Guía de buenas prácticas de GFCE-MERIDIAN

sobre

protección de infraestructuras críticas de la información

para responsables de políticas gubernamentales

MERIDIAN
Connecting and Protecting

PRÓLOGO

La protección de infraestructuras críticas de la información (PICI) es un tema complejo pero importante para los países. En general, las sociedades dependen, y de forma crucial, del correcto funcionamiento de los servicios de sus infraestructuras críticas (IC) tales como el suministro eléctrico, las telecomunicaciones, los sistemas financieros, el agua potable y los servicios gubernamentales. A su vez, estas IC dependen, a menudo, de manera vital, del correcto funcionamiento de las infraestructuras críticas de información (ICI) que engloban tanto las infraestructuras esenciales de la comunicación e información (p.ej. servicios de Internet y telefonía móvil), como los sistemas fundamentales de comunicación e información que forman parte de las IC. Éstas incluyen los sistemas de control que realizan seguimientos y vigilancia de procesos físicos cibernéticos esenciales (p.ej. el funcionamiento remoto de válvulas de oleoductos) y sistemas logísticos y administrativos.

La necesidad de proteger las infraestructuras críticas de la información es cada vez más importante. El riesgo que corre la sociedad por la falta de protección o medidas suficientes, es cada día mayor. Debido a que las infraestructuras de comunicación e información están cada vez más interrelacionadas globalmente, las ICI de un país pueden convertirse en objetivo de *malware*, piratas informáticos, personas que utilizan subversivamente las redes informáticas para realizar protestas y operaciones estales hostiles. Del mismo modo, las infraestructuras críticas de información de un país pueden pasar a ser un medio para atacar a las de otro. Con estas infraestructuras amenazadas, el funcionamiento correcto y sin interrupción de las IC puede estar en peligro y con ello, también, la sociedad, economía y vida cotidiana de la población. Es más, la interconnexión mundial de las ICI implica que cuando una de estas infraestructuras es vulnerable, puede convertirse en el punto débil y, como consecuencia, ser un riesgo para las ICI del resto de países.

Varias naciones trabajan ya en la protección de las infraestructuras críticas (PIC), pero tienen problemas a la hora de avanzar en la protección de infraestructuras críticas de la información. Otras, se encuentran al comienzo de su labor que combina PIC y PICI. Otro grupo de países ya han avanzado en ese ámbito y es posible que hayan experimentado dificultades, pero también desarrollado buenas prácticas. Con el objetivo de incrementar la protección y progresar en la PICI, el Proceso Meridian (Meridian Process) y el Foro Global de Experiencia Cibernética (GFCE, según sus siglas en inglés) adoptaron conjuntamente la iniciativa de crear esta guía de buenas prácticas sobre PICI dirigida a los responsables políticos de las ICI e IC nacionales. Es más, estas buenas prácticas podrían ser útiles para los operadores de IC en el ámbito nacional e internacional. El objetivo de esta guía es ayudar a los países que se encuentran todavía al comienzo del camino, pero también a aquellos que ya están trabajando. Somos conscientes de que cada nación cuenta con una estructura normativa y jurídica propia, diferentes formas de gestionar las IC y las ICI, un nivel de adaptación de tecnologías de la comunicación e información (TCI) igualmente distinto, una cultura diferente, etc. Estas buenas prácticas no son una verdad universal. Están hechas para inspirar al lector. Puede ocurrir, incluso, que al aplicar una buena práctica sea

necesario ajustar el planteamiento para adaptarse a las necesidades. Esperamos que estas buenas prácticas ayuden en la protección y capacidad de recuperación ante ataques de las IC/ICI. Igualmente, quisiéramos destacar que otros países que se encuentran en fases más avanzadas podrían ofrecer su ayuda.

El equipo de redacción junto con señor Peter Burnett (Coordinador de Meridian) y señora Nynke Stegink (Centro de ciberseguridad nacional de los Países Bajos) quienes nos han brindado su colaboración.

Señor Eric Luiijf

ÍNDICE

FIGURAS

TABLAS

1 INTRODUCCIÓN

1.1 NECESIDAD DE PROTEGER INFRAESTRUCTURAS CRÍTICAS DE LA INFORMACIÓN

La protección de infraestructuras críticas de la información (PICI) es un tema complejo pero también importante para los países. En general, las naciones dependen, en gran medida, de servicios de infraestructuras de suma importancia tales como el suministro eléctrico, las telecomunicaciones, los sistemas financieros, el agua potable y los servicios gubernamentales. Estas infraestructuras críticas (IC) se definen como: *"Aquellas infraestructuras esenciales para que las funciones básicas de la sociedad: salud, seguridad, bienestar social y económico de los ciudadanos puedan mantenerse, y cuyos daños o destrucción tendría serias consecuencias"* [CE2008].

Hoy en día, los daños físicos (o incluso la destrucción) de elementos esenciales de las IC no son la única amenaza para el correcto funcionamiento de éstas. Los servicios basados en las tecnologías de la comunicación y la información (TCI) son cada vez más importantes para el funcionamiento de las IC. Un fallo en la infraestructura relacionada con la información puede tener repercusiones muy serias para un país. De aquí surge el concepto de infraestructura crítica de la Información (ICI) que incluye tanto información e infraestructura de (tele)comunicaciones esenciales (p.ej. telefonía móvil y servicios de acceso a Internet), como TCI y sistemas de control de procesos que son cruciales para la prestación de servicios de las infraestructura críticas (Véase figura 1).

Al igual que en las IC, una interrupción en el servicio de las ICI puede deberse a fallos humanos, fallos técnicos o algún tipo de accidente. Ahora bien, no siempre hay un equilibrio entre los beneficios de las ICI (mayor conectividad, control remoto, adaptabilidad, fiabilidad, reducción de costes) y los posibles efectos negativos de un fallo. Las ICI son, cada vez más, parte esencial de las IC, son el "pegamento" entre y dentro de ellas, y se están interconectando globalmente. Al mismo tiempo, las ICI de un país pueden ser tanto objetivos de malware, piratas informáticos, personas que utilizan subversivamente las redes informáticas para realizar protestas y operaciones estales hostiles, como un medio para atacar las ICI de otro país. Unas infraestructuras críticas de información puestas en peligro o cuyo servicio se ha visto interrumpido pueden hacer peligrar la seguridad y estabilidad nacional, el crecimiento económico, la prosperidad de la población y la vida diaria, y el impacto puede incluso llegar a otras naciones debido a su la interconectividad mundial. Es por ello que la mayoría de países considera cada vez más importante contar con estrategias, políticas, y actividades efectivas para la PICI.

1.2 OBJETIVO DE ESTA GUÍA DE BUENAS PRÁCTICAS

Varios países trabajan ya en la Protección de Infraestructuras Críticas (PIC)[1] pero tienen problemas a la hora de avanzar con la protección de infraestructuras críticas de información. Otros, están comenzando su camino para combinar la CIP y la PICI. Sin embargo, también hay ejemplos de otros países que han hecho grandes avances para desarrollar una PICI.

1 Protección de infraestructuras críticas: ***"Toda actividad destinada a garantizar la funcionalidad, continuidad e integridad de las IC con el fin de prevenir, paliar y neutralizar una amenaza, riesgo o vulnerabilidad."*** [CE2008]

Su experiencia, ya sea positiva o negativa, merece la pena ser compartida. Es por ello que el Proceso Meridian (Meridian Process) y el Foro Global de Experiencia Cibernética han tomado la iniciativa de crear una guía de buenas prácticas para fomentar la PICI y ofrecer valiosos conocimientos a los países que todavía están dando los primeros pasos en este campo. La guía está pensada principalmente para las infraestructuras críticas del gobierno y los responsables de las ICI, pero de igual modo puede servir para los operadores de las CI que trabajan en el ámbito nacional e internacional.

Existen numerosas diferencias entre países. Diferencias en las estructuras culturales, de regulación y del ámbito jurídico, diferentes maneras de gestionar las IC y las ICI, diferentes culturas políticas, diferente nivel de adaptación de las tecnologías de la información y comunicación (TIC), etc. Es por ello que las buenas prácticas aquí descritas deben utilizarse de forma flexible. Deben servir de estímulo a los responsables gubernamentales de la formulación de políticas sobre las IC y las ICI, y facilitar la creación de estrategias y planes que se adecúen a los objetivos, a la vez que ayudar a evitar enfoques que se han utilizado en otros países y que no han funcionado. Sepan, que como nación, no se encuentran ustedes solos ya que la protección de infraestructuras críticas de información es un tema global que afecta a todos los países. Uno puede utilizar estas prácticas y preguntar a otros países cómo abordan la PICI, por ejemplo, a través de las comunidades del Proceso Meridian (Meridian Process) y del Foro Global de Experiencia Cibernética, y aprender de ellos.

Estas buenas prácticas complementan el anterior *"Manual de buenas prácticas sobre políticas de PIC para legisladores europeos" [RECIPE]*. Varias de las prácticas recomendadas en ese manual se retoman para el ámbito de la PICI.

1.3 ICI, PICI Y CIBERSEGURIDAD

Aunque el concepto de ICI se acuñó hacia 2001 (véase p.ej. [Bruno2002]) y poco después fue utilizado por el G8 [G8] y la Organización de Cooperación y Desarrollo Económicos [OCDE2007, OCDE2008], todavía no existe un amplio consenso sobre su definición. Varios países sí han ofrecido la suya. Estos son algunos de los ejemplos: "Las infraestructuras cibernéticas/TCI críticas hacen referencia a las ciberinfraestructuras que resultan vitales en servicios esenciales para la sanidad pública, la estabilidad económica, la seguridad nacional, la estabilidad internacional y la sostenibilidad y restablecimiento del ciberespacio esencial" [Unión Africana], "Con TCI de las infraestructuras críticas nos referimos a infraestructuras críticas de información (ICI)" [Victoria], *"Las infraestructuras críticas de información son el subconjunto de recursos de información que repercuten directamente en que el Estado pueda realizar y continuar su labor, y en la seguridad de la sociedad" [Brasil], "Las infraestructuras críticas de información (ICI) pueden referirse a cualquier sistema TI que dé apoyo a recursos y servicios clave en la infraestructura nacional" [RU].*

Basándonos en las definiciones nacionales y nuestros conocimientos (Véase figura 1), desarrollamos una definición global para "infraestructura crítica de información" que reflejara la necesidad de considerar las tecnologías de la comunicación e informática como

una infraestructura crítica en sí misma, y el aspecto del ámbito intersectorial de las infraestructuras críticas por otro lado, debido a que se utilizan las mismas tecnologías y, por lo tanto, existe un riesgo en la mayoría de los procesos vitales de los sectores de las IC:

Infraestructura crítica de la información (ICI): "*Información interconectada e infraestructuras de comunicación esenciales para el mantenimiento de los servicios básicos de la sociedad (salud, seguridad, bienestar económico o social de las personas) cuyos daños o destrucción tendría serias consecuencias".*

Protección de infraestructuras críticas de la información (PICI) surge de la definición de ICI y se define como: *"Toda actividad encaminada a garantizar la funcionalidad, continuidad e integridad de las ICI para prevenir, paliar o neutralizar una amenaza, riesgo o vulnerabilidad, o minimizar el impacto de un incidente".*

Existen numerosas definiciones dispares sobre los conceptos que se abordan en esta guía de buenas prácticas. En [CIPedia©] pueden encontrarse multitud de definiciones nacionales e internacionales en varios idiomas para estos conceptos. Sin embargo, las diferencias que pueda haber no deberían hacer que se desviara la atención de la necesidad de proteger infraestructuras críticas de información. Sólo en los casos de acuerdos detallados con otros países es cuando resulta necesario aclarar las sutiles diferencias que puedan darse en las definiciones e interpretaciones.

Tal y como se muestra en la figura 1, las ICI incluyen tanto las IC de *"infraestructuras críticas de información y comunicación"* (p. ej.: servicios de telecomunicaciones móviles, puntos de intercambio de Internet, servicios de nombre de dominios), como las infraestructuras *cruciales* de la comunicación e información dentro de cada IC, tal como los sistemas físicos cibernéticos esenciales y los sistemas administrativos clave.

Los sistemas ciberfísicos son una combinación de sistemas de control que supervisan y vigilan procesos físicos vitales, por ejemplo: la variación, activada de modo remoto, del flujo de un fluido o gas que pasa por válvulas, el arranque de un motor, o la activación de líneas de alta tensión.[2] Entre las ICI se encuentran los sistemas de control de procesos que vigilan y gestionan la producción de energía eléctrica, sistemas globales de navegación por satélite (p.ej., BeiDou, Galileo, GLONASS, GPS), los servicios de información entre bancos para liquidar cuentas y el acceso a infraestructuras para utilizar servicios globales de Internet.

El hecho de que las TCI estén integradas en las IC beneficia a éstas al proporcionarles mayor flexibilidad en su actividad, como pueden ser, la vigilancia, el acceso remoto (mantenimiento, control y operatividad), la integración en TCI empresariales y la adaptabilidad de los procesos [Luiijf2015]. Es necesario tener presente las nuevas dependencias y vulnerabilidades que surgen en funciones esenciales de las IC debido a que las TCI están globalmente

2 Los sistemas ciberfísicos se definen del modo siguiente: *"Un sistema ciberfísico se define como una TCI y sistemas informáticos que apoyan, gestionan y supervisan bienes materiales".* [ITNCS]

interconectadas, p.ej. el uso de Internet y tecnologías basadas en las TCI para la vigilancia y control de proceso físicos vitales (también conocidos como sistemas ciberfísicos). Se trata de una base importante de las ICI.

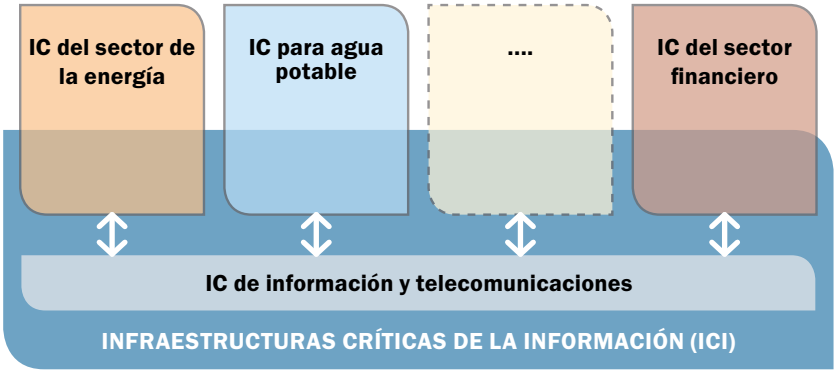


Figura 1. Relación entre infraestructuras críticas de la información e infraestructuras críticas.

Ciberseguridad y estrategias de ciberseguridad son conceptos que aparecen, la mayoría de las veces, en los medios de comunicación, documentos sobre políticas y planes de actuación cuando el tema tratado es el de las infraestructuras y las TCI. Estos conceptos desempeñan un papel respecto a las IC y la PICI, sin embargo, hay discrepancia (nacional) en cuanto a su interpretación. Para poder profundizar y hacer comparaciones, en la entrada "Cyber Security" del listado de la A a la Z en la página de inicio de [CIPedia©][3], pueden verse una gran variedad de definiciones nacionales sobre ciberseguridad. En esta guía se utilizará la siguiente definición [de la ITU]:

Ciberseguridad: *"Ciberseguridad es el conjunto de herramientas, políticas, conceptos sobre seguridad, medidas de seguridad, directrices, métodos sobre gestión de riesgos, medidas, formación, mejores prácticas, control y tecnologías que pueden utilizarse para proteger el ciberespacio y la organización, al igual que los recursos de los usuarios".*

La protección de infraestructuras criticas es un elemento vital de la ciberseguridad y es por ello que a menudo se escribe sobre el tema o se menciona al hablar de ciberseguridad, en particular, en lo relativo a estrategias nacionales de ciberseguridad y centros nacionales de ciberseguridad. Aunque el objetivo de los países es hacer frente a similares amenazas de seguridad cibernética, existe una gran diferencia en cuanto a sus métodos y puntos de vista. La primera diferencia que se observa entre las estrategias está en la definición y alcance. De hecho, solamente un 44 %, (menos de la mitad de los países) definen el concepto de ciberseguridad en sus estrategias, el resto, se basan en la explicación de un texto

3 CIPedia© es un punto de referencia internacional común para los conceptos y definiciones de PIC y PICI.

descriptivo (11 %) o en una definición de seguridad de información (11 %) o, incluso, ni llegan a definirlo (33 %). Los países que sí lo hacen, suelen tener maneras muy diferentes de entenderlo. Del mismo modo, también varía la forma en la que se creó el término.

Figura 2. Alcance y relación entre PIC, PICI y ciberseguridad.

La línea azul bajo los conceptos de la figura 2 refleja la variedad de estrategias nacionales de ciberseguridad que existe en el mundo. Algunas se han redactado sólo desde la perspectiva de la ciberdelincuencia o de la de Internet. Éstas tienden a no tener en cuenta ni la gestión (nacional) de las crisis y daños para las ICI ni el impacto entre sectores. Las estrategias escritas desde el punto de vista de la ciberseguridad, basadas en una evaluación de los riesgos nacionales, adoptarán una perspectiva más amplia en la que habrá cabida para la PIC y la PICI.

Adoptar un enfoque amplio para la estrategia nacional de ciberseguridad puede parecer un poco obvio, pero un estudio sobre PICI de 2016 realizado para Latinoamérica y el Caribe demostró lo contrario [Zaballos]. El estudio reveló que, en general, apenas se adoptaba legislación sobre CIP y que no existían ni estrategias ni normativas sobre PICI. En los casos en los que sí se encontraron iniciativas de protección de infraestructuras críticas de la información, éstas aparecían principalmente debido a situaciones de emergencia. Los países analizados sí contaban con planteamientos sobre IC e ICI, pero no se realizaban de forma sistemática y además presentaban carencias.

Así pues, la protección de infraestructuras críticas de información es un elemento esencial de la estrategias nacionales de ciberseguridad, pero no es lo mismo que la ciberseguridad y no incluye ni los ciberdelitos comunes, cuestiones sobre derechos humamos y privacidad, ni asuntos económicos del ciberespacio.

Por ejemplo, si fuera a presentarse un documento independiente sobre PICI, es probable que el enfoque tecnológico mostrara únicamente normas estándar sobre seguridad informática y principios sobre protección, directrices para la gestión de riesgos y algún tipo de plan para primeras respuestas en situaciones de emergencia. Ese tipo de documento no abarca puntos cruciales sobre gestión, legislación, actores implicados, incentivos, normativa y comunidades de IC/ICI.

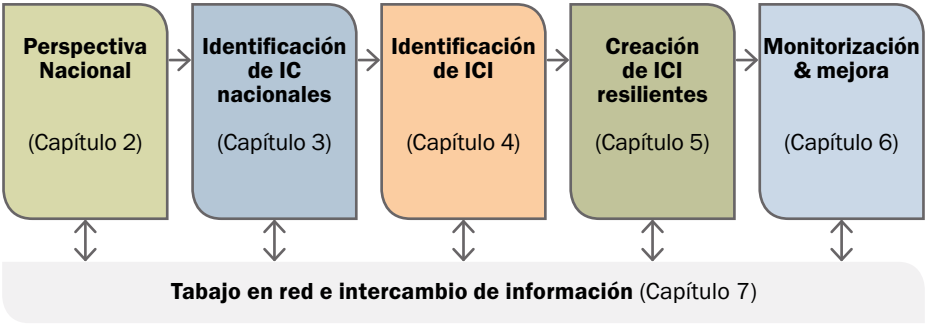


Figura 3. Esquema visual de esta guia.

1.4 CÓMO UTILIZAR ESTA GUÍA DE BUENAS PRÁCTICAS

La protección de las infraestructuras críticas de información es un proceso que sigue una serie de pasos importantes que están respaldados por una estrecha colaboración e interacción de todos los actores pertinentes. Los pasos mostrados en la figura 3 reflejan la estructura de esta guía de buenas prácticas. En el Capítulo 7 se describen los aspectos del trabajo en red y el intercambio de información, y las buenas prácticas a este respecto. Ambas medidas deben llevarse a cabo desde el principio. Cuanto antes se comience, más compromiso y colaboración se recibirá en etapas posteriores.

Sugerimos comenzar con la perspectiva nacional. ¿Cuál es el principal motivo para trabajar en la protección de infraestructuras críticas de información? ¿Qué peso tiene respecto a las otras políticas y temas políticos que aborda el país? Tal y como se describe en el Apartado 2.1.1, realizar una evaluación nacional y un análisis del perfil de riesgos puede servir de ayuda. Debido a que no se puede empezar a trabajar en la PICI sin saber cómo son las IC propias, en el Capítulo 3 se facilitan una serie de pasos y buenas prácticas, a modo de apoyo, al igual que material de referencia sobre identificación de infraestructuras críticas nacionales. Sólo es posible reconocer cuáles son las infraestructuras críticas de información propias, tras haber identificado las infraestructuras críticas. Se trata de una tarea compleja ya que las ICI abarcan dos ámbitos principales: por un lado el de las IC de las (tele)comunicaciones e información esenciales, y por otro lado el de la tecnologías de la información y comunicación en las que están incluidas las propias IC. El Capítulo 4, sobre la identificación de infraestructuras críticas de información, describe las medidas que deben adoptarse y las buenas prácticas al respecto. El siguiente paso es proteger de forma adecuada las ICI en función de los riesgos, tal como se expone en el Capítulo 5 sobre Desarrollo de la Protección de Infraestructuras Críticas de Información (PICI). El Capítulo 6 explica la necesidad de una mejora y control continuo siempre que sean necesarios; p. ej. debido a una revisión de la evaluación de riesgos o importantes cambios tecnológicos. Cada uno de estos capítulos incluye un apartado de buenas prácticas y otro sobre referencias bibliográficas y material de lectura complementario que se aconseja.

Esta guía se realiza con el objetivo de que los responsables de políticas sobre PICI en el gobierno tengan acceso a ella, independientemente de las diferencias que existan. Sin embargo, puede que sea necesario ajustar las prácticas idóneas aquí descritas a las necesidades de cada lugar.

Es más, no todas estas prácticas son adecuadas para ser aplicadas en todos los países. Al igual que el manual de buenas prácticas sobre PIC [de RECIPE], es el lector quien crea las políticas nacionales sobre PICI y los programas de actuación, desarrolla una colaboración con los actores pertinentes y fomenta actividades.

1.5 BIBLIOGRAFÍA Y MATERIAL DE LECTURA COMPLEMENTARIO

[Unión Africana] African Union, African Union Convention on Cyber Security and Personal Data Protection, LC12490, 27th June 2014. [Unión Africana. Convenio de la Unión Africana sobre Seguridad y Protección de Datos Personales, LC12490, 27 de junio 2014]- *Online:* http://pages.au.int/sites/default/

[Brasil] GUIA DE REFERÊNCIA PARA A SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS DA INFORMAÇÃO Versão 01 (Nov. 2010)/ Portaria Nº 34, de 5 de agosto de 2009. [Guía de Referencia para la Protección de Infraestructuras Críticas de Información] Conselho de Defesa Nacional, Secretaria Executiva, 2009. *Online:* http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf

[Bruno2002] S. Bruno and M. Dunn, Critical Information Infrastructure Protection: An Inventory of Protection Policies in Eight Countries [Protección de infraestructuras críticas de información: listado de políticas de protección en ocho países] ETH, Zürich, Switzerland, 2002. *Online:* http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP_Handbook_2002.pdf

[CIPedia©] CIPedia©: a common international reference point for CIP and CIIP concepts and definitions. [CIPedia©: punto de referencia internacional común para conceptos y definiciones de PIC y PICI] *Online:* http://www.cipedia.eu y https://publicwiki-01.fraunhofer. de/CIPedia/index.php/CIPedia%C2%A9_Main_Page

[CE2008] European Council, Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance) [Consejo Europeo, Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección (Texto pertinente a efectos del EEE)] *Online:* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008L0114

[G8] G8, G8 Principles for Protecting Critical Information Infrastructures, 2003 [G8 Principios para Proteger Infraestructuras críticas de información, 2003] *Online:* http://www.cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf

[GFCE] Global Forum on Cyber Expertise website, [Página Web del Foro Global sobre Ciberexperiencia] *Online:* https://www.thegfce.com

[ITNCS] Presidency of the Council of Ministers, National strategic framework for cyberspace security, Rome, Italy (December 2013) [Presidencia del Consejo de Ministros, Marco Estratégico Nacional sobre Ciberseguridad, Roma Italia (Diciembre 2013)] *Online:* https://www.enisa. europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf

[ITU] ITU Security in Telecommunications and Information Technology: An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications, ITU-T, Geneva (2012) - ITU-T X.1205 [Seguridad en Telecomunicaciones y Tecnología de la Información, ITU: sinopsis de cuestiones y aplicación de recomendaciones de ITU-T para telecomunicaciones seguras, ITU-T, Ginebra (2012) - ITU-T X.1205] *Online:* http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

[Luiijf2013] H.A.M. Luiijf, K. Besseling, P. de Graaf, Nineteen National Cyber Security Strategies, International Journal on Critical Infrastructures (IJCIS) [Diecinueve Estrategias Nacionales de Ciberseguridad, Revista Internacional sobre Infraestructuras Críticas], V9 N1/2, 2013, pp.3-31.

[Luiijf2015] H.A.M. Luiijf, B-J. te Paske, GCCS: Cyber Security of Industrial Control Systems, TNO, 2015. [GCCS: Ciberseguridad de Sistemas de Control Industrial] *Online:* http://publications.tno.nl/publication/34616507/KkrxeU/ luiijf-2015-cyber.pdf

[Meridian] Página Web de Meridian Process, https://www.meridianprocess.org

[OECD2007] OECD Working Party on Information Security and Privacy, Development of Policies for Protection of Critical Information Infrastructures: Ministerial Background Report DSTI/ICCP/REG(2007)20/FINAL, OECD, 2007. [Grupo de Trabajo sobre Seguridad de la Información y Privacidad, Creación de Políticas para la Protección de Infraestructuras Críticas: Informe del Ministerio sobre antecedentes DSTI/ICCP/REG(2007)20/FINAL, OECD, 2007]. *Online:* http://www.oecd.org/sti/40761118.pdf

[OECD2008] OECD ICCP Committee and the Working Party on Information Security and Privacy, OECD Recommendation on the Protection of Critical Information Infrastructures [C(2008)35], 2008, OECD. IICP (Comité de Política de la Información, la Informática y las Comunicaciones) de la OECD y Grupo de Trabajo sobre seguridad de la información y privacidad, Recomendación de la la OECD sobre protección de infraestructuras críticas de información [C(2008)35], 2008, OCDE] *Online:* http://www.oecd.org/sti/40825404.pdf

[RECIPE] M. Klaver, E. Luiijf, A. Nieuwenhuijs, Good Practices Manual for CIP Policies for policy makers in Europe, TNO, 2011 [Manual de buenas prácticas sobre políticas de PIC para legisladores europeos, TNO, 2011]. *Online:* http://www.tno.nl/recipereport

[UK] Cyber Security in the UK, Postnote Number 389, September 2011. [Ciberseguridad en RU, Postnote 389, Septiembre 2011 [Sic]] *Online:* http://www.parliament.uk/documents/post/postpn389_cyber-security-in-the-UK.pdf

[Victoria] Victorian Government CIO Council, Critical Information Infrastructure Risk Management, Victoria, Australia, 2012 [Consejería del Director de Información del Gobierno de Victoria, Gestión de Riesgos de Infraestructuras Críticas de Información, Victoria, Australia, 2012]. *Online:* http://www.digital.vic.gov.au/wp-content/uploads/2014/07/SEC-STD-02-Critical-Information-Infrastructure-Risk-Management1.pdf

[Zaballos2016] A.G. Zaballos and I. Jeun, Best Practices for Critical Information Infrastructure Protection (CIIP): Experiences from Latin America and the Caribbean and Selected Countries, 2016 [Mejores Prácticas para la Protección de Infraestructuras Críticas de Información (PICI): Experiencias de Latinoamérica y el Caribe, y de Países Seleccionados, 2016]. *Online:* https://publications.iadb.org/ handle/11319/7848

2 PERSPECTIVA NACIONAL

No existe una única estrategia sobre PICI que convenga a cada país. El tipo de proceso que necesita la PICI depende del perfil de riesgo que tenga esa nación y de la necesidad de mitigar los riesgos, al igual que de su competencia para afrontarlos. La habilidad y la responsabilidad de paliarlos depende tanto de la capacidad que tengan los actores implicados en la protección de estas infraestructuras, como la de cada país para hacer que las partes implicadas de las ICI trabajen conjuntamente para alcanzar unos niveles deseables de protección de infraestructuras críticas. Este modo de abordar la cuestión concuerda con los principios básicos establecidos para la PICI en [NISC.JP2014].

2.1 DESCRIPCIÓN GENERAL Y PRINCIPALES DESAFÍOS

2.1.1 CREAR UN PERFIL NACIONAL SOBRE RIESGOS DE FALLOS EN LAS IC/ICI

Para comenzar con la protección de las IC e ICI podría realizarse, en primer lugar, un perfil de riesgos para todo el país. El objetivo principal de éste es que a través de evaluaciones sistemáticas sobre las vulnerabilidades y amenazas que recibe un país (impacto y frecuencia), haya un conocimiento nacional y común sobre los factores de riesgos a los que se enfrenta esa nación.

El resultado que aporta una evaluación de riesgos es una visión general sobre los factores de riesgo y el impacto y frecuencia con la que pueden darse. Cada riesgo abordado en un estudio nacional de este tipo puede servir de base para un enfoque nacional integrado con el objetivo de prevenir, prepararse y responder ante éstos. Tener en cuenta los riesgos relacionados con las IC e ICI en estos estudios puede ayudar a crear un enfoque integral y equilibrado de gestión riesgos que se base en la protección de infraestructuras críticas de la información.

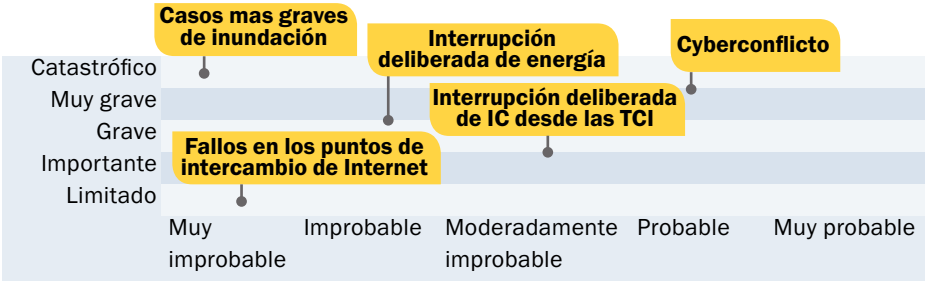


Figura 4. Ejemplo de perfil de riesgo (Fuente: [NLNRA2014]).

La evaluación sistemática de las amenazas supone que todas ellas se analizan utilizando el mismo método y basándose en su impacto y probabilidad de que ocurran. Cuando se evalúan los peligros actuales, tanto los intencionados como los fortuitos, no sólo hay que tener en cuenta los cambios en las amenazas y sus impactos, sino también el hecho de que pueden darse cambios climáticos y acontecimientos geopolíticos.

Realizar un análisis nacional de riesgos específico para las IC y las ICI es una tarea compleja para la cual se facilitan una serie de directrices en el Apartado 2.2.1. Recomendamos especialmente que las partes interesadas se impliquen desde el principio de este estudio, ya que la evaluación de riesgos no es un proceso simplemente racional y es de suma importancia que éstos den su visto bueno. En la práctica, los países que llevan a cabo este tipo de análisis por primera vez pueden plantearse concentrarse en los escenarios que plantean mayores riesgos e incluir otros en una segunda o posteriores fases.

Tabla 1. Lista no exhaustiva de actores implicados en las ICI.

- Ministerios encargados de la coordinación de PICI, p. ej. Interior, Justicia, Defensa, Gabinete de la presidencia
- Ministerios responsables de TCI, p. ej. Comunicaciones, Medios de Comunicación, departamentos encargados de TCI
- Ministerios responsables de IC específicas, p.ej. Economía, Energía, departamentos de Sanidad
- Responsables de ámbitos particulares de las IC
- Fuerzas del orden y otros organismos públicos
- Operadores / empresas de IC e ICI
- Políticos y Parlamento
- Fabricantes, integradores de Sistema y compañías de mantenimiento (terceros)
- Organizaciones multisectoriales (sucursal)
- Equipos de respuesta a incidentes de seguridad informática (CSIRT)
- Centros nacionales de ciberseguridad
- Mundo académico, investigación y desarrollo (“Triple hélice”)

2.1.2 IDENTIFICAR A LAS PARTES IMPLICADAS

Proteger las infraestructuras críticas e infraestructuras críticas de información exige que se tenga una visión sobre su gestión y estructura de participación en ellas, y que se conozca el tipo de actores que están implicados (véase el recuadro). Esto supone que haya que categorizar a las partes implicadas como públicas, semipúblicas o privadas, y como actores que funcionan en el ámbito regional, nacional o internacional. Existen muchos métodos y herramientas disponibles para que las partes implicadas lleven a cabo el análisis, p. ej. [Mitchell1997] y [Yang2011], pero la realización de un estudio sencillo es suficiente para hacerse una idea general sobre el tipo de actores involucrados.

Tabla 2. Tabla de ayuda para el análisis de actores participantes (algunos ejemplos).

	Público	**Semipúblico**	**Privado**
Internacional	OECD		Vendedor multinacional de software, fabricante de SCADA
Nacional	Empresa municipal	Servicio nacional de transporte de gas	Proveedor de telefonía; proveedor de servicio de Internet; intercambio
Regional	Control de tráfico aéreo	Servicios de practicaje costero	Intercambio por internet

2.1.3 DEFINIR LAS OPCIONES DE POLÍTICAS DE ACTUACIÓN

Las autoridades de los países pueden contemplar un amplio conjunto de directrices para llevar a cabo la PICI. Las opciones sobre qué principios son los adecuados para el propósito depende de muchos factores, incluido el tipo de amenaza al que se enfrenta un país y las ICI, el tipo de actores implicados en la protección de éstas, y la historia y cultura política estatal del país. Las opciones para las políticas de actuación son las siguientes:

- Autoregulación;
- Cumplimiento voluntario;
- Programas gubernamentales voluntarios;
- Incentivos y mecanismos comerciales;
- Marcos jurídicos y normativos.

El hecho de que un país utilice programas voluntarios, incentivos (incentivos y sanciones) o marcos jurídicos y normativos depende del tipo de actores implicados en las ICI, su cultura, prácticas establecidas y objetivos y ambiciones respecto a la PICI. Muchos han optado por un planteamiento de riesgos y responsabilidades que establezca las bases para la protección de las infraestructuras críticas de información y deje los detalles sobre la protección de las ICI a operadores de IC/ICI tecnológicamente más avanzados. Cuando las multinacionales se encargan de parte(s) de las ICI, se deben tener en cuenta los acuerdos que éstas hayan hecho con otras naciones.

Los países deberían darse cuenta de que en los casos en los que una multinacional gestiona parte(s) de las ICC surgen tanto oportunidades como retos específicos. Por un lado, las naciones pueden beneficiarse de la experiencia sobre PICI que las multinacionales han adquirido en otros lugares, pero por otro lado, puede resultar más complicado hacer que éstas cambien las actividades que llevan a cabo en un país debido a los acuerdos que han firmado con otros y esto implique tener que recurrir a la cooperación transfronteriza y a medidas internas uniformes.

Figura 5. Riesgo de las ICI dentro del riesgo nacional.

Para responder a estos retos, en el próximo apartado se describen las siguientes buenas prácticas:

- Creación de un perfil nacional de riesgos.
- Retos de las ICI para los países desarrollados.
- Creación de asociaciones público-privadas como opción de política de actuación.
- Adopción de un enfoque interinstitucional y comienzo de intercambios de información.

2.2 BUENAS PRÁCTICAS PARA LA PERSPECTIVA NACIONAL

2.2.1 BUENAS PRÁCTICAS: CREACIÓN DE UN PERFIL NACIONAL DE RIESGOS

La creación de políticas de actuación efectivas para la PICI comienza con la elaboración de un perfil nacional sobre riesgos y la toma de conciencia sobre las consecuencias que tendría un fallo en las IC y las ICI. Es por ello, que recomendamos realizar un análisis en el que se incluya el riesgo de avería de ambas infraestructuras. Elaborar este perfil es una tarea sumamente importante pero también compleja, y los detalles sobre los procesos que se necesitan para ello quedan fuera del ámbito de esta guía de buenas prácticas, por lo que no podrán incluirse. Las políticas de actuación para evaluar la capacidad de gestión de riesgos [CE 2015] pueden servir de ayuda a las autoridades nacionales que pretendan elaborar el perfil. El objetivo de esta guía es ofrecer a los países una metodología exhaustiva y flexible que haga que se entienda cuáles son los elementos necesarios para hacer una evaluación y un perfil nacional sobre riesgos, y se decida qué abarcan sus IC e ICI.

Entre las directrices de la UE se encuentran cuestiones como: la elección de un marco de evaluación de riesgos, implicación de los actores y expertos adecuados, aplicación de la metodología correcta y herramientas de las TCI y, planificación y financiación de la evaluación de riesgos. Para cada una de ellas, se facilita información que ayuda a desarrollar la capacidad de gestión de riesgos. También recomendamos el informe de análisis de evaluaciones nacionales sobre riesgos de ENISA que recoge directrices y buenas prácticas para elaborar un perfil nacional sobre riesgos [ENISA2013].

La evaluación nacional de riesgos de 2015 de Finlandia [Finlandia2015] ofrece un ejemplo sobre cómo incluir un fallo de las IC y las ICI en un perfil nacional de riesgos, y hace una distinción entre una gran variedad de sucesos que tienen repercusiones en la sociedad e incidentes regionales graves. Los fallos en las ICI se clasifican como factores de riesgo en el ámbito informático, que, a su vez, se encuentran dentro de la gran variedad de sucesos que afectan a la sociedad. La Autoridad Nacional de Regulación (NRA, según sus siglas en inglés) describe cómo los fallos en las ICI provocan daños en las IC y en sistemas vitales para la sociedad que pueden traducirse en daños materiales y pérdidas de vidas. Otras evaluaciones sobre riesgos nacionales son: [Cabinet2010], [DSB02014], [NLNRA2009] y [MSB2012].

2.2.2 BUENAS PRÁCTICAS: LOS RETOS DE LAS ICI PARA LOS PAÍSES EN VÍAS DE DESARROLLO

Durante los talleres organizados por la Organización de Telecomunicaciones de la Commonwealth sobre la PICI en 2015, se hizo referencia a una serie de retos:

1. Coste y falta de inversión financiera: los fondos necesarios para crear un marco estratégico para proteger las infraestructuras críticas de la información pueden ser un obstáculo, al igual que la limitación de recursos humanos e institucionales.
2. Complejidad técnica a la hora de llevar a cabo la protección para las infraestructuras críticas de información: es necesario conocer las dependencias y vulnerabilidades *(El Apartado 3.2.3 de este documento puede servir de ayuda).*
3. Conocimientos limitados a la hora de identificar y clasificar las IC: es necesario tener en cuenta la importancia de la función que desempeñan, la población a la que afecta y la dependencia técnica *(El Capítulo 3 de este documento puede servir de ayuda).*
4. Educar sobre seguridad informática y realizar un replanteamiento cultural: es necesario concienciar sobre la importancia de la ciberseguridad y la PICI, y crear una cultura sobre seguridad informática que favorezca la confianza.
5. Falta de estrategias, políticas y marco pertinentes para la PICI *(estas buenas prácticas y sus referencias pueden servir de ayuda).*
6. Falta de intercambio de información y conocimientos *(el Capítulo 7 y [Luiijf2015] pueden ser útiles).*

Cuando se trabaja en la protección nacional de infraestructuras críticas de la información, se deben tener en cuenta, cómo mínimo, los retos que suponen las ICI y las lecciones aprendidas. Si las IC y las ICC de un país han sido privatizadas, los retos que pudieran surgir (como los mencionados anteriormente) pueden gestionarse trabajando con socios privados y estableciendo una colaboración público-privada (CPP), como se verá en el próximo apartado y en el Capítulo 7.

2.2.3 BUENAS PRÁCTICAS: ESTABLECER UNA COLABORACIÓN PUBLICO-PRIVADA COMO OPCIÓN DE POLÍTICA DE ACTUACIÓN

La protección de las IC/ICI forma parte de la seguridad nacional de muchos países, pero la mayoría de las decisiones relacionadas con la seguridad informática las toman los operadores de las ICI. Para asegurarse de que todas las partes implicadas en las infraestructuras críticas de la información tienen en cuenta, a la hora de tomar decisiones, el riesgo que supone para la seguridad nacional un posible fallo en éstas, suele ser necesario que las autoridades nacionales y los operadores de las ICI colaboren entre ellos. Cuando las infraestructuras críticas de la información estén operadas por el sector privado puede que, además, sea necesario establecer también una cooperación público-privada (CPP). Con ello nos referimos a *la colaboración entre un organismo gubernamental y entidades privadas con el objetivo (en el caso de la PIC/PICI) de garantizar el correcto funcionamiento de los servicios de las ICI.* Ésta se basa en la mentalidad con la que uno enfoca la relación, las responsabilidades y la cooperación con los actores implicados, independientemente de que éstos sean públicos o privados. Este mismo planteamiento puede utilizarse también cuando las IC e ICI están operadas por entidades públicas.

Cuando las ICI de un país pertenecen o están gestionadas de forma privada, es importante que los operadores públicos, semipúblicos y privados trabajen conjuntamente de forma coordinada para protegerlas. Se debe tener en cuenta que para la protección de infraestructuras críticas de la información, la idea de una colaboración público-privada puede implicar mucho más que delegar funciones públicas a los actores privados.
El concepto de colaboración, en su sentido más amplio, incluye una puesta en común de recursos, apoyo mutuo y toma de decisiones conjunta. No supone solo externalizar proyectos, sino también contar con redes de colaboración entre organizaciones.
Los detalles de esta colaboración y las buenas prácticas se analizan en el Capítulo 7.

Para que los actores privados se impliquen, el gobierno puede ofrecer a las partes públicas y privadas información fiable facilitada por expertos en el ámbito de infraestructuras y PIC/PICI. El valor añadido que ofrecen los socios privados radica en que el gobierno, de forma individual, visita muchas empresas y con ello se hace una idea general sobre cómo uno o varios sectores implicados en las infraestructuras tratan el tema de la protección Cuando se combina una visión global de la seguridad informática con información sobre amenazas facilitada por servicio de inteligencia, esto puede convertirse en información operativa con la que trabajar. En este sentido, el gobierno puede ser en un valioso colaborador de los operadores de las IC.

2.2.4 BUENAS PRÁCTICAS: ADOPCIÓN DE UN ENFOQUE REALIZADO POR MÚLTIPLES ENTIDADES E INTERCAMBIO DE INFORMACIÓN

Abordar los posibles riesgos de las ICI y la complejidad asociada que conlleva la PICI, requiere, efectivamente, que el gobierno cuente con un enfoque realizado por múltiples entidades tanto para el ámbito estratégico, como táctico y operativo/técnico. Las partes implicadas como los ministerios (p.ej. el ministerio de Comunicaciones, Tecnologías de la Información, Economía, Seguridad, Justicia, Defensa y la Oficina del Gabinete del Gobierno) organismos regionales públicos, organismos o entidades reguladoras deben colaborar en todos los retos: estratégicos, tácticos y operativos/técnicos. Es importante que, en primer lugar, se cree un marco óptimo con todos los actores públicos para abordar, desde el punto de vista estratégico, los retos que presentan las IC y la PICI. Este puede conseguirse a través de mesas redondas que se celebren de forma regular. Lo ideal sería que a partir de los objetivos estratégicos surgieran otros requisitos como: mandatos judiciales, una organización y gestión estructuradas, y una colaboración en el ámbito táctico y operativo/técnico.

Para el aspecto táctico y operativo, se debería considerar la posibilidad de cooperar con fuerzas policiales que trabajan en el sector de la IC y la informática, y con servicios que se dedican a la seguridad nacional y la defensa. Para la parte técnica, será normalmente un equipo nacional de respuesta para emergencias de seguridad informática quien desempeñe un papel en la PICI (véase Apartado 5.2.2).

Incluso cuando se designen ciertos organismos públicos para identificar las IC, las ICI y los procesos de la PICI (y, por lo tanto, se conviertan en sus responsables), se debe ser

consciente de que puede que también haya otros actores públicos implicados directa o indirectamente en la planificación y ejecución de la protección. Tras una primera coordinación entre todas las partes públicas interesadas, los operadores de las ICI y otros actores clave de la industria privada, de las cámaras de comercio, del mundo académico, de la investigación y del desarrollo, etc., estos deben reunirse para abordar conjuntamente los retos que implica proteger las infraestructuras críticas de información.
Los organismos públicos pueden promover o facilitar el intercambio de información entre los actores de la PICI [Luiijf2015]. Si se establecen unas condiciones favorables para esto, organizaciones públicas y privadas como: organismos gubernamentales encargados de la seguridad, operadores de las ICI, fabricantes clave, integradores de sistemas y terceros encargados del mantenimiento, podrían comenzar a intercambiarse información sobre la protección de infraestructuras. Puede que la participación de actores públicos afecte a los privados en su disposición a la hora de compartir información. El Capítulo 7 sobre trabajo en red e intercambio de información está dedicado a la creación de redes de colaboración y el intercambio de información.

2.3 BIBLIOGRAFÍA Y MATERIAL DE LECTURA COMPLEMENTARIO

[Cabinet2010] Cabinet Office, Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure from Natural Hazards, March 2010 [Oficina del Gabinete del Gobierno, Marco Estratégico y Política para Mejorar la Capacidad de Recuperación de Infraestructuras Críticas tras Desastres Naturales, marzo 2010] *Online:* https://www.gov.uk/government/uploads/system/uploads/attachment_data/ file/62504/strategic-framework.pdf

[CTO] Commonwealth Telecommunication Organisation, Critical Information Infrastructure Protection (CIIP) workshops, 2015 [Organización de Telecomunicaciones de la Commonwealth, Talleres sobre Protección de infraestructuras críticas de información (PICI), 2015] *Online:* http://www.slideshare. net/CandiceTang1/cto-ciipgaborone-workshoppresentationfinal18mar2015com pressed

[Dinamarca2013] Danish Emergency Management Agency, National Risk Profile (NRP), April 2013 [Agencia Danesa para la Gestión de Emergencias, Perfil Nacional sobre Riesgos, Abril 2013] *Online:* https://brs.dk/viden/publikationer/Documents/National_Risk_Profile_ (NRP)_-_English-language_version.pdf

[DSB2014] National Risk Analysis 2014: Disasters that may affect Norwegian Society, Norwegian Directorate for Civil Protection (DSB), 2014 [Análisis Nacional de 2014 sobre Riesgos. Desastres que podrían afectar a la sociedad Noruega, Dirección de la Protección Civil de Noruega, 2014] *Online:* https://www.dsb.no/globalassets/dokumenter/rapporter/nrb_2014_english.pdf

[CE2015] European Commission, Commission Notice: Risk Management Capability Assessment Guidelines (2015/C 261/03) [Comisión Europea, Nota de la Comisión: Directrices de Evaluación de la Capacidad de Gestión de Riesgos (2015/C 261/03)] *Online:* http://eur-lex.europa.eu/ legal-content/EN/TXT/PDF/?uri=CELEX:52015XC0808(01)

[ENISA2013] ENISA, National-level Risk Assessments: An analysis report (2013). [ENISA, Evaluaciones de Riesgos en el Ámbito Nacional: Informe de análisis (2013)] *Online:* https://www.enisa.europa.eu/publications/nlra-analysis-report

[Finlandia2015] Ministry of the Interior, Finland, National Risk Assessment 2015, Ministry of the Interior Publication 4/2016 [Ministerio del Interior, Finlandia, Evaluación Nacional de Riesgos de 2015, Publicación 4/2016 del Ministerio del Interior] *Online:* https://www.intermin.fi/download/65647_ julkaisu_042016.pdf

[Klimburg2012] Klimburg, National Cyber Security Framework Manual, NATO CCD-COE Publications, December 2012 [Manual de Referencia sobre Ciberseguridad Nacional, Publicaciones del CCD-COE de la OTAN, Diciembre 2012] *Online:* https:// ccdcoe.org/publications/books/- NationalCyberSecurityFrameworkManual.pdf

[Luiijf2015] Luiijf, H.A.M., Kernkamp, A., GCCS: Sharing Cyber Security Information, TNO, 2015 [GCCS: Intercambio de Información sobre Ciberseguridad, TNO, 2015] *Online:* http://publications.tno.nl/publication/34616508/oLyfG9/luiijf- 2015-sharing.pdf

[Mitchel1997] Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a theory of stakeholder identification and salience: Defining the principle of who and what really counts. Academy of management review, 22(4), 853-886 [Hacia una teoría de la identificación y relevancia de los actores implicados. Definir el principio de quién y qué es lo que realmente importa. *Academy of management review;* 22(4), 853-886].

[MSB2012] Swedish National Risk Assessment 2012, Swedish Civil Contingencies Agency (MSB), Sweden, 2012. [Evaluación de Suecia de 2012 sobre Riesgos Nacionales, Agencia Sueca para Contingencias Civiles (MSB), Suecia 2012] *Online:* https:// www.msb.se/RibData/Filer/pdf/26621.pdf

[NISC.JP2014] The Basic Policy of Critical Information Infrastructure Protection (3rd Edition) – tentative translation, Japan, 2014 [Política Básica para Protección de infraestructuras críticas de información (3ra Edición) – Traducción provisional, Japón, 2014]. *Online:* http://www.nisc.go.jp/eng/pdf/ actionplan_ci_eng_v3.pdf

[NLNRA2009] Ministry of the Interior and Kingdom Relations, Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherlands, The Hague, The Netherlands, October 2009 [Ministerio del Interior y Relaciones del Reino, Trabajar con escenarios, evaluación de riesgos y capacidad de actuación para la seguridad nacional y estrategia de seguridad de los Países Bajos, La Haya, Países Bajos, Octubre 2009] *Online:* http://www. preventionweb.net/files/26422_guidancemethodologynationalsafetyan.pdf

[NLNRA2014] Analistennetwerk Nationale Veiligheid, M. G. Mennen (ed), Nationale Risico-beoordeling 6, Rijksinstituut voor Volksgezondheid en Milieu (RIVM), 2014. *Online:* https://www.nctv.nl/binaries/nat.risicobeoordeling-6-definitief_ tcm31-32706.pdf

[Yang2011] Yang, J., Shen, G. Q., Bourne, L., Ho, C. M. F., & Xue, X. (2011). A typology of operational approaches for stakeholder analysis and engagement. Construction management and economics, 29(2), 145-162 [Tipología de enfoques operativos para la participación y análisis de los actores implicados. Gestión de la construcción y economía, 29(2), 145-162].

3 IDENTIFICACIÓN DE LAS INFRAESTRUCTURAS NACIONALES CRÍTICAS

3.1 DESCRIPCIÓN GENERAL Y PRINCIPALES RETOS

3.1.1 NECESIDAD DE INFENTIFICAR LAS IC

Cuando se compara el conjunto de sectores incluidos en las infraestructuras críticas de diferentes países, se puede observar que existen puntos comunes, pero también grandes diferencias. Una infraestructura en particular puede ser de vital importancia para un país y no así para otro. Así pues, las opiniones sobre lo que se considera que debería incluirse en las infraestructuras críticas varían dependiendo del país. En [PSC2014] puede verse un claro ejemplo, una comparativa de diferencias y algunos debates sobre el tema entre varios países: *"[…] ha habido importantes cambios en la seguridad mundial que han hecho que cada uno de los miembros haya adoptado por nuevas formas para abordar la seguridad de las infraestructuras y la capacidad de recuperación".* [Mattioli2015; tabla 1] llegó a la misma conclusión cuando comparó los sectores que se incluían en las IC de 17 países de la UE.

De la definición de infraestructuras críticas del Apartado 1.3 queda claro que los países tienen la responsabilidad de identificar sus infraestructuras y tomar las medidas necesarias para protegerlas correctamente. Además, la presión para llevar a cabo esta protección, puede llegar de diferentes partes. Desde un punto de vista internacional, iniciativas regionales y grupos de naciones (p.ej. la Unión Africana (UA), la Organización de los Estados Americanos (OEA)), proveedores de ICI (p.ej. la Organización de Telecomunicaciones del Commonwealth (OTC) y organizaciones internacionales (el Banco Mundial, el G8, la ITU, la OTAN, la OCDE) pueden recomendar a los países, incluso presionarles para que presten (más) atención tanto a las infraestructuras críticas como a las infraestructuras críticas de la información. La necesidad de trabajar en su protección puede llegar también a través de evaluaciones de riesgo (véase Apartado 2.1.1) que hacen que un país sea consciente de la importancia que tienen las infraestructuras e infraestructuras de información y el riesgo que corren. También puede suceder que de forma inesperada llegue a comprender el papel tan fundamental que tienen. Una infraestructura puede comenzar a funcionar mal repentinamente y sufrir a continuación una avería, provocando serias repercusiones en la sociedad y/o economía. Este tipo de situaciones imprevistas podría hacer que los actores públicos y privados consideraran o reconsideraran el carácter vital de esa infraestructura.

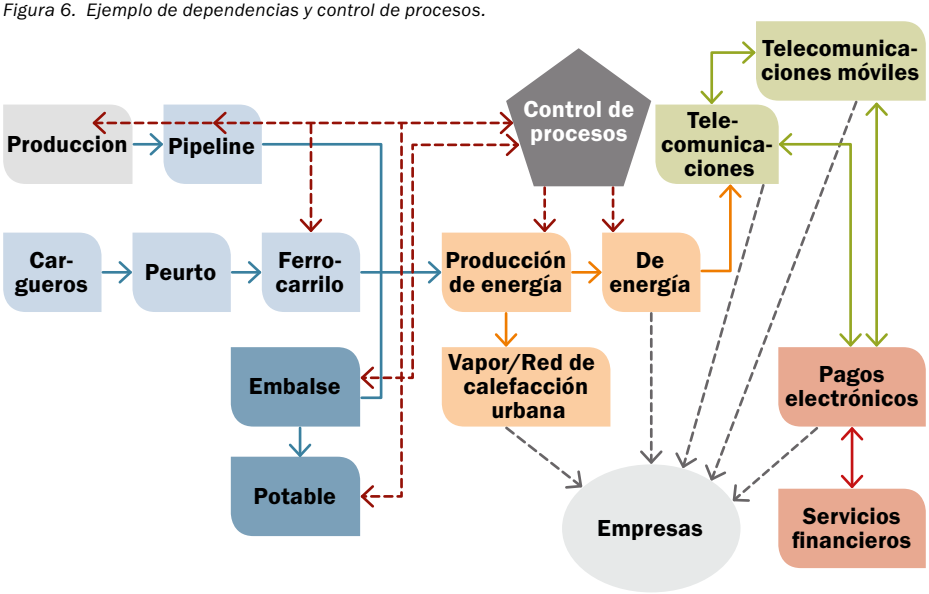
Tradicionalmente, es el gobierno, organismos públicos, países/provincias o ciudades quienes han estado a cargo del funcionamiento de infraestructuras críticas como: el suministro eléctrico, suministro de gas, los servicios postales y de telecomunicaciones. En numerosos países muchos de los servicios de estas infraestructuras fueron liberalizados y privatizados, lo que hizo que en la actualidad, muchas organizaciones privadas y semipúblicas sean las responsables, gestionen las "empresas" y ofrezcan sus servicios para infraestructuras.

Con estas privatizaciones, la seguridad y garantía del suministro de estos servicios recae, en gran medida, en la industria semipública y privada.

El primer paso para proteger estas infraestructuras es identificar las infraestructuras críticas nacionales. Cada país tiene ideas diferentes sobre lo que es vital para él. Es por ello, que esta guía de buenas prácticas no ofrece cifras o indicaciones estrictas, sino una visión general sobre las posibilidades que existen para abordar el proceso de protección.

Independientemente de la estructura de gestión que exista en el país y la variedad de directrices que se pueden adoptar, es importante que las autoridades públicas, los operadores semipúblicos y privados de infraestructuras se impliquen desde el principio. El tipo de gestión que exista para las infraestructuras influirá en el proceso de identificación de las IC. Véase [RECIPE] y el Apartado 3.1.2: “Comenzar identificando sectores de IC”.

Figura 6. Ejemplo de dependencias y control de procesos.



3.1.2 COMENZAR IDENTIFICANDO SECTORES DE IC

Los operadores públicos, semipúblicos y privados de IC ofrecen bienes y servicios. El tipo de bienes y servicios, y el uso que los consumidores hacen de éstos es lo que determina si un servicio de una infraestructura es vital o no. La tabla 3 ofrece ejemplos de sectores de IC y sus servicios. En la entrada ‘Critical Infrastructure Sector’ del listado de la A a la Z en la página de inicio de [CIPedia©] y en [Mattioli2015; tabla 1] se pueden ver más ejemplos de servicios vitales.

Tabla 3. Ejemplos de sectores y servicios de IC.

Sector	Servicios
Comunicaciones	Fija, móvil, comunicaciones por satélite, por navegación
Energía	Electricidad, petróleo, gas, red de calefacción urbana
Sanidad	Hospitales, sector médico
Transporte	Aéreo, ferroviario, por carretera, fluvial, oceánico y marítimo, y puertario
Agua	Agua potable, aguas residuales/alcantarillado
...	

Los planteamientos establecidos por otros países pueden utilizarse para identificar las infraestructuras críticas propias, aunque también pueden usarse otros menos extensos. A continuación se muestran brevemente tres planteamientos que se describirán más adelante en las buenas prácticas en el Apartado 3.2.2:

1. El planteamiento ascendente consiste en ver qué conjunto de sectores y servicios han sido definidos como críticos por otros países. Se puede comenzar analizando otras naciones que tienen una estructura social, geográfica y de desarrollo tecnológico similar (véase Apartado 3.2.1). Con esto, se obtiene una lista de operadores de infraestructuras de estos servicios. Partiendo de las repercusiones evitables que aparecen en la definición de IC, el siguiente paso sería definir en qué consiste el "carácter crítico" de esas infraestructuras identificadas como potencialmente claves.
   Al aplicar este criterio de "carácter crítico" a todos los actores, sectores y servicios, se habrá cubierto el 80-90% del conjunto de sectores y servicios de las IC. Es importante señalar que cuando un sector se califica como infraestructura crítica, no implica que todos los servicios subyacentes también lo sean. Por ejemplo, en el sector de la energía, un servicio de calefacción urbana (por red) no tiene por qué clasificarse como crítico en el ámbito nacional, mientras que el suministro de corriente eléctrica sí lo es. Tras haber alcanzado el 80/90%, existen dos alternativas. La primera es comenzar identificando las ICI (Capítulo 5). La otra, es identificar a los actores pertinentes, como los operadores de las IC, dentro de este grupo provisional de sectores de IC y servicios de IC que se ha establecido (véase Capítulo 7). Tras esto, se debe redefinir, en equipo, este grupo de sectores y servicios críticos analizando la dependencia que existe de las IC (Apartado 3.2.3).
2. Un segundo planteamiento consiste en realizar un estudio analítico utilizando una metodología que contenga unos criterios sencillos y/o métodos. Otros países ya han evaluado su conjunto de IC [CIPedia©]. Es probable que los estudios llevados a cabo y los métodos utilizados no se puedan aplicar directamente sin tener en cuenta las diferencias y especificidades nacionales. Sin embargo, son una excelente fuente de información útil sobre la variedad de enfoques que existen para identificar las infraestructuras críticas y que uno puede utilizar para analizar las suyas propias.
3. El tercer planteamiento es definir, en primer lugar, los métodos detallados, lo que requiere más madurez en la evaluación de la CIP. Tras esto, y utilizando el método explicado en las Buenas Prácticas 3.2.2., se podrá establecer si una infraestructura o servicio de infraestructura debería considerarse crítica o no. Debe indicarse que varios países ya han probado este enfoque y han visto que establecer un método no es una tarea sencilla.

3.2 BUENAS PRÁCTICAS PARA IDENTIFICAR LAS INFRAESTRUCTURAS NACIONALES CRÍTICAS

Este apartado ofrece una serie de prácticas adecuadas para identificar sectores y servicios de las IC:

- adoptar las definiciones realizadas por otros países sobre sectores y servicios de IC;
- adoptar una metodología para identificar sectores y servicios de IC de modo sistemático;
- llevar a cabo un análisis sobre la dependencia que existe (para el ámbito nacional e internacional).

3.2.1 BUENAS PRÁCTICAS: ADOPTAR LAS DEFINICIONES DE OTROS PAÍSES SOBRE SECTORES Y SERVICIOS DE IC

Las definiciones de otros países pueden ser útiles para tomar ideas, pero no se pueden transferir directamente. Comparar las definiciones que todos los países han dado para las IC (enumeradas en la entrada "Infraestructuras críticas" en el listado de la A a la Z en la página de inicio de [CIPedia©]) puede ayudar a que las naciones empiecen a dar forma a su propia definición, preferiblemente, una que se parezca a otra que ya exista. Los países que comiencen a analizar su infraestructura crítica identificarán también diferentes sectores y servicios vitales. Independientemente de la variedad, el objetivo es el mismo: las IC e ICI de un país deben seguir funcionando sin problema alguno tanto tiempo como sea posible.

Para establecer un conjunto inicial de sectores y servicios de IC, pueden tomarse ideas de otros países. En la entrada "Sector de infraestructuras críticas", en el listado de la A a la Z de la página de inicio de [CIPedia©], se enumeran los sectores críticos y, en un par de casos, también los servicios críticos.

3.2.2 BUENAS PRÁCTICAS: ADOPTAR UNA METODOLOGÍA PARA IDENTIFICAR SISTEMÁTICAMENTE SECTORES Y SERVICIOS

¿Cómo enfocar la identificación de los sectores y servicios de IC? A continuación se explican los cuatro puntos de partida básicos indicados en [RECIPE2011] que ofrecen un planteamiento estructurado para llevar a cabo esta identificación. Los pasos se basan en la Directiva sobre las infraestructuras críticas europeas [CE2008] que, de modo ascendente, parte de un sector que podría ser crítico:

1. Aplicar criterios específicos de sectores;
2. Valorar el carácter crítico;
3. Evaluar la dependencia;
4. Aplicar criterios communes.

El orden más útil a seguir en estos criterios depende de la información de la que dispongan los legisladores del país. En algunos casos es posible comenzar fijando y aplicando criterios comunes, seguir con el estudio de la dependencia y la evaluación sobre el carácter crítico, y finalizar aplicando criterios específicos de sectores.

Aplicar criterios específicos de sectores

Se puede llevar a cabo una primera selección de IC y servicios de IC basándose en criterios específicos de sectores. Estos pueden ser: la participación en el mercado, la capacidad de transporte (p.ej. m^3 de flujo de gas por segundo, funcionamiento de una IC que supone un punto único de fallo), conectividad transfronteriza (importación y/o exportación), suministro de servicios vitales al gobierno, la industria o la población. Con este primer paso se obtiene una pequeña lista de IC de un sector particular. También permite restringir el número de posibles operadores de IC en los casos en los que haya múltiples. Hay que tener en cuenta que algunos países pueden considerar estos criterios específicos de sectores como información confidencial ya que pueden revelar algún tipo de dependencia, vulnerabilidad y cuestiones delicadas. De aquí, surge una pequeña lista de IC a partir de la cual se deberá seguir reflexionando. Este método favorece claramente que los criterios que se establecen sean cuantificables y objetivos más que cualitativos y subjetivos.

Tabla 4. Ejemplo: Escala del carácter crítico para infraestructura nacional [Cabinet2010].

Descripción de la escala que valora el carácter crítico	
Cat. 5	Infraestructuras cuya pérdida tendría repercusiones catastróficas para RU. La pérdida de estos bienes, de importancia nacional única, tendría unos efectos nacionales a largo plazo y podría repercutir en una serie de sectores. Se considera que son pocas las infraestructuras que cumplen con los criterios de la Cat 5.
Cat. 4	En esta categoría deberían encontrarse las infraestructuras de mayor importancia para los sectores. Su pérdida se traduciría en una grave repercusión en servicios esenciales y podría afectar a la prestación de servicios vitales para todo RU o millones de ciudadanos.
Cat. 3	Infraestructuras de gran importancia para los sectores y la prestación de servicios esenciales cuya pérdida podría afectar a una amplia región geográfica o varios cientos de miles de personas.
Cat. 2	Infraestructuras cuya pérdida repercutiría de forma importante en la prestación de servicios esenciales y que implicaría la desaparición o interrupción del servicio para decenas de miles de personas o afectaría a países enteros o equivalentes.
Cat. 1	Infraestructuras cuya pérdida podría interrumpir moderadamente la prestación de servicios, muy probablemente de forma localizada, y que afectaría a miles de ciudadanos.
Cat. 0	Infraestructuras cuya desaparición tendría repercusiones menores (en el ámbito nacional).

Valorar el carácter crítico

El segundo paso es evaluar el carácter vital de la lista obtenida en el paso anterior basándose en la definición de IC que tiene un país. Esto requiere tener unos conocimientos sobre los bienes y servicios específicos que ofrece un sector y saber qué o quién es el responsable. Para el sector de la energía, por ejemplo, puede que el carácter crítico sólo esté en el abastecimiento de electricidad y gas. Dentro del sector de las tecnologías de la información y la comunicación, puede que un país considere que un servicio crítico es la disponibilidad de su número de emergía nacional, aunque este tipo de servicio pertenezca al sector de las telecomunicaciones. Es por ello que es importante hacer hincapié en que es posible adoptar ejemplos de los primeros pasos de otros países para identificar sectores y servicios, pero que también entran en juego las diferencias e interpretaciones sobre el carácter crítico.

Evaluar la dependencia

El tercer paso es identificar las dependencias de las IC. Las (inter)dependencias se definen del siguiente modo:

- **Dependencia** es *"la relación que existe entre dos productos o servicios y en la cual se necesita un producto o servicio para que se cree otro producto o servicio".*
- **Interdependencia** es *"la dependencia mutua de productos y servicios".* [Luiijf2009]

Los sectores de IC y sus servicios vitales dependen de otros sectores de IC y sus servicios críticos. Los datos empíricos muestran que la interdependencia entre sectores y servicios es algo que rara vez se da [VEeten2011]. Esto significa que la dependencia entre ellos nunca ha sido algo vital y, por lo tanto, los países no han sufrido nunca problemas serios.

Lo más práctico es identificar las dependencias vitales que existen y que pueden hacer que los servicios sufran cortes en cascada. Es más, estas dependencias pueden cambiar significativamente cuando del funcionamiento normal de las IC (24 horas los siete días de la semana) se pasa, por ejemplo, a una situación de urgencia o recuperación. Puede que un hospital no utilice combustible en el día a día pero necesite diésel para hacer funcionar los generadores de emergencia cuando falla el suministro eléctrico externo. Estos cambios en el "funcionamiento" de las dependencias no son fáciles de evaluar [Nieuwh2008].

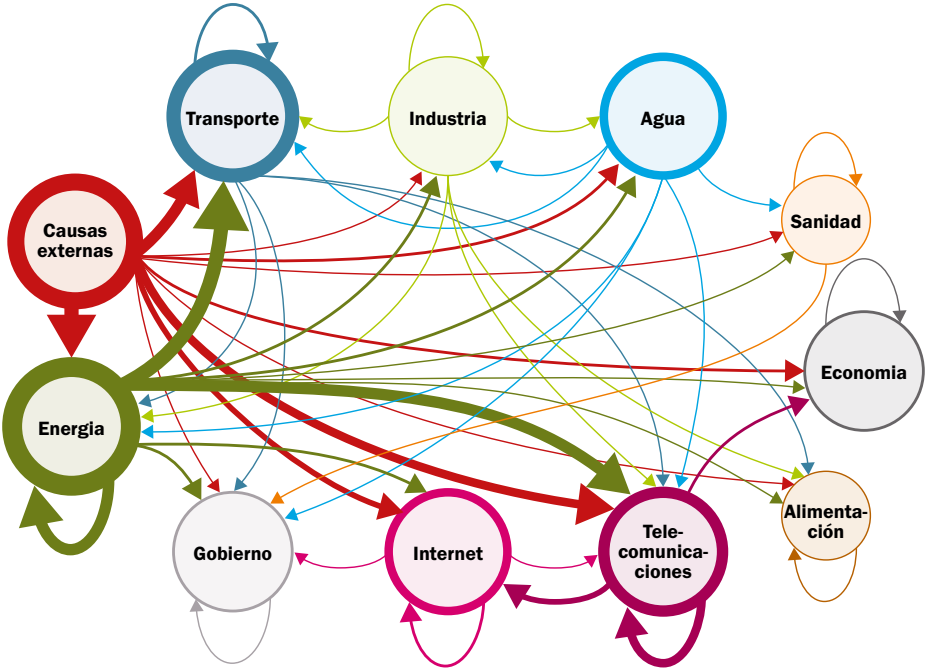


Figura 7. Fallos en cascada en IC en las dependencias que existen en Europa (2005-2009).
Nota: la magnitud relativa de las causas externas se divide en cinco puntos.

Es muy probable que el número de IC que se han determinado aumente tras identificar dependencias de estas infraestructuras. Los sectores y servicios de las IC son parte vital de las diferentes cadenas de servicios y suministros que, cada vez, son más numerosas y están más interconectadas. El uso de las tecnologías de información y comunicación hacen que esta tendencia sea mayor. Por ejemplo, un fallo en un alimentador de una infraestructura externa, como un proveedor de red troncal de telecomunicaciones, podría provocar cortes en la dependencia que existe en toda una serie de procesos de las IC. El funcionamiento de un hospital o la imposibilidad de controlar el flujo que necesita una planta de tratamiento de residuos, sería un ejemplo de ello.

Valorar los criterios comunes

Los criterios comunes pueden servir de base para el carácter crítico de algunas infraestructuras de un país, tanto en circunstancias normales como de urgencia. Estos pueden consultarse en [Catar2014] y [CE2008], por ejemplo:

- Criterio sobre víctimas (cifra de posible víctimas o heridos);
- Criterio de efectos económicos (importancia de posibles pérdidas y/o deterioro de los servicios. Posibles efectos para el medioambiente);
- Criterio de efectos públicos (repercusiones en la confianza de los ciudadanos, grado de sufrimiento físico de la población y nivel de alteración en la vida diaria);

- Criterio de dependencia (p. ej.: posible efectos en cascada en otros sectores: menores, moderados, importantes, incapacitantes);
- Criterio de repercusión (ámbito afectado: local, ámbito amplio o múltiples sectores (parcialmente), nacional o un único sector (por completo), internacional o múltiples sectores (por completo); número de personas afectas y/o densidad de población de la zona afectada);
- Repercusiones en el servicio (p. ej.: tiempo de recuperación en días).

Para más información, consúltese [RECIPE2011], [CE2008], [Mattioli2015] y [Qatar2014].

3.2.3 BUENAS PRÁCTICAS: ANÁLISIS DE DEPENDENCIA (NACIONAL E INTERNACIONAL)

Las dependencias que existan surgirán ya en los primeros pasos al identificar las IC y realizar la evaluación de riesgos, pero también existen métodos específicos para establecerlas. Aparte de las dependencias que pueda haber dentro del país, éstas pueden darse también entre IC nacionales e infraestructuras que se encuentran en países o regiones vecinas. Esto puede influir en el aspecto crítico de una infraestructura nacional particular; por ejemplo, cuando la economía nacional depende en gran medida de la exportación e importación. El método más sencillo es organizar un taller en el que participen actores de diferentes sectores críticos.

3.3 BIBLIOGRAFÍA Y MATERIAL DE LECTURA COMPLEMENTARIO

[Brunner2009] E.M. Brunner and M. Sauer, International CIIP Handbook 2008/2009: An Inventory of 25 national and 7 international Critical Infrastructure Protection Policies, ETH, Zürich, Switzerland, 2009 [Manual Internacional sobre PICI 2008/2009: Listado de 25 Políticas Nacionales y 7 Internacionales sobre Protección de Infraestructuras Críticas, ETH, Zurich, Suiza, 2009] *Online:* http://www.css.ethz.ch/ content/dam/ethz/special-interest/gess/cis/ center-for-securities-studies/pdfs/ CIIP-HB-08-09.pdf

[Bruno2002] S. Bruno and M. Dunn, Critical Information Infrastructure Protection: An Inventory of Protection Policies in Eight Countries, ETH, Zürich, Switzerland, 2002 [Protección de infraestructuras críticas de la información: Listado de Políticas de Protección en Ocho Países, ETH, Zurich, Suiza, 2002] *Online:* http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/ center-for- securities-studies/pdfs/CIIP_Handbook_2002.pdf

[Cabinet2010] Cabinet Office, Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure from Natural Hazards, March 2010 [Oficina del Gabinete del Gobierno, Marco Estratégico y Política para Mejorar la Capacidad de Recuperación de Infraestructuras Críticas tras Desastres Naturales, marzo 2010] *Online:* https://www.gov.uk/government/uploads/ system/uploads/attachment_data/ file/62504/strategic-framework.pdf

[CTO] Commonwealth Telecommunication Organisation, Critical Information Infrastructure Protection (CIIP) workshops, 2015 [Organización de Telecomunicaciones de la Commonwealth, Talleres sobre Protección de infraestructuras críticas de información (PICI), 2015] *Online:* http://www.cto.int/ strategic-goals/cybersecurity/ciip-workshops/

[CE2008] European Council, Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance) [Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección (Texto pertinente a efectos del EEE)] *Online:* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008L0114

[Hyslop] Maitland Hyslop, Critical Information Infrastructures: Resilience and Protection, Springer, 2007 [Infraestructuras críticas de información: Capacidad de Recuperación y Protección, Springer, 2007]

[Luiijf2009] Luiijf, E, Nieuwenhuijs, A., Klaver, M., Eeten, M. van., Cruz, E., Empirical Findings on Critical Infrastructure Dependencies [Conclusiones empíricas sobre dependencias de Infraestructuras críticas] R. Setola, S. Geretshuber (eds), Critical Information Infrastructure Security [Seguridad de infraestructuras críticas de la información], Lecture Notes in Computer Science (LNCS) 5508 [Notas de cursos sobre ciencias informáticas], Springer, 2009, pp. 302-310.

[Macaulay2008] Macaulay, T., Critical Infrastructure: understanding its component parts, vulnerabilities, operating risk, and interdependencies, CRC press, Canada, 2008 [Conocer las infraestructuras críticas de información: partes, puntos débiles, riesgos de explotación e interdependencias, CRC press, Canadá, 2008]

[Mattioli2015] R. Mattioli, C. Levy-Bencheton, Methodologies for the identification of Critical Information Infrastructure assets and services, ENISA, February 2015 [Metodologías para la identificación de bienes y servicios de infraestructuras críticas de información, ENISA, febrero 2015] *Online:* https://www.enisa.europa.eu/publications/methodologies-for-the-identification- of-ciis/at_download/fullReport

[Nieuwh2008] Nieuwenhuijs, A.H., Luiijf, H.A.M., Klaver M.H.A., 'Modeling Critical Infrastructure Dependencies' ["Descripción teórica de las Dependencias de Infraestructuras Críticas"]: IFIP International Federation for Information Processing, Volume 290, Critical Infrastructure Protection II, eds. P. Mauricio and S. Shenoi, (Boston: Springer), October 2008, pp. 205-214, ISBN 978-0-387-88522-3.

[PSC2014] Public Safety Canada/Sécurité publique Canada, Critical Infrastructure Policy, Forging a Common Understanding for Critical Infrastructure. March 2014 [Seguridad Pública Canadá, Política de Actuación para Infraestructuras Críticas, Llegar a un Entendimiento Común sobre Infraestructuras Críticas, Marzo 2014]. *Online:* https://www.dhs.gov/sites/default/files/publications/critical-five-shared-narrative-critical-infrastructure-2014-508.pdf

[Qatar2014] Qatar Ministry of Information and Communications Technology, Qatar National Cyber Security Strategy (السيبراني للأمن الوطنية الاستراتيجية), May 2014 [Ministerio de Información y Tecnología de las Comunicaciones de Catar, Estrategia Nacional de Catar sobre Ciberseguridad, Mayo 2014]. *Online:* http://www.motc.gov.qa/sites/default/files/national_cyber_security_strategy. pdf

[RECIPE2011] M. Klaver, E. Luiijf, A. Nieuwenhuijs, Good Practices Manual for CIP Policies for policy makers in Europe, TNO, 2011 [Manual de buenas prácticas sobre políticas de PIC para legisladores europeos, TNO, 2011]. *Online:* http://www.tno.nl/recipereport

[VEeten2011] M. van Eeten, A. Nieuwenhuijs, E. Luiijf, M. Klaver, E. Cruz, The State and the Threat of Cascading Failure across Critical Infrastructures: The Implications of Empirical Evidence from Media Incident Reports, Public Administration, Vol. 89, No. 2, 2011, (381-400) [El Estado y la Amenaza de los Fallos en Cascada en las Infraestructuras Críticas: Repercusiones de Pruebas Empíricas a partir de Información de los Medios de Comunicación sobre Incidentes]

4 IDENTIFICACIÓN DE INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN

Un segundo paso después de la identificación del conjunto nacional de IC es identificar las ICI. Pueden utilizarse pasos similares a los expuestos en el capítulo precedente, aunque la identificación de las ICI a menudo es más compleja que la identificación de las IC, como se explica más abajo.

4.1 DESCRIPCIÓN GENERAL Y PRINCIPALES DESAFÍOS

La identificación del conjunto nacional de ICI es un proceso arduo. No obstante, si se hace de forma estructurada mediante el empleo de buenas prácticas, se puede llegar a controlar el proceso.

4.1.1 COMENZAR DETERMINANDO EL CONJUNTO DE POSIBLES ICI

Como se muestra en la figura 8, la ICI presenta dos focos de atención:

1. Los servicios de infraestructuras críticas de las TIC utilizados por las IC (p.ej., telecomunicaciones móviles, acceso a Internet);
2. La información crítica, comunicaciones y tecnologías del control de sistemas que se utilizan en y a través de los procesos de IC de los sectores de las IC.

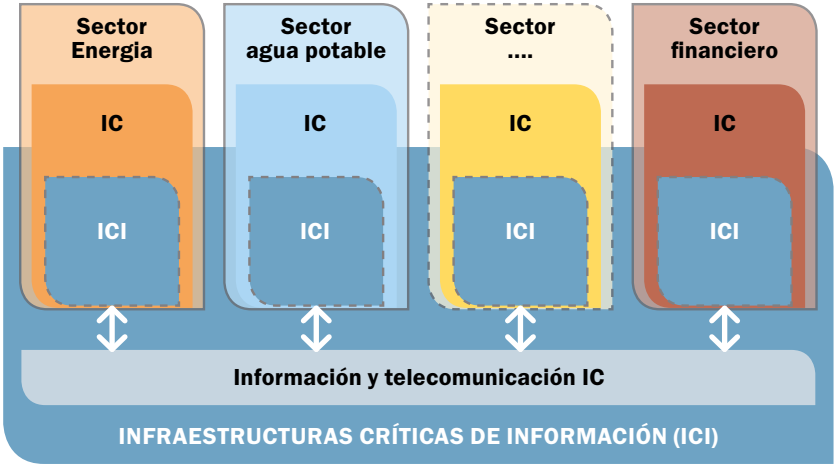


Figura 8. Las ICI incluyen (1) las IC de Información y Telecomunicaciones, y (2) los componentes ICI en IC (p. ej., sistemas de control).

Esto está en consonancia con el acuerdo 2008 de la OCDE de las ICI [OCDE2008]: *"Las ICI Nacionales {...} incluyen normalmente uno o más de los siguientes:*

- *componentes de información que apoyan las IC; y/o*
- *infraestructuras de información que apoyan a componentes esenciales de la gestión gubernamental; y/o*
- *infraestructuras de información esenciales para la economía nacional".*

Gran parte de los textos clásicos y actuales sobre ICI/PICI se centran en el primero de los dos focos de atención. Dicho de otro modo, se centran en las IC relacionadas con la Información y las Telecomunicaciones y en las flechas de interconexión-IC que aparecen en la figura 1. La intersección de las ICI con los distintos servicios de las IC a veces se pasa por alto.

La información crítica, comunicaciones, y tecnologías del control de sistemas que se utilizan en y a través de los procesos de IC de los sectores de las IC:

1. Sistemas de control que monitorizan y controlan partes críticas de sectores y/o servicios específicos de las IC (p.ej., sistemas específicos de control en la producción, transporte y distribución de gas natural). Las razones para considerarlos parte de las ICI son:
   - Las tecnologías del control de sistemas de las ICI son, cada vez con mayor frecuencia, no específicas del sector, disponibles en el comercio, y con el protocolo de Internet ('TCP/IP') activado.
   - Las necesidades de las empresas pueden requerir a los operadores de IC sus sistemas críticos de control para sus redes internas de la empresa y, por ello, de modo indirecto, para redes públicas que incluyan Internet. Al mismo tiempo, operaciones de IC complejas con varios operadores pueden requerir la interconectividad de los sistemas críticos de IC de diferentes operadores.
   - Los fabricantes, las compañías de mantenimiento y los integradores de sistemas pueden requerir acceso remoto las 24 horas a los sistemas de control y a los sistemas ciberfísicos controlados para optimizar los procesos y para buscar deterioros en la instalación, p.ej., en una central eléctrica.
2. Del mismo modo, otros elementos críticos como pueden ser los sistemas financieros y logísticos en otras IC de varios operadores de IC están cada vez más interconectados a la hora de proporcionar conjuntamente servicios fundamentales y de extremo a extremo y que son parte de una infraestructura central internacional de servicios, p.ej., los servicios interbancarios SWIFT).

Basándose en análisis, [NISC.JP2014] definió el conjunto de 13 sectores ICI japoneses como:

- Servicios de información y comunicación
- Servicios financieros
- Servicios de aviación
- Servicios ferroviarios
- Servicios de sumunistro de electricidad
- Servicios de suministro de gas
- Servicios gubernamentales y administrativos (incluidos los servicios públicos municipales)
- Servicios médicos
- Servicios hídricos
- Servicios logísticos
- Industrias químicas
- Servicios de tarjetas de crédito; e
- Industrias del petróleo.

Muchas piezas nuevas de los equipos operan sólo con TIC y pueden requerir conectividad con redes públicas, o con Internet. Esta tendencia ha introducido dependencias de procesos críticos en las IC que son tanto deseadas como inesperadas.

Una proporción cada vez mayor de funciones está siendo subcontratada a terceros. Dichos terceros pueden también operar fuera de las fronteras nacionales. Esta es también la razón por la cual el sector privado a menudo tiene algún tipo de papel en las IC, como se ha dicho antes en esta guía. Por ello, la identificación de las ICI es un proceso que exige flexibilidad y evaluaciones periódicas en el tiempo.

4.1.2 IDENTIFICAR A LOS OPERADORES DE ICI (PÚBLICOS, PÚBLICOS-PRIVADOS, PRIVADOS)

En apartados anteriores se mencionaban las diferencias entre países en lo relativo a las IC. En algunos países, las IC están en manos del sector público, mientras que en otros son las compañías privadas las responsables de las IC. Las empresas suministradoras de agua potable son un ejemplo de esta diferencia. En algunos países, las empresas suministradoras de agua potable están privatizadas, mientras que en otros, el suministro de agua potable es responsabilidad únicamente de una agencia nacional, estatal o municipal encargada de los recursos hídricos. No obstante, incluso si los gobiernos no han privatizado sus servicios críticos, siguen dependiendo del correcto funcionamiento de las ICI. Para muchos países, las ICI son cada vez más importantes para el buen funcionamiento de la sociedad (tanto en términos de procesos críticos como en la vida cotidiana normal), por lo que los operadores públicos y privados de IC están cada vez más involucrados con los operadores de IC nacionales e internacionales. Estos factores podrían hacer que resultara difícil identificar a los operadores de ICI, ya que suprimen procesos obsoletos e introducen nuevos servicios y dependencias basados en las TIC. La construcción de una red tal y como se explica en el Capítulo 7 es un medio para involucrar lo antes posible a todos los actores relevantes en este proceso.

4.1.3 IDENTIFICAR DEPENDENCIAS DE LAS ICI Y CADENAS DE SUMINISTRO DE LA INFORMACIÓN

Muchas de las IC, si no todas, están directa o indirectamente influidas por los sistemas de control[4]. Procesos cruciales en la mayoría de IC y en muchas otras organizaciones se basan, en lo que se refiere a los negocios, en el correcto y normal funcionamiento de los sistemas de control y en las redes de sistemas de control. Los sistemas de control son muy a menudo semiautónomos y realizan tareas automáticas de fondo (monitorizar, realizar tareas rutinarias) y, por lo tanto, normalmente han sido diseñados y construidos para operar en un entorno aislado y operado a distancia durante las 24 horas, siete días a la semana.
Por razones que tienen que ver con la eficacia y la flexibilidad, los sistemas de control están cada vez con mayor frecuencia conectados a redes externas a sus sistemas y a las redes en las cuales operan. A menudo las redes de sistemas de control están conectadas a redes que incluyen Internet.

Un fallo en los sistemas de control puede ocasionar interrupciones (críticas) del servicio y suponer un riesgo para la seguridad de la población y del medio ambiente. En consecuencia, la ciberseguridad de los sistemas de control es sumamente importante para los servicios públicos básicos y para otros operadores de IC, y para todas las organizaciones que utilizan sistemas de control y, por ende, potencialmente para la sociedad en su conjunto.
Una parte de los sistemas de control en las IC vigila y controla los procesos críticos de las IC (p.ej., depuración, producción y distribución del agua potable). Para dichos sistemas de control, resultaría obvio ser parte de sus ICI asociadas.

Las TIC han sido el motor de los sistemas de comunicación desde el principio, pero las TIC han sido ya empleadas, acogidas y adoptadas en distintos pero prominentes entornos no-TIC. Por ejemplo, los sistemas de control operan y vigilan actualmente sistemas que solían operarse manualmente, p. ej., el control de la señalización y las barreras de la red ferroviaria. Esto plantea nuevos desafíos porque las TIC se van a convertir de pronto en un factor a considerar cuando se intente garantizar la continuidad de la producción o de los servicios las 24 horas. Otro aspecto a destacar es que las TIC han sido con frecuencia introducidas en el entorno empresarial sin una conciencia de la seguridad de las TIC o de las potenciales vulnerabilidades. El resultado de esto podría ser que TI que no funcionen correctamente en entornos administrativos podrían causar daños en entornos de producción locales y distantes.

4 Los sistemas de control llevan a cabo la vigilancia y control 24 horas al día, 7 días a la semana, de los sistemas ciberfísicos, p. ej., la generación de energía eléctrica, los procesos de producción de una refinería y la señalización y control de las agujas de la red de ferrocarril. Existe una amplia variedad de conceptos para *´Sistemas de control´:* Sistemas Industriales de Control (SIC), Sistemas Industriales de Automatización y Control (SIAC), Sistemas de Control y Adquisición de Información (SCADA), Sistemas de Control Distribuido (SCD). Sistemas de Control de Proceso (SCP) y otros. Aunque existen ligeras diferencias, a efectos de la presente guía utilizaremos el concepto ´Sistemas de control´.

4.1.4 PERSPECTIVA CRUCIAL DE LAS DEPENDENCIAS NO CONTROLABLES

Enfocarse en las dependencias, los operadores de IC y los actores requiere una visión más amplia. La comunicación global tiene lugar en Internet y las ICI probablemente usan la misma infraestructura para las comunicaciones críticas. La conectividad de un país a la Internet global podría depender en gran medida de los Puntos de Intercambio de Internet y de *hubs* de comunicación tanto a nivel nacional como internacional.

La dependencia de sistemas y servicios interconectados (y de las tecnologías subyacentes) sobre la que no tenemos control directo es inevitable hoy en día. Por ello es esencial obtener una perspectiva del alcance de estas dependencias imposibles de controlar y de los posibles efectos negativos en caso de que se produzca un fallo o un corte. Si el impacto de estos efectos se considera inaceptable, los actores afectados por el mal funcionamiento de procesos críticos deben tomar medidas para prevenirlo, o sustituir el proceso crítico.

Algunos elementos que pueden requerir atención son: autoridades certificadas (AC), comunicaciones vía satélite, plataformas de alojamiento web globales (p.ej., servicios de la nube), puntos de intercambio de Internet (IX), servicios de nombres de dominios (SND), fabricantes de hardware, y otros [Luiijf2015a]. Las dependencias no controlables son una dimensión particular a la que hay que prestar atención. Esta dimensión es única para las TIC debido a su compleja conectividad global que podría interrumpir sistemas internacionales que se basan, por ejemplo, en TIC que se encuentran a mucha distancia.

Pueden existir también dependencias cuando la vieja tecnología es reemplazada por la nueva. Se puede depender de pronto de nuevas tecnologías que son vulnerables a la manipulación, interrupción o averías a causa de las amenazas cibernéticas. Debe observarse cuidadosamente un compromiso entre una mayor eficacia y una reducción de los costes.

4.2 BUENAS PRÁCTICAS PARA LA IDENTIFICACIÓN DE IC

Buenas prácticas para la identificación de ICI son las siguientes:

- Principios G8 para la Protección de Infraestructuras Críticas de Información;
- Identificación de ICI;
- Ir por delante de los avances tecnológicos y las dependencias cambiantes de las ICI.

4.2.1 BUENAS PRÁCTICAS: PRINCIPIOS G8 PARA LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN

En 2003, el G8 observó que las infraestructuras de información son cada vez más una parte esencial de las IC. [G8]. El G8 concluyó que los países deberían proteger sus propias ICI frente a posibles daños y ataques. Una Protección de infraestructuras críticas de información (PICI) eficaz incluye identificar amenazas, reducir las vulnerabilidades, minimizar los daños y el tiempo de recuperación, identificar la causa de la interrupción, y el análisis por parte de expertos y/o la investigación por parte de los organismos de seguridad. Una PIC eficaz requiere asimismo la comunicación, coordinación, y cooperación, tanto a nivel nacional como internacional, entre todas las partes interesadas con el debido respeto a la

seguridad de la información y a la ley aplicable relativa a la asistencia legal mutua y a la protección de la privacidad. Con vistas a alcanzar estos objetivos, el G8 adoptó y promovió los siguientes principios para la PICI:

1. Los países deberían tener redes de alerta de respuesta a emergencias respecto a las cibervulnerabilidades, amenazas e incidentes.
2. Los países deberían aumentar la conciencia de las partes interesadas a fin de que puedan comprender la naturaleza y el alcance de sus ICI, y el papel que cada una de ellas debe tener para protegerlas.
3. Los países deberían examinar sus infraestructuras e identificar dependencias entre ellas, reforzando así la protección de dichas infraestructuras.
4. Las países deberían promover las asociaciones entre las partes interesadas, tanto públicas como privadas, con el fin de compartir y analizar información sobre infraestructuras críticas para prevenir, investigar y responder a posibles daños o ataques a dichas infraestructuras.
5. Los países deberían crear y mantener redes de comunicación para crisis y probarlas para asegurarse de que seguirían siendo seguras y fiables en situaciones de emergencia.
6. Los países deberían garantizar que las políticas de disponibilidad de datos tienen en cuenta la necesidad de proteger las ICI.
7. Los países deberían facilitar la localización de ataques a ICI y, en caso necesario, facilitar dicha información sobre localización a otros países.
8. Los países deberían realizar actividades de capacitación y ejercicios para mejorar sus capacidades de respuesta y testar los planes de continuidad y contingencia en el caso de que se produjera un ataque a una infraestructura de información, y deberían animar a las partes interesadas a desarrollar actividades similares.
9. Los países deberían asegurarse de que tienen una normativa sustantiva y procesal adecuada, como las subrayadas en el Convenio del Consejo de Europa sobre la Ciberdelincuencia del 23 de noviembre de 2001, y personal capacitado que les permita investigar y perseguir ataques a las ICI, y coordinar dichas investigaciones con otros países según proceda.
10. Los países deberían comprometerse con la cooperación internacional, cuando ello sea necesario, para proteger las ICI, incluyendo mediante el desarrollo y la coordinación de sistemas de alerta para emergencias, el intercambio y el análisis de información sobre vulnerabilidades, amenazas e incidentes, y coordinando investigaciones sobre ataques a dichas infraestructuras de conformidad con el derecho interno.
11. Los países deberían promocionar la investigación y el desarrollo, tanto a nivel nacional como internacional, y fomentar la aplicación de tecnologías de seguridad que estén certificadas de conformidad con las normas internacionales.

Estos principios han sido posteriormente examinados y aprobados por la OCDE.

4.2.2 BUENAS PRÁCTICAS: IDENTIFICACIÓN DE ICI

Existe una metodología para realizar análisis profundos e identificar ICI que ha sido documentada por ENISA en [Mattioli2015] y que se alinea en gran medida con las 'Buenas prácticas: Adoptar sistemáticamente una metodología para identificar sectores y servicios ICI' (Apartado 3.2.2). No obstante, este enfoque considera sólo el primer objetivo ICI expuesto en Apartado 4.1.1 supra. Tras la identificación de sectores de infraestructuras críticas, la metodología describe la identificación de servicios críticos como un proceso de dos etapas:

1. Identificación de servicios críticos – puede realizarse desde un enfoque basado en el gobierno o desde el enfoque de un operador de IC, y
2. La identificación de activos IC (aplicaciones) que apoyan servicios críticos.

Determinar el segundo objetivo de la identificación de ICI descrito en el Apartado 4.1 supra, la infraestructura del sector de interconexión ente IC y tecnologías críticas, es mucho más difícil de conseguir. Requiere un fomento de la confianza y una estrecha cooperación (véase el Capítulo 7) con cada uno de los sectores de infraestructuras críticas, y la cadena de suministro de elementos esenciales de las infraestructuras críticas (fabricantes, vendedores, integradores de sistemas, proveedores "llave en mano", compañías de mantenimiento externas).

4.2.3 BUENAS PRÁCTICAS: IR POR DELANTE DE LOS AVANCES TECNOLÓGICOS Y LAS DEPENDENCIAS CAMBIANTES DE LAS ICI

Mantener las ICI seguras y protegidas no es una actividad que se realice una única vez. Por una parte, el panorama de amenazas a la actual base instalada cambia constantemente; por otra, se están desplegando continuamente nuevas tecnologías en las ICI. Por ello, es importante crear una funcionalidad a nivel nacional que esté a la altura de las nuevas amenazas y vulnerabilidades. Más aún, dicha funcionalidad debería evaluar las implicaciones a corto y largo plazo para la seguridad y la resiliencia de las ICI que supondría la introducción de nuevas tecnologías en las ICI. Estas ideas deben compartirse entre los responsables políticos de las ICI y los operadores de ICI nacionales [Luiijf2015].

Para las amenazas y vulnerabilidades actuales es importante establecer un proceso para identificar fuentes relevantes de información, a fin de procesar la información recogida, evaluar el impacto potencial y publicar hojas de datos relevantes y precisas, avisos, etc. (véase el Capítulo 7).

4.3 BIBLIOGRAFÍA Y LECTURAS RECOMENDADAS

[CIPedia©] CIPedia©: un punto de referencia internacional común para los conceptos y definiciones relativos a la PIC y la PICI. *Online:* http://www.cipedia.eu

[G8] Principios G8 para la Protección de Infraestructuras Críticas de Información, G8, 2003. *Online:* http://www.cybersecuritycooperation.org/documents/G8_PICI_Principles.pdf

[Luiijf2015] E. Luiijf, M. Klaver, Symposium on Critical Infrastructures: Risk, Responsibility and Liability. Governing Critical ICT: Elements that Require Attention, European Journal of Risk Regulation, Vol. 6, Issue 2 (2015), pp. 263-270 [E. Luiijf, M. Klaver, Simposio sobre Infraestructuras Críticas: Riesgo, Responsabilidad y Obligaciones. Gobernando las TIC Críticas: Elementos que requieren atención, Revista Europea de Regulación del Riesgo, Vol. 6, Número 2 (2015), págs. 263-270].

[Mattioli2015] R. Mattioli, C. Levy-Bencheton, Methodologies for the identification of Critical Information Infrastructure assets and services, ENISA, February 2015. [R. Mattioli, C. Levy-Bencheton, Metodologías para la identificación de activos y servicios de Infraestructuras Críticas de Información, ENISA, febrero 2015]. *Online:* https://www.enisa.europa.eu/publications/methodologies-for- the-identification-of-ciis-at_download/fullReport

[NISC.JP2014] The Basic Policy of Critical Information Infrastructure Protection (3rd Edition) – Tentative translation, Japan, 2014. [Política Básica para la Protección de Infraestructuras Críticas de Información (3ª edición) – traducción orientativa, Japón 2014].*Online:* http://www.nisc.gojp/eng/pdf/actionplan_ci_eng_v3.pdf

[OECD2008] OECD ICCP Committee and the Working Party on Information Security and Privacy, OECD Recommendation on the Protection of Critical Information Infrastructures [C(2008)35], 2008, OECD. [Comité ICCP (Comité de Política de la Información, la Informática y las Comunicaciones) de la OCDE y Grupo de Trabajo sobre seguridad de la información y privacidad, Recomendación sobre Protección de Infraestructuras Críticas de Información [C (2008)35], 2008, OCDE]. *Online:* http://www.oecd.org/sti/40825404.pdf

[Willke2007] B.J. Willke, A Critical Information Infrastructure Protection Approach to Multinational Cyber Security Events (presentation slides), ENISA, September 2007. [B.J. Willke, Un enfoque de la Protección de Infraestructuras Críticas de Información sobre los sucesos multinacionales de seguridad cibernética (diapositivas de la presentación), ENISA, septiembre 2007]. *Online:* http://www.enisa.europa.eu/topics/national-csirt-network/files/event-files/ENISA_best_practices_for_PICI_Wilke.pdf

5 DESARROLLO DE LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN

5.1 DESCRIPCIÓN GENERAL Y TEMAS PRINCIPALES

La Protección de Infraestructuras Críticas de Información no es sólo una preocupación técnica. Los aspectos de organización que no son propiamente técnicos son igualmente importantes. La conciencia de la gestión de riesgos en la PICI puede garantizar un enfoque equilibrado que abarque el ciclo completo de respuesta a un ciberincidente (proactiva, prioritaria, prevención, preparación, respuesta al incidente, recuperación, asistencia/ seguimiento); véase p.ej., el Capítulo 4: Estructuras y Consideraciones Organizativas en [Klimburg2012]. Después de un arranque inicial, el uso regular de la evaluación de riesgos puede reforzar los esfuerzos actuales para la PICI por estar a la altura del riesgo actual. En comparación con el perfil nacional de riesgo tal y como aparece descrito en Capítulo 2, la gestión de riesgos se entiende en este capítulo como una práctica para los operadores individuales de ICI (o un conjunto de operadores de ICI específicos del sector). Los ejercicios de crisis son un elemento crucial para la PICI, porque combinan los aspectos técnicos de la PICI y los aspectos organizacionales transversales del ciclo de respuesta a incidentes.

5.1.1 GESTIÓN DEL RIESGO

Las acciones para la gestión de riesgos en la PICI pueden ser realizadas por operadores de ICI. Si una infraestructura de información es identificada como crítica, proporcionar herramientas y directrices para la gestión de riesgos puede fomentar su utilización y potenciar la inclusión y la aplicabilidad de la evaluación. Los esfuerzos para la gestión de riesgos pueden establecer un marco común sobre qué partes de las ICI son analizadas, y qué términos, definiciones, criterios, parámetros se utilizan. Una gestión de riesgos para las ICI adecuada tiene en cuenta el riesgo que suponen las dependencias críticas de otros sectores; un aspecto del impacto que puede socavar los intereses directos del operador de una ICI.

Durante estas primeras fases de la PICI, esta perspectiva de la gestión de riesgos sigue dependiendo de lo que se considera posible tanto dentro de cada sector como entre ellos. La figura 9 ilustra la relación entre distintos conceptos de gestión de riesgos.

Figura 9. Relación entre evaluación del riesgo y gestión del riesgo.

Hay un gran número de países que han desarrollado herramientas y directrices para la gestión de riesgos (p. ej., [VanMill2006], [Habegger, 2008]). Aunque difieren considerablemente de unos a otros, tiene algunos elementos en común que contribuyen a su éxito:

1. determinación del contexto del análisis;
2. identificación del potencial riesgo;
3. evaluación de las amenazas, vulnerabilidades (a veces integradas en la determinación de las amenazas) e impactos;
4. determinación de los consiguientes factores de riesgo (y análisis de los mismos).

A fin de identificar y comprender el riesgo, es necesario disponer de información sobre las amenazas, el efecto u efectos del impacto o impactos, y una interpretación común de definiciones y parámetros. Téngase en cuenta que los operadores privados de ICI pueden haber aplicado ya sus propias metodologías para la gestión de riesgos, lo que podría ocasionar roces en el caso de que el gobierno ordenara la aplicación de otro método para la gestión de riesgos de las ICI.

Se puede encontrar más información sobre el tema de la gestión de riesgos y algunas buenas prácticas en el ámbito de las IC/ICI en el Capítulo 7 de [RECIPE] y en [Habegger, 2008].

5.1.2 LA GESTIÓN DE CRISIS NACIONAL DEBE ESTAR PREPARADA PARA LAS CRISIS DE LAS ICI

Si bien hay muchas maneras de intentar evitar que se produzcan incidentes perjudiciales, la prevención no puede eliminar todos los riesgos relativos a las ICI con respecto a los países y a sus ciudadanos. La gestión de crisis nacional organiza y gestiona todas las funciones, responsabilidades y recursos para hacer frente a incidentes y situaciones de emergencia graves y crisis a nivel nacional. Una buena gestión de las crisis a nivel nacional, así como a nivel internacional y regional, tiene en cuenta las ICI como parte de las distintas fases de preparación, respuesta y recuperación por las siguientes razones:

- Por definición, las consecuencias de una interrupción de una ICI pueden ser graves. La prevención de una interrupción de las ICI y una gestión de incidentes adecuada es una tarea primordial para los operadores de ICI. No obstante, la gestión de crisis nacional necesita planificar cómo hacer frente a las interrupciones en las ICI y el impacto de las mismas. Los ejercicios conjuntos intersectoriales pueden mejorar en gran medida la preparación de los operadores gubernamentales y de ICI.
- En cuanto a las organizaciones que se ocupan de la gestión de crisis, la continuidad de los servicios de las ICI puede ser crucial para la eficacia de sus operaciones (véase p.ej. [Luiijf2009]).

De lo que antecede resulta evidente que una gestión de crisis efectiva y eficiente requiere un profundo conocimiento de las ICI, de sus operaciones y sus dependencias. Es necesaria una cooperación estrecha y un entendimiento mutuo con los operadores de IC/ICI en la planificación de la respuesta a un incidente, la preparación ante emergencias (p. ej., una formación conjunta y ejercicios ICI interconectados), respuesta a la crisis y restauración (véase: Capítulo 8 de

[RECIPE]). Un organismo de coordinación de la PICI podría racionalizar los esfuerzos; véase el Apartado 5.2.2 sobre Buenas Prácticas: Crear un organismo de coordinación para la PICI.

5.2 BUENAS PRÁCTICAS PARA DESARROLLAR LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS DE INFORMACIÓN

5.2.1 BUENAS PRÁCTICAS: PARTICIPACIÓN DE EXPERTOS EN ICI COMO FUNCIÓN DE APOYO A LA GESTIÓN DE CRISIS NACIONAL

Para que la toma de decisiones resulte eficaz, la coordinación de la gestión de crisis a nivel nacional debe tener en cuenta las consecuencias de una interrupción de las ICI en un área determinada, incluyendo los efectos en cascada. Los expertos en PICI, que conocen las amenazas a las IC y a las ICI, sus dependencias críticas, sus características de interrupción y restauración, y sus potenciales efectos en cascada, pueden ayudar en la toma de decisiones relativas a la gestión de crisis nacional. Las responsabilidades relativas a la gestión de crisis y a la PICI puede asignarse a distintas partes de la misma organización, pública y/o privada. Vincularlas puede ser esencial. Una estrecha coordinación con las entidades relacionadas con la PICI podría acortar el proceso de recuperación y restauración pero la comprensión común no es un hecho. Esta participación de las partes interesadas de las ICI es similar a la participación de las partes interesadas de las IC, como se describe en [RECIPE] en las páginas 77-82.

En Holanda se ha creado una Comisión de respuesta en el ámbito de las tecnologías de la información y las comunicaciones (TIC) pública/privada (IRB), dentro del Centro Nacional de Seguridad Cibernética de Holanda (NCSC). En el caso de una ciberamenaza importante o una cibercrisis relacionada con las ICI que pudiera afectar o que afectara de una manera activa a la seguridad nacional, el Consejo de Ministros adoptará decisiones basadas en las recomendaciones del NCSC y del IRB. Tras un exhaustivo análisis de la situación actual y de las opciones de respuesta disponibles, el IRB proporciona consejo sobre el nivel táctico a los responsables a nivel estratégico y político. Pueden proporcionar también asesoramiento 'horizontal' a las otras organizaciones IRB privadas, como los operadores de ICI. En la actualidad son miembros del IRB los sectores de infraestructuras críticas de agua potable, electricidad, financiero, gubernamental y de las telecomunicaciones (incluyendo los proveedores de servicios de Internet), la comunidad CERT holandesa, así como expertos académicos y otros [IRB].

5.2.2 BUENAS PRÁCTICAS: CREACIÓN DE UN ORGANISMO DE COORDINACIÓN PARA LA PICI

Los esfuerzos para la PICI pueden ser apoyados por un organismo público de coordinación. Dicho organismo (o conjunto de organismos) puede operar a nivel estratégico o táctico, pero también a nivel técnico/operativo (véase: Capítulo 4 en [Klimburg2012]). La combinación de algunos de estos niveles respecto a la PICI reporta algunos beneficios. Los niveles táctico y estratégico, iniciados principalmente por una voluntad política, podrían, por ejemplo, participar activamente en diseñar estrategias para la PICI, estableciendo conexiones internacionales (a nivel estratégico, táctico, operativo/técnico) y empezar a participar en diálogos internacionales con redes de actores públicos y privados ICI/PICI (véase el Capítulo 7).

Un nivel operativo/técnico en la PICI podrían ser los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT), tanto públicos como privados, conocidos también como Equipos de Respuesta a Emergencias Informáticas (CERT). Los CSIRT a menudo desempeñan un papel importante en el desarrollo de las capacidades técnicas de respuesta a incidentes para las ICI. Para ello, los CSIRT controlan, alertan, advierten y prestan apoyo durante ciberincidentes en su circunscripción. Al enfocarse en la respuesta a incidentes, necesitan información, y por lo tanto progresan bajo una estrecha colaboración e intercambio de información (p. ej. [SEIa], [SEIb]). Un organismo operativo/técnico como un CSIRT puede tener fuertes lazos con una entidad que coordine la PICI a nivel táctico. En el caso de la privatización, los operadores de IC/ICI podrían haber establecido ya un CSIRT para mantener sus ICI ciberseguras. En estos casos, podría ser beneficioso para los organismos públicos interactuar o crear alianzas con los CSIRT privados.

En los últimos años, varios países han creado un Centro Nacional de Seguridad Cibernética (NCSC) en el que las capacidades de los CSIRT o CSIRT son un elemento central. Un centro de estas características puede combinar y coordinar los esfuerzos de los actores públicos en relación con la PICI (identificación de las IC/ICI, evaluación del riesgo, seguimiento y cooperación internacional). Si observamos los NCSC en todo el mundo, vemos que son organismos de coordinación en los que participan activamente actores PICI. Algunos NCSC prestan servicio a participantes públicos y privados. Pueden actuar como un intermediario fiable (no como un modelo de negocio). Crear un NCSC no es apropiado durante los primeros pasos de la PICI, pero puede resultar de gran ayuda a la hora de apoyar los pasos siguientes en el desarrollo de la misma ([NCSC2015]).

Esta funcionalidad variará dependiendo de cada país. Donde exista un Centro nacional de seguridad cibernética, un CERT/CSIRT nacional o una iniciativa similar, esta organización podría tomar la iniciativa en este empeño, pero siempre necesitaría la aportación de los operadores de IC e ICI para evaluar el potencial impacto en las distintas IC y una red internacional pública, privada y académica para tener una información lo más actualizada posible.

5.2.3 BUENAS PRÁCTICAS: EJERCICIOS CONJUNTOS PÚBLICO/PRIVADOS DE GESTIÓN DE CRISIS EN LOS QUE PARTICIPAN SECTORES Y OPERADORES DE ICI

Los operadores de ICI pueden participar en ejercicios de crisis nacionales para involucrarles en la aplicación de políticas para la PICI o probar su funcionamiento en algunas partes de las capacidades para la PICI. Existe una discrepancia en los objetivos que se persiguen al realizar ejercicios para un amplio abanico de peligros y emergencias en las autoridades públicas y operadores de ICI. Los operadores de ICI se aseguran de que la continuidad de producción de su negocio, procesos y servicios son testados para apoyar a sus clientes. Los participantes públicos tienen otros objetivos en los ejercicios de gestión de crisis. En lugar de tratar con operadores de ICI de manera ad hoc, existen numerosas razones para establecer un entendimiento claro y un marco para tratar los incidentes, emergencias y crisis. Si esto no fuera así, un incidente sencillo podría convertirse en una crisis grave. Mediante la realización de ejercicios, se aprende, con frecuencia de una forma difícil, sobre el papel de los demás, sus responsabilidades, sus ciclos de toma de decisiones, sus capacidades, habilidades y terminología. Por último, pero no por ello menos importante,

conocerse unos a otros es un factor importante citado con frecuencia a la hora de disminuir los roces entre los distintos grupos y facilitar la cooperación entre ellos.

Los ejercicios conjuntos públicos-privados, (regionales), nacionales y transfronterizos crean el nivel adecuado de preparación para emergencias de operadores de CM e ICI. Los ejercicios pueden desarrollarse a nivel operativo, táctico y estratégico, y/o comprender varios niveles. Con cada vez mayor frecuencia, los países involucran a los operadores de ICI como socios clave en ejercicios regionales, nacionales e internacionales.

La participación de las ICI en los ejercicios regionales y nacionales puede organizarse de distintas formas:
- Algunos países obligan a sus operadores de ICI a participar en los ejercicios regionales y nacionales de CM.
- Otros países esperan que sus operadores de ICI desempeñen voluntariamente su papel en los ejercicios regionales y nacionales.
- Una minoría de países contrata a operadores de IC/ICI para que participen en sus ejercicios nacionales.

En Europa, algunos países organizan ejercicios nacionales importantes en los que participan ICI y la posibilidad de una interrupción en las IC/ICI con efecto de cascada. Ejemplos de ejercicios internacionales CM-ICI son la serie de ejercicios mundiales conocidos como *Cyber Storm* o Tormenta cibernética organizados en Estados Unidos, y los llamados *Cyber Europe* o Ciber Europa, organizados por ENISA.

Experiencias/lecciones aprendidas
- Un requisito previo para la realización de un ejercicio es definir sus objetivos. Una política que permite errores sin que haya consecuencias ofrece que se aprendan la mayoría de las lecciones para una mejor cooperación CM-ICI.
- Uno de los resultados de los ejercicios es la disminución de las oportunidades de que se produzcan roces y malentendidos en la confusión de una crisis real.
- El intercambio de datos confidenciales privados de la empresa a CM durante los ejercicios requiere salvaguardias para la seguridad de los datos por parte del entorno CM (véase el Apartado 7 sobre intercambio de información).

5.3 BIBLIOGRAFÍA Y LECTURAS RECOMENDADAS

[CIPedia©] CIPedia©: un punto de referencia internacional común para los conceptos y definiciones relativos a la PIC y la PICI. *Online:* http://www.cipedia.eu

[CSA] Cyber Security Agency Singapore, Ministry of Communications and Information. [Agencia de Ciberseguridad de Singapur, Ministerio de las Comunicaciones y la Información]. *Online:* https://www.csa.gov.sg/

[FICORA] Finnish Communications Regulatory Authority. [Autoridad Reguladora de las Comunicaciones de Finlandia]. *Online:* https://www.viestintavirasto.fi/en/cybersecurity.html

[Habegger2008] B. Habegger, International Handbook on Risk Analysis and Management: Professional experiences, ETH, Zurich, Switzerland, 2008. [B. Habegger, Manual Internacional sobre el Análisis y la Gestión de Riesgos: Experiencias profesionales, ETH, Zurich, Suiza, 2008]. *Online:* https://www.files.ethz.ch/isn/47029/HB_RiskAnalysis&Management.pdf

[IRB] Página web del NCSC sobre la 'Comisión de Respuesta TIC (IRB)'. *Online:* https://www.ncsc.nl/english/Cooperation/ict-response-board.html

[Klimburg2012] Klimburg, National Cyber Security Framework Manual, NATO CCD-COE Publications, December 2012. [Klimburg, Manual para el marco nacional de ciberseguridad, Publicaciones OTAN CCD-COE, diciembre 2012] *Online:* https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

[Luiijf2009] E. Luiijf, M. Klaver, 'Insufficient Situational Awareness about Critical Infrastructures by Emergency Management', paper 10 in: Proceedings Symposium on 'C3I for crisis, emergency and consequence management', Bucharest 11-12 May 2009, NATO RTA: Paris, France. RTO-MP-IST-086. [E. Luiijf, M. Klaver, 'Conocimiento insuficiente de la situación sobre Infraestructuras críticas por parte de la gestión de emergencias', papel 10 p: Actas del Simposio sobre 'C3I para la gestión de crisis, emergencias y consecuencias', Bucarest, 11-12 mayo 2008, OTAN ACR: París, Francia. RTO-MP-IST-086.].

[NCSC2015] CSIRT Maturity Kit: A step-by-step guide towards enhancing CSIRT Maturity, NCSC, The Hague, The Netherlands, 2015. [Kit de madurez CSIRT: Guía simple y detallada para fomentar la madurez CSIRT, NCSC, La Haya, Holanda, 2015]. *Online:* https://check.ncsc.nl/static/CSIRT_MK_guide.pdf

[NCSC-UK] Página web del Centro Nacional de Ciberseguridad, Reino Unido. *Online:* https://www.ncsc.gov.uk

[SEIa] Departamento CERT, Instituto de Ingeniería del Software, Carnegie Mellon Institute, Crear una página web CSIRT. *Online:* http://www.cert.org/incident-management/products- services/creating-a-csirt.cfm

[SEIb] Departamento CERT, Instituto de Ingeniería del Software, Carnegie Mellon Institute, Lista de acciones para desarrollar una página web CSIRT. *Online:* http://www.cert.org/incident-management/csirt-development/action-list.cfm

[VanMill2006] B.P.A. van Mil, A.E. Dijkzeul, R.M.A. van der Pennen, A view on Risk: Risk Modelling Handbook - Selection of models and methods for conducting risk analyses, Delft. [B.P.A. van Mil, A.E. Dijkzeul, R.M.A. van der Pennen, Una visión sobre el riesgo: Manual para la modelización del riesgo – Selección de modelos y métodos para realizar análisis de riesgo, Delft]. *Online:* http://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/-rapporten/-2006/09/18/a-view-on-risks/handbook-risk-modelling.pdf

6 MONITORIZACIÓN Y MEJORA CONTINUA

6.1 DESCRIPCIÓN GENERAL Y TEMAS PRINCIPALES

Con una visión actualizada de los factores de riesgo y las vulnerabilidades cambiantes de las ICI, los gobiernos nacionales pueden evaluar si son necesarios cambios en las políticas relativas a la PICI. Idealmente, la evaluación de las políticas relativas a la PICI y la revisión del panorama de los riesgos y de los cambios en las vulnerabilidades se traducen en la aplicación de una hoja de ruta de cambios políticos a fin de mantener la PICI a un nivel deseable.

6.1.1 EMPEZAR A MONITORIZAR LAS ACCIONES Y HACER MEJORAS CONTINUAS

Una vez que se ha desarrollado una estrategia o política relativa a la PICI, continúa siendo importante hacer un seguimiento de su aplicación y eficacia, así como desarrollar un ciclo continuo de mejoras en la PICI. Para poder hacer el seguimiento de la aplicación de acciones relativas a la PICI, es deseable que las políticas tengan unas intenciones y objetivos claramente definidos, y que las actividades estén definidas de forma específica, medible, alcanzable, realista y sujeta a un plazo. [SMART]. Esto permite, por ejemplo, que un parlamento nacional desempeñe su función de supervisión y que el ministerio o ministerios o agencias responsables hagan un seguimiento de los avances de las líneas de acción en la PICI. Incluso sin objetivos definidos SMART, es aconsejable hacer un seguimiento de los avances realizados para conseguir la aplicación de políticas para la PICI y planes de acción.

La vigilancia continua de la aplicación de las actividades para la PICI hace posible realizar ajustes a lo largo del proceso. Asimismo, proporciona la posibilidad de que los participantes responsables de la PICI adopten rápidamente medidas en áreas de las acciones para la PICI en las que no se haya producido avance. Aparte de hacer un seguimiento de las propias acciones y planificación, es también esencial mantenerse al día con un panorama de amenazas en constante cambio, o un panorama que cambió debido a incidentes. A través de un ciclo de continuas mejoras en la PICI se podría observar de una forma eficaz este panorama cambiante.

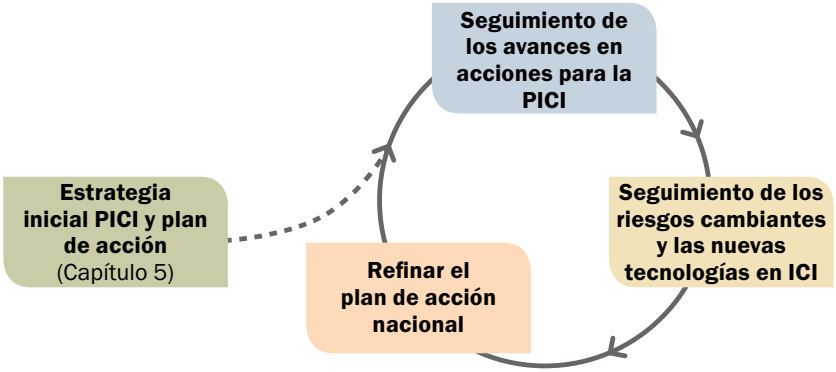


Figura 10. Ciclo de mejora constante en la PICI.

Las perspectivas de un ciclo de mejora de la PICI son:

- *Revisar:* evaluar los avances realizados en la aplicación de las políticas y planes de acción relativos a la PICI.
- *Ajustar:* hacer un seguimiento del perfil de riesgo relativo a las ICI a fin de:
  Evaluar los cambios en el riesgo para las ICI.
  Evaluar los cambios en las vulnerabilidades de las ICI.
- *Perfeccionar:* el plan de acción nacional relativo a la PICI.

***Revisar:* hacer un seguimiento de las acciones para la PICI**

Las políticas relativas a la PICI pueden incluir un amplio abanico de medidas, entre las que se encuentran los marcos políticos y jurídicos, los regímenes de autorregulación de sectores específicos de las IC, o la adopción voluntaria u obligatoria de medidas específicas de protección. Se puede hacer un seguimiento de la aplicación de dichas políticas a través de la investigación para el avance, auditorías, auto-informes sobre incidentes y cuasi accidentes emitidos por los operadores de IC y por agencias operativas.

La supervisión de las políticas relacionadas con la PICI es a menudo una función que corresponde a las autoridades o agencias que trabajan en temas más amplios como impulsar el uso de las TIC y la seguridad cibernética. Algunos países pueden optar por designar una autoridad o agencia especial para supervisor, coordinar y fomentar el avance en la PICI.
Es una buena práctica participar en diálogos internacionales para verificar las propias acciones relativas a la PICI y reflexionar sobre ellas, y para identificar las deficiencias (véase Buenas prácticas 6.2.1).

***Ajustar:* hacer un seguimiento de un panorama de riesgo cambiante y de las vulnerabilidades de las ICI**

Las actividades y planes de acción relativos a la PICI no pueden ser eficaces si no tienen en cuenta el panorama de riesgo cambiante de un país y la evolución de las vulnerabilidades de las ICI. Hacer un seguimiento del panorama de riesgo cambiante empieza por revisar los cambios en el riesgo para el país.
Revisar los riesgos es algo que debería hacerse en relación con todas las ICI identificadas y los componentes y sistemas que forman parte de dichas ICI. Esto se puede hacer, por ejemplo, mediante: revisiones periódicas, un proceso de gestión de riesgo (véase el Apartado 5.1.1), auditorías, incidentes, y lecciones identificadas en ejercicios relacionados con las ICI (véase el Apartado 3.1.2 de [NISCJP]).

Respecto al riesgo para un país, las vulnerabilidades de las ICI también evolucionan con el tiempo. Estas vulnerabilidades pueden proceder, por ejemplo, de una infraestructura de información obsoleta, una sobrecarga, o vulnerabilidades técnicas como un software no actualizado y falta de mantenimiento. Existen varias instituciones internacionales y agencias nacionales que facilitan datos e informes sobre las vulnerabilidades de las TIC (Vulnerabilidades y Exposiciones Comunes (CVE) de Mitre, grupo CERT de los gobiernos europeos (EGC), (US CERT), (ICS-CERT), TF-CSIRT, fabricantes de IC/ICI y compañías de

ciberseguridad, y vendedores de software. Para saber más sobre la notificación voluntaria de las vulnerabilidades, véase Buenas prácticas coordinadas para la divulgación de las vulnerabilidades (6.2.2).

Cuando sea posible, es aconsejable intentar armonizar el ciclo de mejora nacional para la PICI con los ciclos de autoridades subnacionales y las partes interesadas del sector privado, así como con los ciclos que siguen instituciones internacionales si existieran, ya que los resultados de las evaluaciones a estos niveles y la publicación de nuevas políticas relativas a la PICI tanto subnacionales como internacionales, a menudo proporcionan información para las políticas relativas a la PICI a nivel nacional.

***Perfeccionar:* el plan de acción nacional relativo a la PICI**

Este ciclo de mejora continuo está en línea con el ciclo Planeamiento-[Ejecución-Verificación]-Acción (PDCA) que se puede encontrar en la bibliografía, p. ej. [NISC.JP2014].

6.1.2 VISIÓN A LARGO PLAZO: DE LA PROTECCIÓN A LA RESILIENCIA

Se aconseja a los países que están empezando a desarrollar políticas y prácticas relativas a la seguridad de las ICI que comiencen con la PICI. No obstante, el concepto de 'resiliencia' aparece con frecuencia en estrategias, políticas e iniciativas. Es por ello que explicaremos brevemente aquí su significado.

La resiliencia de las infraestructuras críticas de información (CIIR) señala a un ciclo de respuesta a incidentes más amplio: acción, prevención, preparación, respuesta a incidentes, y actividades de recuperación y posteriores al incidente. Si bien la bibliografía existente sobre resiliencia ofrece poco consenso sobre la definición y naturaleza de este concepto [HOSS2016], el Consejo asesor sobre infraestructuras nacionales [NIAC] proporciona una definición de resiliencia en el contexto de las ICI: "la capacidad de reducir la magnitud y/o la duración de acontecimientos perturbadores en las ICI. La eficacia de unas ICI resilientes depende de sus capacidades para anticipar, absorber, adaptarse, y/o recuperarse rápidamente de un acontecimiento potencialmente perturbador". Los marcos de resiliencia ponen de manifiesto el hecho de que la resiliencia incluye todos los aspectos de la seguridad y continuidad del ciclo de respuesta a incidentes [p. ej. LABAKA2015, MARU2016].

Los países que desarrollan iniciativas relativas a la PICI pueden beneficiarse del conocimiento de que la PICI es a menudo seguida por la resiliencia de las infraestructuras críticas de información al incorporar la posibilidad de que las políticas relativas a la PICI incluyan aspectos de la resiliencia de las infraestructuras críticas de información en etapas posteriores o adoptando una perspectiva de la resiliencia de las infraestructuras críticas de información inmediatamente.

6.2 BUENAS PRÁCTICAS PARA LA MONITORIZACIÓN Y MEJORA CONTINUA

6.2.1 BUENAS PRÁCTICAS: PARTICIPAR EN DIÁLOGOS INTERNACIONALES

Hacer un seguimiento de los cambios en el riesgo para las ICI y en las vulnerabilidades es útil para llegar a las comunidades y foros internacionales. Existen varias comunidades y organizaciones internacionales con objetivos diferentes. Las organizaciones a un nivel táctico/estratégico son, p.ej., Europol (EC3), la ITU, la OEA, la Unión Africana, el G8, el Centro Global para la Capacidad Cibernética (GCSCC). Foros con objetivos operativos/técnicos son, p. ej., el TF-CSIRT, el Foro de Respuesta a los Incidentes y Equipos de Seguridad (FIRST), divulgación pública por parte de los CERT en todo el mundo, (ICS-CERT), (EGC), y (US CERT).

Otros ejemplos son el Proceso Meridian y el Foro Global de Experiencia Cibernética (GFCE). El Proceso Meridian pretende intercambiar ideas e iniciar acciones para la cooperación entre los organismos gubernamentales sobre los temas relacionados con la Protección de infraestructuras críticas de información (PICI) a nivel mundial.
Explora los beneficios y oportunidades de cooperación entre gobiernos y proporciona la oportunidad de compartir las mejores prácticas en todo el mundo.

El Proceso Meridian busca crear una comunidad de altos ejecutivos gubernamentales en la PICI al fomentar la colaboración continua. La participación en el Proceso Meridian está abierta a todos los países/economías y dirigida a altos ejecutivos gubernamentales involucrados en temas relacionados con la PICI. Se invita a todos los países/economías a participar en el Proceso Meridian, y a asistir a la Conferencia Meridian anual. La Conferencia Meridian ofrece a todos los participantes, con independencia de su madurez en la PICI, la oportunidad de aprender de otros, intercambiar ideas y asociarse con otros países.

El Foro Global de Experiencia Cibernética (GFCE) es una plataforma global para países, organizaciones internacionales y empresas privadas para intercambiar las mejores prácticas y experiencias en la construcción de capacidades cibernéticas. El objetivo es identificar políticas, prácticas e ideas que hayan tenido éxito y multiplicarlas a un nivel mundial. Junto con socios pertenecientes a organizaciones no gubernamentales (ONG), a la comunidad tecnológica y al mundo académico, los miembros del GFCE desarrollan iniciativas prácticas para mejorar la capacidad cibernética.

El GFCE se ha unido a Meridian específicamente para impulsar iniciativas para la PICI, pero también es responsable de muchas actividades relacionadas con este tema, enfocadas en los CSIRT y en distintos aspectos de la seguridad informática.

6.2.2 BUENAS PRÁCTICAS: SER RECEPTIVO A LA DIVULGACIÓN COORDINADA DE LAS VULNERABILIDADES

Constantemente se producen intentos de atacar, explotar y manipular sistemas y software ICI. Se aprovechan fallos en la seguridad de la TIC, hay intentos no autorizados de acceder a sistemas, y la operación de la TIC puede sufrir interferencias debido a estos intentos
De una u otra forma, se producirán incidentes relacionados con la TIC. Es importante, sin embargo, facilitar los esfuerzos para que personas benévolas notifiquen dichos incidentes.

Con independencia de que se busquen activamente o no fallos en los sistemas TIC, continuarán existiendo si el propietario no es alertado. Existen individuos en todo el mundo que deliberadamente intentan encontrar fallos de seguridad en sistemas y software para que el mundo sea un lugar más seguro. Estas personas benévolas reciben el nombre de hackers éticos. Por otra parte, también existen personas y grupos con fines maliciosos/malas intenciones que quieren explotar o atacar los sistemas TIC. Los hackers éticos o individuos que han encontrado inesperadamente un fallo de seguridad en un sistema TIC con frecuencia se encuentran con que les resulta difícil y peligroso notificar al propietario del sistema la información sobre los fallos. Esto se debe, principalmente, a que no han podido enviar sus descubrimientos a la gente adecuada, y en segundo lugar, a que notificar dichos fallos podría les podría suponer ser procesados.

Una buena práctica para tratar estos esfuerzos de notificar fallos de seguridad en la seguridad de la TIC sería formular e implementar una política de 'divulgación coordinada de las vulnerabilidades' (a veces también denominada Divulgación Responsable) [GFCE]. Los gobiernos, grandes bancos, organizaciones internacionales y otras partes privadas ya han implementado una política de divulgación coordinada de las vulnerabilidades [Microsoft]. El efecto de la implementación es que no denuncian al individuo en cuestión siempre que cumpla ciertos requisitos, garantizan su anonimato y arreglan el fallo que les fue notificado. Los incidentes de seguridad continuarán ocurriendo y éste es un buen ejemplo de buena práctica que ayude a mitigar sus efectos.

6.3 BIBLIOGRAFÍA Y LECTURAS RECOMENDADAS

[CVE] Mitre, página web sobre 'Vulnerabilidades y Exposiciones Comunes (CVE)'. *Online:* https://cve.mitre.org

[EGC] Página web de los CERT de los gobiernos europeos (EGC). *Online:* http://www.egc-group.org

[GCSCS] Página web del Centro Global para la Capacidad en Ciberseguridad. *Online:* https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/front

[GFCE] Página web sobre 'Divulgación coordinada de las vulnerabilidades'. *Online:* https://www.thegfce.com/initiatives/r/responsible-disclosure-initiative-ethical-hacking

[HOSS2016] Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. Reliability Engineering & System Safety, 145, 47-61. [Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). Un estudio de las definiciones y medidas de la resiliencia del Sistema. Ingeniería fiable y seguridad del sistema, 145, 47-61].

[ICS-CERT] Página web de los ICS- CERT. *Online:* https://ics-cert.us-cert.gov

[LABAKA2015] Labaka, L., Hernantes, J., & Sarriegi, J. M. (2016). A holistic framework for building critical infrastructure resilience. Technological Forecasting and Social Change, 103, 21-33. [Labaka, L., Hernantes, J., & Sarriegi, J. M. (2016). Un marco integral para construir resiliencia en las infraestructuras críticas. Previsión tecnológica y cambio social, 103, 21-33]..

[MARU2016] Maruyama, H. (2016). Taxonomy and general strategies for resilience. In Urban Resilience (pp. 3-21). Springer International Publishing [Maruyama, H. (2016). Taxonomía y estrategias generals para la resiliencia. En resiliencia urbana (págs. 3-21). Springer International Publishing [Maruyama, H. (2016).]

[Microsoft] Página web del Centro Técnico sobre 'Informar sobre una vulnerabilidad en la seguridad informática'. *Online:* https://technet.microsoft.com/nl-nl/security/ff852094

[NIAC] Seguridad Interior (DHS)/ Consejo Asesor sobre Infraestructuras Nacionales (NIAC), Informe final y recomendaciones sobre la resiliencia de las infraestructuras críticas. *Online:* https://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf

[SMART] Página web de los objetivos SMART. *Online:* http://www.nationalacademies.org/hmd/About-IOM/Making-a-Difference/Community-Outreach/Smart-Bites-Toolkit/~/media/17F1CD0E451449538025EBFE5B1441D3.pdf

[US CERT] Página web del Equipo de Respuesta a Emergencias Informáticas (CERT) de Estados Unidos *Online:* https://www.us-cert.gov

7 TRABAJO EN RED E INTERCAMBIO DE INFORMACIÓN

7.1 DESCRIPCIÓN GENERAL Y TEMAS PRINCIPALES

Crear redes sólidas y fiables entre actores PICI y permitir el intercambio de información son condiciones importantes para salvaguardar la sociedad. Un intercambio oportuno y rápido de información relativa a la ciberseguridad/seguridad cibernética entre los actores PICI – dentro del gobierno, dentro de sectores críticos, entre sectores, entre organizaciones públicas y privadas, nacional e internacionalmente – se percibe mayoritariamente / es ampliamente percibido como una medida eficaz para abordar algunos de los desafíos relativos a la ciberseguridad/seguridad cibernética a los que se enfrentan los operadores de ICI.

El intercambio de información, en este contexto, se lleva a cabo generalmente entre un grupo de personas cuidadosamente escogidas con un objetivo común: estar al corriente de las amenazas y vulnerabilidades nuevas y emergentes, y de los asuntos relacionados con ellas/y cuestiones conexas. Es importante escoger a personas con un nivel similar de conocimiento técnico, a niveles similares de autoridad y economía y con una tolerancia de riesgo similar [ENISA]. Estas personas intercambian información para poder adoptar las medidas adecuadas de reducción del riesgo con antelación, durante los incidentes pero también después de que se produzcan. Se reunirán periódicamente, desarrollarán una confianza personal, y compartirán información confidencial sobre incidentes, amenazas, vulnerabilidades, buenas prácticas y soluciones. Por lo general, llevan a cabo esto en un entorno de confidencialidad en el que todos se comprometen a no revelar los detalles o la procedencia de la información, pero pueden utilizarla para proteger sus propios sistemas. Existen muchas variaciones de este modelo, como se expone más adelante.

La confianza y el valor son factores clave para un intercambio de información con éxito [Luiijf2015]. Para iniciar y mantener el intercambio de conocimientos e información, los actores PICI necesitan un entorno en el que se pueda establecer y mantener de forma eficiente y efectiva una base de confianza. El entorno físico podría influir en la experiencia y el sentimiento respecto al intercambio de información. Un 'entorno' explícitamente fuera o dentro de un ministerio podría influir en el enfoque de participantes públicos y privados (por ejemplo, existe una diferencia importante entre el marco de un ministerio de Defensa o del servicio secreto y el de un ministerio de Economía). El 'entorno' podría también estar influido por el modo en que se lleve a cabo el intercambio de información (periódico, regulado, normas formales o informales) y por cómo los esfuerzos previos de organismos públicos fueron recibidos por las partes interesadas relevantes.

Crear un entorno de confianza y valor requiere tiempo y compromiso por parte de todos los participantes, pero el valor añadido de un intercambio de información mejorado y fiable supera ampliamente estos esfuerzos necesarios.

El intercambio de información favorece en particular a aquellos actores que gestionan y atenúan el riesgo de ciberseguridad/seguridad cibernética a un nivel operativo. Poder hablar de vulnerabilidades e incidentes con libertad y en una atmósfera de absoluta confianza, las organizaciones públicas, semi-públicas, y privadas obtienen una mejor visión global de posibles amenazas y vulnerabilidades, y del impacto sobre su organización, sector, o en los distintos sectores. La naturaleza de la ciberseguridad/seguridad cibernética ha evolucionado muy rápidamente y seguirá haciéndolo. Los esfuerzos por compartir información deberían también evolucionar para estar a la altura de los cambios en el panorama de la ciberseguridad/seguridad cibernética. Una ventaja del intercambio de información es la oportunidad que supone de aprovechar los recursos del conocimiento, la conciencia, la comprensión y las experiencias en una comunidad más amplia.

Otros países podrían tener experiencias valiosas sobre esfuerzos previos para la PICI. Para intercambiar experiencias, la iniciativa GFCE-Meridian está introduciendo una iniciativa conocida como *'Buddy Initiative'* o ´Iniciativa de Amigos´. Esta iniciativa se menciona como una buena práctica, junto con otras buenas prácticas en el trabajo en red y el intercambio de información. En el Apartado 7.2 pueden encontrarse referencias a otros textos y buenas prácticas:

- Fomentar el intercambio de información relativa a la ciberseguridad/seguridad cibernética;
- establecer roles claros en las Iniciativas de Intercambio en la PICI;
- Estar informado sobre las Normas para el intercambio de información;
- Tener en cuenta la Guía para el Intercambio de información sobre ciberamenazas;
- el ´Sistema de amigos´;
- diversas formas de organización de Asociaciones Público-Privadas para la PIC/PICI;
- Consejo de Ciberseguridad a nivel nacional;
- Traffic Light Protocol (TLP).

7.2 BUENAS PRÁCTICAS PARA EL TRABAJO EN RED Y EL INTERCAMBIO DE INFORMACIÓN

Para muchos actores de las ICI está totalmente claro que ninguna organización podría por sí sola abordar el espectro completo de cuestiones asociadas a la PICI, ya que las organizaciones están cada vez más interconectadas a nivel global, y expuestas a las mismas amenazas a la seguridad global. El propósito del trabajo en red y el intercambio de información relacionada con la seguridad cibernética es reducir la incertidumbre respecto al funcionamiento y la continuidad de las actividades de las ICI en un operador individual de IC, dentro de un sector completo de IC, y/o en cadenas de servicios de IC que son competencia de varias organizaciones. Las siguientes secciones proporcionan varias buenas prácticas sobre este tema. Pueden encontrarse más en la Bibliografía.

7.2.1 BUENAS PRÁCTICAS: FOMENTAR EL INTERCAMBIO DE INFORMACIÓN SOBRE INFORMACIÓN RELATIVA A LA CIBERSEGURIDAD

El intercambio de información proporciona la base para una comprensión común de las amenazas, vulnerabilidades, dependencias, y conocimiento compartido de posibles contra medidas. El intercambio de información mejora la calidad de la gestión de riesgos (véase el Apartado 5.1.1) ya que la información sobre nuevos factores de riesgo podría obtenerse con mayor rapidez. Las medidas de protección de las ICI pueden adaptarse según corresponda.

Cuando se produce una interrupción grave en las ICI, la existencia de una red fiable con un interés y una experiencia comunes ayuda a abordar el incidente de forma conjunta y eficaz. El intercambio de información es, por lo tanto, un enfoque efectivo en apoyo de la gestión conjunta del riesgo para las ICI en un ámbito en el que el panorama de las amenazas cambia constantemente.

Las experiencias de iniciativas *voluntarias* de intercambio de información muestran que la confianza es el principal factor clave para alcanzar el éxito. En apoyo de esto existe un acuerdo sobre cómo utilizar la información intercambiada en la propia organización. En muchos países, el Traffic Light Protocol (TLP); véase el Apartado 7.2.8) es un enfoque probado para permitir el intercambio de información entre organizaciones privadas, semipúblicas y públicas. Sin embargo, el intercambio de información es un concepto de múltiples facetas con muchos aspectos relacionados con la política, tanto del lado público como del privado. Se puede encontrar una discusión sobre todos los temas y un conjunto de Buenas Prácticas en [Luiijf2015]; la figura 11 ilustra algunos de los bloques de construcción que van del verde (relativamente simple) al rojo (esfuerzo importante).

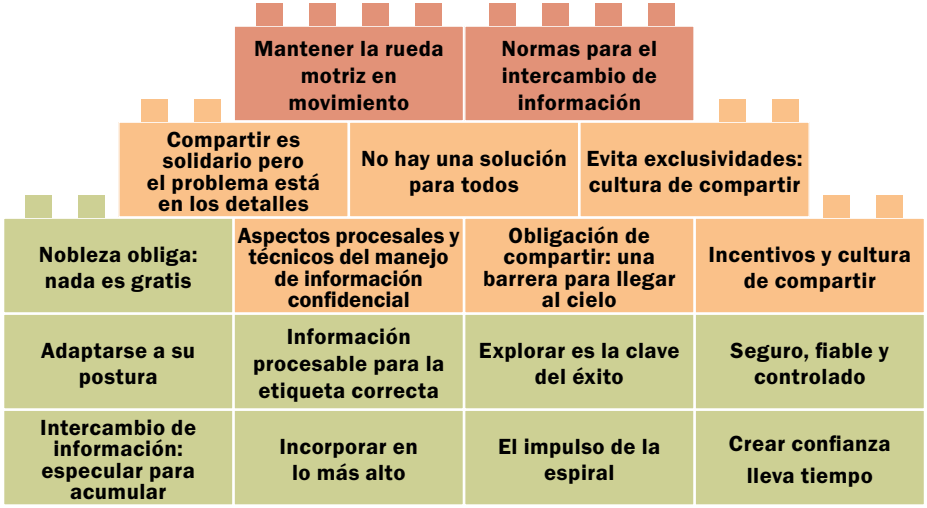


Figura 11. Construir bloques para el intercambio de información [Luiijf2015].

Por ley o mediante una normativa, los países pueden ordenar el intercambio de información entre operadores de ICI sobre ataques a la ciberseguridad e interrupciones de ICI. En ese caso, con frecuencia es difícil garantizar la calidad de la información compartida, ya que la motivación es un palo, y no una zanahoria. Incluso los enfoques obligatorios hacen hincapié por esta razón en el hecho de que para tener éxito en el intercambio de información con operadores de ICI sigue siendo esencial crear un clima de confianza y un espíritu de cooperación voluntaria.

En un entorno internacional, resulta más difícil construir la confianza necesaria para un intercambio de información eficaz debido a los problemas para organizar reuniones presenciales periódicas, sumado a las barreras lingüísticas, culturales, normativas y competitivas. No obstante, algunos países han establecido comunidades transfronterizas que comparten información sobre la PICI, como el Centro de Análisis e Intercambio de Información sobre Servicios Financieros (FS-ISAC). Del mismo modo, el intercambio de información sobre un tema específico de la PICI, como la seguridad del sistema de control y otros, tiene lugar entre países y operadores de ICI (p. ej., el [EUROSCSIE] y la política japonesa para la PICI [NISC.JP2014]).

7.2.2 BUENAS PRÁCTICAS: ESTABLECER ROLES CLAROS EN LA PICI EN INICIATIVAS DE INTERCAMBIO

Existen ejemplos de buenas prácticas en todo el mundo en los que los participantes en la PIC/PICI participan en iniciativas para el intercambio de información a nivel regional, nacional o internacional. Algunas de dichas iniciativas son de gobierno a gobierno (G2G), otras, de empresa a empresa (B2B), pero también existen muchas iniciativas público-privadas. Algunos ejemplos son el Foro de equipos de respuesta de emergencia y seguridad (FIRST), EL Grupo CERT de los gobiernos europeos (EGC), Infragard [Infragard], algunos Centros de Actividades de la Sociedad de la Información (ISAC) en Estados Unidos, la Alianza de ciberseguridad para el intercambio de información del Reino Unido (CISP), la UP KRITIS de Alemania [UP-KRITIS], intercambios de información en el Centro para la Protección de Infraestructuras Nacionales (CPNI) en el Reino Unido [CPNI IE], Centro MELANI de información y análisis para garantizar la información en Suiza [MELANI], y los NCSC ISAC en Holanda [NCSC]. En muchas de estas iniciativas, los participantes en la PICI se unen y comparten de forma activa información sobre amenazas, incidentes, vulnerabilidades y buenas prácticas. A continuación se expone un ejemplo.

MELANI - SUIZA

MELANI sirve a dos grupos de clientes. El primero de ellos es el grupo de clientes abierto que incluye usuarios privados de ordenadores e Internet, y pequeñas y medianas empresas (PYMES) en Suiza. MELANI ofrece a este primer grupo:

- Información sobre amenazas y medidas para usar las modernas tecnologías de la información y la comunicación (p. ej., Internet, e-banking) en la forma de fichas de datos.
- Informar sobre las tendencias y avances más importantes relativos a incidentes y acontecimientos en las tecnologías de la información y la comunicación.
- Un formulario de registro para informar sobre incidentes.

El Segundo grupo de clientes cerrado incluye a operadores específicos de las IC nacionales (p. ej., suministradores de energía, compañías de telecomunicación, bancos, etc.). MELANI tiene las responsabilidad de proteger a estas IC, especialmente cuando dependen críticamente del funcionamiento de las infraestructuras de la información y la comunicación, en otras palabras: las ICI.

El objetivo es que las interrupciones en la red y en los sistemas sean raras, de corta duración, controlables, y con el mínimo impacto. MELANI sólo puede conseguir esta tarea mediante una estrecha asociación y cooperación con dichos operadores de ICI. En esta asociación, MELANI se enfoca en compartir conocimiento y recursos que están disponibles sólo para el gobierno y no para el sector privado, en particular la información de los servicios de inteligencia (p. ej., impedir el espionaje industrial), los Equipos de Respuesta para Emergencias Informáticas (CERT) y los organismos de seguridad.

7.2.3 BUENAS PRÁCTICAS: SER INFORMADO SOBRE LAS NORMAS PARA EL INTERCAMBIO DE INFORMACIÓN

La Organización para el Intercambio de Información y la Organización del Análisis (ISAO) Organización de Estándares [ISAO] es una organización no gubernamental con sede en Estados Unidos que se creó el 1 de octubre de 2015 y cuya misión es mejorar la posición de Estados Unidos respecto a la ciberseguridad mediante la identificación de normas y directrices para un intercambio de información y un análisis riguroso y eficaz relacionado con los riesgos, incidentes y mejores prácticas en la ciberseguridad.

ISAO SO trabaja con las organizaciones existentes para el intercambio de información, los propietarios y operadores de IC, las agencias relevantes, y otros actores de los sectores público y privado a través de un proceso voluntario de desarrollo de estándares comunes para identificar un conjunto común de estándares y directrices voluntarios para la creación y funcionamiento de organizaciones dedicadas al intercambio y el análisis de información. Estos estándares se refieren, aunque no se limitan, a acuerdos contractuales, procesos empresariales, procedimientos operativos, especificaciones técnicas y protección de la privacidad.

Un documento que ha sido publicado recientemente es 'ISAO 300-1: Introducción al intercambio de información' [ISAO300-1] que proporciona una introducción al intercambio de

información sobre ciberseguridad. Este documento describe un marco conceptual para el intercambio de información, los conceptos relativos al intercambio de información, los tipos de información sobre ciberseguridad que una organización puede querer compartir, los modos en los que una organización puede facilitar el intercambio de información, así como las preocupaciones en cuanto a la privacidad y la seguridad que deben ser consideradas.

7.2.4 BUENAS PRÁCTICAS: TENER EN CUENTA LA GUÍA PARA EL INTERCAMBIO DE INFORMACIÓN SOBRE CIBERAMENAZAS

El Instituto Nacional de Estándares y Tecnología (NIST) ha editado la Publicación Especial del NIST 800-150 Guía para las Ciberamenazas en el Intercambio de Información [Johnson2016]. La información sobre ciberamenazas es toda información que pueda ayudar a una organización a identificar, evaluar, monitorizar y responder a ciberamenazas. La información sobre ciberamenazas incluye indicadores de compromiso; tácticas, técnicas, y procedimientos usados por los actores de amenazas; acciones sugeridas para detectar, contener o prevenir ataques; y los resultados de los análisis de los incidentes. Las organizaciones que comparten información sobre ciberamenazas pueden mejorar sus propias posiciones respecto a la seguridad y las de otras organizaciones.

Esta publicación proporciona directrices para crear y participar en relaciones para el intercambio de información sobre ciberamenazas. Esta guía ayuda a las organizaciones a establecer objetivos para el intercambio de información, identificar fuentes de información de ciberamenazas, examinar actividades relativas al intercambio de información, desarrollar normas para controlar la publicación y distribución de información sobre amenazas, interactuar con las comunidades de intercambio de información existentes, y hacer un uso eficaz de la información sobre amenazas para apoyar las prácticas globales en ciberseguridad de la organización.

7.2.5 BUENAS PRÁCTICAS: EL ´BUDDYING SYSTEM´ O ´SISTEMA DE AMISTAD´

Los países con políticas y capacidades para la PICI bien desarrolladas pueden tener contactos con otros países que acaban de empezar a dar sus primeros pasos en el camino de la PICI. Sin embargo, esta sensibilización no siempre está específicamente centrada, o coordinada, en la PICI. Podría ser beneficioso considerar una relación de ´amistad´ bilateral o multilateral más estrecha. Se podrían ofrecer recursos y conocimiento a los países con políticas y actividades menos desarrolladas, que podrían aprender del país ´amigo´ en lo que se refiere a enfoques valiosos en cuanto a la organización y el proceso, y los errores que se deben evitar. Así, su recorrido en la PICI puede ser más rápido que si hacen solos el camino. Antes de seleccionar un país ´amigo´, es aconsejable considerar si ya existe una coincidencia entre los países, salvando las diferencias en las estructuras jurídicas y otras estructuras de gobierno, lingüísticas, etc.

Ofrecerse a ser un país guía, cuando dicho país está por delante de otros en cuanto a la PICI, también aporta beneficios. El país ´amigo´ puede hacer preguntas relativas a la PICI que el país guía puede no haber considerado aún. Además, una PICI reforzada en el país ´amigo´

crea un nodo ICI más seguro en el ciberespacio. Al mismo tiempo, los países guía deberían garantizar la coordinación con los ministerios y agencias competentes en sus países y la concesión de las autorizaciones pertinentes antes de ponerse en contacto con un potencial ´amigo´ No obstante, es posible iniciar conversaciones informales para una ´amistad´ con vistas a establecer la compatibilidad e intereses mutuos, antes de que cada país decida desarrollar una relación ´amistosa´ más formal.

El Proceso Meridian [Meridian] ha anunciado una propuesta de ´amistad´ mediante la cual un país puede considerar participar como ´amigo´ (o como país guía). La Conferencia Meridian anual ha sido diseñada para facilitar las primeras etapas informales de ´amistad´ a través de la creación de un entorno fiable para los países de todo el mundo en el que puedan conocerse y explorar sus similitudes y objetivos. Creando una etapa informal de ´amistad´ puede suceder que dos países consideren una relación más estrecha y formal de amistad más adelante. Sin embargo, los enfoques de amistad en la PICI, ya sean bilaterales o multinacionales, p. ej., mediante la colaboración regional sobre la PICI, también pueden funcionar. Además, no existe ninguna razón por la cual un país no pueda tener más de un amigo, que le preste ayuda en diferentes aspectos del desarrollo de la PICI, o le proporcione la posibilidad de obtener consejo y experiencia. Prácticas actuales para el desarrollo de estrategias de ciberseguridad como las realizadas por la Unión Africana (UA) y la Organización de Estados Americanos (OEA) puede utilizarse como un paso intermedio.

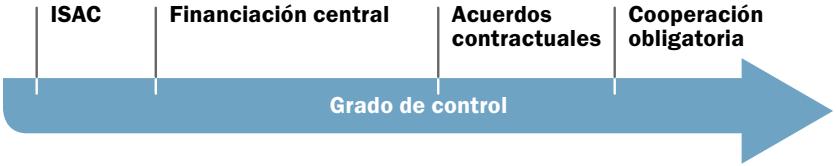


Figura 12. Grado de control en CPP (Fuente: [RECIPE]).

Algunos de los beneficios que la CPP puede aportar a la PIC/PICI son:

1. Una CPP más fuerte influirá positivamente en la capacidad de los operadores de IC/ICI que participen para gestionar las consecuencias de un desastre.
2. Mejoras en la resiliencia de las IC/ICI harán que mejore positivamente la resiliencia de la cadena de suministro.
3. Una mayor capacidad para mantener la continuidad de las operaciones, que tiene como resultado niveles más altos de servicio y confianza entre los proveedores de servicios y los clientes.
4. Un mayor nivel de comprensión de cómo las dependencias entre sectores afectan a las respuestas a las emergencias, lleva a mejores niveles de preparación y respuesta en caso de interrupciones, y acorta la duración hasta la recuperación total.
5. La cooperación puede llevar a reducir el riesgo para todas las organizaciones involucradas.
6. La cooperación puede ayudar a reducir los gastos para todas las organizaciones involucradas.

Si bien no existe un formato que garantice el éxito a la hora de crear una CPP, hay determinados factores que son de la mayor importancia para un PPP de éxito. Estos factores son:

- Confianza: dado que la CPP en CIP/PICI a menudo tiene que ver con temas delicados (comercialmente, en términos de reputación, seguridad, traspaso de responsabilidades), es esencial crear un clima de confianza en la que todas las organizaciones tengan en cuenta la necesidad de cada una de discreción y actúen en consecuencia y de manera coherente. Unas directrices claras de membresía sobre las normas de aplicación pueden ayudar a crear un clima de confianza, p. ej., [FS-ISAC].
- Valor: la participación en una CPP debe reportar beneficios, de otro modo el entusiasmo por participar de desvanecerá en seguida.
- Respeto: todas las organizaciones tiene que reconocer y respetar el valor añadido que aportan las otras organizaciones a la colaboración. Esto puede conseguirse 'vendiendo' el propio valor añadido (en los términos del socio) al tiempo que se busca activamente al valor añadido de los socios.
- Código de conducta: es necesario que haya normas claras, específicas y predecibles que no dejen lugar a la discreción e impidan cualquier conflicto de intereses;
- Conocimiento de las posibilidades y las limitaciones de cada uno de los socios: esto evita el conflicto a causa de una interpretación errónea de la causa de una respuesta negativa y permite un óptimo retorno de los esfuerzos de la alianza. Esto implica que ambas organizaciones deberían conocer a qué se dedica cada una. Una buena manera de conseguirlo es que hayan trabajado juntas durante un largo periodo de tiempo, preferentemente años.
- Expectativas realistas: todas las organizaciones tiene que tener en cuenta la asequibilidad a los recursos, el presupuesto para r desarrollo, etc., para poder forjar expectativas realistas de la CPP.

7.2.7 BUENAS PRÁCTICAS: CONSEJO DE CIBERSEGURIDAD A NIVEL NACIONAL

Algunos países han establecido comités de alto nivel para formular recomendaciones a los gobiernos, pero también al sector privado. Un ejemplo de ello es el Consejo de Ciberseguridad de Holanda (Nederlandse Cyber Security Raad, [CSR]). El Consejo de Ciber Seguridad es un órgano asesor nacional e independiente a nivel estratégico del gobierno holandés e incluye a representantes de organizaciones públicas y privadas y de la comunidad científica en el ámbito de la ciberseguridad, incluidas las ICI. El CSR trabaja para mejorar la ciberseguridad en Holanda en el nivel estratégico.

Debido a la composición única del Consejo (privado-público-científico), puede considerar prioridades, obstáculos e incidentes desde varios ángulos y desarrollar una visión global de las oportunidades y amenazas. El CSR busca prestar asesoramiento que tiene un fundamento teórico y puede llevarse a la práctica.

Se han encomendado al Consejo las siguientes funciones:

- Proporcionar consejo, tanto solicitado como no solicitado, al gobierno y a las partes privadas sobre avances relevantes en ciberseguridad. El Consejo asesora al gobierno sobre la implementación y ejecución de la Estrategia Nacional de Ciberseguridad.

- Proponer temas prioritarios sobre la ciberseguridad, para, entre otras cosas, armonizar los programas de investigación gubernamentales entre ellos y, en la medida de lo posible, con los de los centros de investigación científica y el sector empresarial.
- Contribuir al Programa Nacional para la Investigación en Ciberseguridad.
- Contribuir a salvaguardar la cooperación público-privada.
- Asesorar a la organización de respuesta ante emergencias holandesa en caso de que se produzcan incidentes a gran escala.

La participación de actores privados en el CSR no es esencial para crear un órgano de un nivel tan alto sobre PICI/ciberseguridad a nivel nacional, aunque refleja una mentalidad CPP y es un buen ejemplo de los beneficios de una CPP y de la variedad de formas en que se puede implementar.

7.2.8 BUENAS PRÁCTICAS: TRAFFIC LIGHT PROTOCOL (TLP)

Con el fin de establecer el nivel de confianza necesario para el intercambio de información entre organizaciones públicas y privadas, es necesario establecer procedimientos sobre cómo manejar información confidencial de un modo fiable.

El Traffic Light Protocol (TLP) proporciona un método muy sencillo para establecer el nivel necesario de confidencialidad que requiere la información compartida. Uno de los principios esenciales del TLP es que quien facilite información confidencial establecerá también si dicha información debe ser divulgada y hasta qué punto debe serlo.

El emisor de la información puede etiquetar dicha información con uno de cuatro colores.

- **ROJO – De uso privado, para destinatarios concretos únicamente.** En el contexto de una reunión, por ejemplo, la información de nivel ROJO se limita a aquellos presentes en la misma. En la mayoría de los casos, la información de nivel ROJO se comunicará verbalmente o en persona.
- **ÁMBAR – Distribución limitada.** Los destinatarios pueden compartir la información de nivel ÁMBAR con otros miembros de la organización, sólo bajo el criterio de "necesidad de conocer". Puede esperarse del emisor que especifique los límites previstos para dicho intercambio.
- **VERDE – De ámbito comunitario.** La información manejada en esta categoría puede circular extensamente dentro de una comunidad específica. Sin embargo, la información no puede publicarse o divulgarse públicamente en Internet, ni difundirse fuera de la comunidad.
- **BLANCO – Información de uso no restringido.** Sujeta a las normas estándar sobre derechos de autor, la información de nivel BLANCO puede distribuirse libremente, sin restricciones.

El TLP es utilizado ampliamente, tanto por países como por grupos de trabajo multinacionales. Su punto fuerte es que es muy fácil de utilizar y que la responsabilidad del emisor y del receptor sobre la información está muy clara. Cabe señalar que una ley o norma de la Ley de Libertad de Información (FOIA) puede anular el TLP (véase [Luiijf2015]).

El Foro de Equipos de Respuesta a Incidentes y Seguridad (FIRST) ha anunciado el lanzamiento de la versión 1.0 de su ya consolidado Traffic Light Protocol (TLP).

El FIRST TLP aborda algunas de las críticas que algunos usuarios hacían de la versión anterior, y garantiza que el intercambio internacional pueda llevarse a cabo sin expectativas frustradas. En la actualidad es utilizado por varios tipos de CSIRT, comunidades operativas fiables, organizaciones para el análisis del intercambio de información, agencias gubernamentales e investigadores privados, y ha conseguido de hecho un estatus de normativa internacional.

La comunidad FIRST, en consulta con otras comunidades de intercambio de información, ha establecido un Grupo de interés especial sobre normativas (SIG) para el TLP. El TLP SIG ha elaborado un conjunto de definiciones comunitarias normalizadas para todos los colores del TLP, junto con una guía de empleo clara en la que se explica cómo, cuándo y dónde se debe utilizar [FIRST].

7.3 BIBLIOGRAFÍA Y LECTURAS RECOMENDADAS

[CISP] Página web del Centro Nacional de Ciberseguridad (NCSC) del Reino Unido sobre 'Alianza para la ciberseguridad en el intercambio de información (CiSP)'. *Online:* https://www.ncsc.gov.uk/cisp

[CPNI IE] Página web del Reino Unido para los intercambios de información en el CPNI. *Online:* http://www.cpni.gov.uk/about/Who-we-work-with/Information-exchanges/

[CSR] Página web del NCSC sobre el 'Consejo de Ciberseguridad' de Holanda. *Online:* https://www.ncsc.nl/english/Cooperation/cyber-security-council.html

[EGC] Página web de los CERT de los gobiernos europeos (EGC). *Online:* http://www.egc-group.org

[ENISA] L. Dupré, M. Falessi, D. Liveri, Good Practice Guide on Cooperative Models for Effective PPPs, ENISA 2011. [L. Dupré, M. Falessi, D. Liveri, Guía de buenas prácticas sobre modelos de cooperación para una CPP eficaz, ENISA 2011]. *Online:* www.enisa.europa.eu/publications/good-practice-guide-on-cooperatve-models-for-effective-ppps

[EuroSCSIE] Página web de EuroSCSIE: https://espace.cern.ch/EuroSCSIE/default.aspx

[FIRST] Sitio web del 'Foro de equipos de respuesta a incidentes y seguridad'. *Online:* http://www.first.org/tlp

[FS-ISAC] Normas operativas del Centro de Análisis e Intercambio de Información sobre Servicios Financieros. (FS-ISAC), junio, 2016, *Online:* https://www.fsisac.com/sites/default/files/FS-ISAC_OperatingRules_June2016.pdf

[ICS-CERT] Página web del ICS- CERT. *Online:* https://ics-cert.us-cert.gov

[Infraguard] Sitio web de Infraguard (CPP entre IC y el FBI). *Online:* https://www.infragard.org/

[ISAO] La Organización de Estándares ISAO es una organización no gubernamental. *Online:* https://www.isao.org/

[ISAO300-1] ISAO 300-1: Introduction to Information Sharing, ISAO, September 2016. [ISAO 300-1: Introducción al intercambio de información, ISAO, septiembre 2016]. *Online:* https://www.isao.org/wp-content/uploads/2016/10/ISAO-300-1-Introduction- to-Information-Sharing-v1-01_Final.pdf

[Johnson2016] C. Johnson, L. Badger, D. Waltermire, J. Snyder, C. Skorupka, NIST Special Publication 800-150 Guide to Cyber Threat Information Sharing, National Institute for Standards and Technology, October 2016. [C. Johnson, L. Badger, D. Waltermire, J. Snyder, C. Skorupka, Publicación especial del NIST 800-150 Guía de las ciberamenazas en el intercambio de información, Instituto Nacional de Estándares y Tecnología, octubre 2016]. *Online:* http://nvlpubs.ist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

[Luiijf2015] Luiijf, H.A.M., Kernkamp, A., GCCS: Sharing Cyber Security Information, TNO, 2015. [Luiijf, H.A.M., Kernkamp, A., GCCS: Compartiendo información en ciberseguridad, TNO, 2015]. *Online:* http://publications.tno.nl/publication/34616508/oLyfG9/luiijf-2015-sharing.pdf

[MELANI] Confederación Suiza, Centro de Información y Análisis para la Garantía de la Información MELANI. *Online:* https://www.melani.admin.ch/melani/en/home.html

[NCSC] Página web NCS sobre Centros para el Intercambio y Análisis de Información (ISACS). *Online:* https://www.ncsc.nl/english/Cooperation/isacs.html

[NISC.JP2014] The Basic Policy of Critical Information Infrastructure Protection (3rd Edition) – tentative translation, Japan, 2014. [Política básica de la Protección de Infraestructuras Críticas de Información (3ª edición) – traducción orientativa, Japón, 2014]. *Online:* http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3_pdf

[RECIPE] M. Klaver, E. Luiijf, A. Nieuwenhuijs, Good Practices Manual for CIP Policies for policy makers in Europe, TNO, 2011. [M. Klaver, E. Luiijf, A. Nieuwenhuijs, Manual de buenas prácticas para políticas PIC para responsables políticos en Europa, TNO, 2011]. *Online:* http://www.tno.nl/recipereport

[UP KRITIS] CPP UP KRITIS de Alemania 'Industrie und Kritische Infrastrukturen' [´Infraestructuras industriales y críticas´]. *Online:* htpps://ww.bsi.bund.de/DE/Themen/Industrie_KRITIS/Aktivitaeten/UP_KRITIS/up_ kritis_node.html

[US CERT] Página web del Equipo de Respuesta a Emergencias Informáticas de Estados Unidos (US CERT). *Online:* whttp://ww.us-cert.gov

8 LISTA DE ABREVIATURAS

AAC	Autoridad de Certificación
B2B	Business to business [de empresa a empresa]
CERT	Computer Emergency Response Team [Equipo de Respuesta ante Emergencias Informáticas]
CIR	Critical Infrastructure Resilience [Resiliencia de las Infraestructuras Críticas]
CIIR	Critical Information Infrastructure Resilience [Resiliencia de las Infraestructuras Críticas de Información]
CPP	Cooperación Público-Privada
CPS	Cyber-Physical System [Sistema Ciberfísico]
CSIRT	Computer Security Incident Response Team [Equipos de Respuesta a Incidentes de Seguridad Informática]
CSISP	Cyber-Security Information Sharing Partnership [Alianza para la ciberseguridad en el intercambio de información]
CTO	Commonwealth Telecommunication Organisation [Organización de Telecomunicaciones de la Commonwealth]
CVE	Common Vulnerabilities and Exposures [Vulnerabilidades y exposiciones comunes]
DCS	Distributed Control System [Sistema de control distribuido]
EGC	European Governments CERTs [CERT de los gobiernos europeos]
ENISA	European Union Agency for Network and Information Security [Agencia Europea de Seguridad de las Redes y de la Información]
FIRST	Forum for Incident Response and Security Teams [Foro de equipos de respuesta a incidentes y seguridad]
FOIA	Freedom of Information Act [Ley de Libertad de Información]
GFCE	Global Forum on Cyber Expertise [Foro Global de Experiencia Cibernética]
GLONASS	Globalnaya Navigatsionnaya Sputnikovaya [Sistema de Navegación Global por Satélite]
GPS	Global positioning system [Sistema de Posicionamiento Global]
G2G	Government to government [de gobierno a gobierno]
IACS	Industrial Automation and Control Systems [Sistemas de Control Industrial y Automatización]
IC	Infraestructura crítica
ICI	Infraestructura Crítica de Información
ICS	Industrial Control Systems [Sistemas Industriales de Control]
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team [Sistema de control industrial- Equipo de Respuesta ante Emergencias Informáticas]
IX(P)	Internet Exchange (Points) [Puntos de Intercambio de Internet]
NCSC	National Cyber Security Centre [Centro Nacional de Seguridad Cibernética]
NCSS	National Cyber Security Strategy [Estrategia Nacional de Seguridad Cibernética]
NIAC	National Infrastructure Advisory Council [Consejo Asesor de Infraestructura Nacional]
OCDE	Organización para la Cooperación y el Desarrollo Económicos

OEA	Organización de Estados Americanos
ONG	Organización No Gubernamental
PCS	Process Control System [Sistema de Control de Procesos]
PDCA	Plan-Do-Check-Action [Planeamiento, Ejecución, Verificación y Acción]
PIC	Protección de Infraestructuras Críticas
PICI	Protección de Infraestructuras Críticas de Información
SCADA	Supervisory Control and Data Acquisition [Sistema Supervisor de Control y Adquisición de Información]
TIC	Tecnologías de la Información y las Comunicaciones
TLP	Traffic Light Protocol
UA	Unión Africana
UIT	Unión Internacional de Telecomunicaciones: Agencia especializada de las Naciones Unidas para las Tecnologías de la Información y la Comunicación – TIC]

COLOFÓN

AUTORES

Señor Eric Luiijf
Señor Tom van Schie
Señor Theo van Ruijven
Señor Auke Huistra

TNO

Lange Kleiweg 137
2288 GJ Rijswijk
Holanda
eric.luiijf@tno.nl
TNO.NL

Con colaboraciones de señor Peter Burnett (Coordinador de Meridian) y señora Nynke Stegink (Dutch NCSC), y señor Martijn Neef (TNO).

Esta guía de buenas prácticas ha sido elaborada por GFCE-Meridian. La versión digital de esta guía de buenas prácticas está disponible para descargarse en: www.tno.nl/gcPICI

MERIDIAN

El Proceso Meridian tiene como objetivo intercambiar ideas e iniciar acciones para la cooperación de organismos gubernamentales en temas de Protección Infraestructura de Información Crítica (PICI) a nivel mundial. Explora los beneficios y oportunidades de la cooperación entre los gobiernos y ofrece una oportunidad para compartir las mejores prácticas de todo el mundo.

El Proceso Meridian reconoce que sólo trabajando juntos podemos avanzar en cada uno de nuestros objetivos y metas nacionales respecto a la PICI). / reconoce como premisa fundamental el hecho de que únicamente un esfuerzo conjunto nos permitirá avanzar en nuestros objetivos PICI nacionales.

La participación en el Proceso Meridian está abierta a todos los países / economías y está dirigida a altos responsables gubernamentales involucrados en asuntos relacionados con PICI. Se invita a cada país / economía a participar en el Proceso Meridian, y se le anima a asistir a la Conferencia Meridian anual [www.meridianprocess.org].

GFCE

El Foro Global de Experiencia Cibernética (GFCE) es una plataforma global para países, organizaciones internacionales y empresas privadas para intercambiar las mejores prácticas y experiencias en la construcción de capacidades cibernéticas. El objetivo es identificar políticas, prácticas e ideas que hayan tenido éxito y multiplicarlas a un nivel mundial.

Junto con socios pertenecientes a ONG, a la comunidad tecnológica y al mundo académico, los miembros del GFCE desarrollan iniciativas prácticas para mejorar la capacidad cibernética [www.thegfce.com/].

Noviembre 2016

Esta guía ha sido patrocinado por el Gobierno Holandés.