UNIVERSIDAD NACIONAL DE LA PAMPA

FACULTAD DE INGENIERÍA

DISEÑO DE UN PLAN ESTRATÉGICO PARA LA PROTECCIÓN DE LA INFRAESTRUCTURA DE INFORMACIÓN CRÍTICA EN LA ARGENTINA

Tesis presentada para cumplir con los requisitos finales para la obtención del título de Ingeniería en Sistemas

Autor: Marisa Verónica Voragini

Tutor: Prof. Ing. Juan Manuel Ramón Mosso

Junio del 2011

• INDICE GENERAL

CAPÍTULO 1

1 INTRODUCCIÓN

La Infraestructura de Información Crítica (I2C) de una nación está conformada por diversos activos físicos y lógicos que sirven de soporte a las tecnologías de la información y la comunicación (TIC) las cuales posibilitan una mejora del funcionamiento en las distintas áreas de la sociedad y presentan un valor superior estratégico para el conjunto de la población. En la sociedad moderna, las TIC se han incorporado formando parte de la vida cotidiana y de las I2C, éstas son las que sustentan servicios esenciales para diferentes sectores como el de la salud, la economía, las finanzas, la seguridad, el transporte y la logística, la energía, las comunicaciones e Internet y la industria, entre otros tantos sectores. Por su naturaleza y por la importancia que tienen como factor de desarrollo, la interrupción o destrucción parcial o total de este tipo de infraestructuras poseen el potencial de provocar un gran impacto en la continuidad y en la integridad de las operaciones de los diferentes sectores que hacen uso de éstas, hecho que podría derivar en situaciones que afectan el bienestar de los ciudadanos y el eficaz funcionamiento de los gobiernos.

Además de sustentar al resto de los sectores de la nación, las I2C poseen entidad por si mismas. Este hecho obliga a profundizar sobre los aspectos de protección de las mismas, de manera tal de responder a la demanda de soluciones que den respuesta a sus problemáticas particulares, muchas de ellas orientadas, pero no limitadas a la ciencia de la seguridad de la información.

El mundo está inmerso en sistemas interrelacionados basados en redes de datos, equipos de computación y aplicaciones informáticas, conformando lo que se denomina el "Ciberespacio", activo universal que se ha convertido en la columna vertebral de la sociedad moderna.

Este paradigma de desarrollo se ve amenazado por la existencia de vulnerabilidades vinculadas a los diferentes subsistemas de TIC y a la existencia de personas y/o naciones con intereses contrapuestos. La combinación de vulnerabilidades y amenazas deriva en el surgimiento de riesgos que deben ser mitigados de manera apropiada, intentando evitar o

reducir al mínimo el impacto de un ataque, eludiendo efectos directos y en cascada, consecuencia directa de las interrelaciones entre componentes de los diferentes sectores. Para avanzar en la correcta gestión de riesgos de seguridad en las I2C resulta fundamental comprender la naturaleza de las amenazas, cuales son sus posibles consecuencias y cómo proceder para organizar, operar y mantener un plan estratégico de protección que permita articular recursos y acciones entre los diferentes actores implicados.

El éxito en una empresa como la PI2C depende esencialmente de que el Gobierno Nacional, las organizaciones del sector privado y el sector científico-tecnológico trabajen conjuntamente. Esta comunidad debe contemplar el desarrollo de recursos humanos y tecnológicos, la adecuación de los esquemas legislativos, la integración de fuerzas y capacidades, y el desarrollo de concientización en la ciudadanía acerca de la importancia que tienen la protección de las Infraestructuras de Información Crítica y la Ciberseguridad.

Para que el Plan de PI2C pueda llevarse a cabo exitosamente deberán considerarse los siguientes lineamientos generales:

- Identificar las IC y las I2C,
- Priorizar los niveles de seguridad,
- Analizar los riesgos,
- Establecer metodologías adecuadas proporcionando mecanismos de protección, detección y comunicación,
- Articular respuestas efectivas ante la ocurrencia de eventos de seguridad,

En definitiva, establecer un modelo de gestión de incidentes de seguridad adecuado al nuevo contexto de I2C que atienda las necesidades de los diferentes sectores implicados.

Son muchos los ejemplos de países en el mundo que poseen desarrollos en PI2C, aunque en distintos niveles de maduración. Desde EE:UU que es el pionero en este tipo de iniciativas y cuyo desarrollo es sorprendente, hasta nuestro vecino Brasil que se encuentra desarrollando sus primeros pasos. En los casos mas avanzados, se contemplan planes de PI2C concretos, leyes que

respaldan acciones de protección, IC bien definidas, organismos y agencias conformadas por los sectores públicos y privados con colaboración del sector académico, entre otros.

En Argentina no existe aún un plan de PI2C ni una definición de lineamientos estratégicos para su desarrollo. Solo existen al momento algunos esfuerzos aislados como congresos o simposios cuyo objetivo fundamental es el de despertar conciencia, o algún trabajo técnico llevado adelante en base a los requerimientos de algún sector en particular.

En este trabajo de tesis se trata de mostrar la importancia de las I2C para la sociedad moderna y la necesidad de avanzar en su protección a nivel nacional.

Finalmente se esboza un modelo conceptual de PI2C para aplicar en nuestro país con el objetivo de cubrir la brecha entre la gestión funcional y tecnológica de seguridad de estos entornos, se describen las funciones, la arquitectura, sus participantes, como debería ser la interacción con el resto del mundo y quienes son los destinatarios finales de los productos generados. En definitiva, se presenta una conjunto de lineamientos estratégicos que pueden ser utilizados como base para avanzar en una solución de PI2C en Argentina.

CAPÍTULO 2

2 DEFINICIÓN DEL PROBLEMA GENERAL DE PI2C

Para avanzar en el estudio y análisis del problema general de *Protección de la Infraestructura de Información Crítica* (PI2C) se deben definir previamente una serie de conceptos fundamentales.

Infraestructuras Críticas (IC)

Una IC está constituida por un 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. Por ejemplo, los recursos pueden contemplar diferentes sistemas sobre los cuales se afianzan el gobierno, la economía, la salud, las comunicaciones, etc., y trasciende cualquier ámbito ya que interesa tanto al sector público como al privado.

Infraestructuras de Información Críticas (I2C)

Las I2C hacen referencia a los sistemas soportados por diferentes activos físicos y lógicos sobre los cuales se sustentan las Tecnologías de la Información y la Comunicación (TIC).

Entre los sectores más importantes vinculados a la I2C se destacan:

- Sistemas de Telecomunicaciones
- Sistemas Energéticos
- Sistema Financiero y Bancario
- Sistemas de Transportes
- Sistemas de Agua
- Logística Alimentaria
- Sistemas de Salud
- Servicios de Emergencias

Se entiende como Sistema al conjunto de recursos de carácter público-privado que permiten llevar adelante las operaciones cotidianas en el contexto apropiado.

Por ejemplo: *Los Sistemas de Telecomunicaciones vinculados a la I2C alcanzan a todos los recursos vinculados con conmutación de tráfico de voz y datos, encaminamiento y sistemas de información que soportan las telecomunicaciones, cualquiera sea el carácter de las mismas. En este contexto resulta simple imaginar el impacto de un problema o ataque masivo sobre el Sistema de Telecomunicaciones a nivel nacional.*

Como resultado cada vez mayor de la utilización de TIC en los sistemas asociados a la I2C, el incremento en el uso de tecnologías deriva en una mayor exposición a las vulnerabilidades existentes[2.8] asociadas a los diferentes subsistemas y al elevado costo de esquemas adecuados a tratamientos de riesgos, especialmente en los casos en los que se ha comenzado a utilizar Internet (debido a sus características) como infraestructura de soporte de datos y control.

Los responsables finales de la protección de la I2C son los Gobiernos y/o Estados con sus respectivos departamentos, agencias, secretarías y/o ministerios, en base al principio de que las mismas conforman un recurso indispensable para la nación. El objetivo principal vinculado a la PI2C consiste en preservar y asegurar los intereses, ya sean públicos o privados, de carácter nacional o internacional.

Protección de la Infraestructura de Información Crítica (PI2C)

La 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 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.

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 .

La I2C es considerada un recurso invaluable para la sociedad moderna por lo que la PI2C permite establecer un esquema de seguridad adecuado por medio del cuál enfrentar las diferentes amenazas en base al concepto de tratamiento de riesgos de seguridad.

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 vinculados a los diferentes sistemas en el contexto de I2C.

- Principio 2 "Seguridad Lógica": proteger los diferentes activos de información vinculados a los sistemas en el contexto de I2C.

- Principio 3 "Colaboración": establecer recursos y procesos que permitan abordar la problemática vinculada a la PI2C desde una perspectiva global e integradora, que utilice diferentes recursos de los sectores público y privado por medio de los cuales poder abordar al problema con un frente unificado. La Colaboración implica la generación de recursos que permitan agilizar las comunicaciones y compartirlas (herramientas y datos).

- Principio 4 "Aprendizaje": todas las operaciones desarrolladas en el contexto de PI2C deben aportar el conocimiento sobre el tratamiento de la problemática. El aprendizaje deberá poder se traducido en una estrategia.

En toda situación que comprometa la seguridad de la I2C, las consecuencias de la misma seguramente serán sentidas por la sociedad 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 a escala nacional y multinacional, dependiendo de otras infraestructuras. Debido a esto, cualquier accidente a escala nacional, requerirá de esfuerzos a escala mundial, ya sea por los gobiernos o por el sector privado en el que todos resulten beneficiados.[2.2]

Las operaciones de protección de una IC emplean metodologías analíticas por medio de las cuales es posible detectar e identificar las vulnerabilidades y realizar un análisis que derive en estrategias adecuadas de mitigación del riesgo.

Por ejemplo, pueden realizarse pruebas de penetración sobre la infraestructura ya que es un método relativamente sencillo, rápido y económico para detectar brechas de seguridad en los diferentes sistemas. Este tipo de técnicas es útil especialmente en aplicaciones web soporte de las I2C. Una cuestión importante que debe ser tenida en cuenta es que las metodologías de evaluación del riesgo deben ser consideradas independientemente del modelo de negocio del que se trate, alcanzando tanto al sector privado como al público.

La finalidad de las actividades vinculadas a la PI2C consiste en garantizar que ningún perjuicio pueda poner en peligro la vida de una organización la cuál sea parte de la I2C. En términos prácticos esto equivale a reducir la probabilidad de materialización de las amenazas, limitar las consecuencias de los ataques y los problemas de funcionamiento inducidos y permitir la normalidad y funcionamiento de un sistema tras un siniestro a un costo aceptable y en un plazo razonable.

Las TIC son por sí mismas *Infraestructuras de Información Crítica.*

2.1 LAS INFRAESTRUCTURAS DE INFORMACIÓN CRÍTICAS (I2C) COMO SOPORTE PARA EL CRECIMIENTO ECONÓMICO Y SOCIAL

En la actualidad las TIC, las Redes de Telecomunicaciones, los Satélites, el Software, la Internet, etc., están omnipresentes, siendo cada vez mayor la tendencia hacia la digitalización. La integración ha dado lugar a que la tecnología informática esté presente en productos como electrodomésticos, automóviles o edificios por ejemplo.

Las TIC también sirven para desarrollar la economía en una sociedad, por sus cualidades de rapidez, manejo de grandes volúmenes de información, capacidad de procesamiento de datos, efectividad de los procedimientos y por la velocidad en la transmisión, entre otras. Si bien las TIC han sido fundamentales para el desarrollo de organizaciones en el sector privado, actualmente estas trascienden esta barrera por lo que se están volviendo de especial interés y utilidad en el sector público en el contexto del Gobierno Electrónico. En este sentido, por medio del *Decreto 378/2005* firmado el 27 de abril de 2005 se aprobaron los lineamientos estratégicos por medio de los cuales se ha de regir el *Plan Nacional de Gobierno Electrónico* y los *Planes Sectoriales* para el uso intensivo de las TIC en los organismos de la Administración Pública Nacional (APN) en Argentina [2.22].

En este sentido, las TIC fueron incorporadas en los sectores gubernamentales, políticos, administraciones públicas y privadas, y fundamentalmente a los ciudadanos, generándose cada vez mayor dependencia de las mismas en las actividades cotidianas. Las I2C deben ser pensadas como un conjunto de servicios que permiten crear y generar valor añadido (comercio electrónico, gobierno electrónico, tele-trabajo, educación a distancia, etc.) con independencia de las tecnologías, impulsando la creación, la disponibilidad y la utilización de los servicios basados en la red.

La conexión entre economía y tecnología no es lo único que involucra a la nueva seguridad global. En la medida que el bienestar y la seguridad de los ciudadanos dependen con claridad del sistema económico, éste se convierte en un objetivo de potenciales agresiones mucho más rentable que la vida de las

personas en sí, porque sus efectos alcanzan a millones de ciudadanos.

A pesar de las ventajas que ofrece la I2C para el desarrollo de la sociedad moderna, debe prestarse especial atención a la existencia de amenazas de seguridad que generan un potencial compromiso de la integridad, confidencialidad y disponibilidad de sus recursos. Cotidianamente se efectúan millones de transferencias de información por la vía electrónica, facilitando una cantidad casi inimaginable de procesos, hecho que presenta un escenario con mayores niveles de riesgo asociado. El abanico de amenazas a las cuales se ve sometida una I2C va desde fraude, usurpación de identidad, crímenes financieros, pérdida de la privacidad, hasta ataques de denegación de servicios llevados a cabo en el contexto de operaciones de información en conflictos entre naciones del mundo. Los ataques contra las I2C pueden causar daños a la sociedad de formas nuevas nunca antes pensadas con graves impactos si se ven afectados los recursos críticos.[2.2]

2.2 SECTORES INVOLUCRADOS EN LA PI2C

La PI2C involucra fundamentalmente a dos sectores: el *Sector Privado* y el *Sector Público*.

- El *Sector Privado*, está conformado por aquellas entidades que no están controladas por el estado. Por ejemplo las compañías, corporaciones internacionales y las organizaciones no gubernamentales (ONG).
- El *Sector Público* está constituido por el gobierno en todos sus niveles y por corporaciones e instituciones controladas por el estado, incluyendo departamentos, ministerios, agencias, empresas de capital estatal. [2.1]

El problema de la PI2C no sólo trata de establecer soluciones de ingeniería al problema de seguridad, sino que además establece lineas de trabajo destinadas a favorecer y alentar la investigación y desarrollo, promover la adopción de una cultura de la seguridad, e imponer el cumplimiento de normas mínimas que permitan llevar adelante las operaciones cotidianas soportadas por las I2C.

Reconociendo la complejidad del problema y las limitaciones impuestas por el mismo surge entonces la necesidad de colaboración entre los sectores público y privado para la ejecución de planes de acción a nivel nacional e internacional.

Compete a los Estados la definición de una verdadera política de desarrollo de la sociedad de la información en función de sus valores propios y el aporte de los medios necesarios para ello. En este contexto, la PI2C se vuelve un recurso insustituible que permite alcanzar los objetivos de desarrollo.

Desde un enfoque global, el tratamiento centralizado y coordinado de las diferentes amenazas e incidentes de seguridad vinculados a las I2C exige una respuesta política, económica, jurídica y tecnológica homogénea, susceptible de ser adoptada por los diversos protagonistas de la cadena, copartícipes de la seguridad.

2.2.1 LA ADMINISTRACIÓN PÚBLICA Y SU ROL EN LA PI2C

La administración pública juega un rol fundamental en la PI2C, y si bien las entidades privadas pueden tener un gran nivel de intervención y ofrecer múltiples beneficios, es necesario que el gobierno de el puntapié inicial, aliente, coordine e interactúe con ellas.

A continuación se presenta una serie de cuestiones destacadas vinculadas a la participación de los Estados Nacionales en la PI2C.

- En primer lugar, es necesario que el gobierno solvente o realice aportes económicos sobre las entidades públicas y privadas para que éstas puedan realizar actividades en forma continua. Fomentando una mutua cooperación, se podrán cumplir los objetivos propuestos.
- En segundo lugar, tener al gobierno como intermediario cuando se necesita interactuar con otros países ofrece un marco de seriedad y respaldo importante. Permite crear políticas de seguridad que puedan ser implementadas a gran escala, y establecer un punto en común con otros estados para el intercambio de información y buenas prácticas

sobre la seguridad de la información de las I2C, organizar ejercicios regionales sobre incidentes simulados a gran escala, etc.

- Finalmente, en tercer lugar, permite definir políticas nacionales, tomando medidas dentro de un marco legislativo adecuado, elaborando planes de contingencia nacionales con vista a planes que favorezcan el bien común.

2.2.2 EL ROL DE LA INDUSTRIA

Entre los desafíos generados alrededor de la seguridad en general y de la seguridad interior en particular, aparecen la ciencia y la tecnología como ingredientes esenciales. Este es el principal aporte que puede generar el sector privado al problema de PI2C. En este sentido, el sector privado cuenta con las capacidades para dar respuesta a una demanda no consolidada totalmente vinculada a la seguridad nacional en el contexto de TIC.

Como ha sido expresado al inicio del capítulo, el desarrollo de la industria de las TIC es de mucha utilidad a las empresas, a la sociedad y a la cultura. Esta industria representa una fuente importante de nuevos puestos de trabajo y crecimiento en ciencia y tecnología.

Desde el punto de vista de Seguridad de la Información, la mayoría de las aplicaciones y sistemas en producción en el sector privado son diseñados con foco en la funcionalidad y en el rendimiento desatendiendo, en general, cuestiones vinculadas a la protección. Tiempo atrás, debido a la inviabilidad o a los altos costos de adquisición de tecnologías de interconexión como Redes de Datos, los sistemas estaban aislados por lo que la superficie expuesta a potenciales atacantes estaba relativamente acotada, no así el número de vulnerabilidades.

En la actualidad existe una Integración de los los Sistemas de Información en base a la estandarización de las arquitecturas de procesamiento y comunicaciones (Modelo OSI), y a la disponibilidad de tecnologías económicas y de alto rendimiento como Ethernet, TCP/IP, Paradigma Web y Bases de Datos. Desde el punto de vista de protección, esta integración y apertura de

los Sistema de Información aumenta considerablemente la complejidad y heterogeneidad del problema a tratar, lo que deriva en un incremento de la superficie expuesta y del número de vulnerabilidades.

Desde la óptica de la PI2C, este hecho favorece la posibilidad de "Ciberataques" cuyo impacto puede tener serias consecuencias, incluso en el orden público.

Los ataques a los cuales pueden verse sujetas las I2C son, entre otros: Interceptación y manipulación de Información, Denegación de Servicio, Falseo de Identidad, respuestas no solicitadas, secuestro de sesiones, manipulación de paquetes/protocolos, modificación de datos de registro (logs), control no autorizado, etc.

El resultado de estos ataques pude producir desastres como:

- Acceso NO autorizado, robo o mal uso de información confidencial (Problema vinculado a la "Privacidad" en el Gobierno).
- Publicación de información en lugares no autorizados.
- Pérdida de integridad o disponibilidad de los datos del proceso o información de producción.
- Denegación de servicio: pérdida de disponibilidad.
- Pérdida de capacidad de producción, inferior calidad de productos, pérdidas medioambientales.
- Violación de requisitos de cumplimiento legales.
- Riesgos de salud pública, incluso pérdidas HUMANAS.

Las TIC han evolucionado rápidamente y han entrado en el entorno de los sistemas de control industriales, caso que merece especial atención debido a las consecuencias potenciales de un compromiso de los mismos. En la Sección 2.4 de este capítulo se presenta un ejemplo de seguridad sobre Sistemas SCADA.

Por todo lo mencionado, se deben incorporar buenas prácticas de seguridad en todos los recursos vinculados a las IC [2.21].

2.3 AMENAZA REAL A LAS I2C Y RIESGO

La evaluación del riesgo de seguridad en I2C involucra generalmente a procesos que permiten estudiar a las amenazas y a las vulnerabilidades en las TIC. El manejo del riesgo involucra la implementación de medidas en planes de corto, mediano y largo plazo destinadas a proteger las I2C. El riesgo puede ser analizado de diferentes maneras como por ejemplo mediante una función de tres variables principales: *amenazas, vulnerabilidades e impacto*.

La existencia de amenazas contra las I2C conllevan el surgimiento de riesgos, los cuales son mas o menos significativos en función del tipo de activos de infraestructura al cual estén vinculados. Cuanto mayor sea el valor del activo en riesgo, mayor será el impacto de un posible incidente de seguridad y mayor el impacto en los procesos asociados.

Una de las metodologías de mayor relevancia para proteger las I2C por medio de la reducción del riesgo consiste en la reducción del número de vulnerabilidades presentes en los diferentes subsistemas. El proceso de reducción de vulnerabilidades debe estar basado en un sistema integrado que permita determinar en cada caso la relación de costo-beneficio de los recursos utilizados.

En general, las metodologías de reducción de riesgos están conformadas por los siguientes procesos:

1. *Identificación de los activos y nivel de criticidad de cada uno en la I2C,*
2. *Identificación, caracterización y evaluación de las amenazas,*
3. *Evaluación de las vulnerabilidades de los recursos críticos para amenazas específicas,*
4. *Determinación de los niveles de riesgo, e*
5. *Identificación de los planes de tratamiento o mitigación de riesgos en base a una planificación estratégica.*

1. Identificación de los activos y nivel de criticidad de cada uno en la I2C

La infraestructura de una compañía o de un sector económico consiste en un conjunto de recursos necesarios para los procesos de producción o para la prestación de servicios. La infraestructura de una ciudad, estado, o nación consiste en el conjunto de recursos necesarios para su actividad económica y social. Para ambos casos valen como ejemplo de componentes de infraestructuras las personas, las operaciones y actividades, la información, las instalaciones, el equipamiento, los materiales, etc.

La definición típica de Criticidad asociada a un recurso de infraestructura se basa en la medida de las consecuencias asociadas con la pérdida o degradación del mismo, lo que se traduce como impacto en el sistema afectado. Las consecuencias pueden ser categorizadas como económicas, políticas, financieras, medioambientales, de seguridad social, de salud, y tecnológicas. Es importante destacar que debido al gran grado de interrelación entre muchos de los subsistemas TIC el impacto que puede provocar la pérdida de un recurso puede generar un efecto en cascada, afectando a otras infraestructuras.

El conjunto de recursos o activos de infraestructura es categorizado por el nivel de criticidad asociado al mismo. Este grado es evaluado como bajo, medio y alto, y sus medidas intermedias.

2. Identificación, caracterización y evaluación de las amenazas

Una amenaza es definida como *"cualquier indicación, circunstancia, o evento que cause un daño o pérdida de un recurso"* .

Para que la evaluación del riesgo en base al estudio de vulnerabilidades resulte de utilidad es necesario caracterizar el problema. Las características importantes a relevar en una amenaza incluyen entre otros:

- Tipo (terrorista, militar),
- Medio ambiente (huracán, tornado),
- Intereses o motivación,

- Capacidad, métodos y tendencias (que técnicas se han usado en el pasado y sirven como experiencia para el futuro).

Mientras que las amenaza pueden ser identificadas y caracterizadas de manera determinística en base a las técnicas mencionadas recientemente, los potenciales ataques son estudiados en base a modelos de probabilidades basados en dos parámetros de interés:

a) Si el recurso representa o no un objetivo basado en la motivación del adversario,
b) Si el adversario tiene la capacidad o no de atacar el recurso, y en caso afirmativo los métodos de ataque disponibles.

Otro parámetro a considerar incluye la historia en relación a un determinado ataque sobre un objetivo en particular realizado por el mismo adversario o por otros. El recurso podrá ser vulnerado o no, de acuerdo al método de ataque que se le aplique.

La evaluación de amenazas es un proceso continuo que nunca finaliza. Este hecho se debe a que las infraestructuras cambian, y a que surgen nuevas técnicas y herramientas de ataque en base al estudio de nuevas vulnerabilidades.

Las amenazas pueden ser intencionales o no intencionales, dirigidas a objetivos específicos o de amplio alcance, y pueden provenir de uno o varios orígenes desde el propio país, o desde el extranjero.

Una primera clasificación de la amenazas a las TIC puede ser establecida en base a las técnicas y vectores que permiten el ataque. Algunas de las amenazas más comunes vinculadas a las I2C son: Virus, Gusanos, Caballos de Troya, Spyware y Adware, Ingeniería social, Pishing y Dialers, Hoax, Spam, Ataques de Denegación de Servicios y Ataques a Protocolos. Este tipo de amenazas utilizan técnicas y herramientas para afectar de manera directa la seguridad de los diferentes recursos.[2.12]

Desde una perspectiva mas orientada a la seguridad nacional deberá considerarse un segundo esquema de clasificación de las amenazas el cuál hace referencia a los objetivos a alcanzar por medio del ataque. En este segundo grupo se destacan:

- El Terrorismo, que está definido por aquellas amenazas que utilizan técnicas y herramientas destinadas a causar daños en las infraestructuras de otros países con el objetivo de alterar el orden público nacional e internacional por medio de la generación de situaciones de terror. Por ejemplo: operaciones destinadas a interrumpir el normal funcionamiento de las IC por medio de ataques como operaciones de información ofensivas o utilización de herramientas de destrucción masiva (químicas, biológicas o nucleares).
- El Espionaje, también definido por amenazas pero a aquellas que están vinculadas con las actividades de inteligencia política y militar, y para llevarlas a cabo utilizan mayormente tecnologías TIC. Para países con un fuerte desarrollo científico que sustente el modelo de desarrollo, el espionaje en el sector privado debe considerarse una cuestión de estado.

Un ejemplo del esfuerzo oficial vinculado al control de amenazas vinculadas a TIC en Europa lo conforma el Centro de Informes y Análisis para la Seguridad o MELANI (siglas en inglés de "Reporting and Analysis Centre for Information Assurance"), el cuál presenta informes al menos dos veces al año sobre el robo de información global. Es un ente que además especifica y caracteriza los riesgos sobre la Internet, sobre redes Wireless, teléfonos móviles, pda, y otros. También ofrece servicios tales como la seguridad en banca electrónica y configuraciones de seguridad en las computadoras. Para más información sobre MELANI visitar [2.23]

3. Evaluación de las vulnerabilidades de los recursos críticos para amenazas específicas.

Una vulnerabilidad se define como *"la debilidad que puede ser explotada con el fin de afectar la confidenciabilidad, la integridad, o la disponibilidad de un*

determinado recurso o activo de infraestructura".

Las debilidades pueden ser sujeto de diferentes esquemas de clasificación dependiendo del dominio de conocimiento con el que se trate. En el contexto de seguridad de la información un sistema simple pero eficiente de clasificar las vulnerabilidades consiste en declarar su origen o punto de introducción en el sistema, así surgen tres posibles valores: vulnerabilidades de diseño, vulnerabilidades de implementación y vulnerabilidades de configuración. Podría extenderse este modelo para que contemple vulnerabilidades asociadas a los procedimientos y las operaciones vinculadas con las personas. La evaluación de una vulnerabilidad debe calcular la fiabilidad y efectividad de la misma.

Las vulnerabilidades son evaluadas para analizar el efecto en el marco de ataques específicos, se identifican tres pasos:

a) Determinar como un adversario podría llevar a cabo un ataque contra un recurso específico,

b) Evaluar las medidas existentes de su fiabilidad y efectividad para detectar o retardar un ataque específico,

c) Estimar el estado actual de cada vulnerabilidad y asignarle un valor.

4. Determinación de los niveles de riesgo.

El Riesgo de Seguridad en el contexto de los estándares ISO/IEC 27000 representa la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según el estándar ISO 73:2009, el Riesgo surge de la combinación de la probabilidad de un evento y sus consecuencias sobre los diferentes activos. Finalmente, el estándar ISO/IEC 18044:2004 considera al riesgo como un único evento o una serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones empresariales y de amenazar la seguridad de la información.

El riesgo puede ser evaluado en distintos sentidos tales como el económico, el medioambiental, el del sector de las TIC, el de defensa nacional, etc.; y se le asigna una escala de valores según sea el potencial impacto que puede causar sobre una métrica cuantitativa.

5. Identificación de los planes de tratamiento o mitigación de riesgos en base a una planificación estratégica.

Las medidas a tomar para minimizar el riesgo consisten en:

- Reducir las amenazas,
- Reducir el número de vulnerabilidades,
- Controlar el impacto que puede causar un ataque.

Cada una de las medidas abordadas debe ser evaluada con anticipación cuando se elige la forma de ejecutarla, determinando los efectos que causaría en la I2C, ya que cada opción a elegir posee un costo multidimensional asociado con materiales, equipamiento, instalaciones, entrenamiento, etc.

A los costos de adquisición deben sumarse los costos operacionales, incluyendo el mantenimiento, la reparación y el tiempo. Es importante tener en cuenta que siempre que se evalúe una opción destinada a manejar el riesgo, debe evaluarse el costo-beneficio de la implementación de la misma para priorizar la mejor opción. El costo de la protección del recurso no debería exceder (en un alto porcentaje) el valor total del mismo.[2.3]

En el contexto de I2C, cuando se habla de riesgo no sólo se tiene en cuenta el impacto económico, sino que se evalúa también el impacto que puede ser provocado a diferentes niveles en el contexto local o nacional, intentando mantener los servicios esenciales o de misión crítica de la población en funcionamiento.[2.13]

Puede verse mas información sobre riesgo y técnicas de gestión de seguridad en TIC en los estándares ISO/IEC 73:2009 e ISO/IEC 13335-1:2004 [2.24] respectivamente.

2.4 LA PI2C EN EL CONTEXTO DE DEFENSA NACIONAL

Debido al soporte que ofrecen los diferentes recursos vinculados a la I2C para el desarrollo de las sociedades modernas, la PI2C se ha convertido en un concepto y una disciplina de creciente importancia para la defensa de las naciones, especialmente en los países desarrollados. Actualmente el concepto de PI2C es un punto esencial, teniendo dos factores a considerar:

A) *Evaluar del espectro de las amenazas producidas las cuales tienen como fin específico causar daño.*

B) *Los nuevos tipos de vulnerabilidades adoptadas por la sociedad moderna, característicos de los sistemas de información poco seguros.*

Debido a las características de las I2C en lo que hace a sus componentes, ha surgido una variedad de nuevas amenazas que deben ser estudiadas y tratadas en base al correcto planteo e implementación de políticas de seguridad que consideren el ciclo completo de vida de las mismas.

El ciclo de vida de las amenazas obliga al planteo de temas relacionados con el *¿Cómo?, el ¿Cuándo?, ¿Dónde?, ¿Quién?*, y si es posible el *¿Porqué?* de las mismas. Una particularidad en las amenazas a las I2C consiste en que el origen de las mismas puede ser fácilmente ocultado por medio de la utilización de sistemas intermedios (relays), constituyendo de alguna manera un riesgo incierto e indirecto.

Como resultado de las dificultades de identificar el origen de los incidentes en contextos de riesgos (es decir quienes son los oponentes) en sistemas distribuidos, las políticas de seguridad deben poder tratar con los diferentes actores y sus motivaciones de tal modo que la identificación de los responsables de eventos vinculados con violaciones a las políticas de seguridad pueda ser realizada.[2.16]

El impacto provocado por un incidente de seguridad en las I2C debilitan la seguridad, la economía y el bienestar social de los ciudadanos y pueden generar grandes impactos en cuestiones de seguridad nacional.

Los mecanismos involucrados en la PI2C deben facilitar la diferenciación del

tipo de amenaza al menos en los dos siguientes grupos:

1) ***Las amenazas aleatorias y relativamente limitadas,*** las cuales consisten en adversarios con pocos fondos económicos y organizaciones con objetivos a corto plazo, como puede ser un Hacker, o un pequeño grupo de delincuentes organizados, no llegando en ningún caso a realizar ataques sofisticados contra las I2C que comprometan los atributos de seguridad.

2) ***Las amenazas estructuradas,*** son aquellas realizadas por grupos con solvencia económica, con planes estratégicos de largo plazo, con metas bien claras y con recursos tecnológicos y profesionales a disposición. Son consideradas amenazas las cuales preocupan a la seguridad nacional y pueden poner en riesgo la seguridad de las I2C.

Como ha sido expresado y podrá verse en el siguiente capítulo, la PI2C en los países desarrollados permite alcanzar una solución al problema de seguridad de las I2C en base a estrategias preventivas y mecanismos de respuestas que permitan minimizar el impacto de un potencial ataque. En la Sección 2.6 del presente Capítulo se presentan conceptos generales para el tratamiento de incidentes de seguridad en I2C en base al concepto de Gestión de Incidentes de Seguridad (GIS).

Es importante destacar finalmente que debido a su carácter de criticidad para el desarrollo nacional y para el mantenimiento de las funciones elementales de la sociedad, las I2C se han convertido en objetivos de operaciones militares en conflictos bélicos. Esta realidad ha derivado en la formación de unidades militares en las Fuerzas Armadas de algunos países, las cuales están altamente especializadas en conflictos donde los objetivos son los activos de información y comunicaciones del enemigo. A este tipo de conflicto se lo denomina "Guerra de Información". [2.9][2.10]

2.5 EJEMPLO DE COMPONENTES DE INFRAESTRUCTURA CRÍTICA (IC)

Para poner en contexto al lector se presenta un ejemplo de uno de los componentes con potencial de conformar la IC Nacional.

El ejemplo refiere al *Acueducto de Río Colorado* localizado en la Provincia de la Pampa.

El acueducto forma parte de al menos dos áreas de IC:

- La primera de las áreas pone al Acueducto en una posición relevante desde el punto de vista de provisión de un bien esencial para la vida de los ciudadanos como es el agua.
- La segunda de las áreas alcanza a los sistemas de información que soportan sus operaciones.

Se presentará un análisis general sobre los sistemas de información involucrados en el funcionamiento del acueducto, especialmente sobre los componentes SCADA que controlan su funcionamiento, para luego generar alguna hipótesis sobre el potencial impacto de un incidente de seguridad y sus efectos sobre la sociedad.

Los Sistemas de Supervisión, Control y Adquisición de Datos o SCADA (de las siglas en Inglés de "Supervisory Control And Data Acquisition") conforman un sistema basado en diferentes componentes electrónicos y computadoras que permiten supervisar y controlar en forma remota una instalación de cualquier tipo. A diferencia de los Sistemas de Control Distribuido en los que las acciones de control propiamente dichas se realizan en forma automática, el lazo de control en sistemas SCADA es generalmente cerrado por el operador.

Por ejemplo en el Acueducto del Río Colorado, al sur del límite provincial, se encuentra la obra de toma de agua ubicada sobre el margen izquierdo del río Colorado a unos mil metros aguas arriba de la descarga del río Curacó, en las inmediaciones de Pichi Mahuida. La obra de captación está dividida en tres secciones donde se alojan rejas, vertederos y compuertas de cierre y a continuación se encuentra una cámara sedimentadora con un recinto de

bombeo.

A su vez, la planta de tratamiento está instalada en una meseta de 3.800 metros de la toma, la que tiene unos 40 metros de altura respecto de ésta. Dicha cámara tendrá una capacidad para tratar el caudal máximo posible de 2 metros cúbicos de agua por segundo a través de tres módulos de tratamiento, integrados por una cámara de carga y con la totalidad del manejo computarizado.

El Acueducto del río Colorado conducirá agua potable y no cruda, lo que exige un sistema de cloración en toda la línea, tanto de cloro en estado líquido como gaseoso, garantizando su calidad a lo largo del transporte. La extensión del acueducto tiene un desarrollo de 263 kilómetros en el ducto principal y 268 km en los ductos secundarios.

Uno de los temas a tener en cuenta en la complejidad de la obra del acueducto es que de la cámara de carga se deriva el agua cruda a los floculadores, decantadores, filtros rápidos, galerías de comando, planta de ablandamiento por resinas, edificio de dosificación de cloro gaseoso y se vierte agua potable a la cisterna (C2) de 2.500 m3 de capacidad, para realizar el bombeo al ducto.

En el predio de la Planta Potabilizadora, se ubican además los siguientes edificios e instalaciones: edificio de cloración; cubas para la preparación de salmuera, edificio para la preparación de sustancias químicas, edificio principal con sus secciones de laboratorios, talleres, sala de control, comando y servicios de oficinas de administración. [2.17]

El sistema de comando automatizado se basa en:

a) SCADA: Control de Supervisión y Adquisición de Datos. Es un software de programas de aplicación para el control de procesos y acopio de datos en tiempo real desde sitios remotos y permite controlar condiciones.

b) SCPA: Sistema de control de producción de agua. Genera una lógica para mantener niveles de agua en la Cisterna Principal y producción de agua.

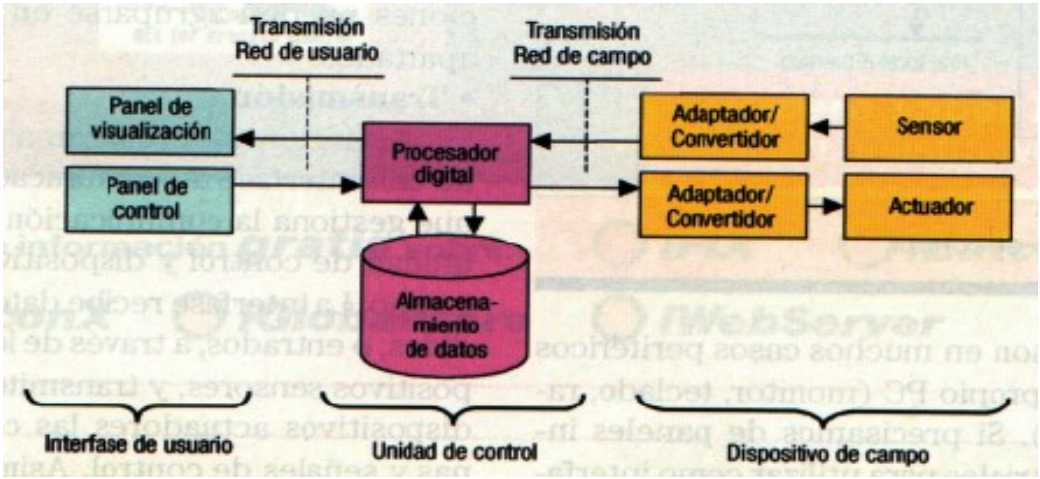
c) SCC: Sistema de control de cloración. Genera una supervisión de la cloración en todo el acueducto y ramales secundarios, ordenando acciones [2.14]

Estructura de un Sistema SCADA

En los sistemas SCADA los datos se procesan para determinar si los valores están dentro de los niveles de tolerancia, para que en los casos en los que resulte necesario se tomen medidas correctivas para mantener la estabilidad y el control.

Un sistema SCADA esta conformado por:

- *Interfaz Operador - Máquinas:* Es el entorno visual que brinda el sistema. Permite la interacción del ser humano con los medios tecnológicos implementados.
- *Unidad Central (MTU):* Conocido como Unidad Maestra. Ejecuta las acciones de mando (programadas) en base a los valores actuales de las variables medidas. También se encarga del almacenamiento y procesado ordenado de los datos, de forma que otra aplicación o dispositivo pueda tener acceso a ellos.
- *Unidad Remota (RTU):* Lo constituye todo elemento que envía algún tipo de información a la unidad central. Es parte del proceso productivo y necesariamente se encuentra ubicada en la planta.
- *Sistema de Comunicaciones:* Se encarga de la transferencia de información del punto donde se realizan las operaciones, hasta el punto donde se supervisa y controla el proceso. Lo conforman los transmisores, receptores y medios de comunicación.
- *Transductores*: Son los elementos que permiten la conversión de una señal física en una señal eléctrica (y viceversa). Su calibración es muy importante para que no haya problema con la confusión de valores de los datos.



Para realizar el intercambio de datos entre los dispositivos de campo y la estación central de control y gestión, requiere un medio de comunicación, existen diversos medios que pueden ser cableados (cable coaxial, fibra óptica, cable telefónico) o no cableados (microondas, ondas de radio, comunicación satelital).[2.18]

Los sistemas SCADA son utilizados por ejemplo en:

- Sistemas de transportes: metro, trenes, puertos o aeropuertos,
- Sistemas industriales: químicas, refinerías, distribución y control de electricidad, agua, gas,
- Centrales nucleares, etc.

Los sistemas de control de procesos fueron diseñados antes del surgimiento de Internet. Fueron pensados para ser sistemas aislados y no conectados en red, por lo que carecen de los mecanismos de seguridad elementales. Para asegurar los sistemas SCADA debe recurrirse a mecanismos tales como sistemas de autenticación y control de accesos, Firewalls, Cifrado, Antivirus, entre otros.

A la hora de proporcionar seguridad a los sistemas SCADA debe definirse el tipo de dispositivos y el Hardware y Software que utilizan, los protocolos de comunicaciones, los mecanismos de seguridad que implementan, los puntos de entrada al sistema, las particularidades a nivel de políticas y

procedimientos, los posibles impactos que la explotación de una vulnerabilidad puede tener, etc.

Vulnerabilidades, Riesgos y Seguridad en un Sistema SCADA

Actualmente es bastante común que las redes SCADA estén mezcladas con las redes de las empresas sin ningún tipo de separación o control de acceso lo que incrementa notablemente el riesgo de seguridad desde el punto de vista operacional. El uso inadecuado de redes Inalámbricas 802.11x empleadas para reducir la necesidad de cableado incrementa el nivel de riesgo de seguridad. La carencia de personal con conocimientos específicos en seguridad deriva muchas veces en la implementación de sistemas con elevado número de vulnerabilidades debido a implementación y configuración de componentes.

Sumado a los problemas identificados anteriormente, la carencia de políticas de seguridad o esquemas de normalización genera situaciones en la que por ejemplo no se contemplan políticas de renovación de contraseñas ni de longitud mínima. Las contraseñas suelen compartirse, incluso suele existir solamente un usuario en los equipos de red que se comparte entre todos los operadores, lo que suele limitar en gran medida la capacidad de auditoría.

Otro problema usual es la falta de comunicación o fluidez entre departamentos de una misma organización, muchas veces ocasionadas por conflictos e intereses.

Es importante abordar la seguridad de las plataformas SCADA con la misma filosofía a la que se tratan los sistemas de TIC convencionales.

Cualquiera de las vulnerabilidades mencionadas aquí, podrían servir de objetivos para atacar al sistema SCADA. Si se piensa en el sistema del Río Colorado, se podría tratar de interferir en la sensórica asociada a los diferentes procesos, o podría tratarse de modificar el comportamiento de la lógica de procesos por medio del compromiso y alteración de los componentes de procesamiento o datos vinculados con la unidad de control. En este punto cabe generar algunas preguntas como la siguiente: *¿Que sucedería si los sistemas*

de control del Acueducto del Río Colorado salen de operación debido a fallas masivas?, ¿Con cuanto tiempo se cuenta para poner nuevamente en operación al Acueducto?, ¿Que sucedería si se alteran los valores de medición de los volúmenes de caudal en el origen del acueducto?, ¿Y si se logran alterar los índices de cloración del agua? … Vale destacar en este punto que los interrogantes arriba planteados surgen de conceptos generales a los cuales cualquier sistema industrial puede ser sometido en el contexto de políticas de continuidad del negocio, por lo que quizás no aplican al caso mencionado.

Para mejorar la seguridad de los sistemas SCADA se debe avanzar en un análisis de seguridad de la información convencional. A nivel de red se podría recomendar el uso de Firewalls y sistemas de detección de intrusos (IDS) y en lo posible migrar a una arquitectura de red segmentada con controles perimetrales robustos. Además, solo se debe permitir la mínima cantidad de conexiones desde servidores externos hacia los dispositivos internos de la red SCADA y todas las permitidas deben estar debidamente documentadas y justificadas.

Los servidores que almacenan los datos históricos del sistema se denominan repositorios, recopilan información de la red SCADA y la almacenan para que esté disponible para consultas y reportes históricos. Estos servidores deben estar situados dentro de la red privada SCADA con sólidos sistemas de autenticación para sus accesos. Con estas medidas se buscaría minimizar la ventana de oportunidad, tanto para atacantes externos como usuarios malintencionados, intentando proteger la infraestructura.

En cuanto a la seguridad referida a políticas y procedimientos, es necesario asegurarse que todos los sistemas están sujetos a estrictos controles de cambio. Se deben incluir asesorías de seguridad en estos procesos. Las plataformas SCADA necesitan estar continuamente operativas por lo que todo evento que pueda ralentizar las comunicaciones o interrumpir el servicio no son aceptables. Es de suma importancia la rápida recuperación ante un incidente por lo que los sistemas SACADA necesitan de una planificación estratégica para lo que se conoce como Continuidad del Negocio y Recuperación de Desastres.

También es importante definir de forma clara y explícita los roles, responsabilidades y los permisos de los gerentes, administradores de sistemas y usuarios.[2.19]

2.6 SISTEMAS DEL NIVEL DE AMENAZAS

Desde el punto de vista de protección de la IC resulta fundamental poder contar con una herramienta por medio de la cuál comunicar información relacionada con los riesgos y amenazas vinculados a actos que atentan contra la integridad, el bienestar y el orden público y privado en el país, desde una perspectiva única e integradora que permita optimizar los procesos asociados al manejo de crisis. El sistema debería poder comunicar información relacionada con el riesgo asociado a actos ilícitos o incluso a ataques terroristas contra la IC en base a una métrica simple basada en *"Grados de Amenaza"*, debiendo ser capaz de incrementar su valor a medida que crece el riesgo asociado en un determinado periodo de tiempo. Un valor específico para el Grado de Amenaza establece las lineas de trabajo sobre las que deberán actuar los diferentes estamentos del estado para lograr reducir el nivel de riesgo y responder al evento o incidente por medio del despliegue de una capacidad adecuada de respuesta.

Para el caso de PI2C, la coordinación del sector público con el sector privado es esencial debido a que gran parte de dicha infraestructura depende de activos y servicios provistos por privados.

El objetivo final del sistema de nivel de amenaza consiste en ofrecer una mirada y un vocabulario común al problema de tratamiento de amenazas y establecer lineas de respuesta coherentes según el contexto. Esto se vuelve particularmente significativo en I2C debido a la complejidad y heterogeneidad de los diferentes sistemas que la conforman. Un elemento significativo que puede proveer los medios destinados a garantizar el cumplimiento del objetivo consiste en un esquema de normalización para el Sistema de Gestión de Incidentes de Seguridad que permita trabajar sobre cualquiera de las fases del ciclo de vida de un incidente.

Algunas de las naciones desarrolladas cuentan con un sistema que les

proporciona un comprensivo y eficaz método de difundir cual es la situación real con respecto a una situación de riesgo, ver Sección 2.7.

A continuación se presenta el sistema utilizado por el "Homeland Security" de los EE:UU establecido en base a la Directiva Presidencial 3 del año 2002. Vale desatacar que dicho sistema esta fuertemente orientado al tratamiento de ataques terroristas. Su naturaleza hace que sea igualmente aplicable a la protección de IC.

El sistema facilita la toma de decisiones de los distintos niveles de los sectores públicos y privados comprometidos en el proceso. La codificación de la información ofrecida por el sistema puede ser la siguiente: *Que el sistema indique una condición asociado a un color el cual indique la situación real.*

Dicho sistema se ha desarrollado de la siguiente forma.

Se definen cinco "Condiciones de Amenaza", cada uno identificado por una descripción y asociadas con un color. El orden va del nivel más bajo, al más alto y son:

- Bajo = Verde;
- Medio = Azul;
- Elevado = Amarillo;
- Alto = Naranja;
- Severo = Rojo.

Por ejemplo, en el nivel más alto, correspondería a una situación de mayor riesgo, como el de un ataque terrorista. El riesgo estará dado por la probabilidad de que un ataque ocurra, y su potencial gravedad.

Las condiciones de amenaza estarán pautadas por un ente de seguridad encargado de evaluar el riesgo y dependerá del gobierno nacional, que es quien está a cargo de la seguridad de la nación, incluyendo otros departamentos o ministerios que servirán de apoyo y asesoramiento para administrar el sistema.

Estas condiciones de amenazas pueden pautarse para la nación entera, o puede seccionarse para un área geográfica particular o un sector industrial, comercial, etc., las cuales podrán sufrir alguna modificación para ajustarse a la situación particular.

En un período de tiempo en el que el valor de la condición de amenaza sea elevado, los sectores público y privado deberán responder y tomar medidas de protección en base a protocolos específicos con el objetivo final de mejorar la situación, es decir neutralizar o reducir sus vulnerabilidades, y aumentar su capacidad de respuesta durante un período de alarma elevada. Estratégicamente será conveniente la coordinación de acciones entre los diferentes órganos de gobiernos y el sector privado.

Los responsables de desarrollar las medidas de protección deberán probar, planear, reformar periódicamente y documentarlas para poder informarlas y llevarlas a cabo a lo largo del tiempo. Anualmente se deberá informar por escrito a las autoridades (Gobierno nacional, autoridades locales, gobernadores, intendentes, autoridades de la justicia, sector privado, etc.), describiendo los pasos que se han tomado para desarrollarlas y como llevar a cabo las medidas de protección apropiadas para cada condición de amenaza presente.[2.15]

La evaluación de la información sobre las amenazas incluirá los siguientes factores:

I. ¿Qué grado de información de la amenaza es creíble?

II. ¿Qué grado de información de la amenaza se puede corroborar?

III. ¿Qué grado de la amenaza es específica y/o inminente?

IV. ¿Cuán grave son las potenciales consecuencias de la amenaza?

- En adelante y para definir las condiciones de amenazas se utilizará el término *Ataque Terrorista,* el cual será definido como la actuación criminal de bandas organizadas que reiteradamente y por lo común de modo indiscriminado, pretende crear alarma social con fines políticos.

Esta violencia es premeditada con la intención de influenciar a un sector determinado.

Cuando una IC es alcanzada por un Ataque terrorista, pone en riesgo un sector de la población impidiendo el normal funcionamiento de éstas. Como se explicó en un principio, las IC son de vital importancia para la sociedad, por lo tanto si están en riesgo de ataques, también lo estará la sociedad.

Según los "Condiciones de Amenazas" nombradas, se definen las medidas a tomar en cada una de ellas.

- ***Condición baja (Verde):*** Esta condición se declara cuando hay un *bajo riesgo* de ataques terroristas. Se deben considerar las siguientes medidas generales:
  - Clarificar y ejercer un plan apropiado de Medidas de Protección.
  - Asegurar que el personal reciba el entrenamiento apropiado en Seguridad Nacional.
  - Institucionalizar un proceso para asegurar que todos los medios y regulaciones evalúan las vulnerabilidades de los sectores periódicamente, y se tomen las medidas más razonables para mitigarlas.

- ***Condición Media (Azul):*** Esta condición se declara cuando hay un *riesgo general* de ataques terroristas. Se deben considerar las siguientes medidas generales incluyendo las anteriores:
  - Verificar el tiempo de respuesta de la emergencia ocasionada y el tiempo que transcurre hasta que es comunicada.
  - Repasar y actualizar los procedimientos de respuesta a las emergencias.

- Proporcionar al público cualquier información que defienda la habilidad de actuar apropiadamente.

- ***Condición Elevada (Amarillo):*** Una Condición Elevada se declara cuando hay un *riesgo significante* de ataques terroristas. Se deben considerar las siguientes medidas generales incluyendo las dos anteriores:
  - Vigilar las crecientes situaciones críticas, es decir la repetición de las mismas.
  - Coordinar la emergencia y planearlas con las jurisdicciones más cercanas.
  - Evaluar si las características precisas de la amenaza requieren las Medidas de protección planificadas.
  - Llevar a cabo un plan de contingencia apropiado y planes de respuesta a emergencias.

- ***Condición Alta (Naranja):*** Una Condición Alta se declara cuando hay un *alto riesgo* de ataques terroristas. Se deben considerar las siguientes medidas generales incluyendo las tres anteriores:
  - Coordinar los esfuerzos de seguridad necesarios con la nación, el Estado, y las agencias de ejecución de leyes locales o cualquier Guardia Nacional u otras organizaciones de fuerzas armadas apropiadas.
  - Tomar precauciones adicionales en los eventos públicos y sitios de acciones alternativos, consideradas iguales.
  - Preparar y ejecutar procedimientos de contingencia, como trasladar o alternar en un sitio las medidas de fuerzas.
  - Restringir las amenazas con acceso sólo a personal autorizado.

- ***Condición Severa (Rojo):*** Una Condición Severa refleja un *riesgo*

severo de ataques terroristas. Se deben considerar las siguientes medidas generales incluyendo las cuatro anteriores, y además será necesario agregar otras medidas de protección específicas acorde a la situación:

- Aumentar el personal destinado a actuar ante las necesidades de emergencias críticas.
- Asignar personal de respuesta a las emergencias, movilizando equipos especializados o recursos específicos.
- Supervisar, remitir, o suspender los sistemas del transporte.
- Cerrar los medios públicos y gubernamentales.

Se deberá preparar un equipo de Emergencias y un Plan en respuestas a las mismas, con el objetivo de informar cómo actuar durante una emergencia. Una medida a tomar sería que todos los ciudadanos informen a las autoridades competentes cuando detecten eventos con potencial impacto en sí mismos, o en su entorno.

Las medidas de protección deben planificarse para ser aplicadas a nivel nacional o a un sector geográfico. Las amenazas que son detectadas y de las cuales se conoce algún tipo de información acerca de cual es su objetivo, o que infraestructura crítica pondrá en riesgo, sirve como un recurso importante para poder evitarlas. Toda la información de interés acerca de las Infraestructuras Críticas, deberán ser informadas mediante el boletín oficial.

Este Sistema de Niveles y codificado con Colores es de gran utilidad usarlo para comunicar tanto a los oficiales de la seguridad pública como a la comunidad en general, siguiendo las directivas correspondientes a cada nivel se podrán llevar a cabo las medidas necesarias para minimizar el impacto de posibles ataques.[2.20]

2.7 GESTIÓN DE INCIDENTES DE SEGURIDAD (GIS)

La Gestión de Incidentes de Seguridad (GIS) conforma uno de los componentes clave vinculados a la PI2C, y como extensión del resto de los componentes de IC. La GIS requiere del establecimiento de una capacidad de respuesta basada en una serie de servicios globales que permitan responder a eventos e incidentes de seguridad de manera adecuada y eficiente, permitiendo sostener el nivel de calidad operativa deseado en base a los requerimientos de los diferentes sectores implicados y al riesgo de seguridad presente.

La capacidad de la GIS hace uso de una serie de procesos para el tratamiento de eventos e incidentes de seguridad en una concepción extremo-a-extremo soportada por el contexto jurídico establecido y por las diferentes políticas de seguridad vinculadas a los sectores público y privado. La GIS requiere además de la presencia de esquemas claros de roles y responsabilidades, de herramientas adecuadas, de recursos de infraestructura y finalmente de un plantel de especialistas de seguridad dedicados a llevar adelante todos los procesos involucrados de tal manera que todas las actividades desarrolladas resulten repetibles en el tiempo.

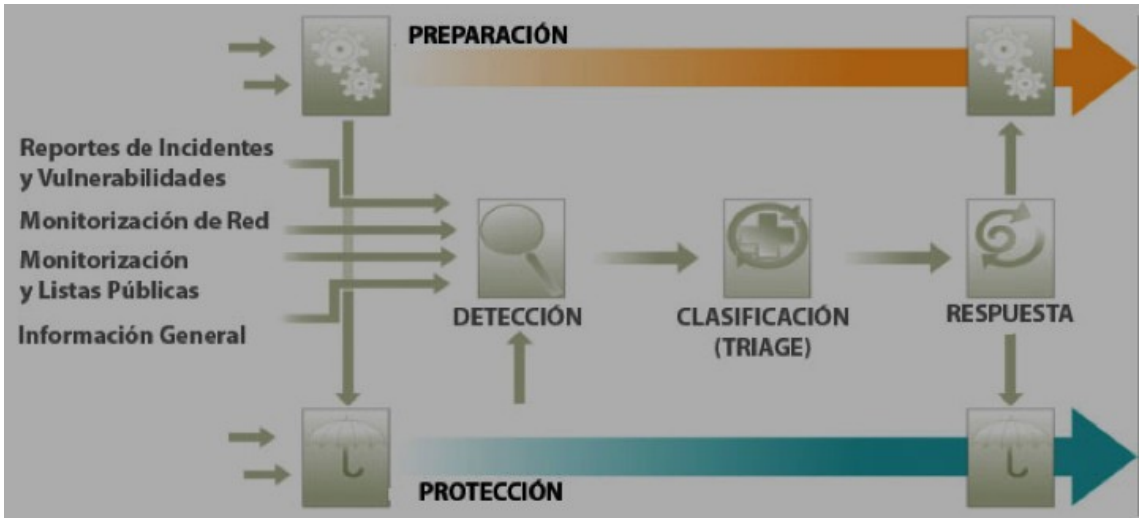
- ***EL Modelo de GIS***

A continuación se presenta una síntesis de los cinco procesos fundamentales que hacen al modelo de GIS:

- **Preparación:** Establecimiento, sostenimiento e implementación de un esquema de trabajo y de mejora continua sobre el grupo de respuesta a incidentes de seguridad, o sobre las áreas afines.
- **Protección:** Implementación de planes de acción y de mejora en cuanto a protección de la infraestructura con el fin de mitigar los riesgos de seguridad.
- **Detección:** Identificación y reporte de eventos de seguridad en el momento de ocurrencia, tratando en cada caso de inferir la posibilidad de futuros eventos relacionados.

- **Clasificación (Triage):** Categorización, priorización, correlación y finalmente asignación de cada evento a un analista para su posterior investigación e implementación de respuestas adecuadas.
- **Respuesta:** Consiste en la planificación, coordinación e implementación de los procedimientos de respuesta a incidentes.

La siguiente figura muestra un esquema general de los principales procesos asociados a la capacidad de la GISe.



Los procesos del modelo pueden ser interpretados de la siguiente manera:

- *Preparación y Protección:* procesos continuos en el tiempo, requieren de la puesta es escena de un conjunto grande de recursos tales como políticas, procedimientos, personal, tecnologías e infraestructura de tal manera que las actividades de gestión de incidentes puedan llevarse adelante a tiempo, de forma coordinada y efectiva. Es interesante visualizar el hecho que los procesos de Preparación y Protección soportan la implementación y operación de los otros procesos del sistema.
- Los procesos de Preparación y Protección obedecen a requerimientos o políticas que establecen reglas a cumplir sobre la estructura y funcionalidad de dichos procesos.
- El nexo presente entre los procesos Preparación y Protección establece

una realimentación de información por medio de recomendaciones de mejora destinada a optimizar la infraestructura de computo. La información realimentada es obtenida por medio de procedimientos de análisis postmortem en el proceso de Preparación.

- Los procesos de *Detección, Clasificación y Respuesta* son presentados en orden, según el flujo de información vinculado a incidentes es procesado. Los eventos que llegan al proceso de Detección deben ser sometidos a análisis para detectar si deben o no ser sujetos a más análisis y evaluaciones. Si en base a la información procesada en la etapa de Detección (reportes de vulnerabilidades o incidentes, un evento sospechoso, etc.) se determina que una respuesta es necesaria, la información es pasada al proceso de Respuesta.
- Los procesos de Protección y Detección deben interactuar bajo la premisa de que si un incidente o una vulnerabilidad es detectada como consecuencia de una evaluación sobre la infraestructura (parte de un proceso de Protección), ésta deberá ser informada al proceso de Detección para su posterior tratamiento.
- Finalmente, el proceso de Respuesta deberá interactuar con los procesos de Preparación y de Protección, según corresponda. En cuanto a la relación con el proceso de Preparación, la información pasada por el proceso de Respuesta tiene como objetivo la mejora de procesos mediante la adopción de análisis Postmortem. Por otro lado, en cuanto a la relación con el proceso de Protección, la información pasada por el proceso de Respuesta tiene como objetivo generar las acciones de respuesta.

Resulta claro que la implementación de la GISe no solo requiere de la aplicación de tecnología para la resolución de incidentes de seguridad, sino que requiere del establecimiento de un plan de acción y de un conjunto de procesos que resulten consistentes, repetibles y de gran calidad.

- ***Consideraciones sobre la GIS***

Como capacidad global, la GIS deberá incorporar elementos de diferentes unidades operativas por lo que resultará imprescindible contar con un plan que defina las interacciones entre los componentes del sistema de tal manera de optimizar la forma en que los diferentes incidentes son manejados.

Como mínimo, el plan para la GIS deberá contemplar:

- Forma de integración de los procesos y estructuras existentes a la GIS,
- Fortalecimiento y mejora de las capacidades de cada uno de los componentes de tal manera que puedan manejarse adecuadamente los eventos de seguridad con el fin de garantizar la confidencialidad, la integridad y la disponibilidad de los activos de información vinculados a la I2C,
- Soportar y complementar los planes existentes de continuidad del negocio o de recuperación de desastres siempre que resulte apropiado,
- Complementar y enriquecer las políticas de negocios y de TI vinculadas con aspectos de seguridad,
- Extender al máximo el alcance de los sistemas de comando y control, establecer roles y responsabilidades e incorporar facilidades de trazabilidad de actividades,
- Conformar la GIS como parte de la estrategia global de protección, y
- Contemplar el establecimiento de procesos para:
    - detectar y clasificar eventos,
    - categorizar y priorizar,
    - notificar y comunicar,
    - analizar y responder,
    - colaborar y coordinar, y finalmente
    - mantener y por trazar eventos e incidentes en base a registros.

- ***Implementación de la GIS***

Los procesos y las tareas desarrollados en la GIS en el marco de PI2C deben contemplar desde el inicio una perspectiva global que permita integrar a todos los actores independientemente del sector al que pertenezcan en base a conceptos de Ingeniería correspondientes a las áreas de Seguridad de la Información y Resiliencia de Sistemas. Desarrollar tal perspectiva requiere que se identifiquen perfectamente cada uno de los siguientes componentes del sistema:

- Los objetivos de negocio de cada componente de las I2C,
- Las áreas intervinientes en la capacidad de GIS,
- La forma de implementación de las comunicaciones entre áreas, contemplando siempre las singularidades por sector,
- Los mecanismos de interacción entre áreas,
- Los esquemas de ejecución de acciones en el marco de las diferentes áreas operativas,
- La forma en la que se relacionará cada uno de los procesos con el modelo global de la GIS,
- Los mecanismos de intercambio de información, y finalmente,
- Los métodos de coordinación de las diferentes acciones.

El primer paso en vías de la implementación de una capacidad la GISe consiste en identificar a las organizaciones, áreas y recursos humanos apropiados para cada tipo de procedimiento involucrado y hacerlas parte del sistema en base a un esquema de roles y responsabilidades perfectamente definido. La selección del personal idóneo para formar parte del GIS es quizás la tarea más desafiante del proyecto. El propósito de cada grupo operativo involucrado en la GIS debe ser cuidadosamente planeado y documentado. Es importante que todos los procesos que vayan a ser incorporados al sistemas de GIS puedan ser modelados mediante diagramas de procesos con el fin de abstraer los componentes esenciales para su análisis. El proyecto de implementación para la GIS requiere de la definición de flujo de trabajo o workflows que

especifiquen de manera simple y clara como un incidente fluye por el modelo, es decir; por cada uno de sus procesos de tal manera que pueda definirse claramente quién lleva adelante cada tarea del plan, de que manera, en que orden y con que requerimientos de tiempo. Los flujos de trabajo evidencian las interacciones y las dependencias entre las tareas y las actividades de un proceso. Realizar un mapa del sistema de GIS en base a la modelización de su estructura permite obtener una visión de alto nivel de todas las actividades, de los roles y de las responsabilidades, de la tecnología, de las interfaces y de las dependencias que se dan en todo proceso de respuesta a incidentes; y como estos se relacionan y dependen unos de otros. Es esencial que se defina un sub proceso Forense a través del cuál se genera análisis postmortem de todos los incidentes clave con el objetivo de mejorar las estrategias de protección de la infraestructura y las políticas y procedimientos de seguridad y respuesta. Es recomendable ejecutar ejercicios de simulación periódicamente para asegurar que todos los involucrados sepan como reportar los incidentes y finalmente, como responder, sobre todo en contextos de crisis.

- ***GIS como formador de valor para la PI2C***

En síntesis, el modelo de GIS puede constituirse en un componente clave en la PI2C ya que permite desarrollar e implementar un conjunto de procesos de seguridad consistentes y confiables destinados a soportar la identificación, detección, análisis y respuesta a incidentes de seguridad en base a una serie de procesos de calidad soportados por personas, tecnologías de la información y las comunicaciones de manera eficiente y sostenible.

Desde un punto de vista estratégico y funcional, la GIS ayuda a establecer las garantías necesarias que permiten asegurar que la I2C seguirá operando de tal manera que pueda alcanzar su misión, incluso en presencia de riesgo operativo producto de fallas internas de los sistemas, de acciones accidentales o deliberadas de personas internas o externas, o de eventos externos. La misión final de la GIS consiste en garantizar "Resistencia Operacional" a la I2C de la Nación en base a la colaboración entre los sectores público y privado, y a un adecuado marco de gestión del riesgo vinculado principalmente a tareas de Gestión de Seguridad (GS), de Continuidad del Negocio y Recuperación de

Desastres (CN/RD), y finalmente de las operaciones asociadas a las áreas de TI. La GIS establece las bases sobre las cuales, independientemente del sector y del área del que se trate, se pueda trabajar en conjunto para sostener el concepto de resistencia operativa.

2.8 CONSIDERACIONES GENERALES SOBRE LEGISLACIÓN

A raíz de los problemas vinculados a la protección de la Infraestructura Crítica debe pensarse en la adopción de una legislación apropiada que permita garantizar la integridad, confidencialidad y disponibilidad de la misma. En el contexto de PI2C, los aspectos jurídicos deberán acompañar a la ciencia de la Seguridad de la Información con el objetivo común de lograr la seguridad de los ciudadanos y el bienestar económico del país.

Es necesario que los países comprendan la necesidad de crear una conciencia y una cultura asociados a la Seguridad de la Información, la cual será de ayuda para entender las implicancias relacionadas a las amenazas crecientes y poder ayudar a protegerlas legalmente, estableciendo funciones legislativas legítimas. Debido al carácter distribuido de muchas de los 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. [2.4]

Un claro ejemplo es la "Cumbre Mundial sobre la Sociedad de la Información" (CMSI), allí se reconocieron los riesgos reales y significativos planteados por

una seguridad inadecuada en I2C. En esta cumbre, los líderes mundiales y los gobiernos allí reunidos designaron a la ITU (Unión de Telecomunicación Internacional) como el organismo dedicado a la creación de normas de seguridad en la utilización de las TIC. La ITU provee un conjunto de herramientas legislativas que ayudan a establecer normas legales en el mundo, relacionadas con la Ciberseguridad.

La ITU lanzó la "Agenda sobre Ciberseguridad Global" (GCA de las siglas en Inglés de Global Cibersecurity Agency), con la colaboración de gobiernos, industrias, organizaciones regionales, 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, con el objetivo de proponer estrategias globales en base a trabajos e iniciativas existentes, generando mayor confianza y seguridad en la sociedad para la utilización de las TIC.[2.7]

La GCA tiene siete objetivos estratégicos principales basados en las cinco áreas de trabajo siguientes:

I. *Medidas Legales:* Estrategias para desarrollar un marco legislativo del cibercrimen, el cual sea operable y aplicable internacionalmente.

II. Medidas Técnicas y de procedimiento: Estrategias par desarrollar un marco de trabajo para protocolos de seguridad, estándares, esquemas aplicables a software y Hardware.

III. Estructuras Institucionales: Estrategias globales para la creación de estructuras políticas e institucionales contra el cibercrimen. Los sistemas deberán predecir, detectar, responder y gestionar la crisis ante un incidente.

IV. Construir Capacidades: Estrategias globales para crear mecanismos de creación de capacidades humanas e institucionales en los puntos I, II y III. Con el fin de aumentar la conciencia, transferir los conocimientos, y colocar a la Ciberseguridad en la agenda de los gobiernos.

V. Cooperación Internacional: Proponer un marco de trabajo para el

diálogo internacional, la cooperación y la coordinación al momento de abordar las ciberamenazas.

A partir de estas áreas, los objetivos estratégicos para desarrollar el marco legal son :

1. Elaborar estrategias para desarrollar un modelo legislativo del Cibercrimen, que sea aplicable en el mundo, y que interopere con medidas legislativas nacionales e internacionales.
2. Elaborar estrategias globales para la creación de estructuras organizacionales y políticas relacionadas con el cibercrimen.
3. Desarrollar una estrategia para establecer los mínimos criterios de seguridad y acreditar esquemas aplicados al hardware y software.
4. Desarrollar estrategias de creación para un marco global mirando, cuidando y respondiendo a incidentes, asegurando una correcta coordinación con las nuevas iniciativas y si hubiera, con las existentes.
5. Desarrollar una estrategia global para la creación de un sistema de identidad digital genérico y universal, necesitando estructuras organizacionales para asegurar el reconocimiento de credenciales digitales a través de distintas áreas geográficas.
6. Desarrollar una estrategia global para facilitar la construcción de capacidades humanas e institucionales reforzando el conocimiento y la habilidad en todos los sectores y áreas.
7. Proponer un marco global con múltiples colaboradores, teniendo como estrategia la cooperación internacional, el diálogo y la coordinación en todas las áreas participantes.

Desarrollar legislaciones adecuadas dentro de una marco jurídico resulta un factor esencial para combatir el ciberdelito. Se requiere la elaboración de leyes penales, ante actos criminales como el fraude informático, la denegación de servicios, acceso ilegal, violaciones del derecho de la propiedad intelectual, usurpación de identidad, pornografía infantil.

En este sentido, en nuestro país la 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 y aplica tanto al sector público como al privado. Se encarga de proteger aspectos de Privacidad.

Por otro lado, la Ley 26.388 establece una reforma del Código Penal en materia de Delitos Informáticos por medio de la derogación y modificación de algunos incisos introducidas por el art. 32 de la Ley 25.326 al Código Penal.

Dicha ley aplica penas a delitos como:

- *La pornografía y exhibición infantil:* Comercio, publicación, facilitación, divulgación o distribución, de actividades sexuales explícitas a menores de edad.
- *y La Violación de Secretos y de la Privacidad:* Acceso indebido, apoderación y publicación de una comunicación electrónica, cartas, documentos. Acceso a un sistema o dato restringido sin el correspondiente permiso. Violación y modificación a sistemas de confidencialidad y banco de datos personales. Alteración del normal funcionamiento de un sistema informático o la transmisión de datos. [2.11]

Si bien existen leyes aplicables a actos cometidos fuera de ambientes de las TIC, éstas mismas leyes en muchas oportunidades no son aplicables al ámbito cibernético. Se necesitarán herramientas e instrumentos jurídicos necesarios para investigaciones en el ciberdelito. Como se especificó anteriormente, las amenazas pueden originarse en cualquier lugar del mundo, enmascarando la identidad del autor tras la red, por tal motivo, las herramientas de investigación no serán las mismas usadas en delitos comunes, y las leyes necesitarán asistencia jurídica mutua, para aplicarse en el lugar de origen del delito.

No todos los sistemas jurídicos del mundo reconocen los potenciales abusos de las nuevas tecnologías, por lo tanto no incluyen las modificaciones necesarias en las actuales leyes penales nacionales. En base a esto resulta fundamental comprender la creciente complejidad introducida por las TIC y trabajar para realizar los ajustes jurídicos pertinentes.

El proceso de ajuste consta de tres etapas:

- En la primera etapa se deberá reconocer la actividad delictiva asociada a las nuevas tecnologías. Se necesitará de autoridades nacionales competentes que cuenten con departamentos específicos calificados para investigar ciberdelitos , como por ejemplo el "CERT Coordination Center" (Equipo de respuesta de emergencias en sistemas computacionales y redes de EE:UU) que funciona en la Universidad de Carnegie Mellon, Equipos de respuesta a incidentes informáticos en organismos privados, etc.
- La segunda etapa consiste en identificar los problemas en el Código Penal, necesarios para garantizar eficaces bases jurídicas. Se necesita comparar situaciones dispuestas jurídicamente, con los nuevos tipos de delitos. Las leyes existentes pueden cubrir delitos que no actúen sobre la cibernética.
- La tercera etapa consiste en redactar una nueva legislación. Tomando como punto de partida las experiencias anteriores, puede resultar difícil para las autoridades nacionales llevar a cabo este proceso de redacción relativo a los ciberdelitos sin la cooperación internacional.

Sin la armonización internacional de disposiciones jurídicas y penales, luchar contra el ciberdelito será de gran dificultad debido a la incompatibilidad de legislaciones propias de cada país. En consecuencia, el trabajo en conjunto sobre las leyes nacionales genera un beneficio enorme ya que permite reutilizar la experiencia de otros países y contar con asesoría jurídica de expertos internacionales.[2.8]

2.9 REFERENCIAS CAPÍTULO 2

[2.1] Introduction to Critical Infraestructure Assurance - What is CIIP.pdf

[2.2] Comunicación EU - Las infraestructuras críticas de información como soporte para el crecimiento económico y social.pdf) -

http://eur-lex.europa.eu/Notice.do?checktexts=checkbox&val=493232:cs&pos=1&page=1&lang=en&pgs=10&nbl=1&list=493232:cs,&hwords=&action=GO&visu=#texte

[2.3] http://www.melani.admin.ch/dokumentation/00123/00124/01109/index.html?lang=en&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1ad1IZn4Z2qZpnO2Yuq2Z6gpJCDdIF6fmym162epYbg2c_JjKbNoKSn6A--

[2.4] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf

[2.5]http://www.wired.com/threatlevel/2010/01/national-archives-data-breach/

[2.6] http://www.wired.com/threatlevel/tag/cybersecurity/

[2.7] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html

[2.8] http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.117.5890

[2.9] América prepares for 'cyber war' with China

http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/06/15/wcyber115.xml

[2.10] Information Operations Roadmap (DOD 2003)

http://information-retrieval.info/docs/DoD-IO.html

[2.11] Ley de Delitos Informáticos

http://infoleg.mecon.gov.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

http://www.segu-info.com.ar/boletin/boletin-113-080607.htm

[2.12] http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-s.pdf

Cybersecurity Guide for Developing Countries

http://www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf

[2.13] C Y B E R S P A C E T H R E A T S A N D V U L N E R A B I L I T I E S - Cyberspace Threats and Vulnerabilities.pdf

[2.14] http://www.construirydecorar.com/scripts/areaservicios/noticia/nota_rubro.asp?IdSeccion=6&IdNota=9199&IdRubro=79

[2.15]https://www.mi5.gov.uk/output/threat-levels.html

http://www.dhs.gov/xabout/laws/gc_1214508631313.shtm

http://www.dhs.gov/files/programs/Copy_of_press_release_0046.shtm

[2.16] Critical Infrastructures- Vulnerabilities, Threats, Responses. - Critical Infrastructures- Vulnerabilities, Threats, Responses.pdf

[2.17] http://www.aguasdelcolorado-lp.com.ar/index.html

http://www.s21sec.com/descargas/scada.pdf

http://www.monografias.com/trabajos11/sisco/sisco.shtml

[2.18] http://www.galeon.com/hamd/pdf/scada.pdf

[2.19] http://www.inl.gov/featurestories/2006-09-28.shtml

[2.20] http://www.dhs.gov/xabout/laws/gc_1214508631313.shtm#1

https://www.mi5.gov.uk/output/threat-levels.html

http://www.dhs.gov/files/programs/Copy_of_press_release_0046.shtm

[2.21]http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/prep_activities/ppp_worshop/index_en.htm

http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/impl_activities/index_en.htm

[2.22] Plan Nacional de Gobierno Electrónico – Decreto 378/2005.

http://www.argentina.gov.ar/argentina/portal/documentos/decreto378.pdf

[2.23] http://www.melani.admin.ch/

[2.24]http://webstore.iec.ch/preview/info_isoiec13335-1%7Bed1.0%7Den.pdf

CAPÍTULO 3

3 PI2C EN EL MUNDO

3.1 ESTADOS UNIDOS DE AMÉRICA (EEUU)

Se puede decir que Estados Unidos de América es el primer país que ha desarrollado y demostrado especial interés en el tema de PI2C.

La seguridad nacional fue reconocida como una responsabilidad del gobierno federal con esfuerzos y colaboración militar, políticas externas y aportes de la comunidad, la PI2C es vista como una responsabilidad compartida, que requiere la coordinación de acciones a través de varios sectores y que deberán ser llevadas a cabo a través de iniciativas de desarrollo de políticas.

El Departamento de Seguridad Interna o "DHS", siglas en Inglés de "Departament of Homeland Security", es una de las principales agencias públicas que existen en Estados Unidos, realiza asistencia a la presidencia con el objetivo de proteger al país y a sus Infraestructuras Críticas.

El DHS posee dos oficinas:

- Oficina de Protección de Infraestructura y
- Oficina de Comunicaciones y Ciberseguridad.

Dentro del DHS, existe una División de Seguridad Cibernética Nacional o "DSCN", siglas en Inglés de "Departament Security Cibernetic National", que trabaja con la colaboración de entidades públicas, privadas, nacionales e internacionales para asegurar el ciberespacio Americano. El objetivo de ésta división es el de construir y mantener un sistema de respuesta eficaz en el ciberespacio y poder llevar a cabo un programa de prevención de riesgo cibernético para la protección de la Infraestructura Crítica.[3.1]

A través de la DSCN, se implementaron los siguientes programas de trabajo:

- El Sistema de respuesta en el Ciberespacio Nacional
- La Red Federal de Seguridad
- Los programas de manejo de riesgos cibernéticos

Estos tres programas intentan asegurar y proteger la Infraestructura Crítica los 365 días del año, por ejemplo a través de sistemas coordinados, de protocolos, de respuestas a incidentes, de priorizar los recursos, de evaluación de riesgos que puedan producirse en departamentos o agencias públicas o privadas, intentando asegurar el espacio cibernético.[3.2]

Las principales responsabilidades del DHS sobre Ciberseguridad se nombran a continuación:

- Desarrollar un plan nacional para la PIC, incluyendo la seguridad cibernética.
- Desarrollar alianzas y coordinarlas con otras agencias federales, estatales, gobiernos locales y el sector privado.
- Mejorar y potenciar sectores públicos y privados los cuales intercambien información cibernética acerca de ataques, amenazas y vulnerabilidades.
- Desarrollar y mejorar las capacidades de alerta y ciber análisis a nivel nacional.
- Proporcionar y coordinar una correcta planificación de respuestas a incidentes y recuperación.
- Identificar y evaluar las vulnerabilidades y amenazas cibernéticas.
- Apoyar los esfuerzos para reducir las vulnerabilidades y las amenazas cibernéticas.
- Promover y apoyar la investigación y desarrollo para fortalecer la seguridad del ciberespacio.
- Promover el conocimiento y la divulgación.
- Fomentar la capacitación y certificación.
- Mejorar la seguridad cibernética en los ámbitos federales, estatales y locales.
- Reforzar la seguridad del ciberespacio internacional.

- Integrar la seguridad cibernética con la seguridad nacional.[3.1]

La Oficina de Responsabilidad Gubernamental o "GAO", siglas en inglés de "Goverment Accountability Office", es capaz de descubrir las amenazas cibernéticas a sistemas de información y a infraestructuras críticas y está en condiciones de definir las deficiencias que estos sistemas e IC poseen como vulnerabilidades.

La GAO realiza informes y reportes periódicamente a distintos organismos, entes y agencias dedicadas a resolver problemas en seguridad de la información y en especial al US-CERT (Equipo de respuesta a emergencias computacionales Americanas), a quién se hará referencia mas adelante, para que puedan implementar programas de seguridad y prevención.

En los últimos años, la GAO ha realizado una serie de recomendaciones para mejorar la seguridad cibernética de las infraestructuras críticas. En sus reportes brinda información acerca de los Orígenes de las Amenazas, Tipos y Técnicas de ataques.

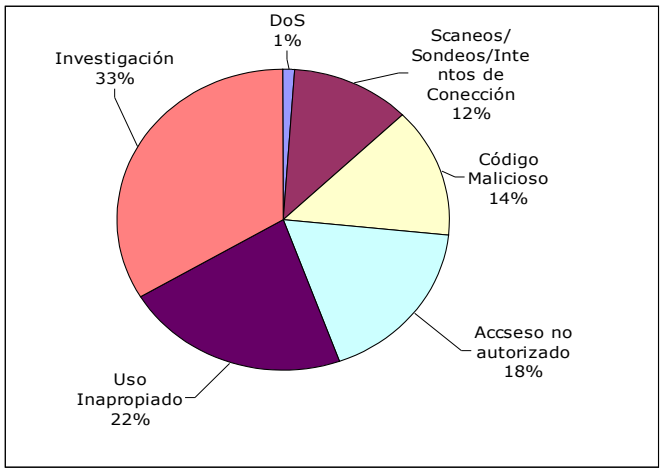


Figura 3.1: Porcentaje de Incidentes Informados al US-CERT entre 02/2006 y 02/2008, discriminado por Categoría

Las vulnerabilidades en los sistemas de información que se han encontrado y se repiten frecuentemente se han clasificado en cinco categorías:

1) Control de acceso, el cual asegura el acceso autorizado a individuos que puedan leer, escribir o borrar datos.

2) El manejo de control de configuración, que proporciona seguridad al Hardware y software implementado y que controla los cambios de configuración de los mismos.

3) Separación de tareas, el cual reduce los riesgos individuales y puede realizar acciones no apropiadas sin ser detectadas.

4) Continuidad de Funciones, éstas planean y mantienen la prevención de fallas en equipos de computación garantizando su funcionamiento.

5) Manejo de la seguridad de la información, ésta proporciona una amplia estructura para asegurar la comprensión de los riesgos y la eficacia de los controles seleccionados y propiamente llevados a cabo.

Estas cinco categorías han sido detectadas por 24 agencias de seguridad en el año 2008, dando un informe anual del siguiente reporte.[3.8]

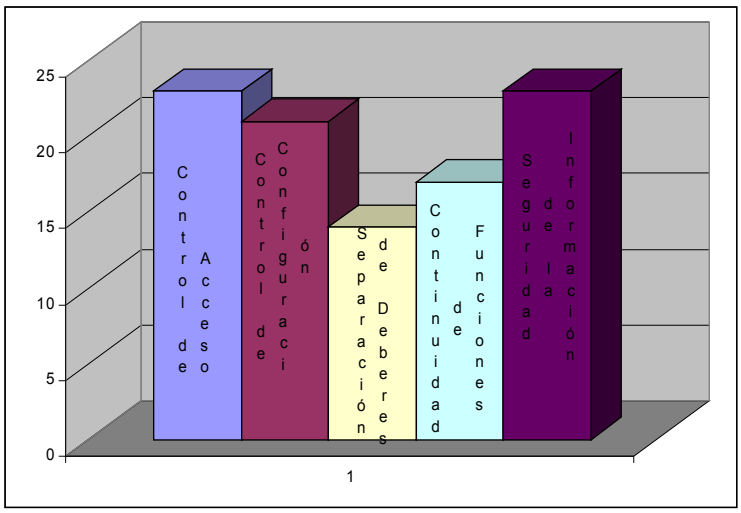


Figura 3.2: Número de Agencias que reportaron debilidades en cada Categoría en el año 2008

Además de las agencias mencionadas anteriormente hay otras Iniciativas y Políticas tales como:

- Estrategia Nacional para asegurar el Ciberespacio (NSSC-national Strategy to Secure Cyberspace)
- Estrategia Nacional para la Protección Física de la Infraestructura Critica y recursos claves.

- Plan de Protección de Infraestructura Crítica Nacional y Plan de Sectores Específicos.
- Estrategia Nacional para la información compartida.

Tanto la DHS, la GAO, como la CCIPS, siglas en inglés de "Computer Crime and Intellectual Property Section" son agencias públicas.

También hay varias Agencias Público-Privadas que trabajan en mutua colaboración como las siguientes:

- ✔ Comité Inter agencia DHS
- ✔ Programa de información de protección de Infraestructura Crítica (PCI2P)
- ✔ ISACs – Centro de análisis e información compartida
- ✔ InfraGard
- ✔ NCSA – Alianza Nacional de Ciberseguridad
- ✔ PCIS – Seguridad para la IC de la sociedad.
- ✔ CSCSWG – Grupo de Trabajo a través del sector de Ciberseguridad.
- ✔ I3P – Instituto para la Protección de la Infraestructura de Información

Y las entidades de prevención de incidentes, que se originaron en USA, pero que recorren el mundo con una filial propia de cada país en el que se desarrolle son:

- ✔ CERT (Equipo de respuesta a emergencias computacionales)
- ✔ US-CERT (Equipo de respuesta a emergencias computacionales Americanas).[3.2]

El CERT es un equipo que permanece constantemente actualizado en cuanto a la información que posee sobre los incidentes que ocurren con más frecuencia, intercambian información con diferentes agencias del mundo y está conformado por un equipo de expertos en Ciberseguridad.[3.2]

Estados Unidos define como infraestructuras críticas los siguientes sectores y recursos:

- Tecnología de la Información
- Telecomunicaciones
- Productos químicos
- Instalaciones Comerciales
- Represas
- Reactores nucleares comerciales, materiales y residuos
- Activos de Gobierno
- Sistemas de Transporte (Tránsito, Transporte aéreo, marítimo, terrestre / ferrocarril y sistemas de tuberías)
- Servicios de Emergencias
- Servicios postales y logísticos
- Agricultura y Alimentos
- Salud pública y asistencia sanitaria
- Sistemas de agua y tratamiento de aguas residuales

3.2 REINO UNIDO (UK)

El gobierno del Reino Unido (UK), tiene como objetivo proteger a la Infraestructura crítica Nacional o "CNI", siglas en Inglés de "Critical National Infrastructure" la cual comprende los elementos claves de la Infraestructura nacional, siendo todas aquellas prestaciones de servicios esenciales para todo el país. Sin estos elementos, el Reino Unido podría sufrir grandes consecuencias incluyendo severos daños económicos, perturbaciones sociales y pérdidas de vidas humanas.

Los servicios críticos esenciales para el bienestar del país dependen de la CNI. Son considerados nueve sectores que ofrecen "servicios esenciales" resumidos a continuación:

- Comunicaciones (comunicaciones de datos, comunicaciones de voz fija, correo, Información Pública, Comunicaciones Inalámbricas)
- Servicios de Emergencias (Ambulancias, Bomberos y grupos de rescate, guardacostas, policía)
- Energía (Electricidad, Gas natural, petróleo)
- Finanzas (Gestión de Activos, Servicios Financieros, Banca de Inversión, mercados, Banca minorista)
- Alimentación (Producir, importar, procesar, distribuir)
- Gobierno y Servicios Públicos (Gobierno Central, Regional y Local; parlamentos y legislaturas, Justicia, Seguridad Nacional)
- Seguridad Pública (químicos, biológicos, radiológicos y nucleares)
- Terrorismo (multitudes y eventos de masas)
- Salud (Atención de Salud, Salud Pública)
- Transporte (aéreo, ferroviario, marino, o carreteras)
- Sistema de Agua (agua corriente, alcantarillado)

El Gobierno británico tiene como objetivo proteger a la CNI, de dos tipos de amenazas:

– Los ataques físicos contra las instalaciones físicas y

– Los ataques electrónicos contra computadoras o sistemas de comunicaciones.

Entre los planes más relevantes que se han desarrollado se encuentra el denominado "Estrategia Nacional de Información de Garantía" el cual tiene como objetivo desarrollar e investigar tres tipos de amenazas:

- Los ataques físicos contra las instalaciones físicas y electrónicas
- Los ataques contra sistemas computacionales o sistemas de comunicaciones
- La seguridad de los datos.

Dando como resultado información acerca de la existencia de estas amenazas producidas en el país.

Por otro lado la "CSIA", siglas en inglés de "Central Sponsor for Information Assurance", brinda información acerca de las buenas prácticas para mantener los sistemas seguros. Es el encargado de prestar ayuda al gobierno tratando de mantener actualizados los datos y realizando las siguientes tareas necesarias para el aseguramiento de la información:

- Habilitar al gobierno a entregar los servicios públicos a través de un apropiado uso de las TIC.
- Fortalecer la seguridad nacional protegiendo los sistemas de información de posibles riesgos.
- Reforzar el bienestar económico y social, el gubernamental y los negocios, en beneficio de las TIC y lo que éstas aportan.

El gobierno Británico ha puesto en práctica monitoreos, guías y entrenamientos para ofrecer la confidencialidad, la disponibilidad, y la integridad de los datos en todos los sistemas de información.

En el Reino Unido, además de las agencias mencionadas destinadas a brindar seguridad, existe una que es la principal responsable de la PI2C y es la llamada Home Office [3.7].

La Home Office está organizada por:

- El Ministro del Interior, el cual se encarga de supervisar todo el trabajo realizado en la Home Office
- Y el Secretario Permanente, el cual es un alto funcionario que se encarga de asegurar de que se cumplan los objetivos fijados por el Ministro del Interior.

La Home Office posee:

- Un pequeño centro estratégico, que asesora a la junta del Ministerio del Interior sobre la estrategia y dirección y la asignación de recursos.
- La Oficina para la Seguridad y contra el Terrorismo, que trabaja con otros departamentos y agencias para asegurar una respuesta eficaz y coordinada a la amenaza terrorista.
- El servicio contra el delito y la vigilancia de grupo, que funciona a través del servicio de policía y otros colaboradores.
- Los servicios profesionales, que incluyen asesoramiento jurídico y apoyo a las comunicaciones, y los programas y apoyo a la gestión del proyecto.

Además de la Home Office, una serie de otros departamentos desempeñan un papel importante en la protección de los diversos sectores de la CNI los cuales contribuyen con recursos y experiencias sobre la PI2C en el Reino Unido. Estas contribuciones son coordinadas por el Centro para la Protección de la Infraestructura Nacional o "CPNI", siglas en inglés de "Centre for the Protection of the National Infrastructure"[3.11].

La CPNI se formó el 1 de febrero de 2007, es el responsable de absorber casi todas las funciones del Centro de Coordinación de Seguridad de la Infraestructura Nacional o "NISCC", siglas en inglés de "National Infrastructure Security Coordination Centre" y del Centro de Asesoramiento de Seguridad Nacional o "NSAC", siglas en inglés de "National Security Advice Centre", entre ellos anteriormente se encontraba el servicio UNIRAS (que proveía de cuidado temprano y servicios de alertas a todo el sector empresarial del Reino Unido) y

el CERT (que se encarga de recibir, revisar y responder a los informes de incidentes de seguridad informática, brindando asesorías y actividades relacionadas).

El NISCC es la organización interdepartamental más importante que trata con la PIC/PI2C. Posee fuertes lazos con el sector privado y la comunidad académica. Es el ente encargado de definir cuales son las Infraestructuras Críticas de este país[3.9]

Aunque UNIRAS ha sido dado de baja, la CPNI ha seguido ejecutando un CERT para sus socios del sector privado que operan con elementos de la infraestructura nacional. Este servicio que asesora sobre la forma de gestionar la respuesta a incidentes y produce advertencias en materia de seguridad se llama el Equipo Combinado de Respuestas a Incidentes de Seguridad o "CSIRTUK", siglas en inglés de "Combined Security Incident Response Team". [3.11]

Los avisos del CSIRTUK están disponibles en [3.12]

La gestión de riesgos de seguridad evoluciona aprendiendo a través de la experiencia de los demás, en consecuencia, a través de el CSIRTUK, el CPNI conoce acerca de los posibles vulnerabilidades de seguridad, incidentes o eventos, ya sea en las esferas de seguridad electrónica, física o personal de las organizaciones de la infraestructura nacional.

Toda la información obtenida es tratada como confidencial, y en caso de identificar individuos u organizaciones, será eliminada.

El CSIRTUK proporciona un punto central para reportar incidentes de seguridad y para recibir asesoramiento y orientación ante estas situaciones concernientes a la seguridad.

La política de la Protección de Información de Infraestructura Crítica, es desarrollada por departamentos gubernamentales, por la CPNI, la Secretaría de Contingencia Civil o "CCS", siglas en inglés de "Central Sponsor for Information Assurance", la oficina de seguridad y la sede del ministerio del interior y comunicaciones o "GCHQ", siglas en inglés de "Government Communications Headquarters".

La responsabilidad de prestar asesoramiento sobre la protección física de la CNI se comparte entre el CPNI, el Servicio de Seguridad, y la policía. La CSIA tiene a su cargo la estrategia de aseguramiento de la información más amplia en el Reino Unido que trata todos los aspectos .

La CSIA, tiene a su cargo la estrategia de aseguramiento de la información más completa. El gobierno también colabora con el sector privado y comparten información entre ambos.

Tanto la CPNI como la CCS, son agencias públicas.

Las asociaciones Público-Privadas en este país son:

- ✔ CPNI's Public-Private Partnerships
- ✔ The Information Assurance Advisory Council
- ✔ The British Computer Society,
- ✔ The Internet Security Forum,
- ✔ The National Computing Centre,
- ✔ The Internet Watch Foundation,
- ✔ The Confederation of British Industry,
- ✔ The Institute of Information Security Professionals,
- ✔ European Information Society Group,
- ✔ Royal United Services Institute,
- ✔ Chatham House.

Y las agencias destinadas a la prevención de incidentes son:

- ✔ CSIRTUK (Equipo de respuestas a incidentes con seguridad combinada)
- ✔ GovCertUK
- ✔ MODCERT (Equipo de Respuesta de emergencias cibernéticas del Ministerio de Defensa) [3.14]
- ✔ GetSafeOnline

3.3 ALEMANIA

Según la constitución Alemana, dice que los estados alemanes deben garantizar la seguridad pública y el orden, por este motivo, es fundamental identificar claramente las Infraestructuras Críticas (IC).

Los siguientes son los sectores de IC definidos en este país:

- Transporte y Tráfico
- Energía
- Materiales Peligrosos
- Telecomunicaciones y Tecnologías de la Información
- Sistemas financiero, monetario y de seguros
- Suministro (incluido el abastecimiento de agua, suministro de alimentos, atención médica, de emergencia y los servicios de rescate)
- Las agencias del Gobierno, Administración y Justicia
- Medios de comunicación, centros de investigación y los bienes culturales

En Alemania existen tres documentos considerados como hitos iniciales con respecto a la PIC y a la PI2C:

- En el 2005, el *Plan Nacional para la Protección de la Infraestructura Crítica o* "NPSI", siglas en inglés de "National Plan for Information Infraestructure Protection" y
- En el 2008, "*Protección de la Infraestructura Crítica"* (Conceptos de Protección) y "*Protegiendo Infraestructuras Críticas"* (Riesgos y manejos de Crisis: una guía para empresas y gobiernos)

El *Plan Nacional para la Protección de la Infraestructura Crítica o* "NPSI", siglas en inglés de "National Plan for Information Infraestructure Protection", tiene como objetivos la prevención y protección de infraestructuras críticas (IC), la elaboración de respuestas efectivas a incidentes sobre las TIC y el

mantenimiento y asistencia a todo lo relacionado con la seguridad de las TIC en base a estándares internacionales.

Esta guía de seguridad implementada, sirve para diseñar medidas y asegurar un alto nivel de seguridad en las TIC a través de la administración federal.

Los documentos "*Protección de la Infraestructura Crítica"* (Conceptos de Protección) y "*Protegiendo Infraestructuras Críticas"* (Riesgos y manejos de Crisis: una guía para empresas y gobiernos), son documentos desarrollados con la cooperación de el Ministerio del Interior Federal o "BMI", siglas en inglés de "Federal Ministry of the Interior", la Oficina Federal de Protección Civil y ayuda en catástrofe o "BBK", siglas en inglés de "Federal Office of Civil Protection and Disaster Assistance" y la Agencia Criminal de la Policía Federal o "BKA", siglas en inglés de "Federal Criminal Police Agency", todas éstas son agencias públicas, además de poseer la colaboración del sector privado, con el fin de crear una guía de recomendaciones y medidas de protección ante ataques terroristas, actos delictivos y desastres naturales, toman como base los conceptos de la PIC que servirán de apoyo en momentos de crisis, siendo de especial interés para sectores empresariales y gubernamentales.

La agencia gubernamental principal que coordina estos planes de protección, y que está a cargo de la gestión y comunicación de seguridad informática es la *Oficina Federal de Seguridad de la Información*, conocida como "BSI", siglas en inglés de "Federal Office for Information Security", ésta forma parte del ministerio del interior y de la carta orgánica del país, es la autoridad máxima correspondiente a Ciberseguridad.

La BSI junto con la BMI, trabajan en conjunto ofreciendo actividades que relacionan el sector público y el privado, desarrollando aplicaciones y estrategias relacionadas con la PI2C. Existe una estrecha colaboración internacional, principalmente con el DHS de Estados Unidos y la cooperación multilateral de otras organizaciones.

Alemania participa activamente en el programa europeo EPCIP (Programa europeo para Protección de la Infraestructura Crítica), en actividades PI2C internacionales y en los proyectos y grupos de trabajo como el SCADA y el E-SCSIE (Intercambio de Sistemas de Información de Control).

Entre las Agencias Públicas ya mencionadas se suman:

- ✔ BMWi (Ministerio Federal de Economía y Tecnología)
- ✔ Agencia Federal de Redes

Las Agencias Público-Privadas que existen son:

- ✔ Plan de implementación PIC
- ✔ Alemania Segura en la Web
- ✔ Iniciativa D21

Con respecto a la legislación en cuanto a la Protección de Infraestructura Crítica, en Alemania existe una ley de libertad y des regularización en el mercado de las telecomunicaciones, también está en vigencia la ley de Firma digital a partir de 2007, y en el Código Penal están plasmados los artículos que penalizan los ataques a sistemas de información, espionaje, alteración e Interceptación de datos y sabotaje, ofreciendo un amplio espectro de seguridad con bases sólidas en entidades concretas y leyes aplicables.[3.3]

3.4 BRASIL

Los problemas focalizados sobre Internet y las telecomunicaciones generan un gran impacto sobre la economía, la política y el sector social, por ello este país ha desarrollado un organismo regulador federal de las telecomunicaciones capaz de comprender los riesgos y las amenazas, desarrollar herramientas, metodologías y software como soporte.

Este organismo es llamado Anatel, siglas en portugués de "Agência Nacional de Telecomunicações", el cual es aplicado a infraestructuras de telecomunicaciones basado en cuatro puntos principales:

- Contextualización
- Estrategia de Protección
- Conjunto de Metodologías
- Herramientas de software para apoyar los puntos anteriores.

Estas metodologías incluyen el desarrollo de herramientas para la identificación de las infraestructuras críticas (de la información y comunicación).

La seguridad de la información ya no se entiende como un problema exclusivo de los sectores relacionados con las TIC, o de una organización en particular, de la industria o del gobierno, más bien se entiende que consiste en un conjunto de estrategias regionales y globales que facilitan una respuesta organizada a las amenazas y las vulnerabilidades asociadas con el uso de la tecnología.

Para crear políticas de seguridad, las TIC deben estar unidas y operando sobre una red segura y con seguridad en las comunicaciones.

El Comité Directivo en Internet de Brasil o "CGI", siglas en inglés de "Brazilian Internet Steering Committee", es un comité creado por el Ministerio de Ciencia y Técnica, conformado por diversos miembros de entidades representantes del gobierno, proveedores de servicios de Internet, comunidad académica, usuarios y operadores.

El comité es el encargado de tres grupos de trabajo:

- Grupo de la ingeniería de red
- Grupo de la seguridad informática. y
- Grupo de la formación de recursos humanos

Estos grupos trabajan con el fin de proporcionar información técnica, administrativa y operativa y sugerir recomendaciones sobre las decisiones realizadas por la comisión.

Por otra parte, se coordinan varios proyectos en áreas de fundamental importancia para el funcionamiento y desarrollo de Internet. Para ejecutar estas actividades, se ha creado el Centro de información de redes Brasileras llamado "NIC.br".

El programa gubernamental E-GOV (Gobierno electrónico), desarrollado a partir del año 2000, puso en práctica tareas muy importantes para el desarrollo, y la seguridad, garantizando canales de comunicación seguros, implementando software libre e integrando actividades electrónicas con diferentes niveles del gobierno.

En cuanto a la prevención y manejo de incidentes, se creó el Centro de tratamiento de incidentes de seguridad en redes de computadoras de la administración pública federal, llamada "CTIR Gov", siglas en portugués de "Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal".

Ésta es una entidad subordinada por la Oficina de Seguridad institucional de La presidencia de la República o "GSI", siglas en portugués de "Gabinete de Segurança Institucional" que tiene la responsabilidad de coordinar respuestas a incidentes de computadoras, asegurar el intercambio de información entre

diferentes puntos y ofrece servicios reactivos y pro-activos ante las distintas amenazas producidas.

El papel principal de Anatel se convirtió en el de la regulación, concesión y supervisión de los servicios de telecomunicaciones en el país. Entre las cuestiones más importantes se encuentran los mecanismos para lograr la cooperación entre el gobierno brasileño y el sector privado. Los primeros pasos se han tomado para abordar la seguridad cibernética, problemas que enfrenta el sector de infraestructuras de telecomunicaciones de Brasil mediante la cooperación entre empresas privadas y este cuerpo regulatorio.
Por otra parte, la metodología propuesta y utilizada por Anatel con el fin de identificar las infraestructuras críticas se utilizó con el propósito de definir las zonas críticas de las infraestructuras de telecomunicaciones de Brasil.

Aunque el gobierno brasileño no ha definido formalmente las Infraestructuras Críticas, son siete los temas considerados extraoficialmente que representan dichos sectores críticos:

- Seguridad Pública
- Sistema Energético
- Sistema Financiero
- Sistemas de Transportes
- Abastecimiento de agua
- Salud Pública
- Telecomunicaciones

Las Agencias Público-Privada más importantes son la SERPRO, además de la CTIRGov y el CERT.br.

En cuanto a la prevención de incidentes se encuentran

- ✔ Alianza de Honeypots Brasileras

- ✔ RNP – National Education and Reserch Network
- ✔ CAIS – Security Incidents Attendance Center

Con respecto a la legislación Brasilera, el 2000 fue un año intenso de elaboración de políticas de seguridad de la información en las áreas de:

- Tratamiento y clasificación de la información
- Investigaciones en las tecnologías
- Acreditación y certificación de productos y servicios
- Seguridad en la interoperabilidad de servicios
- Establecimiento de normativas acerca de la Criptografía
- Confidencialidad, integridad y disponibilidad de los sistemas de información.

También se crearon leyes para el Cibercrimen, definido como una violación a los datos, al acceso no autorizado y oculto a los sistemas de información. Asegurando la privacidad de las personas tal como lo dice en su constitución nacional.

El código penal, también hace su aporte con dos artículos referidos a la seguridad de la información.[3.3]

3.5 RUSIA

En los últimos años, Rusia ha progresado en intentar mejorar la Protección de la Infraestructura Crítica, la seguridad nacional y el bienestar económico. Todas éstas áreas dependen del grado de seguridad aplicada a la información y al progreso tecnológico.

La protección de los intereses nacionales están definidos en la *Doctrina de la Seguridad de la Información de la Federación Rusa*, basada en el documento del G8[2.13] . La seguridad de la información en Rusia, no sólo incluye la seguridad técnica, sino también salvaguardar los secretos de estados.

La *Doctrina de la Seguridad de la Información de la Federación Rusa*, define el contexto de los intereses nacionales y la evaluación de amenazas a la sociedad y al estado, asegurando la información, desarrollando sistemas efectivos, monitoreos de objetos críticos y prediciendo situaciones de emergencias.

Involucra áreas políticas, protección de datos, privacidad personal, copyright, hacking, acceso a la información y secretos de estados, participando internacionalmente con otras entidades para realizar intercambio de información.

La doctrina define el estado de protección de los intereses nacionales en la información definida para los intereses individuales, sociales y del estado.

Está compuesta por cuatro capítulos:

1. Seguridad de la Información
2. Métodos para asegurar la información
3. El aseguramiento de la Información acerca de las políticas de estado y las medidas prioritarias para implementarlas.
4. Bases organizacionales para el aseguramiento de la información.

Los instrumentos jurídicos constituyen uno de los tres enfoques de seguridad de la información mencionada en las medidas de la doctrina técnica y económica. Además, el documento subraya la amenaza de ataques contra la

infraestructura de información Rusa y las amenazas de gobiernos extranjeros con técnicas de guerra de información contra Rusia. Además, se presta especial atención al desarrollo de los sistemas de telecomunicaciones, la integridad de los recursos de información, el reconocimiento basado en el espacio y la guerra electrónica.

Rusia ha centrado todos sus esfuerzos en proteger de posibles amenazas a las infraestructuras de la información Rusa, usando técnicas, desarrollando buenos sistemas de telecomunicación y recursos para proteger la integridad de la información de los Ciberataques.

El proyecto Rusia Electrónica, fue elaborado como un Plan estratégico de desarrollo. Está coordinado por el ministerio de telecomunicaciones e informatización. La base de este programa fue la de reducir un retraso económico en el país, desarrollando una alta tecnología en este sector, el cual fuera posible enriquecerlo con un alto nivel de productividad para así mejorarlo en el sector público. La combinación de implementación y tecnologías, facilitaron poder restringir el nivel de acceso a la información, expandiendo las oportunidades de desarrollo de tecnologías de la Información y de sus usuarios.

Rusia Electrónica, está dirigido a áreas de infraestructura de Internet, e-gobierno, e-educación, regulación del medio ambiente y al marco institucional.

Para lograr estos objetivos se crearon leyes efectivas sobre las Tecnologías de la Comunicación e información (TIC); asegurar una comunicación abierta e interactiva entre los cuerpos de estados, las agencias, y compañías que utilizan tecnologías TIC; han provisto de entrenamientos y actualizaciones a profesionales de las TIC e incentivaron a desarrollar empleos en esas actividades; y han desarrollado la infraestructura de redes en telecomunicaciones (acceso a librerías electrónicas, archivos, base de datos, información científica) para el estado, organizaciones e instituciones educacionales.

Los sectores críticos definidos en este país son:

- Economía
- Política Interior y Exterior
- Ciencia y Tecnología
- Sistemas de Comunicación e Información de Estado
- Defensa
- Justicia
- Respuesta a Desastres e incidentes

Hay varias Agencias, las cuales aportan propuestas, metodologías y ayuda al sector de protección de IC. Las pertenecientes al sector Público son:

- ✔ Convención de seguridad de la federación Rusa
- ✔ Servicio Federal de Seguridad de la Federación Rusa (FSB)
- ✔ Servicio de Guarda Federal de la Federación Rusa.
- ✔ Servicio federal técnico y control de exportación.
- ✔ Ministerio de Información, Tecnologías y Comunicaciones

Y las de carácter Público-Privadas son:

- ✔ Asociación Rusa de Redes y Servicios o RANS siglas en inglés de "Russian Association of Networks and Services"
- ✔ PRIOR

En Rusia, al igual que en otros tantos países, se encuentra la Entidad de prevención de incidentes, RU-CERT (Equipo de respuesta a emergencias computacionales Rusas) además de RIPN, siglas en inglés de Russian Institute for Public Networks, RBNet, siglas en inglés de Russian Backbone Networks y NOC, siglas en inglés de RBNet Network Operation Center.

Con respecto al marco legal, Rusia incluye tres puntos principales,

- Seguridad legal sobre la seguridad de la información.
- Seguridad legal sobre la seguridad de la infraestructura de la información.
- Seguridad legal sobre el estado legal de la seguridad de la información de los sujetos.

Todos están basados en la Constitución de la Federación Rusa, el Código Criminal de la Federación Rusa, las leyes de la Federación Rusa sobre los medios de comunicación masivos y otras leyes, asegurando normas correctas sobre las organizaciones, actividades relacionadas a la información y otros cuerpos de estados.

3.6 INCIATIVAS INTERNACIONALES

Las consecuencias que generan las fallas en las infraestructuras críticas, provocan daños de un impacto incalculable. Ya son muchos los países que han tomado medidas de prevención, entendiendo la gravedad que las vulnerabilidades existentes pueden provocar en los sistemas críticos, tratando así de proteger tanto a éstas como a la sociedad.

Es necesario que se promueva una cultura global de Ciberseguridad y de prevención en las TIC, que puedan desarrollarse e implementarse prácticas tratando de identificar los temas comunes y especialmente los problemas y las fallas más comunes, contando con la colaboración y cooperación de equipos internacionales expertos, analistas e investigadores, que deriven de orígenes académicos, del sector privado o del sector gubernamental.[3.6]

Entre las iniciativas más relevantes a nivel mundial, las cuales han servido y continúan actualmente siendo utilizados como bases de proyectos se encuentran los siguientes:

Manual PI2C Internacional

El Manual de PI2C Internacional es una publicación que ofrece una recopilación y análisis de Ciberseguridad de catorce países, proporciona una apreciación global de los problemas de mayor importancia en el área de PI2C, sirve como un trabajo de referencia para la comunidad interesada, y tiene como base una amplia investigación compilando el material pertinente de cada país.[3.3]

ITU (Unión de Telecomunicación Internacional)

La Unión de Telecomunicación Internacional o "ITU", siglas en inglés de "International Telecommunications Union", es el organismo especializado de la Organización de las Naciones Unidas (ONU), encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras.

Miembros de la ITU han tenido un rol importante en materia de Ciberseguridad, a través de varias resoluciones, decisiones, programas y recomendaciones junto a los representantes del gobierno, la industria, el sector académico e instituciones de investigación, regional e internacional.

La ITU proporciona un foro donde se exponen los diversos puntos de vista en los temas de Ciberseguridad y ciberdelincuencia, con el objetivo de llegar a un entendimiento común entre los países participantes sobre la forma en que estos inconvenientes pueden ser abordados.

La sede de esta organización se encuentra en Ginebra (Suiza).

La ITU está compuesta por tres sectores:

- ✔ ITU-T: Sector de Normalización de las Telecomunicaciones
- ✔ ITU-R: Sector de Normalización de las Radiocomunicaciones
- ✔ ITU-D: Sector de Desarrollo de las Telecomunicaciones de la ITU

En general, la normativa generada por la ITU está contenida en un amplio conjunto de documentos denominados *Recomendaciones*, agrupados por Series. Cada serie está compuesta por las Recomendaciones correspondientes

a un mismo tema.

Aunque en las *Recomendaciones* nunca se "*ordena*", solo se "*recomienda*", su contenido, a nivel de relaciones internacionales, es considerado como mandatario por las Administraciones y Empresas Operadoras.

La Agenda sobre Ciberseguridad Global (GCA) es un marco de la ITU para la cooperación internacional a fin de proponer soluciones para mejorar la confianza y la seguridad en la sociedad de la información. Se basará en las iniciativas nacionales y regionales para evitar la duplicación de trabajo y fomentar la colaboración con todos los interlocutores.

En esta agenda GCA, se definieron cinco temas:

- Medidas legales
- Medidas técnicas y de procedimientos
- Las estructuras orgánicas
- Capacidad de construcción
- Cooperación Internacional

Estos cinco temas constituyen el informe estratégico global internacional, a partir del cual se elaborarán las siguientes estrategias:

- ✔ El desarrollo de un modelo legislativo del cibercrimen
- ✔ La creación de estructuras políticas nacionales y regionales sobre cibercrimen
- ✔ Establecer criterios de seguridad y esquemas de acreditación para aplicaciones de sistemas de software.
- ✔ La creación de un marco legal para observar, prevenir y responder a un incidente.
- ✔ La creación de un sistema genérico universal de identidad digital
- ✔ La facilidad de construir capacidades humanas e institucionales
- ✔ La cooperación internacional, dialogo y coordinación

Es fundamental que cada país incluya el desarrollo de:

- Entender el cibercrimen desde una perspectiva global
- Definir una estrategia de Ciberseguridad a nivel nacional
- Desarrollar el conocimiento público de los desafíos ante el cibercrimen y la Ciberseguridad (los problemas económicos, políticos, sociales, técnicos y legales)
- Promover una cultura en Ciberseguridad (información sobre riesgos, propagación de simples recomendaciones como usar sistemas seguros, reducir las vulnerabilidades evitando situaciones peligrosas)
- Entrenar e informar sobre tecnologías de comunicaciones y problemas de seguridad y proveer de normas legales pertinentes.
- Desarrollar la educación en Ciberseguridad
- Proponer un marco de trabajo unificado el cual incluya una muestra humana, regulatorio, organizacional, económica, técnica y operacional acerca de la Ciberseguridad.
- Colocar estructuras organizacionales como soporte estratégico en distintos puntos del país.
- Crear puntos de alertas regionales que provean de información técnica y asistencia con al cibercrimen y a los riesgos en seguridad.
- Crear leyes efectivas a nivel nacional e internacional.
- Desarrollar prácticas aceptables de protección y reacción
- Establecer cooperación efectiva y promover la cooperación y coordinación a nivel nacional e internacional.
- Forzar a los proveedores de tecnologías a mejorar la seguridad de sus productos y servicios.[3.4]

G8

Se denomina G8 o "Grupo de los ocho" a un grupo de países industrializados del mundo cuyo peso político, económico y militar es muy relevante a escala global. Está formado por 8 países del mundo, Estados Unidos de América,

Reino Unido, Canadá, Francia, Alemania, Italia, Japón y Rusia. Fue creado en 1975 como el G7, en ése momento eran siete los países que lo conformaban.

Anualmente los representantes de estos países se reúnen en las llamadas Cumbres del G8. La finalidad de las reuniones es la de analizar el estado de la política y las economías internacionales e intentar aunar posiciones respecto a las decisiones que se toman en torno al sistema económico y político mundial y a las las relaciones con los países en desarrollo.

A partir de esta base inicial en la agenda de las cumbres realizadas, se ha ampliado considerablemente los temas a tratar incluyendo los micro-económicos tales como el empleo y la autopista de la información, los problemas internacionales como el medio ambiente, la delincuencia y las drogas, y una serie de temas políticos y de seguridad que van desde derechos humanos a través de la seguridad regional hasta el control de armas, enfocándose en el estado actual del terrorismo en el mundo.

En Julio del 2000, en Okinawa, se realizó el "Okinawa Charter on Global Information Society" o la llamada "Carta constitucional","GIS" o siglas en inglés de "Global Information Society", en la cual se enumeran importantes principios para el desarrollo de una información global, acompañada por acciones para prevenir el cibercrimen y crear un ciberespacio seguro en la sociedad mundial.

En este aspecto, la carta constitucional de Okinawa se refiere a las Pautas de la Organización para la Cooperación y el Desarrollo Económico u "OECD", siglas en inglés de "Organisation for Economic Co-operation and Development", en lo que se refiere a la Seguridad de Sistemas de Información. En esta Carta constitucional, el G8 pidió al sector público y al privado a realizar los mayores esfuerzos para unir la información internacional. [3.13].

En el documento "G8 Principios para proteger las Infraestructuras de Información Crítica", del 2003, se da información esencial acerca de las infraestructuras críticas, como protegerlas efectivamente, y como los países deben protegerlas de daños y posibles ataques. Además de poder identificar las causas y el origen de los mismos, sugiriendo una apropiada intercomunicación, coordinación y cooperación entre los distintos países.

Son once los puntos que se enumeran, incentivando a los países a considerarlos en el desarrollo de sus estrategias para reducir los riesgos de Infraestructuras Críticas.[3.5]

OECD (Organización para la Cooperación y el Desarrollo Económico)

La OECD es una organización de cooperación internacional, compuesta por 34 estados, cuyo objetivo es coordinar sus políticas económicas y sociales. Fue fundada en 1960 y su sede central se encuentra en el Château de la Muette, en la ciudad de París, Francia.

En la OECD, los representantes de los países miembros se reúnen para intercambiar información y armonizar políticas con el objetivo de maximizar su crecimiento económico y ayudar a su desarrollo y al de los países no miembros. Se considera que la OECD agrupa a los países más avanzados y desarrollados del planeta, siendo apodada como el club de países ricos.

Los 34 países miembros que lo conforman son: Australia, Austria, Bélgica, Canadá, Chile, República Checa, Dinamarca, Estonia, Finlandia, Francia, Alemania, Grecia, Hungría, Islandia, Irlanda, Israel, Italia, Japón, Corea, Luxemburgo, México, Países Bajos, Nueva Zelanda, Noruega, Polonia, Portugal, República Eslovaca, Eslovenia, España, Suecia, Suiza, Turquía, Reino Unido y Estados Unidos

Los principales objetivos de la OECD son:

- ✔ Contribuir a una sana expansión económica en los países miembros, así como no miembros, en vías de desarrollo económico.
- ✔ Favorecer la expansión del comercio mundial sobre una base multilateral y no discriminatoria conforme a las obligaciones internacionales.
- ✔ Realizar la mayor expansión posible de la economía y el empleo y un progreso en el nivel de vida dentro de los países miembros, manteniendo la estabilidad financiera y contribuyendo así al desarrollo

de la economía mundial.

La OECD, ha desarrollado artículos sobre los temas de seguridad de sistemas de información y redes, incluyendo a las infraestructuras de información crítica. Actualmente la organización está comprometida a dar lucha contra el cibercrimen y contra el uso de software malicioso. Produce constantemente informes analíticos, estadísticas, y guía de políticas, declaraciones y recomendaciones para ayudar al sector gubernamental y al empresarial a desarrollar políticas consistentes en seguridad de la información, relevando el conocimiento público de mayor importancia, para desarrollar una cultura de seguridad en la sociedad.

Las Pautas de la OECD incluyen los siguientes principios complementarios a la política y a los niveles operacionales:

1) ***Conocimiento***: Los partícipes deben ser consciente de la necesidad de segurizar los sistemas de información y redes y de las opciones para reforzar la seguridad;

2) ***Responsabilidad***: Todos los partícipes son responsables sobre la seguridad de los sistemas de información y redes;

3) ***Respuesta***: Los partícipes deben actuar oportunamente previniendo y respondiendo ante diferentes incidentes;

4) ***Ética***: Los partícipes deben respetar los intereses legítimos de los otros;

5) ***Democracia***: La seguridad de sistemas de información y redes debe ser compatible con los valores esenciales de una sociedad democrática;

6) ***Valoración de riesgo***: Los partícipes deben dirigir la valoración de riesgo;

7) ***Plan de Seguridad y aplicación***: Los partícipes deben incorporar la seguridad como un elemento esencial en los sistemas de información y redes;

8) ***Dirección de la Seguridad***: Los partícipes deben adoptar un acercamiento comprensivo en la dirección de seguridad;

9) ***Re-evaluación***: Los partícipes deben repasar y deben imponer la seguridad en los sistemas de información y redes, y realizar las modificaciones apropiadas a las políticas de seguridad, prácticas, medidas, y procedimientos. [3.10]

3.7 REFLEXIONES SOBRE PI2C EN EL MUNDO

En los países vistos en este capítulo, se puede observar que las Infraestructuras Críticas definidas de cada uno de ellos son similares. Es decir, que si bien cada país posee una cultura diferente, el concepto de Infraestructura Crítica no varía.

Las agencias de seguridad y las entidades u organismos encargados de determinar cuales son las infraestructuras críticas de cada país, se originan en ámbitos provenientes del sector público, del sector privado y de una fusión de ambas con la colaboración del sector académico.

Un factor interesante e importante es que los países se integren globalmente y posean una mutua y estrecha colaboración con organismos de escalas mundiales.

No es bueno que los países se mantengan aislados y no intercambien información con el resto, es por ello que si cada uno aporta sus experiencias, sus éxitos, sus inquietudes y sus formas de resolver cada uno de los problemas en materia de amenazas a Infraestructuras Críticas, consecuentemente se generará un sólido lazo para enfrentar los peligros existentes. De esta forma es posible combatir el cibercrimen y mantener el ciberespacio cubierto.

Los referentes más importantes son Estados Unidos y países europeos como Reino Unido o Alemania, poseen muchos años desarrollando planes de protección y cuidando sus IC.

Las convenciones mundiales en las cuales participan activamente aquellos países con planes de protección bien definidos, con organismos, agencias y entidades destinadas específicamente a prestar servicios de seguridad, necesitan estar actualizados constantemente, es por ello que a lo largo del año

realizan reuniones periódicas, si bien se puede tener una comunicación OnLine en cualquier momento o cuando la situación lo requiera con miembros de cada sector, es de suma importancia formalizar y registrar las acciones en forma concreta. Es necesario el debate y el diálogo para acordar ideas y llegar a un punto en común. Y como medida final, una vez que se estipulan las medidas acordadas, es necesario que sean publicadas y dadas a conocer, ya sea a las entidades que conformaron dichas medidas, como a el resto de entidades y agencias mundiales.

Hoy en día, la seguridad es un bien que beneficia a todos, es por ello que actitudes mezquinas no integran el conjunto de las buenas prácticas.

3.8 REFERENCIAS CAPITULO 3

[3.1] **http://www.dhs.gov/xabout/structure/editorial_0839.shtm**

[3.2] **http://www.dhs.gov/files/programs/gc_1158611596104.shtm1**

[3.3] INTERNATIONAL CIIP HANDBOOK 2008 / 2009

(INTERNATIONAL CIIP HANDBOOK 2008 – 2009CIIP_HB_08.pdf)

[3.4] ITU - **http://www.itu.int/osg/csd/**

http://www.itu.int/ITU-D/cyb/
http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf

[3.5] **http://www.usdoj.gov/ag/events/g82004/G8_CIIP_Principles.pdf**.

[3.6] A COMPARATIVE ANALYSIS OF CYBERSECURITY INITIATIVES WORLDWIDE
(Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide)

[3.7] **http://www.homeoffice.gov.uk**

[3.8] GAO-09-661T Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk - U.S. Government Accountability Office, **http://www.gao.gov**

[3.9] **www.NISCC.GOV.UK**,

[3.10] OECD - **http://www.oecd.org/**

[3.11] CPNI - **http://www.cpni.gov.uk**

http://www.cpni.gov.uk/Products/advisories.aspx

[3.12] **http://www.cpni.gov.uk/rss/advisories.xml**

[3.13] Okinawa Charter **www.g8.utoronto.ca/summit/2000okinawa/gis.htm**,

[3.14] **http://www.first.org/members/teams/modcert/**

CAPÍTULO 4

4 ESTADO DE LA PI2C EN ARGENTINA

4.1 ESTADO DE SITUACIÓN ACTUAL EN ARGENTINA

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 Actual del país en la materia.

- Argentina no cuenta actualmente con leyes ni legislación en materia de Protección de Infraestructura Crítica ni de Protección de Infraestructura de Información Crítica [4.1].

- Ante la necesidad de elaborar una Política de Seguridad de la Información para el Sector público, se inicia en Septiembre de 2003 desde una convocatoria de la ONTI[4.7] (Oficina Nacional de Tecnologías de la Información) de la SUBSECRETARÍA DE GESTIÓN PÚBLICA de la JEFATURA DE GABINETES DE MINISTROS, a distintos organismos de la Administración pública para conocer opiniones sobre las estrategias de seguridad. A partir de esto surge la necesidad de que los organismos cuenten con una Política de Seguridad escrita, conformando un grupo de trabajo para la redacción de un Modelo de Política de Seguridad tomando como base la norma ISO/IRAM 17799.

  Una vez redactado el Modelo, se deja a consideración de los organismos nacionales, para luego publicarlo en la página de políticas del ArCERT[4.3].

  En Diciembre del 2004 la Jefatura de Gabinete de Ministros aprueba por Decisión Administrativa 669/2009 y por la Resolución SGP Nº 45/2005, a partir de allí se comienza con la difusión de la Norma y el Modelo.[4.5]

  Esto consiste en:

  - Dictar o adecuar la Política de Seguridad de la Información

- Conformar un Comité de Seguridad de la Información
- Asignar las responsabilidades en materia de Seguridad de la Información

Esta normativa y modelo está dirigida a:

- Administración Nacional.
- La Administración Central.
- Los Organismos Descentralizados (incluidos los de la Seguridad Social).
- Entes Públicos excluidos del punto anterior
- Cualquier Organización estatal no empresarial con autarquía financiera, personería jurídica y patrimonio propio, donde el Estado Nacional tenga el control mayoritario del patrimonio o de la formación de decisiones.[4.2]

➢ El ArCERT[4.3] fue creado en 1999 con el objetivo de centralizar y coordinar esfuerzos para el manejo de incidentes de seguridad que afecten los recursos informáticos de la Administración Pública Nacional. Además cumple funciones de gestor de información y de formador de Recursos Humanos.

ArCERT comenzó a funcionar en mayo de 1999 en el ámbito de la Subsecretaría de la Gestión Pública siendo sus principales funciones:

- Centralizar los reportes sobre incidentes de seguridad ocurridos en la APN (Administración Pública Nacional) y facilitar el intercambio de información para afrontarlos.
- Proveer un servicio especializado de asesoramiento en seguridad de redes.
- Promover la coordinación entre los organismos de la APN para prevenir, detectar, manejar y recuperar incidentes de seguridad.

- Actuar como repositorio de toda la información sobre incidentes de seguridad, herramientas y técnicas de defensa

- No hay estándares técnicos ni manuales de procedimientos de carácter oficial con excepción de un *Manual de Seguridad en Redes* del año 1999 y el *Manual del Instructor en Seguridad de la Información* el cual fue elaborado con el propósito de ayudarlo a desarrollar una propuesta de capacitación y/o concientización en Seguridad de la Información[4.4].

- Resultados del Foro de Telecomunicaciones: "2011 Argentina Conectada" [4.6] . El Ministerio de Planificación Federal, Inversión Pública y Servicios realizó en el mes de abril de 2011 el *Foro de Telecomunicaciones 2011 Argentina Conectada*, con el objetivo de difundir políticas públicas desarrolladas en materia de comunicaciones. La convocatoria estuvo dirigida a diferentes actores sociales que representen todos los sectores involucrados.

- Plan Nacional de Gobierno Electrónico. El 27 de abril de 2005, a través del *Decreto 378/2005* se aprobaron los lineamientos estratégicos que han de regir el *Plan Nacional de Gobierno Electrónico* y los *Planes Sectoriales* para el uso intensivo de las TIC en los organismos de la Administración Pública Nacional (APN). Este portal del estado nacional incluye:

  - Guía de Trámites
  - Directorio de Funcionarios
  - Sistema de Atención en Línea

- La Ley 25.326 de *Protección de Datos Personales* sancionada en el 04/10/2000 ofrece un marco legal para la protección integral de los datos de las personas y aplica tanto al sector público como al privado, esta ley se encarga esencialmente de proteger la Privacidad de las

personas[4.8].

- La Ley 26.388 de *Delitos Informáticos*, sancionada el 04/06/2008 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[4.9] .

- *Normativa de Firma Digital,* ha sido publicada el 12 de febrero en el Boletín Oficial. La Decisión Administrativa N° 06/2007 define los mecanismos que la Subsecretaría de la Gestión Pública utilizará para otorgar y revocar las licencias a quienes deseen operar como Certificadores Licenciados (entidades públicas o privadas) en el marco de la Ley 25.506, para expedir certificados digitales con validez jurídica. Se establecen los pasos a seguir para obtener una licencia, así como los estándares tecnológicos que deben cumplirse en el marco de la Infraestructura Nacional de Firma Digital y otros aspectos vinculados al licenciamiento.

4.2 MUESTREO DE LA REALIDAD A NIVEL NACIONAL

Para obtener una visión de la situación actual en materia de conceptos e ideas acerca de PI2C, se realizaron cinco encuestas a personal jerárquico de diferentes organismos de gobierno y del sector privado.

En primer lugar se confeccionó un cuestionario para todos los entrevistados que consta de tres partes:

- PARTE I: Seguridad de la Información (SI)
- PARTE II: Infraestructura Crítica (IC)
- PARTE III: Organización y Coordinación

En la PARTE I se realizan preguntas relacionadas a conocimientos sobre características técnicas en TIC y Sistemas de Información.

La PARTE II se refiere a conocimientos sobre IC e I2C y sobre Protección de IC y Protección de I2C.

Y en la PARTE III las preguntas son acerca del conocimiento de la Organización y la Coordinación en los organismos que ellos representan, a quién/es acuden en caso que ocurra un incidente y cuál es su opinión sobre la implementación de un Plan de PI2C.

Las encuestas fueron realizadas telefónicamente, acordando previamente dicha entrevista.

ENTREVISTADOS:

- ***Prog. LUCAS ANZOÁTEGUI***

Responsable del área de Seguridad Informática del Instituto de Seguridad Social (ISS) - SEMPRE.

Departamento Desarrollo Subgerencia de Sistemas

Santa Rosa (La Pampa)

- ***DANTE MORENO***

Jefe de Planificación de TIC del Centro de Sistematización de Datos (Ce.Si.Da.) del Ministerio de Hacienda y Finanzas del Gobierno de la provincia de la Pampa

Santa Rosa (La Pampa)

- ***Lic. MARÍA MARTA CORTESINI***

Aguas del Colorado

Gerente Comunicaciones y Servicios

Santa Rosa (La Pampa)

- ***Cnel. JUAN JOSÉ BENITEZ***

Jefe del Comando de Comunicaciones e Informática del Estado Mayor General del Ejército

- ***FERNANDO GRAFFIGNA***

Jefe del Área de Redes y Seguridad de la Municipalidad de Junín.

Pcia. De Buenos Aires.

CONCLUSIONES:

Luego de realizar el cuestionario a éstos cinco referentes a cargo de importantes instituciones en materia de seguridad, es posible extraer información acerca del estado de conocimiento y situación actual sobre seguridad y protección dejando en claro los siguientes puntos:

- ✔ Todos coinciden que las TIC son fundamentales para el crecimiento y el desarrollo económico y social de la nación, así como también representan un activo muy valioso para el sector que cada uno representa.

- ✔ Todos reconocen los términos de amenazas y riesgos los consideran parte de las TIC. También coinciden en que es sumamente necesario implementar estrategias de mitigación de riesgos en los sistemas de información.

- ✔ Si bien es importante desarrollar tareas de coordinación y colaboración en el contexto de seguridad de la información, algunos creen que es muy difícil poder llevarlas a cabo.

- ✔ Los entrevistados conocen los conceptos de IC, de I2C y los sectores que son alcanzados por las mismas.

- ✔ También conocen que es la PIC, la PI2C y son conscientes acerca de la importante necesidad de contar con estos planes de protección para evitar impactos no deseables en la sociedad.

- ✔ Cuando ocurre un incidente relacionado con las TIC todos recurren al Ar-CERT, algunos a proveedores de antivirus o a la ONTI y otros poseen sus propios métodos de solucionar los problemas ocasionados.

- ✔ Todos coinciden en que el Estado es el principal responsable de la Protección de la Infraestructura, porque éste es quien está a cargo de otorgar seguridad a los ciudadanos.

- ✔ Ninguno conoce un Plan de Protección de Infraestructura Crítica en el país y sólo algunos poseen conocimientos de proyectos.

- ✔ Si bien todos creen que el desarrollo de un plan es necesario y fundamental para proteger los activos del país, creen que puede llevar un tiempo considerable lograr implementarlo, tal vez porque aunar esfuerzos con distintos intereses puede resultar complicado.

- ✔ Todos conocen la relevancia del tema y de la necesidad de la existencia de un Plan de PI2C en el país y mostraron total disposición para colaborar con su desarrollo.

4.3 ENTREVISTAS

A) MODELO DE CUESTIONARIO

Ver **ANEXO I**

B) ENCUESTAS

Ver **ANEXO II**

4.4 REFERENCIAS CAPÍTULO 4

[4.1] Política de Seguridad de la Información. Decisión Administrativa 669/2004 de la Jefatura de Gabinete de Ministros.

- http://www.jgm.gov.ar/paginas.dhtml?pagina=303

[4.2] Modelo de Política de Seguridad de la Información de la Oficina Nacional de Tecnologías de Información (ONTI).

- http://www.arcert.gov.ar/politica/PSI_Modelo-v1_200507.pdf

[4.3] ArCERT - **http://www.arcert.gov.ar/**

[4.4] Manual de Seguridad en Redes, 1999 y Manual del Instructor en Seguridad de la Información

http://www.arcert.gov.ar/webs/manual/manual.htm

[4.5] Decreto 378/05 sobre la Decisión Administrativa JGM 669/04.

- http://www.enre.gov.ar/web/bibliotd.nsf/042563ae0068864b04256385005ad0be/725d3547f1852953032570590043619 4?OpenDocument

[4.6] Foro de Telecomunicaciones: "2011 Argentina Conectada".

- http://www.minplan.gov.ar/notas/515-foro-telecomunicaciones-2011-argentina-conectada
- http://www.minplan.gov.ar/notas/517-ministro-vido-inaugura-el-foro-telecomunicaciones-2011-argentina-conectada

[4.7] ONTI - http://www.sgp.gov.ar/contenidos/onti/onti.html

[4.8] Ley 25.322

- http://www.infoleg.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

[4.9] Ley 26.388

- http://infoleg.mecon.gov.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

CAPÍTULO 5

5 PLAN ESTRATÉGICO DE PI2C PARA ARGENTINA

5.1 VIABILIDAD DE PI2C EN ARGENTINA

Las sociedades modernas poseen cada vez más dependencia a las Tecnologías de la Información y la Comunicación las cuales le permiten permanecer interconectadas globalmente, ésto a su vez crea dependencias y riesgos a nivel nacional e internacional. Por este motivo es esencial mejorar la seguridad cibernética y la protección de Infraestructuras de Información crítica.

A nivel nacional esta responsabilidad debe ser compartida por parte de las autoridades gubernamentales, el sector público y el sector privado, exigiendo acciones coordinadas relacionadas con la prevención y la recuperación de incidentes. La cooperación y coordinación de éstos socios es fundamental para la formulación y aplicación de un marco nacional de seguridad cibernética y de PI2C.

En la Argentina, no se ha implementado aún algún Plan de PI2C ni de seguridad cibernética, por tal motivo y en los tiempos que corren es de suma importancia la concientización de los sectores involucrados y los esfuerzos por implementar definitivamente un marco de seguridad.

Al no existir precedentes en el país, la mejor forma de comenzar es mirar a los países que poseen la suficiente experiencia y desarrollo en esta temática.

5.2 PI2C: VISIÓN, MISIÓN Y OBJETIVOS

VISIÓN:

Desarrollar un Plan de PI2C que pueda ser implantado a nivel nacional, tratando que el sector público, el privado y el académico colaboren para tal fin. Un adecuado Plan de Protección de Infraestructura Crítica brindará seguridad a la ciudadanía en general en todos sus ámbitos.

MISIÓN:

Ofrecer a distintos grupos de clientes, desde propietarios y operadores de Infraestructura crítica hasta empresas y usuarios domésticos de Internet, protección y seguridad en las tecnologías de la información y la comunicación.

Disponer de las mejores técnicas de prevención, ofrecer información actualizada de amenazas y disponer del mejor personal calificado en experiencia en incidentes.

Bajar la cantidad de brechas de seguridad en las infraestructuras críticas del país.

OBJETIVOS:

- Establecer una red nacional de Protección de Infraestructura de Información Crítica.
- Lograr una vinculación a nivel Internacional y poder contar con el apoyo y la experiencia de otros países
- Disminuir el número de incidentes en infraestructuras críticas.
- Aumentar el nivel de interés de los sectores participantes (público, privado y académico) para evolucionar en el tiempo y obtener óptimos resultados.

5.3 MARCO GENERAL PI2C

El modelo de este Plan se basa en cuatro procesos o tareas fundamentales. Cada uno realiza actividades específicas, pero necesitan de la interacción mutua para poder realizarlas.

Los Procesos son:

- **Prevención y Alerta Temprana**
- **Detección**
- **Reacción**
- **Gestión de Crisis**

- **Prevención y Alerta Temprana**

Como su nombre lo indica, este proceso desarrolla tareas de prevención ante las amenazas existentes, es decir que se preparan y disponen tareas capaces de evitar o anticipar la ocurrencia de algún daño o pérdida de un recurso.

Aquí el objetivo principal es intentar reducir el número de violaciones de seguridad a las I2C. Si bien existen amenazas de todo tipo de complejidad y de diversos orígenes provocando múltiples tipos de incidentes, es necesario contar con suficientes medidas técnicas, con herramientas y adecuados conocimientos tecnológicos como para afrontar estos incidentes ya sean con medidas preventivas o con medidas reactivas. Siempre existen brechas de seguridad y es imprescindible estar preparados para poder controlar la situación.

Para llevar a cabo estas tareas, es necesario contar con una adecuada instrucción, entrenamientos, serie de recomendaciones y difusión de advertencias, de ejercicios y de consejos, los cuales puedan aplicarse para generar una alerta temprana en el momento oportuno ante amenazas concretas.

Un apoyo importante en este proceso es el sector académico porque cuenta con conocimiento en el tema y con grupos de investigación.

Es necesario que la unidad de PI2C se encuentre en una posición libre de intereses comerciales, ya que al trabajar en conjunto con distintos sectores (el apoyo del sector privado, el académico, los fabricantes de productos de software, las organizaciones no gubernamentales, los medios de comunicación) tiene el privilegio de manejar información reservada. Si la unidad se comporta de forma neutral ante todos sus socios, el plan podrá llevarse a cabo sin ningún tipo de suspicacia y podrá brindar sus servicios a quien lo necesite (desde el gobierno, las empresas, hasta el público en general).

- **Detección**

En este proceso es necesario desarrollar nuevas técnicas de identificación de ataques tan pronto como aparezcan. Por ejemplo, pueden producirse ataques físicos contra instalaciones reales o ataques electrónicos contra sistemas de comunicaciones.

Las amenazas, tanto las existentes como las nuevas que surjan, tiene que ser detectadas tan rápido como sea posible. Es muy amplio el abanico de amenazas que afectan a las I2C, van desde el fraude, la usurpación de identidad, los crímenes financieros, la Ingeniería social hasta ataques de denegación de servicios, Virus, Gusanos, Pishing, Caballos de Troya y Spam entre otros.

En principio, es imprescindible que los operadores de infraestructuras críticas presenten los reportes de incidentes a los cuales representan. Esta colaboración es necesaria para realizar las tareas de detección y de alerta temprana. La unidad de PI2C interactúa con una amplia red nacional e internacional de organizaciones que trabajan con problemas de protección y seguridad, contando con una enorme colaboración del equipo CERT, además de técnicos expertos en informática y en comunicaciones. Los servicios de inteligencia también colaboran ya que son quienes proveen la información necesaria acerca de nuevas organizaciones delictivas.

Un punto importante de la unidad es el manejo de la información. Al recolectar información sobre incidentes de los sectores públicos y privados, es fundamental generar "Confianza". El proceso de intercambio de información es básico, pero deben establecerse normas para mantenerla en estricta confidencialidad.

- **Reacción**

La capacidad de reaccionar ante un evento significa poder identificar el hecho y así posteriormente ejecutar una acción capaz de corregir, evitar o interrumpir el sistema atacado para preservar la información y minimizar el impacto.

En principio la unidad de PI2C no sólo se limita a implementar medidas y ayudas técnicas, sino que además debe proporcionar apoyo, asesoramiento y orientar sobre cómo enfrentar un incidente. Es importante recalcar que no ofrece las soluciones completas, sólo ofrece soporte de ayuda y asesoramiento que debe estar disponible en el momento que se lo requiera, es decir full time. Es sumamente importante que la reacción instrumentada por la unidad de PI2C sea rápida, ya que de ésto depende el impacto de un ataque, es el proceso que está más estrechamente vinculado al proceso de Gestión de incidentes de seguridad (GIS).

Para elegir la reacción adecuada, se debe realizar un análisis de incidentes apropiado, elaborando un informe final sobre el episodio ocurrido. Resulta de suma importancia que se confeccionen correctamente los informes de los hechos ya que servirán para planificar y poder agilizar el intercambio de información.

Para finalizar cabe aclarar que es importante diferenciar que el impacto producido por el incidente va a depender de la organización afectada ya que unas difieren de otras por su nivel de criticidad.

- **Gestión de Crisis**

La Gestión de Crisis, es un proceso que se dedicará a gestionar los problemas generados cuando se suscite un incidente. Esto significa que se ejecutarán actividades destinadas a minimizar los efectos causados por el episodio y se intentará que los sistemas retornen a su estado normal de funcionamiento

luego del accidente. Restablecer los sistemas a su estado original es una de las principales funciones de este proceso. Es por ello que la Gestión de Crisis debe estar bien diseñado ya que es de suma importancia en el Plan. Debe mantenerse actualizado constantemente organizando actividades, ejercicios, realizando entrenamientos y logrando que todos los involucrados en desarrollar tareas estén familiarizados con sus actividades, deberes y funciones. [4.1]

La Gestión de Crisis debe alcanzar un nivel de comunicación directo con las autoridades nacionales ya que es quien debe tomar las decisiones y alertarlas en momentos de crisis, debe estar inmerso en la estructura nacional de manejo de crisis.

La siguiente figura (5.1) muestra un resumen de los cuatro procesos del PI2C:

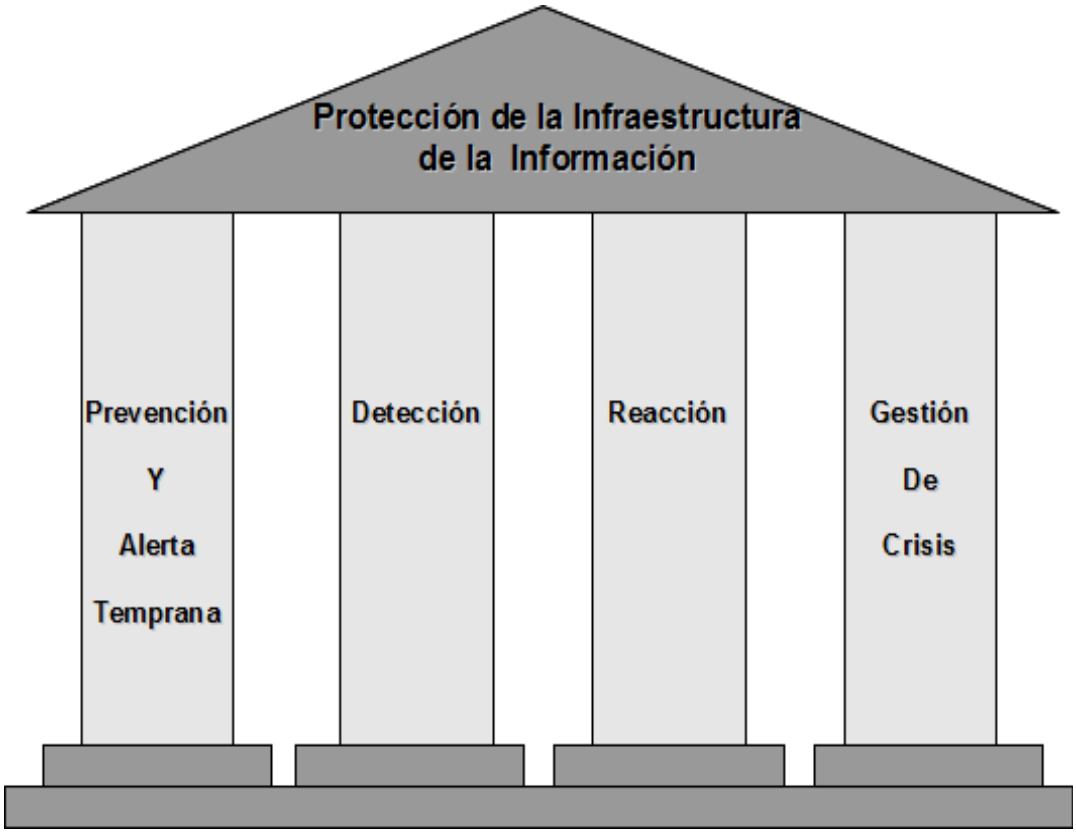


Figura 5.1: Los Cuatro Procesos de la PI2C

5.4 ARQUITECTURA Y COMPONENTES

Cada uno de los procesos nombrados en el punto 5.3 de este capítulo, posee diferentes características en cuanto a su organización y sus requerimientos técnicos y de análisis. También difieren en su estructura interna, su nivel de complejidad y el tipo de coordinación.

Cada proceso se interrelaciona con las demás, esta mutua colaboración es fundamental al momento de implementar el plan exitosamente. Cada una de las tareas será llevada a cabo por personal idóneo, con amplios conocimientos perteneciente al área en cuestión.

La unidad de PI2C debe disponer de tres equipos de trabajo necesarios para la organización y la ejecución de estas tareas:

1) La ***Dirección*** de la unidad de PI2C, que será una agencia Gubernamental, que provea liderazgo, estrategias y que tenga la capacidad de supervisar.

2) Un ***Centro de Análisis de Situación*** que será un centro de análisis de información con un equipo para realizar actividades técnicas, compuesto por personal del servicio de inteligencia.

3) Y una ***Unidad Técnica*** o equipo experimentado que va a estar formado por miembros del CERT nacional capaces de suministrar información técnica.

La ***Dirección*** del Organismo responsable de la PI2C, debe estar formada por autoridades de la administración pública. La PI2C se relaciona con una o varias de las agencias gubernamentales existentes. La posición de ésta debe ser un punto estratégico que le permita eludir obstáculos burocráticos y pueda acceder e interactuar con políticos responsables.

Quien lidere la Administración Directiva de la unidad de PI2C le será requerido poseer profundos conocimientos en Tecnologías de la Información y la

Comunicación (TIC) y en Protección de Infraestructura Crítica (PIC). También necesitará tener buen acceso a los sectores gubernamentales que lo rodean.

El objetivo principal es lograr resolver problemas organizativos, planificar en situaciones de emergencias, otorgar respuestas frente a desastres relacionados con la seguridad de los datos y servicios de Tecnología de la información y poder enfrentar a la ciberdelincuencia. Es de suma importancia que el sector privado tenga absoluta confianza en la Dirección porque será el encargado de manejar la información sensible que ésta le provea la cual deberá ser resguardada.

La interacción dada entre ambos sectores es a menudo difícil de llevar a cabo debido a que la "confianza" es un recurso fundamental, es por ello que se necesitan negociadores con la experiencia necesaria como para lograr coordinarlos. Esta necesidad de interacción y colaboración mutua será necesaria para cumplir con los objetivos de la Dirección, el sector privado le dará el material necesario como para poder realizar sus tareas con hechos concretos.

El ***Centro de Análisis de Situación*** es el encargado de la recolección y análisis de la información. Las rigurosa tarea de analizar la información está localizada en unidades específicas de servicios de inteligencia porque éstos cuentan con la habilidad de acceder a una amplia red de contactos nacionales e internacionales para obtener información acerca del cibercrimen.

Será importante que miembros de este Centro pertenezcan al servicio de inteligencia para actuar como intermediario entre las restantes unidades porque el Centro de Análisis reportará a la Dirección y a la Unidad Técnica la información recolectada para que cada una realice las tareas correspondientes a su área.

La ***Unidad Técnica*** debe estar lista para ayudar en casos de incidentes, además de participar activamente en la prevención mediante el suministro de información, advertencias y consejos. Esta unidad debe de asociarse con el CERT nacional. De esta manera, la unidad puede obtener la competencia

técnica, sin tener que construir su propio cuerpo de personal técnico. El CERT es el responsable de las cuestiones técnicas, debe estar listo en caso de incidentes y participar activamente en la prevención de los mismos. También suministra información, advertencias y consejos preventivos. Están diseñados como centros de conocimientos especializados a cargo de especialistas de información.

Los CERT pueden ser ejecutados por organismos independientes de unidades gubernamentales o por el sector académico. Los CERT ejecutados por unidades académicas son interesantes porque las universidades cuentan con personal dedicado a la investigación con los suficientes conocimientos científicos como para afrontar las distintas situaciones. Además las redes de universidades académicas son convenientes para la investigación y la cooperación con la unidad de PI2C.La unidad de PI2C debe cooperar con el CERT nacional, integrándolo como socio a la unidad.

La composición tripartita y el grado de relación entre ellas puede reflejarse en el siguiente gráfico (figura 5.2):

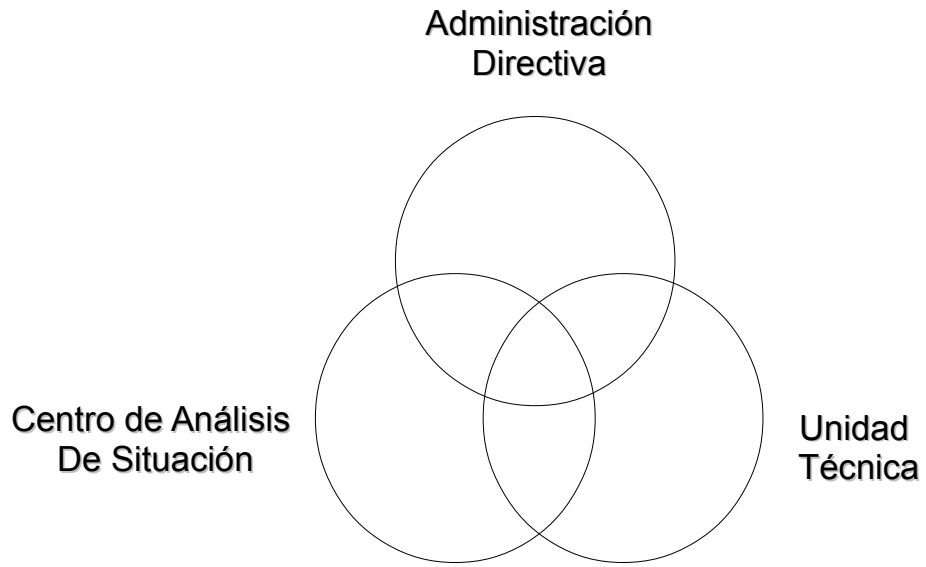


Figura 5.2: Composición Tripartita de la Unidad PI2C

5.5 FUNCIONES

Para que la composición tripartita de la unidad de PI2C descripta en el punto 5.4 pueda otorgar máximos resultados, es de suma importancia que tengan una muy buena organización interna cada una de las partes.

Las ventajas de contar con esta estructura pueden aprovecharse si la organización de la unidad funcional de la PI2C es óptima. Es fundamental establecer con claridad las responsabilidades y deberes de los socios involucrados.

En la siguiente figura (5.3), se grafica la organización de la Unidad PI2C.

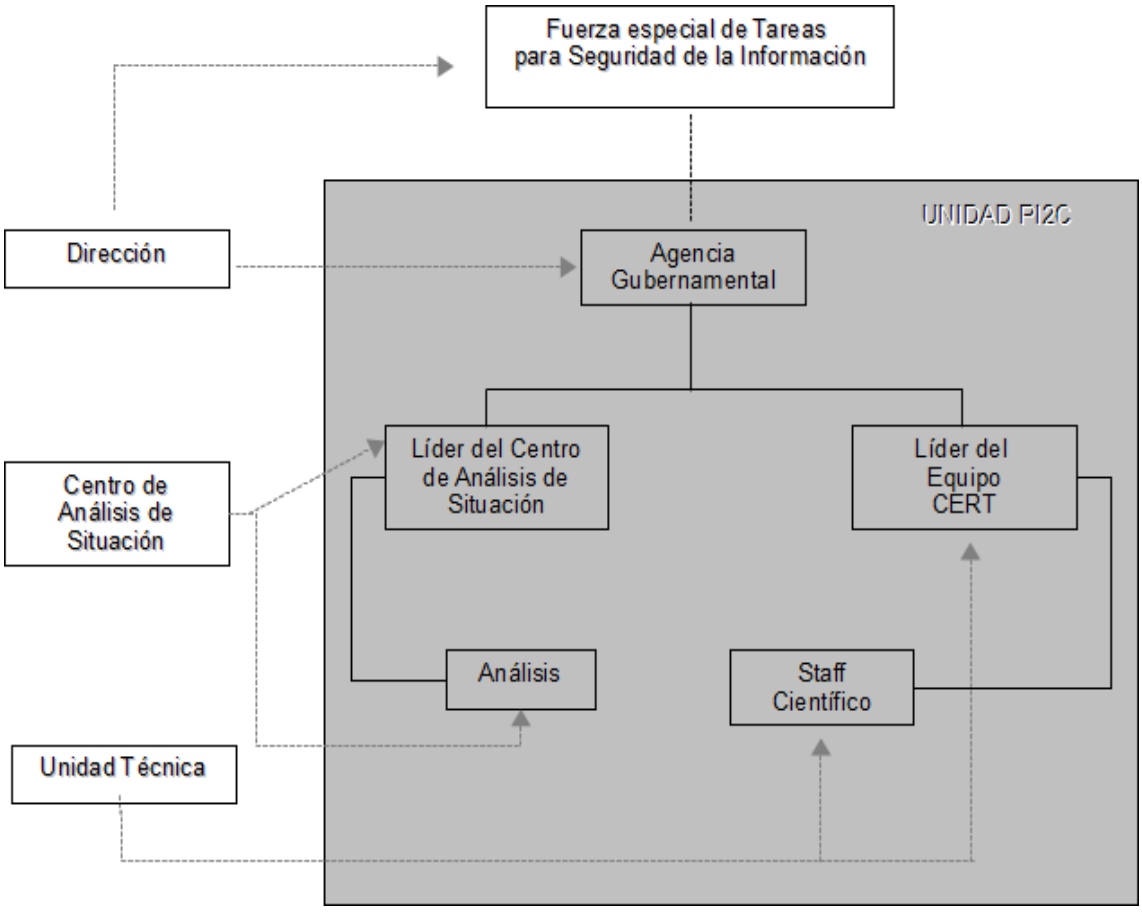


Figura 5.3: Mapa organizacional de la Unidad de PI2C

Como se mencionó anteriormente, la unidad de PI2C debe estar bien posicionada dentro de organismos gubernamentales.

La persona que ocupe el cargo mayor en la Dirección debe ser competente en el trato administrativo, comunicativo con sus relaciones y básicamente realizar tareas estratégicas.

En situaciones de emergencia se debe establecer una Fuerza Especial de Tareas para la Seguridad de la Información, en la cual tanto el sector público como el privado tomarán decisiones importantes. En este caso el encargado de interactuar con este grupo será el líder de la Dirección.

El líder del Servicio de Inteligencia (Centro de Análisis de Situación) no necesita ser experto en Seguridad de la Información, sino que debe tener amplios conocimientos legales y políticos. Está capacitado para evaluar nuevas amenazas y conectarse con autoridades judiciales. Esta unidad es la responsable de instruir a los operadores de infraestructura crítica, debiendo ayudar a incrementar el conocimiento e incentivar a la toma de conciencia en estos tipos de problemas.

Finalmente, el líder del Equipo CERT (Unidad Técnica) debe tener profundos conocimientos en la Seguridad de la Información, así como también poseer formación científica y en comunicaciones. Esta unidad ofrece soluciones puramente técnicas. Como existe una fuerte interacción y colaboración con el CERT nacional, se confía en las respuestas entregadas por dicho equipo. Y de esta forma se minimizan los requerimientos de mano de obra entro de la unidad de la PI2C.

En la siguiente tabla (5.1) se resumen los conocimientos necesarios de los líderes.

POSICIÓN	**HABILIDAD REQUERIDA**
Líder de la Administración Directiva de la Unidad de PI2C	✔ Experiencia en el área de Seguridad de la información o Infraestructura de Información Crítica (I2C). ✔ Buenos contactos con quienes deciden políticas. ✔ Habilidad para la comunicación, la administración y las tareas estratégicas.
Líder del Centro de	✔ Conocimiento Legal y Político.

Análisis de Situación (Servicio de Inteligencia)	✔ 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 5.1

5.6 MODELO DE COLABORACIÓN

Como se describió en el punto 5.4, cada una de los equipos de trabajo que conforman la unidad de PI2C realizan distintas tareas. En este punto se definirán los responsables de contactar a los socios de cada unidad (en realidad se definen las sociedades estratégicas para cada subunidad, no quienes en particular; apunta a aspectos de networking humano).

Los socios más importantes de la unidad de PI2C son los propietarios y operadores de I2C. Aquí se describirán los socios que no operan directamente con la I2C, pero que contribuyen a la unidad de PI2C.

A) SOCIOS DE LA DIRECCIÓN

El jefe de la unidad de PI2C debe familiarizarse con actividades administrativas de otras unidades y tratar de coordinar los recursos existentes. Llevar a cabo esta tarea no es tan simple, ya que cada agencia tiene diferentes puntos de vista, por lo tanto pueden existir contradicciones y conflictos burocráticos.

En primer lugar la Dirección de la unidad de PI2C debe tener contactos con todos los organismos gubernamentales participantes en la PI2C. Por lo tanto los primeros socios identificados son los dirigentes gubernamentales (políticos) y áreas de gobierno vinculadas a la economía, defensa, salud, etc.

Otros de los socios son el sector privado a través de empresas, productores de software, entidades bancarias, compañías de seguros, medios de comunicación, desarrolladores de tecnologías de la información y la comunicación, y también otras unidades de PI2C localizadas en diversos países.

B) SOCIOS DEL CENTRO DE ANÁLISIS DE SITUACIÓN

Con el fin de realizar tareas de recopilación y análisis de información, el Servicio de inteligencia deberá tener fuerte conexión con las unidades policiales dedicadas a la delincuencia de alta tecnología y con otros servicios de inteligencia nacionales y extranjeros.

El motivo de esto es debido a que tanto las unidades policiales como los servicios de inteligencia son las que reciben información acerca de actividades sospechosas y hechos delictivos relacionados con Internet.

En la práctica, las redes formadas por las unidades de policía, la Interpol y los servicios de inteligencia, son tan útiles que sirven de apoyo a las autoridades judiciales, las cuales no cuentan con la experiencia sobre investigaciones de fraudes y hechos delictivos ocurridos vía Internet.

C) SOCIOS DE LA UNIDAD TÉCNICA

En la Unidad técnica, se reconoce un socio fundamental que es el equipo CERT nacional. Este equipo es quien debe mantenerse actualizado sobre la evolución de los ataques, las nuevas formas que van surgiendo, nuevas técnicas de protección y es por ello que necesita contar con la colaboración de expertos en seguridad cibernética. También le corresponde establecer contactos con los desarrolladores de software y empresarios en tecnologías de la información y la comunicación.

El CERT es el responsable en intercambiar información a nivel internacional, siendo el FIRST (Foro de Respuesta a Incidentes y Equipos de Seguridad) la plataforma más importante para hacerlo.

Dado que la cooperación nacional e internacional es fundamental para la protección, es necesario que el equipo CERT de la unidad de PI2C, sea miembro del FIRST. [5.2]

La Figura 5.4 ilustra la red de la unidad:

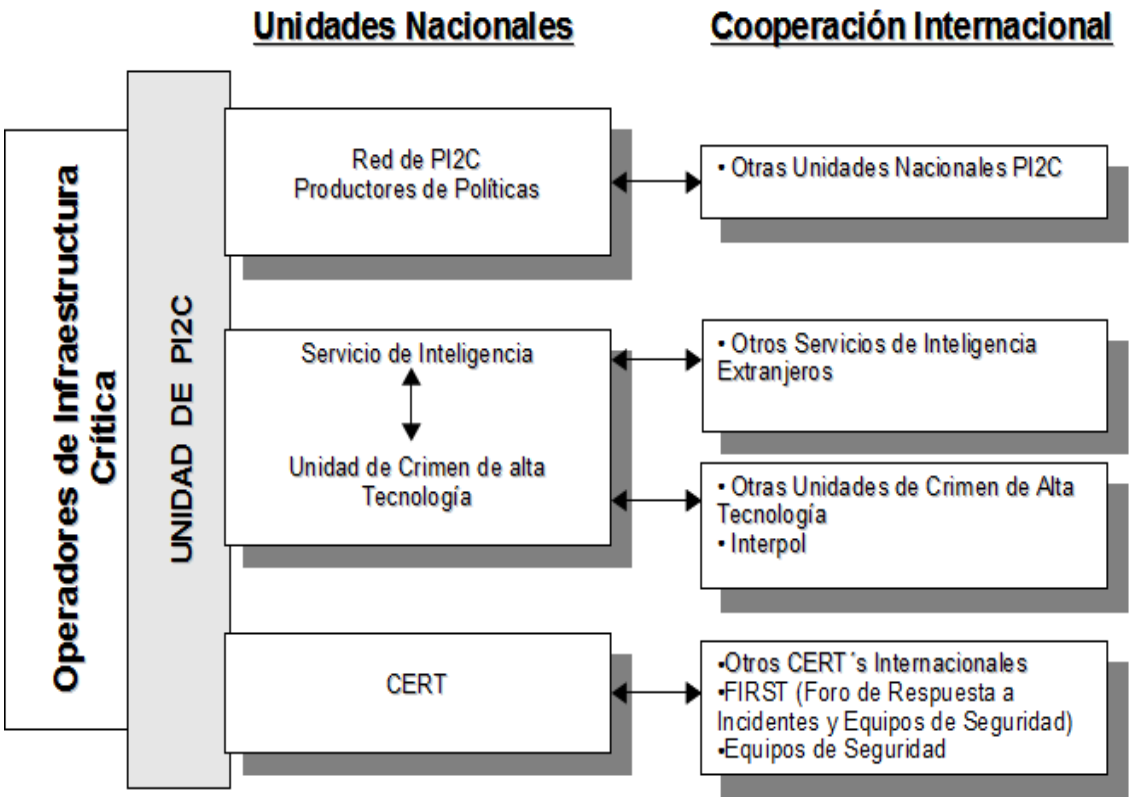


Figura 5.4: Red de la Unidad PI2C

5.7 CLIENTES Y PRODUCTOS DE LA PI2C

La unidad de PI2C define en dos grandes grupos a sus clientes. Los productos y servicios generados por esta unidad son principalmente para propietarios y operadores de infraestructura crítica, pero también es necesario asistir a pequeñas y medianas empresas y al público en general.

Estos dos grupos de clientes poseen diferentes necesidades las cuales deben ser adaptadas a cada uno. Y están definidos como:

1. *El GCC o Grupo Cerrado de Clientes*, comprendidos por propietarios y operadores de Infraestructura Critica.
2. *El GAC o Grupo Abierto de Clientes*, que incluye a pequeñas y medianas empresas y a usuarios domésticos de computación.

1. El GCC o Grupo Cerrado de Clientes

Los clientes que pertenecen a este grupo, tienen un gran dominio en materia de seguridad en las TIC por lo que emplean a sus especialistas y movilizan los conocimientos técnicos y recursos financieros para proteger sus sistemas. Por lo tanto éstos puntualmente buscan información especializada sobre nuevas amenazas y riesgos y esperan que la unidad de PI2C les proporcione la información necesaria y los servicios exclusivos.

El tamaño de este grupo de clientes debe ser pequeño, limitando la cantidad de representantes por empresa y deben de considerarse relaciones de fuerte confianza y cooperación para realizar el intercambio de información ya que ésta es sumamente sensible y confidencial.

El GCC está compuesto de un grupo que posee varios sectores, estos sectores se agrupan por el tipo de infraestructura crítica al que pertenecen (por ejemplo: Energía, comunicación, salud, agua).

Dentro de cada sector, la información manejada será confidencial, y sólo será compartida por otro sector del grupo si la situación lo requiere.

La Figura 5.5 describe el diseño del Grupo Cerrado de Clientes. En este gráfico se puede observar como cada sector representa un tipo diferente de Infraestructura Crítica. No toda la información es compartida por todos los miembros, y entre los distintos sectores, la información será compartida en líneas generales, no totales.

Con el fin de garantizar la integridad de la información compartida, es necesario realizar acuerdos formales. Todos los miembros del GCC, así como todos los socios de la unidad de PI2C, deben firmar un acuerdo de confidencialidad para garantizar que la información está sujeta al control de la empresa de origen. Sin el permiso explícito de ésta ni la unidad de PI2C, ni otros miembros del GCC se les permitirá transmitir información.

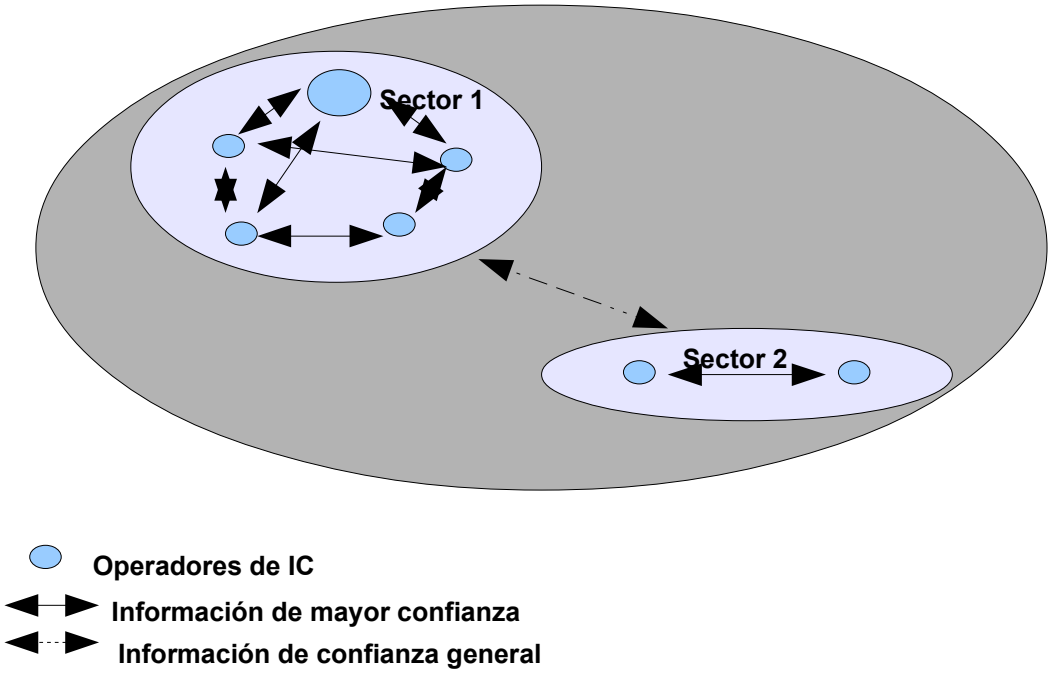


Figura 5.5: Diseño del GCC

Productos y Servicios para el GCC

- Asistencia en caso de incidentes
- Distribución de Información exclusiva
- Reuniones, Workshops, ejercicios

Con el fin de ser eficiente y confiable en el intercambio de información, la unidad de PI2C debe ofrecer una variedad de niveles de clasificación de la información. Cada miembro debe ser capaz de decidir con quien desea compartir su información.

La Figura 5.6 muestra los diferentes niveles de clasificación de la información.

Figura 5.6: Niveles de Clasificación de la Información

Clasificar la información en estos niveles, permitirá a las empresas limitar la propagación de la información.

Construir niveles de confianza lleva más tiempo que destruirlos. Serán necesarias medidas legislativas a fin de permitir el intercambio de información. Es una acción que la unidad de PI2C debe tomar e implementar para obtener conexiones seguras al compartir la información.

2. El GAC o Grupo Abierto de Clientes

El Grupo Abierto de Clientes está conformado por pequeñas y medianas empresas (PyMES) y público en general, éstas al no poseer las mismas necesidades no se le entregarán los mismos servicios. Los usuarios o público en general se interesarán por recomendaciones sobre medidas básicas de protección, mientras que las PyMES estarán buscando una consulta específica.

Dado que en la actualidad las computadoras están conectadas en red y a su vez con Internet, se han incrementado notablemente las amenazas producidas

con el fin de violar la seguridad en estos sistemas.

Es importante diferenciar cuando ocurre un incidente de seguridad en una IC y cuando ocurre en integrante del GAC, la magnitud de las consecuencias producidas en cada uno de los casos son totalmente distintas por lo que cada uno representa. Si bien la unidad de PI2C no puede asumir todas las tareas de prevención necesarias, es capaz de ofrecer productos interesantes.[5.1]

- *Productos y Servicios para el GAC*
    - Concientización
    - Advertencias y guías
    - Asistencia en algunos casos de incidentes

La siguiente tabla (5.2) resume los dos grupos de clientes:

	GCC	**GAC**
MIEMBROS	*OPERADORES DE IC (Miembros Limitados)*	*Pequeñas y medianas empresas – Ciudadanos en general.*
NÚMERO	*2 a 4 Representantes de cada sector.*	*Abierto*
CONFIANZA	*Fuerte nivel de Confianza*	*Débil nivel de Confianza*
CONSTRUCCIÓN DE LA CONFIANZA	*Dentro del grupo de clientes (reuniones periódicas, redes interactivas) y en particular dentro de cada sector.*	*Medios, Internet, exhibiciones con la ayuda de compañeros.*

Tabla 5.2: Cuadro resumen de los dos grupos

5.8 REFERENCIAS CAPITULO 5

[5.1] Generic National Framework For Critical Information Infrastructure Protection (CIIP)

[5.2] www.first.org - FIRST (Forum of Incident Response and Security Team)

6 CONCLUSIONES

En esta Tesis se ha abordado la problemática de establecer una serie de lineamientos estratégicos que permitan avanzar en la formalización de un Plan de Protección de Infraestructura Crítica para implementar en Argentina. Basados tanto en una investigación realizada sobre la situación actual de la PI2C en nuestro país, como en un proceso de entrevistas con la participación de personal jerárquico responsable de TI de importantes instituciones públicas puede deducirse que:

1.) *Existe cierto nivel de conocimiento de la problemática de de Infraestructuras Críticas y de su protección, aunque este debería ser profundizado;*
2.) *Que es necesario avanzar en la problemática de PI2C en Argentina;*
3.) *Que es necesaria la participación colectiva y la colaboración por parte de los sectores Público y Privado, y que este hecho es comprendido por los diferentes actores; y*
4.) *Existe, al menos en la voluntad de los entrevistados, el interés de cooperar con un proyecto destinado a PI2C.*

El modelo planteado requiere de recursos humanos y económicos, y de fluidas relaciones a nivel nacional que aseguren una buena comunicación con gobernantes. La integración internacional también será fundamental para lograr los objetivos propuestos. Si bien cada país del mundo posee sus propias necesidades en términos de PI2C, actualmente se intenta de consolidar esfuerzos con el objetivo de unificar criterios, desarrollar instrumentos legales internacionales y evitar fronteras geográficas. De igual modo resultará esencial la vinculación con el medio científico-tecnológico por medio de la articulación de actividades con Universidades y empresas del sector Privado.

Finalmente, el grado de avance en algunas áreas relacionadas con TIC en nuestro país, algunas de las iniciativas aisladas desarrolladas en torno a la temática de PI2C, y el interés mostrado por responsables de áreas de tecnología tanto de la administración pública como de empresas del sector privado muestran la necesidad de avanzar en una planificación estratégica para la PI2C en Argentina, siendo el presente trabajo nuestro humilde aporte.

ANEXO I - MODELO DE CUESTIONARIO

PARTE I: Seguridad de la Información (SI)

1) ¿Cree usted que las TIC son importantes para el crecimiento económico y social de la Nación?

Si		**No**	

Fundamentación
#

2) ¿Cree usted que las TIC a su cargo conforman un activo valioso para su sector (privado/publico)? ¿Por qué?

Si		**No**	

Fundamentación
#

3) ¿Conoce los conceptos de Riesgo, Amenaza y Vulnerabilidad en SI?

Si		**No**	

4) ¿Cree usted que el Riesgo y la Amenazas son parte del sistema de TIC a su cargo?

Si		**No**	

5) ¿Cree importante desarrollar estrategias de Mitigación del Riesgo / Manejo Adecuado de SI?

Si		**No**	

6) ¿Cree importante desarrollar estrategias de colaboración y coordinación en el contexto de seguridad de la información?

Si		**No**	

PARTE II: Infraestructura Crítica (IC)

1) ¿Conoce el concepto de Infraestructura Crítica (IC)?

Si		**No**	

2) ¿Conoce el concepto de Infraestructura de Información Crítica (I2C)?

Si		**No**	

3) Sabe o Reconoce a que sectores de la nación alcanza la IC?

Si		**No**	

Fundamentación
#

4) ¿Conoce el concepto de Protección de IC/I2C (PIC/PI2C)?

PIC

Si		**No**	

PI2C

Si		**No**	

5) ¿Cree usted que es importante la PIC / PI2C ?

PIC

Si		**No**	

PI2C

Si		**No**	

Fundamentación
#

6) ¿Cree usted que el problema de PIC / PI2C es importante en otros países del mundo?

PIC

Si		**No**	

PI2C

Si		**No**	

7) ¿Cree usted que resultaría de valor desarrollar una estrategia colectiva de PIC / PI2C?

Si		**No**	

PARTE III: Organización y coordinación

1) ¿En caso de una emergencia de seguridad vinculada con las TIC a su cargo, sabe a quién recurrir?

Si		**No**	

Fundamentación
#

2) ¿Cree posible coordinar recursos y acciones entre los sectores público y privado? Para que?

Si		**No**	

3) ¿Quién cree usted que es el responsable final de la Protección de la IC o I2C?

Fundamentación
#

4) ¿Conoce algún Plan Nacional vinculado con la protección de la Infraestructura?

Si		**No**	

Fundamentación
#

5) ¿Cree usted que resultaría importante y de valor avanzar en la formulación de un "Plan Nacional para la Protección de la Infraestructura (de Información) Crítica"?

Si		**No**	

Fundamentación
#

6) Estaría dispuesto a colaborar y cooperar o a formar parte de los grupos de trabajo para implementar la PI2C?

Si		**No**	

ANEXO II - ENTREVISTAS

A) Prog. LUCAS ANZOÁTEGUI

Responsable del área de Seguridad Informática del ISS-SEMPRE.

Departamento Desarrollo Subgerencia de Sistemas

Santa Rosa (La Pampa)

PARTE I: Seguridad de la Información (SI)

1) ¿Cree usted que las TIC son importantes para el crecimiento económico y social de la Nación?

Si	X	**No**	

Fundamentación
Sí, totalmente. No fundamenta porque considera que es demasiado extenso, muy amplio.

2) ¿Cree usted que las TIC a su cargo conforman un activo valioso para su sector? ¿Por qué?

Si	X	**No**	

Fundamentación
Sí, porque son herramientas fundamentales

3) ¿Conoce los conceptos de Riesgo, Amenaza y Vulnerabilidad en SI?

Si	X	**No**	

4) ¿Cree usted que el Riesgo y la Amenazas son parte del sistema de TIC a su cargo?

Si	X	**No**	

5) ¿Cree importante desarrollar estrategias de Mitigación del Riesgo / Manejo Adecuado de SI?

Si	X	**No**	

6) ¿Cree importante desarrollar estrategias de colaboración y coordinación en el contexto de seguridad de la información?

Si	X	**No**	

PARTE II: Infraestructura Crítica (IC)

1) ¿Conoce el concepto de Infraestructura Crítica (IC)?

Si	X	**No**	

2) ¿Conoce el concepto de Infraestructura de Información Crítica (I2C)?

Si	X	**No**	

3) Sabe o Reconoce a que sectores de la nación alcanza la IC?

Si		**No**	

Fundamentación
Reconoce parcialmente, la respuesta sería un mas o menos.

4) ¿Conoce el concepto de Protección de IC/I2C (PIC/PI2C)?

PIC

Si	X	**No**	

PI2C

Si	X	**No**	

5) ¿Cree usted que es importante la PIC / PI2C ?

PIC

Si	X	**No**	

PI2C

Si	X	**No**	

Fundamentación
Sí, Por supuesto. Por el valor a proteger.

6) ¿Cree usted que el problema de PIC / PI2C es importante en otros países del mundo?

PIC

Si	X	**No**	

PI2C

Si	X	**No**	

7) ¿Cree usted que resultaría de valor desarrollar una estrategia colectiva de PIC / PI2C?

Si	X	**No**	

PARTE III: Organización y Coordinación

1) ¿En caso de una emergencia de seguridad vinculada con las TIC a su cargo, sabe a quién recurrir?

Si	X	**No**	

Fundamentación
Si, recurren al Ar-CERT por ser una entidad pública o del gobierno.

2) ¿Cree posible coordinar recursos y acciones entre los sectores público y privado? Para que?

Si	X	**No**	

3) ¿Quién cree usted que es el responsable final de la Protección de la IC o I2C?

Fundamentación
El responsable máximo es el organismo.

4) ¿Conoce algún Plan Nacional vinculado con la protección de la Infraestructura?

Si		**No**	X

Fundamentación
Ha leído algo, parcialmente.

5) ¿Cree usted que resultaría importante y de valor avanzar en la formulación de un "Plan Nacional para la Protección de la Infraestructura (de Información) Crítica"?

Si	X	**No**	

Fundamentación
#Sí por supuesto. Es necesario

6) Estaría dispuesto a colaborar y cooperar o a formar parte de los grupos de trabajo para implementar la PI2C?

Si	X	**No**	

B) DANTE MORENO

Jefe de Planificación de TIC del Centro de Sistematización de Datos (Ce.Si.Da.) del Ministerio de Hacienda y Finanzas del Gobierno de la provincia de la Pampa

Santa Rosa (La Pampa)

PARTE I: Seguridad de la Información (SI)

1) ¿Cree usted que las TIC son importantes para el crecimiento económico y social de la Nación?

Si	X	**No**	

Fundamentación
Sí porque son imprescindibles, Las TIC son transversales a toda actividad. Habilita espacios humanos, en la parte económica y social. La inexistencia de las TIC permitiría no lograr un adecuado desarrollo de los ciudadanos.

2) ¿Cree usted que las TIC a su cargo conforman un activo valioso para su sector? ¿Por qué?

Si	X	**No**	

Fundamentación
Sí, porque las TIC componen la información básica para la gestión pública, a nivel intra y extra gubernamental. Las prestaciones que las TIC ofrecen en los servicios públicos son y generan un gran impacto.

3) ¿Conoce los conceptos de Riesgo, Amenaza y Vulnerabilidad en SI?

Si	X	**No**	

4) ¿Cree usted que el Riesgo y la Amenazas son parte del sistema de TIC a su cargo?

Si	X	**No**	

El riesgo es parte del sistema y las amenazas son parte del contexto.

5) ¿Cree importante desarrollar estrategias de Mitigación del Riesgo / Manejo Adecuado de SI?

Si	X	**No**	

6) ¿Cree importante desarrollar estrategias de colaboración y coordinación en el contexto de seguridad de la información?

Si	X	**No**	

PARTE II: Infraestructura Crítica (IC)

1) ¿Conoce el concepto de Infraestructura Crítica (IC)?

Si	X	**No**	

2) ¿Conoce el concepto de Infraestructura de Información Crítica (I2C)?

Si	X	**No**	

3) Sabe o Reconoce a que sectores de la nación alcanza la IC?

Si	X	**No**	

Fundamentación
Sí, las IC pertenecen a todos o a casi todos los sectores, por ej. energético, de comunicaciones, de salud.

4) ¿Conoce el concepto de Protección de IC/I2C (PIC/PI2C)?

PIC

Si	X	**No**	

PI2C

Si	X	**No**	

5) ¿Cree usted que es importante la PIC / PI2C ?

PIC

Si	X	**No**	

PI2C

Si	X	**No**	

Fundamentación
Por supuesto que es importante proteger las IC y las I2C. Por el valor que poseen y el impacto que genera en la sociedad cuando se ven interrumpidas.

6) ¿Cree usted que el problema de PIC / PI2C es importante en otros países del mundo?

PIC

Si	X	**No**	

PI2C

Si	X	**No**	

7) ¿Cree usted que resultaría de valor desarrollar una estrategia colectiva de PIC / PI2C?

Si	X	**No**	

PARTE III: Organización y Coordinación

1) ¿En caso de una emergencia de seguridad vinculada con las TIC a su cargo, sabe a quién recurrir?

Si	X	**No**	

Fundamentación
Si es a nivel local, es el sector que él dirige, por lo tanto sabe como resolver las

situaciones. Si es a nivel nacional, tiene alguna vinculación con el CERT a quien acudir. Y en otros casos a por ejemplo quien les provee los antivirus, antispam.

2) ¿Cree posible coordinar recursos y acciones entre los sectores público y privado? Para que?

Si	X	**No**	

Cree que es un desafío enorme, si ambos sectores supieran los intereses y el dinero que hay en juego, se intentaría coordinar para intentar minimizar los riesgos y evitar pérdidas.

3) ¿Quién cree usted que es el responsable final de la Protección de la IC o I2C?

Fundamentación
#Sin ninguna duda, el Estado es el primer y último responsable, es el encargado de la soberanía de los ciudadanos.

4) ¿Conoce algún Plan Nacional vinculado con la protección de la Infraestructura?

Si		**No**	X

Fundamentación
Ha leído sobre planes en otros países, en Europa, España y otros pero en la Argentina, no.

5) ¿Cree usted que resultaría importante y de valor avanzar en la formulación de un "Plan Nacional para la Protección de la Infraestructura (de Información) Crítica"?

Si	X	**No**	

Fundamentación
#Sí porque la actual situación de las IC y el uso de la información crítica es motivo suficiente para que el plan sea de interés. Más aún con las inversiones que el estado nacional ha hecho en las provincias y que cada vez son de mayor envergadura.

6) Estaría dispuesto a colaborar y cooperar o a formar parte de los grupos de trabajo para implementar la PI2C?

Si	X	**No**	

C) Lic. MARÍA MARTA CORTESINI

Aguas del Colorado

Gerente Comunicaciones y Servicios

Santa Rosa (La Pampa)

PARTE I: Seguridad de la Información (SI)

1) ¿Cree usted que las TIC son importantes para el crecimiento económico y social de la Nación?

Si	X	**No**	

Fundamentación
Sí, son fundamentales. Son Sirven como base como para promover el desarrollo.

2) ¿Cree usted que las TIC a su cargo conforman un activo valioso para su sector? ¿Por qué?

Si	X	**No**	

Fundamentación
Sí, son básicas para este sector.

3) ¿Conoce los conceptos de Riesgo, Amenaza y Vulnerabilidad en SI?

Si	X	**No**	

4) ¿Cree usted que el Riesgo y la Amenazas son parte del sistema de TIC a su cargo?

Si	X	**No**	

El riesgo y las amenazas siempre existen.

5) ¿Cree importante desarrollar estrategias de Mitigación del Riesgo / Manejo Adecuado de SI?

Si	X	**No**	

6) ¿Cree importante desarrollar estrategias de colaboración y coordinación en el contexto de seguridad de la información?

Si	X	**No**	

PARTE II: Infraestructura Crítica (IC)

1) ¿Conoce el concepto de Infraestructura Crítica (IC)?

Si	X	**No**	

2) ¿Conoce el concepto de Infraestructura de Información Crítica (I2C)?

Si	X	**No**	

3) Sabe o Reconoce a que sectores de la nación alcanza la IC?

Si	X	**No**	

Fundamentación
No sabe si existe alguna normativa que los enuncie.. Cree que a todos los organismos. No sabe si existe a nivel nacional una definición respecto a esto.

4) ¿Conoce el concepto de Protección de IC/I2C (PIC/PI2C)?

PIC

Si	X	**No**	

PI2C

Si	X	**No**	

5) ¿Cree usted que es importante la PIC / PI2C ?

PIC

Si	X	**No**	

PI2C

Si	X	**No**	

Fundamentación
Sí y cree que cada día es más importante.

6) ¿Cree usted que el problema de PIC / PI2C es importante en otros países del mundo?

PIC

Si	X	**No**	

PI2C

Si	X	**No**	

7) ¿Cree usted que resultaría de valor desarrollar una estrategia colectiva de PIC / PI2C?

Si	X	**No**	

Sí, no sabe si funcionaría, pero sí.

PARTE III: Organización y Coordinación

1) ¿En caso de una emergencia de seguridad vinculada con las TIC a su cargo, sabe a quién recurrir?

Si	X	**No**	

Fundamentación
Depende de la situación. A Entes privados, o a públicos. En general conoce en cada situación a quien dirigirse.

2) ¿Cree posible coordinar recursos y acciones entre los sectores público y privado? Para que?

Si	X	**No**	

Sería bueno hacerlo, pero no lo cree posible. Debería serlo. No lo sabe.

3) ¿Quién cree usted que es el responsable final de la Protección de la IC o I2C?

Fundamentación
El estado.

4) ¿Conoce algún Plan Nacional vinculado con la protección de la Infraestructura?

Si		**No**	X

Fundamentación
No en Argentina. En otros países por ahi hay una legislación, pero no tiene dato concreto de ninguno.

5) ¿Cree usted que resultaría importante y de valor avanzar en la formulación de un "Plan Nacional para la Protección de la Infraestructura (de Información) Crítica"?

Si	X	**No**	

Fundamentación
Sí, por supuesto. Por el valor de los activos a proteger.

6) Estaría dispuesto a colaborar y cooperar o a formar parte de los grupos de trabajo para implementar la PI2C?

Si	X	**No**	

Sí, en la medida que tenga tiempo. Es complicado.

D) Cnel. JUAN JOSÉ BENITEZ

Jefe del Comando de Comunicaciones e Informática del Estado Mayor General del Ejército

PARTE I: Seguridad de la Información (SI)

1) ¿Cree usted que las TIC son importantes para el crecimiento económico y social de la Nación?

Si	X	**No**	

Fundamentación
Sí Totalmente. Las TIC son el medio fundamental para el crecimiento y desarrollo económico y social.

2) ¿Cree usted que las TIC a su cargo conforman un activo valioso para su sector? ¿Por qué?

Si	X	**No**	

Fundamentación
Sí Totalmente. En principio las TIC son un activo muy importante para la nación. Las comunicaciones es el medio fundamental para transmitir la información a donde se quiera.

3) ¿Conoce los conceptos de Riesgo, Amenaza y Vulnerabilidad en SI?

Si	X	**No**	

4) ¿Cree usted que el Riesgo y la Amenazas son parte del sistema de TIC a su cargo?

Si	X	**No**	

5) ¿Cree importante desarrollar estrategias de Mitigación del Riesgo / Manejo Adecuado de SI?

Si	X	**No**	

6) ¿Cree importante desarrollar estrategias de colaboración y coordinación en el contexto de seguridad de la información?

Si	X	**No**	

Son tareas fundamentales.

PARTE II: Infraestructura Crítica (IC)

1) ¿Conoce el concepto de Infraestructura Crítica (IC)?

Si	X	**No**	

2) ¿Conoce el concepto de Infraestructura de Información Crítica (I2C)?

Si	X	**No**	

3) Sabe o Reconoce a que sectores de la nación alcanza la IC?

Si	X	**No**	

Fundamentación
Toda información que maneja la nación es información crítica. Son las que poseen por ejemplo los medios financieros, los sistemas energéticos, salud, etc.

4) ¿Conoce el concepto de Protección de IC/I2C (PIC/PI2C)?

PIC

Si	X	**No**	

PI2C

Si	X	**No**	

5) ¿Cree usted que es importante la PIC / PI2C ?

PIC

Si	X	**No**	

PI2C

Si	X	**No**	

Fundamentación
Sí, por supuesto, el estado de protección es primordial. En muchos estados se presta total atención a la ciberguerra, son naciones que la consideran amenazante por el impacto que pueden causar.

6) ¿Cree usted que el problema de PIC / PI2C es importante en otros países del mundo?

PIC

Si	X	**No**	

PI2C

Si	X	**No**	

7) ¿Cree usted que resultaría de valor desarrollar una estrategia colectiva de PIC / PI2C?

Si	X	**No**	

PARTE III: Organización y Coordinación

1) ¿En caso de una emergencia de seguridad vinculada con las TIC a su cargo, sabe a quién recurrir?

Si	X	**No**	

Fundamentación
Sí, se dirigen al Ar-CERT en casos de emergencias. Y por ser una entidad gubernamental, en muchas ocasiones, el Ar-CERT les indican y alertan sobre amenazas a sus sistemas.

2) ¿Cree posible coordinar recursos y acciones entre los sectores público y privado? Para que?

Si	X	**No**	

3) ¿Quién cree usted que es el responsable final de la Protección de la IC o I2C?

Fundamentación
#Sin duda es el Estado. El estado es quien posee la función de otorgar seguridad.

4) ¿Conoce algún Plan Nacional vinculado con la protección de la Infraestructura?

Si	X	**No**	

Fundamentación
Sí, Ha leído y conoce sobre varios proyectos en la Argentina, pero que no han sido implementados aún.

5) ¿Cree usted que resultaría importante y de valor avanzar en la formulación de un "Plan Nacional para la Protección de la Infraestructura (de Información) Crítica"?

Si	X	**No**	

Fundamentación
Sí, totalmente. Es sumamente importante que exista un plan de protección, más aún si la información es crítica.

6) Estaría dispuesto a colaborar y cooperar o a formar parte de los grupos de trabajo para implementar la PI2C?

Si	X	**No**	

E) FERNANDO GRAFFIGNA

Jefe del Área de Redes y Seguridad

de la Municipalidad de Junín.

Pcia. De Buenos Aires

PARTE I: Seguridad de la Información (SI)

1) ¿Cree usted que las TIC son importantes para el crecimiento económico y social de la Nación?

Si	X	**No**	

Fundamentación
Sí, son imprescindibles para el desarrollo.

2) ¿Cree usted que las TIC a su cargo conforman un activo valioso para su sector? ¿Por qué?

Si	X	**No**	

Fundamentación
Sí, porque al pertenecer a un organismo que otorga servicios (Municipalidad) las TIC son las herramientas fundamentales para efectivizar la ejecución de ésos servicios, permite optimizar los tiempos y sobre todo sirven elementos de control y éso en este sector es imprescindible.

3) ¿Conoce los conceptos de Riesgo, Amenaza y Vulnerabilidad en SI?

Si	X	**No**	

4) ¿Cree usted que el Riesgo y la Amenazas son parte del sistema de TIC a su cargo?

Si	X	**No**	

5) ¿Cree importante desarrollar estrategias de Mitigación del Riesgo / Manejo Adecuado de SI?

Si	X	**No**	

6) ¿Cree importante desarrollar estrategias de colaboración y coordinación en el contexto de seguridad de la información?

Si	X	**No**	

Es importante y también es bastante difícil, pero es un punto a tener en cuenta.

PARTE II: Infraestructura Crítica (IC)

1) ¿Conoce el concepto de Infraestructura Crítica (IC)?

Si	X	**No**	

2) ¿Conoce el concepto de Infraestructura de Información Crítica (I2C)?

Si	X	**No**	

3) Sabe o Reconoce a que sectores de la nación alcanza la IC?

Si	X	**No**	

Fundamentación
Sí, las IC pertenece a todos o a casi todos los sectores.

4) ¿Conoce el concepto de Protección de IC/I2C (PIC/PI2C)?

PIC

Si	X	**No**	

PI2C

Si	X	**No**	

5) ¿Cree usted que es importante la PIC / PI2C ?

PIC

Si	X	**No**	

PI2C

Si	X	**No**	

Fundamentación
Sí, es fundamental proteger las IC y las I2C.

6) ¿Cree usted que el problema de PIC / PI2C es importante en otros países del mundo?

PIC

Si	X	**No**	

PI2C

Si	X	**No**	

7) ¿Cree usted que resultaría de valor desarrollar una estrategia colectiva de PIC / PI2C?

Si	X	**No**	

PARTE III: Organización y Coordinación

1) ¿En caso de una emergencia de seguridad vinculada con las TIC a su cargo, sabe a quién recurrir?

Si	X	**No**	

Fundamentación
Si, en algunos casos recurren a la ONTI y al Ar-CERT, pero no en todos los casos.

2) ¿Cree posible coordinar recursos y acciones entre los sectores público y privado? Para que?

Si	X	**No**	

Cree que depende de la voluntad política.

3) ¿Quién cree usted que es el responsable final de la Protección de la IC o I2C?

Fundamentación
El responsable es el estado a través de la implementación de legislaciones. En el sector privado es más sencillo ya que los intereses son otros.

4) ¿Conoce algún Plan Nacional vinculado con la protección de la Infraestructura?

Si		**No**	X

Fundamentación
No conoce.

5) ¿Cree usted que resultaría importante y de valor avanzar en la formulación de un "Plan Nacional para la Protección de la Infraestructura (de Información) Crítica"?

Si	X	**No**	

Fundamentación
#Sí, totalmente. Es una necesidad pero cree que seria complejo porque existen diferentes intereses y cierta desconfianza. Sería un gran soporte para los distintos sectores.

6) Estaría dispuesto a colaborar y cooperar o a formar parte de los grupos de trabajo para implementar la PI2C?

Si	X	**No**	

Sí, totalmente. Aunque algunos sectores no lo creen o no lo ven tan necesario ya sea por su dinámica o sus intereses, es una necesidad fundamental ya que existe poco apoyo relacionado con la protección.

ANEXO III - GLOSARIO

Acceso	Acción de llegar o acercarse. Entrada o paso.
Asegurar	Preservar o resguardar de daño a alguien o algo; defenderlo. Dejar seguro de la realidad o certeza de algo.
Ataque	Perjudicar o causar un daño
Autorizar	Dar o reconocer a alguien facultad o derecho para hacer algo.
Ciber	prefijo que significa 'cibernético'
Ciberataque	De Ataque, aplicado al ciberespacio
Cibercrimen	De Crimen, aplicado al ciberespacio
Ciberdelincuencia	De delinquir, aplicado al ciberespacio.
Ciberespacio	Ámbito de comunicaciones constituido por una red informática
Cibernética	Ciencia que estudia la construcción de sistemas electrónicos y mecánicos a partir de su comparación con los sistemas de comunicación y regulación automática de los seres vivos.
Cibernético	De la cibernética o relativo a ella.
Ciberseguridad	De seguro, aplicado al ciberespacio
Ciberterrorismo	De terrorismo, aplicado al Ciberespacio
Control	Comprobación, inspección, fiscalización, intervención.
Crimen	Acción o cosa que perjudica a alguien o algo.
Crítica	Perteneciente o relativo a la crisis
Dañar	Causar detrimento, perjuicio, menoscabo, dolor o molestia. Maltratar o echar a perder algo.
Delincuencia	Acción de delinquir.
Delinquir	Cometer delito.
Información	Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada.
Infraestructura	Conjunto de elementos o servicios que se consideran necesarios para la creación y funcionamiento de una organización

	cualquiera
Prevención	Acción y efecto de prevenir.
Prevenir	Ver, conocer de antemano o con anticipación un daño o perjuicio. Precaver, evitar, estorbar o impedir algo. Advertir, informar o avisar a alguien de algo. Anticiparse a un inconveniente, dificultad u objeción, prepararse de antemano para algo.
Protección	Acción y efecto de proteger.
Proteger	Amparar, favorecer, defender. Resguardar a una persona, animal o cosa de un perjuicio o peligro
Riesgo	Contingencia o proximidad de un daño.
Seguro	Libre y exento de todo peligro, daño o riesgo. Cierto, indubitable y en cierta manera infalible. No sospechoso.
Sistema	Conjunto de cosas que relacionadas entre sí ordenadamente contribuyen a determinado objeto.
Terrorismo	Forma violenta de lucha política mediante la cual se persigue la destrucción del orden establecido o la creación de un clima de temor e inseguridad
Vulnerabilidad	Cualidad de vulnerable.
Vulnerable	Que puede ser herido o recibir lesión, física o moralmente.

Definiciones extraídas de www.wordreference.com y www.rae.es

ANEXO IV - ABREVIATURAS

Anatel:	Agencia Nacional de Telecomunicaciones, siglas en portugués de "Agência Nacional de Telecomunicações"
Ar-CERT:	Equipo de respuesta a emergencias computacionales Argentinas
APN:	Administración Pública Nacional
BBK:	Oficina Federal de Protección Civil y ayuda en catástrofe o, siglas en inglés de "Federal Office of Civil Protection and Disaster Assistance"
BKA:	Agencia Criminal de la Policía Federal o, siglas en inglés de "Federal Criminal Police Agency"
BMI:	Ministerio del Interior Federal o, siglas en inglés de "Federal Ministry of the Interior"
BSI:	Oficina Federal de Seguridad de la Información
CCS:	Secretaría de Contingencia Civil, siglas en inglés de Central Sponsor for Information Assurance
CCIPS:	Siglas en inglés de "Computer Crime and Intellectual Property Section"
CERT:	Equipo de respuesta a emergencias computacionales
CERT.br:	Equipo de respuesta a emergencias computacionales Brasileras
CGI:	Comité Directivo en Internet de Brasil, siglas en inglés de "Brazilian Internet Steering Committee"
CPNI:	Centro para la Protección de la Infraestructura Nacional, siglas en inglés de Centre for the Protection of the National Infrastructure
CSCSWG:	Grupo de Trabajo a través del sector de ciber seguridad.
CSIRTUK:	Equipo Combinado de Respuestas a Incidentes de Seguridad, siglas en inglés de Combined Security Incident Response Team.
CTIR Gov:	Centro de tratamiento de incidentes de seguridad en redes de computadoras de la administración pública federal, siglas en portugués de "Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal"
DHS:	Departamento de Seguridad Interna, siglas en Inglés de "Departament of Homeland Security"

DSCN:	División de Seguridad Cibernética Nacional, siglas en Inglés de "Departament Security Cibernetic National"
EPCIP:	Programa europeo para Protección de la Infraestructura Crítica
FSB:	Servicio Federal de Seguridad de la Federación Rusa
G8:	Grupo de los ocho
GAO:	Oficina de Responsabilidad Gubernamental, siglas en inglés de Goverment Accountability Office
GCHQ:	Oficina de seguridad y la sede del ministerio del interior y comunicaciones, siglas en inglés de Government Communications Headquarters.
GIS:	Gestión de Incidentes de Seguridad
GSI:	Oficina de Seguridad institucional de La presidencia de la República Brasileña, siglas en portugués de "Gabinete de Segurança Institucional"
I2C:	Infraestructura de Información Crítica
I3P:	Instituto para la Protección de la Infraestructura de Información
IC:	Infraestructura Crítica
ISACs:	Centro de análisis e información compartida InfraGard
ITU:	Unión de Telecomunicación Internacional o siglas en inglés de "International Telecommunications Union"
ITU GCA:	Unión de Telecomunicación Internacional , Agenda Global de Cyberseguridad
ITU-D:	Sector de Desarrollo de las Telecomunicaciones de la ITU
ITU-R:	Sector de Normalización de las Radiocomunicaciones
ITU-T:	Sector de Normalización de las Telecomunicaciones
NCSA:	Alianza Nacional de Ciber Seguridad
NIC.br:	Centro de información de redes Brasileras
NISCC:	Centro de Coordinación de Seguridad de la Infraestructura Nacional, siglas en inglés de National Infrastructure Security Coordination Centre
NPSI:	Plan Nacional para la Protección de la Infraestructura Crítica o, siglas en inglés de "National Plan for Information Infraestructure Protection"

NSAC:	Centro de Asesoramiento de Seguridad Nacional, siglas en inglés de National Security Advice Centre
NSSC:	Estrategia Nacional para asegurar el Ciberespacio, siglas en inglés de National Strategy to Secure Cyberspace
OECD:	Organización para la economía, cooperación y desarrollo, siglas en inglés de "Organisation for Economic Co-operation and Development"
ONU:	Organización de las Naciones Unidas
PCIS:	Seguridad para la IC de la sociedad.
PIC:	Protección de Infraestructura Crítica
PI2C:	Protección de Infraestructura de Información Crítica
PCI2P:	Protected Critical Infraestructure Information Program
RANS:	Asociación Rusa de Redes y Servicios o siglas en inglés de "Russian Association of Networks and Services"
RANS:	Asociación Rusa de Redes y Servicios, siglas en inglés de "Russian Association of Networks and Services"
RU-CERT:	Equipo de respuesta a emergencias computacionales Rusas
TI:	Tecnologías de la Información
TIC:	Tecnologías de Información y la Comunicación
US-CERT:	Equipo de respuesta a emergencias computacionales Americanas

ANEXO V - REFERENCIAS WEB

Links relacionados a agencias y organismos dedicados a la seguridad

- www.enisa.europa.eu - ENISA -the European Network and Information Security Agency
- www.cse.dnd.ca - Communications Security Establishment. Canada's National Cryptologic Agency
- www.dsd.gov.au - Defense Signals Directorate – Australian Government – Departement of Defence
- www.nsa.gov - National Security Agency (USA)
- www.eema.org/ - The European Forum for Electronic Business (EEMA) – The independent European association for e-business
- www.first.org - FIRST (Forum of Incident Response and Security Team)
- www.cesg.gov.uk - National Technical Authority for Information Assurance (UK)
- www.europa.eu.int/information_society/index_en.htm - Europe's Information Society Thematic Portal
- www.melani.admin.ch - Computer and Internet security (CH)
- www.cert.org - CERT – Center of internet security expertize, Carnegie Mellon University (USA).
- www.apcert.org - Asia Pacific Computer Emergency Response Team
- www.jpcert.or.jp/english/index.html - Computer Security Incident Response Team Japan – Supporting the Internet security in Asia
- www.auscert.org.au - AusCERT – Australia Computer Emergency Response Team
- www.niser.org.my - National ICT Security & Emergency Response Centre – Malaysian Computer Emergency Response Team
- https://www.cert.ru - CERT – (Russia)
- www.wikayanet.dz - Algerian Portal of Information Security

- www.crime-research.iatp.org.ua - The Computer Crime Research Center (CCRC) Ukrainian branch
- www.crime-research.ru - The Computer Crime Research Center (CCRC) Russia
- www.clusif.fr - Club de la Sécurité de l'Information Français
- www.cs.purdue.edu/coast/coast.html - COAST (Computer Operations, Audit and Security Technology)
- www.hoaxbusters.ciac.org - Information about hoaxes
- www.spamfighter.com/Default.asp - Information about spam
- www.ripe.net/ripe/wg/anti-spam/index.html - Anti spam working group
- www.secuser.com - About anti-spam anti-intrusion, privacy
- www.antiphishing.org - Anti phishing working group
- www.oecd.org/dataoecd/29/12/35670414.pdf - OECD Task Force on Spam report Anti Spam Regulation released in November 2005
- www.oecd-antispam.org - OECD toolkit on spam
- www.aptsec.org/meetings/2005/NSS/docs/index.htm - Symposium on Network Security and SPAM (22 - 24 Aug. 2005, Jakarta, Indonesia)
- http://wiki.apcauce.org/index.php/Main_Page - APCAUCE, the Asia Pacific Coalition Against Unsolicited Commercial Email
- http://www.justice.gov/criminal/cybercrime/ccips.html – CCIPS - Computer Crime and Intellectual Property Section

Links relacionados con la seguridad en Internet

- www.cybercrimelaw.net - Cybercrimelaw.net is a global information clearinghouse on cybercrime law (Norway)
- http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm - Convention on Cybercrime – Budapest, 23.XI. 2001 – Council of Europe
- www.legi-internet.ro/en/cybercrime.htm - Romanian IT Law

- www.wipo.int/portal/index.html.en - World Intellectual Proprety Organization
- www.ilrg.com - Internet Legal Research Group
- www.cyberlawinformer.com - Legal Issues on Internet
- www.cybercrimelaw.net - Cybercrime Law web site give a comprehensive survey of current legislations from around the world includes the laws of 78 countries.
- www.legalis.net - Jurisprudence, current events and Internet law
- www.foruminternet.org - Information dedicated space about the legal issues concerning Internet end network
- www.cybercrimes.net - The University of Dayton – School of Law (USA)
- www.gseis.ucla.edu/iclp/safe.htm - The UCLA Online Institute for Cyberspace Law and Policy (USA)

Links relacionados con la protección privada de sitios web

- www.privacyinternational.org - Privacy protection
- www.privacy.org - Privacy protection
- www.w3.org/P3P/ - Platform for Privacy Preferences (P3P) Project
- www.cyberrights.org - Cyberrights &cyberliberties protection
- www.epic.org - Electronic privacy Information Center

Links relacionados con el Cibercrimen

- www.ic3.gov - Internet Crime Complaint Center (IC3) (USA)
- www.nw3c.org - National White Collar Crime Center (NW3C) (USA)
- www.cyberwise.ca/epic/internet/incyb-cyb.nsf/en/Home - National Strategy for the Protection of Children from Sexual Exploitation on the Internet

- www.cybercrime.gov/cc.html - Computer Crime & Intellectual Property Section/United States Department of Justice
- www.crime-research.org - The Computer Crime Research Center (CCRC)
- www.fraud.org - National Internet Fraud Information Center
- www.idtheftcenter.org/index.shtml - Identity Theft Resource Center (ITRC)
- www.oecd.org/fatf/ - Financial Action Task Force (FATF-GAFI)
- www.uncjin.org - United Nations Crime and Justice Information Network

Links relacionados con derechos y legislaciones

- www.rcmp-grc.gc.ca/scams/ccprev_e.htm - The Royal Canadian Mounted Police
- www.interpol.int/ - Interpol – international police organization
- www.interpol.int/Public/FinancialCrime/default.asp - Interpol – Financial and High-tech crimes
- www.htcia.org/ - Internet High Technology Crime Investigation Association
- www.cybercellmumbai.com - The Cyber Crime Investigation Cell of Mumbai Police India
- www.scoci.ch - The Swiss Coordination Unit for Cybercrime Control

Otros links de interés

- www.wikipedia.org - Wikipedia: the free encyclopedia
- www.intgovforume.org - Site of the Internet Governance Forum (IGF)
- www.oecd.org - OCDE website Organization for Economic Co-operation and Development - Information Security and Privacy
- www.saferinternet.org - Europe’s Internet Safety portal

- www.warp.gov.uk - Warning, advice and reporting point (UK)
- www.coe.int/T/E/Legal_affairs/Legal_cooperation/Combating_economic_crime/ - Actions against Economic and Organized Crime – Council of Europe