ZAGREB
CONSULTORES LIMITADA

Telecomunicaciones - Ingeniería de Procesos - Control de Gestión

Informe Final

Estudio para la definición e identificación de infraestructura crítica de la información en Chile

SUBTEL

ID 606-11055-LE08

Diciembre 2008

Teléfono: (562) 225-7951 Celular: (569) 895-5657 e-mail: p.boric@entelchile.net

ADVERTENCIA

EN VIRTUD DE LA NATURALEZA DE LA INFORMACIÓN, Y A LO SOLICITADO EXPRESAMENTE POR VARIOS OPERADORES EN EL SENTIDO QUE LA INFORMACIÓN QUE PROPORCIONARON SE ENTREGÓ EN LA MAS ESTRICTA RESERVA, CONSIDERAMOS IMPRESCINDIBLE QUE ESTE INFORME, SUS ANEXOS Y TODA LA DOCUMENTACION DE RESPALDO SEA ADMINISTRADA POR SUBTEL EN FORMA CONFIDENCIAL Y TRATADA CON LA MÁS ABSOLUTA RESERVA

Teléfono: (562) 225-7951 Celular: (569) 895-5657 e-mail: p.boric@entelchile.net

RESUMEN EJECUTIVO

El objetivo general de la consultoría es asesorar a SUBTEL en la definición e identificación de la infraestructura crítica de la información (ICI) para el caso de Chile, en el ámbito de las redes y sistemas de telecomunicaciones, contemplando la revisión de la experiencia internacional en la definición de criterios de criticidad, una propuesta de definición de criterios aplicables al caso chileno, determinar la infraestructura de telecomunicaciones crítica, y definir criterios y grados de criticidad de la misma.

Para el análisis de la experiencia internacional el trabajo se centró en los estudios que han realizado organismos internacionales como la OECD, la UIT y el Centro para Estudios de Seguridad con sede en Zurich. El estudio de la OECD corresponde a un análisis comparativo, del desarrollo de las políticas para la protección de la infraestructura crítica de la información en Australia, Canadá, Corea, Japón, Holanda, Inglaterra y Estados Unidos.

Todos los países se refieren a la ICI como aquella infraestructura de información, que al no tenerla disponible, puede ocasionar pérdidas de vida, serio o grave impacto en la salud, seguridad o economía de sus ciudadanos, y han desarrollado la estrategia y objetivos de la ICI después de haber identificado cual es la infraestructura crítica. Cuentan con una organización vertical en el tema de la ICI, dirigida desde el más alto nivel del gobierno, quien da el ejemplo al resto de la sociedad.

La protección de la infraestructura crítica es coordinada desde una unidad de gobierno, con una sólida cooperación entre el sector privado y el gobierno y mecanismos de intercambio de información para estimular a los dueños y operadores de la ICI a tomar decisiones para asegurar su propia infraestructura crítica.

La metodología utilizada por Australia es la que representa con mayor exactitud lo que realizan los otros países analizados y que se resume a continuación:

- Identificar dependencias e interdependencias entre sistemas de infraestructura críticos.
- Análisis de las consecuencias de fallas de la infraestructura crítica
- Determinar puntos únicos de fallas y otros puntos de alta vulnerabilidad.
- Opciones de inversión y otras estrategias de mitigación de impactos
- Definir escenarios, incluyendo desastres naturales y actos de terrorismo, los cuales puedan ocasionar la interrupción del servicio de infraestructura crítica.

En Chile para el tema de telecomunicaciones, la definición de infraestructura crítica debiera ser: Aquellas redes de telecomunicaciones, cuya interrupción o destrucción podría producir un serio impacto en la salud, seguridad o bienestar de la población o producir un serio impacto en el funcionamiento del gobierno o de la economía del país. En este contexto y de acuerdo a lo solicitado por SUBTEL se consideran en este estudio las siguientes redes: Telefonía fija, Telefonía móvil, Internet, Redes de datos y Redes de transporte.

Se analizaron las arquitecturas de las distintas redes con sus principales inter relaciones, vulnerabilidades y amenazas, para lo cual se presenta un modelo de capas, en el cual la capa inferior está compuesta por las Redes de Servicio y de Acceso, que conectan a los usuarios finales con las redes de servicio. Estas redes de servicio se interconectan a través de las Redes de Transporte Nacional en la segunda capa, preferentemente formadas por elementos que operan sobre un medio de fibra óptica. La última capa corresponde a las Redes de Transporte Internacional, interconectando al país con el resto del mundo.

En este modelo, los servicios provistos a los usuarios finales son más vulnerables en la medida que se acercan a éste, porque dependen de más de una red compuesta por diferentes nodos, y por lo tanto están más expuestas a verse afectadas por la indisponibilidad de alguno de ellos. Las redes de transporte por su carácter eminentemente distribuido en su emplazamiento geográfico y por hacer uso de infraestructura física que concentra altos volúmenes de tráfico, son más vulnerables a todos los fenómenos de la naturaleza como terremotos, inundaciones, destrucciones causadas por la acción del hombre, y similares. En cambio las redes de servicios son vulnerables en sus nodos centrales al estar más concentradas lógicamente. Sin embargo estas redes igualmente dependen de las redes de transporte para la prestación de los servicios.

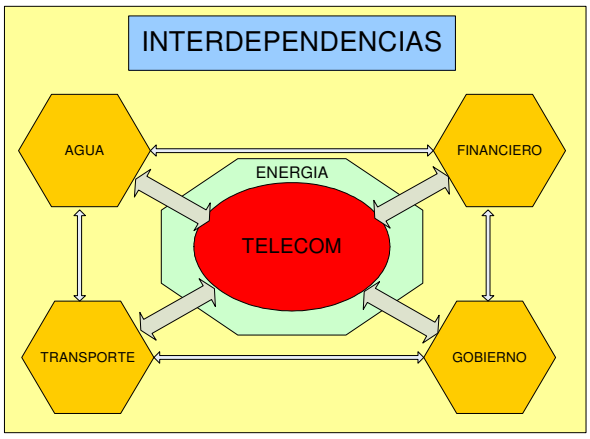
Las vulnerabilidades se clasifican como amenazas (provienen desde el exterior de las redes) y debilidades (propias de la red o su explotación).

Se desarrolló una metodología para determinar indicadores de criticidad, y mediante ellos contar con un ranking que oriente los esfuerzos de análisis detallados sobre las medidas de mitigación para disminuir los niveles de riesgo e impacto. El aspecto más importante para definir la criticidad de una infraestructura es el impacto de una interrupción o mal funcionamiento de sus componentes, condicionado esencialmente por tres factores: la cantidad de usuarios afectados, duración de la interrupción o mal funcionamiento y la extensión geográfica que se afecta en caso de un siniestro. En base a estos parámetros se determina cual sitio es más crítico que otro, y por lo tanto a cuales se les debe prestar una mayor atención en el análisis e implantación de medidas para disminuir al máximo las vulnerabilidades de esos sitios. Otro aspecto es la probabilidad que una amenaza o

debilidad se materialice, de modo que provoque el impacto estimado, lo que se entiende por niveles de riesgo. La metodología establece un indicador de riesgo relativo, reflejando el grado de mitigación con que cuenta el operador del servicio ante la ocurrencia de un evento en los nodos, para posteriormente identificar las acciones a realizar para reducir las probabilidades de ocurrencia, o reducir el impacto de la misma en caso de que ocurran.

Las redes más interconectadas están más expuestas a ataques lógicos que provoquen incidentes de seguridad y entre ellas sobresale la red de Internet, que es evidentemente la más expuesta a este tipo de amenazas. Las redes de transporte están menos propensas a ellas, pero son más dependientes de la infraestructura física como las obras civiles, y por lo tanto pueden ser objeto, por ejemplo, de atentados terroristas que provoquen su destrucción o mal funcionamiento. En particular los nodos y segmentos de redes de fibra óptica normalmente se emplazan en zonas alejadas de los centros urbanos, y por lo tanto es mucho más difícil su vigilancia y seguridad.

Se deben considerar las interrelaciones que los sistemas de comunicaciones tienen con otras industrias, y la dependencia de la operatividad de éstas respecto de los servicios que recibe de otras industrias. Las dependencias más importantes se muestran en la figura siguiente:



El modelo de procesos de gestión del riesgo e impacto aplicado para realizar los análisis de la infraestructura crítica, corresponde a una adaptación de lo recomendado por la OECD.

Este modelo consiste en:

- Definir los criterios de criticidad para los nodos de red.
- Efectuar la identificación de los elementos de red y sitios que cumplen con lo establecido en la etapa anterior.

- La etapa siguiente es priorizar en función de los resultados de las etapas anteriores, los nodos y sitios de mayor impacto,
- Identificar la ICT
- Identificar el listado general de las vulnerabilidades (amenazas y debilidades).

CONFIDENCIAL
Información declarada confidencial por las empresas.

La encuesta es útil como punto de referencia para efectuar en etapas posteriores, una evaluación más detallada en base a la solicitud y análisis de los antecedentes y registros que sustenten lo expresado.

Se preparó un cuestionario dirigido a los principales concesionarios de los servicios materia de esta consultoría, teniendo en cuenta los siguientes aspectos:

- Abarcar todas las redes y servicios considerados dentro del alcance.
- La recopilación de información se focalizó en los elementos de red que tienen un impacto considerable a nivel país, pero se agregó la opción que los concesionarios incluyeran nodos que a su juicio los consideraran críticos.
- Se identificaron categorías posibles de tipos de elementos de red para cada servicio en particular.

La metodología utilizada para la determinación de los índices de impacto y riesgo, usa un sistema de ponderaciones de cada atributo, de tal modo de calcular indicadores para cada elemento de red, el que al estar asociado a su ubicación o sitio identificado por su dirección completa y coordenadas geográficas, permite determinar la concentración de equipos, y a su vez establecer un índice relativo de criticidad para cada recinto.

Para determinar un orden relativo de la importancia de los elementos de red, en cuanto a su nivel de criticidad, se definen aspectos principales e independientes, para lo cual se establecieron sendos índices, formado cada uno de ellos a su vez por un conjunto de atributos con una determinada ponderación, y que corresponden a:

- Índice de ***impacto de nodos***. Este índice refleja en forma relativa el ***impacto*** que causa la indisponibilidad de un servicio.
- Índice de ***riesgo de nodos***. Este índice refleja en forma relativa el grado de mitigación con que cuenta el operador del servicio ante el ***riesgo*** de ocurrencia de una interrupción o indisponibilidad.
- Índice de ***impacto de sitios***. Es la suma de los indicadores de impacto de los elementos de red o nodos que se encuentran instalados en un mismo edificio, independiente de la red o propiedad de ellos. Permitiendo realizar un ranking relativo de los sitios más críticos

Los resultados de las respuestas enviadas por cada operador se tabularon, obteniendo una relación ordenada de los elementos de red, en que el mayor puntaje representa un nivel de riesgo o impacto mayor. Las empresas que respondieron las consultas son las señaladas en la tabla anterior. No respondieron TELMEX, CMET, ni IFX.

El aspecto más importante para decidir futuras acciones necesarias para la Protección de la Infraestructura Crítica de Telecomunicaciones, está dado por la priorización del impacto que tiene sobre los servicios de Telecomunicaciones, las amenazas y debilidades asociadas a un determinado sitio. Un resumen de este indicador se muestra en la tabla siguiente, con los 10 sitios de indicador de impacto más críticos, de acuerdo a lo calculado según la metodología explicada.

CONFIDENCIAL
Información declarada confidencial por las empresas.

La contribución al índice de impacto, de la totalidad de los nodos reportados para cada una de las diferentes redes, se muestra en la siguiente tabla

RED	INDICE DE IMPACTO
TRANSPORTE NACIONAL	71,93%
TELEFONIA MOVIL	10,30%
TRANSPORTE INTERNACIONAL	5,93%
INTERNET	4,97%
DATOS	4,85%
TELEFONIA FIJA	2,01%
TOTAL	**100,00%**

A continuación se presenta un extracto de las conclusiones que se deducen de este estudio, presentándose en primer lugar las que corresponden al estudio de la literatura internacional sobre esta materia, y finalmente las conclusiones obtenidas a partir de la realidad nacional.

Los países, muestran una manera similar de enfrentar la protección de la infraestructura crítica, lo cual se puede resumir en los siguientes puntos:

- En todos los países estudiados existen objetivos políticos claros de protección de la ICI, con un compromiso y soporte visible desde un punto de vista de liderazgo nacional, reflejado en la estructura y organización del rol y responsabilidad del gobierno.
- Cada país cuenta con una organización vertical en el tema de la ICI, dirigida desde el más alto nivel del gobierno, el que por medio de las políticas y acciones tendientes a asegurar sus recursos críticos, da el ejemplo al resto de la sociedad.
- La definición de la infraestructura y sectores críticos es la primera actividad a enfrentar, y requiere la participación del sector privado, además del gobierno.
- Los gobiernos le dan carácter de urgencia y de primera importancia al aseguramiento de sus activos, en especial existe gran preocupación por la seguridad cibernética.
- Se deben tomar en cuenta las interdependencias que existe entre los diferentes sectores que gestionan infraestructura crítica.
- Debe existir una revisión sistemática y periódica de la política y marco legal y esquemas de auto regulación que aplica al manejo de la infraestructura crítica.
- Todos los países reconocen la importancia de la asociación Público-Privado y los gobiernos impulsan el intercambio de información con el sector privado, ya que la mayor parte de la infraestructura es de propiedad y operada por privados.
- Uno de los principales desafíos, es alcanzar un equilibrio entre los requerimientos de seguridad y los imperativos de eficiencia de los negocios. Es relativamente fácil llegar a acuerdos sobre la existencia de problemas y la necesidad de resolverlos, pero es muy difícil llegar a acuerdo sobre las medidas a tomar, los responsables de implementarlas, la responsabilidad legal de dichas medidas y quién las financia.

- Existe conciencia que el riesgo no puede ser eliminado totalmente, y que algún nivel de riesgo debe ser aceptado por la sociedad, existiendo un balance entre costos versus seguridad.
- En la mayor parte de los países se han establecido comités, fuerzas de tarea y grupos de trabajo, cuyo mandato incluye trabajo de escenarios, evaluación de medidas, o establecimiento de sistemas de alerta temprana. Esto llevó al establecimiento de políticas y recomendaciones para establecer organizaciones independientes que se encarguen de los temas de la sociedad de la información y políticas básicas de CIIP.
- Se ha reconocido la necesidad de que la protección requerida a la infraestructura es tanto física como lógica.
- Para la mayor parte de los países el tema de CIIP es un tema de seguridad nacional.

En Chile, existe una amplia dispersión en el nivel de establecimiento de políticas de seguridad de la infraestructura crítica, entre las distintas empresas que respondieron el cuestionario respectivo.

Desde el punto de vista de la criticidad de los elementos de red, los más críticos de acuerdo al indicador de impacto definido, pertenecen a las redes de transporte, y a su vez son los más expuestos a amenazas de tipo físico por sus componentes instalados en espacios no controlados. Si bien estas redes cuentan con respaldo de las de otros operadores, su cercanía en el trazado en ciertos tramos, reduce la efectividad de estos respaldos. Los sitios (edificios), de mayor índice de impacto, están caracterizados fundamentalmente por el grado de concentración de nodos que se produce en dichos sitios.

CONFIDENCIAL
Información declarada confidencial por las empresas.

Respecto de las recomendaciones internacionales, las que se consideran más relevantes para ser aplicadas en Chile incluyen los aspectos de demostrar liderazgo y compromiso gubernamental en la protección de la ICI, gestionar los riesgos que afecten a la ICI, y trabajar en asociación con el sector privado.

Se recomienda profundizar el estudio de impacto de las telecomunicaciones sobre la ICI a nivel país, a partir de los resultados de este estudio. Se debe formar el correspondiente grupo de trabajo con participación de entes gubernamentales, privados, académicos, y representantes de los usuarios de los servicios, liderados por SUBTEL, abordando los siguientes aspectos:

- Realizar análisis detallados de riesgos, vulnerabilidades (amenazas y debilidades) atingentes a los sitios calificados como de mayor impacto.
- Acordar la implementación de los programas de protección, en reuniones uno a uno, entre SUBTEL y el operador de la red.
- Medición de la efectividad de las acciones emprendidas
- Evaluar y retroalimentar en forma permanente el resultado de estos planes.
- Promover y favorecer el intercambio de información, conocimiento y experiencias en la materia.

Una recomendación asociada a los sitios de ICT, es promover medidas para incentivar la desconcentración geográfica de los sitios más críticos, *CONFIDENCIAL, Información declarada confidencial por las empresas*. Para las nuevas instalaciones, se propone incorporar al estudio de su emplazamiento, el análisis de impacto por concentración, evitando la proliferación de instalaciones críticas en una misma zona geográfica, expuesta a los mismos riesgos de las otras ya existentes en el área.

Con el fin de que la población pueda estar protegida al máximo ante eventuales problemas de alguno de los proveedores de servicio móvil se recomienda estudiar la factibilidad de que los usuarios puedan acceder a un número de emergencia cuando no cuente con cobertura de su proveedor de servicio pero sí la tenga de algún otro operador.

Considerando la alta concentración de tráfico en los cables submarinos, es recomendable impulsar una regulación que permita proteger su infraestructura de cables, de los ataques externos producto de actividades industriales.

Considerando que las amenazas hacia la información provenientes de la Internet son cada vez más frecuentes y diversas, se requiere establecer una organización con los adecuados niveles de autoridad y responsabilidades para coordinar acciones de investigación, compartición de información y difusión de temas relativos a la seguridad de la Internet a nivel nacional. Se debe establecer una política para incentivar la compartición de experiencias frente a ataques a las redes y recomendar una estrategia para acordar cómo reaccionar en estos casos.

INDICE DE CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

INDICE DE GRAFICOS

1. INTRODUCCIÓN

El objetivo general de la consultoría es asesorar a SUBTEL en la definición e identificación de la infraestructura crítica de la información (ICI) para el caso de Chile, en el ámbito de las redes y sistemas de telecomunicaciones.

En forma más específica, SUBTEL ha solicitado que este estudio contemple las siguientes actividades:

- Revisar la experiencia internacional en la definición de criterios de criticidad.
- Aplicar la experiencia internacional, para desarrollar una propuesta de definición de criterios aplicables al caso chileno en relación a la infraestructura de telecomunicaciones.
- Determinar las redes de infraestructura de telecomunicaciones para los servicios de telefonía fija, telefonía móvil, e Internet, tanto alámbricas como inalámbricas.
- Definir criterios y grados de criticidad en base a análisis de riesgos

Todos estos objetivos deben abarcar a los actores públicos, privados y civiles.

2. ACTIVIDADES REALIZADAS

A continuación se incluye una breve cronología y relación de las actividades realizadas para lograr los objetivos del estudio solicitado por SUBTEL.

La adjudicación de la licitación fue notificada oficialmente con fecha 13 de Octubre del presente año. Una vez comunicada esta adjudicación, se solicitó a SUBTEL una primera reunión de inicio del proyecto, la que tuvo lugar el día 21 de Octubre. En esa reunión SUBTEL expuso las motivaciones del proyecto e informó de algunas reuniones y actividades previas realizadas con algunos operadores, y mencionó una metodología aplicada en Brasil con fines similares, sobre la cual ofrecieron entregar la información disponible. Además se aclararon algunos aspectos administrativos y de los alcances, y se definieron las contrapartes correspondientes.

Posteriormente los consultores analizaron la información disponible de la metodología utilizada en Brasil, y se analizó la factibilidad de emplearla en esta consultoría, teniendo en cuenta las limitaciones de tiempo y recursos comprometidos. Se concluyó que no era factible aplicarla totalmente, fundamentalmente por restricciones de tiempo, volumen de información, la necesidad de involucrar a más actores, y la poca información disponible respecto de la metodología, su aplicación y software de soporte. Por lo señalado, se rescataron de ella solamente los aspectos que se estimaron apropiados para las condiciones específicas del trabajo a realizar, al menos en esta etapa.

Luego, se procedió a la etapa de investigación y revisión de la experiencia internacional, que se detalla en el punto siguiente número 3, y a la elaboración de solicitud de información que se detalla en el punto número 4.

Posteriormente se realizó el análisis de las arquitecturas de todas las redes involucradas en la consultoría, y el estudio de la información disponible.

La solicitud de información a los concesionarios enviada por los consultores a SUBTEL, fue oficialmente remitida por esta última, el día 24 de noviembre. Las respuestas de las empresas se empezaron a recibir a partir del día 2 de diciembre.

El 4 de diciembre se participó en una reunión entre SUBTEL, algunas de las empresas, y los consultores, donde se aprovechó para aclarar algunas dudas, y conocer la opinión de las empresas.

Se revisó y procesó la información recibida de las empresas, y se sostuvieron reuniones individuales con algunas de ellas, con el objeto de aclarar dudas, y complementar la información que fuese necesaria.

Adicionalmente se sostuvieron reuniones con personal de la División Informática del Ministerio del Interior, encargados de las áreas de Seguridad e Infraestructura, y con un académico de la Universidad de Chile, integrante del cl.CERT

3. REVISIÓN DE LA EXPERIENCIA INTERNACIONAL

En este capítulo se incluye una revisión y el correspondiente análisis de la experiencia internacional sobre la infraestructura crítica de la información y telecomunicaciones. Las fuentes principales utilizadas corresponden a reportes de la Organización para la Cooperación y el Desarrollo Económico, OECD, y del Centro para Estudios de Seguridad con sede en Zurich que elaboró el manual denominado CIIP Handbook. En cada caso se ha extraído la información más relevante, y se seleccionaron los países que poseen características más similares a las de Chile, por su tamaño y nivel de desarrollo.

3.1. Estudio realizado por la OECD

La información que se entrega a continuación ha sido extraída del estudio realizado recientemente (diciembre 2007) por la OECD, titulado DESARROLLO DE POLITICAS PARA LA PROTECCION DE INFRAESTRUCTURA CRITICA DE LA INFORMACION [1].

La OECD es un organismo internacional que ayuda a los gobiernos a encarar los desafíos económicos, sociales y de gobierno en una economía global. Actualmente está formada por 30 países, siendo México el único de Latinoamérica, y Chile ha sido invitado a integrarse a esta organización. La OECD tiene un alcance mundial, siendo muy conocida por sus publicaciones y sus estadísticas, su trabajo cubre temas económicos y sociales desde la macroeconomía al intercambio, educación, desarrollo y ciencia e innovación.

El estudio citado corresponde a un análisis comparativo, del desarrollo de las políticas para la protección de la infraestructura crítica de la información en Australia, Canadá, Corea, Japón, Holanda, Inglaterra y Estados Unidos.

Considerando que cada país analizado, producto de su propia cultura, denomina o presenta un enfoque diferente al tema de las telecomunicaciones, en este estudio el término infraestructura crítica de la información está referido, en forma genérica, tanto a las redes como a la información que ellas soportan.

[1] http://www.oecd.org/dataoecd/25/10/40761118.pdf

El estudio realizado por la OECD, se basó en efectuar a los siete países ya indicados un conjunto de cinco preguntas, y a partir de las respuestas obtenidas se puede concluir lo siguiente:

3.1.1. Estrategia y objetivos

Todos los países se refieren en general, a la Infraestructura Crítica de Información o ICI como aquella infraestructura de información, que al no tenerla disponible, puede ocasionar pérdidas de vida, serio o grave impacto en la salud, seguridad o economía de sus ciudadanos. Todos los países han desarrollado la estrategia y objetivos de la ICI después de haber identificado cual es la infraestructura crítica.

Cada país cuenta con una organización acorde con su cultura, sin embargo la mayoría presenta una organización vertical en el tema de la ICI, la cual es dirigida desde el más alto nivel del gobierno y es éste el que, por medio de las políticas y acciones tendientes a asegurar sus recursos críticos, da el ejemplo al resto de la sociedad.

En términos prácticos existe acuerdo que, cualquiera sea la estrategia y objetivos que se tengan, el riesgo nunca será totalmente eliminado y que por lo tanto algún nivel de riesgo debe ser aceptado por la sociedad, y que debe existir un balance entre costos versus seguridad. Sin embargo, existe una tendencia a no soportar este riesgo remanente, en otras palabras, mientras más medidas preventivas se tomen, menor es la tolerancia al riesgo.

En la mayoría de los siete países analizados, la protección de la infraestructura crítica en general es coordinada desde una unidad de gobierno, el cual tiene la responsabilidad sobre un sector específico. La capacidad de estos sectores para cumplir con sus responsabilidades, depende de una variedad de factores incluyendo el grado de desregulación existente, la existencia de una cooperación entre el sector privado y el gobierno, mecanismos de intercambio de información, entre otros. Estas entidades de gobierno tienen el poder para obligar al sector privado a tomar acciones preventivas para proteger la ICI.

Los siete países tienen en común el haber establecido una asociación público-privado para estimular a los dueños y operadores de la ICI a tomar decisiones para asegurar su propia infraestructura crítica.

3.1.2. Aspectos organizacionales

Cada país tiene su propio marco organizacional con diferentes responsabilidades y han ido progresivamente estableciendo asociaciones público-privado.

En todo caso, cualquiera sea la organización que se tenga sobre la administración de la infraestructura crítica, se requiere de un fuerte liderazgo para implementar los mecanismos de aseguramiento de la infraestructura crítica. El compromiso demostrado por el más alto nivel del gobierno en estas materias entrega un mensaje claro a los dueños y operadores, de la importancia de proteger la infraestructura crítica.

3.1.3. Procesos de gestión del riesgo

Cada país ha desarrollado su propio modelo de proceso de gestión del riesgo. La figura siguiente muestra el proceso implementado en Estados Unidos sobre esta materia.

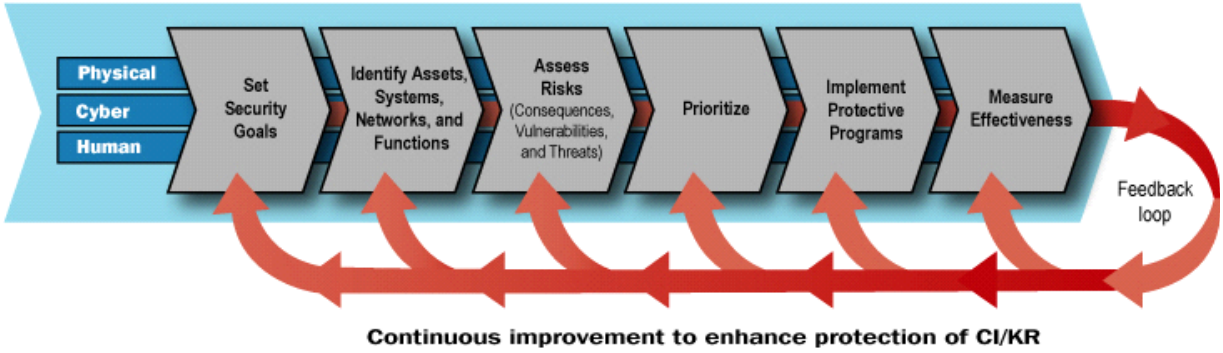


Figura 1 Modelo de procesos de gestión de riesgo

La OECD reconoce que este modelo de proceso puede ser de utilidad para tener un marco común a nivel internacional y que contiene una lógica que puede ser considerada una buena práctica para el desarrollo de una política a nivel nacional.

3.1.4. Prioridades de gestión del riesgo

Cada país analizado ha establecido diferentes prioridades de gestión del riesgo que reflejan las circunstancias así como la cultura y estilo de gobierno. Sin embargo, en todos los países las prioridades de gestión del riesgo de la ICI es parte del proceso formal de implementación de la estrategia de aseguramiento de la ICI.

La metodología utilizada por Australia es la que representa con mayor exactitud lo que de una u otra forma realizan los otros seis países analizados y que se resume a continuación:

- Identificar dependencias e interdependencias entre sistemas de infraestructura críticos.
- Análisis de las consecuencias de fallas de la infraestructura crítica
- Determinar puntos únicos de fallas y otros puntos de alta vulnerabilidad.
- Opciones de inversión y otras estrategias de mitigación de impactos
- Definir escenarios, incluyendo desastres naturales y actos de terrorismo, los cuales puedan ocasionar la interrupción del servicio de infraestructura crítica.

En general se identificó que las consecuencias y vulnerabilidades fueron más fáciles de determinar que las amenazas, lo cual puede traer como consecuencia una sobre reacción frente a las amenazas y por lo tanto una sobre exigencia e inversión para su mitigación. Esto último debiera tratarse en un análisis consensuado entre el sector público y privado para lograr un acuerdo efectivo.

3.1.5. Intercambio de información y otras iniciativas para proteger la ICI

En los siete países analizados existe consenso que el intercambio de información es un factor crítico de éxito.

El intercambio de información al interior de cada uno de los gobiernos a nivel nacional, es fuerte en todos los países. La mayoría de los países realizan reuniones periódicas y teleconferencias entre los principales actores relacionados con el tema de amenazas y vulnerabilidades o debilidades.

Todos los países han o están en el proceso de establecer foros de intercambio de información entre el sector público y privado. Todos reconocen la importancia de una relación de cooperación e intercambio de información entre ambos sectores, sin embargo reconocen que existe un alto grado de dificultad para lograr el nivel que requiere este tema.

Por lo tanto el intercambio de información entre el sector privado y público es todavía un gran desafío para los gobiernos, y en este sentido el tema es cómo manejar la información que puede ser crítica para el sector privado.

A continuación se entrega un resumen de los principales puntos de este estudio:

3.1.6. Puntos principales

- En los siete países estudiados, la infraestructura crítica de la información ICI puede ser descrita como referida a uno o más de los siguientes términos:

    - Componentes que soportan la infraestructura crítica.
    - Infraestructura que soporta componentes esenciales del quehacer del gobierno.
    - Infraestructura esencial a la economía nacional

- Los siete países estudiados cuentan con políticas y objetivos claros de protección de la ICI, con formas consistentes con la cultura de cada país. Todos muestran un compromiso y soporte visible desde un punto de vista de liderazgo nacional, reflejado en la estructura y organización del rol y responsabilidad del gobierno.

- Los siete países cuentan con una entidad a nivel nacional que desarrolla estándares de seguridad para enfrentar las vulnerabilidades (debilidades) y amenazas.

- En cada país, tanto el gobierno como el sector privado, muestran un alto compromiso con la protección de la ICI y trabajan en conjunto con el fin de tener desafíos y objetivos comunes.

3.1.7. Definición de infraestructura crítica

En general cada país analizado, en el contexto de la OECD, tiene su propia definición de infraestructura crítica y esta organización la define como:

- Aquellos sistemas de información interconectados y redes, cuya interrupción o destrucción podría producir un serio impacto en la salud, seguridad o bienestar de la

población o producir un serio impacto en el funcionamiento del gobierno o de la economía del país.

En el caso de Chile para el tema de telecomunicaciones, desde el punto de vista de SUBTEL, consideramos que la definición de infraestructura crítica debiera ser la siguiente:

- Aquellas redes de telecomunicaciones, cuya interrupción o destrucción podría producir un serio impacto en la salud, seguridad o bienestar de la población o producir un serio impacto en el funcionamiento del gobierno o de la economía del país.

En este contexto y de acuerdo a lo solicitado por SUBTEL se deben considerar para este estudio las siguientes redes:

- Telefonía fija
- Telefonía móvil
- Internet

Al aceptar la definición entregada consideramos que además de las redes indicadas se deben agregar las siguientes:

- Redes de datos
- Redes de transporte

3.2. Análisis detallados de cuatro países

Para efectos de este análisis se considerarán en forma más detallada cuatro países, que corresponden a Brasil, Australia, Canadá y Holanda.

Esta información ha sido extraída de CIIP Handbook 2008-2009 del Center for Security Studies, ETH Zurich [2]

[2] http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?lng=en&id=91952

3.2.1. Introducción

La sigla CIIP deriva del inglés por **C**ritical **I**nfrastructure **I**nformation **P**rotection, es decir Protección de Infraestructura Crítica de Información ICI. A su vez, el International CIIP Handbook 2008/2009 fue elaborado por el instituto ETH (por sus iniciales en alemán Eidgenössische Technische Hochschule), que corresponden al Swiss Federal Institute of Technology. El CIIP Handbook se enfoca en los esfuerzos gubernamentales a nivel nacional para proteger la infraestructura crítica de información. El propósito general del CIIP Handbook es proveer una visión de las prácticas de protección en una cantidad cada vez mayor de países.

El manual está principalmente orientado al uso por parte de analistas de políticas de seguridad, investigadores y usuarios finales, pudiendo ser utilizado como un trabajo de referencia para revisar el estado de desarrollo de la formulación de políticas en CIIP, o como un punto de partida para una investigación adicional en mayor profundidad.

Metodología utilizada

La investigación siguió un procedimiento de tres etapas:

- Recolección de antecedentes públicos desde sitios online, documentación gubernamental pública, y conferencias. Con estos antecedentes se escribió una primera versión borrador de la investigación para cada país.

- En una segunda etapa se solicitó a expertos en terreno que corrigieran, completaran, y actualizaran el borrador de investigación para cada país. Estos expertos son de cada país tanto del gobierno, de organizaciones gubernamentales y de instituciones académicas.

- Finalmente, todos los aportes de los expertos nacionales e internacionales se incorporaron en la versión final del estudio de cada país.

Este documento considera:

- La estructura de organizaciones que el estado ha establecido para velar por la seguridad de la información.

- Las relaciones que el estado promueve con la industria privada y comunidad de usuarios, académica e internacional con este mismo objetivo.

- El soporte legal que el estado ha construido para apoyar la seguridad de la información.

A continuación, en los puntos siguientes se entrega un resumen de algunas conclusiones del manual CIIP

3.2.2. Evolución de la Protección de Infraestructura Crítica de Información ICI

El año 1997 la comisión presidencial sobre protección de infraestructura critica de los Estados Unidos de América concluyó que el país era tan dependiente de estas infraestructuras que el gobierno debería mirarlas a través del lente de "seguridad nacional", por las serias consecuencias que se esperan para toda la nación si estos elementos no estuviesen disponibles por tiempo significativo.

Bajo este concepto la infraestructura crítica incluye activos materiales de TI, redes de comunicación, servicios e instalaciones que si son destruidas o interrumpidas provocan un impacto significativo en la salud, seguridad o bienestar económico de la población y en el funcionamiento del gobierno.

Dicha infraestructura puede ser afectada por amenazas estructurales o ataques intencionales.

- La primera categoría está compuesta por catástrofes naturales, fallas provocadas por el hombre (como fallas de diques o accidentes en reactores nucleares), falta de personal por huelga, error humano, fallas técnicas, falta de insumos, etc.

- En la segunda categoría hay una extensa lista de posibilidades, desde adolescentes aburridos, empleados insatisfechos, crimen organizado, fanáticos o terroristas hasta estados hostiles. La modalidad de ataque es igualmente extensa desde los hackers hasta la destrucción física de instalaciones.

Visto así, la infraestructura de información crítica es aquella esencial para la continuidad de los servicios de infraestructura crítica de un país. La infraestructura de información crítica es un subconjunto de la infraestructura crítica y comprende, pero no está limitada, al sector de telecomunicaciones y tecnología de la información, incluyendo componentes de

telecomunicaciones, procesadores/software, Internet, satélites, fibras ópticas, etc., necesarios para la interconexión de computadores y redes por donde fluye la información crítica necesaria para la operación de los servicios críticos.

La visión del estado de ICI en el país considera cinco aspectos

1. La definición de los sectores críticos identificados por el país.

2. Historia y situación actual de políticas e iniciativas de protección de la ICI.

3. Estructura organizacional a alto nivel en el estado para enfrentar los temas de protección de la ICI.

4. Organizaciones responsables de las alertas tempranas y estructuras para respuesta a incidentes.

5. Legislación y leyes para la promoción de la protección de la ICI.

Por otra parte se debe considerar que las amenazas sobre la infraestructura crítica no respetan fronteras, por lo que existen vulnerabilidades e interdependencias globales, sobretodo cuando estas infraestructuras utilizan para su soporte las telecomunicaciones, por lo que la protección de la ICI debe ser un esfuerzo cooperativo entre los gobiernos y los propietarios y operadores de la infraestructura crítica, tanto a nivel nacional como internacional.

Desde este punto de vista, la seguridad del ciber-espacio pasa a ser un tema fundamental de preocupación a nivel global.

3.2.3. Situación del caso de Brasil

3.2.3.1.Sectores críticos

La infraestructura crítica de Brasil incluye las áreas de petróleo, energía eléctrica y telecomunicaciones. Este tema de discusión se abordó con paneles en las áreas de:

- Seguridad pública
- Energía

- Finanzas
- Sistemas de transporte
- Suministro de agua
- Salud pública
- Telecomunicaciones

En lo que respecta a infraestructura de información crítica, el foco está en telecomunicaciones e Internet. En este sentido, ANATEL[3] desarrolló y propuso una nueva metodología para ser aplicada a la infraestructura de telecomunicaciones, de modo de entender los riesgos relacionados a ella y desarrollar un programa basado en cuatro puntos principales: contextualización, una estrategia de protección, un conjunto de metodologías, y herramientas de software para apoyarlas. Estas metodologías incluyen el desarrollo de herramientas para identificar infraestructura crítica (de información y comunicaciones) y las potenciales amenazas, para la creación de escenarios y para diagnóstico. La seguridad de información se entiende como el conjunto de estrategias globales para facilitar una respuesta organizada a las amenazas y vulnerabilidades asociadas al uso de la tecnología (ya no se ve como un problema exclusivo del sector TI, o de una industria, organización o gobierno en particular).

3.2.3.2.Políticas e iniciativas

Las políticas de Brasil para la protección de la infraestructura de información se focaliza en dos aspectos: Internet y Telecomunicaciones. Los dos sectores no pueden ser separados ya que están íntimamente ligados, y los intereses de los proveedores de Internet y telecomunicaciones para operar redes seguras están interrelacionados, y los primeros dependen de los segundos para la infraestructura vertebral y las redes de acceso.

[3] ANATEL, Agencia Nacional de Telecomunicaciones, es el regulador de las telecomunicaciones en Brasil.

3.2.3.2.1. Comité gestor de internet (CGI)

Este comité es una organización creada en 1995 y compuesta por miembros de agencias gubernamentales, operadores de telecomunicaciones, representantes de la industria de los ISP, de usuarios y de la comunidad académica. Las principales tareas de este comité son:

- Proponer las políticas y procedimientos relacionados con la regulación de las actividades de Internet.
- Recomendar los estándares técnicos y procedimientos operacionales para la Internet en Brasil.
- Establecer las directrices estratégicas para el uso y desarrollo de Internet en Brasil.
- Promover los estudios y estándares técnicos para la red y seguridad de los servicios en el país.
- Coordinar la asignación de direcciones Internet y el registro de nombres de dominio.
- Recolectar, organizar y difundir información sobre servicios Internet, incluyendo indicadores y estadísticas.

El comité mantiene tres grupos de trabajo – en ingeniería de redes, en seguridad computacional, y en entrenamiento de personal – de modo de entregar sugerencias técnicas, administrativas y operacionales para las decisiones y recomendaciones del comité. Para ejecutar estas tareas se creó la organización sin fines de lucro NIC.br.

El CGI mantiene el CERT.br (Computer Emergency Response Team Brasil) que desarrolla acciones destinadas a mejorar la seguridad en Internet, habiendo publicado un documento con las mejores prácticas de seguridad en Internet dirigido al usuario final, y otro documento con la Mejores Prácticas para Administradores de Redes Internet.

3.2.3.2.2. Programa de gobierno electrónico de Brasil (E-GOV)

El gobierno de Brasil se ve a sí mismo con un importante rol tanto como promotor y usuario de las tecnologías de información y comunicaciones. El gobierno ha adoptado avanzadas tecnologías para sus procesos administrativos y para la entrega de servicios a los ciudadanos. El año 2000 lanzó una iniciativa de gobierno electrónico con tres objetivos

básicos: universalización de servicios, accesibilidad para todos al gobierno, y mejoramiento de la infraestructura.

Se creó el Comité Ejecutivo de Gobierno Electrónico en 2008. Tres años después se crearon 8 comités técnicos de gobierno electrónico. (http://www.governoeletronico.gov.br).

3.2.3.3.Organización

Los mayores esfuerzos de Brasil en relación a la protección de la ICI incluyen el Comité de Seguridad de la Información, las políticas nacionales sobre ICT establecidas bajo el auspicio del Ministerio de Ciencias y Tecnología y del Ministerio de Comunicaciones, así como del NIC Brasilero.

Los aspectos de seguridad de la información están bajo la jurisdicción del Gabinete de Seguridad Institucional (GSI), [4] el que creó el Comité de Seguridad de la Información.

La cooperación entre los sectores privado y público es impulsada por ANATEL (ente regulador), SERPRO (Servicios de procesamiento de datos federal), y CERT.br (Equipo de Respuesta a Emergencias Computacionales de Brasil).

3.2.3.3.1. Agencias públicas

- COMITÉ GESTOR DE SEGURIDAD DE LA INFORMACION (CGSI)

Se creó el año 2000 y está compuesto por representantes de cada ministerio. http://www.planalto.gov.br/gsi/cgsi. Este define, a través de grupos de trabajo, la dirección de futuras políticas de la administración federal brasilera y controla que se establezcan las políticas de seguridad de información en cada departamento de la administración federal brasilera.

La seguridad de información se define como la protección de la información frente a: denegación de servicio a usuarios autorizados, intrusión o modificación no autorizada de los datos e información. Se mira en un amplio espectro, incluyendo la seguridad de los recursos humanos, de documentos, de áreas e instalaciones de computación y comunicaciones, así como de prevenir, detectar, detener y documentar eventuales amenazas.

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

- POLITICAS NACIONALES DE ICT

El ministerio de Ciencias y Tecnología mantiene un programa dedicado a las tecnologías de la información y comunicaciones (ICT). Este programa establece la política nacional en estos aspectos. El foco es hacia los aspectos de desarrollo tecnológico de las comunicaciones y la información.

El ministerio de Comunicaciones mantiene programas enfocados hacia la inclusión digital, telecomunicaciones y servicios postales.

- CENTRO DE INFORMACIÓN DE REDES DE BRASIL (NIC.BR)

  Sus actividades incluyen servicios – registro.br, CERT.br, y PTT.br (PIT)– al igual que proyectos como antispam.br, indicadores y estadísticas (a través del Centro de Estudios sobre las Tecnologías de Información y Comunicaciones – CETIC.br) y las cartillas de seguridad Internet.

3.2.3.3.2. Asociación público - privada

- ANATEL

La Agencia Nacional de Telecomunicaciones es el ente regulatorio federal del Brasil, creado luego de la privatización de Telebras, siendo su principal rol el de la regulación, concesiones, y supervisión de los servicios de telecomunicaciones en el país. Uno de los aspectos más importantes de su quehacer es el lograr la cooperación entre el Gobierno y el sector privado, habiendo tomado pasos para enfrentar los aspectos de seguridad en lo referente a la infraestructura del sector de telecomunicaciones del Brasil.

La metodología propuesta y utilizada por Anatel para la identificación de la infraestructura crítica – llamada MI2C – es la utilizada para definir los componentes críticos de la infraestructura de telecomunicaciones.

- SERPRO

El servicio de procesamiento de datos provee los servicios de red para sistemas TI de todas las reparticiones del Gobierno. Dispone de un comité de seguridad de 35 personas que desarrollan las políticas de seguridad para los sistemas del gobierno. Coopera en materias de seguridad con CERT.br y con CGI.

- CERT.br

Tiene una estrecha alianza con el Software Engineering Institute (SEI) de Carnegie Mellon en materias de educación, teniendo acceso a cursos en estas materias. Adicionalmente es miembro del centro de coordinación CERT del SEI.

CERT.br es miembro del Forum of Incident Response and Security Teams Global (FIRST) el que aglutina un conjunto de Computer Security Incident Respond Teams (CSIRTs) del sector gobierno, comercial y educacional a nivel mundial.

CERT.br es también miembro del Anti-Phishing Working Group (APWG), asociación industrial y legal a nivel mundial dedicada a la eliminación del fraude y robo de identidades.

3.2.3.4.Alerta temprana y difusión pública

- CTIR Gov

El Centro de Tratamiento de Incidentes de Seguridad en Redes Computacionales de la Administración Pública Federal de Brasil, depende de la GSI y ve todos los aspectos relacionados con incidentes en la redes de la administración pública de Brasil. CIRT Gov coordina la respuesta a incidentes.

- CERT.br

Es el Computer Emergency Response Team de Brasil, depende del NIC.br. Además de manejar actividades relacionadas con el tratamiento de incidentes, trabaja para mejorar la preparación de la comunidad y apoyo para la creación de nuevos CSIRTs.

- BRAZILIAN HONEYPOTS (Cebos) ALLIANCE

Proyecto coordinado en conjunto por CERT.br y el CenPRA (Centro de Pesquisas Renato Archer), un centro de investigación del Ministerio de Ciencias y Tecnología. La red de Cebos tiene la participación de 25 instituciones incluyendo representación académica, gobierno, industria, militar, que proveen el equipamiento y mantienen sus propias redes de Cebo, generando estadísticas diarias de actividades maliciosas observadas y compartiendo esta información para propósitos de detección de intrusión.

- RNP/CASI

Es la red creada por el gobierno para desarrollo de Internet asociado al ámbito académico y de investigación sobre Internet. Esta red tiene su propio Centro de Atención para Incidentes de Seguridad – CASI - encargado de velar por todos los problemas de seguridad dentro de la RNP.

3.2.3.5.Legislación y leyes

Decreto 3505 de 13 junio 2000 establece la política de seguridad de información a utilizarse en el gobierno.

- CODIGO PENAL BRASILERO

Dos enmiendas realizadas al código penal, en el año 2000, incluyen nuevos ilícitos relativos a seguridad de la información que penalizan:

El ingreso de datos falsos, alteración o eliminación de datos en sistemas computacionales o bases de datos de la administración pública, con el propósito de obtener ventajas propias o para terceras personas o para causar daño.

La modificación o alteración de datos en sistemas de información o programas computacionales sin la autorización de una autoridad competente.

- LEYES DE CIBERCRIMEN

La ley brasilera establece como crimen el lograr acceso no autorizado a un sistema computacional o violar la privacidad de un sistema computacional perteneciente a una entidad financiera.
Se define como crimen el acceso no autorizado a sistemas computacionales o data contenido en sistemas o medios físicos de terceros.

Actualmente Brasil discute una ley más especializada del cibercrimen penalizando actividades como:

- Diseminación de códigos maliciosos que pretenden robar claves (phishing).
- Fraude a tarjetas de crédito.

- Clonación de celulares.
- Ofensas al honor.
- Diseminación de códigos maliciosos que pretenden causar daño (virus, troyano, gusanos, etc.).
- Acceso no autorizado a redes computacionales.
- Acceso no autorizado a información.
- Posesión, transporte o entrega de dicha información.
- Publicación no autorizada de bases de datos.
- Interrupción de servicios de utilidad pública.
- Ataque a una red de computadores – DoS, DDos, DNS, etc.

3.2.4. Situación del caso de Australia

3.2.4.1.Sectores críticos

Australia aplica un enfoque global al concepto de protección de infraestructura crítica. La definición por ellos aceptada es "Aquellas instalaciones, cadenas de suministro, tecnología de la información y redes de telecomunicaciones que, si son destruidas, degradadas o están indisponibles por un período de tiempo prolongado, impactan significativamente en el bienestar social o económico de la nación o afectan la capacidad de Australia para llevar a cabo la defensa nacional o asegurar la seguridad nacional." [5]

La infraestructura de información es un subconjunto de la infraestructura crítica. El programa de protección de infraestructura crítica es dirigido por el Attorney-General's Department (AGD), principalmente a través de la interacción con los 9 sectores considerados críticos en Australia [6]. Estos sectores son:

[5] Attorney-General's Department National Security Website.
http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_CriticalInfrastructureProtection
[6] http://www.tisn.gov.au/agd/WWW/TISNhome.nsf/Page/Business-Govt_partnership

- Comunicaciones
- Energía
- Bancos y Finanzas
- Alimentación
- Servicios de Emergencia
- Salud
- Sitios de congregación de personas
- Transporte
- Servicios Básicos

3.2.4.2.Políticas e iniciativas

Principios rectores de la política CIP de Australia [7]

La protección de infraestructura crítica (CIP) requiere la participación activa de los propietarios y operadores de la infraestructura, reguladores, entidades profesionales y asociaciones de industria, en cooperación con todos los niveles de gobierno y el público.

Para asegurar la cooperación y coordinación, todos los partícipes deben adherir al siguiente conjunto de principios comunes de CIP.

- La CIP se centra en la necesidad de minimizar los riesgos a la salud pública, seguridad y confianza, para asegurar la economía australiana y mantener la competitividad del país, para asegurar la continuidad de los servicios prestados por el gobierno.

[7] http://www.tisn.gov.au/

- Los objetivos de CIP son identificar la infraestructura crítica, analizar sus vulnerabilidades e interdependencia, y proteger a Australia de, y prepararse para todos los riesgos.

- Considerando que no puede protegerse toda la infraestructura de todas las amenazas, se deben utilizar técnicas de gestión de riesgos para determinar su impacto relativo y duración, el nivel de protección, y para establecer prioridades para la asignación de recursos y la aplicación de las mejores estrategias para la continuidad de las actividades.

- La responsabilidad de la gestión de riesgos en la instalaciones, cadenas de suministro, tecnologías de la información y redes de comunicaciones, reside primordialmente en los dueños y operadores.

- La CIP se debe enfocar con una visión de toda amenaza, con total consideración de las interdependencias entre negocios, sectores, jurisdicciones y organizaciones de gobierno.

- CIP requiere de una asociación cooperativa permanente entre propietarios y operadores de infraestructura crítica y gobierno.

- El compartir información de amenazas y vulnerabilidades apoyarán al gobierno, a los propietarios y operadores de infraestructura crítica para una mejor gestión de riesgos.

- Se debe cuidar que al referirse a amenazas de seguridad nacional a la infraestructura crítica, incluyendo terrorismo, se evite ocasionar preocupación desmedida en la comunidad nacional y sobre potenciales turistas e inversores internacionales.

- Mejores capacidades de investigación y análisis pueden asegurar que las estrategias de mitigación de riesgos se adapten a las circunstancias particulares de la infraestructura crítica de Australia.

- CIP Y POLITICA ANTI-TERRORISMO

El Comité Nacional Anti Terrorismo (NCTC) tiene la responsabilidad de vigilar la protección de infraestructura crítica del terrorismo. La CIP, en general, es una responsabilidad compartida entre el sector corporativo y el gobierno. En el campo de CIIP la coordinación es efectuada por el Attorney-General's Department Commonwealth of Australia. ("National Counter-Terrorism Plan", (2nd ed.), September 2005). [8]

Las acciones del gobierno se encuadran en los siguientes campos:

- Identificación de la infraestructura crítica de Australia y determinación de las áreas de riesgo generales.

- Asistencia a la industria en la mitigación de sus riesgos a través de la cooperación gobierno-empresa, como lo hace a través del TISN y Grupos de Asesoría para Aseguramiento de Infraestructura (IAAGs) y a través de los gobiernos locales.

- Promoción de las mejores prácticas domésticas e internacionales en CIP.

- E – SECURITY

El gobierno estableció en 2007 una política nacional de e-security. Se creó un comité (E-Security Policy and Coordination – ESPaC) con responsabilidades amplias para coordinar la política e-security a través de las diferentes áreas. (Australian Government. "E-Security National Agenda 2007"). [9]

En la agenda se definen tres prioridades para asignar roles y responsabilidades a entidades del gobierno:

- Reducir los riesgos de e-security sobre la información y sistemas de comunicaciones del gobierno.

[8] http://www.nationalsecurity.gov.au/agd/WWW/rwpattach.nsf/VAP/(5738DF09EBC4B7EAE52BF217B46ED3DA)~NCTP_Sept_2005.pdf/$file/NCTP_Sept_2005.pdf.

[9] http://www.dbcde.gov.au/data/assets/pdf_file/71201/ESNA_Public_Policy_Statement.pdf

- Reducir los riesgos de e-security sobre la infraestructura crítica.

- Mejora la protección de usuarios domésticos y PYMEs de fraudes y ataques electrónicos.

Una de las mayores iniciativas fue la expansión del Australian Government Computer Emergency Readiness Team (GovCERT.au).

3.2.4.3.Organización

El programa CIP es liderado por el AGD, en colaboración estrecha con los propietarios y operadores de infraestructura crítica. Los esfuerzos de CIP son primordialmente coordinados a través de TISN [10], el que provee el marco para la cooperación público-privada en el campo de CIIP.

El ESPaC es un comité con responsabilidades por la política e-Security, todos los involucrados CIIP colaboran estrechamente, así lo hace(DSD), la Dirección de Señales de Defensa, la Organización Australiana de Inteligencia de Seguridad (ASIO), y la Policía Federal Australiana (AFP), los que están involucrados en arreglos operacionales conjuntos para el levantamiento y análisis de vulnerabilidades y amenazas, la respuesta a los incidentes críticos que afecten la integridad de la infraestructura de información australiana.

3.2.4.3.1. Agencias públicas

- FISCALIA GENERAL (AGD)

La fiscalía general apoya al gobierno para la mantención y mejora del sistema legal, su seguridad nacional y sistemas de gestión de emergencia. Su objetivo es promover una sociedad justa y segura. (The Attorney-General's Department. "About the Department".)[11]

En la fiscalía, la División de Seguridad e Infraestructura Critica (SCID) es responsable por el desarrollo y administración de las leyes relacionadas con el anti-terrorismo, seguridad nacional, interceptación de comunicaciones y protección de infraestructura crítica. La división coordina las acciones del gobierno para la protección de infraestructura crítica

[10] http://www.tisn.gov.au/.
[11] http://www.ag.gov.au/www/agd/agd.nsf/Page/About_the_Department

desempeñando un rol de liderazgo en el desarrollo de la relación gobierno-empresa para la protección de la infraestructura crítica. [12]

- POLITICA DE E-SEGURIDAD Y COORDINACIÓN (ESPAC COMMITTEE)

El Comité de Coordinación de Política de E-Seguridad (ESPaC) tiene como tareas: mejorar conciencia (awareness), promover las capacidades de e-seguridad, promover la investigación y desarrollo, y coordinar las políticas de gobierno relativas a e-Security. El Comité es dirigido por la AGD y está compuesto por representantes de diferentes entidades de gobierno.

- DEPARTAMENTO DE BANDA ANCHA, COMUNICACIONES Y ECONOMIA DIGITAL (DBCDE)

Participa en las actividades XIP del gobierno a través de la RED de COMPARTICION DE INFORMACIÓN CONFIABLE (TISN). Dirige y da soporte de secretaría al Grupo de Consultores Expertos en Seguridad (ITSEAG). Este grupo provee asesoría al TISN en aspectos de seguridad vigentes y nuevos que afecten a los propietarios y operadores de infraestructura crítica, incluyendo:

  - Sistemas de VoIP
  - Sistemas SCADA
  - Servicios Inalámbricos

DBCDE también provee apoyo de secretaría para el Grupo de Asesoría para el Aseguramiento de Infraestructura del Sector Comunicaciones del TISN, el que ha desarrollado un modelo de gestión de riesgo para la infraestructura crítica de comunicaciones. [13]

- EQUIPO DE RESPUESTA EMERGENCIA COMPUTACIONAL DEL GOBIERNO DE AUSTALIA (GovCERT.au)

Este equipo depende del AGD y se estableció para impulsar la preparación de Australia ante ataques sobre la seguridad de información.

[12] http://www.ag.gov.au/www/agd/agd.nsf/Page/Organisational_StructureNational_Security_and_Criminal_JusticeSecurity_and_Critical_Infrastructure

[13] http://www.dbcde.gov.au/communications_for_business/security/critical_infrastructure_security.

- GovCERT.au es responsable por:

  - Actuar como enlace con los Equipos de Respuesta a Emergencias Computacionales de otras naciones.

  - Coordinar los requerimientos de gobiernos extranjeros sobre aspectos de seguridad cibernética que afecten la infraestructura critica de Australia.

  - Coordinar la política del gobierno de Australia en cómo prepararse para, responder a, y recuperarse de una emergencia computacional que afecte la infraestructura de información nacional.

  - Gestionar el Programa de Activos de Vulnerabilidad de la Red Computacional, [14] el que provee de fondos a los propietarios y operadores de infraestructura crítica para enfrentar las inversiones de seguridad de sus sistemas IT y redes, incluyendo aspectos de seguridad física y de personal de esas redes.

GovCERT.au no se involucra en los incidentes computacionales del día a día.

- OFICINA DE GESTION DE INFORMACION DEL GOBIERNO AUSTRALIANO (AGIMO)

AGIMO es parte del Ministerio de Hacienda y Administración, provee asesoría estratégica, para actividades relacionadas con la aplicación de ICT en la administración del gobierno, su información y servicios.

Las responsabilidades de AGIMO incluyen:

- Promover la mejora de los servicios del gobierno a través de la interoperatividad técnica e interacción de los procesos de negocio a través del gobierno australiano.

- Desarrollando y mejorando los procesos del gobierno de compras electrónicas (e-procurement).

[14] http://www.tisn.gov.au/agd/WWW/tisnhome.nsf/Page/CIP_Projects#section2.

- Promoviendo convenios integrales de telecomunicaciones para todo el gobierno.

- Identificar y promover el desarrollo de la infraestructura ICT necesaria para implementar las estrategias emergentes para todo el gobierno.

- Desarrollar un marco de referencia para la autenticación en el e-gobierno de modo de verificar a los usuarios en las comunicaciones electrónicas.

En cooperación con otros organismos del estado, AGIMO lleva los contactos internacionales y representa a Australia en los foros mundiales en materias relacionadas con ICT. Asimismo, AGIMO es el encargado de administrar el dominio .gov.au.

- DIRECCIÓN DE SEÑALES DE DEFENSA (DSD)

La Dirección de Señales de Defensa es la autoridad nacional en seguridad de información e inteligencia de señales. La DSD tiene un rol integral en la protección de los sistemas de información y comunicaciones oficiales de Australia. Desarrolla sus actividades proveyendo ayuda experta a los organismos Australianos en relación a criptografía, seguridad de redes, y desarrollando guías y políticas sobre seguridad de la información.

Las actividades del Grupo de Seguridad de Información del DSD (INFOSEC) incluyen la recolección de información e incidentes, servicios de análisis y alertas, establecimiento de estándares, medidas defensivas incluyendo medidas de protección, convenios para respuesta y planes de contingencia. INFOSEC además de apoyar a las unidades del gobierno juega un importante rol trabajando con la industria en el desarrollo de nuevos productos de criptografía.

- ORGANIZACIÓN DE SEGURIDAD E INTELIGENCIA AUSTRALIANA (ASIO)

Es el servicio de inteligencia nacional y su principal rol es recabar información y producir inteligencia que permita alertar al gobierno sobre actividades o situaciones que pudiesen poner en riesgo la seguridad nacional. La ley ASIO define la seguridad como la protección de Australia y su gente del espionaje, sabotaje, violencia política, ataque a los sistemas de defensa australianos y actos de interferencia extranjera.

- POLICIA FEDERAL AUSTRALIANA (AFP)

La ley de ciber-crimen establece la necesidad de crear una organización nacional que se preocupe de las amenazas del ciber-crimen. Con este objetivo se estableció el Centro de Alta Tecnología del Crimen (AHTCC), el que provee una acción coordinada para tratar con aquellas instancias criminales de alta tecnología que afecten la jurisdicción Australiana, incluyendo la investigación de ataques contra la Infraestructura de Información Nacional.

3.2.4.3.2. Asociación público – privada

- RED SEGURA DE INFORMACIÓN PARA PROTECCIÓN DE INFRAESTRUCTURA CRÍTICA (TISN)

Ya que la mayor parte de la infraestructura crítica es de propiedad privada y operada en una base comercial, la colaboración público-privada es un componente crítico de la CIIP.

El TISN está organizado de acuerdo con los sectores de infraestructura crítica Australiana.

Cada grupo de sector (Infraestructura Assurance Advisory Group – IAAG) es dirigido por un representante del sector al que se refiere la infraestructura crítica. La membrecía se restringe a los propietarios y operadores de la infraestructura crítica y al gobierno. El soporte logístico del grupo lo da el organismo de gobierno que trata con el sector día a día.

Cada sector es representado por su presidente en el Consejo Asesor de Infraestructura Crítica (CIAC). El CIAC reporta al Fiscal General.

3.2.4.4.Alerta temprana y difusión pública

Existen dos organizaciones claves que proveen servicios de alerta temprana ante ciber-ataques. El DSD que apoya a las redes de gobierno y el Equipo de Respuesta a Emergencia Computacional Australiano (AusCERT) que provee servicios similares a operadores del sector privado.

- ESQUEMA DE REPORTE DE DETECCIÓN DE INCIDENTES DE SEGURIDAD DE INFORMACIÓN Y ANALISIS (ISIDRAS)

El DSD opera este esquema, a través del cual recolecta información de los incidentes que afectan la seguridad y operatividad de los sistemas computacionales y de comunicaciones del gobierno.

ISIDRAS permite el análisis de alto nivel de incidentes asociados a la seguridad de información del gobierno, con el objeto de mejorar el conocimiento de amenazas y vulnerabilidades, permitiendo una protección más efectiva.

- EQUIPO AUSTRALIANO DE RESPUESTA A EMERGENCIA COMPUTACIONAL (AusCERT)

AusCERT es una organización independiente, sin fines de lucro localizada en la Universidad de Queensland. Provee información de seguridad al sector privado y a algunos organismos del estado en base a un pago por servicio. Los objetivos son reducir la probabilidad de éxito de los ataques, reducir los costos de seguridad a las organizaciones, y reducir los riesgos de daños. El gobierno auspicia el Servicio Nacional de Alerta para Tecnología de la Información del AusCERT (NITAS), el que provee servicio sin costo a los suscriptores, la mayor parte de los cuales son propietarios y operadores de NII.

3.2.4.5.Legislación y leyes

- LEY DE TRANSACCIONES ELECTRONICAS

Esta ley establece las regulaciones para el uso de comunicaciones electrónicas en las transacciones, facilitando el comercio electrónico en Australia. La ley permite a la comunidad y a las empresas la opción de utilizar comunicación electrónica para tratar con las agencias de gobierno.

- LEY DE CIBER-CRIMEN

Modifica leyes anteriores para hacerlas aplicables a la búsqueda y obtención de información guardada en forma electrónica. Autoriza la investigación de grupos que utilicen la Internet para planear y llevar a cabo ciber-ataques que pudiesen interferir con el funcionamiento del gobierno, el sector financiero y la industria.

- LEY DE SEGURIDAD (TERRORISMO)

Esta ley incluye aspectos de ciber-terrorismo, incluyendo acciones o amenazas de acción que interfieran con, ó interrumpan, ó destruyan, un sistema electrónico incluyendo, pero no limitado a sistema de información, de telecomunicaciones y financiero. (Security

Legislation Amendment Terrorism Act 2002, No. 65, 2002. "An Act to enhance the Commonwealth's ability to combat terrorism and treason and for related purposes"). [15]

- LEY SPAM

Se incorporó legislación anti-spam como respuesta a la preocupación por el impacto que el spam tiene en la efectividad de las comunicaciones electrónicas y por los costos que impone a los usuarios finales. Esta prohíbe el envío de mensajes electrónicos comerciales sin el consentimiento del destinatario. [16]

3.2.5. Situación del caso de Canadá

3.2.5.1.Sectores críticos

La infraestructura crítica está compuesta por las instalaciones físicas y de tecnología de la información, redes, activos esenciales para la salud, seguridad, protección o bienestar económico de los Canadienses, y para el efectivo funcionamiento del gobierno[17]. El gobierno clasifica la infraestructura crítica en los siguientes 10 sectores:

- Energía
- Comunicaciones y Tecnología de la Información
- Finanzas
- Salud
- Alimentación
- Agua
- Transporte
- Seguridad
- Gobierno
- Industria

El gobierno reconoce que la infraestructura crítica puede estar expuesta a amenazas físicas y cibernéticas, ya sea de origen humano o natural.

[15] http://scaleplus.law.gov.au/html/comact/11/6499/pdf/0652002.pdf.
[16] http://www.dbcde.gov.au/__data/assets/pdf_file/0008/40220/Report_on_the_Spam_Act_2003 _Review-June_2006.pdf
[17] http://publicsafety.gc.ca/prg/em/nciap/about-en.asp

3.2.5.2.Políticas e iniciativas

El año 2003 el gobierno organizó bajo un departamento (Public Safety and Emergency Preparedness Canada – PSEPC), [18] la responsabilidad de mantener a los canadienses a salvo de una serie de riesgos, incluyendo desastres naturales, crímenes y terrorismo. En sus responsabilidades incluye el asegurar respuestas coordinadas a amenazas y desarrollar iniciativas y programas destinados a reforzar la infraestructura crítica de Canadá.

Dada la interdependencia entre sectores críticos, PSC ha liderado el establecimiento de asociaciones entre propietarios de infraestructura crítica pública y privada, llegando a desarrollar la Estrategia Nacional y Plan de Acción para Infraestructura Crítica.

- ESTRATEGIA NACIONAL Y PLAN DE ACCION PARA INFRAESTRUCTURA CRÍTICA

Este documento se ha elaborado para asegurar la coordinación que permita fortalecer la infraestructura crítica. Para esto la Estrategia Nacional establece un modelo para la asociación público-privada, un marco de intercambio de información y una metodología para la protección de infraestructura crítica en base a un modelo de riesgo. El Plan de Acción identifica las acciones de corto plazo para establecer las prioridades nacionales, objetivos, y requerimientos de modo que los recursos se puedan aplicar de la manera más efectiva [19].

El gobierno apoya los esfuerzos de la industria con actividades como:

- Proveyendo en forma oportuna y exacta información útil relativa a riesgos y amenazas.

- Asegurando que la industria se involucre lo antes posible en el desarrollo de actividades de gestión de riesgo y gestión de planes de emergencia.

- Trabajando con la industria para desarrollar y priorizar las actividades claves para cada sector.

[18] http://www.publicsafety.gc.ca/abt/index-eng.aspx
[19] http://www.publicsafety.gc.ca/prg/em/cip/_fl/nat-strat-critical-infrastructure-eng.pdf

El gobierno establece foros para el intercambio de información y discusión de los temas fundamentales para la protección de cada sector. Así mismo establece foros nacionales intersectoriales donde se identifican y discuten interdependencias.

El gobierno ha establecido todo un soporte a la privacidad de la información compartida en el marco de la protección de infraestructura crítica, de modo que este intercambio asegure la identificación de amenazas y vulnerabilidades, mejore las capacidades de alerta y se analicen los ataques para desarrollar mejores defensas y respuestas.

3.2.5.3.Organización

Public Safety Canada, es el organismo encargado de CIP y CIIP. En Canadá más del 80% de la infraestructura crítica es de propiedad y operada por privados, esto obliga a tener una relación efectiva entre el gobierno y el sector privado.

3.2.5.3.1. Agencias públicas

- PUBLIC SAFETY CANADA

Es el organismo encargado de asesorar en las políticas y dar apoyo al ministerio de seguridad pública en materias relacionadas con seguridad nacional, gestión de emergencias, temas policiales y otros. Al combinar la protección de infraestructura crítica con la gestión de emergencias se busca asegurar una posición de seguridad nacional más fuerte e integrada.

PSC es el punto donde se concentra la coordinación, análisis y compartición de información relacionada con amenazas físicas y virtuales sobre la infraestructura crítica.

- CENTRO INTEGRADO DE EVALUACION DE AMENAZAS (ITAC)

Este centro se creó para facilitar la recopilación de inteligencia de varias fuentes y poder dimensionar las amenazas. Esto se basa en la inteligencia y análisis de tendencias para evaluar tanto la probabilidad como las potenciales consecuencias de las amenazas. Con esta información se apoya al gobierno para coordinar las actividades de respuesta a amenazas específicas de un modo más efectivo para prevenir o mitigar los riesgos de seguridad pública.

- FORO DE ALTO NIVEL FEDERAL Y PROVINCIAL PARA EMERGENCIAS

El gobierno ha solicitado a las provincias y territorios a establecer un foro permanente de alto nivel sobre emergencias de modo que los principales actores nacionales puedan llevar adelante una discusión estratégica sobre la gestión de emergencias.

3.2.5.3.2. Asociación público-privado

El sector privado juega un rol preponderante en la seguridad del ciberespacio ya que es propietario y opera más del 80% de la infraestructura crítica nacional. Las asociaciones nacionales sectoriales han sido muy activas en los esfuerzos de mejora a CIP/CIIP, en el sector Telecomunicaciones opera la Canadian Telecommunications Emergency Preparedness Association (CTEPA). El foco actual de trabajo es en la mejora del intercambio de información entre los miembros, con el gobierno e intersectores.

3.2.5.4. Alerta temprana y difusión pública

El Centro de Respuesta Canadiense a Incidentes Cibernéticos (CCIRC) [20] del PSC encabeza las acciones a nivel nacional y es el punto de coordinación de respuestas a ciber incidentes para lo que monitorea el ambiente de amenazas las 24 horas, 7 días a la semana.

- CENTRO DE OPERACIONES DEL GOBIERNO (GOC)

El GOC es parte de PSC y opera 24 horas los 7 días de la semana para proveer la coordinación estratégica y dirigir la respuesta a un evento que afecte los intereses nacionales. Recibe y emite información relacionada con una amenaza a la seguridad de la infraestructura crítica. La información recibida por el GOC es verificada, analizada y distribuida a la organización de respuesta correspondiente, asegurando que los recursos adecuados estén en el lugar correcto en los plazos correctos.

3.2.5.5.Legislación y leyes

- CODIGO PENAL CANADIENSE

Establece castigos a que se exponen los que sin autorización obtienen servicios computacionales o interfieren funciones de un sistema computacional o cometen un delito con computadores o su información. Asimismo se castiga al que destruye o altera datos o

[20] http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx

obstruye su adecuado uso; o interfiere en la comunicación de cualquier persona autorizada para acceder a los datos.

- LEY DE GESTION DE EMERGENCIA 2007

Entró en vigor en agosto 2007 y mejora la anterior ley con medidas nuevas y más completas para fortalecer el rol federal en la gestión de emergencias y en la protección de infraestructura crítica.

Establece las tareas y responsabilidades del ministro para liderar, a nombre del gobierno, la gestión de emergencias.

En particular se hace cargo de una preocupación fundamental en el sector privado, esto es, la confidencialidad de la información compartida con el gobierno, y en particular su protección para que no sea difundida ya que esto puede dañar la posición competitiva y el negocio de un proveedor de servicio o dañar la asociación de confianza entre la industria y el gobierno.

3.2.6. Situación del caso de Holanda

3.2.6.1.Sectores críticos

El gobierno Holandés definió que su infraestructura crítica compromete a 12 sectores y 33 productos y servicios críticos. (Ministry of the Interior and Kingdom Relations. "Critical Infrastructure Protection in the Netherlands", (April 2003)). [21].

La infraestructura se considera crítica si ellas son esenciales, es un servicio indispensable para la sociedad, y si su indisponibilidad traería rápidamente un estado de emergencia o pudiese tener un efecto adverso en la sociedad a más largo plazo. Los sectores (y productos y servicios) críticos incluyen lo siguiente:

- Telecomunicaciones (Servicios de red de telecomunicaciones fijas, móviles, radiocomunicación y Navegación, comunicaciones satelitales, servicios de difusión, Acceso a Internet, servicios de correos y courier).

[21] http://cipp.gmu.edu/archive/NetherlandsCIreport_0403.pdf

- Suministro de agua potable.
- Energía (Electricidad, Gas Natural y Petróleo).
- Sector Financiero (Público y privado).
- Alimentos (Suministro y seguridad).
- Salud (Centros de Urgencia/Hospitales, Medicina Nuclear, Vacunas).
- Orden Legal (Administración de Justicia, Imposición de la ley).
- Orden Público y seguridad (Mantenimiento del orden público y la seguridad).
- Administración Pública.
- Transporte.
- Industria Química y Nuclear

La Infraestructura de Información Crítica (CII) de Holanda consiste principalmente en la infraestructura interna de soporte de sectores críticos como la energía, transporte, sector financiero que son a su vez basados en los servicios que le prestan los sectores de energía y telecomunicaciones.

3.2.6.2.Políticas e iniciativas

En Holanda se percibe CIP/CIIP como temas claves de seguridad nacional.

- PRIMEROS ESFUERZOS PARA PROTEGER LA INFORMACIÓN Y LA INFRAESTRUCTURA DE COMUNICACIONES.
    - EL DELTA DIGITAL

La publicación de este documento establece las primeras medidas en relación a la política del gobierno sobre las tecnologías de información y comunicaciones.

- INFODROME & BITBREUK

El gobierno, a través del estudio realizado por Infodrome publicó el ensayo BITBREUK para impulsar la discusión en la necesidad de protección de la CII. Este documento ofrecía un análisis inicial de vulnerabilidades y postulaba una serie de hipótesis para su posterior examen y discusión por parte de las autoridades, en cooperación con organizaciones públicas y comerciales. Esto dio origen posteriormente a la generación del programa KWINT para la mejora de la seguridad de información.

- REPORTE Y PROGRAMA KWINT

El reporte concluye en 2001, que la infraestructura Holandesa de Internet era altamente vulnerable. Hace recomendaciones respecto a políticas de educación y conciencia, coordinación de incidentes, protección y seguridad. Concluye que las medidas se deben adoptar a través de una cooperación publico-privada, siendo el gobierno responsable de desarrollar un rol de coordinador y facilitador.

Se formó un grupo de trabajo transversal con miembros de distintos ministerios. Se creo el equipo de respuesta a emergencias computacionales de gobierno GOVCERT.NL y se establecieron servicios de alerta sobre malware para la PYME y el público [22]. El programa ha estado enfocado en la protección y seguridad de Internet.

El sucesor del programa KWINT es el programa VEC, correspondiendo a una asociación público-privada que apunta a mejorar la conciencia sobre seguridad de la información y considera un proyecto piloto para apoyar a la PYME en la lucha contra el ciber-crimen.

- PROYECTO DE PROTECCIÓN DE INFRAESTRUCTURA CRITICA

En 2002 el gobierno inicia el proyecto con el objetivo de desarrollar una serie de medidas para proteger la infraestructura del gobierno y la industria, incluyendo ICT.

El proyecto incluye cuatro etapas:

- Un análisis rápido de la infraestructura para identificar los productos y servicios vitales para la nación y su interdependencia.

[22] http://www.waarschuwingsdienst.nl

- Estimulo de una asociación público-privada.
- Análisis de amenazas y vulnerabilidades.
- Análisis del gap de medidas de protección.

Para la identificación de sectores y productos críticos se desarrolló una encuesta a los diferentes organismos de gobierno, la información recolectada se presentó en sesiones de trabajo con representantes de sectores público y privado. Los resultados iniciales fueron perfeccionados en 17 reuniones de trabajo. En paralelo, expertos en seguridad evaluaron el impacto potencial de la pérdida o indisponibilidad de productos y servicios vitales (pasando a ser la esencia del problema la definición de lo que es vital a nivel nacional).

El paso siguiente incluye la identificación de los nodos vitales para cada servicio crítico, el análisis de riesgo y vulnerabilidades para cada sector crítico. Se ha establecido un proyecto CIP bajo la responsabilidad del Ministerio del Interior.

- PROGRAMA DE TRABAJO EN ESTRATEGIA DE SEGURIDAD NACIONAL

La estrategia define los objetivos de las políticas de seguridad, identifica y analiza las amenazas y riesgos, y desarrolla métodos de planificación estratégica. Considera que la seguridad nacional está bajo amenaza cuando los intereses vitales del estado y la sociedad son dañados hasta el punto en que la sociedad se puede desestabilizar. [23] .

3.2.6.3. Organización

Las responsabilidades de CI y CII en Holanda recaen sobre varios actores tanto públicos como privados. La cooperación entre estos sectores desempeña un rol crucial en la CIP y CIIP. En relación a la protección de infraestructura crítica de información, el NCO-T es el que permite la colaboración entre compañías de telecomunicaciones y el gobierno en lo que se refiere a planes de continuidad y respuesta de crisis.

[23] http://www.minbzk.nl/bzk2006uk/subjects/public-safety/national-security

3.2.6.3.1. Agencias públicas

- MINISTERIO DEL INTERIOR

Este es el responsable de la política general de CIIP, la coordinación de actividades nacionales interministeriales e intersectoriales. Adicionalmente es responsable de la CIIP de la infraestructura del gobierno, gestión de emergencias nacionales y de los aspectos CIP de los servicios de emergencia.

- MINISTERIO DE ECONOMIA

Es el responsable de coordinar CIIP con el área privada en los sectores de energía y telecomunicaciones, incluyendo Internet. Es responsable también de las políticas CIIP de la industria privada, incluyendo las PYMES.

Otros ministerios son responsables de actividades relacionadas con otros sectores críticos.

3.2.6.3.2. Asociaciones público-privada

- PLATAFORMA DE COMERCIO ELECTRONICO EN HOLANDA (ECP.NL)

Es la encargada de establecer el programa de cooperación público-privado para implementar lo establecido por el KWINT.

- PLAN NACIONAL DE CONTINUIDAD DE LAS TELECOMUNICACIONES (NACOTEL) Y FORO NACIONAL DE CONTINUIDAD DE TELECOMUNICACIONES (NCO-T)

NACOTEL fue establecido en 2002 para estructurar una política de contingencia y gestión de crisis en el sector Telecomunicaciones. Se estableció una asociación público-privada basada en la cooperación voluntaria y con la participación de empresas privadas y el Ministerio de Economía. Los miembros discutieron las posibilidades de reforzar la seguridad del sector telecomunicaciones, siendo la creación de confianzas un punto esencial en el proceso. Sin embargo, se hizo patente que una administración efectiva de crisis no se podía lograr en base a cooperación voluntaria, ya que en una crisis es probable que ciertos operadores tengan que realizar acciones que van contra sus intereses. Esto llevó a la

decisión de que la participación en el acuerdo público-privado fuese obligatoria para todos los operadores de servicios de telecomunicaciones críticos, dando origen a NCO-T [24].

- JUNTA ESTRATEGICA PARA CIP (SOVI)

Se estableció en 2006 como una asociación público-privada dedicada para la protección de infraestructura crítica. Todos los sectores críticos están representados en esta junta. En 2007 SOVI inició el estudio de la dependencia de varios sectores críticos de la energía eléctrica y su capacidad para manejar cortes de energía prolongados. La investigación incluye dependencias secundarias como es la dependencia de varios sectores del suministro de petróleo para la operación de generadores de respaldo.

- CENTRO NACIONAL DE INFRAESTRUCTURA CRITICA (NAVI)

NAVI tiene el conocimiento y experiencia en la seguridad de infraestructura crítica y su objetivo es compartir estos con empresas y entidades de gobierno de sectores críticos.

NAVI ofrece servicios de soporte para análisis de riesgo y asesoría en seguridad, buenas prácticas y contactos internacionales.

- INFRAESTRUCTURA NACIONAL CONTRA EL CIBER CRIMEN (NICC)

El NICC opera el punto de intercambio de información sobre ciber-crimen, donde las organizaciones públicas y privadas comparten información confidencial, y desarrolla y apoya proyectos y pruebas para resolver problemas concretos y para generar conocimiento sobre ciber-crimen. En esta organización cada sector dirige su propio grupo, decidiendo a qué reuniones pueden asistir entes gubernamentales y qué información se puede compartir con otros sectores.

3.2.6.4.Alerta temprana y difusión pública

- SURFCERT

Es el Equipo de Respuesta a Emergencia Computacional de SURFnet, el proveedor de Internet para las instituciones de educación superior y para muchas organizaciones de investigación en Holanda. SURFCERT maneja todos los incidentes de seguridad que

[24] http://www.ez.nl/content.jsp?objectid=150712&rid=150996

involucren usuarios de SURFnet, distribuyendo también a estos usuarios toda la información relativa a seguridad.

- GOVCERT.NL

Es el Equipo de Respuesta a Emergencia Computacional para el gobierno [25]. Opera bajo la responsabilidad del Ministerio del Interior. Este grupo opera en conjunto con el Servicio de Alerta del Ministerio de Economía / Dirección General para Energía y Telecom, el que es responsable de emitir alertas y asesoría al público y PYMEs sobre virus y otro software malicioso.

3.2.6.5.Legislación y leyes

- CODIGO PENAL

El Código Penal prohíbe ataques a Infraestructura Crítica.

- LEYES DE CRIMEN COMPUTACIONAL

La ley de Crimen Computacional II fue aprobada en Septiembre 2006.

- LEY DE TELECOMUNICACIONES

Esta ley establece los requisitos que deben cumplir los operadores de servicios públicos de telecomunicaciones en relación a capacidad, calidad y otras características de los servicios ofrecidos, así como las regulaciones relacionadas con aspectos de seguridad y privacidad que deben satisfacer en sus redes y servicios.

- CODIGO CRIMINAL, ARTICULOS 138A y 138B

Establece las penas a que quedan expuestos quienes acceden sin autorización a sistemas automáticos de almacenamiento o procesamiento de datos. Asimismo penaliza a quienes interfieren en la operación de sistemas automatizados, enviando información.

[25] http://www.govcert.nl/render.html?it=41

4. ARQUITECTURAS DE REDES

En este capítulo se presenta una visión general de las arquitecturas de las distintas redes que soportan la prestación de los servicios de telecomunicaciones a los usuarios finales, y se analizan sus principales vulnerabilidades y amenazas, además de plantearse las relaciones existentes entre esas redes y las dependencias de otras infraestructuras.

4.1. Diagramas de arquitectura de red y elementos principales

4.1.1. Modelo de capas de las distintas redes

La figura siguiente muestra las distintas redes y servicios en un modelo de capas. La capa inferior está compuesta por dos tipos de redes. En primer lugar, las Redes de Servicio (Telefonía Fija, Telefonía Móvil, Datos, e Internet) que están constituidas por un conjunto de elementos de red llamados generalmente nodos o switches, y en segundo lugar las Redes de Acceso que conectan a los usuarios finales con dichas redes de servicio. Estas redes de acceso pueden ser de distintas tecnologías, como alámbricas o inalámbricas, y las primeras a su vez pueden estar formadas por pares de cobre, cable coaxial o fibra óptica, y pueden a su vez tener distintas topologías como punto a punto, anillo, etc. Estas redes de acceso corresponden a lo que se conoce habitualmente como "la última milla".

Las distintas redes de servicio se interconectan a través de las Redes de Transporte Nacional que aparecen en la segunda capa, las cuales están preferentemente formadas por fibra óptica, aunque también existen en menor medida redes de microondas, que a su vez pueden ser terrestres y satelitales. Cada una de estas redes de transporte tiene su correspondiente equipamiento multiplexor, hoy día mayoritariamente SDH[26], y en el caso de la fibra óptica se emplea también el multiplexor WDM[27] que permite transportar distintas señales ópticas cada una de distinto λ[28], por un mismo filamento de fibra. Normalmente los cables de fibra óptica, a su vez están compuestos por varios filamentos de fibra, lo que permite que estas redes dispongan de capacidades finales sumamente altas.

La última capa corresponde a las Redes de Transporte Internacional que conceptualmente cumplen una función similar a la de las de transporte nacional, pero ahora interconectando a un país con el resto del mundo. Estas redes son mayoritariamente de fibra óptica, con cables submarinos y terrestres, y en menor medida de microondas satelitales.

[26] SDH: Synchronous Digital Hierarchy ó Jerarquí Digital Sincrónica
[27] WDM: Wavelenght Digital Multiplex ó Multiplexación Digital de Longitud de Onda
[28] Símbolo "lambda" utilizado normalmente para designar la longitud de una onda.

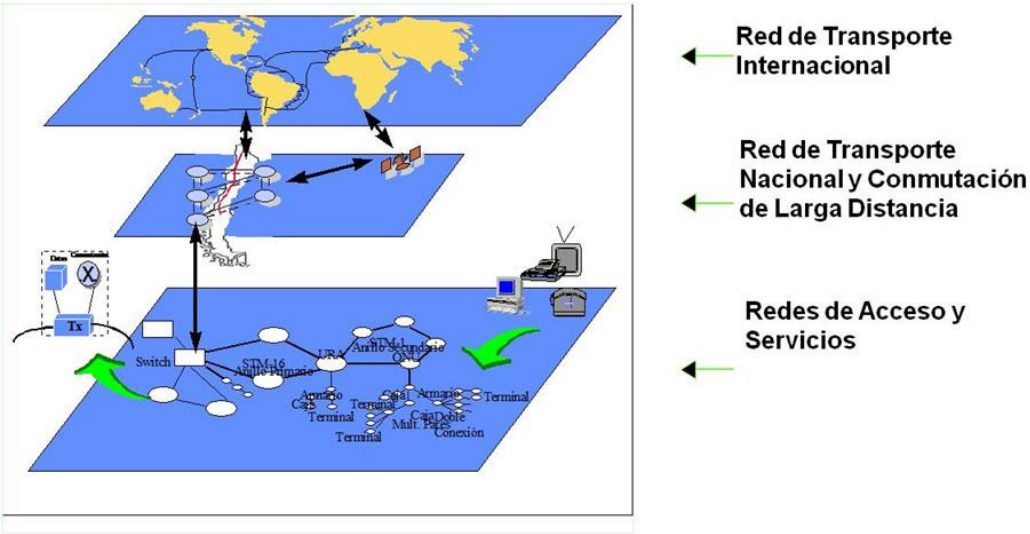


Figura 2 Modelo de capas de las distintas redes y servicios

A continuación se incluyen diagramas y descripciones de cada tipo de red considerada en el alcance del estudio. Esta información se obtuvo a través de entrevistas con los operadores, información disponible en medios públicos, información disponible de SUBTEL, y fuentes propias de los consultores. La información mencionada representa la arquitectura de alto nivel de estas redes, focalizándose en aquellos componentes más relevantes según la agregación de servicios cursados por dichas redes.

4.1.2. Telefonía fija

En este tipo de servicios, se distinguen dos tipos de arquitectura que coexisten en mayor o menor medida, dependiendo del operador específico. En el primer tipo, predomina la formada por nodos o centrales telefónicas convencionales de tecnología TDM[29], los que se interconectan a través de redes de transporte mayoritariamente de fibra óptica canalizadas con multiplexores WDM y SDH. Este tipo de arquitectura presenta una cierta jerarquía de acuerdo a la clasificación tradicional de centrales locales, primarias y de tránsito de orden superior.

[29] TDM: Time Division Multiplex ó Multiplexación por División en el Tiempo.

La segunda arquitectura corresponde a la formada por centrales de tecnología IP pertenecientes a las redes de nueva generación (NGN), y que se conocen bajo el nombre de softswitch. Estos últimos se conectan directamente usando protocolos de red y transporte TCP/IP a través de las redes de datos IP / MPLS[30], que finalmente usan la misma red de transporte de fibra óptica.

En nuestro país algunos operadores poseen mayoritariamente nodos TDM, y han incorporado sólo parcialmente la tecnología softswitch, mientras que otros operadores presentan la situación inversa, es decir la componente principal de su red telefónica está formada por softswitch y en términos secundarios por centrales TDM.

En el caso de las soluciones TDM, la arquitectura típica consiste en centrales locales o de primer nivel jerárquico, que se conectan a los abonados, ya sea directamente o a través de URAs (Unidad Remota de Abonado). Varias centrales locales agregan tráfico a través de las centrales primarias, (éstas también pueden recibir en ciertos casos conexiones directas de abonados), las que a su vez se interconectan al nivel jerárquico superior que corresponde a los centros secundarios, situación que está reflejada en las figuras siguientes. Incluso, puede existir un nivel jerárquico superior, conocido como terciario, sin embargo la tendencia de los últimos años con las nuevas tecnologías, es disminuir la cantidad de niveles jerárquicos. Las centrales de nivel superior no se conectan directamente a los usuarios finales, sino que actúan como Tándem o de paso.

[30] MPLS: Multi Protocol Label Switching

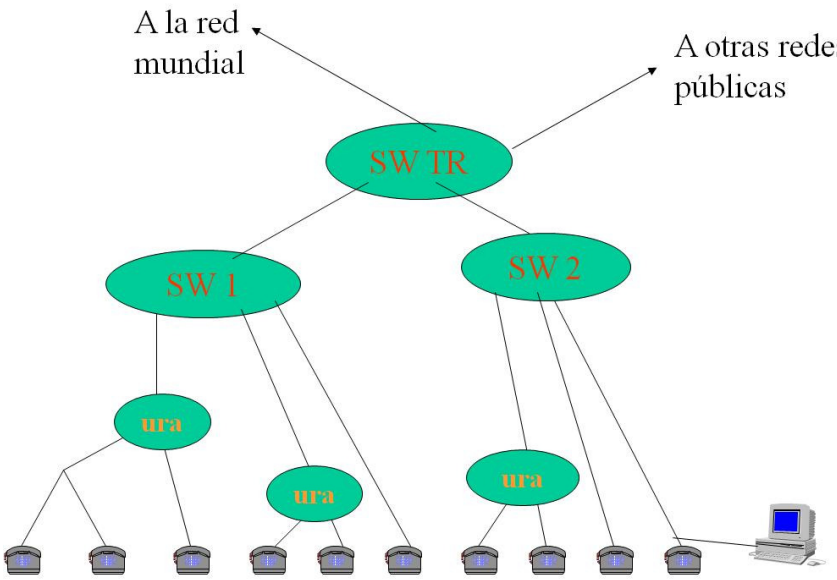


Figura 3 Arquitectura simplificada Telefonía Fija TDM

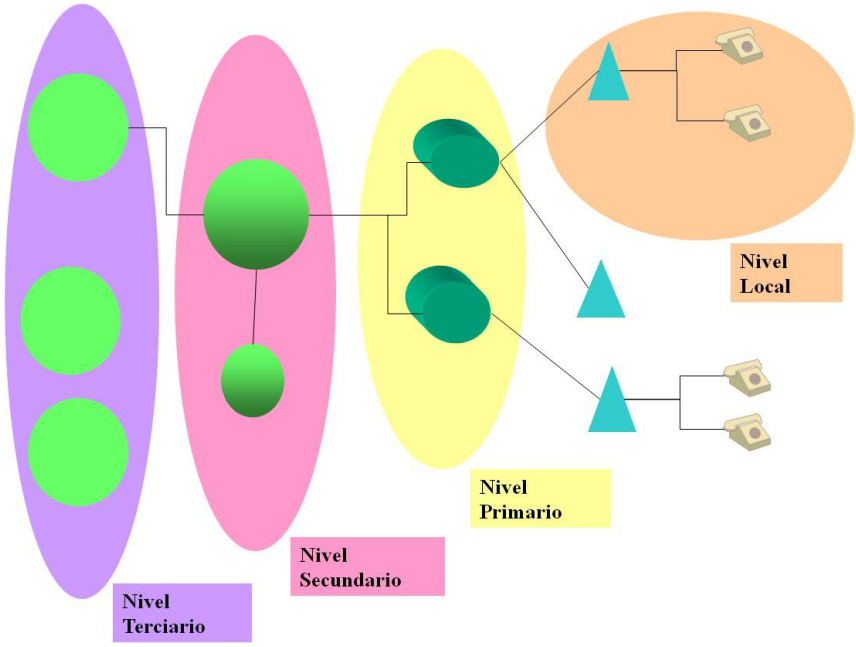


Figura 4 Arquitectura Clásica Telefonía Fija TDM

En el caso de la arquitectura NGN o softswitch, el servicio de telefonía fija que se brinda al usuario final, se cursa por la red de datos IP, usando redes de servicio ATM o MPLS, a través de un softswitch centralizado, que cumple funciones de control y señalización.

Existen además gateways que interconectan esta red con la red telefónica pública TDM convencional. Las figuras siguientes muestran en primer lugar una de las posibles configuraciones de arquitectura de red en este caso, y luego la arquitectura desde el punto de vista del servicio

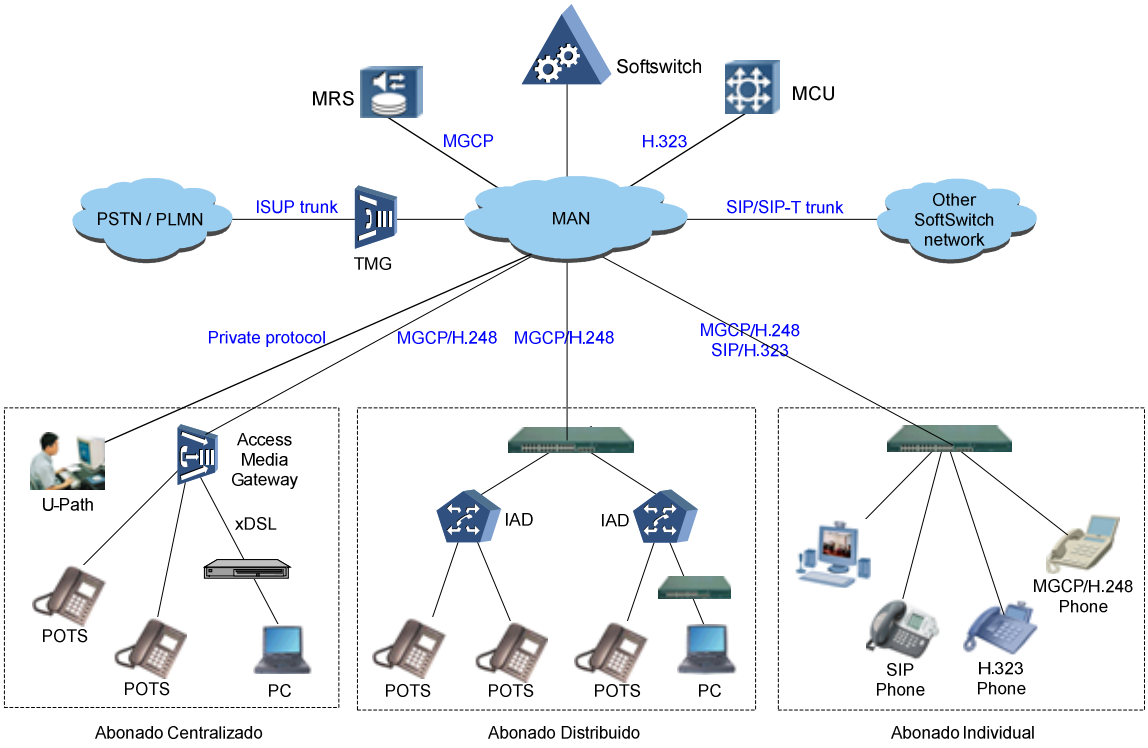


Figura 5 Arquitectura Red Telefonía Fija NGN ó IP

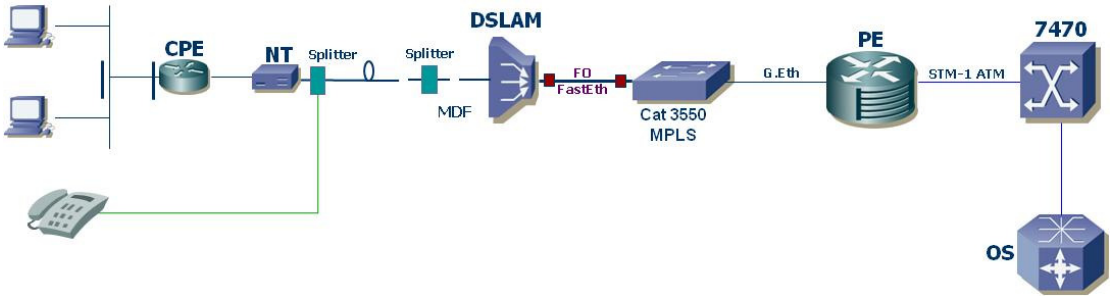


Figura 6 Arquitectura de un servicio de Telefonía Fija NGN ó IP

4.1.3. Telefonía móvil

A continuación se presentan las arquitecturas típicas de redes móviles de segunda y tercera generación, ambas actualmente utilizadas por los tres operadores de telefonía móvil en Chile.

4.1.3.1. Redes móviles de segunda generación

La figura siguiente muestra un esquema típico de este tipo red.

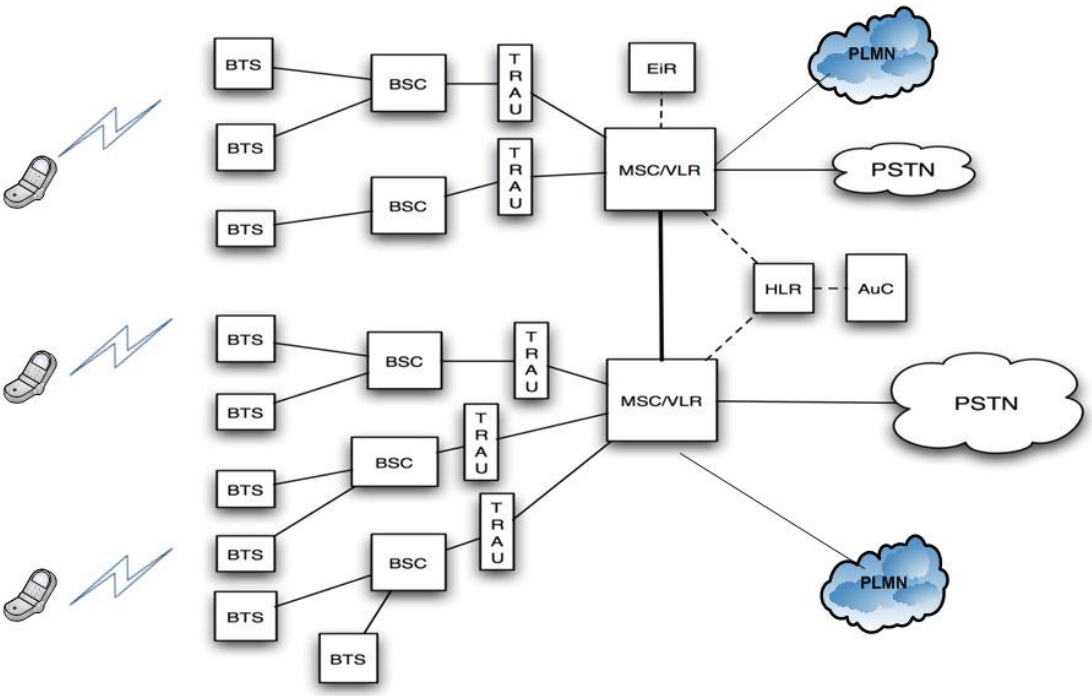


Figura 7 Esquema de red móvil 2G

En la figura se aprecia una red GSM[31] con sus principales nodos los cuales se describen brevemente a continuación. Esta red móvil no muestra los nodos involucrados en el

[31] GSM: Groupe Spécial Mobile ó Sistema Global para Comunicaciones Móviles

transporte de servicios de datos, y debe ser considerada como el estado inicial básico de las redes móviles digitales a mediados de los 90s.

Teléfono móvil o estación móvil: Es usado por el abonado para comunicarse con el núcleo del sistema celular, permitiendo al usuario acceder a los servicios proporcionados por la red, a través de la interfaz de radio. La estación móvil es anónima y no puede funcionar hasta que se le personaliza al insertarle la tarjeta inteligente SIM (Subscriber Identity Module). Esta tarjeta inteligente contiene entre otras cosas la identidad internacional del abonado, denominada IMSI (International Mobile Subscriber Identity), mientras que la identidad internacional del equipo móvil denominada IMEI (Internacional Mobile Equipment Identity) se encuentra contenida en el equipo móvil. Estos parámetros están involucrados en la autentificación del abonado.

Estaciones Transceptoras Base ó BTS (Base Transceiver Station): Corresponde al elemento de la red que hace la conexión del sistema radiante con la parte fija o cableada de la red. La BTS se compone de receptores y transmisores (Transceptores), equipos de radio, antenas, torres de soporte, pararrayos, etc.

Controlador de Estaciones Base ó BSC (Base Station Controller): Este nodo es encargado de gestionar varias BTS en lo que es relativo a los recursos de radio, como la asignación, utilización, y liberación de frecuencias, los traspasos (handover) y saltos de frecuencia.

Unidad de adaptación de velocidades y de transcodificación ó TRAU (Transcoding and Rate Adapter Unit): Esta entidad se encarga de entregar al MSC las llamadas a 64 Kbps según la codificación PCM (Pulse Code Modulation) y hacer la adaptación de velocidades. Convierte la codificación proveniente del teléfono desde 16 Kbps a PCM. El TRAU, dependiendo del proveedor, puede estar dentro del BSC o fuera de él como una entidad independiente. Como entidad independiente puede colocarse en el mismo sitio donde se encuentre el MSC reduciendo los costos de transmisión.

Centro de conmutación de móviles ó MSC (Mobile Switching Center): Este nodo es el encargado de realizar todas las acciones de control, conmutación y encaminamiento de las llamadas desde y hacia otros sistemas como el de telefonía pública conmutada PSTN (Public Switching Telephone Network), o hacia la misma u otras redes móviles. Este es el nodo central de una red móvil, es decir todas las llamadas desde redes externas hacia la red móvil y de la propia red móvil hacia teléfonos móviles y fijos

llegan al MSC, quien realiza la conmutación y control de ellas. Además el MSC realiza a diferencia de un conmutador tradicional de telefonía fija, las acciones relativas al sustento de la movilidad. Es el encargado de los procedimientos para la localización y registro de abonados y su actualización, de los procedimientos del traspaso de llamadas, gestión de llamadas, de la gestión de los protocolos de señalización. Una red móvil puede tener varios MSC y cada uno de ellos atiende una zona geográfica distinta.

Registro general de abonados ó HLR (Home Location Register): Es una base de datos que contiene toda la información relativa a los abonados de la red móvil, tales como información de ubicación del móvil y parámetros de identificación. Los datos que contiene se pueden dividir en datos permanentes y datos actualizables. Entre los permanentes esta el IMSI, servicios suplementarios suscritos, restricciones y limitaciones del servicio. Los datos actualizables son los relativos a la localización del móvil, a fin de encaminar las llamadas entrantes al MSC donde está registrado el móvil. Estos datos actualizables son por ejemplo el MSRN (Mobile Suscriber Roaming Number) utilizado para encaminar las llamadas terminadas en un móvil. En general los operadores, dependiendo de la cantidad de clientes, tienen uno o más HLR. Desde el punto de vista de la criticidad éste es un elemento esencial para el establecimiento de una comunicación móvil. Por otra parte cada MSC debe estar conectado al conjunto de HLRs, lo cual hace que también sea crítico el enlace de conexión que debe existir entre estos elementos. La interrupción del servicio de un HLR afecta a un conjunto de abonados que están distribuidos en todo el territorio.

Registro de abonados itinerantes ó VLR (Visitor Location Register): El VLR es una base de datos asociada a un MSC, donde se almacena información dinámica sobre los usuarios transeúntes en la zona controlada por ese MSC. Cuando una estación móvil se mueve fuera del área servida por un MSC y entra a una servida por otro MSC y por tanto otro VLR, este nuevo VLR se comunica con el HLR y le avisa que ese móvil ha cambiado de ubicación geográfica produciéndose una modificación en la información del HLR. El HLR a su vez envía el perfil de servicios al VLR para que el abonado pueda hacer uso de ellos en la red. El VLR guarda en sus registros la información del nuevo móvil que ahora se encuentra en su zona de cobertura hasta el momento en que el móvil abandona esa zona. Los VLRs se pueden considerar como el HLR en forma distribuida.

Centro de autentificación ó AuC (Authentication Center): Es una base de datos donde se guardan las IMSI de los abonados y la clave secreta de identificación de cada usuario, la clave secreta de identificación se encuentra también en la SIM.

Registro de identificación de equipos ó EIR (Equipment Identity Register): Es una base de datos que contiene las identidades de los equipos móviles, IMEI (International Mobile Equipment Identity), que identifican a los equipos por sus códigos de fabricación. Cuando un teléfono móvil trata de realizar una llamada, el MSC consulta al EIR si ese móvil posee IMEI válida. La implementación de esta plataforma es opcional para el operador móvil.

PSTN y PLMN: Corresponden a las redes genéricas de telefonía pública conmutada y a las redes públicas móviles respectivamente.

4.1.3.2.Redes móviles de tercera generación

La figura siguiente muestra un esquema típico de este tipo red.

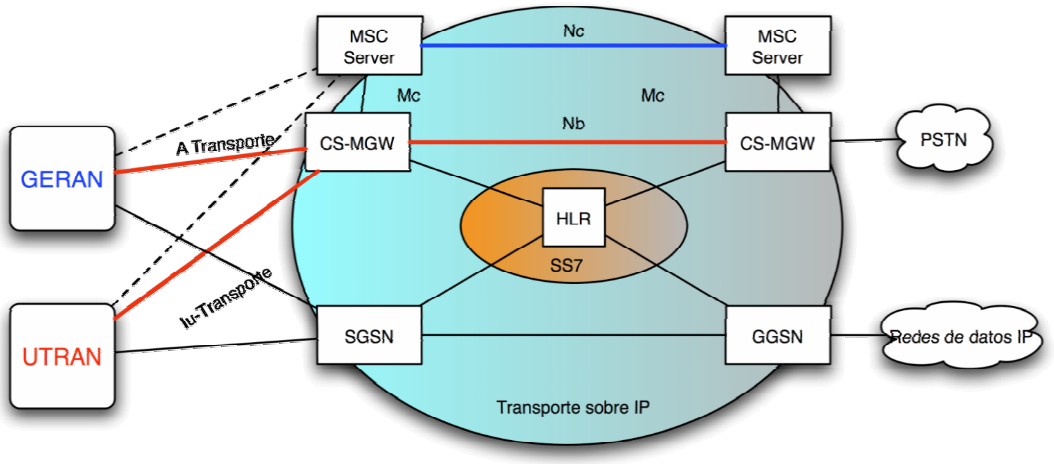


Figura 8 Arquitectura de red móvil 3G

El principal cambio de esta red con respecto a las de segunda generación es la división del dominio de circuitos conmutados, en dos entidades. En otras palabras el clásico MSC (Mobile Switching Center) es dividido en MSC Server MSC–S) y Circuit Switched Media

Gateway (CS-MGW), el MSC-S hace las partes de control y de la movilidad de la llamada de un MSC tradicional, y por su parte el CS-MGW realiza la parte del transporte del MSC tradicional.

Esta acción apunta a ofrecer una mejor eficiencia en el transporte y convergencia a nivel de transporte con el dominio de paquetes.

El MSC tradicional posee funciones de conmutación de llamadas, control de las llamadas, maneja las peticiones de traspasos de llamadas, maneja la movilidad notificando al VLR cada vez que entra y sale un móvil a su zona, interviene en los procesos para generar registros de llamadas de los abonados, mantiene una comunicación constante con las bases de datos, en definitiva interviene en casi todos los procesos que se deben hacer para que una red móvil funcione bien.

En una red de tercera generación principalmente se separan las funciones del MSC en entidades distintas, conocidas como MSC-S (Mobile Switching Center- Server) y M-MGW (Mobile Media Gateway). El primero encargado del control y movilidad de las llamadas, mientras que el segundo encargado de la conmutación de las llamadas.

La separación de las funcionalidades del MSC implica la aparición de nuevos protocolos y nuevas interfaces

Se debe mencionar que existen pocos operadores a nivel mundial que han desplegado UTRAN (UMTS Terrestrial Radio Access Network) como red de acceso, y Chile no es la excepción.

4.1.3.2.1. Entidades principales de la arquitectura de capas

- Servidor de centro móvil de conmutación o MSC-S (MSC- Server)

Este nodo se encarga de las funciones de movilidad y control de llamadas que efectúa un MSC tradicional. Como tal es responsable del control del establecimiento, mantención y terminación de las llamadas originadas y terminadas en el dominio de circuitos conmutados de la red móvil. Se comunica con los nodos de otros tipos de redes (PSTN, ISDN) para notificar y administrar las llamadas entrantes a la red móvil, para esto maneja los servicios de señalización número 7 a través de conexiones de señalización.

Este nodo es el encargado de controlar varios MGWs. También es el encargado de cambiar el formato de la señalización usuario-red al formato de señalización red-red (entre entidades del núcleo de red de conmutación).

El VLR se mantiene en esta parte de la división del MSC tradicional para, al igual que en la arquitectura anterior, reducir los tiempos de procesamiento de las llamadas.

- Puerta de enlace de medios o CS-MGW (Circuit Switched Media Gateway)

Este nodo une la parte de transporte entre las redes de acceso y el núcleo de la red móvil, o si se quiere entre el BSC y el núcleo de la red. Como se dijo, muy pocos operadores han implementado UTRAN la cual utiliza transporte ATM el MGW debe soportar varios tipos de transporte. Por ejemplo TDM desde redes de telefonía pública o desde la red de acceso GERAN en la interfaz A, ATM desde redes que utilicen ATM (UTRAN) e incluso IP para redes que utilicen IP como transporte. Al MGW se pueden conectar las redes PSTNs, ISDN, y redes de acceso móvil GSM y WCDMA, y núcleos de otras redes móviles.

El MGW es capaz de cambiar y administrar los códigos de voz empleados en diferentes redes. El transporte de la voz comprimida lo hace mediante ATM o IP.

El MGW cumple múltiples funciones en la capa de transporte que está relacionada con el usuario final, como el control de los portadores (ATM o IP) y el control del estado de la conexión.

Todas las funciones que efectúa el MGW son controladas por el MSC-S.

4.1.4. Internet

La arquitectura general de Internet corresponde a la que se presenta en la figura siguiente

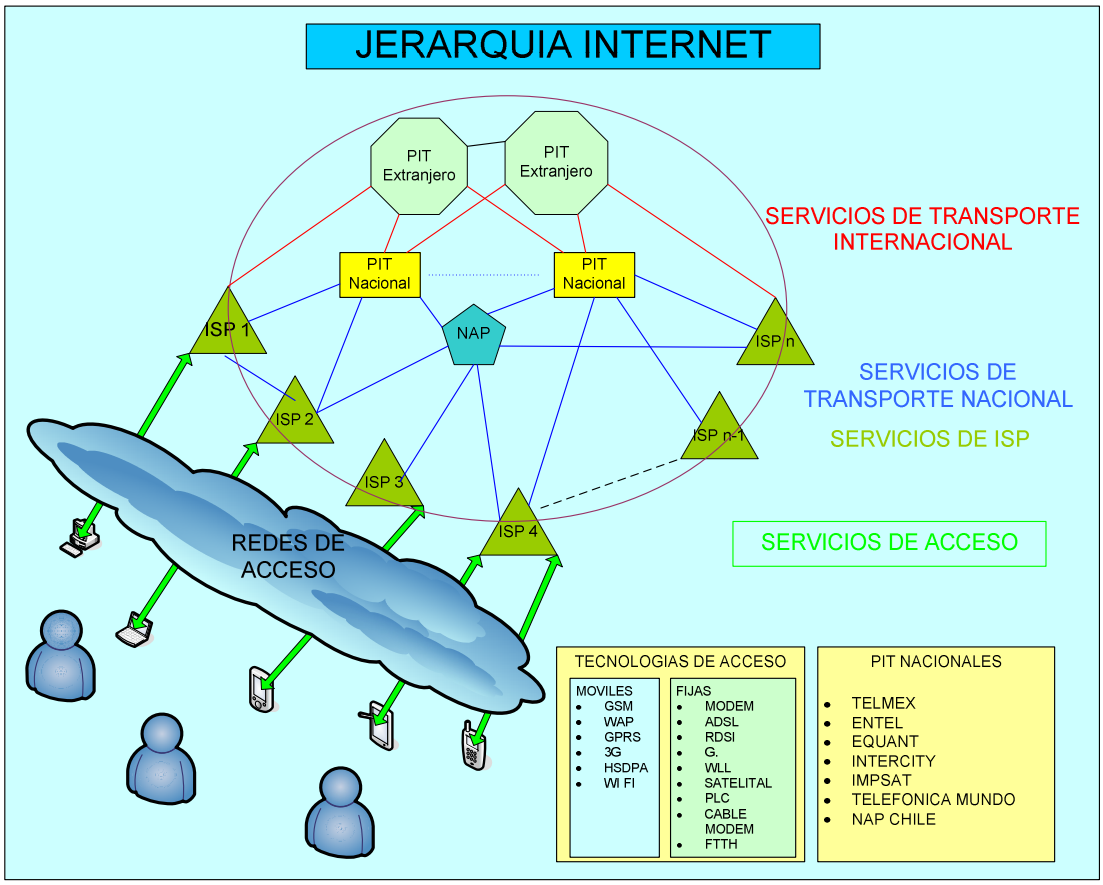


Figura 9 Arquitectura de Internet

Dentro de cada ISP se pueden distinguir diferentes elementos de red utilizados para la prestación del servicio al usuario final, como se muestra en la figura siguiente. Entre ellos se deben destacar los de uso común al universo común a los clientes, como los servidores de autenticación AAA (Accounting, Authentication, Authorization), servidor de nombres de dominios DNS, que efectúan la traducción entre la URL y la dirección IP real, el Firewall o cortafuego, y otros servidores que entregan servicios adicionales de valor agregado, como correos, antivirus, antispam, mensajería y otros. Un esquema de esta arquitectura se representa en la figura siguiente

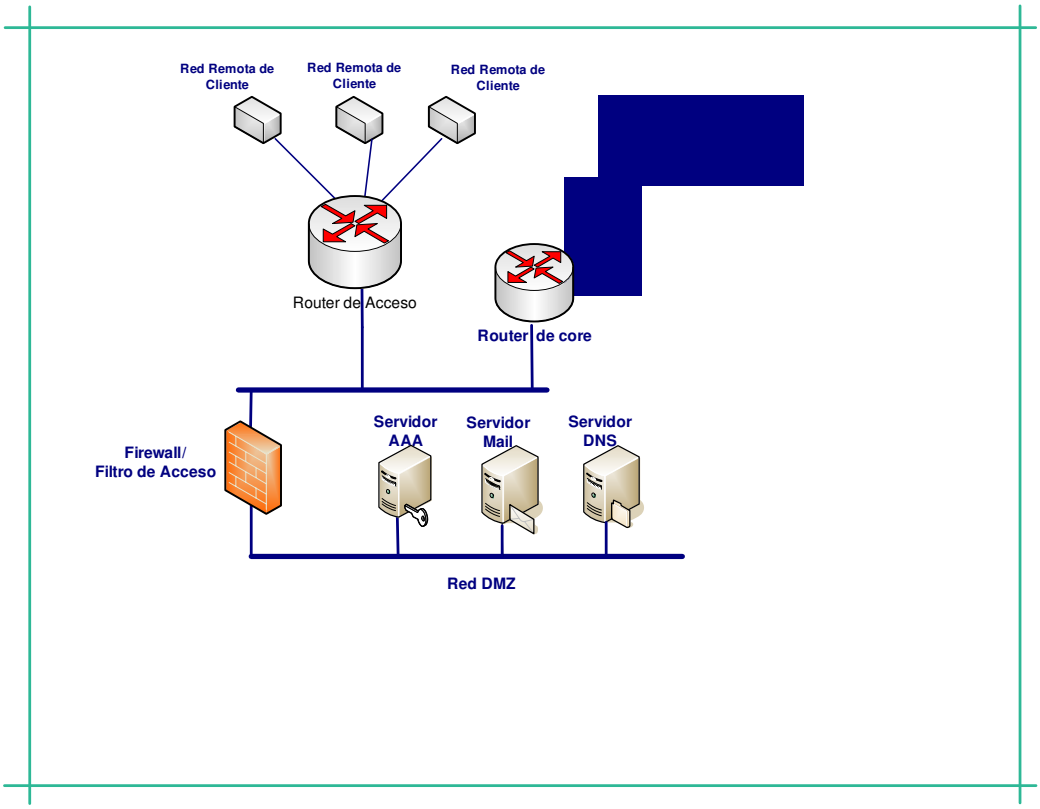


Figura 10 Arquitectura de ISP

4.1.5. Redes de Datos

La arquitectura de las redes de datos está compuesta por una capa de acceso, donde principalmente se usan redes TDM o xDSL, un backbone IP formado por nodos MPLS o ATM, y el transporte o interconexión entre los nodos se realiza mediante enlaces de fibra óptica con multiplexores SDH y WDM. Además poseen un centro de gestión de red, para funciones de operación y mantenimiento de red, y provisión y configuración de los servicios a los usuarios finales.

El diagrama siguiente muestra la arquitectura general, para el caso de una red de datos con nodos MPLS.

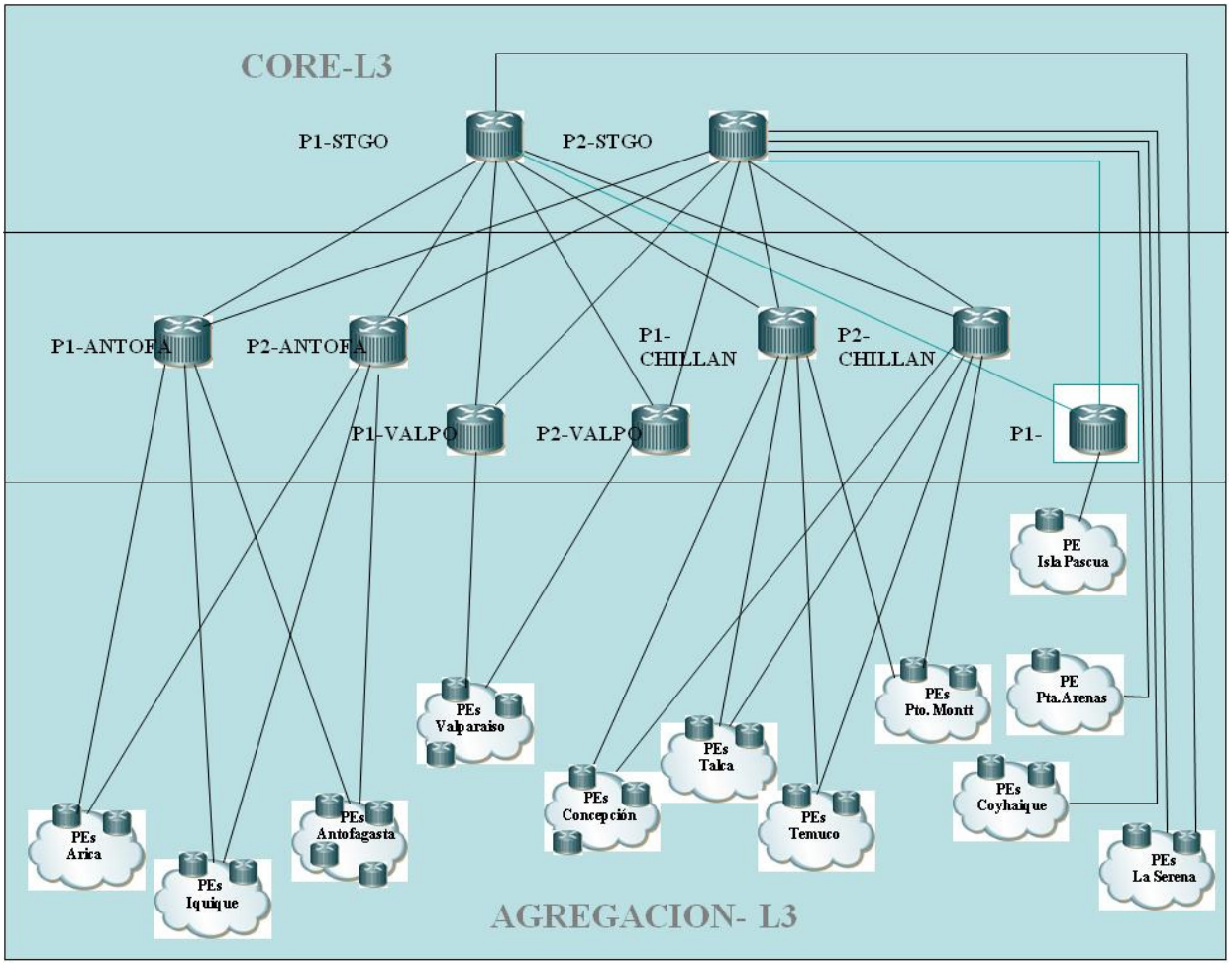


Figura 11 Arquitectura de una red de datos MPLS

4.1.6. Transporte Nacional

Tal como se comentó en el modelo de capas de red, la red de transporte nacional está formada mayoritariamente por cables de fibras ópticas y sus respectivos multiplexores SDH, más los WDM.

A continuación, se muestra un diagrama general de la arquitectura de estas redes, en que aparecen los diversos nodos interconectados a través de fibra óptica. Se debe destacar que la gran mayoría de estas redes tiene topología lineal, de acuerdo a las características geográficas de nuestro país, pero sin embargo cada operador tiene contratado respaldos con las redes similares de los otros operadores, lo que les da mayor confiabilidad. Normalmente este respaldo opera en la modalidad hot stand-by, es decir el tráfico de un operador se cursa simultáneamente por la fibra propia de éste, y a la vez por la fibra de otro operador que actúa como respaldo. De esta forma al interrumpirse la fibra óptica principal, el tráfico se sigue cursando sin interrupciones por la vía de respaldo.

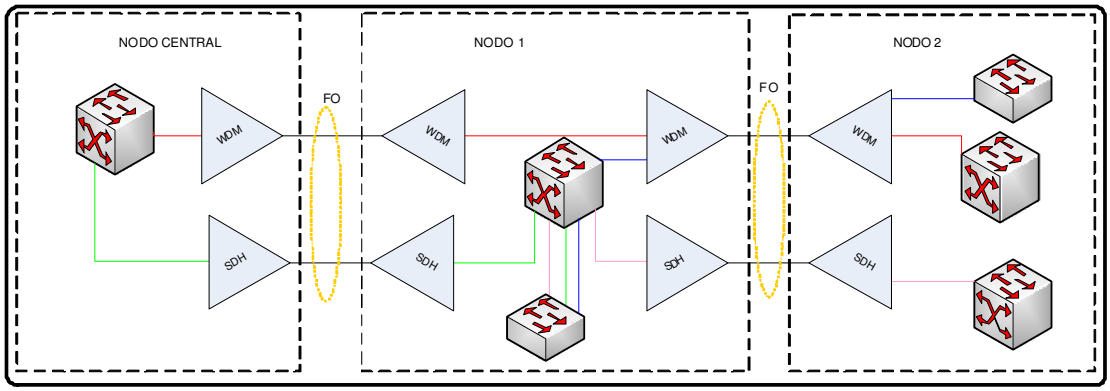


Figura 12 Arquitectura de la red de transporte de fibra óptica

4.1.7. Transporte Internacional

Tal como se adelantó, estas redes están compuestas mayoritariamente por cables de fibra óptica de tendido submarino, que usan una topología en anillo los que se cierran en el caso de Sud América por un cable terrestre.

Los operadores principales son consorcios internacionales, y para el caso de Chile éstos son TIWS (Telefónica Internacional Wholesale Services, ó Emergia), y Global Crossing (Impsat). En las figuras siguientes se grafica el trazado de estos dos anillos en el área de interés para Chile.

CONFIDENCIAL
Información declarada confidencial por las empresas.

Figura 13 Trazado red de transporte de fibra óptica internacional TIWS

CONFIDENCIAL
Información declarada confidencial por las empresas.

Figura 14 Trazado red de transporte fibra óptica internacional Global Crossing

4.2. Análisis de arquitecturas de red

4.2.1. Análisis general

Tal como se adelantó al presentar el modelo de capas en el punto 4.1.1, existe una fuerte relación entre las distintas redes que poseen los operadores, y que permiten entregar los servicios a los usuarios finales. En la figura siguiente se esquematiza con mayor detalle esta relación, indicándose además la dependencia con aspectos de infraestructura de uso común.

En primer lugar se muestran los cuatro servicios disponibles a los usuarios finales considerados en el presente estudio, Telefonía Fija, Telefonía Móvil, Datos e Internet. Cada uno de ellos requiere de la red de acceso para llegar al usuario, la que en el caso de Telefonía Móvil es siempre inalámbrica, mientras que en los otros tres casos puede ser alámbrica (usando en ese caso la planta externa), o inalámbrica.

Las redes de servicio usan además la Red de Transporte para interconectar los distintos elementos de red; y a su vez estas Redes de Transporte utilizan además los nodos de datos para una mayor eficiencia de los recursos de red.

Esto hace que estas redes de transporte tengan mayor importancia desde el punto de vista de su impacto, ya que por ellas se cursa todo tipo de tráfico. Generalmente los usuarios finales no hacen uso directo de las redes de transporte, ya que la mayoría contrata solamente servicios finales, pero algunas empresas sí lo hacen, al contratar también servicios de transporte.

A su vez, cada red de servicio tiene sus elementos de red o componentes específicos que la diferencian de las otras redes.

Por último, todas las redes requieren de cierta infraestructura básica para su implantación y operación, como obras civiles, terrenos, energía eléctrica, climatización, suministro de agua, combustibles, servicios logísticos de transporte de personal y otros, seguridad física, etc., lo que hace que todas estas redes dependan de dichos elementos para su correcto funcionamiento.

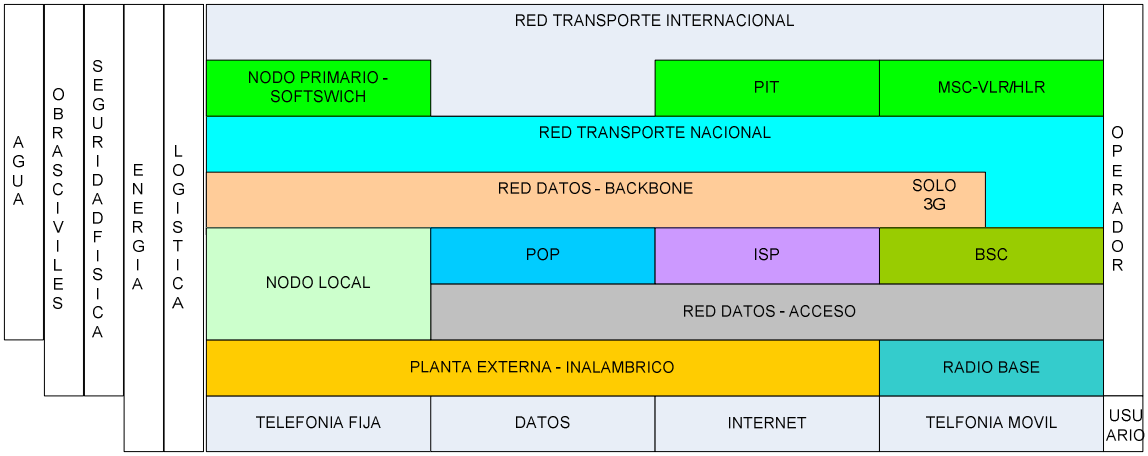


Figura 15 Relaciones entre las redes

4.2.1. Vulnerabilidades

El análisis anterior permite concluir en términos generales, y antes de considerar la situación específica de cada operador, que los servicios provistos a los usuarios finales son más vulnerables en la medida que se acercan a éste, porque dependen de más de una red compuesta por diferentes elementos y nodos, y por lo tanto están más expuestas a verse afectadas por la indisponibilidad de alguno de los elementos en la red. En el acceso al usuario final, la red de Telefonía Móvil es menos dependiente que las restantes, al no usar la planta externa que puede ser común a los otros servicios.

Por otra parte, las redes de transporte por su carácter eminentemente distribuido en su emplazamiento geográfico y por hacer uso de infraestructura física que concentra altos volúmenes de tráfico, son más vulnerables a todos los fenómenos de la naturaleza como terremotos, inundaciones, destrucciones causadas por la acción del hombre, y similares. Si bien estas redes disponen generalmente de respaldo mutuo con las otras redes de operadores, en muchos casos estas redes tienen trazados comunes por lo que el respaldo tiene carácter limitado.

En cambio las redes de servicios son vulnerables en sus nodos centrales al estar más concentradas lógicamente, como es el caso del HLR de la Telefonía Móvil. Sin embargo

estas redes igualmente dependen de las redes de transporte para la prestación de los servicios.

Las vulnerabilidades las podemos clasificar en amenazas (provienen desde el exterior de las redes) y debilidades (propias de la red o su explotación). En este sentido el listado de amenazas y debilidades aplicables a la Infraestructura Crítica de Telecomunicaciones es el que se muestra en el ANEXO 4.

Para el caso específico de las redes de cables submarinos que se utilizan mayoritariamente en el transporte internacional, una amenaza importante la constituye la pesca de arrastre. En los últimos dos años se han producido varios cortes debido a esta causa, que han interrumpido importantes sistemas internacionales, por espacio de varios días.

4.2.1.1. Vulnerabilidades de las redes de Internet [32]

Para el caso específico de las redes de Internet, hoy en día son muchos los puntos de entrada o "vectores de amenaza" utilizados para comprometer la seguridad de personas y organizaciones. Es así como existen amenazas que están orientadas a los dispositivos móviles y a equipos inseguros; a debilidades en los sistemas operativos, aplicaciones de productividad de oficinas y herramientas de criptografía; así como a numerosos otros vectores.

Amenazas en línea

En términos de la cantidad y difusión, las amenazas más significativas durante 2008 estuvieron relacionadas con las actividades "en línea". Estas amenazas en línea continúan creciendo en número y alcance.

Principales preocupaciones de seguridad

Cada día las amenazas y criminales son más rápidos, inteligentes y logran un mayor alcance, observándose que:

- Continúa la especialización e innovación en la economía del crimen en línea
- Los ataques son cada vez mas enfocados para mejorar su efectividad

[32] Según Cisco 2008 Annual Security Report

- Están ganando en frecuencia y popularidad muchos ataques del tipo "reputation hijacking" (ataques que explotan la confianza de los usuarios en la reputación de ciertos lugares)
- Cada día son más comunes las amenazas que combinan el correo electrónico, sitios Internet y el uso de técnicas de ingeniería social.

Las actividades ilícitas explotan vulnerabilidades a lo largo de toda la red para lograr el control de computadores y redes, es así como la Infección de Botnets es habitual y peligrosa. Las Botnets son redes de computadores que han sido infectados con Bots y son utilizados para realizar ataques, Bot es un programa ejecutable que puede ser activado por comandos remotos bajo el control de un sistema central. Los comandos remotos pueden incluso ir incorporados en archivos de imágenes.

- Las vulnerabilidades conocidas no son corregidas con los correspondientes parches y se ignoran las políticas de seguridad, facilitando su explotación por parte de hackers.
- La utilización de tecnologías colaborativas a través de la Internet, que mejoran la productividad de las empresas, traen nuevos riesgos a éstas.
- Las "amenazas invisibles" (tales como la infección de sitios web legítimos) están aumentando y frente a estos las soluciones de seguridad tradicionales no se muestran efectivas.
- La pérdida de información está constantemente amenazada por la explotación de vulnerabilidades en la tecnología y por la naturaleza humana. En estos casos, la reputación, confianza y finanzas de una empresa pueden verse seriamente afectadas.

Los vectores de riesgo incluyen las amenazas en línea, los dispositivos móviles y los usuarios internos. De las amenazas en línea, los *Botnets* son la base de éstas en el ciberespacio.

Los principales usos de Botnets son:

- Spamming (correo basura), incluyendo mail de phishing (delito en el ámbito de las estafas, caracterizado por intentar adquirir información confidencial de forma fraudulenta)
- Difusión de Malware (software malicioso que tiene como objetivo infiltrarse en un computador sin el conocimiento de su dueño)

- Instalación de avisos que son clickeados por los cuales alguien paga al host comercial por cada clic.
- Ataques de DDoS (denegación de servicio)
- Manipulación de encuestas en línea
- Sniffing de trafico (monitoreo)
- Key logging (registro del tecleado)

Vulnerabilidades de la Web

Siendo utilizada la Internet cada vez por una mayor cantidad de personas, para más propósitos, de maneras nuevas y no probadas, las vulnerabilidades a lo largo de todo el sistema de la red –incluyendo navegadores, aplicaciones web, servidores y parte de la infraestructura de soporte de la web- continúan creciendo en cantidad e importancia.

Muchas vulnerabilidades conocidas continúan siendo explotadas por los criminales.

Vulnerabilidades de los equipos de red

La actualización de los equipos de red normalmente no es una actividad que desarrollan los encargados de los sistemas TI, esto puede ser peligroso en el futuro si las vulnerabilidades de estos son criminalmente explotadas.

Vulnerabilidades de la Virtualización

Las empresas están cada día yendo más a la virtualización. Sea con trabajadores remotos, centros de proceso virtuales, redes virtuales, se obtienen ventajas desde el punto de vista de la flexibilidad y costo-efectividad. La virtualización requiere de buenas herramientas de administración y seguridad, probadas en ambientes reales. Durante el 2008 se observó un alto número de reportes de seguridad asociados a productos de virtualización.

DNSSEC

La industria y muchos países están trabajando duro para mitigar las vulnerabilidades del DNS (el aspecto más activo de seguridad a mediados de 2008). La implantación de DNSSEC (Domain Name System Security Extensión) se ve como crucial para proveer integridad a la información de DNS.

4.2.2. Impacto ante eventual ocurrencia de un siniestro

El aspecto más importante para definir la criticidad de una infraestructura es el impacto de una interrupción o mal funcionamiento de sus componentes, lo que queda condicionado por tres factores, que son la cantidad de usuarios que se ven afectados, duración de la interrupción o mal funcionamiento y la extensión geográfica que se afecta en caso de un siniestro.

El resultado de la etapa anterior permite, al agrupar los nodos por sitio, determinar cual sitio es más crítico que otro, y por lo tanto a cuales se les debe prestar una mayor atención en el análisis e implantación de medidas para disminuir al máximo las vulnerabilidades, (amenazas y debilidades), de esos sitios en particular.

Estos aspectos se desarrollan en forma cuantitativa en la parte correspondiente al análisis de las respuestas de los operadores.

4.2.3. Indicadores de riesgo

Otro aspecto a considerar es la probabilidad que un tipo de amenaza o debilidad se materialice, de modo que provoque el impacto estimado, y esto es lo que se entiende por niveles de riesgo. En este sentido, la metodología busca establecer un indicador de riesgo relativo, que refleje el grado de mitigación con que cuenta el operador del servicio, ante la ocurrencia de un evento en los nodos que utiliza cada servicio, de modo que posteriormente se pueda realizar un análisis más detallado que permita identificar las mitigaciones que se deben implementar para reducir las probabilidades de ocurrencia del siniestro (es decir disminuir el riesgo), o para reducir el impacto de la misma en caso de que ocurran.

En términos generales, las redes más interconectadas o abiertas al mundo son las que están más expuestas a ataques que provoquen incidentes de seguridad como la pérdida o modificación de datos, suplantación de identidades, difusión de virus informáticos, spam, denegación de servicios, y similares; y entre ellas sobresale la red de Internet, que es evidentemente la más expuesta a este tipo de amenazas. Sin embargo, las otras redes de servicio no están exentas de estas amenazas, y en la medida que en forma más creciente la tecnología las hace más dependiente de elementos de software, dichas redes pueden también verse afectadas por este tipo de ataques, afectando a la configuración de sus servidores, o a sus sistemas de tasación y facturación.

Las redes de transporte están menos propensas a este tipo de amenazas, pero son más dependientes de la infraestructura física como las obras civiles, y por lo tanto pueden ser objeto de atentados terroristas que provoquen su destrucción o mal funcionamiento. En particular los nodos y segmentos de redes de fibra óptica normalmente se emplazan en zonas alejadas de los centros urbanos, y por lo tanto es mucho más difícil su vigilancia y seguridad; en cambio para el caso de las redes de servicio si bien también están afectas a estas amenazas, es más fácil mitigarlas.

4.3. Análisis de dependencia de otras infraestructuras

Un aspecto destacado en los estudios de protección de infraestructura crítica de información, es la importancia de considerar las interrelaciones que los sistemas de comunicaciones tienen con otras industrias, y la dependencia de la operatividad de éstas respecto de los servicios que recibe de otras industrias.

Las dependencias más importantes se muestran en la Figura siguiente

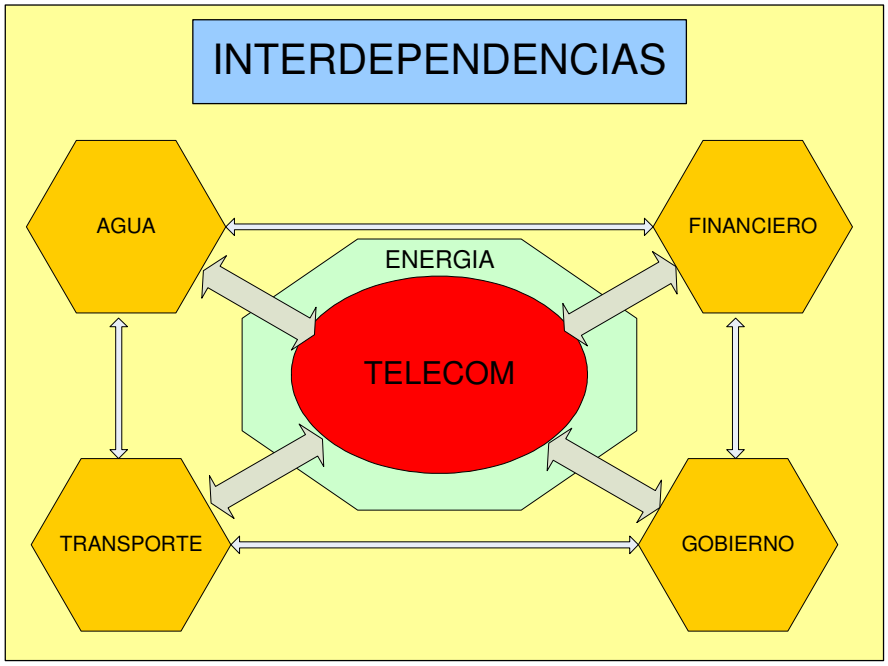


Figura 16 Interdependencia de las telecomunicaciones con otros sectores

Ejemplos de estas dependencias se indican en la siguiente tabla:

Sector	Comentario/Efecto Potencial
Energía	Se requiere del suministro de energía para mantener la operatividad de los equipamientos. Los sistemas de respaldo de energía normalmente están diseñados para un tiempo específico, si hay cortes de suministro de energía industrial más prolongados, el servicio de comunicaciones se verá interrumpido.
Transporte	El transporte es esencial: Para la operación de los canales de distribución de equipos y suministros. Para la mantención y reparación de equipamiento en terreno Para el suministro de nuevo equipamiento necesario Para el transporte de combustible a sistemas de respaldo de energía
Agua	El suministro de agua es esencial para mantener en operación los sistemas de climatización en las dependencias donde operan equipos de comunicaciones.
Servicios de Emergencia	Durante emergencias es fundamental asegurar el acceso a los sitios para la restauración de los servicios Asimismo, es necesaria una oportuna respuesta en caso de incendio u otra emergencia que afecte a un sitio crítico.
Financiero	Se requiere disponer de acceso a efectivo para mover a personal y vehículos hacia los sitios requeridos. Transacciones financieras para asegurar la provisión de servicios y equipos.

Tabla 1 Interdependencias del sector telecomunicaciones con otros sectores

A su vez, estos sectores de los cuales dependen en forma externa las telecomunicaciones, hacen un uso importante de las tecnologías de información y comunicaciones, y por lo tanto también se ven expuestos a los riesgos de ver afectada su operación normal al producirse eventos en dichos sistemas, sean éstos provistos por redes públicas o por medios propios. Además estos sectores como el de generación y distribución de energía, transporte público, suministro de agua potable, y otros, tienen un gran impacto sobre el público en general, y por ello es recomendable que se analice en forma más global el concepto de infraestructura crítica a nivel nacional, en forma multisectorial, lo cual está fuera de los alcances de este estudio.

5. IDENTIFICACIÓN DE LA INFRAESTRUCTURA CRÍTICA

5.1. Modelo de procesos

El modelo de procesos de gestión del riesgo e impacto aplicado por ZAGREB Consultores para realizar los análisis de la infraestructura crítica, corresponde a una adaptación de lo recomendado por la OECD. Este modelo consiste en:

- Definir los criterios de criticidad para los nodos de red, cuyo detalle se especifica en el punto 5.2

- Posteriormente se efectúa la identificación de los elementos de red y sitios que cumplen con lo establecido en la etapa anterior. Para la realización de esta etapa se solicitó a los concesionarios, en base a cuestionarios y planillas Excel, que detallaran los nodos que cumplían con los criterios de criticidad definidos, adjuntando además la información de la ubicación física en la cual se encuentran instalados.

- La etapa siguiente es priorizar en función de los resultados de las etapas anteriores, los nodos y sitios de mayor impacto y prestarles mayor atención. El método para determinar el nivel de riesgo e impacto de un elemento de red o nodo se explica en el punto 5.4.2 y los resultados obtenidos y comentarios se encuentran en el capítulo 6 de este informe.

- A continuación se deben identificar las vulnerabilidades (amenazas y debilidades), en los términos generales que se detallan en el Anexo 4.

- Las fases siguientes, que no están consideradas en el alcance de este estudio, se señalan en el Capítulo 8, Recomendaciones.

Para implementar las primeras etapas de este modelo, se preparó un cuestionario dirigido a los principales operadores y concesionarios de los servicios materia de esta consultoría, es decir telefonía local, telefonía móvil, Internet, redes de datos, y redes de transporte, incluyendo además los principales operadores internacionales de sistemas de cable submarinos con presencia en Chile, orientado a obtener la información necesaria para completar esta actividad y las siguientes.

La propuesta de solicitud de información a enviar a los concesionarios, se presentó a SUBTEL en reunión sostenida el día 4 de noviembre. En esa reunión se recibieron comentarios y sugerencias, los que se tomaron en cuenta para elaborar una propuesta definitiva, la que fue enviada a SUBTEL con la misma fecha.

Una vez recibida y analizada la información proporcionada por los concesionarios se procedió, en algunos casos específicos, a tener reuniones aclaratorias de la información entregada, o bien a solicitar correcciones o completar información faltante.

5.2. Aspectos de la solicitud de información a relevar

En la elaboración de la solicitud de información a los concesionarios se tuvieron en cuenta los siguientes aspectos, de acuerdo a la revisión de la experiencia internacional y la metodología aplicada:

- Abarcar todas las redes y servicios que están consideradas dentro del alcance definido por SUBTEL, es decir telefonía local, telefonía móvil, Internet, redes de datos, y redes de transporte, nacional e internacional. No se consideraron los servicios de televisión ni de radio difusión, por no estar incluidos en el alcance de la licitación.

- Por ello, y teniendo en cuenta la topología típica de las redes y servicios a nivel nacional, se prepararon cuatro planillas similares a ser llenadas por las diferentes empresas, separadas por tipo de servicio, (telefonía local, telefonía móvil, Internet, redes de datos) y dos planillas para las redes de transporte, (separadas en nacional e internacional), que soportan en forma común a los diferentes servicios que se prestan al usuario final. Algunas empresas debieron llenar varias planillas, mientras que a otras les correspondió una sola planilla, de acuerdo a los tipos de servicios según sus concesiones o giro del negocio.

- Focalizarse solamente en los elementos de red que tienen un impacto considerable a nivel país, nuevamente de acuerdo a la definición de ICI. Para ello se solicitó que los concesionarios identificaran las características principales de los elementos de red que afectan a un determinado volumen, definiéndose que el mínimo a considerar sería 50.000 usuarios para los servicios, o un tráfico equivalente de un STM – 16 (2,5 Gbps.) a nivel de red de transporte. De esta forma se le da prioridad a los elementos de mayor impacto, y se evita recargar el trabajo de recolección y

procesamiento de información, considerando que de otra forma cada operador o concesionario debería haber relevado varios miles de nodos.

- A petición de SUBTEL, se agregó la opción que los concesionarios incluyeran nodos que a su juicio los consideraran críticos, aunque no cumplieran con las condiciones de volumen de tráfico indicadas en el punto anterior. De esta forma, se permite incluir otros aspectos como el tipo de servicios o usuarios, o considerar aspectos como la cobertura de una región específica, o el aislamiento

- El criterio anterior, definió la recomendación respecto del universo de concesionarios a consultar, habiéndose sugerido no incluir en este primer estudio aquellos concesionarios que por su tamaño o características se sabe no poseen elementos de red del volumen mínimo definido anteriormente.

- En cuanto a las consultas específicas, teniendo en cuenta las características de las redes descritas en el capítulo 4, y para facilitar su procesamiento posterior, se identificaron categorías posibles de tipos de elementos de red para cada servicio en particular. Es así como se pre definieron los siguientes tipos de elementos de red por tecnología, de acuerdo a la tabla siguiente:

Telefonía Local	*Telefonía Móvil*	*Internet*	*Red de Datos*	*Red de Transporte*
CENTRAL TELEFONICA LOCAL	BSC	NODO DE COMUNICACIONES (SWITCH, ROUTER, OTRO)	NODO IP / MPLS	CABLE FIBRA OPTICA
CENTRAL TELEFONICA LD	MSC	SERVIDOR AUTENTIFICACION	NODO ATM	NODO WDM
CENTRAL TELEFONICA LOCAL Y LD	HLR	DNS	NODO TDM	NODO SDH
CENTRAL TELEFONICA INTERNACIONAL	MSC SERVER (MSS)	DHCP	NODO FRAME RELAY	MMOO
UINDAD REMOTA ABONADO	MEDIA GATEWAY	FIREWALL	NODO DSLAM	OTRO (IDENTIFICAR EN OBSERV.)
SOFTSWITCH	PLATAFORMA PREPAGO	PIT	OTRO (IDENTIFICAR EN OBSERV.)	
NODO SEÑALIZACION	GATEWAY DE TRANSITO	OTRO (IDENTIFICAR EN OBSERV.)		
OTRO (IDENTIFICAR EN OBSERV.)	PLATAFORMA SMS			
	OTRO (IDENTIFICAR EN OBSERV.)			

Tabla 2 Tipos de elementos de red

Para ponderar el impacto de una indisponibilidad, se establecieron rangos de cantidades de usuarios, mientras que para las redes de transporte, se pidió identificarlas en cantidades de tramas STM –16 equivalentes[33]. Los rangos de usuarios posibles para los diferentes servicios se segmentaron en base a las cantidades abajo indicadas o un subconjunto de ellas

- Entre 50.000 a 100.000
- Entre 100.000 a 500.000
- Entre 500.000 a 1.000.000
- Mayor que 1.000.000

Para los elementos de red de los diferentes servicios y redes que cumplieran con las condiciones de cantidad de usuarios o de tráfico, se solicitó a los concesionarios que indicaran los siguientes atributos que permitirán definir su nivel de riesgo e impacto (para el caso de las redes de transporte nacional e internacional, se agregaron además otros parámetros, atendiendo a su propiedad común a nivel de servicios):

Atributos redes de servicio (TF Fija, Móvil, Internet, Red de Datos)	**Atributos redes de transporte nacional e internacional**
Redundancia de partes comunes	Redundancia de partes comunes
Nodo redundante	Nodo propio redundante
N. A.	Redundancia con otro operador, o propia con ruta alternativa (ejemplo: anillos)
Respaldo energía	Respaldo energía
Comparte ubicación con otro nodo de la misma red	Comparte ubicación con otro nodo de la misma red
Comparte ubicación con otro nodo de otra red	Comparte ubicación con otro nodo de otra red
Comparte ubicación con otro nodo de otra red de otro operador	Comparte ubicación con otro nodo de otra red de otro holding
N. A.	Transporta servicios TF fija
N. A.	Transporta servicios TF móvil
N. A.	Transporta servicios Internet
N. A.	Transporta servicios datos
Rango de usuarios directos o indirectos	Capacidad ocupada (N° STM-16 o equivalentes)
Cantidad de regiones en que se distribuyen los usuarios	Cantidad de regiones en que se distribuyen los usuarios

Tabla 3 Atributos para redes de servicio y de transporte

[33] En la jerarquía SDH, una trama STM–16 tiene una capacidad de 2,5 Gbps., equivalentes a 30.720 canales telefónicos de 64 kbps.

La metodología considera aplicar un sistema de ponderaciones, que se detalla en el punto 5.4.2 de este capítulo, a cada uno de los distintos atributos, de tal modo de calcular un nivel de riesgo e impacto de cada elemento de red. De esta forma, para cada empresa concesionaria se obtendrá una lista priorizada de elementos de red, de mayor a menor riesgo e impacto en el servicio.

Además, en las mismas planillas se solicitó información de carácter geográfico, que permitirá identificar claramente a cada elemento de red, su ubicación a nivel de sitio identificando éste por su dirección completa y coordenadas geográficas. Por este mismo mecanismo se podrá también obtener una relación de concentración de equipos en determinadas instalaciones, lo que permitirá a su vez evaluar el grado de criticidad de dichos recintos.

La información solicitada de ubicación para cada nodo es la siguiente:

- Región
- Localidad
- Comuna
- Nombre del sitio
- Dirección
- Latitud (° sexagesimal en formato decimal DATUM WGS84)
- Longitud (° sexagesimal en formato decimal DATUM WGS84)
- Urbano /Rural

Toda la información anterior, se complementó con una solicitud adicional requerida a las empresas, en términos que ellas identifiquen los diez lugares o sitios que consideren más críticos (entendiendo por sitios cualquier ubicación que aloje equipamiento destinado a la prestación de uno o más de los servicios de Telefonía fija, Telefonía móvil, Internet, Redes de datos privadas y Transporte de señales nacional e internacional), desde el punto de vista de mayor impacto hacia los usuarios considerando para ello, que una probable indisponibilidad de estos sitios, podría afectar a una gran cantidad de usuarios y cobertura geográfica. También se les solicitó a las empresas que incluyan aquellos sitios por la relevancia del tipo de usuario al cual el nodo presta servicio, por ejemplo, si los usuarios o clientes son hospitales o entidades de gobierno o entidades financieras o empresas productivas, relevantes desde el punto de vista de sus necesidades de comunicación[34].

[34] Esta información no fue proporcionada por ningún operador por lo que no fue posible considerarla en el análisis de impacto de los elementos de red o nodos

Por último, como tercera categoría de información solicitada, se elaboró un cuestionario destinado a evaluar la situación general de la empresa respecto al aseguramiento de infraestructura crítica, sus políticas, procedimientos, difusión y otros aspectos relacionados.

A partir de dicho cuestionario se obtiene una visión general de la aplicación de las mejores prácticas a nivel mundial en la materia, aplicadas a la realidad nacional y para cada empresa del sector.

En los anexos aparecen los detalles de cada documento elaborado para requerir la información y las respuestas de los operadores.

5.3. Análisis de riesgo de la infraestructura y su impacto.

5.3.1. Criterios generales

Para realizar los análisis de riesgo de la infraestructura crítica y su estimación de impacto, se adoptó la metodología planteada por ZAGREB Consultores en su propuesta, y que en términos generales es similar a la utilizada en Australia, la que contiene los siguientes puntos:

- Identificar las dependencias e interdependencias entre los diferentes elementos que forman parte de la infraestructura crítica de los sistemas de Telecomunicaciones, aspecto que fue cubierto en los puntos 4.2 y 4.3 de este informe.

- Realizar un análisis de las consecuencias en caso de indisponibilidad de esta infraestructura crítica.

  Como primera aproximación en este aspecto, se parte de la base que todos los elementos o componentes de las redes que soportan estos servicios son igualmente importantes. Este supuesto se base en que:

  - los elementos de red o nodos en muchos casos soportan diversos servicios, condición que se acentuará en el futuro.

  - para algún sector del país es posible que hoy un servicio en particular no sea tan importante para su funcionamiento, pero en el corto plazo, en virtud de

los desarrollos que se están haciendo, podrán ser críticos. Ejemplos de esta realidad la constituyen el teletrabajo y la introducción de aplicaciones especializadas en distintas industrias, como la salud, agricultura, minería, educación y otras.

- permite realizar un primer análisis para la determinación de infraestructura crítica, concentrarse en aquellos lugares de instalación con nodos o elementos de red más críticos desde el punto de vista de cantidad de usuarios que se atienden, las áreas geográficas cubiertas por los servicios o el tráfico que cursan, incluyendo la determinación de puntos únicos de fallas y otros puntos de alta vulnerabilidad.

5.4. Metodología de cálculo

5.4.1. Metodología de cálculo de políticas de aseguramiento

Tal como se dijo anteriormente, uno de los aspectos a evaluar es la situación general de las empresas respecto al aseguramiento de infraestructura crítica, sus políticas, procedimientos, difusión y otros aspectos relacionados, lo cual se realizó en base a un cuestionario. Considerando que cada pregunta de este cuestionario tiene una valoración de 0 a 4, los rangos posibles y su correspondiente valoración, se pueden agrupar de la siguiente forma:

- Menos de 40 por ciento: El sistema global de aseguramiento de infraestructura crítica es débil, no se cumple, se cumple en aspectos parciales, y deben tomarse medidas correctoras urgentes y globales para implantar un sistema eficaz de seguridad de la información.

- Entre 40 y 60 por ciento: El sistema global de aseguramiento de infraestructura crítica se cumple, pero con deficiencias en cuanto a documentación o a la continuidad sistemática de su cumplimiento, o tiene una fidelidad deficiente con las actividades realmente realizadas. Se deberán solucionar las deficiencias urgentemente, para que el sistema sea eficaz.

- Entre 60 y 85 por ciento: El sistema global de aseguramiento de infraestructura crítica se cumple, pero con leves deficiencias en cuanto a documentación o a la continuidad sistemática de su cumplimiento, o respecto a la fidelidad con las

actividades realmente realizadas. Se deberán solucionar las deficiencias a corto plazo, para que el sistema no deje de ser eficaz. Su tendencia hacia la Gestión de la Seguridad de la información de clientes es muy positiva. Les sugerimos analicen sus puntos sobresalientes y apliquen medidas similares a los temas con más baja puntuación.

- Más de 85 por ciento: Se gestiona adecuadamente la infraestructura crítica, y son ejemplo para otras empresas del sector.

5.4.2. Metodología de cálculo de índices de criticidad

Para determinar un orden relativo de la importancia de los elementos de red, en cuanto a su nivel de criticidad, esto se define en base a aspectos principales e independientes, para lo cual se establecieron sendos índices, formado cada uno de ellos a su vez por un conjunto de atributos con una determinada ponderación, y que corresponden a:

- Índice de ***impacto de nodos***. Este índice refleja en forma relativa el ***impacto*** que causa la indisponibilidad de un servicio. Este índice está asociado a la prestación del servicio al usuario, y está dado por la cantidad de usuarios afectados, su cobertura geográfica y tiempo de restauración o duración del evento. Parámetros como la existencia de redundancia, respaldos mutuos o propios, y respaldo de energía, se consideran en virtud de la variable tiempo asociada a la restauración del servicio. En este caso, para evaluar el grado de impacto no se considera la variable relacionada con el hecho que un nodo comparta ubicación física con otro nodo sea de la misma red, de otra red o de otro operador.

- Índice de ***riesgo de nodos***. Este índice refleja en forma relativa el grado de mitigación con que cuenta el operador del servicio ante el ***riesgo*** de ocurrencia de una interrupción o indisponibilidad. El riesgo está asociado a la continuidad operacional de un equipamiento o nodo que presta un servicio, considerando los respaldos, redundancia, presencia de personas en el sitio donde se encuentra instalado el nodo sean éstas del mismo operador o pertenecientes a otros operadores del mismo holding o de otro holding. En este sentido los parámetros como cantidad de usuarios y cantidad de regiones no tienen relación con el riesgo, sino que sólo con el impacto.

Para disminuir el grado de subjetividad inherente a este proceso de determinación de índices, se tuvo especial cuidado en validar la asignación de los ponderadores, en cuanto a

que el orden relativo del peso o ponderador de cada atributo, guardara relación con su incidencia en el impacto o riesgo, según correspondiera.

- Índice de ***impacto de sitios***. Los índices de impacto y riesgo se calculan para cada nodo que cumple con los criterios pre establecidos, ahora bien, también se debe determinar el indicador de impacto o criticidad de los sitios o edificios que alojan los nodos analizados. Para esto, se suma el indicador de impacto de los elementos de red o nodos que se encuentran instalados en un mismo edificio, independiente de la red o propiedad de ellos. De esta forma se puede realizar un ranking de los sitios más críticos y concentrar en ellos, en una primera instancia, los esfuerzos tendientes a mitigar las consecuencias de las debilidades y amenazas a las que están expuestos.

En el punto siguiente se detalla la metodología empleada que permite ordenar en importancia cada uno de los atributos.

5.4.2.1. Priorización de atributos

El procedimiento para determinar el nivel de importancia relativo entre los atributos, es el siguiente:

- Determinar los atributos relevantes a clasificar y asignarles una identificación.

- Colocar la identificación asignada en las filas y columnas de la matriz de priorización como se muestra más adelante (esta es una matriz cuadrada, es decir tiene la misma cantidad de filas y columnas).

- Colocar una marca en la diagonal de la matriz (sobre la diagonal no habrá ninguna clase de información).

- Completar cada una de las celdas de la fila *x*, por encima de la diagonal respondiendo a la siguiente pregunta: El ítem de la fila *x*, ¿es más importante que el ítem de la columna *y*? Si la respuesta es afirmativa, se debe colocar un 1 en la celda de la fila *x* – columna *y*, en caso contrario, un 0. En el ejemplo, el ítem 1 (en la fila) es más importante que el ítem 2 (en la columna) y por este motivo se coloca un 1 en la celda de fila 1, columna 2.

- Cuando todas las celdas de una fila (por encima de la diagonal) están completas, las celdas de la columna correspondiente al mismo ítem se deben llenar con el inverso del número (donde hay un 1 se coloca 0 y viceversa).

- Se pasa a completar las celdas sobre la diagonal de la fila siguiente con el mismo procedimiento que se utilizó para llenar las celdas de la fila anterior, y así sucesivamente. El llenado de la columna 2 se realiza siguiendo el mismo procedimiento utilizado para el llenado de la columna 1.

- Cuando todas las celdas están llenas, se las suma obteniéndose el total de cada fila.

- Luego de calcular los totales por fila, se asigna un número de orden (un 1) a aquella fila cuyo total es el mayor, y así sucesivamente siguiendo en forma decreciente de importancia.

- Si dos de los totales son iguales, se asigna mayor prioridad al ítem que la tiene con respecto al otro. En el ejemplo, puesto que a los ítems 3 y 7 les corresponde el mismo total (en este caso 3), debido a que el ítem 3 es más importante que el ítem 7, se le asigna al primero el número de orden 3 y al ítem 7, el número de orden 4.

- En la columna "Orden" se obtiene la secuencia de ítems con su prioridad, uno respecto del otro.

		... que el ítem que está en la columna?							Total fila	Orden
		Item 1	Item 2	Item 3	Item 4	Item 5	Item 6	Item 7		
¿El ítem que está en esta fila es más importante...	Item 1	-	1	0	0	1	1	1	4	2
	Item 2	0	-	1	0	1	0	0	2	6
	Item 3	1	0	-	0	0	1	1	3	3
	Item 4	1	1	1	-	1	1	1	6	1
	Item 5	0	0	1	0	-	0	0	1	7
	Item 6	0	1	0	0	1	-	0	2	5
	Item 7	0	1	0	0	1	1	-	3	4

Figura 17 Matriz de priorización

- Finalmente, se ordena la lista de ítems de acuerdo al resultado obtenido. En todo caso, debe tenerse presente que la importancia relativa de un ítem respecto a otro incorpora elementos subjetivos, por lo cual los ponderadores definitivos deben ser corregidos considerando dichos elementos, pero siempre respetando el orden obtenido.

La aplicación de esta metodología permite clasificar los atributos en forma ordenada de mayor a menor incidencia, para la construcción de los dos índices, de impacto y de riesgo.

A continuación, en las dos figuras siguientes se muestra un ejemplo del resultado de la aplicación de la metodología antes explicada para la determinación del orden relativo de cada atributo, para el caso de los indicadores de impacto y de riesgo de los nodos pertenecientes a cualquiera de las redes de servicio. El caso de las redes de transporte es muy similar, y no se muestra el detalle completo.

¿Cuál atributo tiene mayor incidencia en riesgo?	REDUNDANCIA DE PARTES COMUNES	NODO REDUNDANTE	RUTA ALTERNATIVA PROPIA O DE TERCEROS	RESPALDO ENERGIA	COMPARTE UBICACIÓN CON OTRO NODO DE LA MISMA RED	COMPARTE UBICACIÓN CON OTRO NODO DE OTRA RED	COMPARTE UBICACIÓN CON OTRO NODO DE OTRA RED DE OTRO OPERADOR	Puntaje por Riesgo	Priorización por Riesgo
REDUNDANCIA DE PARTES COMUNES		0	0	0	1	1	1	3	4
NODO REDUNDANTE	1		0	0	1	1	1	4	3
RUTA ALTERNATIVA PROPIA O DE TERCEROS	1	1		0	1	1	1	5	2
RESPALDO ENERGIA	1	1	1		1	1	1	6	1
COMPARTE UBICACIÓN CON OTRO NODO DE LA MISMA RED	0	0	0	0		0	0	0	7
COMPARTE UBICACIÓN CON OTRO NODO DE OTRA RED	0	0	0	0	1		0	1	6
COMPARTE UBICACIÓN CON OTRO NODO DE OTRA RED DE OTRO OPERADOR	0	0	0	0	1	1		2	5

Figura 18 Matriz de priorización para índices de riesgo en redes de servicio

¿Cuál atributo tiene mayor incidencia en el impacto?	REDUNDANCIA DE PARTES COMUNES	NODO REDUNDANTE	REDUNDANCIA DE OTRO OPERADOR O PROPIA	RESPALDO ENERGIA	RANGO DE USUARIOS DIRECTOS O INDIRECTOS	CANTIDAD DE REGIONES EN QUE SE DISTRIBUYEN LOS USUARIOS	Puntaje por Impacto	Priorización por Impacto
REDUNDANCIA DE PARTES COMUNES		0	0	0	0	0	0	6
NODO REDUNDANTE	1		0	0	0	0	1	5
REDUNDANCIA DE OTRO OPERADOR O PROPIA	1	1		0	0	0	2	4
RESPALDO ENERGIA	1	1	1		0	0	3	3
RANGO DE USUARIOS DIRECTOS O INDIRECTOS	1	1	1	1		1	5	1
CANTIDAD DE REGIONES EN QUE SE DISTRIBUYEN LOS USUARIOS	1	1	1	1	0		4	2

Figura 19 Matriz de priorización para índices de impacto en redes de servicio

5.4.2.2.Criterios aplicados

Para el caso mostrado en las figuras anteriores, se observa que el atributo de mayor incidencia en el riesgo está dado, por la existencia o no de respaldo de energía (número de orden 1), seguido a continuación por la existencia de un nodo completo de respaldo (número de orden 2), o la existencia de partes comunes como fuente de poder o procesador redundante (número de orden 3), y así sucesivamente hasta llegar al atributo de menor incidencia (número de orden 6). Luego, al atributo de mayor incidencia (número de orden 1), se le asigna el factor de ponderación más alto de todos, (en este caso factor 7), y en forma proporcional se asigna el resto de los factores.

Para el índice de impacto el procedimiento es similar, en este caso el atributo de mayor incidencia es el rango de usuarios directos o indirectos, (número de orden 1), seguido por la cantidad de regiones afectadas (número de orden 2), y así sucesivamente. En este caso, el factor de ponderación al atributo de mayor incidencia es de 6.

En base a lo anterior, los criterios finales aplicados en la tabulación de las respuestas para todos los nodos, para determinar el riesgo y el impacto fueron los siguientes:

Atributos de los nodos	**Valores posibles de la variable**	**Factor de Ponderación**	
		Riesgo	**Impacto**
Redundancia de partes comunes	0(SI), 1(NO)	4	1
Nodo propio redundante	0(SI), 1(NO)	5	2
Redundancia otro operador (sólo redes de transporte)	0(SI), 1(NO)	6	3
Respaldo energía	0(NO), 1(SI)	7	4
Comparte ubicación con otro nodo de la misma red	0(NO), 1(SI)	1	N. A.
Comparte ubicación con otro nodo de otra red	0(NO), 1(SI)	2	N. A.
Comparte ubicación con otro nodo de otra red de otro operador	0(NO), 1(SI)	3	N. A.
Transporta servicios TF fija (sólo redes de transporte)	0(NO), 1(SI)	N. A.	3
Transporta servicios TF móvil (sólo redes de transporte)	0(NO), 1(SI)	N. A.	3
Transporta servicios Internet (sólo redes de transporte)	0(NO), 1(SI)	N. A.	3
Transporta servicios datos (sólo redes de transporte)	0(NO), 1(SI)	N. A.	3
Rango de usuarios directos o indirectos (sólo redes de servicio)	rangos variables	N. A.	6*N
Capacidad ocupada (N° STM-16 o equivalentes) (sólo redes de transporte)	1 a 10, M 15, M > 10	N. A.	6*M
Cantidad de regiones en que se distribuyen los usuarios	1 a 15	N. A.	5*R

Tabla 4 Criterios ponderación de riesgo e impacto de los nodos

La mayor parte de las respuestas son de opción SI /NO aplicándoseles según corresponda el respectivo valor; en cambio las respuestas relacionadas con cantidad de usuarios, cantidad de tramas, y cantidad de regiones tienen rangos de valores posibles, y en esos casos se multiplica el factor de ponderación por el valor de la variable de acuerdo al orden del rango, diferenciando así por ejemplo el nodo que afecta a más usuarios o regiones geográficas de otro que afecta a menor cantidad y por lo tanto tiene un menor impacto.

El valor de N se define en función de la cantidad de usuarios directos o indirectos, de acuerdo a los siguientes rangos:

Hasta 50.000 usuarios	N = 1
Entre 50.000 y 100.000 usuarios	N = 2
Entre 100.000 y 500.000 usuarios	N = 3
Entre 500.000 y 1 millón de usuarios	N = 5
Sobre 1 millón de usuarios	N = 8

El valor de M se define en función de la cantidad de tramas STM - 16, de acuerdo a los siguientes rangos:

Entre 1 y 10	M = cantidad de tramas
Sobre 10 tramas	M = 15

El valor de R se define en función de la cantidad de regiones administrativas del país, cubiertas por el servicio, en forma lineal de 1 a 15

La definición de estos rangos y ponderadores, tienen por objetivo diferenciar en forma notoria la infraestructura de comunicaciones que atiende a la mayor cantidad de usuarios, tramas, o regiones.

De esta forma se tabulan los resultados de las respuestas enviadas por cada operador, obteniendo así una relación ordenada de los elementos de red, para cada uno de ellos, en que el mayor puntaje representa un nivel de riesgo o impacto mayor. Esto permite efectuar un ranking de los nodos más críticos por cada operador, y a su vez efectuar comparaciones entre los distintos operadores, identificando los nodos más importantes a nivel país.

5.4.2.3.Determinación de los Índices de Riesgo y de Criticidad

Para determinar estos índices se definieron las siguientes variables

- Puntuación por la respuesta señalada para cada aspecto o variable de un nodo (p)
- Factor de ponderación de riesgo (r)
- Factor de ponderación de impacto (i)

Estos se incluyeron en las planillas de respuesta en las filas superiores.

CONFIDENCIAL
Información declarada confidencial por las empresas.

Figura 20 Ejemplo de cálculo variables p, r, e i en Redes de Telefonía Móvil

Así para cada tipo de elemento de red incluido en las respuestas, se asigna el valor a la variable de acuerdo a la lógica indicada en la segunda columna de la tabla anterior.

Para cada variable de cada nodo se calcula un índice de riesgo (R_i) multiplicando el valor de la variable p_i por el valor correspondiente del ponderador de riesgo r_i

De esta forma, $R_i = p_i * r_i$ así posteriormente se calcula el Indice de Criticidad Riesgo para este elemento como $R = \Sigma R_i$

Para el caso de las planillas de redes de transporte se consideraron los siguientes valores

RED TRANSPORTE			
IDENTIFICADOR ELEMENTO RED	Valor variable	Ponderador Riesgo	Ponderador Impacto
INDICE DE CRITICIDAD RIESGO			
INDICE DE CRITICIDAD IMPACTO			
TIPO ELEMENTO RED CON TRAFICO STM16 O SUPERIOR			
REDUNDANCIA DE PARTES COMUNES	SI=0 NO=1	4	1
NODO PROPIO REDUNDANTE	SI=0 NO=1	5	2
REDUNDANCIA OTRO OPERADOR	SI=0 NO=1	6	3
RESPALDO ENERGIA	SI=0 NO=1	7	4
COMPARTE UBICACIÓN CON OTRO NODO DE LA MISMA RED	SI=1 NO=0	1	0
COMPARTE UBICACIÓN CON OTRO NODO DE OTRA RED	SI=1 NO=0	2	0
COMPARTE UBICACIÓN CON OTRO NODO DE OTRA RED DE OTRO HOLDING	SI=1 NO=0	3	0
TRANSPORTA SERVICIOS TF FIJA	SI=1 NO=0	0	3
TRANSPORTA SERVICIOS TF MOVIL	SI=1 NO=0	0	3
TRANSPORTA SERVICIOS INTERNET	SI=1 NO=0	0	3
TRANSPORTA SERVICIOS DATOS	SI=1 NO=0	0	3
CAPACIDAD OCUPADA (N*STM16 O EQUIVALENTES)	=N =15 SI>10	0	6
CANTIDAD DE REGIONES EN QUE SE DISTRIBUYEN LOS USUARIOS	1	0	5

Figura 21 Ejemplo de cálculo variables p, r, e i en Redes de Transporte

De forma similar se calcula un índice de impacto (I_i) multiplicando el valor de la variable p_i por el valor correspondiente del ponderador de impacto i_i

De esta forma, $I_i = p_i * i_i$ así posteriormente se calcula el Indice de Criticidad Impacto para este elemento como $I = \Sigma I_i$

Aquellos elementos que se consideró que no tienen influencia en el cálculo de alguno de los índices se les asigna un ponderador 0.

En el CD que se entrega adjunto, se incluye una planilla con un resumen de todas las tablas relacionadas para el cálculo de estas variables, y además aparecen las respuestas de los operadores debidamente tabuladas.

6. RESULTADOS

6.1. Introducción

En este capítulo se entregan los resultados que se obtuvieron al aplicar la metodología, indicada en el punto anterior para determinar los indicadores de políticas de aseguramiento, riesgo e impacto, este último tanto a nivel de elemento de red o nodo como de sitio.

CONFIDENCIAL
Información declarada confidencial por las empresas.

Una primera conclusión es que los operadores reportaron un total de 230 sitios diferentes, mientras que el total de nodos fue de 776

6.2. Resultados de políticas de aseguramiento

Para desarrollar este aspecto, se evaluaron las respuestas recibidas al "Cuestionario para evaluar la situación de la empresa respecto al aseguramiento de infraestructura crítica", que figura en el Anexo N° 1.

Los resultados obtenidos para las distintas empresas que entregaron las respuestas al cuestionario, varían entre un 48% y un 100%, es decir estarían entre el segundo y cuarto rango como se señala en el punto 5.4.1, y se presentan en la tabla que aparece a continuación.

Cabe destacar que esta información corresponde a una autoevaluación realizada por cada empresa y no hay ningún tipo de antecedente o referencia que corrobore lo expresado por ellas.

En estas condiciones, la encuesta realizada no es comparable directamente entre empresas, pero sí es útil como punto de referencia para efectuar en etapas posteriores, una evaluación más detallada en base a la solicitud y análisis de los antecedentes y registros que sustenten lo expresado. Este análisis se debería realizar al momento de definir las actividades que permitan mejorar la protección de la infraestructura crítica de telecomunicaciones.

CONFIDENCIAL
Información declarada confidencial por las empresas.

Tabla 5 Resultados de evaluación de aseguramiento de infraestructura crítica

Se debe considerar que estas respuestas pueden verse afectadas por un grado de subjetividad, ya que algunas empresas pueden auto evaluarse con criterios más permisivos que otras. Lo ideal sería poder validar las afirmaciones que se hacen en dicho cuestionario, como por ejemplo confirmar la existencia de procedimientos documentados, así como la existencia, aplicación y difusión de políticas, tener acceso a los registros de resultado de auditorías de pruebas de contingencia realizadas, y en general auditar todas las respuestas entregadas de la encuesta.

También se puede comentar, que en los resultados obtenidos influyen variables como la extensión geográfica de los servicios prestados por cada empresa, el tamaño de la organización, y la diversidad de tecnologías y redes que opera una empresa; así también como la cultura organizacional y la propiedad por parte de holdings internacionales, más proclives a la implantación de este tipo de políticas de aseguramiento de la infraestructura crítica.

6.3. Resultados relativos al índice de impacto

En base a las respuestas recibidas y como ya se explicó, se determinó el impacto que la interrupción o mal funcionamiento de un nodo provoca, en función de la cantidad de usuarios o de tráfico, regiones del país afectadas, tipo de servicio directamente involucrado, otras redes afectadas, etc.

A continuación se muestra una tabla donde aparece una relación ordenada de los 50 nodos con mayor índice de impacto a nivel nacional. La lista completa de los más de 700 nodos se encuentra en el archivo correspondiente, que se encuentra en los anexos.

CONFIDENCIAL
Información declarada confidencial por las empresas.

Tabla 6 Listado de nodos de mayor índice de impacto

Un análisis adicional realizado es como contribuyen las diferentes redes, a través de la totalidad de los nodos reportados en cada una de ellas, al índice de impacto. Los resultados se presentan en la siguiente tabla y gráfico:

RED	INDICE DE IMPACTO
TRANSPORTE NACIONAL	71,93%
TELEFONIA MOVIL	10,30%
TRANSPORTE INTERNACIONAL	5,93%
INTERNET	4,97%
DATOS	4,85%
TELEFONIA FIJA	2,01%
TOTAL	**100,00%**

Tabla 7 Índice de impacto por tipo de red

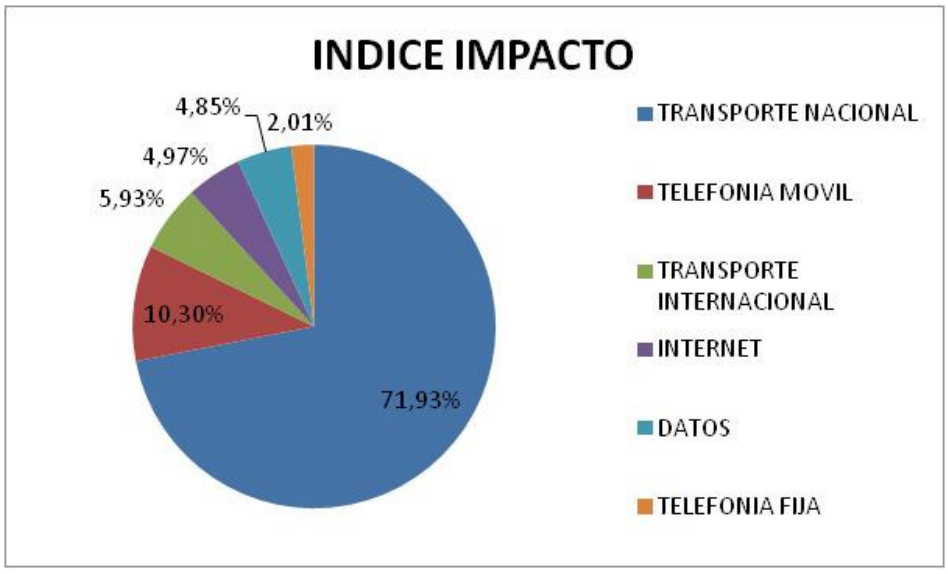


Gráfico 1 Índice de impacto por tipo de red

También se muestra la relación entre el tipo de elemento de red y el índice de impacto, concluyéndose que los más importantes son los nodos SDH y WDM, que en conjunto contribuyen al 77 % del impacto total, como se aprecia en el gráfico siguiente:

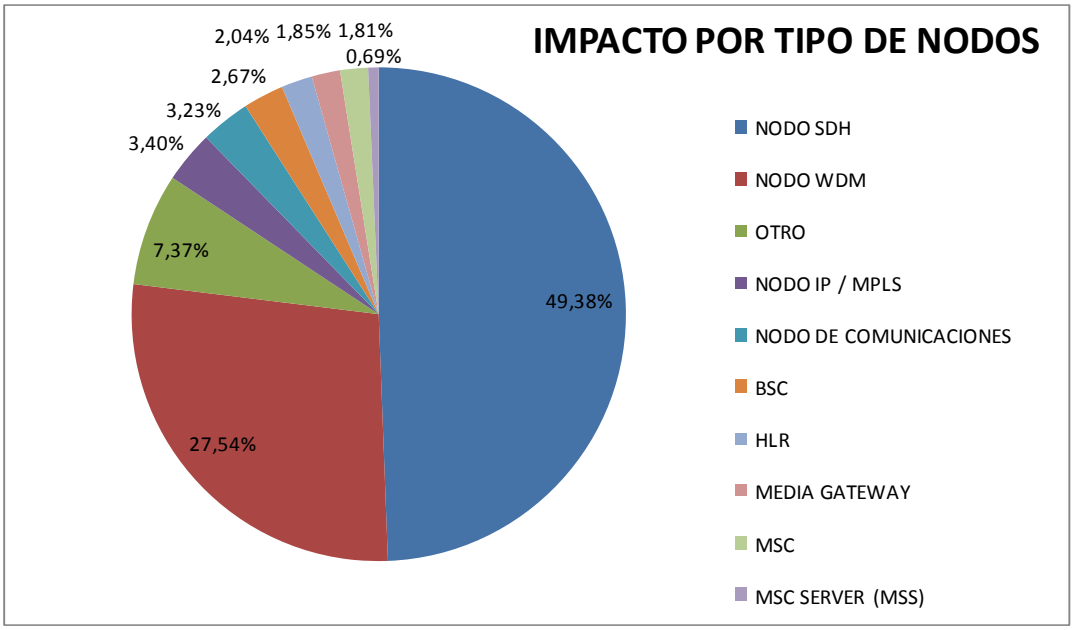


Gráfico 2 Índice de impacto por tipo de elemento de red

6.4. Resultados relativos al índice de riesgo

En forma similar al punto anterior, se determinó el nivel de riesgo operacional de los diferentes nodos, basado en las condiciones de respaldo y redundancia de ellos. La tabla siguiente muestra esta relación ordenada para los 30 nodos con mayores índices de riesgo:

CONFIDENCIAL
Información declarada confidencial por las empresas.

Tabla 8 Listado de nodos de mayor índice de riesgo

Al analizar como contribuyen la totalidad de los nodos reportados para cada una de las diferentes redes al índice de riesgo, se obtienen resultados muy similares a los del índice de impacto. En ambos casos, impacto y riesgo, la red más importante es la de transporte nacional, seguida por la de telefonía móvil, con una contribución sumada del orden del 80%.

RED	INDICE DE RIESGO
TRANSPORTE NACIONAL	62,74%
TELEFONIA MOVIL	17,63%
TRANSPORTE INTERNACIONAL	2,58%
INTERNET	8,46%
DATOS	3,99%
TELEFONIA FIJA	4,59%
Total	**100,00%**

Tabla 9 Índice de riesgo por tipo de red

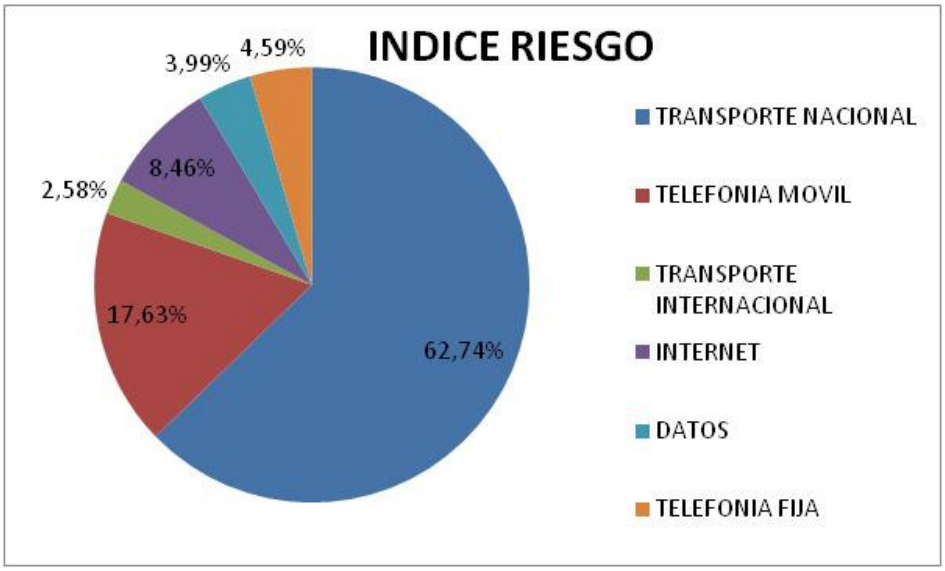


Gráfico 3 Índice de riesgo por tipo de red

6.5. Resultados relativos al indicador de impacto para sitios

El aspecto más importante para la toma de decisiones respecto de futuras acciones que fuesen necesarias para la Protección de la Infraestructura Crítica de Telecomunicaciones, está dado por la priorización del impacto que tiene sobre los servicios de Telecomunicaciones, las amenazas y debilidades asociadas a un determinado sitio o edificio.

El listado definido por la metodología incluye un ordenamiento relativo entre sitios de las diferentes compañías para definir los de mayor índice de impacto a nivel nacional.

En este sentido, para priorizar la importancia relativa de los diversos sitios se ha elaborado un indicador calculado mediante la suma de los puntajes de impacto asociados a todos los nodos que físicamente están ubicados en una misma localización.

El resultado de este indicador se muestra en la tabla siguiente, donde aparecen los 30 sitios con indicador de impacto más alto, de un total de 230 sitios diferentes identificados, y de acuerdo a lo calculado según la metodología explicada. En este proceso, se homologaron los sitios informados por las distintas empresas, a través del análisis de las direcciones y ubicación geográfica, y se consolidaron en aquellos casos en que un mismo sitio sirve para las instalaciones de más de una empresa, ya sea que pertenezcan a un mismo holding o bien que entreguen facilidades de housing a terceros no relacionados.

CONFIDENCIAL
Información declarada confidencial por las empresas.

Tabla 10 Sitios con mayor indicador de impacto

De esta manera como lo muestra la tabla anterior, se logra tener un índice de criticidad para la localización, permitiendo priorizarlas de modo de orientar posteriormente hacia estas instalaciones, el estudio de análisis de riesgo y medidas de mitigación para la mejora de índices de disponibilidad de los servicios que aloja.

Este análisis de riesgo y las medidas de mitigación debieran hacerse en conjunto, entre SUBTEL y el concesionario del servicio y propietario de esa instalación en particular, en reuniones de trabajo uno a uno.

CONFIDENCIAL
Información declarada confidencial por las empresas.

Tabla 11 Nodos con mayor indicador de impacto y su respectivo sitio

CONFIDENCIAL
Información declarada confidencial por las empresas.

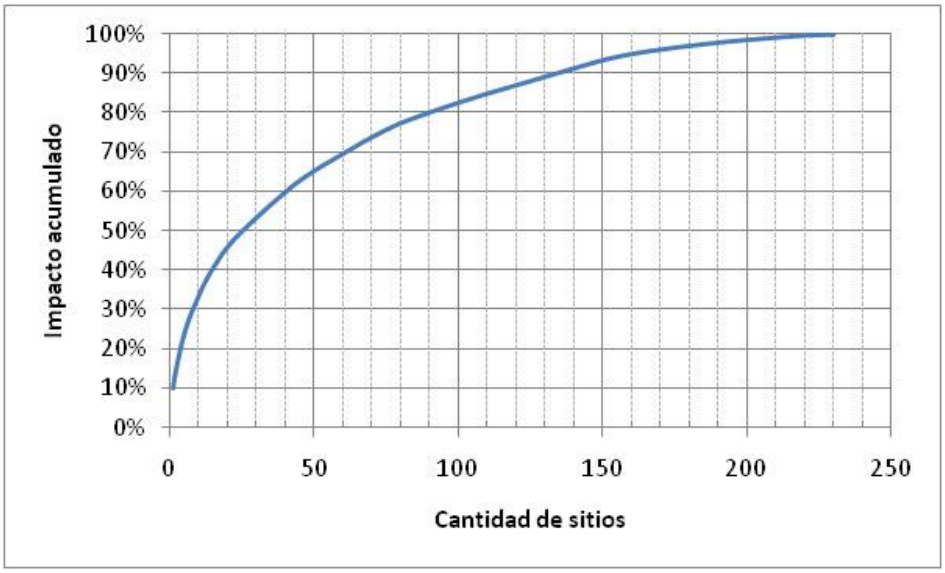


Gráfico 4 Índice de impacto acumulado por cantidad de sitios

A continuación se muestra una imagen donde aparecen geo referenciados algunos de los sitios de mayor impacto, lo cual se hizo en base a la información de ubicación entregada por cada operador, como direcciones y coordenadas geográficas. Esta información se validó en algunos casos en terreno a través de instrumentos GPS y otras herramientas similares, y la imagen está construida sobre la aplicación Google Earth

CONFIDENCIAL
Información declarada confidencial por las empresas.

Figura 22 Ubicación de sitios de mayor impacto, ciudad de Santiago

CONFIDENCIAL
Información declarada confidencial por las empresas.

Figura 23 Ubicación de sitios de mayor impacto, comuna de Santiago

CONFIDENCIAL
Información declarada confidencial por las empresas.

Figura 24 Ubicación de sitios de mayor impacto, Valparaíso

Los archivos respectivos, de extensión .kmz, donde aparecen estos sitios geo referenciados se adjuntan en el CD y pueden ser ejecutados desde la aplicación Google Earth u otras.

CONFIDENCIAL
Información declarada confidencial por las empresas.

Tabla 12 Comunas con sitios de mayor índice de impacto

En forma complementaria, la tabla siguiente muestra el listado consolidado de sitios críticos informados por cada operador, a los que se les había solicitado informaran hasta diez sitios críticos según su criterio, desde el punto de vista operacional y ordenados de mayor a menor importancia.

CONFIDENCIAL
Información declarada confidencial por las empresas.

Tabla 13 Sitios críticos reportados por los operadores (parte I)

CONFIDENCIAL
Información declarada confidencial por las empresas.

Tabla 14 Sitios críticos reportados por los operadores (parte II)

A diferencia del listado confeccionado con nuestra metodología, esta relación de sitios críticos entregada por cada operador, no considera la consolidación de instalaciones de diferentes empresas en un mismo sitio físico, como por ejemplo:

CONFIDENCIAL
Información declarada confidencial por las empresas.

De todas maneras, pese a estas diferencias las tablas anteriores permiten observar que hay una alta correlación entre los sitios definidos como críticos por la metodología aplicada, y los informados por las propias compañías.

CONFIDENCIAL
Información declarada confidencial por las empresas.

7. CONCLUSIONES

A continuación se entregan las conclusiones que se deducen de este estudio, analizándose en primer lugar las que corresponden a la fase de estudio de la literatura internacional sobre esta materia, y luego las conclusiones obtenidas a partir de la realidad nacional.

.

7.1. Experiencia internacional

Todos los países analizados, ya sea en detalle o en forma general, muestran una manera similar a la hora de enfrentar la protección de la infraestructura crítica, lo cual se puede resumir en los siguientes puntos:

- Existe amplio consenso en definir a la Infraestructura Crítica de Información o ICI como aquella que al no tenerla puede ocasionar pérdidas de vida, serio o grave impacto en la salud, seguridad o economía de sus ciudadanos.

- En todos los países estudiados existen objetivos políticos claros de protección de la ICI, con un compromiso y soporte visible desde un punto de vista de liderazgo nacional, reflejado en la estructura y organización del rol y responsabilidad del gobierno.

- Cada país cuenta con una organización acorde con su cultura, sin embargo la mayoría presenta una organización vertical en el tema de la ICI, la cual es dirigida desde el más alto nivel del gobierno y es éste el que, por medio de las políticas y acciones tendientes a asegurar sus recursos críticos, da el ejemplo al resto de la sociedad. A modo de ejemplo en la figura siguiente se muestra la organización en Australia.

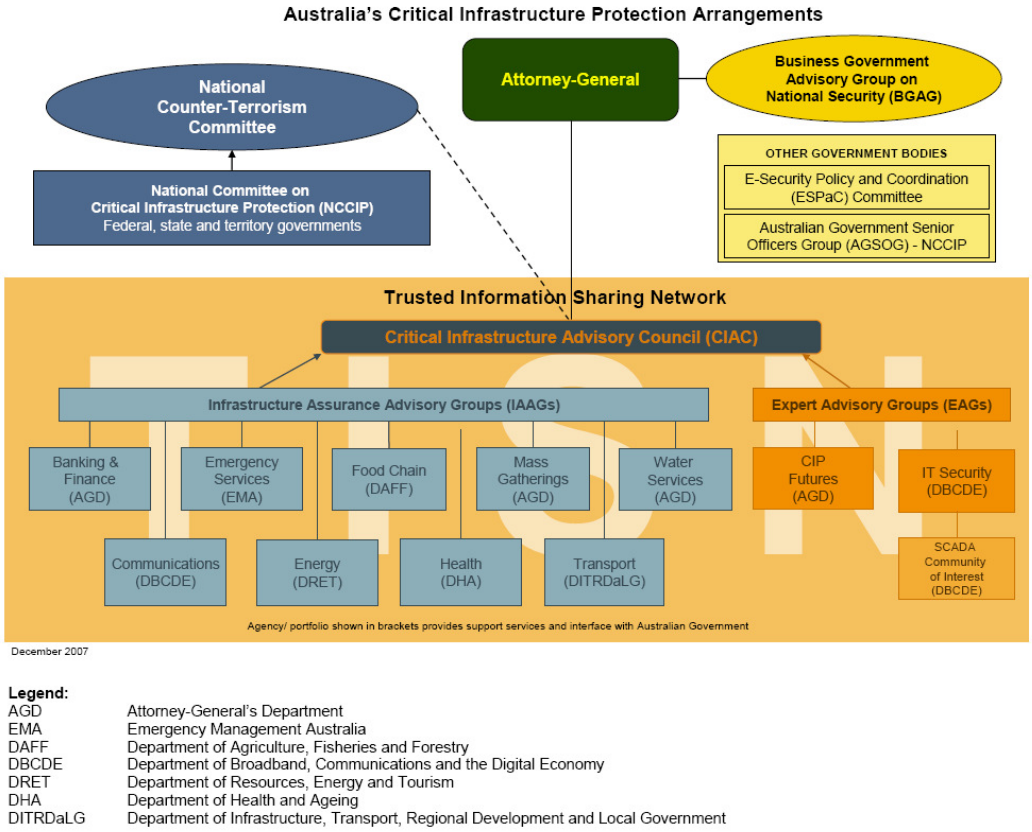


Figura 25 Organización de CIIP en Australia

- La elección de la infraestructura y sectores a considerar como crítica requiere la participación del sector privado, además de los expertos del gobierno. Normalmente un componente o un sistema se lo califica como crítico en razón a su posición dentro de toda la infraestructura, y en particular debido a la interdependencia que éste tenga con otras infraestructuras. Los sectores que más frecuentemente se clasifican como críticos son los siguientes:

  - Banca y Finanzas
  - Gobierno Central / Servicios de Gobierno

- Telecomunicaciones/ Tecnologías de Información y Comunicaciones
- Energía / Electricidad
- Transporte / Logística / Distribución
- Suministro de Agua
- Salud (servicios de emergencia)

- En cada país el tema en cuestión es de vital importancia y han conformado la estructura operacional correspondiente.

- En la mayoría de los casos revisados, las primeras actividades han correspondido a la definición de lo que entienden por infraestructura crítica, y cuáles son los sectores involucrados, y posteriormente han desarrollado la estrategia y objetivos de la ICI. Sin embargo, algunos países como Brasil y otros, no tienen una identificación clara y formal de cuáles son sus sectores críticos.

- El trabajo conjunto gobierno-sector privado es vital y en general se han conformado grupos de trabajo interdisciplinarios para abordar el tema.

- Se requiere de un fuerte liderazgo desde el más alto nivel del gobierno, para implementar los mecanismos de aseguramiento de la infraestructura crítica.

- Los gobiernos le dan carácter de urgencia y de primera importancia al aseguramiento de sus activos, en especial se nota gran preocupación por el tema de la seguridad cibernética. En este sentido en algunos países, el equivalente a lo que en Chile se entiende como la Contraloría, tiene la potestad de efectuar auditorías a los sistemas informáticos del gobierno e instituciones públicas en el tema informático.

- Se deben tomar en cuenta las interdependencias que existe entre los diferentes sectores que gestionan infraestructura crítica, ya que no basta analizar un sector específico, como las telecomunicaciones u otro cualquiera, en forma aislada sin considerar sus interrelaciones.

- Debe existir una revisión sistemática y periódica de la política y marco legal y esquemas de auto regulación que aplica al manejo de la infraestructura crítica

- Todos los países reconocen la importancia de la asociación Público-Privado y los gobiernos impulsan el intercambio de información con el sector privado, ya que la mayor parte de la infraestructura es de propiedad y operada por privados.

- Uno de los principales desafíos a futuro en muchos países, es alcanzar un equilibrio entre los requerimientos de seguridad y los imperativos de eficiencia de los negocios. Se ha observado que es relativamente fácil llegar a acuerdos sobre la existencia de problemas y la necesidad de resolverlos, pero es muy difícil llegar a acuerdo sobre las medidas a tomar, los responsables de implementarlas, la responsabilidad legal de dichas medidas y respecto de quién financia la implantación de las medidas.

- Además, existe conciencia que el riesgo no puede ser eliminado totalmente, y que algún nivel de riesgo debe ser aceptado por la sociedad, existiendo un balance entre costos versus seguridad.

- En la mayor parte de los países se han establecido comités, fuerzas de tarea y grupos de trabajo, cuyo mandato incluye trabajo de escenarios, evaluación de medidas, o establecimiento de sistemas de alerta temprana. Esto llevó al establecimiento de políticas, tales como recomendaciones para establecer organizaciones independientes que se encarguen de los temas de la sociedad de la información y políticas básicas de CIIP.

- Asimismo, se ha reconocido la necesidad de que la protección requerida a la infraestructura es tanto física como lógica.

- El estado de implantación de políticas es muy variable de un país a otro existiendo desde sugerencias hasta regulaciones detalladas. Para la mayor parte de los países el tema de CIIP es, en algún grado, un tema de seguridad nacional.

7.2. Experiencia nacional

Existe una amplia dispersión en el nivel de establecimiento de políticas de seguridad de la infraestructura crítica, entre las distintas empresas que respondieron el cuestionario respectivo. Además, dichas respuestas están sujetas a un nivel de subjetividad, lo que hace recomendable por un lado enfatizar la conveniencia de extender la aplicación de estas

políticas en todas las empresas, y por otra parte se estima conveniente realizar alguna comprobación acerca de la realidad de esta situación.

Desde el punto de vista de la criticidad de los elementos de red, los más críticos de acuerdo al indicador de impacto definido, pertenecen a las redes de transporte, y a su vez son los más expuestos a amenazas de tipo físico por sus componentes instaladas en espacios no controlados. Si bien estas redes cuentan con respaldo de las de otros operadores, su cercanía en el trazado en ciertos tramos, reduce su efectividad.

En cambio, los sitios (edificios), de mayor índice de impacto, están caracterizados fundamentalmente por el grado de concentración de redes y nodos que se produce en dichos sitios.

CONFIDENCIAL
Información declarada confidencial por las empresas.

Por otra parte, la experiencia de los consultores en el sector de telecomunicaciones, muestra que este sector ha tenido una buena respuesta ante situaciones de crisis o emergencias, principalmente proveniente de desastres naturales, exceptuando lo que guarda relación con problemas lógicos de congestión que se producen inmediatamente ocurridos estos fenómenos. Además, los operadores han actuado cooperativamente en temas de respaldos mutuos, como por ejemplo es el caso de las redes de transporte nacional en base a fibra óptica. A su vez, cada operador cuenta con los elementos de protección en sus elementos de red o nodos que le permiten proveer el servicio con un alto nivel de disponibilidad. En consecuencia uno de los temas que debiera abordarse para disminuir los niveles de riesgo y por ende de impacto sería, efectuar un análisis detallado y en conjunto con cada operador de las posibles amenazas a los sitios con mayor indicador de impacto, mejorando las coordinaciones con organismos del estado, como Carabineros, Investigaciones, CONAF; con organismos de emergencia como Bomberos, y analizando las interdependencias con otros sectores de servicio, como por ejemplo el eléctrico, agua, transporte, etc.

El presente estudio no abarca servicios de Data Center, sin embargo hemos observado que este servicio, cada día más, pasa a formar parte del mix comercial que los operadores de

telecomunicaciones ofrecen a sus clientes. Desde este punto de vista es recomendable indagar sobre las vulnerabilidades y los medios de protección con que cuentan en estos emplazamientos para la protección de la Infraestructura Crítica de Información que opera en ellos. Estos sitios pueden tener un alto grado de impacto sobre la operación de diversas industrias a nivel nacional.

8. RECOMENDACIONES

8.1. Introducción

A continuación se entregan las principales recomendaciones que se deducen de este estudio, las que se dividen en varios aspectos y categorías y que son las siguientes:

- Recomendaciones derivadas de la OECD.
- Recomendaciones de la UIT.
- Recomendaciones para la implementación de un plan de protección de la ICI / ICT en Chile.
- Recomendación específica para la red móvil
- Recomendación específica para la protección de cables submarinos
- Recomendación específica para la protección lógica de la red Internet

8.2. Recomendaciones derivadas de la OECD

La OECD emitió en Abril del 2008) una serie de recomendaciones a sus países miembros, para la protección de la infraestructura crítica de información (CIIP)[35]. De éstas, se exponen a continuación las más relevantes y aplicables a nuestro país, las que se pueden clasificar en dos grandes grupos, a nivel interno nacional, y a nivel internacional

8.2.1. Recomendaciones a nivel nacional:

- Demostrar liderazgo y compromiso gubernamental en la protección de la ICI, por medio de las siguientes acciones
    - Adoptar objetivos políticos claros al más alto nivel de gobierno.

[35] http://www.oecd.org/dataoecd/1/13/40825404.pdf

- Identificar agencias de gobierno y organizaciones con autoridad para ejecutar estos objetivos políticos.
- Establecer cooperación mutua con los operadores privados de ICI, para la implementación de estos objetivos.
- Efectuar revisiones sistemáticas del marco regulatorio, político y legal, relacionado con ICI.
- Mejorar los niveles de seguridad de las redes y sistemas de información que constituyen ICI

- Gestionar los riesgos que afecten a la ICI, por medio de:
  - Desarrollar una estrategia nacional que obtenga el compromiso de todos los actores involucrados, tanto del gobierno como del sector privado.
  - Considerar las interdependencias que afectan al sector.
  - Realizar una evaluación de riesgos a través de un análisis de vulnerabilidades y amenazas que afecten a la ICI.
  - Desarrollar procesos de gestión de riesgos a nivel nacional que establezcan la organización detallada, las herramientas y mecanismos de supervisión, para implementar la estrategia de gestión de riesgos a diferentes niveles.
  - Desarrollar capacidad de respuesta a incidentes, por medio de equipos tipo CERT (**C**omputer **E**mergency **R**esponse **T**eam) responsables de monitorear, alertar y efectuar acciones de recuperación de la ICI.

- Trabajar en asociación con el sector privado por medio de:
  - Crear relaciones de confianza pública privadas, focalizadas en la gestión de riesgos, respuesta de incidentes y recuperación.
  - Intercambiar información mutua periódicamente.

- Promover la innovación, investigación y desarrollo que favorezcan la seguridad de la ICI

8.2.2. Recomendaciones a nivel internacional:

Teniendo en cuenta que las amenazas a la ICI traspasan las fronteras de los países y superan las capacidades individuales de éstos, se deben realizar esfuerzos y coordinaciones entre distintos países, por medio de:

- Compartir el conocimiento y experiencias en el desarrollo de políticas y práctica sistemas nacionales, y de modelos para la coordinación con el sector privado
- Desarrollar entendimiento común de gestión de riesgos, vulnerabilidades y amenazas de la ICI, que faciliten acciones colectivas frente a eventos de amplia difusión, como software malicioso y fallas de seguridad
- Difundir información de las agencias nacionales encargadas de la protección de la ICI, facilitando la identificación de las contrapartes y mejorando los tiempos de respuesta
- Participar en redes internacionales de monitoreo y respuesta ante incidentes

8.3. Recomendaciones de la UIT

8.3.1. Introducción

La UIT encargó al Centro para Estudios de Seguridad ETH (por su sigla en alemán) de Zurich, (es decir al mismo organismo que emitió el CIIP Handbook ya citado anteriormente en este informe), una investigación con el objeto de desarrollar un marco de acción genérico simple que pudiera ser aplicable por los países en desarrollo para establecer un programa de protección a la ICI (CIIP).

Como resultado de esta investigación, se publicó en Agosto del año 2007 el reporte "A Generic National Framework for Critical Information Infrastructure Protection" [36]. La

[36] http://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf

importancia del citado reporte, aparte de que fue encargado por la UIT, es que está dirigido a los países en desarrollo que no tienen la misma disponibilidad de recursos que otros países más avanzados, y que recién se inician en el tema de la protección a la ICI, requiriendo un marco genérico inicial simple y de bajo costo. Estas dos condiciones se aplican para el caso de Chile.

El reporte enfoca los problemas de protección de la ICI principalmente desde los puntos de vista relacionados con aspectos de seguridad de la información, pero son igualmente aplicables en un sentido más general. Este reporte ha sido incorporado a uno de los grupos de estudios permanente de la UIT

A continuación se analizan las principales recomendaciones del estudio encomendado por la UIT.

8.3.2. Modelo de los cuatro pilares

El reporte recomienda, que teniendo en consideración la gran variedad de tareas relacionadas con la protección de la ICI, las primeras acciones se centren en definir las prioridades y responsabilidades esenciales de la organización a cargo del tema. Se propone un grupo de cuatro grandes tareas, organizadas bajo un modelo de cuatro pilares que son los siguientes:

- Prevención y alertas tempranas

Las tareas de prevención y alertas tempranas son componentes indispensables de una estructura de protección de ICI, cuyo principal objetivo consiste en reducir la cantidad de incidentes y amenazas. Sin embargo, no es posible pretender que todos los incidentes puedan ser previstos, en especial los relacionados con la seguridad de la información, y por lo tanto un enfoque realista consiste en asegurarse que las ICI sean menos vulnerables a las interrupciones, y que las alteraciones sean de corta duración, limitadas en alcance y la restauración de los sistemas de información cuando ellos se vean interrumpidos, sea lo más rápida posible. El objetivo principal de la prevención es asegurar que las empresas responsables estén lo más preparadas posibles para resolver los incidentes que se presenten.

La prevención incluye actividades de difusión de recomendaciones y consejos, avisos oportunos y confiables de amenazas, entrenamiento y ejercitación

- Detección

La detección constituye el segundo pilar de este modelo, ya que es crucial que las nuevas amenazas sean descubiertas en forma temprana, lo cual requiere disponer de mecanismos de información a nivel nacional e internacional, en especial en el campo de la seguridad, actuando en colaboración cercana con equipos CERT, en la ayuda de la identificación de nuevas técnicas de ataques informáticos. Se requiere compartir información a nivel internacional, ya que en general los riesgos de seguridad superan las fronteras, y además es conveniente la coordinación con organismos de inteligencia.

- Reacción

La reacción incluye la identificación de las causas que provocan una interrupción, y las medidas correctivas correspondientes. El rol de la unidad de CIIP es principalmente de apoyo y coordinación, pero la responsabilidad principal le corresponde al operador o empresa dueña del la red o sistema afectado.

Una vez resuelto el incidente, es importante se realicen los análisis correspondientes para determinar sus causas, y obtener las conclusiones apropiadas para evitar se repitan eventos similares. Es conveniente que estas lecciones sean adecuadamente difundidas entre todos los actores para aprovechar esa experiencia.

- Gestión de crisis

La gestión de crisis persigue minimizar los efectos de cualquier interrupción hacia la sociedad, y a la unidad a cargo de la CIIP le puede corresponder un rol importante, alertando a los responsables y autoridades de gobierno, y ejecutando las medidas a nivel nacional que disminuyan el impacto del incidente.

Gráficamente este modelo se puede representar como lo muestra la figura siguiente

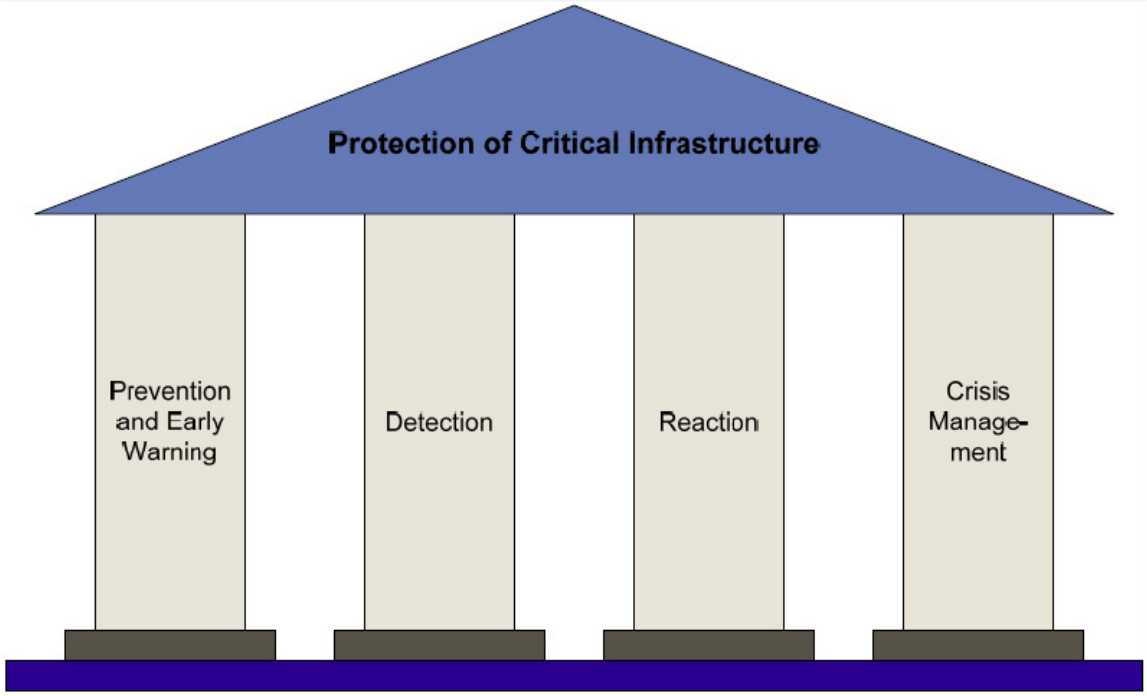


Figura 26 Modelo de los cuatro pilares para la CIIP

8.3.3. Modelo de cooperación

La unidad a cargo de la protección de la ICI requiere competencias especializadas, y una organización compleja. Esta organización se puede simplificar por medio de la cooperación con otros actores que posean competencias especializadas. Los actores que deben formar parte de esta red de cooperación son los siguientes:

- Una agencia gubernamental, que provea liderazgo estratégico y supervisión, actuando como cabeza de la CIIP.
- Un centro de análisis, conocido como Centro de Situación, que posea fuertes vínculos con las áreas de inteligencia del país.
- Un centro de especialización técnica, que puede estar compuesto por personal de staff de equipos CERT, de especialistas de los mismos operadores, o del mundo académico o de la consultoría.

Esto da origen a una composición tripartita de la unidad encargada de la protección de la ICI, como se grafica en la siguiente figura.

Figura 27 Composición tripartita de la CIIP

8.3.4. Aspectos organizacionales

De acuerdo al modelo tripartita expuesto, la organización de la unidad responsable de la CIIP, debe estar formada por un ejecutivo responsable perteneciente a un organismo de gobierno, que actúa como representante oficial, y nexo con el mundo político. Este responsable debe tener experiencia en temas de seguridad de la información y tecnológicos, y poseer habilidades de comunicación, relaciones con el mundo político, y liderazgo.

Para situaciones de emergencia, se debe constituir una fuerza de tareas especiales, integrada por actores del mundo público y privado.

El Centro de Situación está a cargo de las actividades no técnicas, y su responsable se contacta con las áreas de inteligencia, requiriendo conocimientos legales y políticos, más que de seguridad de la información.

Por último el área de staff, formada por equipos CERT y especialistas de comunicaciones, realiza las labores técnicas requiriendo la correspondiente especialización en dichas áreas. Lo habitual es que esta área se integre con otros equipos CERT del mundo académico, y reciba el apoyo de los especialistas de las empresas operadoras, evitando de esta forma el aumentar la complejidad de la organización.

8.4. Recomendaciones para la implementación de un plan de protección de la ICI / ICT en Chile

Como consecuencia del análisis y revisión de la experiencia internacional en la materia, y del estado de situación en nuestro país, se recomienda un conjunto de actividades que en forma lógica conducirían a la concreción de un plan para proteger la Infraestructura Crítica de Información a nivel de nuestro país.

A continuación se presentan las etapas principales de este plan:

- Incorporar el objetivo de protección de la ICI como un compromiso a nivel de gobierno, identificando responsables y estableciendo metas y plazos. Con el objetivo de asegurar la participación de todos los sectores involucrados, y hacerse cargo de las relaciones e inter dependencias, este plan debe ser impulsado desde el nivel superior de gobierno, comprometiendo la participación de entes públicos como privados. Desde el punto de vista de los plazos, se considera adecuado definir metas de mediano plazo, por ejemplo tres años, y programas de acción con hitos anuales.

- Definir una estructura de trabajo inicial para desarrollar lo anterior. Se debe establecer un responsable a nivel gubernamental para liderar, organizar y coordinar los grupos de trabajo de cada sector específico, teniendo en cuenta que esta es una tarea multisectorial.

- Identificar la Infraestructura Crítica de Información ICI a nivel país, y para cada sector de la actividad nacional, más allá de la infraestructura crítica de telecomunicaciones cubierta en este estudio. Como parte del trabajo a desarrollar por los grupos de trabajo que se definan en la etapa anterior, se deberá determinar la

ICI a nivel país, teniendo en consideración todos los sectores y actividades nacionales.

- Identificar las interrelaciones y dependencias que afectan a la ICI a nivel país. En cada sector, la infraestructura crítica depende de servicios provistos por otros sectores de la economía, por lo que se deben considerar estas relaciones de dependencias.

- Profundizar el estudio de impacto de las telecomunicaciones sobre la ICI a nivel país. A partir de los puntos anteriores, se requiere precisar en detalle la Infraestructura Crítica de Telecomunicaciones, continuando el trabajo específico del sector telecomunicaciones a partir de los resultados de este estudio. Se debe formar el correspondiente grupo de trabajo para la ICT, con participación de entes gubernamentales, privados, académicos, y representantes de los usuarios de los servicios. Estas actividades debieran ser lideradas por SUBTEL, y entre otras tareas, se deben abordar:

  - Realizar análisis detallados de riesgos, vulnerabilidades (amenazas y debilidades) atingentes a los sitios calificados como de mayor impacto de acuerdo a este estudio, para realizar las recomendaciones de acciones a tomar tendientes a mitigar estas debilidades y amenazas.
  - Implementación de los programas de protección, los cuales debieran ser acordados en reuniones uno a uno, entre SUBTEL y el operador de la red o propietario del sitio de mayor impacto, lo que está fuera del alcance de este estudio.
  - Medición de la efectividad de las acciones emprendidas
  - Evaluar y retroalimentar en forma permanente el resultado de estos planes, reiniciándose cada vez que sea necesario, como un programa de mejora continua en el esquema Planear – Hacer – Verificar - Actuar.
  - Promover y favorecer el intercambio de información, conocimiento y experiencias en la materia

8.5. Otras recomendaciones

Teléfono: (562) 225-7951 Celular: (569) 895-5657 e-mail: p.boric@entelchile.net

Para las nuevas instalaciones, incorporar al estudio de su emplazamiento, el análisis de impacto por concentración, evitando la proliferación de instalaciones críticas en una misma zona geográfica, expuesta a los mismos riesgos de las otras ya existentes en el área.

8.5.1. Recomendación específica para el servicio de telefonía móvil

Con el fin de que la población pueda estar al máximo protegida ante eventuales problemas de los proveedores de servicio móvil se recomienda que:

- Considerando que todos los operadores de telefonía móvil trabajan en el mismo estándar, se estudie la factibilidad de que los usuarios puedan acceder a un número de emergencia cuando no cuente con cobertura de su proveedor de servicio pero sí la tenga de algún otro operador. Esta propuesta está alineada con la implementación, a nivel de plan piloto, de un número único de emergencias en la región del Maule.

8.5.2. Recomendación específica para la protección de cables submarinos

A nivel mundial los cables submarinos son el principal soporte para las telecomunicaciones internacionales, estimándose que dichos sistemas cursan sobre un 90 % del tráfico internacional.

De acuerdo con la información proporcionada por TIWS, entre un 60 y 80% de las fallas en los cables submarinos son producto de agresión externa (principalmente producto de las actividades de pesca); entre un 5 y 20% por fallas de componentes, y entre un 10 y 15% por otras causas.

En general, los tiempos de reparación en caso de fallas para estos elementos, son de larga duración (semanas)

Recientemente se produjeron fallas simultáneas en tres cables submarinos en el Mar Mediterráneo, que interconectan Europa con el Medio Oriente y que afectaron seriamente las comunicaciones de Internet y otros servicios a los países de Egipto, Emiratos Árabes y

la India. Anteriormente, a principios del 2008 fallas similares ocurrieron en un total de cinco cables afectando a más de 80 millones de usuarios distribuidos en cuatro países del mismo sector.

Considerando estas características, es recomendable estudiar una regulación que permita proteger la infraestructura de cables submarinos, de las intervenciones externas producto de actividades de pesca y otras.

8.5.3. Recomendación específica para la protección lógica del servicio Internet

Las amenazas que combinan uno o más de los elementos en línea – Internet, spam, malware y botnets – continúan creciendo en número y sofisticación. Para mejorar su efectividad, los criminales están cada vez más escogiendo blancos específicos y explotando sitios web legítimos y sistemas de entidades de confianza. Las amenazas son cada vez mas difíciles de detectar y pueden engañar aún a usuarios suspicaces, utilizando ventajas de eventos actuales que les permiten aparecer creíbles ante sus victimas.

Simultáneamente el malware que se propaga en la red esta siendo constantemente rediseñado para hacerlo mas inteligente y tiene una alta tasa de crecimiento. Los Botnets, continúan difundiendo malware, enviando millones de correos spam, albergando sitios maliciosos y atacando sitios legítimos.

Las actividades ilícitas en la red explotan debilidades antiguas y nuevas en las tecnologías y sistemas para crear sus botnets. Al mismo tiempo, el aumento en el uso de dispositivos móviles, trabajo remoto, virtualización y nuevas formas de colaboración están expandiendo el perímetro de seguridad y haciendo mas permeables los bordes de la red. Esto impone un desafío grande para mejorar sus defensas e implantar políticas y tecnologías de seguridad más avanzadas.

Considerando lo señalado anteriormente, se requiere establecer una organización con los adecuados niveles de autoridad y responsabilidades para coordinar acciones de investigación, compartición de información y difusión de temas relativos a la seguridad de la Internet a nivel nacional.

Se deben incluir las actividades anti malware y componentes preventivas de botnets en las estrategias de seguridad, para contrarrestar estas amenazas.

Se debe establecer una política para incentivar la compartición de experiencias frente a ataques a las redes y recomendar una estrategia para acordar como reaccionar en estos casos.

Además se debe definir una estrategia de incentivos para que los privados inviertan en seguridad y compartan sus experiencias.

Otros aspectos a tener presente para orientar las políticas de seguridad son:

Mantener el foco. Un aspecto esencial es mantenerse enfocado en aplicar medidas de protección sobre infraestructura mas crítica, ya que al pretender protegerlo todo, se termina protegiendo nada. El tiempo, energía y recursos se deben enfocar en medidas de protección de los sitios más críticos.

Mantener el software actualizado para eliminar las vulnerabilidades. Una parte importante de las amenazas vigentes hacen uso de vulnerabilidades conocidas, por lo que se debe poner énfasis en aplicar las actualizaciones (parches) que resuelven estas vulnerabilidades conocidas. Alrededor del 80% de los ataques más comunes hacen uso del 20% de las vulnerabilidades de alto impacto, las que en general son básicas y sin embargo continúan sin ser parchadas en muchos ambientes.

Impulsar una actitud proactiva. El cumplir con las políticas establecidas no asegura que se estén protegiendo la infraestructura crítica, ya que las amenazas evolucionan en el tiempo. Se deben llevar a cabo revisiones de brechas de seguridad en forma regular para mejorar y actualizar los procedimientos existentes, de modo de enfrentar las nuevas amenazas que vayan surgiendo.

Hacer de la seguridad algo simple. Procurar que las soluciones y herramientas de seguridad sean simples de implementar y utilizar, y que el cumplimiento de las políticas sea fácil de seguir.

9. ANEXO N° 1 CUESTIONARIO

Cuestionario para evaluar la situación de la empresa respecto al aseguramiento de infraestructura crítica.

I. Instrucciones

Conteste a las preguntas de este cuestionario indicando, mediante una X, la valoración 0, 1, 2, 3 ó 4, eligiendo de las cinco descripciones siguientes, la que más se adapte a la situación actual de la organización evaluada:

0	Prácticamente no se realiza
1	Se realiza parcialmente (en ocasiones puntuales)
2	Se realiza generalmente (en la mayoría de los casos)
3	Se realiza sistemáticamente y en casi todas las áreas.
4	Se realiza siempre y de forma total.

II. Contexto

En el entendido que los servicios que presta su empresa son críticos para distintas actividades del quehacer nacional, sus clientes esperan que éstos se presten con altos estándares de continuidad de servicio, ante eventos de contingencias mayores que pudiesen generar un serio impacto en la salud, seguridad y bienestar de los ciudadanos o que podría afectar el funcionamiento del gobierno o de la economía del país.

Para esto efectos se debe considerar solamente los servicios de Telefonía fija, Telefonía móvil, Internet, Redes de datos privadas y Transporte de señales nacional e internacional, según corresponda a las concesiones de su empresa.

III. Cuestionario

Explique cuál es el criterio general aplicado por su empresa para definir la criticidad de sus diferentes servicios e instalaciones

_____
_____
_____
_____
_____
_____
_____

En este contexto, se deberá señalar si para la prestación de los servicios al cliente:

1) Existen procedimientos establecidos formalmente y documentados para identificar los sitios o nodos críticos para la continuidad en la prestación de servicios a los clientes

0	1	2	3	4

2) Está establecida formalmente una política de aseguramiento de la infraestructura crítica necesaria[37] para la continuidad operativa de los servicios prestados, está documentada y es de conocimiento de todo el personal

0	1	2	3	4

3) Apoya la dirección de la empresa la política antes señalada disponiendo de los recursos humanos, instalaciones y equipamiento necesarios.

0	1	2	3	4

4) Están asignadas las responsabilidades para el aseguramiento de la infraestructura crítica necesaria para la prestación de los servicios

0	1	2	3	4

[37] Entiéndase como "política de aseguramiento de la continuidad operativa de los servicios prestados", la gestión por parte del operador para instalar respaldos, holguras, stock de bodega para cubrir fallas, planes de recuperación de desastre, etc.

5) Existe un responsable del mantenimiento y revisión de la política de aseguramiento de la infraestructura crítica necesaria para la prestación de los servicios
.

0	1	2	3	4

6) Se desarrollan programas de educación y entrenamiento en los temas asociados al aseguramiento de la infraestructura crítica necesaria para la prestación de los servicios
.

0	1	2	3	4

7) Existen procedimientos formales para tratar los incidentes en aseguramiento de la infraestructura crítica

0	1	2	3	4

8) Se aplican procesos de gestión de cambios, claros, específicos y controlados para cada red operada por la empresa. Proceso de gestión de cambios es el destinado a controlar el impacto de cualquier cambio en la configuración física o lógica de los elementos que prestan servicios. Incluye las pruebas de aseguramiento de calidad y de impacto previa a la aplicación de los cambios en equipos y sistemas en producción, la planificación de vuelta atrás y restauración de servicios en caso de problemas al aplicar los cambios.

0	1	2	3	4

9) Los contratos con empresas proveedoras de servicio consideran explícitamente el resguardo y aseguramiento de la infraestructura crítica.

0	1	2	3	4

10) Se controlan los procedimientos de difusión de los compromisos, señalados en el punto anterior, hacia el personal de las empresas prestadoras de servicio.

0	1	2	3	4

11) Existe un plan de gestión de continuidad de servicios[38] para cada red operada por la empresa.

0	1	2	3	4

12) Existen los procedimientos para mantener la disponibilidad de cada servicio en el evento de un desastre

0	1	2	3	4

13) Se prueban estos procedimientos al menos una vez al año para asegurar su vigencia y el conocimiento de los mismos por parte del personal encargado de aplicarlos.

0	1	2	3	4

14) Existen procesos formales para evaluar el comportamiento de la gestión de aseguramiento de la infraestructura crítica necesaria para la prestación de los servicios y la realimentación de sugerencias para su mejoramiento.

0	1	2	3	4

15) Se efectúan auditorias al menos una vez al año para validar la aplicación de los procedimientos destinados a garantizar el aseguramiento de la infraestructura crítica necesaria para la prestación de los servicios.

0	1	2	3	4

16) El equipamiento utilizado para prestar los servicios a los clientes (tanto los ubicados en sitios o estaciones, como los puntos de concentración de planta externa), se encuentra ubicado dentro de un área segura, protegidos por un perímetro de seguridad definido.

0	1	2	3	4

[38] La gestión de continuidad de servicios debe incluir la definición de los niveles de servicio comprometidos, su medición y registro de cumplimiento, los procesos para implantar las mejoras necesarias que aseguren su cumplimiento y plan de mejora de los índices comprometidos.

17) El equipamiento utilizado para prestar los servicios a los clientes se encuentra protegido contra fallas de suministro de energía.

0	1	2	3	4

18) Se cuenta con los procedimientos para realizar pruebas de operatividad en los sistemas destinados al aseguramiento de la infraestructura crítica necesaria para la prestación de los servicios.

0	1	2	3	4

19) Se realizan pruebas de operatividad de los sistemas destinados al aseguramiento de la infraestructura crítica y se registran las pruebas efectuadas y sus resultados.

0	1	2	3	4

20) Existen políticas formales de asignación de privilegios para el acceso a la configuración lógica de los equipos con los que se da servicio a los clientes, con mecanismos de autenticación adecuados para usuarios y equipos.

0	1	2	3	4

21) Participa la empresa en grupos de trabajo a nivel de industria para compartir metodologías de operación destinadas al aseguramiento de la continuidad de servicios críticos

0	1	2	3	4

22) Mantiene la empresa acuerdos de respaldo mutuo de la infraestructura crítica con otras empresas del sector, para el aseguramiento de la continuidad de servicios críticos

0	1	2	3	4

Instrucciones para llenado de planilla Excel de entrega de información de los nodos o elementos de red

En la planilla Excel adjunta: "ENCUESTA ELEMENTOS DE RED", se deberá incluir la información correspondiente a cada nodo o elemento de red que cumpla con el criterio de dar servicio a mas de 50.000 usuarios o transportar 1 o más STM16 ó su equivalente.

Para esto efectos, se deben considerar en hoja separada, los nodos o elementos de red que están involucrados en la prestación de cada uno de los siguientes servicios, según corresponda a las áreas de actividad de su empresa:

- Telefonía fija,
- Telefonía móvil,
- Internet,
- Redes de datos privadas
- Transporte de señales nacional
- Transporte de señales internacional.

Las características técnicas de los elementos de red está compuesta, por ejemplo, por la siguiente información:

- Identificador de elemento de red
- Tipo elemento de red
- Redundancia
- Cantidad de usuarios o tráfico soportados
- Cobertura geográfica del servicio atendido por el nodo respectivo
- Otra

La información de ubicación del nodo o elemento de red está compuesta por la siguiente información:

- Región
- Localidad
- Comuna
- Nombre del sitio
- Dirección
- Latitud
- Longitud

El llenado de las planillas, en varios de los conceptos requeridos, se debe hacer en base a la selección de respuesta desde la lista desplegable de opciones que se ha incorporado.

Instrucciones para llenado de planilla Excel de entrega de información de los 10 sitios más críticos

Señale los 10 sitios de mayor impacto hacia los usuarios debido a la indisponibilidad de uno o más servicios, en caso de verse sometido, dicho sitio, a una contingencia mayor.

solicita a Ud. que se informen los 10 sitios (entendiendo por sitios cualquier ubicación que aloje equipamiento destinado a la prestación de uno o más de los servicios de Telefonía fija, Telefonía móvil, Internet, Redes de datos privadas y Transporte de señales nacional e internacional) o emplazamientos que su representada considere de mayor impacto hacia los usuarios considerando, para ello, que una probable indisponibilidad de estos sitios, podría afectar a una gran cantidad de usuarios y cobertura geográfica. Al respecto, solicitamos a Ud. que como uno de los criterios para considerar un nodo como crítico, tome en cuenta, dentro de lo posible, la relevancia del tipo de usuario al cual el nodo presta servicio, por ejemplo, si los usuarios o clientes son hospitales o entidades de gobierno o entidades financieras o empresas productivas, relevantes desde el punto de vista de sus necesidades de comunicación.

Le solicitamos que en dicha planilla, se señalen los 10 sitios de mayor impacto hacia los usuarios debido a la indisponibilidad de uno o más servicios, en caso de verse sometido, dicho sitio, a una contingencia mayor. Aunque en la planilla se solicita se informe sólo sitios con más de 50.000 usuarios, si su empresa considera que debe informar dentro de esta lista de sitios críticos alguno con un número menor de usuarios, ya que dicho sitio atiende a usuarios muy importantes en el contexto del tema analizado en esta consulta, le solicitamos que nos lo informe en una planilla separada, con el mismo formato, indicando la cantidad de usuarios que atiende y las razones por las que dichos nodos son considerados críticos.

Para estos efectos se deben considerar los sitios (o emplazamientos) que están involucrados en la prestación de uno o más de los siguientes servicios, según corresponda a las áreas de actividad de su empresa:

Telefonía fija,
Telefonía móvil,
Internet,
Redes de datos privadas y
Transporte de señales nacional e internacional.

En este contexto, se considera un sitio, cualquier ubicación que aloje equipamiento destinado a la prestación de uno o más de los servicios arriba señalados.

Para la entrega de la información requerida sírvase llenar la planilla Excel adjunta: "SITIOS CRITICOS", indicando en primer lugar los datos del sitio mas crítico (o de mayor impacto) y así sucesivamente a medida que baja el nivel de criticidad de los diferentes sitios. También se solicita agregar diagramas de alto nivel para las redes que soportan los servicios anteriormente indicados.

10. ANEXO N° 2 PLANILLAS

Planillas para evaluar Elementos de Red, y Planilla para evaluar Sitios Críticos

Ver archivos Excel adjuntos en CD.

11. ANEXO N° 3 RESPUESTAS RECIBIDAS

En los archivos adjuntos en CD, se incluyen todas las respuestas recibidas de los operadores, junto con los puntajes obtenidos según la metodología explicada

12. ANEXO 4 DEBILIDADES Y AMENAZAS DE LA INFRAESTRUCTURA CRÍTICA DE TELECOMUNICACIONES

A continuación se presenta un listado de las principales vulnerabilidades (debilidades y amenazas), a la que puede estar expuestas la infraestructura de telecomunicaciones.

Debilidades

a. Nivel Política

i. Falta de identificación de la infraestructura crítica
ii. Falta de políticas generales sobre protección de infraestructura crítica
iii. Falta de sensibilización del tema a nivel país
iv. Falta de un sistema de identificación de amenazas, coordinación de respuestas, evaluación de daños y reconstrucción
v. Falta de instancia superior, a nivel de la industria, que permita a los operadores compartir experiencias en protección de infraestructura crítica
vi. Falta de una instancia a nivel gobierno que permita promover la cooperación público-privada en la protección de infraestructura crítica.

b. Nivel Operativo

i. Interdependencia con otras redes o servicios críticos (agregación de servicios sobre redes de transporte)
ii. Compartir Infraestructura de instalaciones con otras redes o servicios
iii. Insuficiente autonomía para sistemas de generación eléctrica de respaldo
iv. Insuficiente capacidad de almacenamiento de agua para sistemas de climatización
v. Falta de capacidad de monitoreo en tiempo real (7x24) de variables del entorno de operación en estaciones aisladas
vi. Falta de disponibilidad de recursos inmediatos para habilitar una reacción ante la falla de elementos críticos (recursos de personal calificado, repuestos, medios de movilización y financieros)

vii. Normativa interna muy restrictiva para coordinar reacción ante falla de elemento crítico.
viii. Falta de educación y entrenamiento en los temas asociados al aseguramiento de la infraestructura crítica
ix. Falta de capacitación hacia personal de empresas contratistas en lo relativo al aseguramiento de la infraestructura critica
x. Falta de acuerdos ínter empresas para respaldo mutuo en caso de fallas de servicios críticos. Falta de procedimientos para aplicar los respaldos y probarlos.
xi. Falta de procedimiento para el reporte y registro de fallas de infraestructura crítica; de su seguimiento de solución con posterior evaluación del caso, analizando causas y respuestas; propuestas de mejora.
xii. Falta de un sistema de seguimiento para validar la implantación de las mejoras propuestas para robustecer la protección de la infraestructura crítica.
xiii. Falta de interacción con organismos tipo CERT
xiv. Falta de herramientas en operadores ISP para controlar virus, malware y spam.

Amenazas

a. De origen humano

i. Propagación de software maligno (virus, trojanos, malware, spyware, etc.)
ii. Acción de Hackers (robo de información, cambio de datos, borrado de datos, etc.)
iii. Ataques contra aplicaciones (DoS, alteración DNS, otras)
iv. Aplicaciones ilícitas (phishing, suplantación identidades, otras)
v. Sabotajes a sitios e instalaciones
vi. Robos (de cables, de equipos, repuestos, combustibles, otros)
vii. Acciones de Terrorismo
viii. Errores de operación o mantenimiento

b. De origen natural o Fuerza Mayor

i. Tormentas (eléctricas, viento, lluvia, nieve)

ii. Aluviones
iii. Inundaciones
iv. Marejadas
v. Terremotos
vi. Incendios (forestales o de otra naturaleza)

c. De interdependencia

i. Corte en el suministro eléctrico
ii. Corte en el suministro de agua
iii. Corte de caminos, puentes, vías lacustre para acceder a las instalaciones
iv. Corte de transporte público que afecte al personal operativo
v. Indisponibilidad de soporte técnico de alto nivel

El análisis específico de los riesgos a los cuales está expuesto cada sitio crítico de infraestructura de telecomunicaciones, se deberá abordar en etapas posteriores, para lo cual se recomienda focalizarse en un análisis con cada empresa operadora, que cubra cada uno de los sitios de mayor índice de impacto, según lo definido en el punto 6.5 de este estudio.

13. ANEXO 5 ANALISIS DETALLADOS DE AUSTRALIA, CANADA Y HOLANDA EXTRAIDO DE DOCUMENTO DE LA OECD

El análisis fue realizado en base a consultas específicas que se les hicieron a estos países en relación al tema de la ICI, las preguntas y respuestas se entregan a continnuación.

Pregunta N° 1 corresponde a:

13.1.1. ¿Cuáles son sus políticas de seguridad nacional, estrategias y estructura existente de autoridades y agencias?

13.1.1.1. Australia

13.1.1.1.1. Política y estrategia de seguridad nacional

En Australia, la Estrategia Nacional de Protección de Infraestructura Crítica provee los principios generales para la protección de la infraestructura crítica, describe las principales tareas y asigna las responsabilidades para su aplicación. La Estrategia define en el caso de este país a la infraestructura crítica nacional como: "aquellas facilidades físicas, cadenas de proveedores, tecnologías de la información y redes de telecomunicaciones que si fueran destruidas, degradadas o no estuvieran disponibles por un período extenso de tiempo, podrían provocar un impacto significativo en el bienestar social y económico de la nación, o afectar la capacidad de Australia para conducir la defensa nacional y seguridad de la nación".

La Estrategia es aplicable no sólo para todos los niveles del gobierno sino que también para los dueños y operadores de la infraestructura, la cual en gran medida se administra sobre una base comercial.

13.1.1.1.2. Autoridades de Gobierno y Agencias

La Estrategia para la protección de la infraestructura crítica descansa en una relación de fuerte cooperación y coordinación entre las diversas entidades que conforman el Gobierno de Australia en todo el territorio nacional, cada una con sus respectivos roles y responsabilidades.

13.1.1.2. Canadá

13.1.1.2.1. Política y estrategia de seguridad nacional

Canadá reconoce que la protección de la infraestructura crítica IC incluyendo la infraestructura crítica de la información ICI, requiere del compromiso y colaboración de todos los participantes. Canadá se ha enfocado en modernizar su legislación y marco regulatorio para facilitar acuerdos e intercambio oportuno de información entre IC e ICI a todos los niveles del gobierno y con el sector privado.

Dado que el intercambio de información es un elemento esencial para la protección y aseguramiento de la IC y de la IC cibernética las nuevas Actas de Gestión de Emergencias, tienen como objetivo facilitar el intercambio de información relativo a emergencias, incluyendo avisos de amenazas, activos vulnerables, planes de continuidad de negocios. Un elemento crítico en este intercambio de información guarda relación con la habilidad para proteger de su divulgación la información sensible relacionada con IC, ICI.

La política de seguridad de Canadá está contenida en el documento Securing an Open Society: Canada´s National Security Policy. El objetivo de esta política es asegurar que el gobierno está preparado para enfrentar y responder a diversas amenazas de seguridad, incluyendo actos terroristas, enfermedades infecciosas, desastres naturales, ataques cibernéticos a infraestructura crítica y extremismo doméstico.

13.1.1.2.2. Autoridades de Gobierno y Agencias

El gobierno de Canadá cuenta con una estructura compuesta por diferentes cuerpos legales, cada uno con roles y responsabilidades debidamente coordinadas. Estas organizaciones son:

- Public Safety and Emergency Preparedness Canada (PSEPC).
- Government Operations Centre.
- Canadian Security Intelligence Service (CSIS).
- Communications Security Establishment (CSE).
- Royal Canadian Mounted Police (RCMP)

Adicionalmente el gobierno federal ha establecido el Canadian Cyber Incident Response Centre.

13.1.1.3. Holanda

13.1.1.3.1. Política y estrategia de seguridad nacional

El plan de respuesta de emergencia nacional de Holanda incluye una estructura genérica e intercambio de información que debe seguir el grupo encargado de la crisis. Este paragua es válido para todas las autoridades públicas encargadas de participar durante una emergencia. El desarrollo, implementación y mantención del plan genérico es responsabilidad del Ministro del Interior. En relación a emergencias o crisis relacionadas específicamente con la ICI está en desarrollo el plan específico.

13.1.1.3.2. Autoridades de Gobierno y Agencias

En Holanda ha sido implementado un plan de emergencia nacional, el cual incluye una estructura genérica e intercambio de información. Esta estructura es válida para las autoridades públicas que participan de alguna manera durante la crisis. Adicionalmente cada ministro ha implementado medidas de respuestas específicas para su sector. El Ministro de Asuntos Económicos como responsable del sector de telecomunicaciones ha desarrollado e implementado medidas específicas para responder ante situaciones de crisis que puedan ocurrir en el sector de telecomunicaciones.

Pregunta N° 2 corresponde a:

13.1.2. ¿Qué se entiende por infraestructura crítica de la información en su país y cuáles son sus políticas y objetivos? ¿Cómo identifica su gobierno lo que constituye ICI?

13.1.2.1. Australia

La Infraestructura de información nacional (NII) en Australia es un subconjunto de la infraestructura crítica nacional y está compuesta por los sistemas electrónicos que soportan servicios críticos tales como telecomunicaciones, transporte y distribución, energía, electricidad, banca y finanzas.

La infraestructura es considerada crítica si es que su falla puede afectar a la economía y sistema social, o afectar la posibilidad de asegurar la seguridad nacional. Cada una de estas infraestructuras en forma creciente es dependiente de la infraestructura de información para el monitoreo y control de sus operaciones, sin embargo, la infraestructura de información es

simultáneamente dependiente del acceso a la energía eléctrica y otros servicios, resultando un complejo sistemas de interdependencias y vulnerabilidades.

El Gobierno de Australia reconoce que desde el año 2001 el ambiente en línea ha cambiado significativamente. Es actualmente de una naturaleza altamente interconectada y que la seguridad de los sistemas cibernéticos no pueden ser conducidos a través de esfuerzos discretos aislados.

En la identificación de qué infraestructura se considera crítica, se tiene en cuenta a quien está soportando dicha infraestructura. Los análisis de riesgo de infraestructura crítica han sido conducidos en un contexto de su relevancia a la comunidad o sector que le sirve. Esto significa que cada sector del país y del gobierno fue requerido para que identificara la infraestructura crítica para su funcionamiento.

El Gobierno de Australia está desarrollando un modelamiento del análisis y protección de la infraestructura crítica con la capacidad de examinar las dependencias e interdependencias entre infraestructura crítica nacional y las consecuencias de fallas de la infraestructura crítica.

13.1.2.2. Canadá

Canadá define su infraestructura crítica nacional (NCI) como: aquella tecnología física o de información, redes, servicios, las cuales si fueran interrumpidas o destruidas, podrían provocar un serio impacto en la salud, seguridad o bienestar de los canadienses o el funcionamiento efectivo del gobierno. Esto incluye componentes físicos como cibernéticos.

La infraestructura crítica nacional en Canadá está compuesta de diez sectores.

- Energía eléctrica, gas natural, producción y transporte de petróleo.
- Tecnología de las comunicaciones e información (telecomunicaciones, sistemas de broadcasting, software, hardware, y redes incluyendo internet).
- Finanzas
- Salud
- Alimentación

- Agua
- Transporte
- Seguridad
- Gobierno
- Fabricas (materiales de defensa, industria química)

En Canadá la protección de la infraestructura crítica puede ser definida como las acciones y programas que:

- Identifican la infraestructura crítica y sus componentes específicos
- Analizan las vulnerabilidades
- Mitiga o toma medidas preventivas para reducir las vulnerabilidades
- Mejora la gestión del riesgo

Dada la interdependencia y conexión entre las infraestructuras críticas, una interrupción de cualquiera de ellas podría producir un efecto en cascada de interrupción de otros sistemas considerados críticos.

13.1.2.3. Holanda

En Holanda la infraestructura crítica de información consiste de los sistemas de información (software, hardware o data) que soporta una o más infraestructura crítica y cuya interrupción o falla podría ocasionar un daño severo al funcionamiento de esa infraestructura crítica en particular.

En Holanda el gobierno tiene la responsabilidad de mantener operativa la infraestructura crítica de información. Para aquellas que son de propiedad o controladas por organizaciones del gobierno, éste tiene la completa autoridad para ejecutar análisis de riesgo e implementar las medidas de mitigación que estime pertinente.

Para aquellas que son controladas o que pertenecen a organizaciones privadas, el gobierno es responsable de que las respectivas partes efectúen sus propios análisis de riesgo e implementen las medidas que consideren apropiadas. La capacidad legal del gobierno para cumplir con este mandato, depende de la regulación vigente para cada sector en particular. Si la regulación no obliga a las compañías a desarrollar actividades como gestión del riesgo o implementar medidas de continuidad operacional el gobierno tiene un rol de consejero.

El Ministerio de Asuntos Económicos inició un proyecto relacionado con la identificación de la infraestructura crítica de telecomunicaciones. Las actividades para lograr este fin son las siguientes:

- Cuestionario para identificar servicios vitales.
- Cuestionario para identificar nodos vitales.
- Proceso de selección para determinar servicios/nodos críticos.
- Estudio de aspectos de interconexión de servicios e infraestructura.
- Cuestionario del impacto de una interrupción de servicios/nodos críticos.
- Selección de escenarios crisis o desastres que podrían ocurrir como entrada para el análisis de riesgo.
- Análisis de vulnerabilidades de servicios/nodos críticos seleccionados.
- Listado realístico y apropiadas recomendaciones para mejorar la protección contra interrupciones.

Pregunta N° 3 corresponde a:

13.1.3. ¿Cuál es el rol del gobierno en la gestión del riesgo de la ICI?

13.1.3.1. Australia

El Gobierno de Australia juega un rol importante en la protección de la infraestructura crítica y la agencia respectiva National Infraestructure Information es responsable entre otras cosas de:

- Proveer el liderazgo estratégico y coordinación en el desarrollo e implementación de un plan nacional consistente para la protección de la infraestructura crítica.

- Asegurar protección de los servicios esenciales del Gobierno.

- Comunicar información de inteligencia relevante a todos los participantes involucrados en la protección de la infraestructura crítica.

- Asegurar que se hayan realizado los acuerdos necesarios para la protección de la infraestructura crítica en los sectores regulados.

- Desarrollar y mantener una base de datos de la infraestructura crítica.

- Asistir a los dueños y operadores de infraestructura crítica de los sectores regulados en el desarrollo, validación y auditoría de planes relevantes.

- Gestionar y coordinar la información pública y con los medios de difusión.

Los operadores de infraestructura crítica y sus dueños, tienen la responsabilidad para asegurar en forma adecuada sus activos y aplicar técnicas de gestión del riesgo a sus procesos.

El Gobierno Australiano ha adoptado una estrategia de cinco puntos para la protección de la infraestructura crítica, que son:

- Desarrollo de una política que incluye Commonwealth, industria y el estado y territorios.

- Recolección de información y análisis.

- Medidas defensivas, incluyendo medidas de seguridad como de advertencia temprana.

- Medidas de respuestas desde aspectos técnicos a incidentes puntuales como manejo de crisis.

- Planes de contingencia que cubren tanto incidentes puntuales como de amplio impacto.

Además, la agencia de gobierno encargada del tema de continuidad de funcionamiento de la infraestructura crítica soporta al gobierno y a la industria en general en:

- Identificar conexión entre nodos de infraestructura crítica dentro de un mismo sector como a través de varios sectores de la economía.
- Análisis de relaciones e interdependencias.
- Examina los efectos en cascada de fallas en la infraestructura crítica.
- Identifica puntos únicos de fallas y otras vulnerabilidades.
- Analiza opciones de inversión en medidas de seguridad.
- Desarrolla planes de mitigación y continuidad operacional.

13.1.3.2. Canadá

Canadá se encuentra desarrollando su Estrategia de Protección a la Infraestructura Crítica Nacional, en la cual se le da gran importancia a la promoción de una gestión integrada del riesgo de la infraestructura crítica, incluyendo componentes físicos y cibernéticos y que sean aplicados tanto en el sector público como privado.

En general, los componentes de la gestión del riesgo de la infraestructura crítica incluye:

- Entender y advertir las interdependencias de la infraestructura crítica.
- Asegurar la infraestructura crítica a través de análisis de amenazas y vulnerabilidades, mitigación y preparación.
- Gestionar respuesta y recuperación a través de la facilitación de coordinación entre los distintos sectores.

Otro elemento clave en la gestión del riesgo es el intercambio de información. Mientras más es la información disponible acerca de potenciales amenazas y vulnerabilidades, mejor es el entendimiento del riesgo y se puede asegurar la continuidad de los servicios esenciales.

13.1.3.3. Holanda

Un tema relevante es el acuerdo entre el gobierno y los grandes proveedores de infraestructura crítica, en el sentido que informen las interrupciones o fallas, a partir de ciertos niveles de severidad, que puedan presentar los sistemas que administran.

Pregunta N° 4 corresponde a:

13.1.4. ¿Cómo es el intercambio de información y otros mecanismos utilizados al interior de su gobierno y con otros participantes para manejar el tema de la ICI?

13.1.4.1. Australia

El principal mecanismo empleado en Australia para el intercambio de información relevante relacionada a la protección de la infraestructura crítica entre el gobierno y el sector privado es la Trusted Information Sharing Network for Critical Infraestructure Protection, la cual fue establecida en el año 2004 y está compuesta por un grupo de analistas de nueve sectores específicos que cubren las áreas de banca y finanzas, comunicaciones, energía, servicios de emergencia, cadenas de alimentos, salud, transporte y lugares de alta concentración de gente.

13.1.4.2. Canadá

El gobierno de Canadá se ha comprometido en desarrollar e implementar la National Cyber Security Strategy para reducir la vulnerabilidad del Canadá a ataques o accidentes cibernéticos. Se han realizado consultas a los sectores de infraestructura crítica sobre la composición y mandato de la National Cyber Security Task Force la cual examina el estado de la seguridad cibernética en Canadá.

13.1.4.3. Holanda

En Holanda el intercambio de información se realiza en diferentes foros entre otros en las reuniones periódicas del National Crisis Centre y el intercambio de información entre el gobierno y el sector privado es una parte integral de la gestión de riesgo en este país.