AVANCES EN LA ESFERA DE LA INFORMACIÓN Y LAS TELECOMUNICACIONES EN EL CONTEXTO DE LA SEGURIDAD INTERNACIONAL

Evaluación General de los temas relacionados con la seguridad de la información

Durante los últimos años se ha presentado un progreso significativo en el desarrollo y aplicación de las Tecnologías de la Información y las Comunicaciones, lo que ha generado importantes cambios y beneficios que han contribuido considerablemente al desarrollo de los países y, ha favorecido la expansión de la cooperación internacional con el objetivo de optimizar la difusión de la información.

No obstante, y de manera simultánea, el avance de esta tecnologías pone de manifiesto una profunda preocupación entorno a la posibilidad de que estos desarrollos sean utilizados con el propósito de quebrantar la estabilidad y seguridad internacional, y de afectar la integridad de la infraestructura de los Estados, afectando a su vez, la seguridad en los ámbitos civil y militar de los mismos.

Bajo este marco, para Colombia el uso de las nuevas tecnologías para generar amenazas informáticas, y la amenaza que actualmente genera la criminalidad en el ciberespacio, es un asunto de la mayor preocupación e interés nacional.

Por lo anterior, para Colombia resulta imperativo definir políticas y estrategias con el fin de impedir que las Tecnologías de la Información sean utilizadas con objetivos terroristas o delictivos.

Medidas Adoptadas a nivel nacional para fortalecer la seguridad de la información y contribuir a la cooperación internacional

Respuestas normativas e institucionales:

En el año 2005, Colombia elaboró la norma ISO-27001, concebida como un sistema de gestión que establecía unos estándares de calidad de seguridad de la información en las entidades nacionales, y propendía por la preservación de las características de Confidencialidad, Integridad y Disponibilidad[1] de la información.

Cuatro años después, el Congreso de la República de Colombia promulgó la Ley 1273 de 2009, por medio de la cual se modificó el Código Penal creando un nuevo bien jurídico tutelado, denominado "De la Protección de la información y de los datos". Modificación que permitió la creación de un marco jurídico nacional que permitiría a las entidades competentes perseguir y judicializar los delitos asociados al uso de las tecnologías de la información.

En este marco, Colombia penalizó entre otras cuestiones, el acceso ilícito, la Interceptación ilícita; los ataques a la integridad de datos; los ataques a la integridad de sistemas; el abuso de dispositivos; la falsificación informática; el fraude informático; la Pornografía infantil; y los delitos contra la propiedad intelectual y derechos afines.

En el año 2011, a través del documento CONPES 3701, Colombia puso en marcha una política y estrategia nacional en materia de Ciberseguridad y Ciberdefensa basada en tres pilares esenciales:

[1] *Confidencialidad*: evitar que la información sea utilizada por individuos o procesos n autorizados. *Integridad:* proteger la precisión y completitud de cualquier cosa que posee valor para una organización. *Disponibilidad*: información accesible y utilizable bajo petición de las entidades autorizadas.

a. La adopción de un marco interinstitucional apropiado para prevenir, coordinar, controlar y generar recomendaciones para afrontar las amenazas y los riesgos que se presenten.
b. El desarrollo de programas de capacitación y formación especializada en seguridad de la información.
c. El fortalecimiento de la legislación nacional en estas materias, así como el fortalecimiento de la cooperación internacional. Y en este marco, adelantar la adhesión de Colombia a los diferentes instrumentos internacionales, es decir, a la Convención de Budapest.

Con el objetivo de desarrollar de manera integral las precitadas líneas estratégicas, Colombia diseñó y puso en marcha cuatro (4) instancias:

1. La *Comisión Intersectorial* encargada de fijar la visión estratégica de la gestión de la información, así como de establecer los lineamientos de política respecto de la gestión de la infraestructura tecnológica información pública y Ciberseguridad y Ciberdefensa;
2. El *Grupo de Respuesta a Emergencias Cibernéticas de Colombia* (colCERT) ente coordinador a nivel nacional en aspectos de Ciberseguridad y Ciberdefensa;
3. El *Comando Conjunto Cibernético de las Fuerzas Militares* (CCOC) que tiene la función de prevenir y contrarrestar toda amenaza o ataque de naturaleza cibernética que afecte los valores e intereses nacionales;
4. y finalmente se implementó el *Centro Cibernético Policial* (CCP), encargado de la Ciberseguridad del territorio colombiano, ofreciendo información, apoyo y protección ante los delitos cibernéticos.

Igualmente, Colombia cuenta con un Marco Jurídico en materia de protección de datos personales, establecido por la Ley 1581 de 2012 y el Decreto 1377 de 2013, por el cual se reglamenta parcialmente esta Ley. Adicionalmente, en la Superintendencia de Industria y Comercio se creó una Delegatura para la Protección de Datos Personas.

Por otra parte, el Ministerio de Tecnologías de la Información y las Comunicaciones diseño e implementó la Estrategia de Gobierno en Línea en la que se incorporan los requerimientos de las entidades en la adopción de Sistemas de Gestión de Seguridad de la Información. Igualmente, desde el año 2008, este Ministerio ha capacitado cerca de 6.300 funcionarios en procesos asociados a gestión de las Tecnologías de la Información.
Finalmente, es importante mencionar que en materia de capacidades se está avanzando en la identificación de la infraestructura crítica nacional (aquella que en caso e ser afectada tiene el potencial de generar pérdidas de vidas humanas, económicas o de gobernabilidad en el país) con miras a mantener la seguridad en materia cibernética de estos lugares.

<u>Cooperación Internacional:</u>

En el año 2013, Colombia solicitó formalmente la adhesión del país al Convenio de Europa sobre Cibercriminalidad, el cual establece los principios del acuerdo internacional sobre Seguridad Cibernética y la sanción de los delitos de esta naturaleza, y cuyo principal objetivo radica en proteger a la sociedad de la Ciberdelincuencia a través del establecimiento de una legislación oportuna y de la cooperación internacional.

Adicionalmente, en el año 2012 Colombia se unió a un Convenio Multilateral con el Foro Económico Mundial, denominado "Alianza para la Resiliencia Cibernética", dirigido a identificar y abordar los riesgos sistemáticos globales derivados de la conectividad, cada vez mayor, entre las personas, los procesos y los objetos.

Por otro lado, la Secretaría del Comité Interamericano contra el Terrorismo (CICTE) de la OEA, ha establecido un enfoque integral en la construcción de capacidades en materia de Ciberseguridad entre los

Estados Miembros. El principal logro de la Secretaría ha sido el establecimiento de grupos nacionales de "alerta, vigilancia y prevención", también conocidos como "Equipos de Respuesta a Incidentes", que cuentan con el mandato y la capacidad de responder ante crisis, incidentes y amenazas a la seguridad cibernética.

Bajo este marco y gracias a la Cooperación del CICTE, Colombia ha desarrollado grupos nacionales de "alerta, vigilancia y prevención" que contribuyen al desarrollo de Estrategias Nacionales sobre Ciberseguridad. Igualmente, ha participado en Talleres, cursos y Congresos sobre el manejo de incidentes relacionados con la Seguridad de la Información y el Delito Cibernético.

Finalmente, cabe mencionar que el país ha suscrito acuerdos con empresas y organizaciones internacionales pertenecientes a la industria de la información y las comunicaciones, dentro de los que se destacan el acuerdo con Microsoft en función de acceder a instancias como el "Cybercrime Center" y a otros programas de Ciberseguridad; y el acuerdo con la Organización "Antipishing Working Group" con el fin de hacer parte de la coalición de autoridades legales, empresas de la industria y entidades de gobierno a nivel mundial que trabajan para contar con mecanismos de alarma y respuesta a incidentes cibernéticos más eficientes.

Medidas internacionales para fortalecer la seguridad de la información

La ciberseguridad no es un problema exclusivo del Gobierno, ni puede resolverlo sólo, se requiere el concurso de otros actores – la academia, la industria y la sociedad civil – para afrontar de manera efectiva los riesgos asociados al uso cada vez más intensivo de las Tecnologías de la Información y las Comunicaciones en todos los ámbitos.

Bajo este marco, para Colombia, con miras a fortalecer la seguridad de la información internacional a escala mundial, es importante que la comunidad internacional:

- Busque mecanismos para crear una mayor conciencia en la sociedad, en los mandatarios y en las entidades de cada Estado, sobre la necesidad de generar una cultura de Seguridad de la Información y la importancia de la cooperación internacional en la lucha contra el delito cibernético.

- Promueva la obligación de los Estados de generar estrategias encaminadas a fortalecer las capacidades nacionales en materia de Ciberseguridad y Ciberdefensa.

- Exhorte a los Estados a identificar sus infraestructuras críticas y establecer un programa específico para mejorar su seguridad y resilencia.

- Incentive la adecuación de los marcos normativos nacionales a los instrumentos internacionales existentes en materia de Ciberseguridad. Una mayor armonización normativa entre los países facilita el establecimiento de canales de cooperación en materia de prevención, investigación, y judicialización del Delito Cibernético entre los Estados.

  Esta labor de armonización debe contemplar el fomento de la tipificación de los delitos asociados al uso de las tecnologías, así como el establecimiento de reglas claras sobre jurisdicción y competencia para el enjuiciamiento.

- Promueva el establecimiento de obligaciones para los Estados y las Entidades Nacionales, públicas y privadas, respecto a la preservación de los registros de naturaleza informática, con el fin de que estos puedan ser utilizados durante un proceso de investigación y judicialización.

- Elabore un glosario de términos informáticos inherentes a la Ciberdelincuencia, que por lo general, son desconocidos por los operadores del sistema de justicia penal, para asegurar la confidencialidad e integridad de los sistemas, redes y datos informáticos.

- Promueva el intercambio de experiencias y buenas prácticas en materia de Ciberdefensa y Ciberseguridad, así como el establecimiento de redes de formación especializada en esta materia.

- Exhorte a los Estados a ser partes de las redes de alerta sobre incidentes cibernéticos.