgo cibernético y de integralidad en el abordaje de la seguridad.

Enrique Antonio Degenhart Asturias
Ministro de Gobernación



Uno de los mayores retos que presenta la Estrategia Nacional de Seguridad Cibernética es la incorporación del ciberespacio en los ámbitos de seguridad planteados en el Sistema Nacional de Seguridad, de tal manera que se generen espacios de articulación estratégicos para formular acciones encaminadas a la protección de los ciudadanos, su patrimonio y sus datos personales con el fin de garantizar el libre ejercicio de sus derechos en dicho ámbito.

La dependencia de plataformas digitales y la necesidad de mecanismos de intercambio de información de manera rápida y segura, hacen que garantizar la disponibilidad, integridad y confidencialidad de las mismas se convierta en una prioridad nacional. En este sentido, se ha identificado que es fundamental la participación de todos los sectores del país y la articulación de todos los

instrumentos estratégicos para gestionar de forma adecuada los incidentes cibernéticos. Es en esta articulación donde el rol y posicionamiento del IV Vicedespacho de Tecnologías de Información y Comunicaciones del Ministerio de Gobernación se hace relevante para potencializar su función de proponer políticas, estrategias y planes para la integración tecnológica del Sistema Nacional de Seguridad.

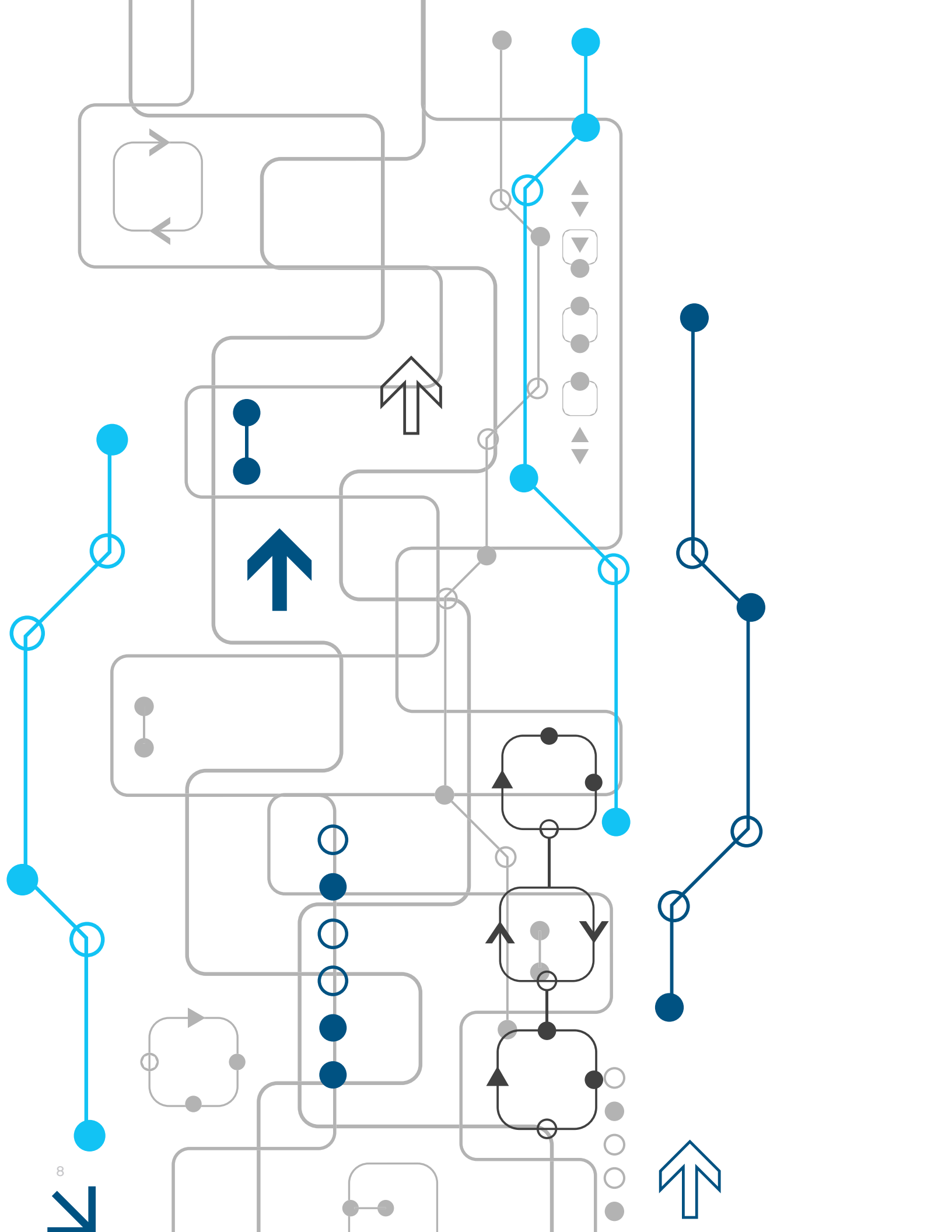
Esta integración tecnológica se logrará con las acciones que la Estrategia Nacional de Seguridad Cibernética propone y que serán implementadas a través de los Comités Técnicos conformados según las temáticas utilizadas para la discusión y construcción de este documento como la academia, sociedad civil, infraestructuras críticas, sector privado y financiero; y el sector público. De la misma manera, se propone la conformación de un espacio de articulación de alto nivel, siendo este el Comité Nacional de Seguridad Cibernética que coordinará, y dará seguimiento a las políticas y estrategias en materia de seguridad cibernética fortaleciendo los mecanismos de colaboración, cooperación y coordinación intersectorial, requeridos para asegurar la plena integración tecnológica en los ámbitos de funcionamiento del Sistema Nacional de Seguridad.

Con base a lo anterior, se diseñarán los planes de acción en los distintos ámbitos con la participación de todos los sectores de la sociedad guatemalteca, donde se definirán los responsables, los recursos y los tiempos necesarios para alcanzar el objetivo general de la Estrategia con una visión coordinada, participativa e integral.

Esto inicia una nueva etapa en Guatemala en donde a través de una responsabilidad compartida, bajo los principios de eficiencia y proporcionalidad, se fortalecen las capacidades de la Nación para ser resilientes ante incidentes cibernéticos; elevando el nivel de conciencia sobre la importancia de este tema en todos los sectores del país.

Gabriel Juárez Lucas

Cuarto Viceministro
De Tecnologías de Información y Comunicaciones





INTRODUCCIÓN

La Estrategia Nacional de Seguridad Cibernética, constituye el primer paso para establecer directrices y objetivos basados en el Eje de Transformación tecnológico planteado en la Política Nacional de Seguridad, que constituye una de las dimensiones interrelacionadas y complementarias que conforman y propician el ambiente de Seguridad de la Nación. Así también, permite dar cumplimiento a la Resolución de la Organización de Estados Americanos AG/RES. 2004 (XXXIV-O/04)¹ denominada “Adopción de una estrategia interamericana integral de seguridad cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética”, en la que se insta a los Estados a fortalecer una red regional de cooperación, coordinación y comunicación a través de la implementación de un CSIRT Nacional.

Esta Estrategia es de gran importancia para Guatemala, dado que las amenazas y ataques cibernéticos surgen y evolucionan derivado de las diversas actividades que se desarrollan por la interconexión de medios digitales, lo cual representa una complejidad de condiciones que requieren la participación de todos los sectores del país, para poder desarrollar los marcos técnicos y jurídicos que fortalezcan la seguridad cibernética tanto a nivel nacional como global.

Los ataques a los sistemas de información ponen en peligro la integridad, confidencialidad y disponibilidad de los datos, incidiendo de tal forma, en la vulnerabilidad de las personas, la competitividad de sus economías y su estabilidad, razón por la cual Guatemala, debe contar con una Estrategia Nacional de Seguridad Cibernética, que permita mitigar las amenazas y ataques provenientes del ciberespacio, sin perder todas las ventajas que suponen las tecnologías de la información; y en caso de un incidente, contar con la **resiliencia** necesaria para reestablecer los servicios en el menor tiempo posible, evitando pérdida de información crítica y daños mayores.

¹ <https://www.sites.oas.org/cyber/Documents/Estrategia-seguridad-cibernetica-resolucion.pdf>

Los daños provocados por los ataques cibernéticos con toda su gama de variaciones, así como la participación de la delincuencia organizada que actúa a nivel transnacional, invitan a la reflexión para establecer nuevas líneas de acción que fortalezcan las normativas y a la adopción de estándares en seguridad cibernética con el fin de proteger los bienes jurídicos de las personas, instituciones y sistemas informáticos.

Para efectos de la presente Estrategia se adoptará la definición de Seguridad Cibernética determinada por la Unión Internacional de Telecomunicaciones, organismo especializado de la Organización de las Naciones Unidas para las tecnologías de la información y la comunicación, que establece en la Recomendación UIT-T X.1205, aprobada con la Resolución 181.10, lo siguiente:

*“La Seguridad Cibernética 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 Seguridad Cibernética 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. Los objetivos de seguridad incluyen una o más de las siguientes: **disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; confidencialidad”.***

En ese orden de ideas, las iniciativas internacionales impulsadas desde la Organización de Estados Americanos, el Consejo de Europa, y la Cumbre Mundial de la Sociedad de la Información, proponen el marco de la visión de los objetivos estratégicos planteados en la Estrategia Nacional de Seguridad Cibernética que buscan direccionar el potencial de la tecnología de la información y la comunicación de una manera sostenible.

En el contexto de la Política de Desarrollo K’atun: Nuestra Guatemala 2032, el crecimiento económico, el manejo sostenido de los recursos y servicios ambientales y el fortalecimiento de las organizaciones, son considerados como medios para el desarrollo de las capacidades esenciales de la personas. Por lo que esta Estrategia propone líneas de acción que contribuyen al cumplimiento del Plan Nacional de Desarrollo para que los guatemaltecos puedan disfrutar de una vida larga y saludable, alcanzar educación, acceder a los recursos básicos y lograr un nivel de vida digno, en un ámbito y espacio seguro en su más amplia expresión.

La Estrategia Nacional de Seguridad Cibernética, ha sido elaborada a partir de un proceso de consulta y validación con actores claves a nivel nacional y regional, contando con la participación de más de 160 representantes de los distintos sectores de la sociedad guatemalteca. En el contexto de Seguridad Cibernética, se articula a los instrumentos de Seguridad de la Nación, aportando al desarrollo de los programas estratégicos de la Política






Nacional de Seguridad, así como a la implementación del Plan Estratégico de Seguridad de la Nación 2016–2020. Orientada por la Agenda Nacional de Riesgos y Amenazas y la Agenda Estratégica de Seguridad de la Nación, presentando un análisis del escenario deseado que permita mitigar los riesgos y amenazas provenientes del ciberespacio, estableciendo acciones estratégicas para alcanzar las metas y objetivos propuestos.

Se plantean objetivos encaminados al fortalecimiento de las capacidades y actuaciones de las instituciones que conforman el Sistema Nacional de Seguridad, bajo la perspectiva del Programa Estratégico para la implementación de la Gestión Integral de la Seguridad de la Nación (GISEG), estableciendo una adecuada actuación interinstitucional y efectividad de sus aportes y responsabilidades con respecto a las actuaciones internas y externas del Sistema.

Estos objetivos y acciones buscan también la integralidad en el abordaje de la seguridad planteado en el Programa Estratégico orientado a la promoción de la Seguridad para el Desarrollo (SEGDE). Al ser las tecnologías de información y comunicaciones un componente sustantivo para este programa, la Estrategia coadyuva a gestionar el desarrollo por medio del fortalecimiento de los mecanismos que construyen las capacidades y competencias del Sistema Nacional de Seguridad, actuando en los elementos que mejoran los retornos sociales de las inversiones económicas en áreas de intersección de la seguridad y el desarrollo.

Bajo la perspectiva de la gobernanza integral, esta Estrategia es coherente con los principios orientadores, los lineamientos y programas estratégicos establecidos en la Política Nacional de Seguridad; de igual manera, articula otras como la Política Nacional de Desarrollo Rural Integral, la Política Criminal Democrática del Estado de Guatemala, Política de Defensa de la Nación, Política Nacional Prevención de la Violencia y el Delito, entre otras.

La Estrategia Nacional de Seguridad Cibernética, se presenta con 5 capítulos:

- | | |
|---|---|
|  | 1 Diagnóstico Nacional sobre el Estado de la Seguridad Cibernética en el país, |
|  | 2 Construcción de la Estrategia, |
|  | 3 Visión y Principios Generales, |
|  | 4 Ejes, Objetivos y Acciones, |
|  | 5 Gobernanza de la Seguridad Cibernética |

El **capítulo (I)** Diagnóstico Nacional de la Seguridad Cibernética en Guatemala, presenta la justificación para la elaboración de esta Estrategia por medio de: información relevante del nivel de penetración de internet; evaluación de infraestructuras críticas; índice de desarrollo en las tecnologías de información y telecomunicaciones; investigación y estado de respuesta a incidentes cibernéticos; y la gestión gubernamental relacionada a la seguridad cibernética.

En el **capítulo (II)** Construcción de la Estrategia, se detalla la metodología utilizada y adaptada de organismos internacionales como la Organización de Estados Americanos y la Unión Europea; así también, de los lineamientos y la orientación técnica que proveyó la Secretaría de Planificación y Programación de la Presidencia (SEGEPLAN), para la construcción del presente documento.

En el **capítulo (III)** se presenta la Visión y Principios Generales que enmarcan los fundamentos que rigen el diseño, así como la fuente de inspiración para la implementación de la Estrategia Nacional de Seguridad Cibernética.

En el **capítulo (IV)** se describen los Ejes, Objetivos y Acciones que constituyen los elementos base para la construcción de los planes de acción bajo una visión alineada y un enfoque multisectorial.

Por último, en el **capítulo (V)** Gobernanza de la Seguridad Cibernética, se plantea bajo el enfoque de gestión integrada y dentro del marco del Sistema Nacional de Seguridad, la coordinación de la seguridad cibernética a nivel nacional.

Antecedentes

Guatemala, en cuanto a desarrollo tecnológico se refiere, ha buscado diversos medios para implementar proyectos en dicho ámbito, desde equipar escuelas con computadoras y llevar tecnología a las aulas, hasta promover proyectos tecnológicos en materia de seguridad y la salud².

El uso de las tecnologías de información y comunicación; así como el creciente acceso a la internet, juegan un papel transformador cada vez más significativo en todos los sectores económicos y sociales de Guatemala. Estas herramientas digitales se han convertido en un factor clave para que ciudadanos, empresas y gobierno; se interconecten e interactúen entre sí, considerando que la Superintendencia de Telecomunicaciones, por medio de su boletín estadístico del 2do semestre³ del año 2016, indica que la cantidad de números móviles en operación alcanza los 18.26 millones, esto supone que un buen porcentaje de la población cuenta con al menos un dispositivo o medio informático de comunicación. Estas herramientas empoderan a los ciudadanos en su vida cotidiana a través del fomento de la inclusión social y la comunicación en sectores vulnerables; de igual manera, incrementa la productividad al enriquecer las bases de información, y mejora la gobernanza gracias a la eficacia y la innovación tecnológica permitiendo una mayor participación y rendición de cuentas.

En esa línea, el Gobierno de Guatemala, no escatima esfuerzos en proyectos como Gobierno Electrónico, Gobierno Abierto por medio del Plan de Acción Nacional 2016–2018⁴; y también en la Agenda “Nación Digital”⁵ lanzada en el mes de febrero de 2017, que buscan integrar de forma objetiva y efectiva, todos los esfuerzos que en materia de desarrollo tecnológico se están realizando en el país enfocados en cinco ejes de acción: Salud, Educación, Seguridad, Desarrollo y Transparencia. Estos proyectos se gestionan con distintas mesas técnicas de carácter multisectorial y se realizan con la visión de integrar esfuerzos, implementando una metodología inclusiva, en donde Sociedad Civil, Academia, Organismos Internacionales e instituciones de Gobierno, juegan un papel protagónico basados en las premisas de transparencia y participación.

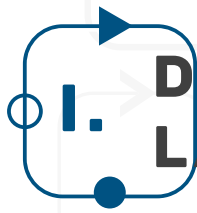
Este compromiso de fomentar el desarrollo tecnológico y la seguridad en el ciberespacio, permitió dar un paso importante con la aprobación de la Estrategia Nacional de Seguridad Cibernética, en la I reunión ordinaria de 2018 del Consejo Nacional de Seguridad, que es la máxima autoridad del Sistema Nacional de Seguridad y le corresponde la definición políticas y estrategias en la materia.

² http://repositorio.cepal.org/bitstream/handle/11362/35499/S2013129_es.pdf?sequence=1&isAllowed=y

³ <https://sit.gob.gt/download/boletin-2do-semester-2016/?wpdmdl=4013>

⁴ <http://mingob.gob.gt/wp-content/uploads/2016/11/Tercer-Plan-de-Gobierno-Abierto-2016-2018.pdf>

⁵ <https://www.naciondigital.gob.gt/>



DIAGNÓSTICO NACIONAL DE LA SEGURIDAD CIBERNÉTICA

Este apartado presenta un análisis del estado actual de la seguridad cibernética en el país enfocado en varios ejes importantes con el fin de justificar la necesidad de articular a todos los actores responsables del tema por medio de un instrumento estratégico que presente las líneas de acción necesarias para lograr una coordinación nacional adecuada.

El diagnóstico se elaboró con base a entrevistas y consultas a expertos del tema, y por medio de mesas de trabajo interinstitucionales e intersectoriales conformadas para discutir temáticas específicas que fueron la base para la definición de los ejes estratégicos y que se presentan a continuación:

Infraestructuras Críticas

Uno de los grandes retos a los que se enfrentan los gobiernos ante las distintas amenazas que han surgido durante el desarrollo tecnológico, es la formulación de iniciativas que fortalezcan los marcos jurídicos específicos para la protección de infraestructuras críticas.

Guatemala está inserta en marcos internacionales que regulan la cooperación en el tema de infraestructuras críticas, los cuales han sido liderados por países como Estados Unidos, que resulta ser el primer país en generar un documento relacionado a la protección de infraestructuras críticas denominado Directiva Presidencial número 39 (PDD-39)⁶, en donde se declara la necesidad de crear un Comité para revisar las vulnerabilidades de las mismas ante ataques terroristas. Estas fórmulas y experiencias como la planteada por la Unión Europea que es priorizar la protección de las infraestructuras con dimensión transnacional⁷, se han incluido dentro de las estrategias de seguridad cibernética en otros países del continente americano.

Es importante señalar que los principales objetivos de actos delincuenciales relacionados al cibercrimen se centran en los crecientes y complejos ataques a las infraestructuras críticas, dentro de las cuales resaltan la red eléctrica, red de telecomunicaciones y transporte. Por lo que es importante desarrollar y fortalecer los marcos normativos y regulatorios relacionados a infraestructuras críticas debido a que si se interrumpe el funcionamiento de las mismas se tendría un impacto negativo considerable en la seguridad, salud, bienestar económico de las

⁶ <https://fas.org/irp/offdocs/pdd/pdd-39.pdf>

⁷ El enfoque de la Unión Europea, es plantear como objetivo prioritario la protección de las infraestructuras con dimensión transnacional. Esto dio inicio al Programa Europeo para la Protección de las Infraestructuras Críticas PEPIC, con la finalidad de identificar las mismas, analizar sus vulnerabilidades y su interdependencia; así también, presentar soluciones que prevengan y protejan ante todo tipo de peligros. Dicho programa ayuda a integrar las variables de la amenaza y sus consecuencias en sus evaluaciones del riesgo. Las Fuerzas y Cuerpos de Seguridad y de Protección Civil de los Estados miembros también integran el PEPIC en sus tareas de planificación e información.

personas y en el eficaz funcionamiento de las instituciones del Estado y las administraciones públicas⁸.

En Guatemala, algunas infraestructuras críticas son propiedad del Estado, mientras que otras pertenecen al sector privado. En las entrevistas y cuestionarios, se mencionó que falta un listado claro de las infraestructuras y sistemas de información críticos nacionales. Tampoco existen normas que obliguen la adherencia a buenas prácticas de seguridad de la información.

Uno de los desafíos a la Seguridad de la Nación, según el Libro Blanco de Seguridad, es la optimización de la gestión de riesgo, que buscará articular las instituciones públicas y privadas para desarrollar resiliencia, defensa civil, protección de infraestructuras críticas, investigación científica y tecnológica.

De igual forma, cabe señalar que el Plan Estratégico de Seguridad de la Nación 2016-2020 propone reformas legislativas, entre las cuales incluye una Ley de Tecnología y Seguridad Cibernética. Aunque este Plan contiene aspectos importantes acerca de la gestión de riesgo e identificación de vulnerabilidades, no establece acciones específicas en el ámbito de la Seguridad Cibernética y Protección de Infraestructuras Críticas.

La Política Nacional de Seguridad sí contiene un lineamiento específico que instruye a:

Desarrollar mecanismos efectivos encaminados a la protección del ciberespacio y la construcción de cultura de ciberseguridad en la sociedad.

En esa línea, la Coordinadora Nacional para la Reducción de Desastres (CONRED), ha desarrollado un plan para la recuperación de desastres naturales, y en Guatemala se llevan a cabo ejercicios para la gestión de crisis. Sin embargo, no se realizan ejercicios o planes específicos para la gestión de incidentes o ataques cibernéticos contra la infraestructura crítica nacional a pesar que la Ley Marco del Sistema Nacional de Seguridad establece en el ámbito de Gestión de Riesgos y Defensa Civil, que la prevención, preparación, mitigación, respuesta y recuperación debe enfocarse ante eventos tecnológicos además de los de orden natural y social.

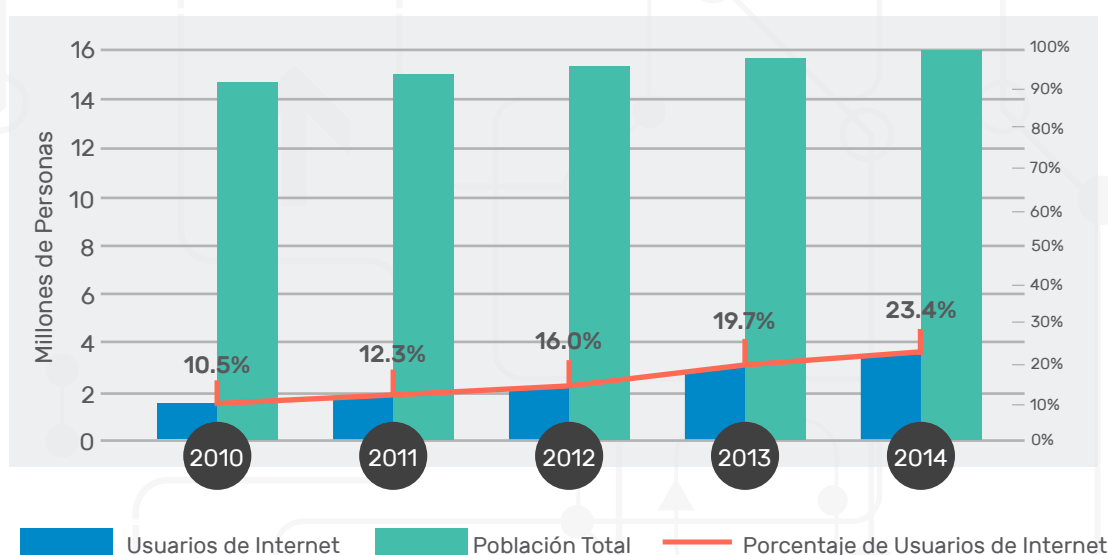
Por último, el reporte de incidentes cibernéticos críticos no es obligatorio para los operadores de las infraestructuras críticas nacionales. Durante las entrevistas y cuestionarios realizados a expertos para la formulación de esta Estrategia, se destacó la importancia de reglamentar esta práctica, ya que políticas voluntarias de informes de incidentes cibernéticos serían difíciles de implementar sin dicha reglamentación.

⁸ Directiva europea: 2008/114/CE del 8 de diciembre de 2008.

Las Tecnologías de Información y Comunicaciones

En términos porcentuales, la penetración de Internet en Guatemala mostró un incremento significativo en los últimos años, dado que aumentó de un 10.5 por ciento en 2010 a un 23.4 por ciento en 2014; es decir, más de 12.9 puntos porcentuales en cuatro años (Gráfico 1). Sin embargo, el país sigue con una de las tasas más bajas de penetración de la región. El porcentaje de hogares con Internet es de sólo 15 puntos porcentuales, según los datos de la Unión de Telecomunicaciones Internacional (UTI). El Foro Económico Mundial (WEF, por sus siglas en inglés), a través del Reporte Global de las Tecnologías de la Información de 2016, indica que Guatemala se encuentra en el puesto 84 de 137 países en términos del costo de la banda ancha fija, y en el puesto 103 de 139 países en cuanto al índice de preparación tecnológica.

Gráfico 1: Población Total vs Usuarios de Internet (2010-2014)



Fuente: Indicadores del Desarrollo Mundial (IDM) – Banco Mundial. Recuperado el 10 de agosto de 2016.

Pese a la enorme brecha digital de las tecnologías de la información y comunicación; es decir, la separación que existe entre las personas que utilizan las TICs como una parte rutinaria de su vida diaria y aquellas que no tienen acceso a las mismas; en las entrevistas a expertos se destacó que existe una alta aceptación y uso de las tecnologías de la información y comunicación en todos los sectores. El acceso a Internet es ofrecido por entidades comerciales, y los teléfonos inteligentes son de alta utilización en Guatemala; sin embargo, es importante recalcar que existe una brecha digital extensa entre las zonas urbanas y rurales en términos de conexión y uso de las tecnologías.

De acuerdo con el Índice de Desarrollo de las TICs (IDI, por sus siglas en inglés) formulado por la Unión de Telecomunicaciones Internacional (UIT) en 2016⁹, Guatemala se encuentra en el puesto 123 de 175 países y tiene un IDI de 3.20 de un total de 10 puntos; el cual está por debajo del promedio mundial en 2016, que es 4.94 puntos. El IDI contempla 11 indicadores cuantitativos relativos a (Gráfico 2):

Gráfico 2: Guatemala - Índice de Desarrollo de las TICs (2015-2016)



Fuente: Índice de Desarrollo de las TICs - UIT. Recuperado el 2 de febrero de 2017.

⁹ <http://reports.weforum.org/global-information-technology-report-2016/economies/#economy=GTM>

Tabla 1. Indicadores de infraestructuras de TIC y acceso

Indicadores de acceso a las TIC	4.47
Suscripciones telefónicas fijas por cada 100 habitantes	10.57
Suscripciones de telefonía móvil-celular por cada 100 habitantes	111.48
Ancho de banda de Internet Internacional (bit/s) por usuario de Internet	24676.45
Porcentaje de hogares con una computadora	22.16%
Porcentaje de hogares con acceso a Internet	17.38%
Indicadores de uso de las TIC	1.4
Porcentaje de personas que utilizan Internet	27.1%
Suscripciones de banda ancha fija por cada 100 habitantes	2.83
Suscripciones de banda ancha móvil activas por cada 100 habitantes	10.08
Indicadores de habilidades en las TIC	4.29
Promedio años de escolaridad	7.01
Tasa media matrícula secundaria	63.53
Tasa media matrícula terciaria	18.33

Fuente: <http://www.itu.int/net4/ITU-D/idi/2016/#idi2016countrycard-tab>M>

Cabe señalar que en términos de acceso a las TICs, la puntuación del país en cuanto a suscripciones de celulares es significativa, al igual que la puntuación para el ancho de banda internacional de Internet por usuario, que equivale a 24.6 Kilobits/s.

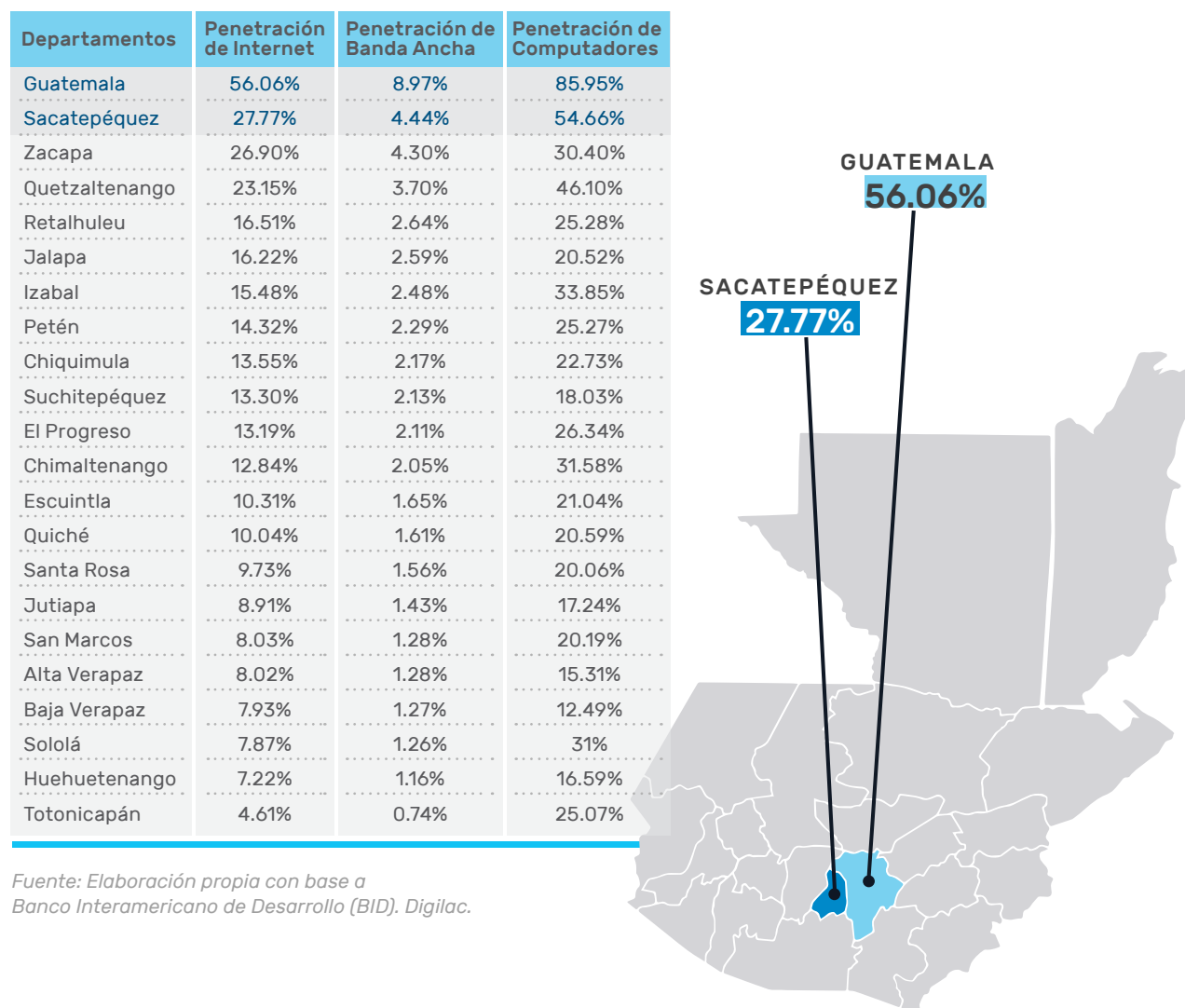
La suscripción de celulares, es una de las más altas de la región, con más de una suscripción por persona. El porcentaje de suscripciones telefónicas fijas es el 10.57 por ciento, siguiendo una tendencia mundial de disminución debido a la preferencia de los nuevos usuarios por tecnologías móviles. No obstante, el número de hogares con equipo de cómputo es muy bajo, solamente el 22.16 por ciento, al igual que el porcentaje de hogares con acceso a Internet con el 17.38 por ciento. Por otro lado, según un estudio de la Comisión Económica para América Latina y el Caribe (CEPAL), Guatemala está entre los países de la región que tuvieron las mayores tasas de crecimiento del número de hogares conectados a Internet entre 2010 y 2015.

De acuerdo con los datos de 2015 del Índice de desarrollo de la banda ancha para la región de América Latina y el Caribe del Banco Interamericano de Desarrollo (BID), los precios

mensuales del servicio de banda ancha móvil están entre los más altos de Centroamérica, a pesar de que Guatemala presenta un mercado de banda ancha móvil relativamente competitivo. En cuanto a los servicios de banda ancha fija, los precios son los más bajos de Centroamérica a pesar también de que existe una menor competencia en la prestación de servicios. Sin embargo, los datos del Foro Económico Mundial, demuestran que Guatemala se encuentra en el puesto 84 de 139 países en relación al costo de la banda ancha fija del índice de preparación tecnológica de 2016, índice que busca analizar el nivel de innovación y la tendencia de los países a aprovechar las oportunidades que ofrecen las TICs.

Además, es importante observar que la brecha digital entre las zonas urbanas y rurales en términos de conexión, se demuestra en los porcentajes de penetración de internet en donde Guatemala y Sacatepéquez, que son los departamentos con mayor índice de urbanidad, tienen los porcentajes de penetración más altos con: 56.06 y 27.77 por ciento, respectivamente (Gráfico 3).

Gráfico 3: Guatemala - Porcentajes de Penetración de Internet

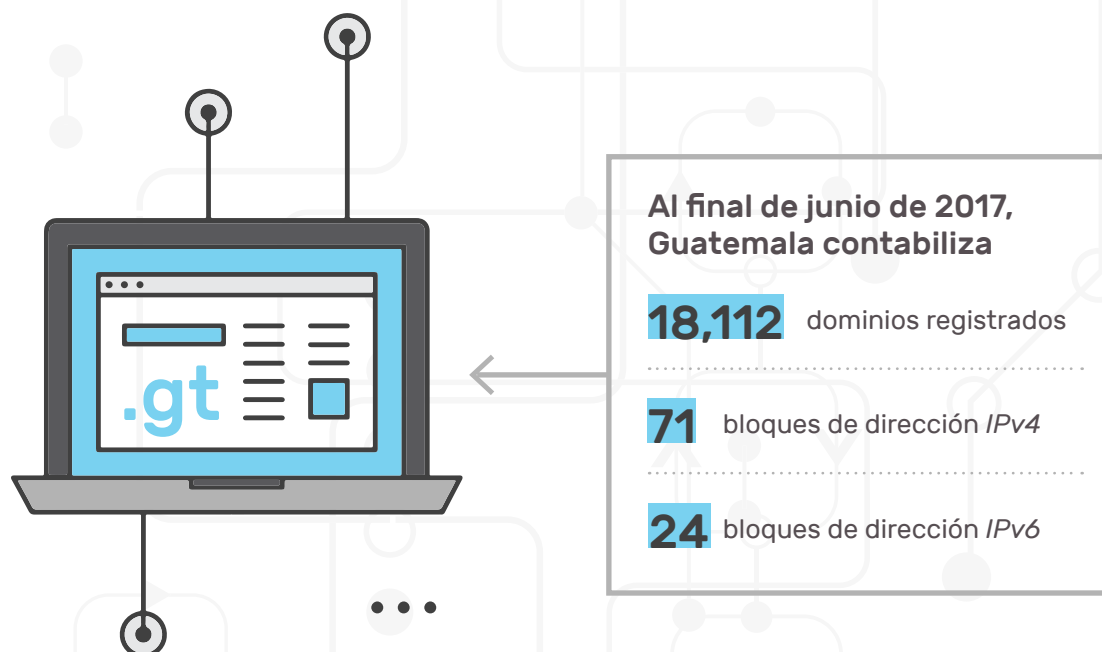


Fuente: Elaboración propia con base a Banco Interamericano de Desarrollo (BID). Digilac.

En el uso de las tecnologías a nivel empresarial, Guatemala es superior a la mayoría de los países de Centroamérica, ya que hacen un mayor uso del Internet para sus transacciones comerciales en comparación con los países vecinos. De hecho, en el indicador sobre el uso de TICs por las empresas, del índice de preparación tecnológica del Reporte Global de las Tecnologías de la Información del 2016, Guatemala se encuentra en el puesto 45 de 139 países que buscan integrar las empresas con las TICs en un entorno propicio a la innovación tecnológica y al incremento de la productividad.

Con respecto al nivel de adopción de tecnologías por el gobierno, Guatemala presenta una puntuación relativamente baja en el Índice de Desarrollo del Gobierno Electrónico del Departamento de Asuntos Económicos y Sociales de las Naciones Unidas. Este Índice clasifica al país en el puesto 102 de 103, y también le otorga una calificación de 0.4790, un poco más alto que el promedio sub-regional de 0.4770.

También es importante hacer mención a algunos aspectos de la gestión de los recursos críticos de internet en Guatemala, como el nombre del **dominio nacional** “.GT” y las direcciones de Protocolo de Internet (IP, por sus siglas en inglés) asignadas al país. El dominio “.GT” es el **dominio** de nivel superior (ccTLD, por sus siglas en inglés) asignado a Guatemala, bajo la responsabilidad del Registro de Dominios “.GT”¹⁰. En 1992, la Autoridad de Números Asignados en Internet (IANA, por sus siglas en inglés) delegó la administración del Dominio de Nivel Superior del código del país “.GT” a la Universidad del Valle de Guatemala (UVG). Con el fin de fomentar el uso de Internet en la educación y el Gobierno Electrónico, a partir del 2 de enero de 2007, los nombres de dominio registrados bajo los subdominios .edu.gt, .gob.gt y .mil.gt quedaron exonerados del pago de tarifas.



¹⁰ <https://www.gt/index.php>

Por último, cabe mencionar que Guatemala no cuenta con Puntos de Intercambio de Internet (IXP, por sus siglas en inglés), que ayudan a mantener el tráfico local dentro de infraestructuras locales y a reducir los costos asociados con el intercambio de tráfico entre proveedores de servicios de Internet. La ausencia de IXPs compromete la habilidad para construir un ecosistema y una economía de Internet local robustas, ya que estas pueden mejorar la calidad de los servicios reduciendo los retrasos asociados al enrutamiento innecesario del tráfico funcionando como un centro apropiado para alojar valor agregado e infraestructura crítica del país.

La Investigación y Respuesta a Incidentes Cibernéticos

En cuanto a los mecanismos coordinados de respuesta a incidentes cibernéticos, han existido esfuerzos e iniciativas como el Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT-gt), un equipo ad hoc que operó bajo la gestión del Ministerio de la Defensa; que por falta de un marco jurídico y regulatorio que lo soportara dejó de funcionar. Actualmente no existe entidad que coordine a nivel nacional la respuesta a incidentes cibernéticos, es por ello, que la Estrategia Nacional de Seguridad Cibernética pretende abordar este tema en el marco del Sistema Nacional de Seguridad con el trabajo y monitoreo conjunto de sus componentes, como el Ministerio de Gobernación y el Ministerio de la Defensa Nacional; así también otros actores institucionales como el Ministerio de Comunicaciones Infraestructura Vivienda, para atender asuntos relacionados con la seguridad cibernética y defensa cibernética en los ámbitos de seguridad interior, exterior y gestión de riesgos respectivamente.

En Guatemala, no existe normativa específica que aborde los delitos cibernéticos acorde a estándares internacionales; tampoco existe normativa relacionada con la protección de datos personales. Sin embargo, en el Decreto número 17-73 del Congreso de la República, Código Penal, se encuentran tipificados algunos delitos informáticos tales como la destrucción de registros informáticos (destruir, borrar o inutilizar información); alteración de programas, reproducción de instrucciones o programas de computación, registros prohibidos (que afecten la intimidad de las personas); manipulación de información (ocultar, alterar o distorsionar información); uso de información (acceso ilícito); programas destructivos (registros, programas o equipos); y, alteración maliciosa de número de origen. De la misma forma, el delito relacionado con pornografía infantil, no se encuentra incluido dentro del marco jurídico nacional como delito cibernético, sino que está regulado en el Decreto del Congreso de la República 9-2009 Ley contra la violencia sexual, explotación y trata de personas. Sin la tipificación apropiada de los delitos cibernéticos, el sistema de justicia guatemalteco no puede sancionar de manera adecuada este tipo de delincuencia y se le dificulta la coordinación a nivel internacional sobre este tema, haciendo del país un paraíso para los delincuentes cibernéticos.

Este análisis del marco jurídico de Guatemala en relación a los delitos cibernéticos y las discusiones realizadas en las mesas de trabajo para el desarrollo de esta Estrategia, determinó la importancia de que el país se adhiera al Convenio de Budapest, para generar y fortalecer esos vínculos de coordinación y cooperación internacionales facilitados por un marco

jurídico armonizado con los países adscritos a dicho Convenio. Cabe señalar que el Gobierno de Guatemala ya expresó el interés de adherirse al mismo, y está siendo gestionado por el Ministerio de Relaciones Exteriores. Los entrevistados durante el proceso de formulación de esta Estrategia destacaron la importancia de una ley de delitos cibernéticos, así como de incentivar una cultura de prevención de ciberdelincuencia en el sistema educativo del país y a nivel del sector justicia.

Adicionalmente, en las entrevistas y cuestionarios se observó que a pesar de que existen investigaciones y enjuiciamientos por delitos cibernéticos, estos han sido enfocados en el tema de derecho de propiedad intelectual y de pornografía infantil y no en lo relativo al ciberespacio en general. Asimismo, se puso de manifiesto en la información recabada, la existencia de Organizaciones No Gubernamentales (ONG) y otros grupos de peritos forenses digitales que están trabajando para el establecimiento de estadísticas de ciberdelitos con el fin de desarrollar el “Observatorio Guatemalteco de Delitos Informáticos” (OGDI); sin embargo, hace falta información particularmente del sector privado.

En términos de capacitación para la investigación de delitos cibernéticos, se destaca la falta de conocimiento de las autoridades sobre la aplicación de la ley acerca de una prueba digital, así como de la cadena de custodia digital, el traslado y la sustracción de la evidencia sobre el ISO 27037. De igual manera, las salas de audiencia no están equipadas para recibir evidencia digital, y hace falta también instrumentos para la adecuada recolección, preservación, transporte y análisis de la evidencia digital (ej. bolsas de Faraday utilizadas para preservar dispositivos móviles como evidencia).

Actualmente, existe una unidad en la Policía Nacional Civil (PNC) encargada de la investigación de delitos cibernéticos que es necesario reforzar e impulsar al igual que la Unidad Científica de Peritaje Forense del Instituto Nacional de Ciencias Forenses de Guatemala (INACIF). Sin embargo, el Ministerio Público aún no cuenta con una Unidad de Delitos Cibernéticos, la cual deberá ser creada y reforzada para trabajar en conjunto con las demás unidades relacionadas al tema.

Se remarcó la disposición de instituciones que pueden facilitar la capacitación de las autoridades en delitos relacionados con la informática y en el manejo de evidencias electrónicas, como la Red Latinoamericana de Informática Forense¹¹ y la consultoría INFOGTM¹². Asimismo, se discutió la importancia de ofrecer capacitaciones a los profesionales del derecho, no sólo a las autoridades.

Debido a que no existe una normativa que regule el apoyo de los proveedores de Internet, se enfatizó que una regulación apropiada es necesaria para intercambiar información con las instituciones de seguridad y justicia específicamente en las investigaciones, para determinar

¹¹ <http://www.redlifguatemala.org>

¹² <http://www.infogtm.com>

la fuente de un ataque cibernético. Sin una regulación o legislación clara, este tipo de cooperación sería muy compleja, dado que podría afectar la relación de los proveedores con sus clientes. De hecho, algunos de los clientes más grandes exigen cláusulas de confidencialidad en sus contratos, lo cual podría impedir que el proveedor brindara la colaboración requerida por las autoridades de seguridad y justicia. De manera similar, sería necesaria una regulación para que las empresas del sector privado compartieran información acerca de las vulnerabilidades de sus redes y sistemas cuando sus capacidades se vean superadas con el fin de encontrar soluciones de forma coordinada a través del intercambio de mejores prácticas y lecciones aprendidas.

En general, los ataques contra las empresas se resuelven internamente o con contrataciones externas, pero no hay una adecuada comunicación con autoridades relacionadas con la aplicación de la ley. El incidente cibernético es solucionado, pero muchas veces no hay una persecución penal por la falta de mecanismos de preservación de la evidencia digital, como se mencionó anteriormente. Esto es alarmante cuando se considera lo reportado por el Grupo de Trabajo *Anti-Phishing*¹³ (APWG, por sus siglas en inglés), en donde Guatemala, en el cuarto trimestre de 2015, se encontraba en el puesto 5 entre los países más infectados por malware, con una tasa de infección de 39.58 por ciento.

Con respecto a la remoción de contenidos ilegales del Internet (*takedown*), esto sería posible solo si la orden es válida y proviene de un juez competente. Sin embargo, se señaló que no existe una legislación clara acerca de cuáles serían estos contenidos ilegales y los procedimientos de remoción de los mismos en línea. En este contexto, durante las reuniones y en los cuestionarios se destacó la necesidad de revisar la Iniciativa de Ley de Cibercrimen 5254, así como de generar leyes que tengan coherencia y crear métodos que sean aplicables en el corto, mediano y largo plazo.

La Administración Pública

De acuerdo a la información obtenida, se destacó que no existe una gestión centralizada en el gobierno para la compra de tecnologías de la información (TI) y seguridad cibernética. En este sentido, los esfuerzos de seguridad de la información se dan a nivel de cada institución; es decir, sin una entidad que los coordine.

Por otra parte, con relación al desarrollo e implementación de servicios y productos orientados al ciudadano, Guatemala se adhirió a la Alianza para el Gobierno Abierto (OGP, por sus siglas en inglés), el 27 de julio de 2011, que posteriormente ratificó en 2012, habiendo implementado a la fecha tres Planes de Acción Nacional de Gobierno Abierto en períodos bianuales, el último correspondiente al período de 2016 a 2018.

¹³ https://docs.apwg.org/reports/apwg_trends_report_q1-q3_2015.pdf

La Iniciativa de Gobierno Abierto se convierte en un mecanismo propicio para la prevención de la corrupción y transformación de la gestión pública, mediante un espacio de discusión y diálogo de representantes de instituciones públicas y organizaciones de sociedad civil en la construcción de 22 compromisos que forman parte del Plan de Acción Nacional de Gobierno Abierto 2016-2018, basados en 5 ejes de trabajo:



Lo anterior conduce a establecer mecanismos que permitan incorporar tecnologías de información con estándares de interoperabilidad y seguridad cibernética dentro de sus planes de acción, para una gestión transparente, coordinada e inclusiva con todos los sectores del país.

El Sector Privado y Financiero

Con respecto a la gestión de incidentes cibernéticos, no existe una norma o gestión nacional desarrollada e implementada. Por ende, las redes privadas implementan sus propios métodos de respuesta y gestión de incidentes cibernéticos. Algunos entrevistados mencionaron que sus instituciones cuentan con sistemas de prevención de intrusos y con algunas medidas de seguridad en sus redes y sistemas con base a estándares requeridos por entes internacionales. Cabe destacar que existe una brecha en el intercambio de información entre el sector privado y el sector público acerca de las amenazas y vulnerabilidades cibernéticas; esta brecha podría reducirse solo por medio de una reglamentación específica que regule y fomente el intercambio de información.

En las entrevistas se destacó la importancia de crear una **cultura de seguridad informática** a nivel nacional, para que sea posible una gestión de incidentes cibernéticos. Representantes de las empresas de informática enfatizaron la importancia de la concientización de los empresarios sobre la seguridad informática, ya que el sector privado es ampliamente afectado por incidentes cibernéticos, tales como el *phishing* y *ransomware*. Se mencionó también la importancia de crear alianzas público-privadas, con una mayor participación del sector privado en el debate para el desarrollo de políticas de seguridad cibernética.

En cuanto al sector financiero, la Superintendencia de Bancos es la entidad encargada de reglamentar la actividad bancaria en Guatemala, incluso en términos de seguridad cibernética. Se informó la existencia de una resolución de la Superintendencia de Banco con normas de TICs para las redes bancarias; sin embargo, esta resolución necesita ser actualizada debido a que hay que considerar aspectos de coordinación y cooperación con otros sectores, especialmente el sector público.

A pesar de que la Asociación Bancaria de Guatemala (ABG) cuenta con un grupo de seguridad colaborativo, las acciones son ad hoc y permanentes. Por ejemplo, los bancos implementan las normas emitidas por la Superintendencia de Bancos pero de manera aislada; de igual forma, existe un intercambio de información sobre incidentes cibernéticos entre los bancos, pero éste no está institucionalizado.

El sector financiero es el blanco de una gran cantidad de ataques cibernéticos en el país. Generalmente los ataques contra los sistemas financieros y otras empresas se resuelven recurriendo a los proveedores de servicios de telecomunicaciones o empresas privadas de seguridad cibernética, sin una comunicación con autoridades de aplicación de la ley. Se señaló la importancia de un mayor acercamiento entre el gobierno y las entidades bancarias para una mejor coordinación en relación a los esfuerzos en seguridad cibernética.

Por último, se destaca la necesidad de concientizar a los empleados y clientes sobre buenas prácticas en seguridad cibernética, ya que según la información obtenida en las entrevistas, muchos de los problemas que enfrentan en este tema son a causa de vulnerabilidades internas como la fuga de información. Con respecto a sus clientes, los bancos hacen controles y alertas de riesgo para algunas cuentas de sus clientes; sin embargo, se discutió la vulnerabilidad de los usuarios y la importancia de capacitar a los clientes en buenas prácticas de seguridad cibernética.

Sensibilización y Educación

Se destacó una preocupación mayor en relación a la necesidad de un entendimiento compartido y definiciones comunes en seguridad cibernética, con el fin de fomentar una **cultura de seguridad cibernética** entre los distintos sectores y entre la población en general. No hay mucho involucramiento de la sociedad civil en cuestiones de gobernanza de internet, o sensibilización pública sobre la seguridad digital. Los pocos esfuerzos que existen han sido unilaterales y aislados, sin una coordinación nacional.

Los representantes de la academia que participaron en la formulación de la Estrategia Nacional de Seguridad Cibernética remarcaron la importancia de fomentar una triangulación entre gobierno-academia-sector privado para el desarrollo de políticas de investigación, desarrollo e innovación **(I+D+I)**. Esta alianza es fundamental para la obtención de recursos y para el desarrollo de centros de investigación dedicados a la temática de la seguridad informática.

Estos recursos son necesarios para fortalecer programas de becas orientadas a temas de TICs. En Guatemala es posible acceder a estos programas vía la Secretaría de Planificación y Programación de la Presidencia (SEGEPLAN) que, a su vez, es la entidad responsable de generar las directrices generales de las políticas públicas de Estado. Así también, el Instituto Técnico de Capacitación y Productividad (INTECAP) promueve la innovación tecnológica a través de becas al extranjero con el apoyo de las universidades del país.

En términos generales, existe una limitada oferta de cursos y formación en la materia para los distintos sectores y segmentos de la sociedad, en particular, para niños y niñas de la educación primaria. Si bien existe el Currículo Nacional Base de Guatemala (CNB), en éste no se incluye actualmente un módulo de seguridad cibernética; de igual manera, es necesario dotar a las escuelas de recursos tecnológicos que permitan cubrir las necesidades básicas con respecto a la tecnología como conectividad en las aulas y herramientas informáticas que faciliten la enseñanza y el aprendizaje.

Se identificó la existencia de algunas iniciativas del Ministerio de Educación para niños y niñas, como los Proyectos INNOVA, que formulan criterios técnicos, pedagógicos y metodológicos en el campo de aplicación de las TICs. También se observaron otras iniciativas apoyadas por el sector privado como parte de sus políticas de responsabilidad social atendiendo la necesidad de que tanto los niños y niñas deban ser capacitados en seguridad cibernética, como también los padres y maestros para atacar la problemática del analfabetismo digital en todos los sectores.

Como conclusión se estableció importante coordinar iniciativas de educación en materia de seguridad cibernética con todos los actores involucrados, especialmente el Ministerio de Educación y el Consejo Nacional de Ciencia y Tecnología (CONCYT) para mejorar los índices de concienciación y educación digital que corresponden el primer paso para crear una **cultura de seguridad cibernética** fortalecida y actualizada.

CONSTRUCCIÓN DE LA ESTRATEGIA

La elaboración de la Estrategia Nacional de Seguridad Cibernética se formuló sobre la base de una visión nacional para lograr objetivos a cumplirse en un tiempo estipulado, que contribuyan a la seguridad en el ciberespacio.

El proyecto de formulación de la Estrategia Nacional de Seguridad Cibernética se valió de actividades participativas de reflexión, discusión, entrevistas y aportes individuales, orientadas metodológicamente por el documento base denominado **“Desarrollo de una Estrategia de Seguridad Cibernética”**. Este documento fue presentado por la Organización de Estados Americanos, donde se plantean los resultados obtenidos con la aplicación del modelo de madurez de seguridad cibernética del Centro Global de Capacitación de Seguridad Cibernética de la Universidad de Oxford, preparado conjuntamente con el Banco Interamericano de Desarrollo.

Este modelo informa sobre el estado actual del país en relación a la seguridad cibernética a partir de 49 indicadores distribuidos en cinco dimensiones: Política y Estrategia, Cultura y Sociedad, Educación, Marcos Legales y Tecnologías, cuyos resultados se encuentran en el anexo.

El proceso consideró cuatro fases:

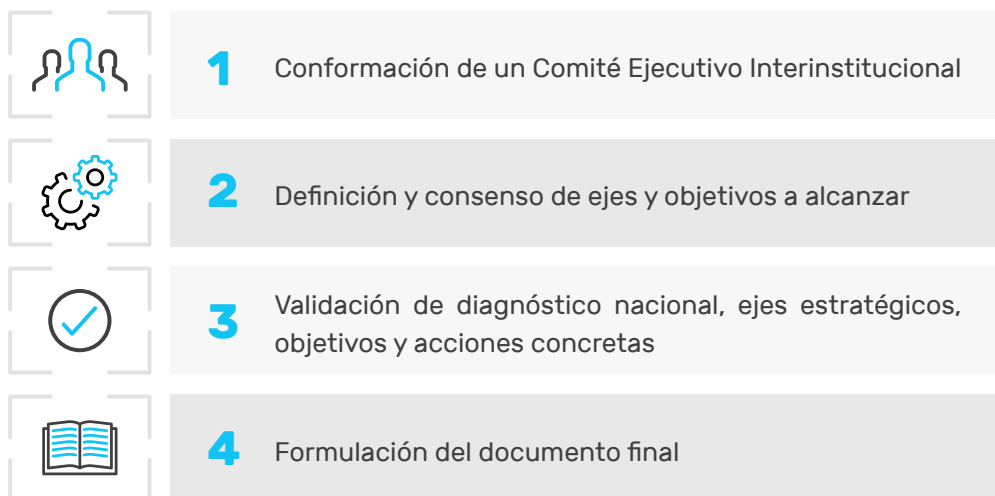


Figura 1. Fases para el desarrollo de la Estrategia Nacional de Seguridad Cibernética

Durante la primera fase se gestionó la integración del Comité Ejecutivo Interinstitucional con representantes del Ministerio de Relaciones Exteriores, Ministerio de la Defensa, Ministerio de Gobernación, Ministerio de Comunicaciones Infraestructura y Vivienda a través de la Superintendencia de Telecomunicaciones, Secretaría Técnica del Consejo Nacional de Seguridad y la Secretaría Nacional de Ciencia y Tecnología, quienes formularían la estructura temática y metodología del proceso; la investigación necesaria para el planteamiento de los temas de discusión y análisis; y la integración y retroalimentación de los aportes obtenidos a través de las sesiones de trabajo en un documento final.

De forma paralela, se integraron las mesas de trabajo sectoriales, las cuales estuvieron integradas por representantes de instituciones gubernamentales, financieras, infraestructuras críticas, sociedad civil, universidades y centros de investigación, con el objeto de retroalimentar y fortalecer la Estrategia Nacional de Seguridad Cibernética.



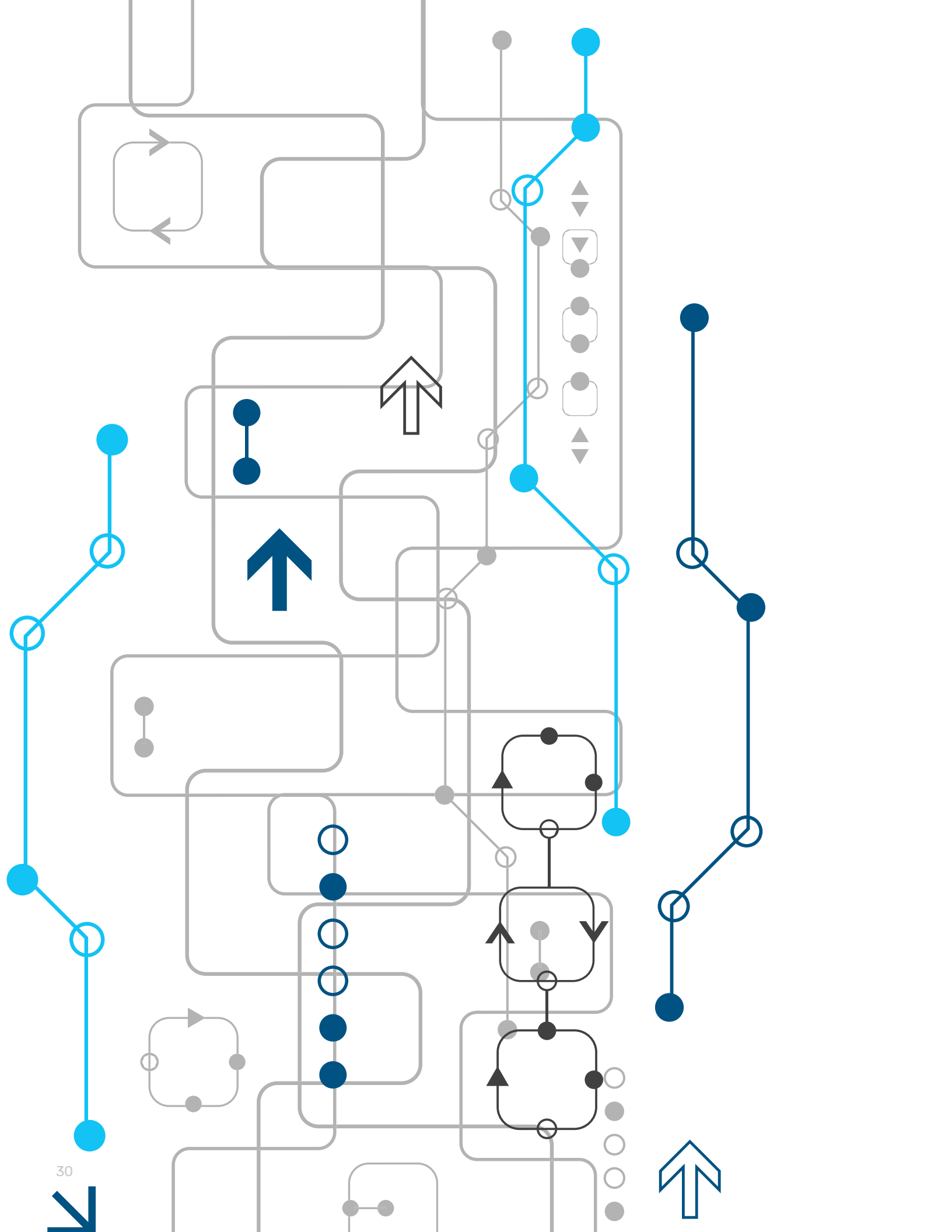
Figura 2. Organización de las mesas de trabajo.

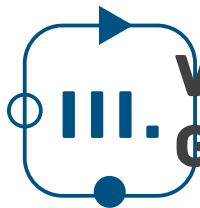
Para la segunda y tercera fase, se programaron reuniones con los distintos representantes de las mesas sectoriales, para abordar la evolución de los retos que plantea la seguridad en el ciberespacio en aras de promover una mayor inclusión y mejorar la gobernanza digital. Estas mesas presentaron el entorno propicio para generar entrevistas y cuestionarios a expertos de cada ámbito, lo cual permitió generar un diagnóstico robusto de la situación nacional de la seguridad cibernética.

Se trazaron metas específicas para ser alcanzadas en el corto plazo basadas en el análisis del contexto nacional y global, relacionadas con buenas prácticas y lecciones aprendidas en las distintas esferas de la seguridad cibernética; asimismo, se consideraron los lineamientos, objetivos y acciones estratégicas contenidos en el Plan Estratégico de Seguridad de la

Nación 2016-2020, para contar con una estrategia alineada dentro del Sistema Nacional de Seguridad.

En la fase final, se implementó una consulta pública, abriendo espacios de participación a toda la ciudadanía y organizaciones de la sociedad civil, tanto nacionales como extranjeras, que permitió consolidar el documento final.





VISION Y PRINCIPIOS GENERALES



Visión

Derivado del ejercicio participativo para la construcción de la Estrategia Nacional de Seguridad Cibernética, se trazó una visión integradora, en un marco de gestión de riesgos que se plantea como:



Que los guatemaltecos tengan un mayor nivel de conciencia sobre la importancia de la seguridad cibernética, entendiéndola, valorándola y aprovechando los medios informáticos de manera efectiva, con un enfoque multisectorial en todos sus ámbitos.



Principios

En la Estrategia Nacional de Seguridad Cibernética, se entiende como principios generales al sistema de valores que dirigen los actores involucrados en la implementación e interpretación de la misma; abarcan los establecidos en la Política Nacional de Seguridad¹⁴ y se complementan con:

Responsabilidad compartida

Se entiende que la promoción y protección de la seguridad cibernética compete en forma concertada a todos y cada uno de los actores sociales, públicos y privados, gubernamentales o no, que deberán cooperar entre sí en todo momento para la consecución de tal objetivo.

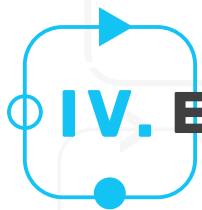
Eficacia y Proporcionalidad

Se refiere a un enfoque en las medidas que sean adecuadas para garantizar a las personas un uso seguro del ciberespacio y el ejercicio de sus derechos, priorizando en las oportunidades que éste ofrece, a través de una gestión de riesgos que se haga cargo de identificar, prevenir y dar respuesta proporcional a las amenazas de manera eficaz.

Cooperación internacional

En materia de seguridad cibernética se refiere al esfuerzo conjunto de gobiernos, apoyado por el dinamismo de organismos internacionales, sociedad civil, academia y sector privado, para promover acciones que contribuyan a generar espacios de participación seguras en el ciberespacio a través de la transferencia, recepción e intercambio de información, conocimientos, tecnologías, experiencias y recursos, respetando los principios del derecho internacional y respeto a los derechos humanos.

¹⁴ Primacía de la persona humana, respeto al estado de derecho, observancia de los derechos humanos, equidad de género, respeto a la diversidad cultural, fortalecimiento de la gobernanza local y ejercicio de los controles democráticos.



IV. EJES, OBJETIVOS Y ACCIONES

La incorporación del Ciberespacio como un ámbito de actuación en el Sistema Nacional de Seguridad, requerirá de esfuerzos en todos los sectores de la sociedad guatemalteca, con el fin de crear las capacidades necesarias para salvaguardar la seguridad e integridad de las personas y el libre ejercicio de sus derechos en dicho ámbito.

Una adecuada y articulada gestión del riesgo cibernético, así como el desarrollo e implementación de estrategias de prevención, demandan fortalecer tanto el marco jurídico en materia de seguridad cibernética, como la cooperación internacional y diligenciar la suscripción de convenios internacionales. De forma paralela, se requiere establecer lineamientos para la capacitación especializada y profesionalización en seguridad de la información e implementar instancias apropiadas para prevenir, coordinar, atender, controlar, recomendar y regular los incidentes o emergencias cibernéticas con el propósito de generar un ambiente apropiado para el desarrollo y la participación en el ciberespacio manteniendo niveles aceptables de seguridad y resiliencia.

Para lo anterior se plantea el objetivo de la Estrategia Nacional de Seguridad Cibernética como:

“

Fortalecer las capacidades de la Nación, creando el ambiente y las condiciones necesarias para asegurar la participación, el desarrollo y el ejercicio de los derechos de las personas en el ciberespacio.

”

La Estrategia Nacional de Seguridad Cibernética está compuesta por 4 ejes estratégicos, 10 objetivos y 37 acciones que deben ser asumidas e implementadas por todos los actores y sectores involucrados directa o indirectamente:



Figura 3. Ejes Estratégicos de la Estrategia Nacional de Seguridad Cibernética

EJE. 1

MARCOS LEGALES





Marcos Legales



Investigación Criminal



Estrategia de Divulgación



EJE 1. MARCOS LEGALES

El presente eje proporciona las bases sobre las cuales se construye y determina el alcance y naturaleza de la seguridad cibernética en el país y propone tres objetivos relacionados con la armonización de los delitos cibernéticos, el fortalecimiento de los procesos investigativos y la admisibilidad de la evidencia electrónica.



1.1 Adecuar el marco legal guatemalteco con un enfoque de prevención y manejo de riesgos cibernéticos para fortalecer la seguridad cibernética

1. Adecuar los instrumentos legales del Sistema Nacional de Seguridad para incluir la seguridad cibernética con un enfoque de prevención y gestión de riesgos.
2. Crear, aprobar e implementar una ley contra la ciberdelincuencia, con referencia en estándares internacionales aplicados a la realidad guatemalteca.
3. Modernizar las instituciones del sector justicia y adecuar normas y estándares en los procesos judiciales y el manejo de la evidencia digital.
4. Crear, aprobar e implementar la ley de privacidad y protección de datos con referencia en convenios internacionales de derechos humanos.
5. Crear, aprobar e implementar la ley de infraestructuras críticas para identificar y catalogar las que prestan servicios esenciales al país y el establecimiento de medidas de prevención, protección y recuperación contra riesgos y amenazas.
6. Adecuar y proponer estándares de seguridad cibernética de las TIC para establecer un marco de gestión en los distintos sectores de la sociedad.
7. Adecuar la normativa del sector bancario y privado que permita la adopción de formas de pago que incentive el comercio electrónico.



1.2 Promover la investigación criminal para mantener niveles aceptables de seguridad cibernética

1. Desarrollar capacidades institucionales que incluyan los recursos humanos, procesales y tecnológicos en las instituciones del sector justicia y relacionadas, para investigar y manejar casos provenientes de delitos cibernéticos.

2. Establecer el marco de cooperación público-privado-academia para diseñar e implementar mecanismos de investigación y desarrollo que mejoren la eficiencia de los procesos judiciales.
3. Desarrollar e implementar procesos ágiles y oportunos para la colaboración y el intercambio de información transnacional en materia de delincuencia cibernética.



1.3 Determinar una estrategia de divulgación que promueva la transparencia de la información

1. Formular e implementar reglamentaciones y directrices relacionadas a la divulgación responsable de las vulnerabilidades cibernéticas.

EJE. 2

EDUCACIÓN

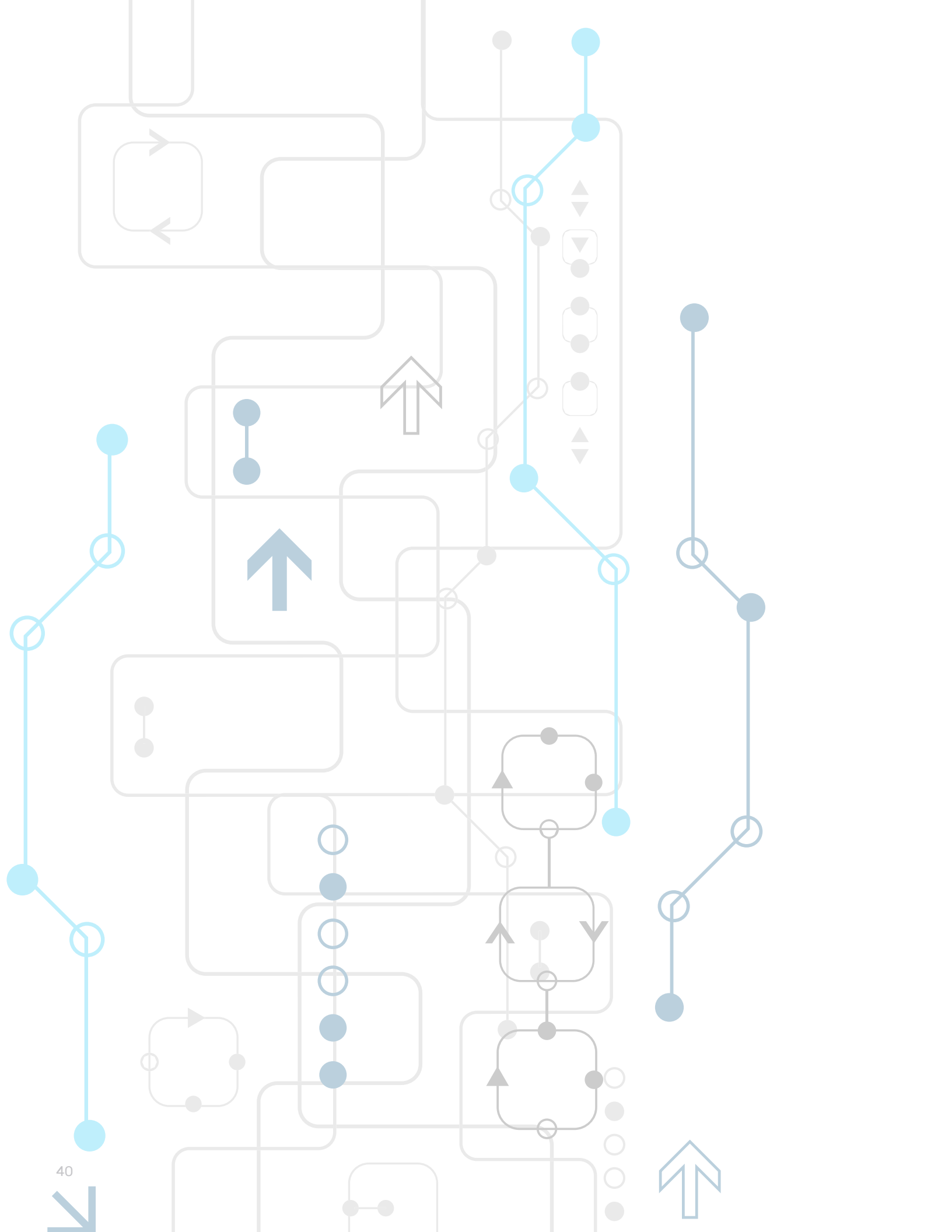




Promover la oferta educativa y formativa en seguridad



Programas de educación para la formación y la investigación





EJE 2. EDUCACIÓN

El eje de Educación, juega un papel de suma importancia para fortalecer las capacidades de la Nación de brindar protección en el ciberespacio en todos sus ámbitos.

Sus objetivos se centran en incrementar la oferta educativa nacional y la formación en materia de seguridad cibernética, de tal manera que se pueda cubrir la demanda técnica y profesional en todos los sectores del país.



2.1 Promover la oferta educativa y formativa en Seguridad Cibernética que permita cubrir la demanda técnica y profesional en el país

1. Elaborar un diagnóstico nacional para determinar las necesidades en el ámbito de la seguridad cibernética.
2. Diseñar indicadores que permitan medir la oferta educativa a las necesidades del entorno de la seguridad cibernética.



2.2 Desarrollar e implementar programas de educación para la formación y la investigación/desarrollo de la seguridad cibernética

1. Diseñar una propuesta de requisitos de formación y contenidos curriculares, acorde a las tendencias regionales sobre los distintos roles técnicos en seguridad cibernética.
2. Modernizar y capacitar a todos los actores del sector justicia sobre los delitos cibernéticos e informática forense, especialmente en la identificación, preservación, análisis y presentación de la evidencia digital.
3. Diseñar e implementar contenidos para la creación de capacidades y estrategias pedagógicas de parte de la comunidad educativa.
4. Promover la inclusión de los componentes de seguridad cibernética en el currículo nacional base.

EJE. 3

CULTURA Y SOCIEDAD





Gestión de la Seguridad Cibernética:
prevención, detección y reacción



Sensibilización en gestión
de riesgos y amenazas

EJE 3. CULTURA Y SOCIEDAD

El ciberespacio abre las oportunidades de desarrollo personal y profesional; sin embargo, mantener un nivel de respuesta a incidentes cibernéticos aceptable, no es posible sin la inclusión de todos los sectores de la sociedad a través de una cultura de seguridad cibernética sólida y actualizada, la cual debe ser abordada de forma integral, para lo cual se han formulado 2 objetivos relacionados con:




3.1 Gestionar la Seguridad Cibernética para la prevención, detección y reacción ante amenazas del ciberespacio

1. Fortalecer el marco institucional para la implementación de la Estrategia Nacional de Seguridad Cibernética dentro del Sistema Nacional de Seguridad.
2. Crear e implementar el Comité Nacional de Seguridad Cibernética para asesorar al Consejo Nacional de Seguridad en el seguimiento de las temáticas estratégicas relacionadas a la seguridad cibernética.
3. Adaptar y reglamentar buenas prácticas de seguridad cibernética en el sector gubernamental con un enfoque de gestión del riesgo.
4. Adecuar y modernizar los procesos y manuales de funciones dentro de las instituciones gubernamentales bajo el marco de valores, estándares y mejores prácticas de seguridad cibernética.
5. Identificar y promover el uso de buenas prácticas de seguridad cibernética en las empresas del sector privado.
6. Diseñar y promover acorde a la realidad guatemalteca, políticas, programas y materiales para manejar la privacidad en línea y protección de accesos no autorizados.



3.2 Establecer programas de sensibilización para contribuir en la gestión efectiva de riesgos y amenazas cibernéticas

1. Diseñar e implementar programas de concienciación sobre seguridad cibernética a los distintos grupos etarios y sectoriales de la sociedad guatemalteca.

- 
2. Establecer convenios público-privados para la implementación de los programas de concienciación sobre seguridad cibernética.
 3. Diseñar y promover campañas orientadas a la promoción de la confianza en el uso de productos y servicios en línea bajo un entorno seguro.
 4. Promover el incremento de los servicios electrónicos gubernamentales fiables y seguros; a través de la implementación de una Política de Datos Abiertos.
 5. Establecer campañas para promover el uso de documentos digitales y comercio electrónico a través de la implementación y utilización de firma electrónica avanzada.

EJE. 3

TECNOLOGÍAS DE INFORMACIÓN





Regular la protección de sistemas de información público y privado



Centros de Respuesta ante incidentes cibernéticos intersectoriales



Plan de Protección Nacional de Infraestructura críticas

EJE 4. TECNOLOGÍAS DE INFORMACIÓN

El eje de Tecnologías de Información, plantea acciones relacionadas a la sistematización en la continuidad de los servicios digitales en los distintos sectores del país. También, propone el establecimiento de las organizaciones de coordinación de la seguridad cibernética nacional y los planes de protección de infraestructuras críticas.



4.1 Regular la protección de los sistemas de información digital en los sectores público y privado, para garantizar la continuidad de sus servicios

1. Identificar estándares de seguridad de la información y buenas prácticas, estableciendo procedimientos y normativas para su adopción, implementación y cumplimiento.
2. Identificar, promover y adoptar metodologías de desarrollo de sistemas orientados a la integridad y capacidad de recuperación.



4.2 Establecer las organizaciones de coordinación para implementar la seguridad cibernética nacional

1. Planificar, implementar y establecer el Centro de Seguridad Interinstitucional de Respuesta Técnico-jurídica ante incidentes informáticos-Guatemala (CSIRT-GT), como punto focal y registro central de incidentes a nivel nacional.
2. Diseñar el CSIRT-Gubernamental para proveer servicios de seguridad cibernética en el sector público. Su implementación será en un ambiente controlado y se determinarán las instituciones en un plan piloto.
3. Promover la implementación y la coordinación entre CIRT, CERT y SOC **intersectoriales** (sector defensa, privado, financiero, salud, empresas y proveedores de servicios de telecomunicaciones, sector de proveedores de servicios básicos, sociedad civil, academia, entre otros) con roles y responsabilidades definidas para conformar un frente común de mitigación de amenazas y la coordinación de respuestas a incidentes provenientes del ciberespacio; así también, la elaboración de protocolos para los canales de comunicación ante situaciones de crisis.



4.3 Diseñar un plan de protección nacional de infraestructuras críticas para fortalecer los planes de contingencia y de recuperación

1. Diseñar e implementar un catálogo de infraestructuras críticas y definir las entidades encargadas de su coordinación, prevención y protección. El catálogo se desarrollará bajo un enfoque de riesgos y amenazas, el cual contendrá los planes, procesos y procedimientos de prevención, mitigación, respuesta y recuperación a nivel nacional.
2. Crear el Consejo Nacional de Protección de Infraestructuras Críticas para coordinar y darle seguimiento a las políticas, estrategias, planes y acciones tanto a nivel estratégico como técnico relacionadas a la protección de infraestructuras críticas.
3. Diseñar e implementar el Centro de Respuesta ante Incidentes de Seguridad a Infraestructuras Críticas (CSIRT-GT-IC) para coordinar la gestión intersectorial de los eventos relacionados a la materia.
4. Promover convenios de cooperación público-privado, nacionales e internacionales para mejorar la eficiencia en la gestión de la seguridad cibernética.



V. GOBERNANZA DE LA SEGURIDAD CIBERNÉTICA

La Constitución Política de la República de Guatemala y la Ley Marco del Sistema Nacional de Seguridad, establecen el Sistema Nacional de Seguridad, cuyas directrices son determinados por el Presidente de la República desde el Consejo Nacional de Seguridad como órgano de máxima autoridad, el cual ha desarrollado distintos instrumentos de carácter funcional como lo son: La Política Nacional de Seguridad, la Agenda Nacional de Riesgos y Amenazas, la Agenda Estratégica de Seguridad de la Nación y el Plan Estratégico de Seguridad de la Nación.

La Ley Marco del Sistema Nacional de Seguridad, establece cuatro ámbitos de funcionamiento: Seguridad Interior, Seguridad Exterior, Inteligencia de Estado y, Gestión de Riesgos y Defensa Civil.

En su conjunto, estos ámbitos e instrumentos conforman el marco general de Seguridad de la Nación y por ello, con el fin de evitar planteamientos fragmentarios que obstaculicen la coordinación interinstitucional, la Estrategia Nacional de Seguridad Cibernética desarrolla una visión integral y coherente con estos instrumentos e instituciones creadas para el efecto, para lo cual se considera pertinente la creación del Comité Nacional de Seguridad Cibernética en el marco del Sistema Nacional de Seguridad.

La gobernanza de la seguridad cibernética se entiende entonces como las políticas, instrumentos estratégicos, procesos e instituciones necesarias para administrar, gestionar y coordinar lo relacionado con la seguridad del ciberespacio a nivel nacional. En este sentido, esta Estrategia propone varias líneas de acción que instan a crear la institucionalidad y la coordinación de la seguridad cibernética en el país, como la conformación de Comités de Seguridad Cibernética tanto a nivel estratégico como técnico que permitirá generar los canales y espacios de intercambio de información necesarios entre el sector público y privado para actuar bajo un marco común de normas y lineamientos.

Comité Nacional de Seguridad Cibernética

El Comité Nacional de Seguridad Cibernética se propone como ente asesor del Consejo Nacional de Seguridad y requerirá la formulación normativa apropiada para su creación.

El Comité incentiva y favorece los espacios de coordinación de las políticas interinstitucionales e intersectoriales, así como la canalización de los esfuerzos en la vinculación de los distintos planes estratégicos con una visión compartida que permita alcanzar los objetivos de la Estrategia Nacional de Seguridad Cibernética.

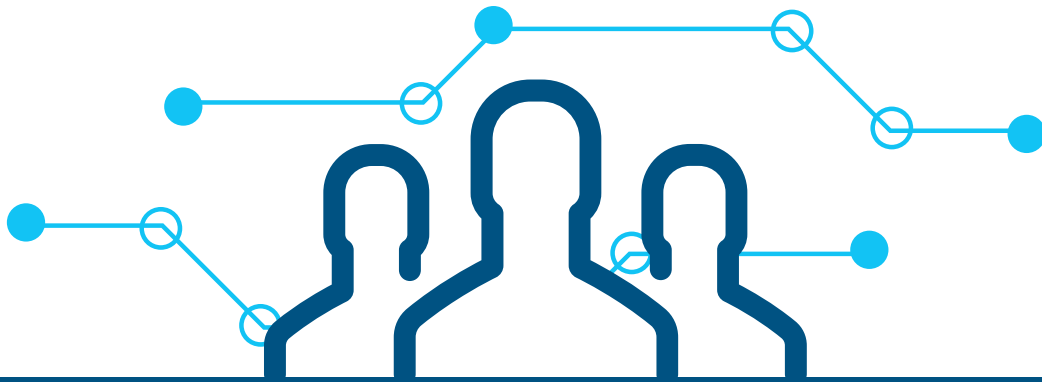
La integración de dicho Comité se plantea en la figura 5.



Figura 5. Instituciones participantes en el Comité Nacional de Seguridad Cibernética

En el Comité podrán participar otros actores relevantes del sector privado y especialistas cuya contribución se considere necesaria para reducir la brecha en la coordinación e intercambio de información entre el sector público y privado. Dicho Comité en coordinación con el CSIRT-GT, dará seguimiento y permitirá la creación de subcomités para coordinar aquellas actuaciones que se deban abordar de forma conjunta, con el fin de elevar los niveles de seguridad cibernética en todo el país. Estos subcomités estarán organizados con las temáticas siguientes:

-  **1** Gubernamental (Ejecutivo, Legislativo y Judicial)
-  **2** Bancos, Aseguradoras, Financieras, etc
-  **3** Infraestructuras Críticas
-  **4** Sociedad Civil, Academia y Centros de Investigación
-  **5** Sector Privado



Funciones del Comité Nacional de Seguridad Cibernética

- 1** Asesorar en materia de seguridad cibernética al Consejo Nacional de Seguridad a través de su Secretaría Técnica.
- 2** Coordinar a los actores y esfuerzos interinstitucionales de la Estrategia Nacional de Seguridad Cibernética, estableciendo las prioridades y los planes de acción en su implementación.
- 3** Promover e incentivar la cooperación intersectorial a nivel nacional e internacional en materia de seguridad cibernética.
- 4** Establecer y gestionar los mecanismos legales/técnicos para el intercambio de información nacional e internacional en seguridad cibernética.
- 5** Gestionar y proponer estándares y buenas prácticas en la normativa nacional para la gestión de riesgos en la seguridad cibernética.
- 6** Diseñar e Implementar los mecanismos de gestión por resultados para medir el cumplimiento de la Estrategia Nacional de Seguridad Cibernética.
- 7** Diseñar e implementar planes de gestión de crisis y una valoración recurrente de los riesgos y amenazas en materia de seguridad cibernética.

Comité Técnico de Seguridad Cibernética

Este Comité Técnico estará presidido por un delegado del Comité Nacional de Seguridad Cibernética y reforzará las relaciones de colaboración, cooperación y coordinación entre los distintos sectores y partes interesadas en la seguridad cibernética como lo son: **Gobierno, Sector Privado, Academia, Sociedad Civil, Infraestructuras Críticas, Sector Financiero, Sector de Tecnologías de Información y Comunicaciones.**

Desde este espacio, cuyo esquema se presenta en la Figura 6, se promoverán análisis, estudios y propuestas de iniciativas tanto en el ámbito nacional como internacional, que favorezcan el ecosistema de la seguridad cibernética en el país.

El delegado estará retroalimentando al Comité Nacional de Seguridad Cibernética a través de reportes periódicos y avances en la implementación de los planes de acción a nivel nacional; asimismo, promoverá el intercambio de información y el desarrollo e implementación de procesos y sistemas interoperables entre los distintos sectores.

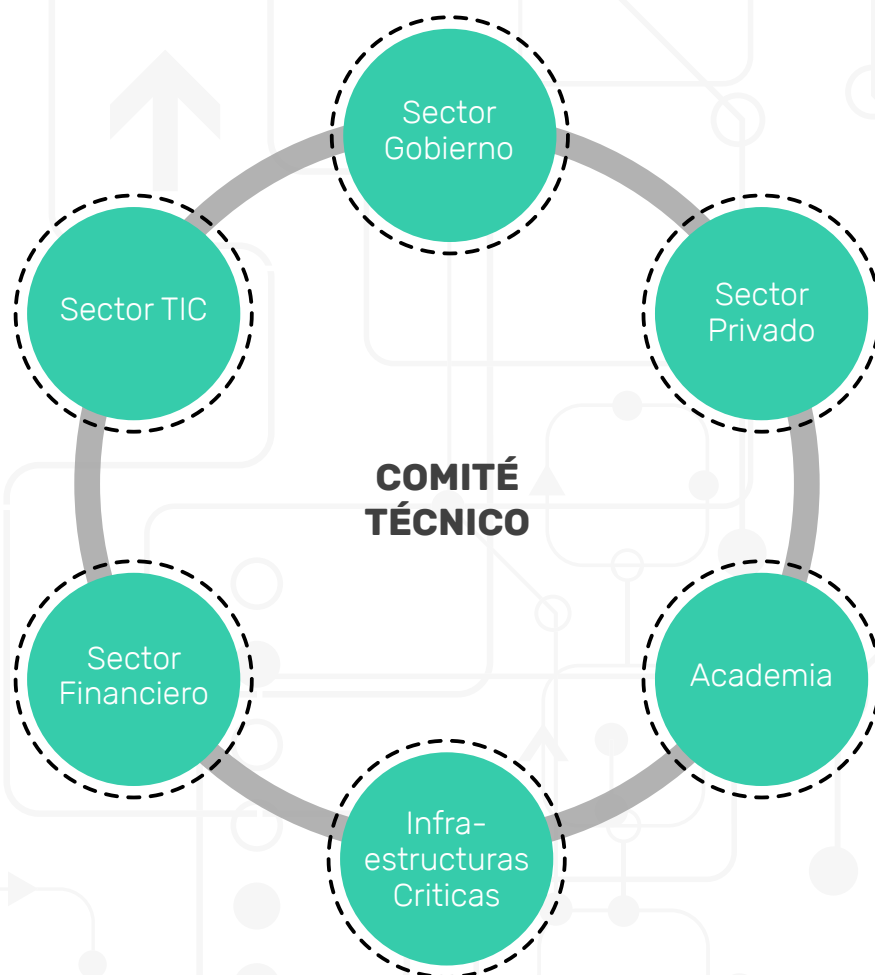
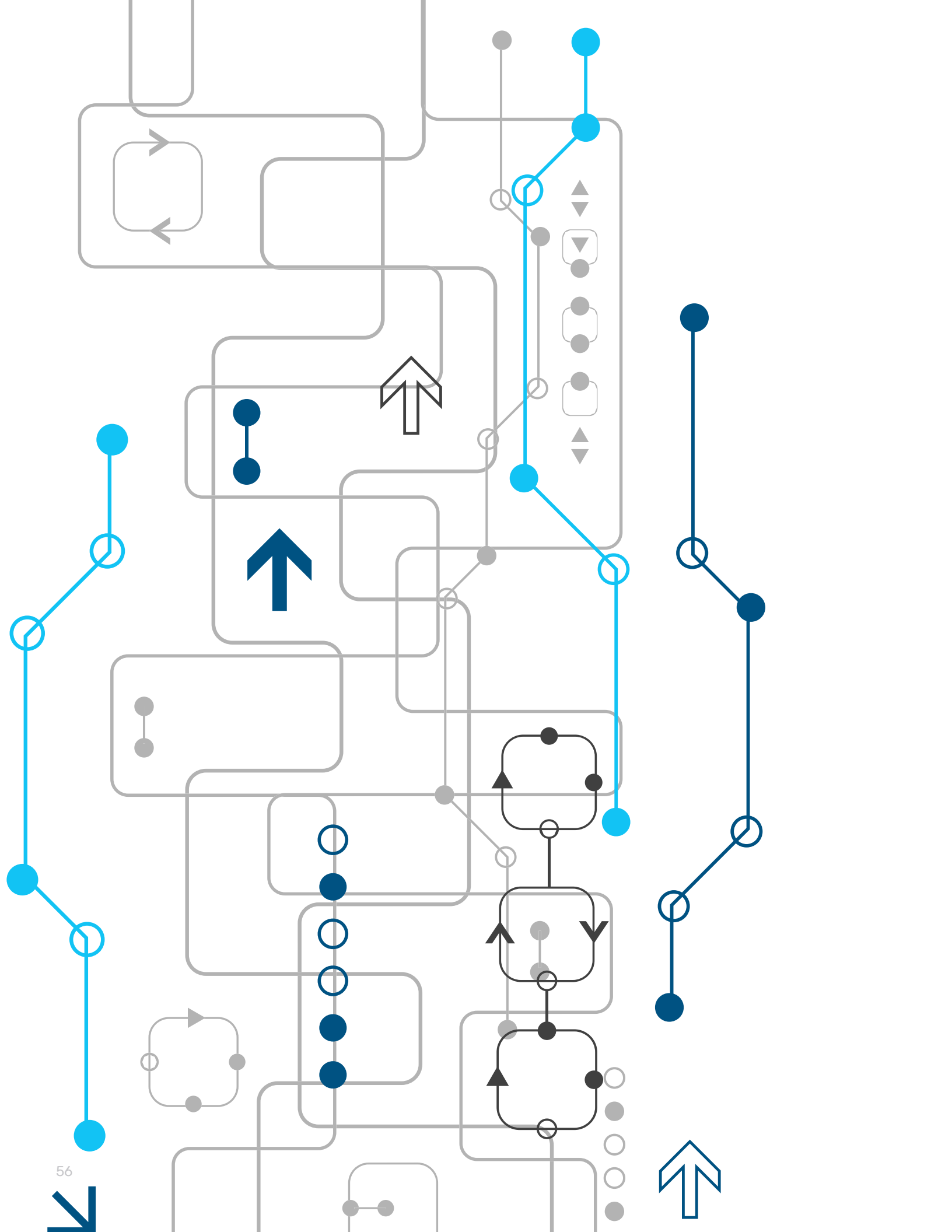


Figura 6. Estructura del Comité Técnico

Monitoreo y Evaluación

El Comité Nacional de Seguridad Cibernética establecerá los mecanismos de colaboración, cooperación y coordinación intersectorial, requeridos para asegurar la plena integración de la Estrategia Nacional de Seguridad Cibernética en los ámbitos de funcionamiento del Sistema Nacional de Seguridad.

El Plan Estratégico de Seguridad de la Nación constituye el instrumento que facilita el enlace político-estratégico a la planificación institucional del Sistema Nacional de Seguridad, por lo que los planes de acción de seguridad cibernética que incluyen los mecanismos de monitoreo y evaluación, se incorporarán en dicho instrumento para desarrollar los Programas Estratégicos de Gobernanza Integral en una arquitectura programática y presupuestaria que dé cumplimiento a la Política Nacional de Seguridad.





ACRÓNIMOS

CERT	Equipo de Respuesta a Emergencias Informáticas.
CICTE	Comité Interamericano contra el Terrorismo
CIDH	Comisión Interamericana de Derechos Humanos
CNS	Consejo Nacional de Seguridad
Convención Americana	Convención Americana sobre Derechos Humanos
Convenio Europeo	Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales
Corte Interamericana	Corte Interamericana de Derechos Humanos
CSIRT	Equipos de Respuesta a Incidentes de Seguridad Informática
CSIRT-GT	Centro de Seguridad Interinstitucional de Respuesta Técnico-jurídica ante incidentes informáticos – Guatemala
ENSC	Estrategia Nacional de Seguridad Cibernética
GISEG	Gestión Integral de la Seguridad de la Nación
GOBLOC	Gobernanza Local
IOT	Internet de las Cosas
OEA	Organización de Estados Americanos
ONU	Organización de las Naciones Unidas
PNS	Política Nacional de Seguridad
SEGDE	Seguridad para el Desarrollo
SOC	Centro de Operaciones de Seguridad
STCNS	Secretaría Técnica del Consejo Nacional de Seguridad
TI	Tecnologías de Información
TIC	Tecnologías de Información y Comunicaciones
UIT	Unión Internacional de Telecomunicaciones

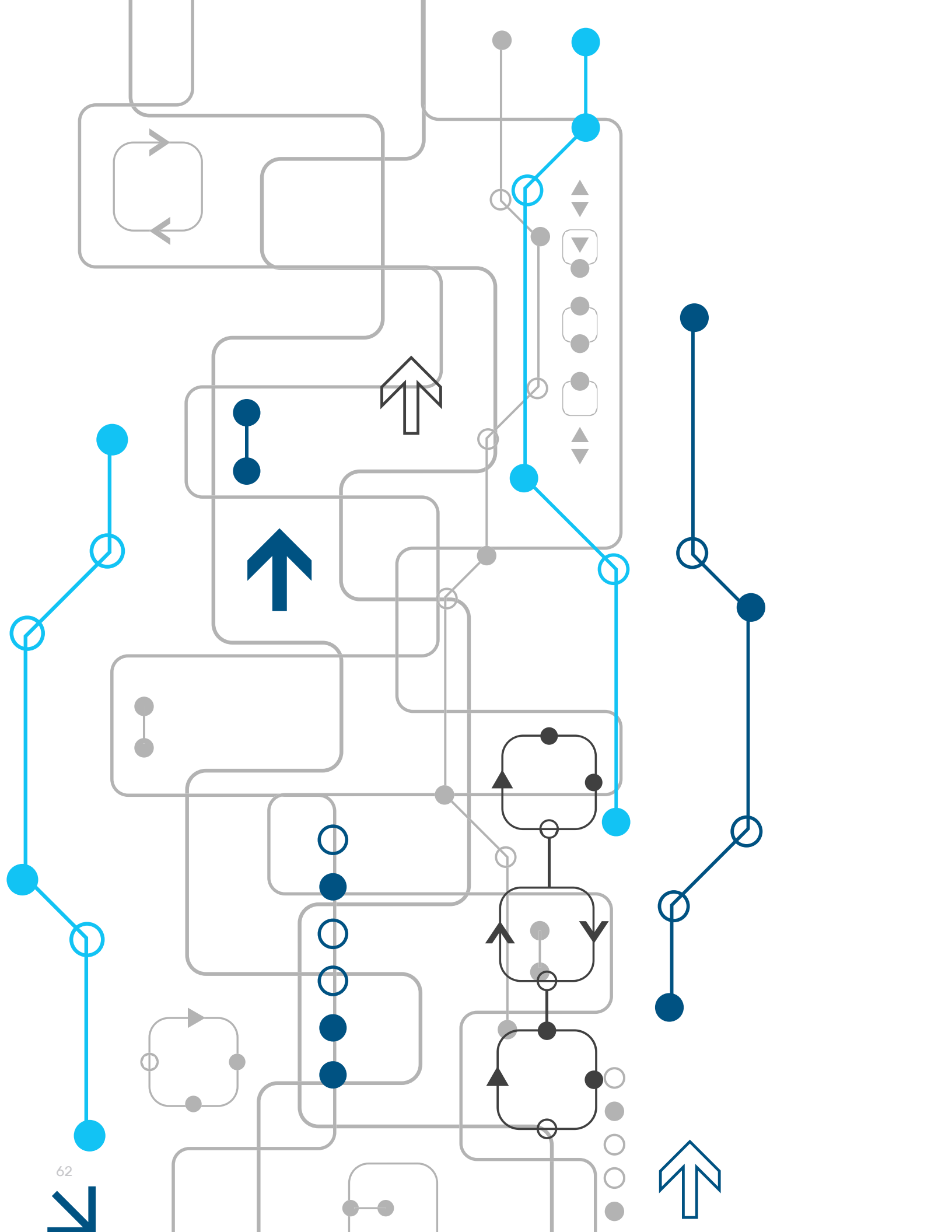
GLOSARIO

<i>Activo de información</i>	<p>Algo de valor tangible o intangible que vale la pena proteger, incluidas las personas, la información, infraestructura, finanzas y reputación.</p> <p>Fuente: ISACA 3era Edición 2015</p>
<i>Ataque</i>	<p>Intento de destruir, exponer, alterar, deshabilitar, robar, obtener acceso o uso de un activo no autorizado.</p> <p>Fuente: ISO/IEC 27000:20016</p>
<i>Ataque informático y cibernético</i>	<p>Un intento de obtener acceso no autorizado a los servicios del sistema, recursos, información, o un intento de comprometer la integridad del mismo.</p> <p>Fuente: SP 800-32</p>
<i>Ciberdelincuencia</i>	<p>Es toda aquella actividad que involucra el uso de tecnologías de información y comunicaciones con la finalidad de cometer actos ilegales en contra de personas, instituciones o Estados.</p> <p>Fuente: OF 000600 CB/2520 16016355 Ministerio de la Defensa</p>
<i>Ciberdefensa</i>	<p>Son todas aquellas políticas, estrategias, planes, procedimientos, técnicas y tácticas, encaminadas a proteger al Estado, con el objeto de minimizar amenazas, riesgos y otros desafíos a la infraestructura crítica o recursos estratégicos en el ciberespacio, dentro del marco de la Seguridad y Defensa de la Nación.</p> <p>Fuente: OF 000600 CB/2520 16016355 Ministerio de la Defensa</p>
<i>Ciberentorno</i>	<p>Incluye a usuarios, redes, dispositivos, software, procesos, información almacenada o que circula, aplicaciones, servicios y sistemas que están conectados directa o indirectamente a las redes.</p> <p>Fuente: UIT-T X.1205.</p>
<i>Ciberespacio</i>	<p>Es una red interdependiente de infraestructuras de información y comunicaciones, que incluye internet, redes de telecomunicaciones, sistemas informáticos, procesos y controles embebidos.</p> <p>Fuente: US-CERT NICCS Cyber Glossary</p>
<i>Confidencialidad</i>	<p>Propiedad que la información no está disponible o divulgada a personas o entidades no autorizadas.</p> <p>Fuente: ISO/IEC 27000:20016</p>

<i>Datos informáticos</i>	Representación simbólica (numérica, alfabética, algorítmica, espacial) de un atributo o variable cuantitativa o cualitativa. Los datos describen registros, hechos empíricos, sucesos, condiciones y entidades.
<i>Disponibilidad</i>	Propiedad de ser accesible y utilizable a pedido de una entidad autorizada. Fuente: ISO/IEC 27000:20016
<i>Dominio</i>	Sinónimo de dirección de una página principal en Internet. Es utilizada para referirse a la identificación de uno o varios servidores conectados a la Red. La asignación de dominios está regulada por el Sistema de Nombres de Dominio (DNS, por sus siglas en inglés).
<i>Evento</i>	Ocurrencia o cambio de un conjunto particular de circunstancias. Fuente: ISO/IEC 27000:20016
<i>Incidente de seguridad informático</i>	Uno o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones y amenazar la seguridad de la información. Fuente: ISO/IEC 27000:20016
<i>Información</i>	Un activo que es esencial para una organización. Eso puede existir en muchas formas: se puede imprimir o escribir en papel, almacenado electrónicamente, transmitido por correo o usando medios electrónicos, mostrados en media, o hablados en conversación. Fuente: ISACA 3era Edición 2015
<i>Infraestructura Crítica</i>	Aquellas instalaciones, bases de datos, redes, servicios y equipos físicos de tecnologías de la información necesarios para el funcionamiento normal de los servicios esenciales, cuya interrupción o destrucción debida a causas naturales, técnicas o por ataques deliberados, tendría un impacto mayor en la vida, la salud, la seguridad, el flujo de suministros vitales, el bienestar económico y las garantías de las personas.
<i>Integridad</i>	La protección contra la información incorrecta, modificación o destrucción de la misma, asegurando el no repudio y autenticidad. Fuente: ISACA 3era Edición 2015
<i>Phishing</i>	Denominación que recibe la estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial de forma fraudulenta. Fuente: Glosario de términos de Ciberseguridad INCIBE.

<p><i>Prueba de penetración / Pentest</i></p>	<p>Es un ataque a un sistema, software o hardware con el objetivo de encontrar vulnerabilidades. El ataque implica un análisis activo de cualquier vulnerabilidad potencial, configuraciones deficientes o inadecuadas, tanto de hardware como de software, o deficiencias operativas en las medidas de seguridad.</p> <p>Fuente: Glosario de términos de Ciberseguridad INCIBE.</p>
<p><i>Ransomware</i></p>	<p>El ciberdelincuente, toma control del equipo infectado y «secuestra» la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos.</p> <p>Fuente: Glosario de términos de Ciberseguridad INCIBE.</p>
<p><i>Redundancia</i></p>	<p>Capacidad de un sistema de comunicaciones para detectar un fallo en la red de la manera más rápida posible y que a la vez, sea capaz de recuperarse del problema de forma eficiente y efectiva.</p>
<p><i>Resiliencia</i></p>	<p>Capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido.</p> <p>Fuente: Real Academia Española</p>
<p><i>Riesgo</i></p>	<p>El riesgo está asociado con el potencial que las amenazas explotarán vulnerabilidades de un activo de información o grupo de activos de información causando daños a una organización.</p> <p>Fuente: ISO Guide 73:2009</p>
<p><i>Seguridad Cibernética o Ciberseguridad</i></p>	<p>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. Las propiedades de seguridad incluyen una o más de las siguientes: - disponibilidad; - integridad, que puede incluir la autenticidad y el no repudio; - confidencialidad.</p> <p>Fuente: UIT-T X.1205.</p>

<p><i>Seguridad de la información</i></p>	<p>La seguridad de la información garantiza la confidencialidad, disponibilidad e integridad de la información, por medio de la aplicación y gestión de controles apropiados que implican la consideración de una amplia gama de amenazas, con el objetivo de garantizar el éxito organizacional y la continuidad, minimizando las consecuencias de los incidentes de seguridad de la información.</p> <p>Fuente: ISO/IEC 27000:2016</p>
<p><i>Sistema de Información</i></p>	<p>La combinación de actividades estratégicas, gerenciales y operacionales involucradas en la recolección, procesamiento, almacenamiento, distribución y uso de información y sus tecnologías relacionadas.</p> <p>Fuente: ISACA 3era Edición 2015</p>





ANEXOS

➤ **Madurez de la Seguridad Cibernética en Guatemala**

El Índice Mundial de Ciberseguridad (IMC) surge de la asociación de colaboración entre el sector privado y una organización internacional, con el fin de impulsar la cuestión de la ciberseguridad hasta el primer plano de las agendas nacionales. El IMC es un proyecto conjunto emprendido por el Centro Global de Capacitación de Seguridad Cibernética de la Universidad de Oxford y la Unión Internacional de Telecomunicaciones, que contribuye a una mejor comprensión del compromiso de los estados soberanos con la ciberseguridad. La fuente de información es a través del informe “Ciberseguridad: ¿estamos preparados en América Latina y el Caribe?”¹⁵.

El IMC tiene sus raíces en la Agenda sobre Ciberseguridad Global de la UIT y considera el nivel de compromiso en 49 indicadores con cinco ámbitos: medidas jurídicas, medidas técnicas, medidas organizativas, creación de capacidades y cooperación internacional. El resultado es un índice a nivel de país y una clasificación mundial de la preparación para la ciberseguridad. El IMC no pretende determinar la eficacia ni el éxito de una medida particular, sino simplemente la existencia de estructuras nacionales para implementar y promover la ciberseguridad. Los indicadores tienen una calificación de madurez ponderada de 1 (mínimo o embrionario) a 5 (Máximo).

Para la construcción de los resultados, se remitieron a todos los Estados Miembros de la UIT, las encuestas a nivel de país, complementadas con una investigación cualitativa a fondo. Se recopiló información sobre leyes, reglamentos, CERT y CSIRT, políticas, estrategias nacionales, normas, certificaciones, formación profesional, sensibilización, y asociaciones de colaboración.

El propósito del IMC es ofrecer una instantánea de la situación de los países en cuanto a su compromiso con la ciberseguridad a nivel nacional. La idea concebida es fomentar la sensibilidad sobre la ciberseguridad y la importancia del papel que deben desempeñar los gobiernos en la integración de los mecanismos oportunos para apoyar y promover esta disciplina crucial.

Para la elaboración del primer documento –en calidad de borrador– de la Estrategia, se inició planteando y validando la información cualitativa y cuantitativa existente en el país, para ello se distribuyó desde el mes de noviembre de 2016, un informe preliminar preparado por la Organización de Estados Americanos. De lo anterior se organizó un taller en Antigua Guatemala, los días 23 y 24 de enero de 2017 en donde se convocó a todos los participantes a evaluar el anexo 1 de dicho informe, requiriendo 3 acciones concretas:

- Verificar la información recopilada durante la primera etapa del Desarrollo de una Estrategia Nacional de Ciberseguridad para Guatemala;

¹⁵ <https://publications.iadb.org/handle/11319/7449?locale-attribute=es&>

- Complementar la información recopilada durante la primera etapa con datos adicionales, de modo que se pueda preparar un diagnóstico efectivo de la ciberseguridad en el país, identificando las debilidades, amenazas, fortalezas y oportunidades en materia de seguridad cibernética;
- Formular propuestas de ejes de acción y objetivos que contengan la Estrategia Nacional de Ciberseguridad de Guatemala.

A continuación se presenta los resultados del Diagnóstico:

> Estrategia Nacional Oficial

Desarrollo de la estrategia (nivel 1): No hay evidencia de la existencia de una estrategia nacional de seguridad cibernética; si bien el país cuenta con una ley marco de seguridad nacional, no existe un plan y componentes de gestión de incidentes y respuesta cibernéticos.

Organización (nivel 1): No existe una entidad global para la coordinación de la seguridad cibernética;

Contenido (nivel 1): Ante la falta de una estrategia nacional, tanto los contenidos como la seguridad cibernética se maneja de forma independiente en todos los sectores del país.

> Cultura y Sociedad

Mentalidad de seguridad cibernética

En el gobierno (nivel 1): A raíz de un aumento en ataques cibernéticos contra la infraestructura del gobierno en los últimos años, las entidades guatemaltecas han comenzado a tomar medidas para proteger sus activos nacionales, aunque con poca comunicación formal. Los operadores de Infraestructuras Críticas Nacionales han desplegado algunas medidas de seguridad y software que cumplen con la norma ISO 27000 y otras normas internacionales. La infraestructura de tecnología suele delegarse a un tercero y el gobierno tiene un control mínimo de la misma.

En el sector privado (nivel 2): Empresas líderes han comenzado a darle prioridad a una mentalidad de seguridad cibernética mediante la identificación de prácticas de alto riesgo.

En la sociedad (nivel 1): La sociedad desconoce las amenazas cibernéticas y no puede tomar medidas concretas de seguridad cibernética o la sociedad es consciente de las amenazas cibernéticas, pero no toma medidas proactivas para mejorar su seguridad cibernética.

Conciencia de seguridad cibernética

Sensibilización (nivel 1): La necesidad de tomar conciencia de las amenazas y vulnerabilidades de seguridad cibernética en el sector público y privado no es reconocido o se encuentra en una fase inicial de discusión.

Confianza en el uso de Internet

En los servicios en línea (nivel 2): La confianza en los servicios en línea se identifica como una preocupación; los operadores de infraestructuras toman en consideración medidas para fomentar la confianza en los servicios en línea, sin embargo, no se establecen medidas.

En el gobierno electrónico (nivel 1): De acuerdo al índice de Gobierno Electrónico 2016¹⁶, en la página 61, Guatemala estuvo en 2014 en el puesto 137 y se posicionó en 2016 en el número 60, haciendo un salto positivo de 77 lugares en dicho índice. De acuerdo a dicha calificación, el gobierno ofrece varios servicios electrónicos y se encuentra desarrollando e impulsando otros que permitan empoderar a todos los sectores de la sociedad guatemalteca.

En el comercio electrónico (nivel 2): Los servicios de comercio electrónico han evolucionado en el país y como referente se puede observar en el Boletín Anual de Estadísticas del Sistema Financiero 2016 de la Superintendencia de Bancos¹⁷, el volumen del monto de tarjetas de crédito en el sistema bancario es de 9.2 millardos de quetzales, equivalente al 50% del monto global del rubro "Otros Créditos", lo que indica un alto uso como forma de pago en dicho sector. Las partes interesadas y los usuarios reconocen la necesidad de seguridad en servicios electrónicos, con lo que han iniciado inversiones entre los proveedores de servicios.

Confianza en el uso de Internet

Normas de privacidad (nivel 2): De acuerdo a la iniciativa de ley en el Congreso de la República de Guatemala, se consideran nuevas leyes y políticas que promuevan el acceso a datos personales recogidos y almacenados por todo el gobierno y otras instituciones públicas.

Privacidad del empleado (nivel 1): No hay debate, o es mínimo, entre los líderes del sector privado con respecto a las cuestiones de privacidad en el lugar de trabajo.

¹⁶ <http://workspace.unpan.org/sites/Internet/Documents/UNPAN96407.pdf>

¹⁷ http://www.sib.gob.gt/c/document_library/get_file?folderId=1094937&name=DLFE-25704.pdf

> Educación

Disponibilidad nacional de la educación y formación cibernéticas

Educación (nivel 2): Existe mercado para la educación y la formación en seguridad de la información con evidencia de asimilación; las iniciativas de los profesionales están dirigidas a incrementar el atractivo de las carreras en seguridad cibernética y la pertinencia de roles de liderazgo más amplias.

Formación (nivel 2): Existe capacitación en seguridad de la información, pero es ad-hoc y sin coordinación; cursos de formación, seminarios y recursos en línea pueden estar disponibles para los datos demográficos específicos, pero no existen medidas de efectividad.

Desarrollo nacional de la educación de seguridad cibernética

Desarrollo nacional de la educación (nivel 1): No existen, o son pocos, instructores profesionales en seguridad cibernética; no existe un programa para capacitar a instructores en seguridad cibernética; o no existe o apenas está siendo discutida la justificación del presupuesto para la educación y la investigación.

Formación e iniciativas educativas públicas y privadas

Capacitación de los empleados (nivel 2): No hay transferencia de conocimientos por parte de los empleados de seguridad cibernética capacitados; debido a una formación limitada, solo hay uso informal de herramientas, modelos o plantillas existentes para la planeación de la seguridad cibernética de la organización, sin la integración automatizada de datos.

Gobernanza corporativa, conocimiento y normas

En las empresas estatales y privadas (nivel 2): Las juntas directivas tienen algún conocimiento de cuestiones de seguridad cibernética, pero no de la forma en que estas podrían afectar a la organización, o cuáles serían las amenazas directas que pudieran enfrentar de la organización, sin la integración automatizada de datos.

> Marcos Legales

Para la seguridad de las TIC (nivel 1): La legislación relativa a la seguridad de las TIC aún no existe o está en el proceso de desarrollo; si está en proceso, se han hecho los esfuerzos para llamar la atención sobre la necesidad de crear un marco jurídico sobre la seguridad cibernética y pueden incluir la necesidad de un análisis de gestión de riesgos.

Privacidad, protección de datos y otros derechos humanos (nivel 2): Existe legislación parcial respecto a la privacidad, protección de datos y libertad de expresión.

Derecho sustantivo de delincuencia cibernética (nivel 2): Existe una legislación parcial en el derecho penal sustantivo que aplica los marcos legales y regulatorios a algunos aspectos de los delitos cibernéticos; está siendo discutido el derecho penal sustantivo para la delincuencia cibernética entre los legisladores, pero ha comenzado el desarrollo de la ley.

Derecho procesal de delincuencia cibernética (nivel 1): No existe el derecho penal procesal adecuado para la delincuencia cibernética y el uso de la prueba electrónica en otros crímenes, o existe el derecho penal procesal general y se aplica ad-hoc a la delincuencia cibernética y al uso de la prueba electrónica en otros crímenes.

Investigación jurídica

Cumplimiento de la ley (nivel 2): Existen capacidades básicas para investigar los delitos relacionados con las pruebas electrónicas de conformidad con el derecho y normativa interna, sin embargo es necesario desarrollarlas y elevarlas a niveles que la tecnología actual amerita.

Fiscalía (nivel 1): La evidencia digital es una categoría de evidencia relativamente nueva y una esfera en rápido desarrollo. Pese al marco temporal limitado de que se dispone para investigaciones científicas básicas, actualmente es preciso basar los procedimientos de búsqueda, obtención y análisis de evidencia digital en principios fiables desde el punto de vista científico. Pese a las abundantes investigaciones ya realizadas, existen varios ámbitos a los que los científicos deberían prestar atención. Por consiguiente, es importante proseguir las investigaciones científicas en ámbitos polémicos tales como la fiabilidad de la evidencia en general o la cuantificación de las posibles tasas de error. Los efectos de la evolución constante no se limitan a la necesidad de proseguir las investigaciones científicas; puesto que los progresos pueden plantear nuevas dificultades para el examen forense, es preciso impartir formación a expertos de manera constante. Los fiscales no están entrenados adecuadamente y no tienen los recursos técnicos / jurídicos para plantear ante tribunales los delitos relacionados con la informática; los recursos orientados a la cadena de custodia cibernética son limitados e incidir en las pruebas electrónicas.

Tribunales (nivel 2): Aunque la informática y las tecnologías de red se utilizan a escala mundial, las dificultades que plantea la admisibilidad de la evidencia digital en los tribunales son –no se han establecido de manera generalizada unas normas jurídicas vinculantes sobre la evidencia digital. En lo que respecta al derecho penal sustantivo y los instrumentos de procedimiento en la lucha contra el ciberdelito, la esfera de la evidencia digital también adolece de falta de armonización de las normas jurídicas a escala mundial. Un número limitado de jueces tiene capacidad para presidir un caso sobre el delito cibernético, pero esta capacidad es en gran medida ad-hoc y no sistemática; no existen recursos judiciales y de formación en delincuencia cibernética.

Divulgación responsable de la información

Divulgación responsable de la información (nivel 1): No se reconoce la necesidad de una política de divulgación responsable en las organizaciones del sector público y privado.

> Tecnologías

Adhesión a las normas

Aplicación de las normas y prácticas mínimas aceptables (nivel 1): A la fecha, no se han formalizado a nivel nacional la adopción de normas o prácticas para la seguridad de la información, asimismo se adolece de un esfuerzo concertado para aplicar las mismas.

Adquisiciones (nivel 1): No hay evidencia de uso de las normas relacionadas con la seguridad cibernética en la orientación de los procesos de adquisición, o está disponible algún reconocimiento de la orientación, pero no existe ningún esfuerzo para utilizarlo.

Desarrollo de software (nivel 1): Existe de forma aislada iniciativas para la identificación de las normas de desarrollo de software en el sector público y privado.

Organizaciones de coordinación de seguridad cibernética

Centro de mando y control (nivel 1): No existe un centro de mando y control de la seguridad cibernética a nivel nacional.

Capacidad de respuesta a incidentes (nivel 1): La capacidad de respuesta de incidentes no es coordinada y se lleva a cabo de manera ad-hoc.

Respuesta a incidentes

Identificación y designación (nivel 2): Se han clasificado ciertos eventos cibernéticos o amenazas y se han registrado como incidentes o desafíos a nivel nacional.

Organización (nivel 1): La respuesta a incidentes nacional es limitada, reactiva y ad-hoc.

Coordinación (nivel 1): La responsabilidad de la respuesta a incidentes a nivel nacional, no existe.

Resiliencia de la infraestructura nacional

Infraestructura tecnológica (nivel 2): Se realiza el despliegue no estratégico de la tecnología y los procesos en los sectores público y privado; están disponibles en línea servicios públicos en línea, información y contenidos digitales, pero son limitadas la implementación y el proceso.

Resiliencia nacional (nivel 1): El gobierno tiene un control mínimo, de infraestructura tecnológica; las redes y sistemas son delegados a terceros, con potencial de adopción por parte de mercados de terceros poco fiables; puede haber una dependencia de otros países en tecnología de la seguridad cibernética.

Protección de infraestructura crítica nacional (ICN)

Identificación (nivel 1): Se entiende poco o nada de los activos y las vulnerabilidades de la ICN, pero no han sido identificadas las vulnerabilidades o categorización formal.

Organización (nivel 1): Hay interacción básica entre los ministerios gubernamentales y los propietarios de los activos críticos; no existe un mecanismo de colaboración formal.

Planeación de respuesta (nivel 1): La planeación de la respuesta a un ataque a los activos críticos no ha sido discutida ampliamente.

Coordinación (nivel 1): Los procedimientos informales de diálogo entre el sector público y privado pueden estar desarrollados, pero hacen falta parámetros de intercambio de información y generalmente o son de forma individual o no estructurada, o son inexistentes.

Gestión de Riesgo (nivel 1): La sensibilización de amenazas por los operadores de ICN existe de forma aislada; las habilidades y comprensión básicas de gestión de riesgos pueden ser incorporadas en las prácticas empresariales en la línea de seguridad cibernética y protección de datos.

Gestión de crisis

Planeación (nivel 1): No hay entendimiento, o es mínimo, de que la gestión de crisis es necesaria para la seguridad nacional; se ha asignado en principio la autoridad de planeación y diseño del ejercicio, pero no se ha esbozado la planeación.

Evaluación (nivel 1): No se ha realizado ninguna evaluación de los protocolos y procedimientos de gestión de crisis; los resultados de los ejercicios no informan a la gestión global de crisis.

Redundancia digital

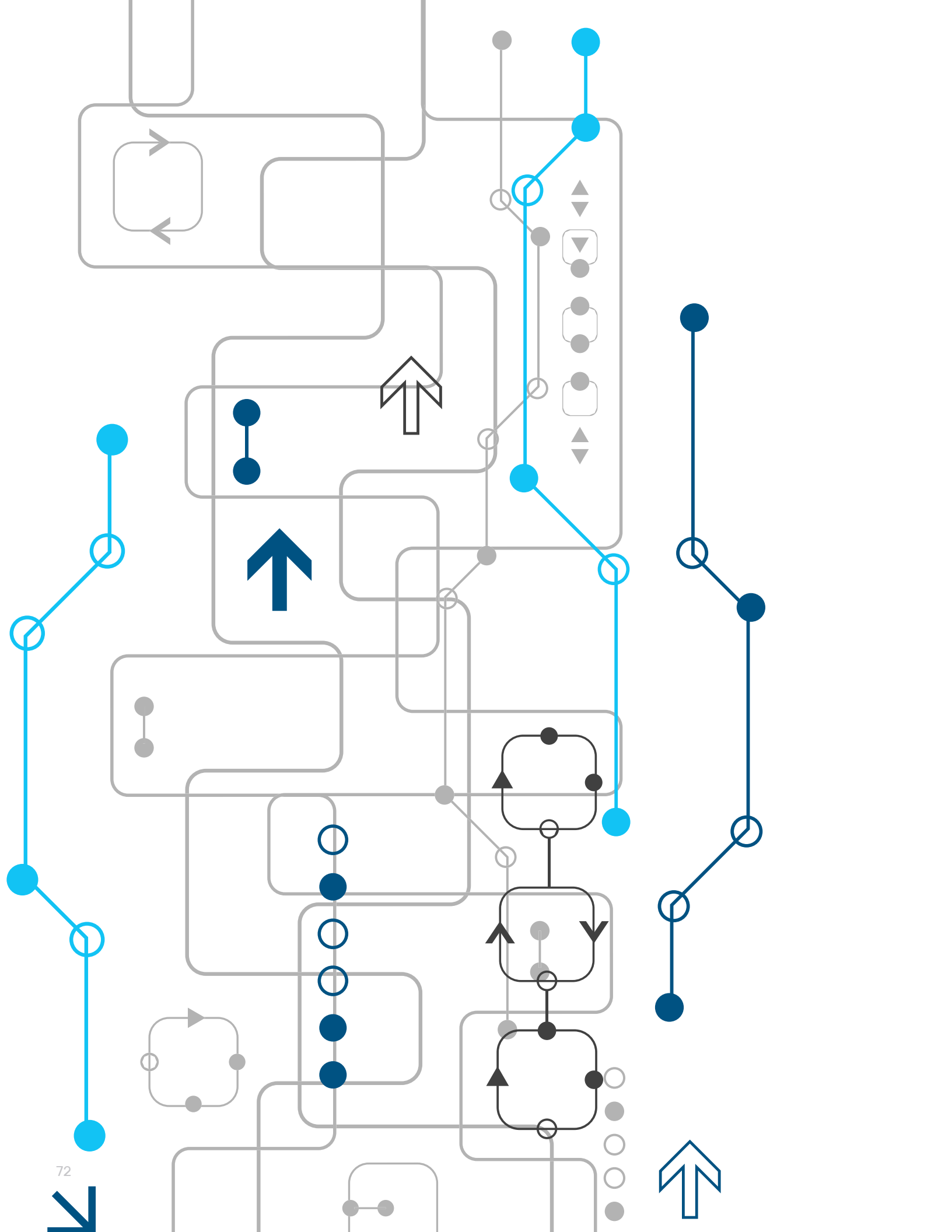
Planeación (nivel 1): Las medidas de redundancia digitales actualmente son de carácter optativo o no considerado.

Organización (nivel 1): Los activos de respuesta de emergencia actuales no han sido identificados; si se identifican, carecen de cualquier nivel de integración.

Mercado de la ciberseguridad

Tecnologías de seguridad cibernética (nivel 1): Poca o ninguna tecnología se produce en el país; pueden estar restringidas las ofertas internacionales o son vendidas con un sobreprecio.

Seguros de delincuencia cibernética (nivel 1): La necesidad de un mercado en seguro de la delincuencia informática no ha sido identificada; a través de la evaluación de riesgos financieros para el sector público y privado.



AGRADECIMIENTOS

El Señor Ministro de Gobernación agradece la invaluable colaboración a todos los integrantes de las distintas mesas del Sector Privado, Gubernamental, Sociedad Civil, Academia, Infraestructuras Críticas y empresas relacionadas a las Tecnologías de Información y Comunicaciones que participaron en los talleres para la fase de formulación del presente documento.

También se otorga de manera especial un agradecimiento al Comité Interamericano contra el Terrorismo de la Organización de Estados Americanos, a las Embajadas de Canadá y España, los representantes de los Ministerios de Relaciones Exteriores, Defensa, Gobernación, la Secretaría Nacional de Ciencia y Tecnología, Secretaría Técnica del Consejo Nacional de Seguridad y la Superintendencia de Telecomunicaciones, por su invaluable apoyo al brindar el espacio de discusión e intercambio de experiencias para la formulación de la Estrategia Nacional de Seguridad Cibernética.





9 789929 764897