Lineamientos Estratégicos para la Protección de Infraestructuras de Información Críticas (PI2C) en Argentina.

Autores:

Juan Manuel **Ramon Mosso,** Bachuss, Sarmiento 537 PB B, Rosario {jmanuel@bacchuss.biz}

Dante **Moreno**, Comisión de Gobierno Electrónico del Consejo Federal de la Función Pública {DMoreno@lapampa.gov.ar}

Marisa **Voragini**, Universidad Nacional de la Pampa {marisa_v2000@yahoo.com.ar}

RESUMEN

Las TIC se han convertido en una parte fundamental de la sociedad moderna. Las infraestructuras de información crítica son aquellas infraestructuras soportadas por TIC sobre las cuales se sustentan diferentes procesos que garantizan el desarrollo social y económico de la Nación. Este tipo de infraestructuras esta sometida a niveles de riesgo de seguridad producto de errores, ataques o desastres naturales los cuales deben ser mitigados. En el peor de los casos, las consecuencias de un incidente de seguridad en infraestructuras criticas poseen el potencial de impactar directamente en la vida de las personas llevando a la consumación de daños irreparables.

La protección de las infraestructuras críticas debe involucrar a los sectores Público y Privado con el objetivo de alcanzar una solución consolidada que resulte aplicable tanto al entorno nacional como al multinacional. Todos los emprendimientos en este sentido apuntan al desarrollo de recursos humanos, metodologías, tecnologías, regulaciones y legislación adecuados para cada caso. Es importante destacar finalmente que aunque la solución al problema de protección involucra necesariamente a todos los actores de la sociedad, el responsable final es el estado Nacional.

Introducción

El presenta trabajo describe el problema de Protección de Infraestructuras de Información Críticas y su abordaje desde la perspectiva de la planificación estratégica que debería afrontar y promover la Administración Pública Nacional en Argentina por medio de la definición de lineamientos generales.

Se entiende por Infraestructuras Críticas (IC) al conjunto de recursos sobre los cuales se soportan diferentes procesos que resultan esenciales para el normal desarrollo de la vida de los ciudadanos de una nación. Estos recursos conforman sistemas sobre los cuales se afianzan el gobierno, la economía, la salud, la logística, etc. Las Infraestructura de Información Crítica (I2C) hacen referencia a los sistemas vinculados a IC basados en TIC. Dos ejemplos claros de I2C lo conforman los diferentes sistemas vinculados al Gobierno Electrónico para el sector Público, y las compañías de Telecomunicaciones para el sector Privado.

Como resultado de la cada vez mayor dependencia en la utilización de TIC en todos los procesos de la sociedad moderna, el nivel de riesgo de seguridad asociado a este tipo de escenario se ve incrementado. Este incremento obedece a la cada vez mayor cantidad de vulnerabilidades y amenazas de las cuales son sujeto los diferentes sistemas. Esta problemática requiere de esquemas adecuados de tratamiento de riesgo y de esquemas de vinculación, comunicación, y transferencia efectivos. La Protección de Infraestructura de Información Crítica (PI2C) contempla al conjunto de subsistemas destinados a garantizar la seguridad de los diferentes recursos y procesos vinculados a la I2C. La PI2C se basa en un conjunto de leyes, personas, recursos físicos, sistemas de comunicación e información, normas y procedimientos, de carácter indispensables para la vida de la nación, en base a los cuales se logra garantizar la continuidad de las operaciones aún en caso de desastres. Si bien el problema de PI2C trasciende cualquier ámbito ya que interesa tanto al sector Público como al Privado, es el Gobierno Nacional el que tiene la obligación de avanzar en su tratamiento. Es este el responsable de definir políticas de desarrollo de la sociedad de la información en función de valores propios y del aporte de los medios necesarios para ello, y es en este contexto que la PI2C se vuelve un recurso insustituible que permite alcanzar los objetivos de desarrollo. El éxito de cualquier estrategia que aborde el problema de PI2C debe basarse en la colaboración entre todos los sectores de la sociedad por medio de la generación de leyes, de la modernización de los instrumentos jurídicos, y de la investigación y del desarrollo tecnológico, con el objetivo final de fomentar una cultura de la seguridad.

Relevancia para el Interés Público

La relevancia para el interés público está dada por el carácter significativo que tienen las I2C como soporte fundamental de diferentes procesos que garantizan el normal funcionamiento de la nación y de la sociedad. Si bien estos procesos alcanzan tanto al sector Privado como al Público, es este último el que posee la responsabilidad final y por lo tanto la obligación de administrar y coordinar los medios y recursos necesarios que permitan avanzar en la materialización de una estrategia coherente de PI2C.

Indicadores objetivos de la relevancia que tiene la problemática en el contexto mundial pueden verse en países líderes como EE.UU., Inglaterra, Alemania y aún en Brasil, entre otros. En cuanto a nuestro país, ha sido llevado adelante el Primer Congreso Internacional de Protección de Infraestructuras Críticas de la República Argentina (CIPIC) desarrollado en Marzo de 2011 en la Universidad Argentina de la Empresa (UADE), evento que contó con la participación de expertos nacionales e internacionales, así como autoridades y empresarios del sector. En el mismo, el Subsecretario de Tecnologías de Gestión de la Jefatura de Gabinete de Ministros de la Nación, Eduardo Thill**,** señaló la necesidad de institucionalizar la protección de infraestructuras críticas en nuestro país, necesarias para la provisión de servicios esenciales. “Tenemos como ejemplo el terrible efecto de los desastres naturales sobre los servicios públicos, caso Japón y Chile. Es necesario tener respuesta para garantizar la continuidad de los servicios públicos y entender los riesgos de las infraestructuras críticas, para eso tenemos que trabajar colaborativamente el sector público, el sector privado y la sociedad civil mirando el bien común [1]”. Otra exposición de la relevancia del tema fue la presentación de "Experiencias en la Protección de recursos Informáticos y Tecnológicos en el Sector Público en el Modelo Español de Atención e Infraestructura Crítica" celebrada en los "10 AÑOS de ArCERT" en 2009 [2]. Además, en la Memoria 2010 de Gestión de ONTI se informa sobre el planteo de una serie muy acotada de objetivos y logros en el contexto de PIC [3]. El grado de desarrollo internacional del que es sujeto la PI2C y la serie de iniciativas nacionales mencionadas arriba muestran que es relevante, oportuno y necesario avanzar en la temática en Argentina mediante el desarrollo de un planeamiento estratégico por medio del cual puedan articularse políticas públicas, legislación, colaboración internacional, formación de RR:HH, investigación, y tecnologías.

Análisis

Definir con precisión el concepto de PI2C requiere de una serie de conceptos que deben ser abordados previo al avance en el análisis de la problemática.

Infraestructuras de Información Críticas (I2C)

Una IC conforma un sistema complejo sobre el cual se soportan diferentes procesos que resultan esenciales para el normal desarrollo de la vida de los ciudadanos de una Nación. Este tipo de sistema es soportado por un conjunto de servicios de carácter crítico sobre los cuales se afianzan el gobierno, la sociedad y la economía. Una característica relevante de los sistemas de IC es que trascienden cualquier ámbito ya que interesan tanto al sector Público como al Privado. En este sentido puede decirse que un sistema de IC esta conformado por un conjunto de recursos de carácter Público-Privado que permite llevar adelante las operaciones cotidianas en el contexto apropiado. A continuación se presentan algunos ejemplos de sectores vinculados a las IC en el mundo:

- Sistemas de la Administración Pública y Sistemas Militares,
- Sistemas de Telecomunicaciones,
- Sistemas Energéticos,
- Sistema Financiero y Bancario,
- Sistemas de Transporte, Logística Alimentaria, y Sistemas de Agua,
- Sistemas de Salud y Servicios de Emergencias, Sistemas de Manejo de Crisis, etc.

Las TIC sirven de sustento para el desarrollo económico y social de las naciones debido a sus cualidades de rapidez, manejo de grandes volúmenes de información, capacidad de procesamiento de datos, efectividad de los procesos y procedimientos, y por la velocidad en la transmisión, entre otras. Si bien el contexto de aplicación tradicional lo constituyó el sector Privado, las diferentes iniciativas vinculadas a Gobierno Electrónico hacen que su aplicación sea igual de importante para el sector Público, siendo ya algunos de los sistemas de información de Argentina de carácter crítico para las tareas de administración, tal es el caso de los sistemas de información de ANSES, AFIP, entre otros.

Las I2C son IC sustentadas en TIC. Por su naturaleza, al igual que las áreas de seguridad de la información en las empresas, las I2C resultan transversales al resto de las IC ya que proveen diferentes servicios y recursos a todos los sectores. En algunos casos, las IC conforman I2C en si mismas. Un ejemplo claro de esto lo conforma el Sistemas de Telecomunicaciones que alcanzan a todos los recursos vinculados con conmutación de tráfico de voz y datos, encaminamiento y sistemas de información que soportan las telecomunicaciones, Internet, comunicaciones de emergencia y seguridad, transporte de transacciones financieras, sistemas de manejo de crisis, comunicaciones militares, etc. Las I2C debe ser pensadas como un conjunto de servicios que permiten crear y generar valor añadido (comercio electrónico, gobierno electrónico, teletrabajo, educación a distancia, comando y control, procesos de control distribuido, etc.) con independencia de las tecnologías, impulsando la creación, la disponibilidad y utilización de estos en un contexto abierto basado en redes.

Como resultado cada vez mayor dependencia en TIC de los sistemas de IC y de la mayor interconectividad e interdependencia entre estos, se genera un aumento sensible en los niveles de exposición debido a la existencia de vulnerabilidades y amenazas [4] asociadas a los diferentes subsistemas y al elevado costo de adquisición, operación y mantenimiento de esquemas adecuados de gestión de riesgos de seguridad, especialmente en los casos en los que se utiliza Internet como componente de infraestructura. Un ejemplo de la problemática asociada a la seguridad de las infraestructuras de TIC puede verse en [5].

Protección de Infraestructuras de Información Crítica (PI2C)

La PI2C contempla al conjunto de subsistemas destinados a garantizar la seguridad de los diferentes servicios vinculados a la I2C, sus recursos y procesos. La PI2C se basa en un conjunto de leyes, personas, recursos físicos, sistemas de comunicación e información, normas y procedimientos de carácter indispensables para la Nación, en base a los cuales se logra garantizar la continuidad de las operaciones de los sistemas vinculados a la I2C aún en casos de desastre. Las I2C pueden ser sujeto de errores involuntarios, de desastres naturales (huracanes, tornados, terremotos, inundaciones, etc.), de accidentes (interrupciones, nucleares, radiológicos, biológicos o sustancias químicas), o de ataques deliberados causados por personas o naciones (terroristas, criminales, hackers) con intereses contrapuestos a los de una organización.

Desde el punto de vista estratégico, la PI2C cumple sus objetivos en base a los siguientes principios:

- Principio 1 “Seguridad Física”: proteger los activos físicos de carácter crítico.
- Principio 2 “Seguridad Lógica”: proteger los diferentes activos de información y comunicaciones.
- Principio 3 “Colaboración”: perspectiva global e integradora para ofrecer un frente unificado.
- Principio 4 “Aprendizaje”: aporte de conocimiento, y transformación de este en estrategia.

Toda situación que comprometa la seguridad de la I2C posee el potencial de afectar de manera directa a la sociedad, principalmente en los aspectos políticos, sociales y económicos, provocando en algunos casos situaciones de pánico y temor por los daños causados. Debido a su carácter crítico, es de esperar que los recursos vinculados a las I2C no estén aislados entre si de tal modo que pueda garantizarse su continuidad en situaciones de desastre. Para esto deben contemplarse arquitecturas de interconexión y servicios redundantes a escala nacional y multinacional, dependiendo de otras infraestructuras. En términos prácticos, la PI2C apunta a reducir la probabilidad de materialización de las amenazas, limitar las consecuencias de los ataques y los problemas de funcionamiento, y finalmente permitir la vuelta a la normalidad tras la ocurrencia de un siniestro, a un costo aceptable y en un plazo razonable.

Los Sectores Público y Privado en el Contexto de PI2C

Como ha sido mencionado arriba, la PI2C involucra a dos sectores: *el Público y el Privado*. El sector Privado está conformado por aquellas entidades que no están controladas por el Estado (empresas nacionales, corporaciones transnacionales y organizaciones no gubernamentales). El problema de protección en este tipo de organizaciones se reduce a la seguridad de sus activos de información y servicios con la meta de preservar la toma de utilidades en el tiempo. Por otro lado, el sector Público está constituido por el gobierno en todos sus niveles y por corporaciones e instituciones controladas por el estado (departamentos, ministerios, agencias, consulados, etc.) [6], siendo su objetivo esencial el de la preservación de continuidad de todos los recursos y servicios necesarios para la Nación y el crecimiento y mejora de la calidad de vida de los ciudadanos en su conjunto.

Pese a que en primera instancia las metas de protección de ambos sectores parecen no tener puntos en común, nada mas alejado que esto en la realidad. Como muestra la experiencia de los EE.UU., especialmente en la etapa posterior al 11/9, la seguridad de un sector no puede ser alcanzada sin la colaboración del otro. Esto es especialmente significativo para el caso del sector Público el cual requiere de la participación y coordinación de acciones y recursos con el sector Privado, con lo que este último se vuelve un factor clave. El Estado Nacional es el responsable final de la PI2C por medio de su poder económico, político y militar, para lo cuál requiere de la colaboración de agencias de inteligencia y del sector Privado. Compete a los Estados la definición de una verdadera política de desarrollo de la sociedad de la información en función de sus valores y del aporte de los medios necesarios para ello. En este contexto, la PI2C se vuelve un recurso insustituible que permite alcanzar los objetivos de desarrollo social y económico.

Riesgo de Seguridad en I2C

Se entiende por riesgo de seguridad a la probabilidad de que suceda un evento con impacto negativo. Por un lado, en su concepción mas simple, el riesgo puede ser pensado como una función del valor de los activos y del factor de exposición de los mismos, factor que depende esencialmente del número de vulnerabilidades y amenazas presentes. Por otro lado, el manejo del riesgo involucra la implementación de medidas en planes de corto, mediano y largo plazo destinadas a proteger las I2C. Las amenazas contra las I2C toman especial relevancia en la actualidad ya que permiten el desarrollo de conflictos por vías alternativas a la confrontación militar o política directa. Según expone Michael A. Vatis [7] este tipo de amenazas puede surgir de países o ciudadanos extranjeros, pero también de usuarios corporativos o domésticos del interior con el potencial de seleccionar como objetivos diferentes componentes de infraestructura con motivaciones militares, políticas, religiosas, espionaje, e incluso por entretenimiento.

PI2C en el Contexto de Defensa Nacional

Basados en el Preámbulo de la Constitución Argentina: "... *con el objeto de constituir la unión nacional, afianzar la justicia, consolidar la paz interior, proveer a la defensa común, promover el bienestar general, y asegurar los beneficios de la libertad* " [10], y considerando los posibles escenarios de crisis generados por la afectación de IC por errores, omisiones o ataques deliberados, cualquiera sea su naturaleza, la PI2C permite la consolidación de aspectos de resiliencia de las I2C que resultan un factor crítico para el mantenimiento de los derechos y garantías de los ciudadanos los cuales sirven de soporte para el mantenimiento de la seguridad, de la estabilidad, y de la paz de la Nación.

Los ataques contra las IC pueden generar alteraciones serias e incluso interrupciones en el funcionamiento de las estructuras de Gobierno y de Negocios. Estos poseen además el potencial de disparar efectos en cascada que trasciendan los objetivos originales y se extiendan a otras infraestructuras lo que puede derivar en catástrofes en términos de pérdida de vidas humanas, de la salud del medio ambiente, de la propiedad, con un profundo impacto en la moral y en la integridad de la Nación. Este tipo de escenario se amplifica si se considera el uso de componentes de IC como armas de destrucción masiva.

Consideraciones Generales sobre Legislación

Antes de comenzar es importante mencionar que en Argentina no existe actualmente legislación concreta en relación a PI2C. La creación de un marco jurídico en relación a esta temática deberá permitir avanzar en aspectos vinculados con garantías de integridad, confidencialidad y disponibilidad de los diferentes servicios vinculados a I2C. Es importante considerar que los aspectos jurídicos deberían acompañar a la ciencia, a la tecnología, y al desarrollo humano, y no ser impuestos desde posiciones duras, sin un previo análisis de la problemática y de su impacto en la sociedad.

Es necesario que los países comprendan la necesidad de crear una conciencia y una cultura asociados a la seguridad de la información que permita entender las implicancias relacionadas a las amenazas con el objetivo de protegerlas legalmente estableciendo funciones legislativas legítimas. Debido al carácter distribuido de muchas de las componentes vinculados a las I2C, e incluso a la utilización de recursos de infraestructura compartidos con el resto del mundo como es el caso de Internet, se requiere la cooperación internacional para facilitar la creación de un marco legal para combatir el crimen. Las medidas legales, técnicas, procesales, estructurales y orgánicas necesitan ser emprendidas a nivel nacional, regional y multinacional por lo que cada nación deberá colaborar estrechamente con sus socios estratégicos en el abordaje del problema para identificar los actuales desafíos, considerando las amenazas futuras, y proponiendo estrategias globales. Esta responsabilidad compartida requiere de acciones coordinadas para la prevención, respuesta y recuperación de las funciones y actividades tras un incidente que afecte a los sectores Público o Privado, e incluso a los mismos ciudadanos [8]. Un claro ejemplo de este tipo de acciones coordinadas lo conforma la Cumbre Mundial sobre la Sociedad de la Información [9] en la que los líderes mundiales allí designaron a la Unión Internacional de Telecomunicación (ITU) como el organismo idóneo para la creación de normas de seguridad en la utilización de las TIC, y para el desarrollo de un conjunto de herramientas legislativas que ayudan a establecer normas legales en el mundo relacionadas con la ciberseguridad. Como resultado del trabajo realizado se crea la Agenda Global de Cyberseguridad (GCA) con la colaboración de la ITU, de gobiernos, industrias, organizaciones regionales, y de instituciones académicas y de investigación. La GCA constituye un marco de alcance mundial con el fin de coordinar respuestas internacionales a los retos planteados por la seguridad en infraestructuras basadas en TIC.

Desarrollar una legislación adecuada dentro de un marco jurídico determinado resulta un factor esencial para combatir el ciberdelito. Se requiere la elaboración de leyes penales que aborden la problemática de actos criminales como el fraude informático, la denegación de servicios, el acceso ilegal o no autorizado, las violaciones del derecho de la propiedad intelectual, la usurpación de identidad, y la pornografía infantil entre otros. Debido a las características especiales de los delitos cometidos en base a TIC, se hace necesario el desarrollo de instrumentos jurídicos que faciliten la investigación de este tipo de incidentes. Como se especificó anteriormente, las amenazas pueden originarse en cualquier lugar del mundo y los ataques pueden quedar enmascarados permitiéndole a los instigadores cubrir su verdadera identidad. No todos los sistemas jurídicos del mundo reconocen los potenciales abusos de las nuevas tecnologías por lo que no incluyen las modificaciones necesarias en las actuales leyes penales. Es por esto que resulta fundamentar comprender la creciente complejidad introducida por las TIC y trabajar para realizar los ajustes jurídicos pertinentes.

En nuestro país la Ley 25.326 de Protección de Datos Personales sancionada en el año 2000 ofrece un marco legal para la protección integral de los datos de las personas (Privacidad) y aplica tanto al sector Público como al Privado. Por otro lado, la Ley 26.388 de Delitos Informáticos establece una reforma del Código Penal por medio de la derogación y modificación de algunos incisos introducidas por el Art. 32 de la Ley 25.326 al Código Penal. Esta ley aplica penas a delitos como la violación de secretos y de la privacidad, donde se contemplan acciones tales como acceso indebido a sistemas y redes, apropiación y publicación de una comunicación electrónica, etc. [11]. Para adaptar el sistema jurídico a los nuevos desafíos impuestos por las PI2C deberían considerarse los tres siguientes hitos importantes: *1.) Reconocimiento de la actividad delictiva asociada a las nuevas tecnologías, 2.) Identificación de los problemas en el Código Penal, y 3.) Redacción de una nueva legislación.*

Políticas de PI2C en el Mundo: Caso EEUU

En EE.UU. las IC son definidas en base a conceptos establecidos en el Acto Patriota del año 2001 [12], trabajo que lleva a la creación de la Directiva Presidencial 7 (HSPD-7, 2003) del Departamentp de Seguridad Interna (DHS, ó "Department of Homeland Security") en la que se reconocen 18 IC y se definen los roles y las responsabilidades asociados a la protección de las mismas. El Plan Nacional de Protección de IC del 2009 [13] reafirma las definiciones de la HSPD-7, y la estrategia Nacional para la Seguridad Interna reconoce la importancia de la PI2C para la seguridad nacional [14].

Un cambio radical que plantea la problemática de PI2C es que a diferencia de las metodologías de resolución tradicionales de problemas de seguridad en la que intervienen a la cabeza en Gobierno central en conjunto con militares, agencias de inteligencia y oficinas de relaciones externas; la PI2C requiere de acciones coordinadas entre varios sectores. A tal fin, el Gobierno de los EE.UU. ha desarrollado un conjunto de iniciativas y políticas entre las cuales vale destacar:

- *Presidential Commission on Critical Infrastructure Protection* (PCCIP) (Clinton, 1996),
- *Presidential Decision Directives (PDD) 62 and 63* (Clinton, 1998),
- *National Plan for Information Systems Protection* (Clinton, 2000), deriva en el trabajo "Defending America's Cyberspace" [15],
- *Homeland Security Executive Orders (EO1 y EO2)* (Bush, 2001) [16] [17]. Las EO permitieron establecer además el "National Infrastructure Advisory Council" (NIAC),
- *Homeland Security Presidential Directive* (HSPD-7) (Bush, 2003), reemplaza a la PDD63, establece una política nacional para todos los departamentos y agencias federales que permita identificar y proteger IC de ataques terroristas,
- *National Strategy for Homeland Security* (Bush, 2002 y 2007) [18] [19],
- *National Strategy to Secure Cyberspace* (NSSC) (2003) [20],
- *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* [21],
- *National Infrastructure Protection Plan (NIPP) y Sector-Specific Plans (SSP) (2006)* [22] [23], y
- *National Strategy for Information-Sharing* [24].

Desde la perspectiva organizativa, tradicionalmente la responsabilidad de coordinar temas de PIC estaba a cargo de la Critical Infrastructure Assurance Office (CIAO) la cual formaba parte del Departamento de Comercio, y del National Infrastructure Protection Center (NIPC) el cuál funcionaba como una división del Federal Bureau of Investigation (FBI). Actualmente la responsabilidad ha sido absorbida por el DHS que es la encargada del Gobierno de coordinar los esfuerzos para la PI2C. A continuación se mencionan las principales agencias públicas soporte de la PI2C:

- *Department of Homeland Security (DHS),*
- *Office of Infrastructure Protection (OIP),*
- *Office for Cybersecurity and Communications (CS&C),*
- *US Department of State (DOS),*
- *Government Accountability Office (GAO),*
- *Department of Defense (DOD),*
- *Computer Crime and Intellectual Property Section(CCIPS, parte del DOJ).*

Abajo se presenta una lista de organizaciones de colaboración Público-Privada:

- *The National Infrastructure Advisory Council (NIAC),*
- *Critical Infrastructure Partnership Advisory Council (CIPAC),*
- *National Security Telecommunications Advisory Committee (NSTAC),*
- *Protected Critical Infrastructure Information Program (PCIIP),*
- *Information Sharing and Analysis Centers (ISACs),*
- *InfraGard,*
- *National Cyber Security Alliance (NCSA),*

- *Partnership for Critical Infrastructure Security (PCIS),*
- *The Cross Sector Cyber Security Working Group (CSCSWG),*
- *Institute for Information Infrastructure Protection (I3P).*

Sistemas de Advertencia Temprana:

- *CERT Coordination Center, Carnegie Mellon University,*
- *US-CERT*
- *National Cyber Alert System,*
- *Federal Bureau of Investigation (FBI) en base a PCCIP,*
- *Information-Sharing and Analysis Centers (ISACs),*
- *OnGuardOnline.gov.*

Leyes y Legislación:

- *Federal Advisory Committee Act (FACA) 1972,*
- *Computer Fraud and Abuse Act (CFAA) 1986,*
- *Homeland Security Act 2002,*
- *Freedom of Information Act (FOIA),*
- *Critical Infrastructure Information Act: Procedures for Handling Critical Infrastructure Information,*
- *The Terrorism Risk Insurance Act 2002.*

Políticas de PI2C en el Mundo: Caso Brasil

Basado en la Conferencia SecGov celebrada en Brasilia en 2006 [25] (esponsorizado por Gabinete de Seguranca Institucional – GSI) en la que se discutió la seguridad de las IC, Brasil estableció siete tópicos que en principio pueden ser considerados IC. Estos tópicos son: *Seguridad Pública, Energía, Finanzas, Sistemas de Transporte, Agua, Salud Pública, Telecomunicaciones, y Terrorismo*. Respecto a la I2C, se reconoció que las principales problemas se relacionaban con las Telecomunicaciones y con Internet por lo que el Ente de Regulación de las Telecomunicaciones, Anatel, fue el encargado de desarrollar una estrategia [26]. Brasil logró avanzar en la comprensión del problema de seguridad en base a una concepción global del tema, donde son necesarias estrategias locales, regionales y globales para una correcta respuesta a las amenazas actuales contra la I2C [27]. Las iniciativas de Brasil en el contexto de PI2C se enfocan en generar confianza en dos aspectos particulares: Internet y Telecomunicaciones. Estos dos aspectos tienen un gran impacto en la sociedad por lo que no pueden ser separados, mas aún, la protección de ambos es altamente interdependiente si se piensa a nivel de redes backbone [28]. Algunas iniciativas relevantes:

- *Comité Directivo de Internet en Brasil* (Comite Gestor da Internet no Brasil – CGI) (1995, 2003, 2004). Formado por el Gobierno, operadores de backbones, ISP, usuarios y por la comunidad académica [29], y
- *Brazilian Electronic Government Program (e-gov)* (2000) [30].

Desde la perspectiva de organización, la PI2C en Brasil depende del Comité Directivo de Internet en Brasil, de las políticas de TIC sustentadas por el Ministerio de Ciencia y Tecnología y del Ministerio de Comunicaciones, y del Centro de Información de Redes. Las cuestiones de seguridad de la información recaen en Gabinete de Seguridad Institucional (Gabinete de Seguranca Institucional – GSI) [31].

Agencias Públicas:

- *Comite Gestor da Seguranca Informacao - CGSI), y*
- *Centro de Información de Redes de Brasil (NIC.br).*

Colaboración Público-Privada:

- *Agencia Nacional de Telecomunicacoes (Anatel), y*
- *Servico Federal de Processamento de Dados (SERPRO).*

Alerta Temprana:

- *Centro de Tratamento de Incidentes de Seguranca em Redes de Computadores da Administracao Publica Federa (CTIR Gov) [32],*
- *CERT.br,*
- *Alianza Brasilera de Honeypots [33],*
- *Rede Nacional de Ensino e Pesquisa (RNP), y*
- *Centro de Atendimento a Incidentes de Seguranca (CAIS).*

En cuanto a la Legislación, en el año 2000 se establece la política de seguridad que debe ser utilizada en el Gobierno y en todos los socios.

- *Código Penal de Brasil,*
- *Leyes de Crímenes Cibernéticos [35], y*
- *Proyecto de Ley de Delitos Informáticos [36].*

Argentina: Situación en el contexto de I2C

Antes de plantear los lineamientos estratégicos elementales para el abordaje de la problemática de la PI2C en Argentina vale hacer una síntesis de la situación y de algunos instrumentos existentes en el país en materia de seguridad de la información y de IC:

- Argentina no cuenta con legislación en materia de PIC ni PI2C,
- Política de Seguridad de la Información para el Sector Público (DA 669/2004 JGM) [37],
- Modelo de Política de Seguridad (ONTI Disp. 006/2005) [38],
- ArCERT (1999) [39],
- No hay estándares técnicos ni manuales de procedimientos de carácter oficial con excepción de un "Manual de Seguridad en Redes" del año 1999 [40],
- ReCoRD (Iniciativa de la Comisión de Gobierno Electrónico (CGE) del Consejo Federal de la Función Pública (COFEFUP)) [41],
- Plan Federal de Gobierno Electrónico (PEFeGE) [42],
- Bases y Lineamiento para una Agenda Digital en Argentina (2008) [43]
- Grupo de Trabajo Multisectorial creado en el ceno de la JGM, particularmente el Ítem b del Artículo 2 del Decreto Nacional 512/09 relacionado con la Agenda Digital [44],
- Carta Iberoamericana de Gobierno Electrónico [45], y
- Resultados del Foro de Telecomunicaciones: "2011 Argentina Conectada" [46], entre otros.

Argentina: Lineamientos Estratégicos para la PI2C

La Visión del presente proyecto consiste en desarrollar un Plan Estratégico de PI2C sustentable que pueda ser implantado a nivel nacional, con estrechos vínculos internacionales, tratando que los sectores Público, Privado y Científico-Académico colaboren a la finalidad de brindar seguridad a la ciudadanía en general y a la vida de la Nación.

La Misión involucra entre otros: *1.) Ofrecer a distintos grupos de clientes, desde el Gobierno y propietarios y operadores de IC, hasta empresas y usuarios domésticos de Internet, protección y seguridad en el uso de las TIC, 2.) Disponer de técnicas y herramientas adecuadas y desarrollar los RRHH, y 3.) Reducir las vulnerabilidades de las infraestructuras críticas de la Nación.*

Los Objetivos del proyecto pueden ser sintetizados como: *1.) Establecer una red nacional que soporte la PI2C, 2.) Lograr vinculación a nivel Internacional y contar con el apoyo y la experiencia de otros países, 3.) Disminuir el número de incidentes en I2C de la Nación, y 4.) Aumentar el nivel de interés de los sectores participantes (público, privado y académico).*

Argentina: Modelo de Procesos para PI2C

Los lineamientos estratégicos plantean la inclusión de un Modelo de Procesos para la PI2C el cual se basa en cuatro actividades fundamentales que establecen un esquema de roles y responsabilidades:

- *Prevención y Alerta Temprana:* desarrollo de tareas de minimización del número de brechas de seguridad por medio de la reducción de vulnerabilidades. Tareas vinculadas a la preparación.
- *Detección:* descubrimiento de nuevas amenazas y formas ataque de la manera mas rápida posible, interacción con CERT, y soporte de detección de intrusos en componentes de I2C.
- *Reacción:* capacidad de respuesta a eventos de seguridad, requiere mecanismos para la identificación y priorización de incidentes, contempla acciones de contención y corrección.
- *Gestión de Crisis:* minimización del impacto de un incidente y reestablecimiento de los sistemas a su estado original, requiere de facilidades de comunicación entre organismos.

Argentina: Modelo de Colaboración

El modelo de colaboración intenta identificar actores en el contexto de PI2C que, en base a sus capacidades existentes, resulten lo mas apto posible para llevar adelante la solución, y conformar un esquema claro de colaboración entre estos en base al modelo de procesos. El organismo responsable de la PI2C deberá disponer de tres equipos de trabajo:

I. *Administración:* conformado por una Agencia de Gobierno que lidere y supervise, requiere de fuertes vínculos con los sectores Público, Privado y Científico-Tecnológico.

II. *Centro de Análisis de Situación:* recolección y análisis de información vinculadas con amenazas, estrecha vinculación con servicios de inteligencia nacionales e internacionales con el objetivo de combatir el cibercrimen a nivel global.

III. *Unidad Técnica de Especialistas:* especialidad en temas referentes a seguridad de la información, generalmente se asigna a CERT que intervienen en caso de incidentes, pero también poseen la capacidad de generar información de vulnerabilidades, procedimientos, etc. Debido a su naturaleza, es recomendable un CERT vinculado al sector Académico.

El éxito de los resultados obtenidos por el Órgano responsable de la PI2C dependerá de la adecuada definición del esquema de funciones de cada uno de sus tres componentes. En la Figura 1 puede verse un esquema general de funciones elementales:

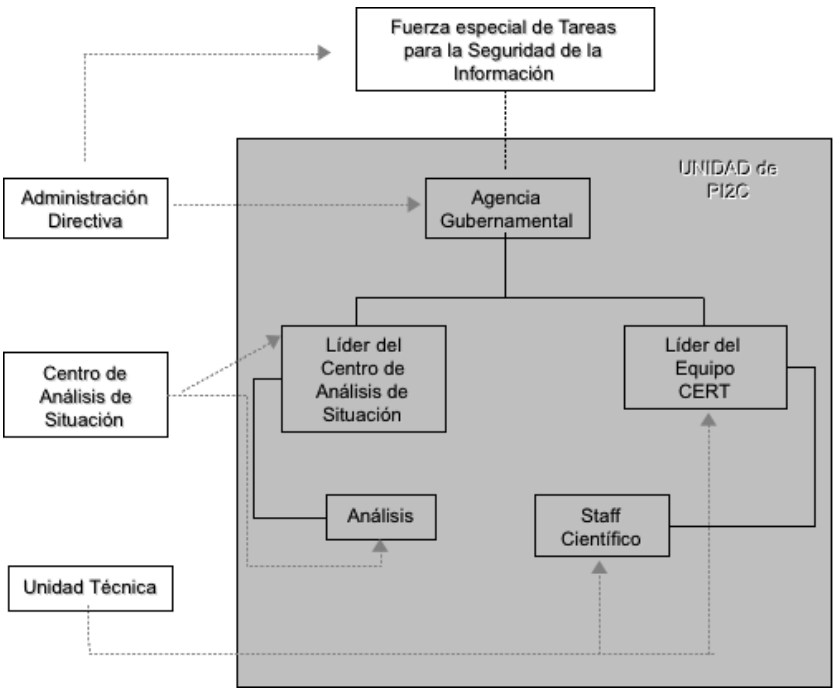

Figura 1. Mapa organizacional de la Unidad PI2C.

La Tabla 1 muestra un resumen de las principales habilidades requeridas para cada función:

Posición	Habilidades requeridas
Líder de la Administración de la Unidad de PI2C	• Experiencia en Seguridad de la información o I2C. • Buenos contactos con quienes deciden políticas. • Habilidad para la comunicación, la administración y las estrategias.
Líder del Centro de Análisis de Situación (Servicio de Inteligencia)	• Conocimiento Legal y Político. • Ser un eslabón con los servicios de Inteligencia. • Experiencia en la persistencia del trabajo.
Líder de la Unidad Técnica (Equipo CERT)	• Extensas habilidades técnicas. • Habilidad para enseñar y comunicar. • Miembro de un CERT Nacional.

Tabla 1. Requerimientos por tipo de responsabilidad.

Argentina: Red de Trabajo para PI2C

Cada una de las tareas llevadas adelante por las diferentes unidades del Órgano de PI2C requiere de contactos específicos dentro de redes nacionales e internacionales (ver esquema general en Figura 2):

- *Administración:* las gran cantidad de tareas administrativas fuerza a la necesidad de contar con buenos contactos en otros organismos públicos que estén involucrados en la PI2C (economía, la política, defensa militar y civil, comunicaciones, salud, etc.). Además se requiere de una cooperación fluida con el sector Privado el cuál en definitiva es el propietario y operador de gran parte de las I2C, resultando fundamental el desarrollo de confianza mutua. Finalmente, deberán preverse mecanismos de colaboración con organismos de PI2C de otros países.
- *Centro de Análisis de Situación:* para llevar adelante el proceso de recolección y análisis de información se debe disponer de contactos consolidados con fuerzas de seguridad como la policía y las fuerzas armadas, y con otras unidades de inteligencia nacionales e internacionales. En este sentido, las fuerzas de seguridad vinculadas con el cibercrimen resultan de gran valor debido a su capacidad de colaboración. Mientras que a nivel estratégico la Administración de PI2C colabora con otros organismos internacionales, el Centro de Análisis lo hace a nivel operativo como por ejemplo en el caso de INTERPOL [47]. Es esencial como soporte legal en casos.
- *Unidad Técnica (CERT):* la tarea técnica de analizar nuevas vulnerabilidades y formas y herramientas de ataque es sumamente demandante por lo que se deberá contar con una red de contactos de expertos en la temática de seguridad de la información de los sectores Privado y Científico-Académico. El contacto con unidades técnicas a nivel internacional es necesario ya que posibilita el tratamiento de eventos de carácter internacional, para esto es recomendable formar parte del Foro para Grupos de Seguridad y Respuesta a Incidentes (FIRST) [48].

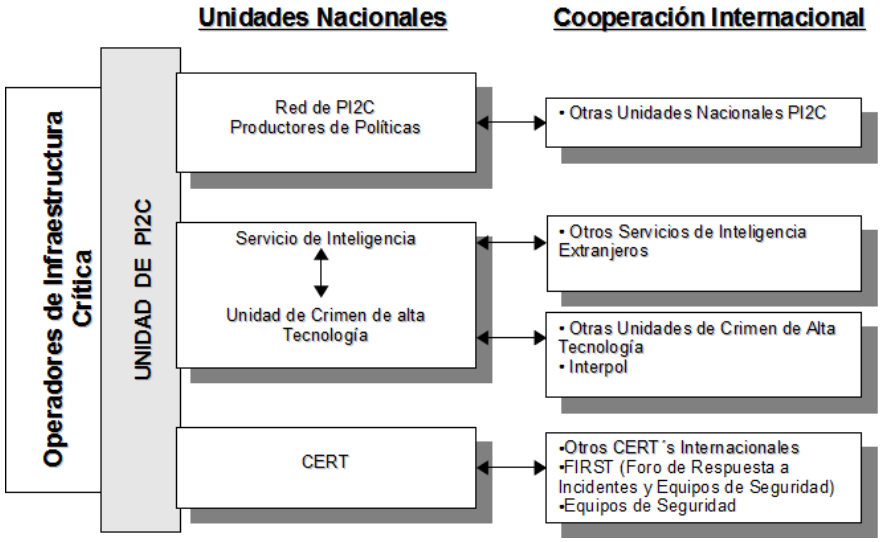

Figura 3. Red de Contactos del Órgano de PI2C.

Argentina: Productos, Servicios y Clientes relacionados con PI2C

Es de vital importancia definir el conjunto de clientes a los cuales servirá el Órgano de PI2C. Existen tres grupos de clientes fundamentales, a saber: *1.) Propietarios y Operadores de I2C (POI2C), 2.) El Estado Nacional, y 3.) Empresas del sector privado, los usuarios domésticos.* Cada uno de estos tres grupos de clientes posee requerimientos especiales de acceso a los diferentes servicios por lo que pueden ser agrupados según el siguiente esquema general:

- *Grupo Cerrado de Clientes (GCC): constituido por propietarios y operadores de I2C, y*
- *Grupo Abierto de Clientes (GAC): involucra al resto de los clientes.*

Grupo Cerrado de Clientes (GCC):

La colaboración con el Órgano de PI2C resulta de interés solo si este es capaz de brindar servicios e información exclusivos, por ejemplo nuevas amenazas y riesgos, ya que en general este tipo de clientes cuenta con recursos y conocimiento especializados en seguridad de la información. Es importante destacar que los productos y servicios dependen a su vez de los mismos clientes por lo que se debe alentar y favorecer la colaboración Público-Privada (CPP). El GCC quedará conformado por POI2C, y debe ser capaz de acomodarse a cambios en el medio por lo que su estructura deberá poder adaptarse a demandas de los diferentes sectores en el futuro.

Debido a que la información es el principal activo sobre el que se trabajará en el modelo de CPP, el intercambio de esta solo se puede lograr si se establece una relación de suma confianza entre las partes, con todos lo problemas que esto presupone [49]. Este factor hace que el tamaño del GCC sea un factor relevante por lo que debe ser de tamaño adecuado y de membresía los mas estable posible para que puedan cultivarse las relaciones personales, base de la confianza [50]. Es recomendable que el GCC sea dividido de tal manera que puedan plasmarse los intereses de cada uno de los sectores intervinientes. En la Figura 4 puede verse un esquema de las relaciones en el GCC el cual contempla aspectos de confidencialidad entre diferentes sectores del GCC.

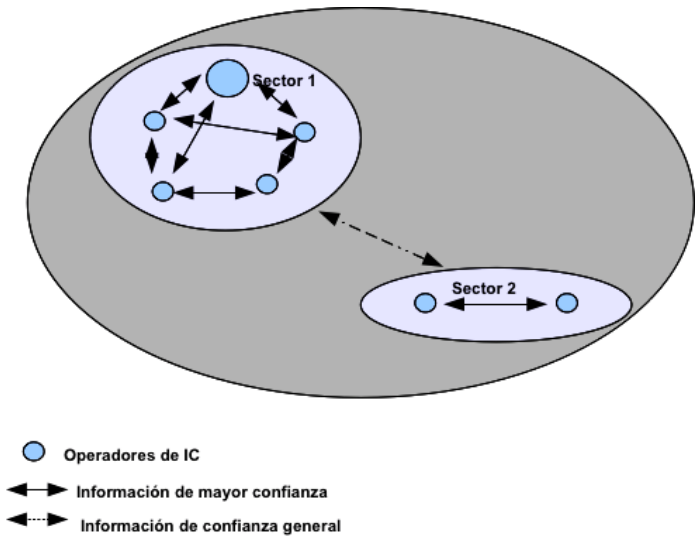

Figura 4. Relaciones de Confianza en el GCC.

El intercambio de información debe ser promovido como principio fundamental para el éxito de la PI2C. Este principio puede verse afectado por varios factores: Primero, por rivalidad, ya que diferentes empresas en el GCC pueden ser competidoras en el mercado. Segundo, el principio afecta de manera directa a cuestiones de seguridad de la información de las compañías. En este punto vale insistir con la necesidad de llevar adelante reuniones acotadas en el número de asistentes, especializadas por tipo de sector, y sobre la constitución de marcos formalizados de cooperación que establezcan entre otros, una Política de Confidencialidad. La legislación afecta también al principio de colaboración ya que en el contexto del GCC, las leyes en general alientan la libre competencia, y en ocasiones prevén instrumento para forzar la liberación de información, por lo que deberá avanzarse también en este sentido.

En cuanto a los productos y servicios para el GCC, el Órgano de PI2C deberá prever: *1.) Prevención, 2.) Asistencia en caso de incidentes, 3.) Generación y/o distribución de información exclusiva, 4.) Seminarios y cursos, y 5.) Ejercicios y simulaciones.*

Grupo Abierto de Clientes (GAC):

La problemática central que se trata de abordar mediante la definición del GAC es la de que cualquier computadora o recurso de TIC vulnerable plantea una amenaza para el resto de los sistemas interconectados de I2C. Los productos y servicios dirigidos al GAC son mas acotados que los dirigidos al GCC, especialmente aquellos relacionados con prevención. Deberá considerarse que los servicios ofrecidos a organismos del sector Público deben contemplar un elevado grado de compromiso debido a la responsabilidad de las acciones llevadas adelante por estos. En este caso, los servicios base deberán ser: *1.) Concientización, 2.) Alertas, y 3.) Asistencia en caso de incidentes.*

Debido a la naturaleza heterogénea y a las diferentes expectativas de los miembros del GAC, el Órgano de PI2C debe establecer claramente su responsabilidad y debe comunicarla al público en general. Este Órgano es visto como una institución del sector Público por lo que debe tener la capacidad de mostrarse como un centro con competencias destacables en la ciencia de seguridad de la información. En este caso, si bien es de gran interés la detección de incidentes vinculados con el GAC, la asistencia no podrá involucrar dedicación por parte del Órgano de PI2C por lo que resultará de valor una buena articulación con las fuerzas de seguridad para poder al menos responder a preguntas técnicas y legales.

En la Tabla 2 pueden verse definiciones generales sobre los GCC y GAC.

	GAC	**GCC**
Miembros	Operadores seleccionados de I2C (Miembros Limitados)	PyMES y ciudadanos en general
Número	2 a 4 representantes de cada miembro	Abierto
Confianza	Fuerte nivel de Confianza	Nivel de Confianza débil
Construcción de Confianza	Alcanza a todo el GCC (reuniones periódicas, redes interactivas) y en particular dentro de cada sector	Medios, Internet, exhibiciones y con la asistencia de socios estratégicos

Tabla 2. Definiciones generales sobre GCC y GAC.

Conclusión y Sugerencias

La PI2C constituye una problemática que debe ser abordada en conjunto por los sectores Público y Privado. Por un lado, el Gobierno Nacional es el responsable final de garantizar la resiliencia de las I2C las cuales conforman un factor crítico para el desarrollo social y económico de la Nación por lo que deberá instrumentar los medio necesarios para llevar adelante una iniciativa adecuada y sustentable. Por otro lado, los propietarios y operadores de I2C asignan recursos privados para dar soporte a problemas de seguridad de sus propios componentes de infraestructura. Alcanzar una solución consolidada al problema de PI2C requiere de esfuerzos conjuntos que permitan desarrollar un frente unificado que permita romper con la fragmentación tradicional existente en esfuerzos de cooperación Público-Privada. El éxito en la conformación y en el funcionamiento de un Órgano de PI2C depende de una correcta definición de los diferentes roles y responsabilidades, del desarrollo y fortalecimiento constante de la estructura y los canales de colaboración, y del establecimiento de relaciones de confianza y cooperación entre los diferentes actores en base a políticas y acuerdos formales. Sin bien la mayoría de los servicios ofrecidos estarán orientados a los propietarios y operadores de I2C, parte de los esfuerzos deberían estar dedicados a las PyMES y a los usuarios domésticos.

En Argentina no existe al momento legislación concreta ni estructuras técnico-científicas que traten la PI2C, solo algunos instrumentos legales establecidos orientados a dar solución a problemáticas particulares y una serie de iniciativas vinculadas principalmente a la ONTI y al COFEFUP en el contexto de Gobierno Electrónico.

En base a lo expuesto en el presente trabajo y a la relevancia de la temática para el desarrollo Nacional se sugiere que se ponga en consideración el inicio de un estudio de factibilidad para lograr desarrollar y afianzar un Órgano de PI2C en Argentina.

Referencias

[1.] http://www.agendadigital.ar/index.php/component/content/article/6-principal/67-las-infraestructuras-criticas-en-argentina

[2.] http://www.arcert.gov.ar/10_aniv/programa.html

[3.] Informe de Gestión 2010 - Subsecretaría de Tecnologías de Gestión

[4.] Loscocco P.A., Smalley S.D., Muckelbauer P.A., Taylor R.C., Turner S.J., Farrell J.F.: "The Flawed Assumption of Security in Modern Computing Environments". In Proceedings of the 21st National Information Systems Security Conference The Inevitability of Failure, 1998.

[5.] Adams J.: "A private-sector solution to cybercrime vulnerabilities". In Proceedings of the 1998 Conference on Defending Cyberspace, Bethesda, MD, September 23-25 1998.

[6.] Introduction to Critical Infrastructure Assurance - What is CIIP.pdf

[7.] "Critical Information Infrastructure Protection: The Threat is Real" U.S Senate, Subcommittee on Technology, Terrorism, and Goverment Information, Committee on the Judiciary, DC, 1999.

[8.] "ITU Toolkit for Cybercrime Legislation". ICT Applications and Cybersecurity Division. Policies and Strategies Department. ITU Telecommunication Development Sector. Draft Rev. 2010.

[9.] Cumbre Mundial sobre la Sociedad de la Información. http://www.itu.int/wsis/index-es.html.

[10.] Constitución de la Nación Argentina. 1994.

[11.] Ley de Delitos Informáticos http://infoleg.mecon.gov.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

[12.] USA Patrot Act http://www.epic.org/privacy/terrorism/hr3162.html.

[13.] National Infrastructure Protection Plan. http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

[14.] National Strategy for Homeland Security. http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf

[15.] William J. Clinton. “Defending America’s Cyberspace: National Plan for Information Systems Protection Version 1.0”, An Invitation to a Dialogue, (Washington, 2000).

[16.] George W. Bush. “Executive Order 13228”, Establishing the Office of Homeland Security and the Homeland Security Council (Washington, 8 October 2001). http://www.fas.org/irp/offdocs/eo/eo-13228.htm.

[17.] George W. Bush. “Executive Order 13231”, Critical Infrastructure Protection in the Information Age”, Washington, 16 October 2001. http://www.fas.org/irp/offdocs/eo/eo-13231.htm.

[18.] Office of Homeland Security. “National Strategy for Homeland Security”, (Washington, July 2002). http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.

[19.] National Strategy for Homeland Security 2007.

[20.] The White House. “National Strategy to Secure Cyberspace”, (Washington, 2003). http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.

[21.] National Strategy for Physical Protection of Critical Infrastructure and Key Assets. http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

[22.] National Infrastructure Protection Plan (NIPP). http://www.dhs.gov/files/programs/editorial_0827.shtm

[23.] Department of Homeland Security. “Information Technology: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan”, 2007.

[24.] National Strategy for Information-Sharing. http://www.fas.org/sgp/library/infoshare.pdf

[25.] http://www.secgov.com.br.

[26.] Regina Maria De Felice Souza. “Critical telecommunication infrastructure project”. In: InfoCitel Electronic Bulletin no. 33, March 2007. http://www.citel.oas.org/newsletter/2007/marzo/infraestructura_i.asp

[27.] 2nd COLAIS. “2nd Latin American Conference for Security Incident Response”. 2006. http://www.rnp.br/en/events/colaris/.

[28.] Shaw R.: “Creating Trust in Critical Network Infrastructures: The Case of Brasil”. ITU Workshop on Creating Trust in Critical Network Infrastructures, 2002.

[29.] El Comite de Dirección de Internet en Brasil fué creado por medio del decreto interminiterial no. 147 en 1995, y modificado en 2003 por decreto presidencial no. 4829. Desde 2004 la sociedad civil participa directamente en deliberaciones relacionadas con la temática.

[30.] http://www.governoeletronico.gov.br.

[31.] http://www.presidencia.gov.br/estrutura_presidencia/gsi/sobre.

[32.] http://www.ctir.gov.br

[33.] http://www.honeypots-alliance.org.br.

[34.] Goodman M. and Brenner S.W.: “The Emerging Consensus on Criminal Conduct in Cyberspace”. In: UCLA Journal of Law and Technology, Vol. 6, issue 1, 2002.

[35.] Azeredo E.: “Cybercrime legislation in Brasil”, 2007.

[36.] Senado Federal, Gabinete do Senador Eduardo Azeredo. Octopus Interface Conference – cooperation against Cybercrime, 2007.

[37.] Política de Seguridad de la Información. Decisión Administrativa 669/2004 de la JGM Argentina.

[38.] Modelo de Política de Seguridad de la Información de la ONTI. http://www.arcert.gov.ar/politica/PSI_Modelo-v1_200507.pdf

[39.] http://www.arcert.gov.ar/

[40.] Manual de Seguridad en Redes, 1999.

[41.] http://www.sgp.gov.ar%2Fcontenidos%2Fcofefup%2Fdocumentos%2Fdocs%2FComision_Gobierno_Electronico-Manual_RECORD.pdf

[42.] Plan Federal de Gobierno Electrónico (PEFeGE). http://www.cofefup.misiones.gov.ar/index.php?option=com_docman&task=doc_download&gid=31&Itemid=6

[43.] Bases y Lineamiento para una Agenda Digital en Argentina. Documento desarrollado por CABASE, CESSI, CICOMRA Y RODAR, Agosto 2008. http://www.cofefup.misiones.gov.ar/index.php?option=com_docman&task=doc_download&gid=4

[44.] Decreto Nacional 512/09. http://www.cofefup.misiones.gov.ar/index.php?option=com_docman&task=doc_download&gid=6&Itemid=6

[45.] Carta Iberoamericana de Gobierno Electrónico. http://www.cofefup.misiones.gov.ar/index.php?option=com_docman&task=doc_download&gid=2&Itemid=6

[46.] Foro de Telecomunicaciones: "2011 Argentina Conectada". http:// www.minplan.gov.ar%2Fadjuntos%2F128%2FProgramaForoTelecomunicaciones2011.pdf

[47.] Interpol Information Technology Crime http://www.interpol.int/Public/TechnologyCrime/default.asp.

[48.] Forum for Incident Response and Security Teams (FIRST). http://www.first.org.

[49.] Prieto, D.B.: Information Sharing with the Private Sector: History, Challenges, Innovation, and Prospects. Cambridge University Press, 2006.

[50.] United States Government Accountability Office (GAO): Information Sharing: Practices That Can Benefit Critical Infrastructure Protection, p. 7. 2001.