MISIÓN DE ASISTENCIA TÉCNICA EN SEGURIDAD CIBERNÉTICA

CONCLUSIONES Y RECOMENDACIONES

4 de abril de 2014
Bogotá, Colombia

Organización de los
Estados Americanos

El gobierno de Colombia solicitó a la Organización de los Estados Americanos (OEA) el apoyo para organizar una Comisión de Expertos Internacionales para evaluar el estado de la seguridad cibernética del país, lo que refleja el deseo del Señor Presidente de la República de Colombia, S.E. Juan Manuel Santos Calderón, hacer de las tecnologías de información y comunicaciones una parte integral del plan de desarrollo del país. Después de visitar las instituciones colombianas con responsabilidad en la seguridad cibernética nacional, de escuchar presentaciones de actores relevantes de seguridad cibernética en Colombia, y de entablar un intercambio de ideas con expertos colombianos sobre el estado de la seguridad cibernética en el país, los expertos internacionales prepararon una serie de recomendaciones para ser tenidas en cuenta por el gobierno de Colombia. La Comisión Internacional de Expertos Internacionales brindó su experiencia en políticas de seguridad cibernética, marcos institucionales, respuesta a incidentes de seguridad cibernética, investigación y legislación de delitos cibernéticos, ciberdefensa y cooperación internacional. Los expertos internacionales que participaron de esta Misión de Asistencia Técnica, son funcionarios de los gobiernos de Canadá, España, Estados Unidos, el Reino Unido, República Dominicana, Estonia, Israel, República de Corea y Uruguay. De igual forma, además de funcionarios de la OEA, esta Comisión Internacional contó con la participación de representantes del el Consejo de Europa (COE), el Foro Económico Mundial (WEF), INTERPOL, Organización de las Naciones Unidas (ONU), la Organización para la Cooperación y el Desarrollo Económico (OCDE), y la Universidad de Oxford. Las recomendaciones de los expertos fueron redactadas en sesiones privadas, garantizando un análisis equilibrado e imparcial de las necesidades y pasos a seguir que deberían ser considerados por el gobierno colombiano. Aunque la OEA organizó esta Comisión Internacional de Expertos, este documento no refleja posición u opinión alguna de esta organización internacional.

CONTRIBUIDORES

EXPERTOS INTERNACIONALES

ADRIÁN ACOSTA
INTERPOL
CLAUDIO PEGUERO
POLICÍA NACIONAL DOMINICANA
DARKO LOVRIC
FORO ECONÓMICO MUNDIAL
DIRK NONNINGER
DIRECCIÓN EJECUTIVA DEL COMITÉ CONTRA EL TERRORISMO DE LA ONU
ELVIRA TEJADA
FISCALÍA GENERAL DE ESPAÑA
EREZ KREINER
OFICINA NACIONAL DE ASUNTOS CIBERNÉTICOS DE ISRAEL
ERWIN DOTZAUER
UNIVERSIDAD DE OXFORD
GWEN BEAUCHEMIN
DEPARTAMENTO DE SEGURIDAD PÚBLICA DE CANADÁ
IAN MABBOTT
AGENCIA DE COMERCIO E INVERSIÓN DEL REINO UNIDO
LAURENT BERNAT
ORGANIZACIÓN PARA LA COOPERACIÓN Y DESARROLLO ECONÓMICO (OCDE)
LAURI LUHT
AUTORIDAD DE SISTEMAS DE INFORMACIÓN DE ESTONIA
MANUEL SICILIA SAN JOSÉ
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURA CRÍTICA (CNPIC) DE ESPAÑA
MARCOS SALT
CONSEJO DE EUROPA
NATHAN DOYEL
DEPARTAMENTO DE ESTADO DE LOS ESTADOS UNIDOS
ROBERT GORDON
DEPARTAMENTO DE SEGURIDAD PÚBLICA DE CANADÁ
RODOLFO ORJALES
REUNIONES DE MINISTROS DE JUSTICIA U OTROS MINISTROS PROCURADORES O FISCALES GENERALES DE LAS AMÉRICAS (REMJA)

SANTIAGO PAZ
AGENCIA DEL GOBIERNO ELECTRÓNICO
Y SEGURIDAD DE LA INFORMACIÓN (AGESIC) DE URUGUAY
YOUNG-JUN KIM
AGENCIA DE INTERNET Y SEGURIDAD DE COREA

EXPERTOS NACIONALES

MINISTERIO DE DEFENSA
SONIA JULIANA GARCÍA VARGAS
OSCAR JAVIER ARIAS ARIAS
WILSON PRIETO
CORONEL FREDDY BAUTISTA
MAYOR LUIS ATUESTA
MAYOR ALEX DURAN
TENIENTE JHON GUEVARA
CF. WILLIAM HERNANDEZ
C. MILENA REALPE
M. DIDIER SUAREZ
MAYOR DANIEL UCRÓS
JAIRO BECERRA
GUILLERMO MENDOZA
YANETH YATE HURTADO
WILSON FERNANDO CARVAJAL
JAVIER PABON RIVAS
MANUEL DÍAZ HOYOS
CORONEL MARTHA LILIANA SANCHEZ
CR. JAIRO ANDRÉS CÁSERES
CF. CONSTANZA BERMUDEZ
CF. GERMÁN GARZÓN
TE. ZABALA LOPEZ
TE. PINTO ANDREA
TE. ANDRÉS FELIPE CAMPOS
TC. JAVIER BARRERA

MINISTERIO DE TIC
MARÍA ISABEL MEJÍA
JORGE FERNANDO BEJARANO
LUIS ALEJANDRO BECERRA
HUGO SIN TRIANA
ALEJANDRO DELGADO
LUCIA ALEMAÑY
JULIAN DAVID ZULUAGA
CLAUDIA HURTADO

MINISTERIO DE JUSTICIA Y EL DERECHO
AUGUSTO IBAÑEZ
ORLANDO SARMIENTO
PAULA GALLO CAICEDO
MARIA FERNANDA FUENTES

RAMA JUDICIAL
ALEXANDER DÍAZ

SECTOR PRIVADO Y ACADEMIA

DIEGO ZULUAGA
JEIMY CANO
JOSÉ MONTOYA
MANUEL SANTANDER
ANDRES GALINDO
GONZALO ROMERO
JOSÉ MIGUEL DE LA CALLE
CLAUDIA BUSTAMANTE
MANUEL DÁVILA
BIATRIZ CAICEDO
JUAN DIEGO JIMENEZ
ANDRÉS GUZMAN

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA)

NEIL KLOPFENSTEIN
SECRETARIO EJECUTIVO
COMITÉ INTERAMERICANO CONTRA EL TERRORISMO (CICTE)

PABLO MARTINEZ
GERENTE DE PROGRAMA PRINCIPAL
Y COORDINADOR DE PROGRAMAS, OEA/CICTE

BELISARIO CONTRERAS
GERENTE DE PROGRAMA
DE SEGURIDAD CIBERNÉTICA, OEA/CICTE

BRIAN DITO
GERENTE ASISTENTE DE PROGRAMA
DE SEGURIDAD CIBERNÉTICA, OEA/CICTE

1 - FORTALECIMIENTO DE LAS CAPACIDADES INSTITUCIONALES DE CIBERSEGURIDAD Y CIBERDEFENSA

Las siguientes recomendaciones se centran en las cinco áreas que se consideran que son las más fundamentales. Se reconoce que puede haber otros aspectos que merecen tenerse en cuenta, como la sensibilización del público, desarrollo de habilidades, etc.

En este documento, el término "ciberseguridad" incluye los conceptos de "ciberseguridad" y "ciberdefensa" como se define en el CONPES 3701.

Las siguientes recomendaciones tienen en cuenta los problemas específicos de la seguridad nacional que enfrenta Colombia y el papel fundamental desempeñado por el Ministerio de Defensa, y ese papel debe continuar. Nuestras recomendaciones reconocen la necesidad de preservar la capacidad de los organismos de seguridad de Colombia.

Desafío 1. Los esfuerzos de Colombia para abordar la ciberseguridad están limitados por la falta de una visión general clara.

La seguridad no es un fin en sí mismo. Es un medio de soporte de objetivos de más alto nivel.

Aunque el CONPES 3701 representa un importante paso adelante, no aborda los problemas a un alto nivel de forma que proporcione una visión estratégica clara. En la etapa actual, la comprensión del Gobierno sobre ese tema (por ejemplo, definición de ciberseguridad y ciberdefensa) y los objetivos generales parecen más bien estar motivados por consideraciones e intereses institucionales más que por una visión clara para el país que trascienda estas consideraciones. Aunque los asuntos institucionales son esenciales para poner en práctica una visión estratégica, estos solo cubren un aspecto. Deben ser el resultado de la visión y no al revés.

Recomendación 1: desarrollar una visión global ("la visión") para la ciberseguridad.

La visión debe:

- Formular claramente los objetivos amplios y de alto nivel que se buscan y articular por qué son esenciales para la nación.
- Distinguir claramente los objetivos de:
  1. la prosperidad económica y social,
  2. la defensa del país (por ejemplo, militar, de inteligencia, etc.), y
  3. la lucha contra el cibercrimen.

La naturaleza de estos 3 objetivos es diferente y se deben abordar por separado. Sin embargo, también se superponen en algunas áreas. Esta superposición debe abordarse específicamente (por ejemplo, a través de mecanismos de coordinación adecuados) en vez de volverse la guía de toda la visión.

- Reconocer la necesidad de respetar los valores establecidos en la Constitución.
- Ser liderada por el más alto nivel del gobierno. Esto se asegurará de que:
    - La visión sea entendida y seguida por todos al interior del gobierno, y en aspectos económicos y de la sociedad.
    - Los tres objetivos anteriores, a veces contradictorios y que compiten entre sí, se equilibran para el mejor beneficio de la nación.
- Incluir la cooperación internacional. El entorno digital es inherentemente global. La mayoría de los aspectos de la gestión del riesgo de la ciberseguridad tienen un carácter internacional.

Desafío 2. El enfoque global de la ciberseguridad no se basa en la gestión de riesgos.

Se están adoptando medidas de seguridad sin que sean el resultado de una evaluación o gestión sistemática del riesgo. El enfoque actual tiene como objetivo lograr la seguridad en lugar de gestionar los riesgos. Un enfoque de gestión de riesgos tiene como objetivo obtener los beneficios de un entorno digital para lograr la prosperidad económica y social. Como Colombia es cada vez más digital, un enfoque de seguridad (es decir, no basado en la gestión de riesgos) será cada vez más insostenible y costoso sin que efectivamente se proteja la economía y la sociedad. Esto será especialmente claro con respecto a la protección de infraestructuras críticas.

Desde una perspectiva organizacional, existen dos cuestiones principales: 1) El nivel más alto de gobierno no cuenta con una evaluación exhaustiva de la situación de riesgo global de ciberseguridad en todo el país y por lo tanto no puede tomar decisiones basadas en el riesgo, 2) Las actividades en los niveles inferiores no se basan en la gestión del riesgo.

Recomendación 2: Adoptar un enfoque global de la gestión de riesgos de ciberseguridad.

- Basar la visión global en un enfoque de gestión de riesgos.
- Establecer un programa nacional de gestión de riesgos (incluida la evaluación, el tratamiento, la selección de medidas de seguridad, la preparación, la recuperación), y la metodología para que todos los actores evalúen y gestionen los riesgos de ciberseguridad, incluida la sensibilización, la formación, etc.
- Establecer una capacidad para desarrollar una evaluación integral de riesgos de ciberseguridad nacional.

Desafío 3. La responsabilidad no está distribuida claramente en todo el gobierno y algunas instituciones tienen la responsabilidad pero sin la autoridad o recursos para actuar.

El marco institucional es complejo y no es claro quién es responsable de qué. La impresión que deja es que la responsabilidad es vaga, la coordinación es compleja y no existen mecanismos claros.
La asignación y planificación de los recursos no están claras y no son el resultado de una evaluación exhaustiva de la situación de riesgo general de ciberseguridad en todo el país, que cubra los 3 objetivos identificados anteriormente.

La ausencia de una autoridad responsable de coordinación general conduce a una posible duplicación de esfuerzos y menor eficiencia. La dinámica institucional existente parece estar motivada por la asignación de recursos en lugar de los objetivos de gestión de riesgos de ciberseguridad.

Recomendación 3: establecer un marco institucional claro.

Este marco debería:

- Establecer un órgano de coordinación permanente (organismo coordinador) con un rol que se extienda por todo el gobierno. Este organismo debería responder directamente al Presidente.
- Asignarle a la instancia de coordinación:
  - La autoridad y responsabilidad legal para actuar, que incluya recursos presupuestales para poder responder a la visión.
  - La responsabilidad de dirigir la formulación de la política pública para asegurar un enfoque de conjunto gubernamental coherente.
  - El establecimiento de un programa nacional de gestión de riesgos mencionado.
- Proporcionarle al organismo de coordinación la capacidad de desarrollar una evaluación integral de los riesgos de ciberseguridad nacional.

Debería considerarse la posibilidad de localizar el CERT nacional (actualmente el colCERT), al interior del órgano coordinador. Este órgano de coordinación debe garantizar la independencia de las entidades constitucionalmente establecidas para ejercer funciones judiciales.

Desafío 4. El mecanismo para el vínculo integral con todas las partes interesadas (incluido el sector privado, la academia, la sociedad civil, y entidades internacionales) no está lo suficientemente desarrollado[1].

Se ha iniciado un diálogo público-privado. Sin embargo, para llegar al siguiente nivel de madurez para gestionar el riesgo de la ciberseguridad, este debe ser mejorado significativamente y deben participar todos los actores de la economía y la sociedad. Todas las partes interesadas tienen la responsabilidad de la gestión de los riesgos de ciberseguridad, de acuerdo con su función. Por lo tanto, la implementación de la visión se basa en su compromiso completo. Es esencial involucrar a todos los actores (públicos y privados) en el desarrollo de la visión, las políticas y en su implementación, para maximizar su compromiso.

Recomendación 4: establecer un proceso sistemático para involucrar a todos los interesados en el desarrollo de la estrategia y su implementación.

- Consultar con todas las partes interesadas sobre la forma de organizar el diálogo sistemático entre todas las partes interesadas
- Establecer reglas para consultar sistemáticamente a todas las partes interesadas en la fase inicial y a lo largo de la elaboración de políticas
- Sobre la base de los esfuerzos existentes, crear foros para que todos los interesados participen en la ejecución de la visión
- Desarrollar un plan a corto, mediano y largo plazo para llegar progresivamente a todos los actores gubernamentales y no gubernamentales

Desafío 5. Es limitado el enfoque del gobierno en relación con la protección de la infraestructura crítica

La política de infraestructura crítica está en la agenda del gobierno y ya se inició un proceso de identificación de las infraestructuras críticas y asuntos relacionados (por ejemplo, relacionados con la cadena de oferta). Sin embargo, aún no se ha desarrollado una definición de lo que es la infraestructura crítica y por lo tanto se desconoce lo que hay que proteger. Colombia está en la etapa temprana de la formulación de la política de infraestructura crítica. La mayoría de la infraestructura crítica es propiedad y está operada por el sector privado y, por tanto, debe estar en el centro del desarrollo de la política de protección de infraestructura crítica. Sin embargo, ese no parece ser el caso en la política de protección de la infraestructura crítica que se planea.

[1] Se puede consultar una orientación adicional sobre este tema en las recomendaciones de las secciones de “marcos legales” y “cooperación internacional”.

Recomendación 5. El gobierno debe adoptar una política para la protección de la infraestructura crítica, teniendo en cuenta los aspectos de personal, físicos y lógicos.

- Los aspectos digitales de la política de protección de la infraestructura crítica debe ser parte de la visión. El aspecto digital (o ciber) de protección de la infraestructura crítica debe ser un subgrupo del enfoque global de la protección de la infraestructura crítica.
- La política de la infraestructura crítica contribuye tanto a la prosperidad económica y social del país, como a su defensa. Por lo tanto, la entidad de coordinación debe liderar este proceso de formulación de políticas para asegurar que los objetivos que a veces compiten entre sí se equilibren adecuadamente, para el máximo beneficio del país.
- La descripción de la función del colCERT en el CONPES 3701 ("Esquema relacional del colCERT", en el gráfico 6) refleja un enfoque apropiado para la protección de la infraestructura crítica con respecto a la aplicación de la visión en el ámbito de la protección de la infraestructura crítica. Sin embargo, dado que la política de la infraestructura crítica se sobrepone a la prosperidad económica y social y a la defensa del país, esta función debe ubicarse como parte del órgano de coordinación (y no debería llamarse un "CERT").

2 - ESTABLECIMIENTO Y MEJORA DE LOS MARCOS LEGALES EN CIBERSEGURIDAD

1. Se recomienda al gobierno de Colombia, de conformidad con el planteamiento del Grupo de Expertos en Delitos Informáticos de la REMJA (OEA), que reforme su legislación armonizándola con la Convención de Budapest, especialmente en lo referido a las cuestiones de Derecho Procesal Penal, para posteriormente adherirse a la citada Convención del Consejo de Europa. Adicionalmente, se recomienda tomar en cuenta legislaciones cibernéticas exitosas tales como la Ley 53-07 de la Republica Dominicana y la Ley 109/2009 del 15 de Septiembre de Portugal. A los fines de la redacción de los tipos penales, se recomienda tomar en cuenta la importancia de la utilización de términos tecnológicamente neutrales, a fin de facilitar la interpretación y aplicación de la Ley Penal.

2. Las cuestiones que tienen que ver con la persecución de los delitos informáticos deben ser adecuadamente separados de las cuestiones de Ciberdefensa y Ciberguerra, definiendo la unidad policial que se va encargar específicamente de la prevención, investigación y persecución de los delitos informáticos. Todo ello sin perjuicio de la colaboración interinstitucional oportuna.

3. Establecer un régimen rápido y eficiente para asegurar la cooperación internacional en la prevención, investigación y persecución penal de los delitos informáticos. Entre ellas, específicamente se recomienda establecer un punto de contacto para La Red 24 / 7, disponible las 24 horas del día, 7 días a la semana, con la finalidad de garantizar la prestación de ayuda inmediata para los fines de las investigaciones o procedimientos relacionados con delitos vinculados a sistemas y datos informáticos, o para la obtención de pruebas electrónicas de un delito.

4. Adoptar medidas que prevean la responsabilidad de las personas jurídicas conforme a lo establecido en el Artículo 12 de la Convención Europea de Budapest.

5. En toda la regulación referida a los poderes procesales para la investigación de delitos informáticos se debe tomar especialmente en cuenta la necesidad de un adecuado balance entre eficiencia de la investigación y la protección de garantías individuales, especialmente en lo que se refiere a la intimidad y al derecho a la protección de datos.

6. Reconociendo que la evidencia digital requiere de una atención rápida e inmediata, teniendo en cuenta el carácter volátil de la evidencia digital, se recomienda promover medidas y poderes procesales para posibilitar la preservación especifica de datos, de acuerdo a lo previsto en el artículo 16 y 17 de la Convención de Budapest.

7. Implementar legislativamente en Colombia la retención mandatoria de datos de tráfico por un término mínimo de un año, garantizando los derechos constitucionales del país, en particular los derechos a la privacidad y protección de datos personales, así como los pactos internacionales suscritos por Colombia.

8. Solicitar de los gobiernos en los que se encuentran las principales empresas proveedoras de servicios de internet, que albergan servidores con datos de ciudadanos de Colombia, que revisen los mecanismos de cooperación en materia penal, a fin de posibilitar que estas compañías respondan en tiempo las solicitudes de asistencia en materia penal.

9. Aconsejar la creación de unidades nacionales especializadas de Fiscales con preparación especifica para la investigación y el ejercicio de la acción penal, respecto de los ciberdelitos y de los delitos en los que estén implicados evidencias electrónicas.

10. Se recomienda especialmente la organización de cursos de capacitación para jueces, fiscales y policías tanto en materia de delitos informáticos como en los aspectos técnicos y jurídicos de la obtención de evidencia digital, en la legalidad y constitucionalidad de la extracción de la evidencia digital.

11. Promover, con la participación del sector privado, leyes y reglamentaciones que regulen las obligaciones para las empresas que tienen bajo su control infraestructura critica, de reportar los incidentes de seguridad cibernética en un plazo no mayor a 48 horas, bajo garantía de confidencialidad.

Para la aplicación de las recomendaciones anteriores, entendemos que resulta de fundamental importancia tomar en consideración las opiniones de los operadores del Sistema Penal, del Sector Académico y de la Sociedad Civil.

3 - GENERACIÓN DE CAPACIDADES DE CIBERSEGURIDAD Y CIBERDEFENSA

1. Establecer una capacidad nacional de ciberseguridad civil que incluya un Centro de Respuesta a Incidentes de Seguridad Cibernética y un centro nacional de operaciones de seguridad civil al interior del órgano de coordinación permanente mencionado anteriormente. Tomará tiempo establecer la madurez de la ciberseguridad y se debe considerar la posibilidad de establecer un programa de transformación para asegurar que este se lleve a cabo de manera oportuna y coordinada.

2. Establecer canales de intercambio bidireccional de información. El centro de respuesta a incidentes informáticos ("el Centro") necesita recibir información sobre incidentes por parte de todos los actores (elementos de infraestructura crítica, centros de operaciones de seguridad del sector público y privado, y entidades gubernamentales, incluyendo políticas, militar e internacional). El Centro servirá de orientación y apoyo a las infraestructuras críticas, que incluye el asesoramiento sobre las normas de ciberseguridad aplicables u obligatorias. El Centro informaría a los actores afectados acerca de los incidentes operacionales que requieran acción.

3. El Centro, los centros de operaciones de seguridad y otras autoridades deben establecer una sólida capacidad analítica y técnica. Se deberán adquirir las herramientas de análisis y la capacitación requerida para utilizarlas de manera que se puedan estudiar las tendencias en el ámbito de amenazas nacional, incluidas las capacidades de ingeniería inversa para lograr un profundo trabajo técnico en análisis de malware, asuntos cibernéticos emergentes, tecnología móvil, seguimiento de las nuevas infraestructuras de banda ancha nacional, analítica de grandes volúmenes de datos, sistemas de control de procesos, desarrollo de herramientas avanzadas de visualización y automatización, entre otros.

4. Para abordar la ciberseguridad en Colombia, se requieren recursos humanos y financieros suficientes para cumplir sus mandatos nacionales de ciberseguridad. El gobierno deberá establecer una academia de cibernética profesional para capacitar a profesionales de la ciberseguridad y promover la acreditación y la certificación de otro tipo de educación cibernética en el país. Del mismo modo, el órgano de coordinación debe identificar las descripciones de los puestos de trabajo cibernéticos y los conocimientos, habilidades y antecedentes necesarios. Se debe sensibilizar a la población con respecto a carreras en ciberseguridad y agencias cibernéticas para atraer y retener a trabajadores talentosos, que incluye el intercambio de profesionales.

5. El órgano coordinador deberá garantizar que los servicios profesionales clave estén certificados, como las pruebas de penetración, ejercicios de simulacro con equipos opuestos, y otros.

6. Se deben establecer centros de innovación donde los colombianos puedan buscar iniciativas empresariales en ciberseguridad. Se le debe dar relevancia a las pequeñas y medianas empresas, que son fuentes importantes de innovación.

7. Se debe tener en cuenta la carga financiera de las pequeñas y medianas empresas, y sectores con pocos recursos financieros para desarrollar capacidades de ciberseguridad, a través de incentivos fiscales, subvenciones u otros mecanismos.

8. El órgano de coordinación deberá ser un repositorio de mejores prácticas de ciberseguridad en Colombia, incluida la orientación y el asesoramiento sobre las normas y marcos para la acreditación y la certificación.

4 - COOPERACIÓN INTERNACIONAL Y COOPERACIÓN ENTRE MULTIPLES PARTES INTERESADAS

La ciberseguridad es un tema que involucra múltiples partes interesadas. Una labor eficaz en este campo requiere una cooperación profunda y sostenida con el sector privado (nacional e internacional), así como con los gobiernos extranjeros, organizaciones internacionales y expertos académicos.

Las recomendaciones descritas aquí deben ser adoptadas por las instituciones respectivas al interior del gobierno de Colombia, y deben incluir una amplia consulta con el sector privado.

1. Desarrollar una estrategia escrita para la cooperación internacional que aborde la ciberseguridad y el cibercrimen, en donde se identifiquen prioridades, socios internacionales y objetivos. Todas las áreas del gobierno involucradas con cibercrimen y ciberseguridad deberán participar en el desarrollo del mismo, y el documento deberá ser aprobado por los más altos niveles del gobierno. La estrategia deberá integrarse en las estrategias más amplias del gobierno sobre política exterior, documentos de planificación, y solicitudes de recursos.

2. Ampliar el papel del Ministerio de Relaciones Exteriores en la cooperación internacional en relación con la ciberseguridad. Fortalecer la capacidad de la Cancillería para adelantar la cooperación internacional requerida.

3. Estudiar la posibilidad de crear la posición de Coordinador de Política Cibernética Internacional, cuya responsabilidad principal será la implementación de la estrategia de cooperación internacional. Al mismo tiempo, esta persona deberá mantener una relación fuerte y establecer una retroalimentación con los funcionarios que toman decisiones y desarrollan políticas internas y con los expertos técnicos, para que todos las partes interesadas tengan una visión integral de las políticas de ciberseguridad.

4. Establecer cooperación entre el sector público y privado, nacional e internacional, en el área de ciberseguridad mediante la creación de un mecanismo formal entre el gobierno y el sector privado, que sea seguro y disponible, para el intercambio de información de incidentes de ciberseguridad nacional e internacional. Este mecanismo deberá permitir compartir la información de forma bidireccional[2] entre el gobierno y el sector privado y deberá incluir el intercambio activo de información respecto a las políticas de ciberseguridad y permitir un intercambio mutuo de ideas entre el gobierno y un ámbito más amplio del sector privado.

[2] Intercambio de información bidireccional: El mecanismo deberá permitir una relación de ganancia mutua, en el que el gobierno recibe información sobre incidentes de seguridad y el sector privado recibe productos útiles como alertas tempranas y evaluación de amenazas.

5. Invertir en un plan de capacitación internacional apoyado por los altos niveles de gobierno con el objetivo de disminuir la brecha de conocimiento. El plan puede incluir programas de intercambio de corto, mediano y largo plazo con organismos relevantes en ciberseguridad, evaluaciones técnicas de y hacia otros países, y mayor cooperación con expertos internacionales. El plan de formación deberá incluir las necesidades de los funcionarios de todas las áreas del gobierno involucradas en la ciberseguridad y el cibercrimen, así como fiscales, jueces y todo otro funcionario encargado de la aplicación de la ley. Esta iniciativa deberá ser acompañada por informes ejecutivos frecuentes para los funcionarios de alto nivel para que permanezcan informados acerca de los desarrollos en el ámbito de la ciberseguridad y cibercrimen.

6. Iniciar un proyecto y hacer uso de las relaciones existentes para facilitar el intercambio de datos con respecto a incidentes de ciberseguridad. Colombia deberá aplicar lo anterior a través de entidades regionales o internacionales pertinentes, por ejemplo, *el International Watch and Warning Network,* el *Forum for Incident Response* y Equipos de Seguridad.

7. Con el fin de facilitar el intercambio rápido de datos relacionados con la ciberseguridad y cibercrimen, Colombia deberá adherir al sistema I-24/7 de INTERPOL para todas las unidades de las fuerzas de seguridad de cibercrimen de Colombia.

8. Fortalecer conocimientos académicos existentes a través de la cooperación internacional por medio del desarrollo conjunto de cursos, visitas de profesores extranjeros, y programas de intercambio para estudiantes que aborden contenido de gestión de riesgos de ciberseguridad, gestión de incidentes, defensa de redes, análisis forense, nuevas tecnologías, etc.

9. Establecer un marco para facilitar el intercambio directo de información entre equipos de respuesta a incidentes cibernéticos de otros países.

10. Identificar las contrapartes en la región en las que la cooperación y la creación de medidas de generación de confianza serían de mutuo beneficio.

11. Participar activamente en los foros internacionales de ciberseguridad para avanzar en los objetivos identificados en la estrategia de cooperación internacional. Fomentar activamente la creación y participación en ejercicios técnicos a nivel regional y global de manera frecuente.

12. Asegurarse de que todas las actividades internacionales que involucran el intercambio de datos personales respeten las leyes internacionales de derechos humanos, incluido el derecho a la privacidad.

Organización de los Estados Americanos (OEA)
Programa de Seguridad Cibernética