Unión Internacional de Telecomunicaciones

CUESTIÓN 22/1

Informe Final

UIT-D COMISIÓN DE ESTUDIO 1 4.º PERIODO DE ESTUDIOS (2006-2010)

CUESTIÓN 22/1:

Garantía de seguridad en las redes de información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad

LAS COMISIONES DE ESTUDIO DEL UIT-D

De acuerdo con lo dispuesto en la Resolución 2 (Doha, 2006), la CMDT-06 mantuvo dos Comisiones de Estudio y determinó las Cuestiones que éstas habrían de tratar. Los procedimientos de trabajo que han de aplicar dichas Comisiones de Estudio se definen en la Resolución 1 (Doha, 2006) adoptada por la CMDT-06. Para el periodo 2006-2010, se encomendó a la Comisión de Estudio 1 el estudio de nueve Cuestiones en el ámbito de las estrategias y políticas para el desarrollo de las telecomunicaciones. A la Comisión de Estudio 2 se le encomendó el estudio de diez Cuestiones en el ámbito del desarrollo y la gestión de los servicios y redes de telecomunicaciones, y aplicaciones de las TIC.

Para toda información

Sírvase ponerse en contacto con:

Sr. Souheil MARINE/Sra. Christine SUND
Oficina de Desarrollo de las Telecomunicaciones (BDT)
UIT
Place des Nations
CH-1211 GINEBRA 20
Suiza
Teléfono: +41 22 730 5323/5203
Fax: +41 22 730 5484
E-mail: souheil.marine@itu.int
christine.sund@itu.int

Para solicitar las publicaciones de la UIT

No se admiten pedidos por teléfono. En cambio, pueden enviarse por telefax o e-mail.

UIT
Servicio de Ventas
Place des Nations
CH-1211 GINEBRA 20
Suiza
Fax: +41 22 730 5194
E-mail: sales@itu.int

Librería electrónica de la UIT: www.itu.int/publications

UIT-D COMISIÓN DE ESTUDIO 1 4.° PERIODO DE ESTUDIOS (2006-2010)

CUESTIÓN 22/1:

Garantía de seguridad en las redes de información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad

DECLINACIÓN DE RESPONSABILIDAD

En la elaboración del presente Informe han participado muchos voluntarios, provenientes de diversas administraciones y empresas. Cualquier mención de empresas o productos concretos no implica en ningún caso un apoyo o recomendación por parte de la UIT.

ÍNDICE

Página

Introducción 1

PARTE I – Formulación y obtención de un acuerdo sobre la estrategia nacional de ciberseguridad 6

I.A Visión general de las Metas correspondientes a esta Parte 7

I.B Medidas específicas para lograr estas Metas 7

PARTE II – Establecimiento de relaciones de colaboración entre el Estado y el sector privado 11

II.A Visión general de las Metas correspondientes a esta Parte 12

II.B Medidas específicas para lograr estas Metas 12

PARTE III – Disuasión del ciberdelito 15

III.A Visión general de la Meta correspondiente a esta parte 15

III.B Medidas específicas para lograr esta Meta 15

PARTE IV – Creación de capacidades nacionales de gestión de incidentes: vigilancia, advertencia, respuesta y recuperación 21

IV.A Visión general de las Metas correspondientes a esta Parte 21

IV.B Medidas específicas para lograr estas Metas 21

PARTE V – Promoting A National Culture of Cybersecurity 25

V.A Visión general de la Meta correspondiente a esta Parte 25

V.B Medidas específicas para lograr esta Meta 26

Apéndice 1 – Lista de acrónimos 29

Apéndice 2 – Estrategia para hacer efectiva la cooperación en materia de ciberseguridad y medición de su eficacia 31

Anexo A – Estudio de Caso: Spam 34

Anexo B – Gestión de Identidades 48

Anexo C – Enlaces y referencias 60

CUESTIÓN 22/1

Introducción

En el presente Informe se ofrece a las administraciones un panorama general de los módulos esenciales necesarios para abordar el tema de la ciberseguridad en el plano nacional, así como para estructurar su enfoque en materia de ciberseguridad nacional[1]. Dado que las capacidades nacionales varían y las amenazas que se plantean se encuentran en constante evolución, en el Informe no se proporciona una receta prescriptiva para proteger la seguridad del ciberespacio. En lugar de ello, se ha preferido describir un enfoque flexible aplicable para ayudar a las administraciones nacionales a revisar y mejorar sus instituciones, políticas y relaciones sobre ciberseguridad. Aunque el presente Informe se centra en la ciberseguridad, hay que señalar que la protección de la red física es una prioridad que reviste igual importancia. Hay que indicar también que las prácticas óptimas en materia de ciberseguridad deben proteger y respetar las disposiciones en materia de privacidad y libertad de expresión, tal como se recogen en las disposiciones relevantes de la Declaración de los Derechos Humanos y en la Declaración de Principios de Ginebra[2].

Los elementos clave del presente Informe son los siguientes:

- Elaboración de una estrategia nacional de ciberseguridad.
- Establecimiento de relaciones de colaboración entre el Estado y el sector privado en el plano nacional.
- Disuasión del ciberdelito.
- Creación de capacidades nacionales para la gestión de incidentes.
- Promoción de una cultura nacional de ciberseguridad.

Cada uno de estos elementos debe ser parte integral de un enfoque nacional completo en materia de ciberseguridad. El orden en el que se enumeran no es indicativo de orden de prioridad entre los elementos. Podría haber otros basados en el contexto nacional.

A los efectos del presente Informe, por ***ciberseguridad*** se entiende, tal como se define en la Recomendación UIT-T X.1205, el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes:

- Disponibilidad.
- Integridad, que integridad, que puede incluir la autenticidad y el no repudio.
- Confidencialidad.

Es importante entender la relación existente entre la ciberseguridad, la infraestructura esencial (CI, critical infrastructures), la infraestructura de información esencial (CII, critical information infrastructure), la protección de la infraestructura de información esencial (CIIP, critical information infrastructure protection) y la infraestructura no esencial. Esta relación queda ilustrada en la Figura 1.

---

1 Se invita a los lectores interesados a considerar el resultado de ISO 27001 a 27003.

2 Véase CMSI, Agenda de Túnez para la Sociedad de la Información, párrafo 42.

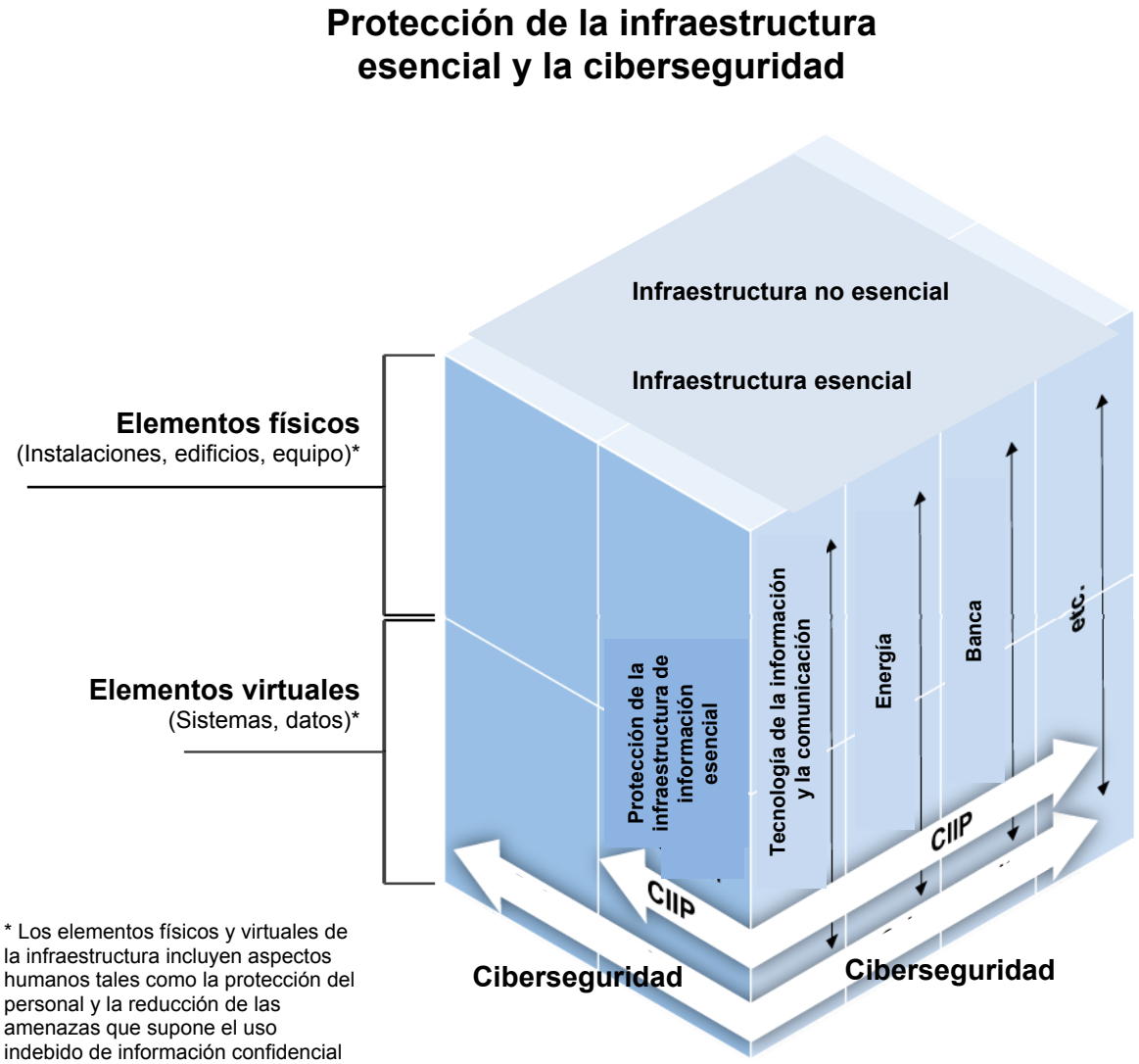
Aunque las definiciones pueden variar ligeramente, por ***infraestructuras esenciales*** (CI) se entiende por regla general los sistemas, servicios y funciones fundamentales cuya perturbación o destrucción puede afectar adversamente la salud y la seguridad públicas, el comercio y la seguridad nacional, o cualquier combinación de los mismos. Las infraestructuras esenciales están integradas por elementos físicos tales como facilidades y edificios, y elementos virtuales, por ejemplo, sistemas y datos (véase la Figura 1). El significado del término "esencial" puede variar según sea el país considerado, pero normalmente incluye elementos de la tecnología de la información y la comunicación, incluyendo las telecomunicaciones, (TIC) y los sectores de la energía, banca, transporte, salud pública, agricultura y alimentación, suministro de agua, industria química, industria naviera y servicios públicos esenciales. En todas sus etapas de desarrollo, los países deben planificar y elaborar políticas que protejan lo consideren sus infraestructuras esenciales (en otras palabras, protección de la infraestructura esencial, incluida la protección física y virtual), para garantizar un nivel razonable de resistencia y seguridad de tales infraestructuras y así contribuir al logro de los objetivos y la estabilidad económica nacionales.

Si bien cada uno de los sectores económicos mencionados cuenta con sus propios activos físicos, por ejemplo, los edificios bancarios, las plantas de generación eléctrica, los trenes, los hospitales y las oficinas públicas, dichos sectores esenciales de la economía de un país dependen de las tecnologías de la información y la comunicación. En todas partes, dichos sectores y sus activos físicos dependen actualmente del funcionamiento fiable de esta ***infraestructura de información esencial*** (CII), para prestar los servicios y realizar las actividades comerciales necesarias. Así pues, una perturbación apreciable de la CII no sólo afectaría el sector de las TIC, pues incidiría también de forma inmediata y adversa en la capacidad de un país para desempeñar sus políticas esenciales en muchos sectores. Un programa de ***protección de la infraestructura de información esencial*** (CIIP) protege el componente virtual de la CII.

Tal como se indica en la Figura 1, la CIIP es un subconjunto de la CIP y de la ciberseguridad. La ciberseguridad protege contra todo tipo de ciberincidentes, fortaleciendo la seguridad de la infraestructura de información esencial, infraestructura de la cual dependen sectores cruciales y garantizando la seguridad de las redes y los servicios que atienden a las necesidades diarias de los usuarios. Los ciberincidentes pueden incidir en infraestructuras de información esenciales y no esenciales y adoptar muchas formas de actividad maliciosa, por ejemplo, la utilización de redes robot para llevar a cabo ataques de denegación de servicio y difundir correo electrónico basura y soporte lógico perjudicial (virus, gusanos, etc.) que reduzcan la capacidad de funcionamiento de las redes. Además, los ciberincidentes pueden incluir actividades ilícitas tales como la peska o hurto de identidades y credenciales financieras (phishing) y la kosecha o clonación de servidores de nombres de dominio (kosecha o pharming) así como el robo de identidad. Aunque es cierto que sigue aumentando el número de ciberamenazas, y la capacidad y refinamiento técnicos de los ciberdelincuentes, también lo han hecho las herramientas y metodologías necesarias para combatirlos. Hay que añadir que todos los países, con independencia del grado de desarrollo en que se encuentren, han experimentado dichos ciberincidentes.

Una de las funciones de un enfoque nacional respecto a la ciberseguridad es promover conciencia entre el público acerca de la existencia del ciberriesgo, así como crear estructuras para abordar la ciberseguridad y establecer las relaciones necesarias para afrontar los eventos que puedan producirse. Evaluar el riego, adoptar medidas de mitigación, y gestionar las consecuencias, son también elementos de un programa nacional de ciberseguridad. Un buen programa de ciberseguridad nacional contribuirá a proteger el funcionamiento normal de la economía de un país, a promover la continuidad de la planificación en todos los sectores, proteger la información almacenada en los sistemas de información, preservar la confianza pública, mantener la seguridad nacional y garantizar la salud y la seguridad públicas.

Figura 1: Relación conceptual entre la protección de la infraestructura de información esencial y la ciberseguridad



La mejora de la ciberseguridad no puede quedar limitada a una estrategia nacional, aunque ésta constituya un factor muy importante, sino que debe completarse con estrategias de ámbitos regional y global, tal como se recoge en los resultados de las dos fases de la CMSI (2003 y 2005) y en la subsiguiente Línea de Acción C5 basada en los epígrafes 35 y 36 de la Declaración de Principios de Ginebra y en el epígrafe 39 de la Agenda de Túnez, así como en la implementación de los acuerdos de la Cumbre Mundial de la Sociedad de la Información a través de sus Resoluciones, Acciones e Iniciativas pertinentes adoptadas por la UIT, tales como:

a) Meta 4 de la Resolución 71 de la Conferencia de Plenipotenciarios (Rev. Antalya 2006), "Plan Estratégico de la Unión para 2008-2011".

b) Resolución 130 de la Conferencia de Plenipotenciarios de la UIT (Rev. Antalya 2006), "Fortalecimiento del papel de la UIT en la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación".

c) Las partes relevantes del Plan de Acción de Doha de la CMDT-06, incluyendo el Programa 3 sobre ciberestrategias y aplicaciones de las TIC que identifican la ciberseguridad como una prioridad para la BDT, con una serie de actividades definidas y, en particular, la adopción de la Resolución 45 (Doha, 2006) "Mecanismos para mejorar la cooperación en materia de ciberseguridad, incluida la lucha contra el correo indeseado" La Resolución 45 encarga al Director de la BDT a que organice reuniones para considerar a manera de mejorar la ciberseguridad, con inclusión, entre otras cosas, de un Memorándum de Entendimiento (MoU) entre los Miembros para mejorar la ciberseguridad y combatir el correo indeseado, y notificar el resultado de dichas reuniones a la Conferencia de Plenipotenciarios de 2006. El Informe de la BDT a la Conferencia de Plenipotenciarios de 2006 puede encontrarse en www.itu.int/md/S06-PP-C-0024/en[3].

d) El amplio trabajo realizado por la Comisión de Estudio 17 del UIT-T, Comisión líder en materia de ciberseguridad, y las actividades complementarias de la Comisión de Estudio 13.

e) La reciente Resolución 58 adoptada por la AMNT (Johannesburgo, 2008), titulada " Fomento de la creación de equipos nacionales de intervención en caso de incidente informático, especialmente para los países en desarrollo", que ha reconocido el trabajo realizado en el seno de la Cuestión 22/1 del UIT-D.

f) El Informe del Presidente del Grupo de Expertos de Alto Nivel a la Agenda sobre Ciberseguridad Global de la UIT (GEANC) lanzada por el Secretario general el 17 de mayo de 2007 hace una reseña de las propuestas de expertos sobre las siete Metas estratégicas principales de la iniciativa, con especial atención en las Recomendaciones pertinentes sobre las cinco áreas de trabajo siguientes:

- Medidas legales.
- Medidas técnicas y de procedimiento.
- Estructuras institucionales.
- Creación de capacidades.
- Cooperación internacional.

Entre dichas áreas de trabajo, la relativa a "Medidas legales" se ocupa sobre cómo abordar los desafíos legislativos de las actividades criminales cometidas en las redes de las TIC en un ámbito internacional. Las "Medidas técnicas y de procedimiento" se centran en medidas fundamentales para promover la adopción de enfoques reforzados que mejoren la seguridad y la gestión del riesgo en el ciberespacio, incluyendo esquemas de acreditación, protocolos y normas. La relativa a "Estructuras institucionales" se centra en la prevención, detección, respuesta y gestión de crisis ante ciberataques, incluyendo la protección de los sistemas de infraestructura de información esencial. La "Creación de capacidades" se centra en la elaboración de estrategias para que los mecanismos de creación de capacidades contribuyan a promover conciencia, transferencia de conocimiento y aumento de la ciberseguridad en las respectivas agendas políticas nacionales. Finalmente, la "Cooperación internacional" se centra en promover la cooperación internacional, el diálogo y la coordinación en la respuesta a las ciberamenazas.[4, 5]

g) El proyecto de Opinión 4 adoptado recientemente por Foro Mundial de Política de las Telecomunicaciones (FMPT) de 2009 sobre "Estrategias cooperativas para crear confianza y seguridad en cuanto a la utilización de las TIC"[6], señalando en particular las secciones invita a la UIT e invita a los Estados Miembros.

---

[3] Sobre la base de la experiencia adquirida en los últimos cuatro años, los Estados Árabes están convencidos de que la mejor solución para atender las necesidades mundiales y/o regionales es la concertación de un Memorándum de Entendimiento entre los Estados Miembros con el fin de realzar la ciberseguridad y combatir el correo basura.

[4] Los Expertos de los Estados Árabes manifestaron su acuerdo con todas las Recomendaciones contenidas en el Informe del Presidente del GEAN.

[5] El sitio electrónico www.itu.int/osg/csd/cybersecurity/gca/docs/Report_of_the_Chairman_of_HLEG_to_ITU_SG_03_sept_08.pdf contiene detalles sobre el Informe del Presidente del GEAN.

[6] El texto completo del proyecto de Opinión 4 del FMPT figura en www.itu.int/osg/csd/wtpf/wtpf2009/documents/opinion4.pdf

h) Las actividades de la BDT relativas al Programa 3 (ciberaplicaciones), ya sea mediante asistencia directa a Estados Miembros de países en desarrollo, mediante proyectos y creación de capacidad/conjuntos de herramientas de autoevaluación de la protección de información y telecomunicaciones esenciales (CIIP)/Ciberseguridad Nacional de la UIT, mediante el conjunto de herramientas de la UIT para la defensa contra las redes robot (Botnet) y el conjunto de herramientas para la implantación de equipos nacionales de intervención en caso de incidentes informáticos (CIRT).

i) En noviembre de 2008 se adoptó la Iniciativa sobre Protección de la Infancia en Línea (COP, *Child Online Protection*), como una red de colaboración internacional para fomentar la protección en línea de los niños y jóvenes de todo el mundo, mediante el suministro de orientaciones sobre un comportamiento seguro en línea, junto con otros organismos de las Naciones Unidas y Asociados. Los principales objetivos de la iniciativa COP son: 1) identificar los principales riesgos a los que están expuestos los niños y jóvenes en el ciberespacio; 2) crear conciencia acerca de los riesgos y problemas por múltiples canales; 3) elaborar herramientas prácticas para ayudar a las instituciones públicas, las organizaciones y los pedagogos a minimizar esos riesgos; y 4) intercambiar conocimientos y experiencias, al tiempo que se promueven las asociaciones estratégicas internacionales para definir y adoptar iniciativas concretas.

j) La colaboración establecida por la UIT y la Asociación Multilateral Internacional contra las Ciberamenazas (IMPACT), en el marco del Programa Mundial de la UIT sobre Ciberseguridad, destinado a agrupar a importantes interesados y asociados de los gobiernos, las empresas del sector privado y los círculos académicos, con el fin de proporcionar a los Estados Miembros de la UIT la competencia, las instalaciones y recursos necesarios para combatir con eficacia las ciberamenazas. Los principales objetivos de la colaboración entre la UIT e IMPACT son: 1) establecer un marco mundial para el control, la alerta y la respuesta frente a incidentes; 2) establecer políticas y estructuras orgánicas nacionales y regionales adecuadas, tales como los equipos nacionales de respuesta ante incidentes informáticos (CIRT); 3) promover la creación de capacidades humanas e institucionales a través de los sectores; y 4) facilitar la cooperación internacional y mundial entre múltiples interesados.

PARTE I

Formulación y obtención de un acuerdo sobre la estrategia nacional de ciberseguridad

El diseño y la implementación de un plan nacional de ciberseguridad hace necesario adoptar una estrategia global que entrañe un amplio análisis inicial de la adecuación de las prácticas nacionales de un país y la consideración de la función desempeñada por todas las partes interesadas (autoridades públicas, sector privado y ciudadanos) en este asunto.

Por motivos de seguridad nacional y para preservar el bienestar económico, los gobiernos deben posibilitar, promover y garantizar la protección de sus infraestructuras de información esenciales. Actualmente, esas infraestructuras son comunes a varios sectores industriales y sobrepasan las fronteras nacionales. La ubicuidad de las infraestructuras de información esenciales brinda muchas oportunidades y ventajas económicas.

Ahora bien, estas ventajas vienen acompañadas de interdependencias y riesgos que implican costos importantes. En un estudio encargado por la Oficina de Desarrollo de las Telecomunicaciones (BDT) de la UIT se hace el siguiente resumen de estos costos[7]:

> El soporte lógico perjudicial y el correo basura inciden en los costos e ingresos de todas las partes interesadas en la red de valor de los servicios de información como, por ejemplo los vendedores de software, los operadores de red, los proveedores de servicios Internet (PSI) y los usuarios. Estas incidencias pueden afectar, aunque no de manera exclusiva, los costos relativos a las medidas preventivas y de rehabilitación, los costos directos de la anchura de banda y los equipos, así como los costos de oportunidad en materia de congestión. Todo ello se complica aún más debido a que el correo basura y el soporte lógico perjudicial crean también nuevas corrientes de ingresos, tanto legítimas como ilegítimas, es decir propician modelos comerciales legítimos (por ejemplo, antivirus y productos para combatir el correo basura, infraestructura y anchura de banda) así como modelos comerciales de carácter delictivo (alquiler de grupos de programas informáticos robot, comisiones sobre ventas impulsadas por el envío de correo basura, acciones con precios inflados (pump and dump stock schemes, etc.). Por consiguiente, ambos crean incentivos de carácter mixto y, a veces, conflictivo para las partes interesadas, lo cual complica la búsqueda de respuestas coherentes para solucionar el problema.

Durante muchos años la mayoría de los países han considerado que la red telefónica pública conmutada (RTPC) nacional era una infraestructura esencial y, por esa razón, la han protegido. En un gran número de naciones hay empresas que detentan importantes segmentos de la infraestructura RTPC y han cooperado con el Estado entre sí para protegerla. Sin embargo, el rápido crecimiento de las TIC digitales sobrevenido en las redes de comunicaciones alámbricas e inalámbricas interconectadas ha alterado radicalmente la naturaleza de la seguridad de las redes y las correspondientes necesidades, puede hacer que las políticas y procedimientos de seguridad tradicionales basados en la RTPC resulten insuficientes para atender a las nuevas exigencias en materia de seguridad.

Los cambios a que han dado lugar las TIC exigen hacer mayor hincapié en la cooperación con los gobiernos, las empresas, otras organizaciones que diseñan, poseen, proporcionan, gestionan y utilizan sistemas y redes de información y dan servicio a los mismos. Aunque suele suceder que los gobiernos sigan desempeñando un cometido rector a la hora de establecer la política pública que debe seguirse en cuanto a la seguridad de redes, resulta indispensable garantizar que otras partes interesadas relevantes, incluidos los operadores y vendedores de infraestructura, participen en la planificación y el proceso político globales. Los gobiernos y el sector privado pueden mancomunar sus respectivos conocimientos especializados y colaborar para gestionar los riesgos que pesan sobre la CII. Esta integración promueve una mayor confianza y garantiza que

---

7 Véase el proyecto de estudio sobre "Aspectos financieros de la seguridad de las redes: Soporte lógico perjudicial y correo basura", UIT-D 1/144 (6 de mayo de 2008).

las políticas y tecnologías se diseñen y apliquen de la forma más adecuada y eficaz posible. En el plano internacional, la protección de las infraestructuras de información esenciales y el mejoramiento de la ciberseguridad requiere la cooperación y coordinación entre los Estados y los asociados internacionales.

I.A Visión general de las Metas correspondientes a esta Parte

I.A.1 Incorporar en las políticas nacionales la cuestión de la ciberseguridad/protección de las infraestructuras de la información esenciales y reconocer la necesidad de tomar medidas en el plano nacional y de cooperar internacionalmente.

I.A.2 Preparar una estrategia nacional para proteger las infraestructuras de información esenciales y el ciberespacio contra ataques electrónicos y físicos.

I.A.3 Participar en las acciones internacionales que se emprendan para coordinar las actividades nacionales relativas a la prevención, respuesta y recuperación ante incidentes y a la preparación contra los mismos.

I.B Medidas específicas para lograr estas Metas

Si bien las Metas precitadas son comunes a todos los países, las medidas específicas que habrá que tomar para implementar dichos objetivos corresponden a las necesidades y circunstancias únicas de cada país. En muchas naciones es el Estado el que deberá adoptar estas medidas.

I.B.1 Persuadir a los actores clave del Estado de la necesidad de adoptar medidas nacionales para contrarrestar las amenazas y vulnerabilidades de la ciberinfraestructura nacional mediante debates de política.

1) En el caso de un país que desee garantizar la seguridad de sus infraestructuras de información esenciales, el primer paso será decretar que la ciberseguridad es un asunto de política nacional. Por regla general, en una declaración nacional de política de ciberseguridad: 1) se reconoce la importancia de la CII para el país; 2) se identifican los riesgos que pesan sobre la CII (normalmente en el marco de un enfoque contra todos los peligros que puedan plantearse[8]); 3) se definen los objetivos de la política de ciberseguridad; y 4) se señala en líneas generales la forma de llevar a la práctica la declaración, entre otras cosas, colaborando con las partes interesadas relevantes.

   Una vez que se haya definido la política global de ciberseguridad, podrá darse a ésta mayor alcance a través de una estrategia nacional en la que se delineen las funciones y responsabilidades, identifiquen las prioridades y establezcan los marcos y métricas de implementación. Por otra parte, gracias a la política y estrategias nacionales es posible situar los esfuerzos nacionales en el contexto de otras actividades internacionales de ciberseguridad. Para que una política global de ciberseguridad tenga éxito, tal vez resulte necesario promover conciencia entre los principales formuladores de decisiones sobre los problemas que se plantean. Estos formuladores deberán entender que es posible que transcurra un largo periodo antes de que se alcancen las metas de ciberseguridad acordadas.

2) El marco nacional de ciberseguridad no debe quedar comprometido por la adopción de políticas rígidas. En efecto, dicho marco y políticas deberían ser flexibles y poder responder a un entorno dinámico de riesgo. En ese marco los organismos públicos y las entidades privadas deberían establecer objetivos de política para colaborar con el fin de lograr las metas planteadas de la manera más eficiente posible.

3) La política nacional deberá ser fruto de la cooperación y la consulta con los representantes de todos los grupos participantes pertinentes, entre otros, organismos gubernamentales, sector privado, mundo universitario y asociaciones interesadas. Esta política debería ser promulgada en el plano nacional, preferiblemente por el jefe de gobierno o del Estado.

---

8 La adopción en la gestión de riesgos de un enfoque contra todos los peligros o contra varios peligros, obliga, entre otras cosas, a considerar todos los peligros que puedan suscitarse, ya sean naturales o tecnológicos, lo que incluye las situaciones de emergencia y las catástrofes naturales o antropogénicas (accidentales o intencionales).

I.B.2 Identificar un dirigente y una institución que dirijan a nivel nacional los esfuerzos necesarios; determinar en qué sector público conviene crear un equipo de respuesta en caso de incidentes de seguridad informática (CSIRT)[9], al que habría que conferir atribuciones nacionales; identificar las instituciones que responderán de cada uno de los aspectos de la estrategia nacional[10].

1) El lanzamiento de una iniciativa de ciberseguridad obliga a designar en la etapa inicial a una persona que dirija los esfuerzos nacionales de ciberseguridad, una persona encargada de políticas en el gobierno que entienda las cuestiones de ciberseguridad y pueda dirigir y coordinar los esfuerzos de las instituciones gubernamentales e interactuar eficazmente con el sector privado. Lo ideal sería que dicha persona tuviera estatura política y acceso al jefe de gobierno o del Estado. Esta autoridad de alto nivel es necesaria para garantizar la coordinación entre entidades que deben interactuar. Con el tiempo, este esfuerzo de coordinación proporcionará bases institucionales sobre las que se apoyen los líderes técnicos y organizaciones de ciberseguridad del país.

2) Una vez que el país de que se trate haya lanzado una iniciativa de ciberseguridad, puede suceder que dejen de ser necesarios los servicios de las personas o instituciones que participaron en dicho lanzamiento.

3) Habrá que identificar otras instituciones encargadas de definir e implementar las diferentes partes de una estrategia nacional.

I.B.3 Identificar a los correspondientes expertos y formuladores de políticas en las autoridades gubernamentales y el sector privado, así como sus funciones.

1) Una acción nacional eficaz exige inculcar a los participantes una "cultura de ciberseguridad". Las personas e instituciones que trabajan dentro o fuera del gobierno para diseñar, poseer, proporcionar, gestionar y utilizar sistemas y redes de información o dar servicio a éstos, deben entender el cometido que han de desempeñar y las medidas que es preciso que adopten. Los formuladores de políticas de alto nivel y los dirigentes del sector privado han de definir metas y prioridades en sus instituciones. Los expertos técnicos de nivel superior deben establecer directrices y marcos de acción.

I.B.4 Identificar disposiciones de cooperación entre los participantes y dirigidas a éstos.

1) El gobierno central debería promover la adopción de disposiciones de colaboración formal e informal que permitan y alienten el intercambio de comunicación e información entre el sector privado y el Estado. La ciberseguridad se llevará a cabo a nivel técnico u operativo a través de un conjunto de instituciones, tanto gubernamentales como no gubernamentales. Por otra parte, estos esfuerzos deberán coordinarse y venir acompañados, entre otras cosas, por mecanismos de intercambio de información.

I.B.5 Establecer mecanismos de cooperación entre las entidades públicas y privadas en el plano nacional.

1) El diseño de políticas y la elaboración e implementación del plan nacional deben realizarse mediante procesos abiertos y transparentes, y en estos esfuerzos habrá que tener en cuenta las opiniones e intereses de todos los participantes.

I.B.6 Identificar los interlocutores internacionales y promover esfuerzos internacionales para abordar diferentes aspectos de la ciberseguridad, lo que incluye actividades de intercambio de información y asistencia, habida cuenta de los resultados de la implementación del proyecto previsto en la Resolución 45 de la CMDT-06.

---

9 Un CSIRT es un equipo de expertos en seguridad IT cuya función principal consiste en responder a incidentes de seguridad informática. Este equipo proporciona los servicios requeridos para afrontar tales incidentes y ayuda a las entidades que representan los expertos a solventar los daños generados por intrusiones (*A Step-by-Step Approach on How to Set Up a CSIRT puede verse en* (www.enisa.europa.eu/act/cert). En ocasiones se denominan los CSIRT equipos de intervención ante emergencias informáticas o equipos dispuestos a intervenir ante emergencias informáticas (CERT). En todo caso los CSIRT y los CERT desempeñan la misma función. El término "informáticas" en la sigla CSIRT se utiliza en el presente Informe de manera integradora para abarcar, entre otras cosas, encaminadores, servidores, dispositivos móviles IP y aplicaciones conexas.

10 A los efectos del presente Informe, cabe denominar "CSIRT" a un CSIRT designado a nivel nacional.

1) Los esfuerzos encaminados a mejorar la ciberseguridad nacional serían facilitados mediante la participación en foros regionales o internacionales, conferencias, talleres, etc., que permitan fomentar la educación y la capacitación. En esos foros se fomenta conciencia acerca de los problemas planteados, se oyen disertaciones de expertos y los representantes nacionales pueden compartir ideas, experiencias y perspectivas. Estos esfuerzos se verían impulsados, también mediante la participación en organizaciones regionales e internacionales encargadas de conseguir objetivos similares, y/o gracias a la adhesión categoría de miembro a dichas organizaciones. Éste es uno de los objetivos del proyecto previsto en la Resolución 45.

2) La participación en los programas y actividades disponibles de las organizaciones multilaterales que procuran mejorar y ampliar la ciberseguridad global, es una forma más de fomentar la colaboración internacional. Entre las organizaciones multilaterales que cabe citar en ese sentido, figuran la Unión Internacional de Telecomunicaciones (Línea de Acción C5 de la CMSI), la Organización de Cooperación y Desarrollo Económicos (OCDE), la Organización de Estados Americanos (OEA) y la Cooperación Económica Asia-Pacífico (APEC), etc. Por otra parte, existen otras conferencias en que los gobiernos pueden compartir información sobre asuntos de ciberseguridad, por ejemplo la Conferencia del Meridiano.

3) Asimismo, habría que considerar también la participación en esfuerzos liderados por el sector privado, por ejemplo los desplegados por el Grupo de Trabajo contra el phishing y otras tentativas internacionales similares.

I.B.7 Establecer un proceso integrado de gestión de riesgos para identificar los esfuerzos de protección que se requieran con el fin de garantizar la ciberseguridad, así como definir un orden de prioridades entre dichos esfuerzos.

1) Sólo si entienden los riesgos suscitados, los gobiernos y los propietarios de infraestructura y operadores (incluidos los vendedores que les prestan apoyo) podrán iniciar una colaboración entre los ámbitos público-privado-personas, para identificar funciones y elementos clave de protección, así como establecer un orden de prioridades entre los mismos. Una vez identificadas, podrá asignarse un orden de prioridades o una puntuación a las funciones de infraestructura, para determinar cuáles son las más significativas y en qué contexto. Resulta importante recordar que el carácter de "esencial" depende de la situación considerada y que algo puede ser esencial en un caso y no así en el siguiente. Al identificar funciones esenciales y establecer un orden de prioridades entre tales funciones, los países deben ser conscientes de que lo que se considera esencial se modificará con los adelantos tecnológicos y las mejoras que se introduzcan en la infraestructura y los procesos.

2) Conseguir proteger la CII y el ciberespacio es algo muy arduo. En efecto, salvaguardar la CII, el ciberespacio y las funciones esenciales conexas exige la continua aplicación de prácticas de gestión de riesgos (evaluar las amenazas y las vulnerabilidades, y, por consiguiente, identificar controles y medidas de mitigación, implementar controles y medir la eficacia) para permitir que los operadores puedan gestionar riesgos y garantizar la solidez de sus misiones esenciales. Los diferentes proveedores de infraestructura de información aplican por regla general metodologías y prácticas de gestión de riesgos avanzadas, ya que deben prestar en tiempo real sus servicios. Con todo, su interconectividad e interdependencia, así como la complejidad técnica de la infraestructura de información limitan la posibilidad de evaluar fácilmente sus riesgos o su disposición globales, lo que explica que sea muy útil recurrir a que el sector público y el sector privado entablen relaciones de colaboración para evaluar dependencias y riesgos de infraestructura comunes (catástrofes naturales, insuficiencias tecnológicas, ataques terroristas, etc.).

I.B.8 Evaluar y revaluar periódicamente el estado de los esfuerzos de ciberseguridad y diseñar prioridades de programa.

1) En una estrategia nacional de ciberseguridad habrá que contar con un mecanismo de evaluación nacional que pueda emplearse para autoevaluar los progresos realizados, como parte de la capacitación con la asistencia de terceros. A partir de una herramienta de evaluación común, los países podrán identificar los puntos fuertes y las posibles lagunas de sus marcos nacionales de ciberseguridad y establecer un proceso para ajustarlos a sus metas perseguidas. La BDT ha diseñado

una herramienta de autoevaluación, la herramienta de autoevaluación CIIP/Ciberseguridad nacional de la UIT, para acompañar el presente documento sobre prácticas idóneas.

I.B.9 Identificar requisitos de formación y los medios para satisfacerlos.

1) Después de comparar las prácticas óptimas recomendadas en este Informe con sus propias prácticas de ciberseguridad (es decir, tras realizar un análisis de carencias), es posible que un país decida que algunos de los aspectos de los programas de ciberseguridad deben mejorarse. La solución puede ser de índole técnica (por ejemplo, nuevos equipos o soporte lógico), jurídica (por ejemplo, la formulación de nuevas leyes o normas que aborden las conductas indebidas en el ámbito de la ciberseguridad) y organizativa. El análisis de carencias podría permitir detectar las esferas en que se requiere un mayor desarrollo de los recursos humanos (formación).

PARTE II

Establecimiento de relaciones de colaboración entre el Estado y el sector privado

Proteger la infraestructura de información esencial y el ciberespacio es una responsabilidad que incumbe no sólo a todos los niveles del Estado sino también al sector privado, que posee y explota gran parte de la infraestructura. En todo caso, el Estado debe tener la última palabra sobre cualquier decisión nacional que se tome. Resulta importante reconocer que, si bien en el mundo los sistemas de seguridad de la información forman parte de una red global interoperable e interconectada, la estructura de estos sistemas puede variar en gran medida, según sea el país considerado. Esto explica que la eficacia y sustentabilidad de un sistema dado de seguridad puedan ser fortalecidas por la colaboración de los propietarios y operadores de todos estos sistemas.

Como al Estado y al sector privado les interesa garantizar de manera constante la resistencia de la infraestructura, resulta crucial que exista la colaboración entre los ámbitos público-privado personas para fomentar la ciberseguridad, ya que ninguno de ellos puede proteger por sí solo toda la infraestructura. En un gran número de países es el sector privado quien posee y/o explota la infraestructura, por lo que se recomienda que el Estado y el sector privado, cada uno dentro de sus respectivas esferas de competencia, colaboren en grado apreciable. El éxito de dicha colaboración pública-privada exige atender a tres importantes requisitos: 1) formular una propuesta clara de valor; 2) delinear con precisión las funciones y responsabilidades; y 3) fomentar la confianza.

Propuesta de valor

El éxito de la colaboración entre el Estado y el sector privado depende de los beneficios que ésta pueda traer consigo para los dos. Las ventajas para los gobiernos consisten en que los vendedores y operadores de infraestructura proporcionen capacidades que no figuran entre las competencias básicas del Estado como por ejemplo:

- garantizar la titularidad y la gestión de la mayoría de la infraestructura esencial en muchos sectores, y ello en un gran número de países;
- entender los diferentes aspectos de los activos, las redes, los sistemas, las instalaciones, las funciones y otras capacidades;
- contar con conocimientos especializados y experiencia en materia de respuesta ante incidentes;
- poder innovar y proporcionar productos, servicios y tecnología, para responder rápidamente a las necesidades planteadas;
- diseñar, desplegar, explotar, administrar y mantener la Internet mundial.

A la hora de evaluar la propuesta de valor para el sector privado, hay que señalar que colaborar con el gobierno para mejorar la CIIP y la ciberseguridad redunda en claros beneficios. En efecto, los gobiernos pueden aportar valor a la relación de colaboración, y ello de diferentes formas, por ejemplo:

- proporcionar a propietarios y operadores información oportuna, analítica, exacta, agregada y útil sobre amenazas fundamentales contra la infraestructura;
- hacer participar al sector privado desde un principio en la preparación de iniciativas y políticas CIP;
- señalar a los dirigentes empresariales, mediante el recurso a plataformas públicas y comunicaciones directas, los beneficios empresariales y nacionales que reportaría invertir en medidas de seguridad que vayan más allá de sus estrategias empresariales específicas;
- crear un entorno que aliente a las empresas y capte su interés para adoptar voluntariamente sólidas prácticas de seguridad ampliamente aceptadas y, en su caso, a actualizar y mejorar sus operaciones y prácticas de seguridad más allá de lo que exigen sus estrictos intereses empresariales;

- colaborar con el sector privado para definir misiones y establecer prioridades claras entre las mismas, así como hacer posible su protección y/o restauración;
- respaldar la investigación necesaria para promover los futuros esfuerzos de protección de la CI;
- identificar los recursos que se requieran para emprender estudios de interdependencia intersectorial, mediante ejercicios, simposios, sesiones de capacitación y modelado con asistencia de computador, estudios de cuyos resultados beneficien los formuladores de decisiones para seguir planificando en su campo de actividad; y
- permitir el intercambio de información oportuna, así como prestar durante incidentes apoyo de restauración y recuperación a las facilidades y servicios de infraestructura prioritarios.

Funciones y responsabilidades

El Estado y el sector privado pueden colaborar para llegar a un entendimiento común de sus respectivas funciones y responsabilidades en lo que concierne a la seguridad. El Estado puede proporcionar coordinación y liderazgo en lo que concierne a los esfuerzos de protección. Por ejemplo, la continuidad de las actividades estatales exige garantizar la seguridad y disponibilidad de la infraestructura cibernética y física que los gobiernos requieren para apoyar sus misiones y servicios esenciales. Por otra parte, el Estado puede desempeñar un papel clave de coordinación durante una catástrofe o prestar su ayuda cuando el sector privado carezca de los recursos suficientes para responder a un incidente. El Estado puede promover y alentar los esfuerzos que despliegue voluntariamente el sector privado para mejorar la seguridad, lo que incluye el establecimiento de las políticas y protocolos necesarios para compartir de manera oportuna información analítica y utilizable acerca de las amenazas que puedan plantearse, así como dar incentivos al sector privado para promover la seguridad más allá de sus intereses económicos. Por último, el Estado puede patrocinar y financiar estudios, así como investigación y desarrollo, para mejorar los procesos y mecanismos de seguridad.

Confianza

Un elemento esencial de una colaboración exitosa entre el Estado y el sector privado es la confianza, elemento que resulta necesario para establecer, desarrollar y mantener relaciones de intercambio entre el Estado y el sector privado. Un sólido intercambio de colaboración e información entre el sector privado y el Estado fomentará la conciencia de las situaciones que puedan suscitarse, facilitará la cooperación para resolver problemas estratégicos, contribuirá a gestionar el ciberriesgo y contribuirá a las actividades de respuesta y recuperación. Intercambiando y analizando información mejorada, tanto el Estado como el sector privado se encontrarán en mejores condiciones para identificar las amenazas y las vulnerabilidades, así como para intercambiar tácticas y recursos de mitigación y prevención.

A continuación, se señalan las metas generales que los diferentes gobiernos deberían considerar en sus relaciones de colaboración con el sector privado.

II.A Visión general de las Metas correspondientes a esta Parte

II.A.1 Desarrollar relaciones de colaboración entre sectores público-privado que contribuyan a gestionar eficazmente el ciberriesgo y proteger el ciberespacio.

II.A.2 Crear un mecanismo que permita relacionar diferentes perspectivas, situaciones semejantes y conocimientos, para llegar a un consenso y progresar en materia de seguridad nacional.

II.B Medidas específicas para lograr estas Metas

II.B.1 Incorporar los puntos de vista del sector privado en las primeras fases de la definición e implementación de la política de seguridad y los esfuerzos afines.

1) En muchos países la propiedad y la explotación de la mayoría de las infraestructuras esenciales y los ciberelementos de los que éstas dependen corresponden a empresas privadas. Las tecnologías que crean y soportan ciberespacio evolucionan rápidamente, gracias a las innovaciones que genera el sector privado. Así pues, los gobiernos no pueden por sí solos proteger en medida suficiente el

ciberespacio. Tener presente las perspectivas del sector privado y tomar en consideración a los propietarios primarios y operadores de las infraestructuras esenciales es algo que los gobiernos deben hacer, si desean desplegar eficazmente sus esfuerzos de ciberseguridad con el fin de diseñar e implementar políticas de ciberseguridad y marcos de gestión de riesgos. El sector privado puede informar a los gobiernos sobre el particular, si éstos participan en grupos de trabajo mixtos con participación de representantes gubernamentales y del sector privado, solicitan comentarios de la industria para diseñar e implementar sus políticas de ciberseguridad y concebir estrategias, y coordinar esfuerzos con entidades del sector privado, sobre la base de mecanismos de intercambio de información. Los gobiernos deberían garantizar que el sector privado participe en las fases iniciales del diseño, implementación y mantenimiento de iniciativas y políticas.

2) Los gobiernos y el sector privado deberían colaborar para adoptar un enfoque respecto a la gestión de riesgos que permita que el sector público y el sector privado identifiquen ciberinfraestructura, analicen amenazas, evalúen vulnerabilidades, ponderen consecuencias e identifiquen métodos de mitigación.

3) Los gobiernos y el sector privado deberían colaborar para proseguir las actividades de investigación y desarrollo (I+D) encaminadas a gestionar el ciberriesgo. El hecho de que el sector privado y el sector público sean conscientes de las prioridades e iniciativas emprendidas en materia de I+D, garantizaría que los recursos se asignen y utilicen eficientemente, que las iniciativas I+D se emprendan de manera oportuna y, en última instancia, que los productos y servicios se pongan a disposición a tiempo para fomentar la ciberseguridad nacional.

II.B.2 Alentar el desarrollo de grupos del sector privado de diferentes industrias de infraestructuras esenciales para abordar en colaboración con el Estado intereses de seguridad comunes.

1) El establecimiento de dichos grupos, entre los cuales, cabe citar las asociaciones de empresas por parte de varios sectores de infraestructura esencial puede contribuir a abordar necesidades de ciberseguridad comunes. Estos grupos pueden centrar sus actividades en asuntos estratégicos u operacionales, así como en la gestión de los problemas de seguridad que se plantean en el sector privado, considerada en su conjunto. Entre estos temas, cabe citar la gestión de riesgos, la sensibilización, la concepción y traducción a la práctica de políticas y muchos más. Estos grupos del sector privado representan un proceso institucionalizado en el que puede fomentarse la participación del Estado, así como un foro de debate para responder a los problemas que suscita la ciberseguridad.

2) En ciertos países diferentes sectores de infraestructura crítica han establecido grupos con el fin de que los representantes de todos los sectores intercambien información sobre amenazas contra la seguridad, vulnerabilidades y efectos. Por otra parte, estos grupos suelen proporcionar alertas y avisos en tiempo real a sus miembros, con la idea de facilitar los esfuerzos emprendidos para mitigar los incidentes que hayan afectado a infraestructuras esenciales, así como para responder a los mismos y adoptar las correspondientes medidas de recuperación.

3) Estos grupos deberían considerar la posibilidad de adoptar prácticas que permitan que sus miembros (esto es, gobierno y sector privado) colaboren e intercambien información en un foro fiable. Alguna de estas prácticas tienden, entre otras cosas, a proporcionar: anonimato a sus miembros, acceso al plan intersectorial e información gubernamental, acceso a productos que respondan a amenazas, vulnerabilidades y necesidades de análisis, y conocimientos especializados sobre coordinación de prácticas operacionales y ejercicios de respuesta ante emergencias. Al considerar estas prácticas que promueven la colaboración, importa tener en cuenta los medios existentes para proteger información patentada e información confidencial de las empresas.

II.B.3 Hacer colaborar a los grupos del sector privado y el Estado en foros dignos de confianza para abordar desafíos comunes en materia de ciberseguridad.

1) Es necesario reunir una serie de requisitos para promover la confianza y fomentar una colaboración exitosa entre el Estado y el sector privado. Se recomienda la concertación de acuerdos escritos que orienten la colaboración y el intercambio de información entre el Estado y el sector privado. Los participantes deben contar con una visión y propósito comunes. Cuando una persona o una organización adopta un sólido liderazgo, es posible definir prioridades, atribuir recursos y adquirir

los compromisos necesarios para mantener la colaboración entre sectores público-privado. Por otra parte, es preciso establecer reglas de compromiso para orientar los comportamientos individuales e institucionales en el marco de las relaciones de colaboración.

2) Los participantes deben ver resultados tangibles y mensurables. Definir un objetivo de interés en cuanto a la colaboración de individuos y organizaciones y traducir a la práctica con claridad dicho interés, es esencial, si se desea que se entablen y mantengan relaciones de colaboración entre sectores público-privado.

II.B.4 Alentar la cooperación entre grupos e industrias interdependientes.

1) Los incidentes que afecten a una infraestructura determinada pueden aparejar efectos en cascada que incidan en otros tipos de infraestructura. Por ejemplo, las interrupciones del suministro eléctrico pueden perturbar los servicios telefónicos de Internet. Además, aunque sea posible planificar situaciones de emergencia en un, sector dado, los interesados deberán tener presente también el impacto de los incidentes que puedan sobrevenir en otros sectores. Compartir información sobre diferentes infraestructuras puede contribuir a responder a incidentes que incidan en varios sectores y acarreen consecuencias en el plano nacional.

II.B.5 Concertación de acuerdos de cooperación entre el Estado y el sector privado para la gestión de incidentes.

1) Llevar a cabo rápidamente la identificación, el intercambio de información y la rectificación necesarios suele reducir el daño ocasionado por los ciberincidentes. En el plano nacional, se requiere la colaboración pública-privada para realizar análisis, dar alertas y coordinar los esfuerzos de respuesta.

2) El Estado y el sector privado deberían colaborar a diseñar un marco estratégico, operacional y de sensibilización para coordinar las actividades encaminadas a mejorar la gestión de incidentes. Este marco debería contener un modelo formal para intercambiar información que incluya coordinadores para encargarse de cuestiones de política y el intercambio de información operacional. En este marco habría necesidad de prever también políticas y procedimientos para enfrentarse colectivamente a incidentes e informar sobre los mismos, proteger y difundir información patentada sensible (tanto pública como del sector privado), y establecer mecanismos de comunicación y difusión de la información. La información del sector privado suele contener información patentada de las diferentes empresas privadas, información ésta que en caso de darse a la luz podría redundar para dichas empresas en una pérdida de su cuota de mercado, publicidad adversa u otras consecuencias adversas. Asimismo, cabe la posibilidad de que la información pública tenga carácter reservado o sensible y que, por tanto, no esté destinada a darse a conocer. Habría que adoptar medidas políticas y técnicas para salvaguardar dicha información, sin olvidar por ello el derecho del público a ser informado. Los gobiernos podrían seguir fomentando confianza, mejorando las políticas destinadas a intercambiar la información y las relaciones entre el Estado y el sector privado, mediante la continua evaluación de tales políticas. Cabría también la posibilidad de realizar ejercicios cibernéticos para probar las comunicaciones y la coordinación entre el Estado y el sector privado, en lo que concierne a la respuesta ante ciberincidentes y los esfuerzos de recuperación, aplicando los mecanismos previstos para situaciones reales de crisis.

PARTE III

Disuasión del ciberdelito

Es posible mejorar en gran medida la ciberseguridad, entre otras formas, estableciendo y modernizando de los elementos de apoyo, el derecho, los procedimientos y las políticas penales para impedir, desalentar y perseguir el ciberdelito, así como responder al mismo.

III.A Visión general de la Meta correspondiente a esta parte

III.A.1 Promulgar y vigilar el obligado cumplimiento de un conjunto completo de leyes sobre ciberseguridad y ciberdelito.

Todos los países necesitan leyes que se opongan al ciberdelito considerado en sí mismo, así como los procedimientos necesarios para realizar investigaciones por vía electrónica y la asistencia de otros países. Estas leyes pueden quedar incorporadas en uno o varios códigos nacionales. En aras de la simplicidad, en este documento se supone que cada país cuenta con un código básico relativo al ciberdelito, así como con un conjunto de textos jurídicos de procedimiento y asistencia mutua. Huelga decir que las diferentes naciones deberían establecer cualesquiera estructuras que, a su juicio, se ajusten más adecuadamente a las circunstancias nacionales.

III.B Medidas específicas para lograr esta Meta

III.B.1 Asesorar a los autoridades legislativas respecto a la eficacia de las leyes. El país debe examinar código penal vigente, incluyendo los procedimientos pertinentes, a fin de determinar si procede para afrontar los problemas actuales (y futuros). Se sugieren las siguientes medidas:

1) Formular, según convenga, la legislación necesaria sobre este asunto, teniendo en cuenta especialmente iniciativas regionales. Dicha legislación debería abordar, entre otros, el daño o la destrucción de datos informáticos, los mecanismos de procedimiento para apoyar la investigación, incluyendo la posibilidad de analizar la fuente de mensajes de correo electrónico, etc., y una posible cooperación jurídica internacional (por ejemplo, en lo que concierne a la obtención de pruebas).
2) Un país debería determinar si sus leyes se basan en expectativas tecnológicas obsoletas. Por ejemplo, cuando en una ley se contempla únicamente el seguimiento de transmisiones vocales. Dicha ley tal vez deba modificarse para tener en cuenta también la transmisión de datos.
3) La ley nacional contra el ciberdelito debería ser sometida a la evaluación de todos los ministerios y comisiones legislativas competentes que puedan tener un interés en ella, así no guarden relación con la justicia penal, para que no pase inadvertida ninguna idea que pueda resultar útil. Un funcionario que trabaje con tecnologías de la información podría señalar, por ejemplo, que la ley contra el ciberdelito no abarca cierta tecnología de uso creciente pero que es desconocida para los legisladores del país considerado.
4) Adicionalmente, se recomienda que las leyes penales vigentes se sometan también a la evaluación de algunas o de todas las siguientes entidades: las empresas del sector privado local, las empresas filiales locales del sector privado internacional, las organizaciones no gubernamentales locales, el sector académico y expertos o asociaciones de ciudadanos de renombre.
5) Los países pueden solicitar a otros países asesoría sobre estos temas.

III.B.2 Formular y adoptar leyes y políticas sustantivas sobre los procedimientos y la asistencia mutua para afrontar el ciberdelito.

1) Se recomienda que los países participen activamente en formular, según convenga, la legislación necesaria, tomando especialmente en cuenta las iniciativas regionales, entre las cuales cabe citar, entre otras, el Convenio del Consejo de Europa sobre el ciberdelito. Se recomienda que los países entablen relaciones de colaboración regionales e internacionales para luchar contra el ciberdelito y fortalecer la ciberseguridad, así como para crear los mecanismos necesarios para fomentar la cooperación en materia de ciberseguridad, lo que incluye la lucha contra el correo electrónico basura, el soporte lógico perjudicial, las redes robots, etc.

2) Un proyecto de ley sobre ciberdelito de un país debería ser evaluado por todas las autoridades gubernamentales y órganos legislativos. Dicho proyecto debería publicarse para recabar comentarios y abordar todas las posibles tecnologías, infracciones u otras cuestiones pertinentes que no hubieran sido contempladas originalmente.

3) Toda normativa contra el ciberdelito no sólo debe abarcar el ciberdelito comúnmente conocido, que incluye los delitos informáticos y la intromisión informática, sino que también debe proteger las pruebas electrónicas en redes relacionadas con otros tipos de delitos.

4) Las leyes redactadas para la vida civil y comercial no deben extenderse o interpretarse de forma tal que se obstaculice inadecuadamente el intercambio de pruebas delictivas entre los países.

5) Los países que decidan contratar consultores para la formulación deberán analizar las competencias de éstos y supervisar su trabajo durante todo el proceso. Quienes no hayan recibido formación respecto a las leyes particulares de un país dado, podrían integrar inadecuadamente algunas de las disposiciones necesarias, en especial las secciones relacionadas con los procedimientos y la asistencia jurídica mutua. Es más, quienes no posean experiencia en aspectos procesales posiblemente no tengan apropiadamente en cuenta los aspectos prácticos relacionados con el suministro de pruebas. Algunos consultores tendrán la capacidad de apoyar la redacción de leyes de comercio electrónico, pero no la de leyes penales.

6) Es posible hacer consultas a otros países, quienes podrían presentar sugerencias complementarias al convenio. Por ejemplo, algunos países pueden exigir que los proveedores de servicio de Internet almacenen durante cierto tiempo, por lo general durante seis meses, parte de la información que cursa por sus sistemas; o pueden exigir que los incidentes de cierta magnitud sean comunicados a las autoridades oficiales; o que las personas deban identificarse apropiadamente antes de hace uso de un cibercafé.

7) Si hay tiempo para ello, el país puede solicitar a otros países y organizaciones multilaterales comentarios sobre la ley contra la ciberdelito (o enmiendas a la misma). Dichos comentarios se pueden solicitar privadamente y, como se indica anteriormente, conviene conocer el punto de vista de otros países basada en sus experiencias.

8) Tan pronto como sea posible (dependiendo de los procedimientos nacionales), el país puede consultar el punto de vista de todos los que tengan un interés reconocido en el tema en cuestión, como el sector privado, las empresas filiales del sector privado internacional, las organizaciones no gubernamentales locales, el sector académico, las personas independientes con intereses particulares y otros.

III.B.3 Crear o identificar unidades nacionales contra la ciberdelito.

1) Independientemente de su nivel de desarrollo, para cada país es importante poder contar con al menos las posibilidades básicas de investigación en materia de ciberdelito. Por ejemplo, el uso de teléfonos celulares se ha disparado aun en los países en desarrollo, y estos aparatos se pueden utilizar para cometer fraudes, transferir dinero, conspirar, transmitir virus hacia redes informáticas, hacer estallar explosivos, etc.

2) Cada país debe seleccionar o entrenar uno o varios servicios de policía que se capacitarán para adelantar investigaciones relacionadas con la ciberdelito. Algunas veces es fácil determinar el o los servicios de policía que se encargarán de esto. Otras veces las fuerzas de policía competirán por ser seleccionadas y serán las autoridades superiores las encargadas de tomar la difícil decisión. Aunque parezca que en el país no haya nadie con las habilidades necesarias, normalmente en alguna parte existe un oficial de policía interesado en tecnología electrónica dispuesto a aprender más y a avanzar en el tema.

3) Las unidades investigadoras sobre ciberdelito, aun si las componen un número limitado de investigadores, requieren de apoyo. Necesitan contar con equipos relativamente actualizados, conexiones de red bastante fiables y formación continua. Este apoyo puede proceder de fuentes oficiales o gubernamentales, de organizaciones internacionales u otros países y de donaciones del sector privado.

4) Si es posible, convendría que las unidades contasen al menos con una capacidad forense informática básica. Esta capacidad haría necesario el uso de herramientas informáticas y formación adicional. (Si no es posible obtener esta capacidad forense, los países deberían aceptar de antemano que es posible que se pierdan pruebas cruciales, aun en los casos más importantes.) En algunas circunstancias otros países pueden prestar apoyo forense en casos concretos. Adicionalmente, otros países y algunas organizaciones pertinentes podrían ofrecer formación en ciencias forenses del ciberespacio. Por ejemplo, el Centro de Coordinación del equipo de intervención ante emergencias informáticas (Computer Emergency Response Team Coordination Center) de la Universidad Carnegie-Mellon de Estados Unidos (www.cert.org) ofrece formación gratuita o a bajo coste, en línea o en CD-ROM, sobre ciencias forenses del ciberespacio.

5) Una vez creada, la unidad contra el ciberdelito debería dar a conocer su existencia y capacidades a los demás servicios de policía y a los fiscales del país. Si una fuerza de policía regional está investigando un crimen espantoso en el que se utilizaron medios electrónicos, no sería útil tener en la capital una unidad contra el ciberdelito si la unidad regional desconoce que existe y que está en capacidad de escudriñar el ordenador en cuestión u ofrecer otro tipo de servicio. Desafortunadamente, es común, a nivel mundial, que los estamentos encargados de aplicar las leyes desconozcan la existencia en el país de una unidad contra el ciberdelito.

6) Las unidades contra el ciberdelito, o que sean candidatas a serlo, deben, en lo posible, ponerse en contacto con sus contrapartes internacionales. En las primeras etapas, los otros países y las organizaciones de policía internacionales podrían prestar asesoría sobre la constitución de la unidad. En etapas posteriores, otros países, organizaciones de policía internacionales, organizaciones multilaterales pertinentes y el sector privado podrían prestar servicios de formación de diversos tipos e incluso suministrar equipos y programas informáticos. Hay otro motivo por el cual es valioso establecer este tipo de contacto: en un mundo que cada día estará más y más interconectado, será fundamental poder solicitar la ayuda de organismos extranjeros encargados de aplicar la ley.

7) Las unidades contra el ciberdelito deben establecer contactos con cada uno de los sectores pertinentes e interesados en el país, por ejemplo las organizaciones no gubernamentales, los equipos de intervención en caso de incidentes de seguridad informática, entidades del sector privado y entidades del sector académico, a fin de asegurar que conozcan la existencia y capacidades de la unidad, puedan colaborar con ella y saber cómo informar de posibles ciberdelitos.

III.B.4 Establecer vínculos de colaboración con otros elementos de la infraestructura de ciberseguridad nacional y el sector privado.

1) Es importante que existan relaciones de colaboración entre las autoridades oficiales, otros elementos de la infraestructura de ciberseguridad nacional y el sector privado, por diversos motivos:
   a) para intercambiar información entre los grupos (por ejemplo, para anunciar que se piensa formular una nueva ley o que se está concibiendo una nueva tecnología);
   b) para intercambiar opiniones (por ejemplo, "si formulamos una ley en ese sentido, ¿cree usted que se susciten inconvenientes de privacidad?" o "¿puede usted modificar la tecnología de forma que siga siendo posible rastrear correos en situaciones legítimas de seguridad pública?");
   c) para intercambiar programas de formación, aunque normalmente es el sector privado quien ofrece estos programas al gobierno;
   d) para intercambiar alertas sobre amenazas y vulnerabilidades;
   e) para que las personas de los diversos sectores puedan conocerse lo suficientemente bien como para que exista confianza mutua durante las emergencias.

2) Un primer paso al establecer estas relaciones consiste en que una o varias personas creen una lista en la que se indiquen los nombres de todos los responsables en cada uno de los sectores pertinentes, y que luego se complemente con información sobre cómo contactarlos. Posiblemente es preferible que esa lista sea informal, para evitar herir susceptibilidades sobre la pertenencia o no a la lista.

3) En cada país, es posible que muchos sectores pertinentes puedan contribuir valiosamente a la ciberseguridad: legisladores, ministerios, organizaciones no gubernamentales, equipos de respuesta en caso de incidentes de seguridad informática, sector académico, sector privado y particulares.

Algunos de éstos pueden ser estrictamente nacionales y otros, filiales de entidades extranjeras más grandes.

III.B.5 Promover la comprensión de las cuestiones sobre el ciberdelito entre fiscales, jueces y legisladores.

1) Para abordar adecuadamente los diferentes aspectos del ciberdelito importa que los fiscales y jueces comprendan hasta cierto punto esferas tales como la de computadores, soporte lógico y redes, así como la creciente importancia de disponer de pruebas electrónicas. Asimismo, entre los legisladores debería prevalecer cierto grado de comprensión de estos asuntos y el hecho de si en las leyes nacionales se aborda este punto adecuadamente. Si lo anterior plantea problemas, una posible solución al respecto es la formación.

2) De ser necesario puede obtenerse formación técnica básica de diversas fuentes, dependiendo de los recursos del país:
   a) cualquier servicio o ministerio nacional con competencias técnicas, como el servicio de policía o el ministerio encargado de tecnologías de la información;
   b) gobiernos extranjeros;
   c) organizaciones multinacionales competentes;
   d) el sector privado nacional;
   e) el sector privado internacional, especialmente (aunque no necesariamente) si actúa en el plano nacional;
   f) entidades competentes del sector académico;
   g) equipos nacionales y extranjeros de respuesta a incidentes de seguridad informática; y
   h) organizaciones no gubernamentales nacionales y extranjeras pertinentes.

3) Asimismo, puede ser conveniente formar a las principales personas encargadas de formular políticas, a altos funcionarios, etc., sobre las amenazas a las que están expuestas las redes electrónicas (por ejemplo, sobre los posibles ataques al sistema bancario nacional) y la utilización de las redes electrónicas con fines delictivos (por ejemplo, el uso de Internet para localizar niños vulnerables para tráfico sexual). Las fuentes antes señaladas deberían estar en condiciones de ofrecer formación en estos aspectos de las redes electrónicas.

4) Convendría que los diferentes países formasen fiscales y jueces respecto a las acciones judiciales en materia de ciberdelitos o de otros crímenes por medios electrónicos, o en el uso de medios electrónicos o en métodos para acceder a la colaboración internacional. Esta formación se puede obtener a través de:
   a) cualquier servicio o ministerio nacional con las competencias adecuadas, como la fiscalía y el ministerio de justicia;
   b) gobiernos extranjeros;
   c) organizaciones multinacionales pertinentes;
   d) entidades pertinentes del sector académico;
   e) organizaciones no gubernamentales nacionales y extranjeras pertinentes, y
   f) personas independientes pertinentes.

5) Los países podrían desear formación sobre formulación de leyes. Los grupos mencionados en el párrafo anterior podrían estar en capacidad de ofrecer dicha formación. El sector privado local y el sector privado internacional, especialmente (aunque no necesariamente) si actúa de forma local, pueden ser fuente de conocimientos técnicos especializados. No obstante, es más probable que las entidades del sector privado puedan prestar asesoría en la formulación de leyes de comercio electrónico que en la formulación de leyes sobre ciberdelito, procedimiento penal y asistencia jurídica mutua internacional.

6) En todos estos tipos de formación, las fuentes podrían realizar la formación directamente en el país solicitante o a través de módulos de formación (por medios electrónicos o impresos) que los instructores del país en cuestión podrían emplear para la realizar ellos mismos la formación. En algunos casos, como es el de la formación CERT-CC descrita en la sección III.B.3.4, la formación puede ofrecerse sin costo o a costo mínimo.

7) En algunos países, el apoyo de altos funcionarios, o a veces de un solo alto funcionario, en especial si están encargados del control presupuestario, ha resultado fundamental para el fomento de conciencia nacional en materia de ciberdelito. Si se sabe que uno de los ministros está muy interesado en ciberseguridad, su ministerio, y tal vez el resto del gobierno, podría ofrecer un mayor apoyo a los empleados que estén trabajando en el tema.

III.B.6 Adscripción a la red 24/7 de puntos de contacto sobre ciberdelito.

1) En 1997, el Subgrupo contra la delincuencia de alta tecnología del Grupo de los ocho países más industrializados (G8) estableció la Red 24/7 de Puntos de Contacto sobre el ciberdelito formado por los Ministros de Justicia e Interior del G8 a fin de mejorar la asistencia internacional, tratándose de investigaciones urgentes que entrañen la obtención de pruebas electrónicas. Un gran número de investigadores sobre ciberdelitos consideraban que era demasiado difícil saber dónde acudir para obtener una ayuda rápida de otros países. Otros muchos investigadores estimaban que los tratados de asistencia mutua vigentes durante varias décadas no eran útiles en casos que requerían de una actuación rápida ante, por ejemplo, intromisiones informáticas a media noche en los sistemas financieros de un país. Esta red ha ido creciendo y a comienzos de 2007 ya abarcaba 50 países. La red está abierta a cualquier país con la capacidad necesaria para ofrecer la ayuda que se describe más adelante.

2) Para formar parte de la red, los países deben presentar un punto de contacto con el que se pueda comunicar 24 horas al día, 7 días a la semana. De ahí el nombre con que se conoce informalmente la red: "la red de 24/7". El punto de contacto mencionado puede ser alguien que esté disponible bien sea directamente o a través de una oficina. Esa persona debe tener muy claro lo siguiente: 1) la tecnología, de forma que puedan comunicársele solicitudes sin prolongadas explicaciones técnicas; 2) el derecho nacional al que es necesario someterse; y 3) la ley nacional que le faculta para brindar asistencia a otros países. Si no conoce directamente alguno de estos tres asuntos, el punto de contacto debe estar en condiciones de acceder inmediatamente a los funcionarios de su gobierno autorizados para brindar ayuda, sin tener que esperar al siguiente día laborable.

3) Las comunicaciones deben fluir, al menos inicialmente, del punto de contacto 24/7 del País A hacia el punto de contacto 24/7 del País B, a fin de garantizar coherencia y seguridad. Esto significa que los puntos de contacto no deben suministrar información de los contactos entablados a otras entidades de su país, y son dichos puntos los encargados de establecer el primer contacto internacional en nombre de la entidad solicitante de su respectivo país (por ejemplo, una fuerza de policía provincial). Una vez creado el canal de cooperación inicial entre los dos países, el punto de contacto puede, si así se desea, retirarse de la investigación y permitir que la correspondiente entidad policial provincial del País A se comunique directamente con el País B.

4) La adscripción a la red no garantiza la asistencia mutua entre los países, y la red de puntos de contacto no reemplaza la asistencia jurídica mutua normal entre los países. Dicha red de contacto garantiza únicamente que el país solicitante reciba inmediatamente una atención inteligente y eficaz, aun durante la noche. Tras la asistencia inicial, los países podrían (o no) exigir que se utilicen canales menos ágiles de asistencia mutua.

5) Que haya una disponibilidad de 24 horas al día no significa que sea necesario mantener una oficina con un cierto número de computadores e investigadores en ciberdelitos esperando llamadas telefónicas o correos electrónicos. La mayor parte de los países no posee ese tipo de oficinas. Normalmente, cuentan con un oficial de policía (o posiblemente varios cumpliendo turnos) disponible por teléfono, al que se puede contactar por teléfono celular incluso durante la noche.

6) Para adherirse a la red, los diferentes países deben ponerse en contacto con el Subgrupo contra la delincuencia de alta tecnología del G8 (el número de miembros no está limitado a ocho, es más, ya hay cerca de 50 Países Miembros). Es necesario rellenar un formulario sencillo[11]. El proceso no exige que haya acuerdos internacionales oficiales, tales como Memorandos de Entendimiento ni

---

[11] El formulario debe remitirse por fax al número +1 202-514-6113, dirigido a Coordinator, 24/7 Network, Computer Crime and Intellectual Property Section, US Dept of Justice, Washington, D.C., U.S.A. También puede enviarse por correo electrónico a richard.green@usdoj.gov.

tratados. Ocasionalmente, la red de 24/7 ofrece a las personas de contacto formación y conferencias sobre redes. De ser necesario, se subvencionan los gastos de viaje para atender dichas conferencias.

7) Las unidades que se adhieran a la red tienen la responsabilidad de hacer que otros servicios de policía interesados y otras unidades contra el ciberdelito de su país tomen conocimiento de su existencia y de su disponibilidad para ayudar a entablar contactos en el exterior.

PARTE IV

Creación de capacidades nacionales de gestión de incidentes: vigilancia, advertencia, respuesta y recuperación

Es importante que el Estado cree o identifique una organización nacional que sirva de piedra angular para la seguridad del ciberespacio y la protección de las infraestructuras de la información esencial, y cuya misión principal abarque esfuerzos de vigilancia, advertencia, respuesta y recuperación y la facilitación de la colaboración entre las entidades gubernamentales a nivel nacional, estatal y local, las entidades pertinentes del sector privado, el sector académico y la comunidad internacional.

Algo esencial es que al abordar la ciberseguridad en el plano nacional los gobiernos se preparen para detectar, gestionar y responder a los ciberincidentes que puedan producirse. La gestión eficaz de incidentes exige que se consideren la financiación, los recursos humanos, la formación, la capacidad tecnológica, las relaciones entre el Estado y el sector privado y los requisitos jurídicos. Para inculcar una mayor conciencia de los posibles ataques y de las medidas que permitan remediarlos, es necesaria la colaboración entre el gobierno y el sector privado, el sector académico y las organizaciones internacionales. Los gobiernos tienen un papel esencial que desempeñar para garantizar la coordinación entre las entidades precitadas.

IV.A Visión general de las Metas correspondientes a esta Parte

El establecimiento de capacidades nacionales para la gestión de incidentes exige realizar una serie de actividades estrechamente relacionadas, entre las cuales cabe citar las siguientes:

IV.A.1 Diseñar un sistema nacional de respuesta coordinada en cuyo marco se adopten medidas de prevención, detección, disuasión, respuesta y recuperación en relación con los ciberincidentes.

IV.A.2 Establecer un coordinador para la gestión de ciberincidentes que promueva la colaboración entre elementos esenciales del Estado (incluida la vigilancia del cumplimiento obligatorio de la ley) y elementos esenciales de los operadores y vendedores de infraestructura, con el fin de reducir el riesgo de incidentes y su magnitud.

IV.A.3 Participar en los mecanismos establecidos para intercambiar información de vigilancia, advertencia y respuesta ante incidentes.

IV.A.4 Diseñar, probar y traducir a la práctica planes, procedimientos y protocolos de respuesta ante emergencias, con el fin de garantizar que el Estado y los colaboradores no gubernamentales puedan promover una confianza recíproca y entablar eficaces relaciones de coordinación ante situaciones de crisis.

IV.B Medidas específicas para lograr estas Metas

El establecimiento de capacidades de gestión de incidencias es un esfuerzo a largo plazo que empieza con la creación de un equipo nacional de intervención en caso de incidentes informáticos (N-CIRT)[12, 13].

IV.B.1 Identificar o constituir un equipo nacional de intervención en caso de incidentes de seguridad (CIRT).

1) La intervención oportuna ante los ciberincidentes telemáticos puede limitar el daño en los sistemas informáticos, garantizar un medio eficaz de intervención y reducir el costo y el tiempo empleado para la recuperación. Es necesario contar con un equipo de intervención en caso de incidentes de seguridad informática (CIRT), constituido por los sectores público y privado, que actúe como punto

---

[12] Véase la Resolución 58 de la AMNT. En algunos países el CIRT se denomina equipo nacional de intervención en caso de incidentes de seguridad informática (NCSIRT) o equipo de nacional de intervención en caso de incidentes de seguridad (N-SIRT).

[13] Los resultados del trabajo a realizar por el UIT-T de conformidad con la Resolución 58 pueden afectar a la Parte IV de estas prácticas óptimas.

de contacto principal del gobierno, en especial en caso de incidentes de envergadura nacional, y que coordine la defensa frente a estos incidentes e intervenga si ocurren. En estos casos, el CIRT debe trabajar mancomunadamente con las autoridades de inteligencia y las encargadas de aplicar la ley, pero no controlará sus actividades.

2) Es de esperarse que el CIRT ofrezca servicios y soporte para prevenir e intervenir en lo referente a ciberseguridad y sirvan de punto único de contacto donde se informen los incidentes contra la ciberseguridad, se coordinen las acciones y se centralice la comunicación. Entre los objetivos de los CIRT deben figurar análisis, advertencia, intercambio de información, reducción de la vulnerabilidad, reducción de los efectos y apoyo a los esfuerzos nacionales de recuperación de las infraestructuras de información esenciales. Concretamente, los CIRT deben cumplir diversas funciones a nivel nacional, que incluyen, entre otras:

- detectar e identificar actividades anómalas;
- analizar amenazas y vulnerabilidades informáticas y difundir información de advertencia sobre la amenaza;
- analizar y sintetizar información respecto a incidentes y vulnerabilidades difundida por terceros, incluidos los fabricantes y los expertos en tecnología, a fin de ofrecer orientación a las partes interesadas;
- crear mecanismos fiables de comunicación y facilitar la comunicación entre las partes interesadas, para intercambiar información y tratar cuestiones relativas a la ciberseguridad;
- ofrecer información sobre alertas tempranas, incluida información sobre cómo reducir las vulnerabilidades y los posibles problemas;
- elaborar estrategias de intervención y reducción de los efectos e intervenir coordinadamente en caso de incidentes;
- intercambiar datos e información sobre los incidentes y las correspondientes acciones de respuesta;
- rastrear y supervisar la información a fin de determinar tendencias y formular estrategias correctivas a largo plazo; y
- dar a conocer las prácticas más idóneas generales en materia de ciberseguridad y orientaciones respecto a la prevención y el tratamiento de incidentes.

IV.B.2 Establecer en el plano estatal uno o varios mecanismos de coordinación de los organismos civiles, de aplicación de la ley, de defensa y de inteligencia.

1) Una de las principales funciones del CIRT designado consiste en difundir información a las partes interesadas, incluida la información sobre las vulnerabilidades y amenazas actuales. Una de las partes interesadas que debe intervenir en las actividades de respuesta es el gobierno, incluidos los organismos civiles, de aplicación de la ley, de defensa y de inteligencia pertinentes.

2) La coordinación efectiva con estas entidades puede tomar múltiples formas, por ejemplo, una página web para intercambiar información, la distribución de información mediante listas de correo, incluidas circulares de noticias, informes de tendencias y análisis; elaboración de publicaciones que incluyan alertas, consejos e información sobre diversos aspectos de la ciberseguridad, incluidas las nuevas tecnologías, vulnerabilidades, amenazas y consecuencias.

IV.B.3 Establecer asociaciones con el sector privado para estar preparados para los incidentes informáticos nacionales, detectarlos, y estar en disposición de intervenir y participar en la recuperación.

1) El Estado y el CIRT nacional deben colaborar con el sector privado. Como en muchos países la mayor parte de los activos de la infraestructura de la información y de la tecnología de la información esenciales pertenecen al sector privado, el gobierno debe trabajar mancomunadamente con el sector privado para poder cumplir su meta general de gestionar eficazmente los incidentes.

2) Las relaciones de colaboración con el sector privado basadas en la confianza permiten a los gobiernos conocer buena parte de la infraestructura esencial que posee y explota el sector privado. La colaboración entre los ámbitos público-privado-personas puede reducir el riesgo inherente a las amenazas informáticas, sus vulnerabilidades y consecuencias y fomentan la toma de conciencia sobre la situación mediante promoción y compromisos bilaterales.

3) Alentar el desarrollo de prácticas de intercambio de información entre el sector privado y el Estado para compartir información operacional en tiempo real.

4) Para fomentar estas alianzas se pueden emprender actividades que incluyan la identificación de los beneficios tanto del Estado como del sector privado, la creación y desarrollo de programas que garanticen la protección de la información privada crucial, el establecimiento de grupos de trabajo de los sectores público y privado sobre la gestión de ciberriesgos y la gestión de incidentes, el intercambio de material didáctico e información sobre prácticas óptimas en torno a la intervención en caso de incidentes y su gestión y la definición conjunta de las funciones y responsabilidades del Estado y del sector privado sobre gestión de incidencias para la puesta en práctica de protocolos consistentes y predecibles.

IV.B.4 Establecer puntos de contacto de organismos gubernamentales, el sector privado y socios internacionales para así facilitar la consulta, la colaboración y el intercambio de información con la CIRT.

1) Para contar con un mecanismo nacional e internacional eficaz de intervención en caso de incidentes es primordial identificar los puntos de contacto adecuados y establecer relaciones de trabajo de colaboración para la consulta, la cooperación y el intercambio de información. Las relaciones mencionadas pueden fomentar la alerta temprana de posibles incidentes informáticos y estimular, entre las entidades de intervención y otras partes interesadas, el intercambio de información sobre tendencias, amenazas e intervención.

2) Mantener actualizada la lista de puntos de contacto y canales de comunicación con las comunidades interesadas puede ayudar al intercambio dinámico y oportuno de información sobre tendencias y amenazas y a facilitar la intervención. Es importante que, en la medida de lo posible, se establezcan los contactos sobre la base de las funciones de los departamentos y no así del nombre de las personas, con las que deba entrarse en contacto para así garantizar que los canales de comunicación permanezcan abiertos aun cuando una de estas personas haya dejado la organización considerada. Normalmente las relaciones se inician mediante el establecimiento de lazos de confianza con particulares, pero deben luego evolucionar hacia un acuerdo más formal a nivel institucional.

IV.B.5 Emprender actividades internacionales cooperativas de intercambio de información.

1) Los Estados deben alentar la colaboración con organizaciones, vendedores y otros expertos en la materia a fin de 1) hacer que la respuesta avanzada a incidencias sea una disciplina de ámbito mundial, 2) promover y apoyar que los CIRT participen en conferencias y foros de ámbito mundial y regional a fin de crear capacidades para mejorar el estado del arte en la respuesta a incidencias sobre una base regional, y 3) colaborar en el diseño de material destinado a la creación de los CIRT nacionales y para lograr una comunicación efectiva con las autoridades del CIRT.

IV.B.6 Crear herramientas y procedimientos para la protección de los recursos informáticos de las entidades gubernamentales.

1) La gestión eficaz de incidentes también exige que se formulen y apliquen políticas, procedimientos, metodologías, controles de seguridad y herramientas para proteger los activos informáticos, sistemas, redes y funciones del gobierno. Desde la perspectiva de los CIRT, esto incluye los procedimientos normalizados de operación (SOP, Standard Operating Procedures), orientaciones para la operación interna y externa, políticas de seguridad aplicables a la coordinación de las partes interesadas, instalación de redes informativas seguras para los CIRT y comunicaciones seguras. En su calidad de entidades coordinadoras de la intervención, los CIRT deben ponerse de acuerdo entre sí y ayudar a facilitar la colaboración con otras entidades de respuesta ante incidentes. Los gobiernos también deben proporcionar formación continuada a los efectivos nuevos y antiguos en el tema de intervención en caso de incidentes.

IV.B.7 Establecer una unidad dentro del CIRT nacional con la capacidad necesaria para coordinar operaciones públicas y responder a ciberataques en gran escala y recuperarse de sus efectos.

1) En caso de que se produzca un incidente que adquiera significación nacional, habrá necesidad de disponer de un punto de contacto central para entablar relaciones de coordinación con otras entidades públicas, así como con otras comunidades de participantes, tales como el sector privado.

Resulta importante preparar planes y procedimientos para garantizar que el CIRT esté preparado para responder ante los incidentes que puedan sobrevenir.

IV.B.8 Promover prácticas de información responsables para proteger operaciones y la integridad de la ciberinfraestructura.

1) Ocasionalmente, pueden descubrirse vulnerabilidades en productos de tecnología de la información tales como equipos y programas informáticos. Las decisiones sobre divulgación pública deben tomarse caso por caso, para evitar que la información sobre vulnerabilidad se utilice indebidamente. Se debe conceder a los vendedores un amplio periodo de aviso antes de revelar ese tipo de vulnerabilidades.

PARTE V

Promoción de una cultura nacional de ciberseguridad

Considerando que los computadores personales son cada día más potentes, que las tecnologías convergen, que cada vez se utilizan más las TIC y que cada día son más las conexiones transfronterizas, quienes creen o posean servicios, los suministren o los gestionen y utilicen redes de información deben comprender los problemas de la ciberseguridad y tomar las medidas que correspondan a sus funciones para proteger las redes. Los gobiernos deben desempeñar un papel primordial en la creación de esta cultura de ciberseguridad y en el apoyo de los esfuerzos de los demás actores.

V.A Visión general de la Meta correspondiente a esta Parte

V.A.1 Promocionar una cultura nacional de ciberseguridad que responda a las Resoluciones 57/239, Creación de una cultura mundial de seguridad cibernética[14], y 58/199, Creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales[15] de la Asamblea General de las Naciones Unidas.

1) La promoción de una cultura nacional de ciberseguridad tiene que ver no solamente con el papel que desempeña el Estado a la hora de garantizar el funcionamiento y la utilización de las infraestructuras de información, entre otras, los sistemas explotados por el Estado, pero también proporcionar información sobre el particular al sector privado, la sociedad civil y los particulares. Asimismo, este elemento abarca la formación de usuarios de sistemas públicos y privados, las futuras mejoras de la seguridad y otros asuntos importantes, por ejemplo, la privacidad, el correo basura y el soporte lógico perjudicial.

2) Según la OCDE, los principales motores de una cultura de seguridad en el plano nacional son las aplicaciones y servicios de cibergobierno y la protección de infraestructuras de información nacionales esenciales. Así pues, las administraciones nacionales deberían implementar aplicaciones y servicios de cibergobierno, para mejorar sus operaciones internas y proporcionar mejores servicios al sector privado y a los ciudadanos. Por otra parte, habría que abordar la seguridad de los sistemas y redes de información no sólo desde el punto de vista tecnológico, sino también teniendo en cuenta factores tales como la prevención de riesgos, la gestión de riesgos y la sensibilización de los usuarios. A juicio de la OCDE, los efectos beneficiosos de las actividades de cibergobierno han ido más allá de las administraciones públicas y se están haciendo sentir por el sector privado y los particulares. Las iniciativas y cibergobierno han actuado, al parecer, como multiplicador para fomentar la difusión de una cultura de ciberseguridad.

3) Los países deberían adoptar, mediante actividades colaborativas y a través de algún tipo de acuerdo, una óptica multidisciplinaria y multipartita para implementar la ciberseguridad, y algunas naciones se encuentran estableciendo una estructura de gobernanza de alto nivel para aplicar políticas nacionales. La sensibilización y las iniciativas de educación, así como el intercambio de prácticas óptimas, la colaboración entre los participantes y la utilización de normas internacionales, se consideran actuaciones muy importantes.

4) La cooperación internacional, así como el papel que desempeñan las organizaciones regionales para facilitar interacciones e intercambios, se consideran aspectos sumamente importantes del fomento de una cultura de seguridad.

---

14 www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_57_239.pdf.

15 www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199.pdf.

V.B Medidas específicas para lograr esta Meta

V.B.1 Implementar un plan de ciberseguridad de los sistemas públicos.

1) La primera medida que debe adoptar un gobierno es garantizar la seguridad de los sistemas públicos, por lo que es necesario formular y ejecutar un plan nacional de seguridad. La preparación de dicho plan debe abordar la gestión del riesgo, así como el diseño y puesta en marcha de la seguridad. Tanto el plan como su ejecución deben evaluarse periódicamente a fin de medir el avance e identificar los campos en que se requiere mejorar el plan o su ejecución. Asimismo, en el plan habría que prever la gestión de incidentes, incluidas la respuesta, la vigilancia, la advertencia y la recuperación y los canales de intercambio de información. Por otra parte, el plan de seguridad debe abordar las actividades señaladas en el punto V.B.2 con objeto de formar a los usuarios de estos sistemas oficiales y obtener la colaboración mutua del gobierno, el sector privado y la sociedad civil respecto a la formación y a las iniciativas en materia de seguridad. Los temas principales de la formación son la sensibilización y la responsabilidad.

V.B.2 Poner en marcha programas de sensibilización e iniciativas en materia de seguridad para los usuarios de los sistemas y redes públicos.

1) Un programa eficaz de sensibilización con respecto a la ciberseguridad nacional debería contribuir a promover conciencia de ciberseguridad entre el público en general y las comunidades más importantes, así como a mantener las relaciones entabladas con los profesionales de ciberseguridad en el sector público, para intercambiar información sobre iniciativas de ciberseguridad, así como fomentar la correspondiente colaboración en materia de ciberseguridad. Habría que considerar tres componentes funcionales a la hora de diseñar un programa de sensibilización: 1) el suministro de información a las partes interesadas y compromiso de éstas, lo que promueve y mantiene relaciones de confianza entre el sector privado, el Estado y el mundo académico, con el fin de sensibilizar en materia de ciberseguridad y garantizar de manera eficaz seguridad del ciberespacio; 2) la coordinación necesaria para garantizar relaciones de colaboración en cuanto a los eventos y actividades de ciberseguridad en todos los niveles del Estado; y 3) las comunicaciones y mensajes, actividad que se centraría en el desarrollo de comunicaciones internas (dentro de los organismos gubernamentales encargados de este programa) y externas (con otros organismos gubernamentales, la industria, las instituciones educativas, los usuarios de computadores en el hogar y el público en general).

V.B.3 Alentar el desarrollo de la cultura de seguridad en las empresas

1) Desarrollar una cultura de seguridad en las empresas puede lograrse aplicando una serie de métodos innovadores. Un gran número de iniciativas gubernamentales se han dirigido a sensibilizar a las pequeñas y medianas empresas. El diálogo entre el Estado y las asociaciones de empresas o la colaboración entre ámbitos público-privado-personas puede ayudar a las administraciones a concebir e implementar iniciativas educativas y de capacitación. Entre tales iniciativas cabe citar: poner a disposición información (fuera de línea y en línea), por ejemplo, folletos, manuales, políticas modelo y conceptos; establecimiento de sitios web concretamente destinados a las PYME y otras partes interesadas; suministro de formación, (en línea); suministro de una herramienta de autoevaluación en línea; ofrecimiento de asistencia financiera y apoyo en materia fiscal u otros incentivos para promover la producción de sistemas seguros o adoptar medidas proactivas destinadas a fomentar la ciberseguridad.

V.B.4 Apoyar el suministro de información a la sociedad civil y en este sentido conceder especial atención a las necesidades de niños, jóvenes, personas con discapacidad y usuarios particulares.

1) Algunos gobiernos han colaborado con el sector empresarial para sensibilizar a los ciudadanos sobre las nuevas amenazas y las medidas para contrarrestarlas. En algunos países se organizan eventos concretos, como el día o la semana de la seguridad de la información, con actividades encaminadas a promocionar la seguridad de la información entre el público en general. El objetivo de la mayoría de las iniciativas consiste en ofrecer educación a niños y estudiantes bien sea a través de profesores, catedráticos y padres, o mediante la distribución directa de material de orientación. El material de apoyo utilizado puede variar de páginas web, juegos y herramientas en línea a tarjetas postales, libros de texto y diplomas que certifican los cursos tomados. Entre los ejemplos de dichas

iniciativas se cuentan cursos de formación dirigidos a los padres de jóvenes en los que se les informa sobre los riesgos a la seguridad, suministro de material de apoyo a los profesores, suministro a los niños de herramientas lúdicas en línea a través de las cuales se les transmite mensajes educativos relativos a la seguridad de la información, elaboración de libros de texto y juegos, diseño de un examen de certificación y una prueba sobre cómo navegar con seguridad por la web.

2) El Estado y el sector privado pueden compartir las lecciones aprendidas al diseñar los planes de seguridad y al formar a los usuarios, aprender de los éxitos e innovaciones de los otros y trabajar para mejorar la seguridad de las infraestructuras nacionales de la información.

V.B.5 Promocionar un programa nacional integral de sensibilización para que todos los actores, las empresas, los trabajadores considerados en general, y la población en general garanticen la seguridad de su parte del ciberespacio.

1) Muchas de las vulnerabilidades de los sistemas de información sobrevienen por falta de conciencia respecto a la seguridad por parte de los usuarios, los administradores de sistemas, los productores de tecnología, los encargados de compras, los auditores, los directores y los consejos de administración. Estas vulnerabilidades pueden entrañar riesgos importantes para las infraestructuras, aun cuando no formen parte de la infraestructura misma. Por ejemplo, la falta de conciencia en materia de seguridad de los administradores de sistemas suele convertirse en un punto débil de los planes de seguridad de las empresas. Promocionar los esfuerzos del sector privado para formar al personal y adoptar certificaciones del personal ampliamente reconocidas en materia de seguridad ayudará a reducir tales vulnerabilidades. La coordinación, por parte de los gobiernos, de las actividades nacionales de promoción y sensibilización tendentes a fomentar una cultura de seguridad fortalecerá la confianza del sector privado. La ciberseguridad es una responsabilidad compartida. Los portales electrónicos y las páginas web pueden servir para promover un programa de sensibilización nacional, que permita a los organismos públicos, el sector comercial y los consumidores particulares emprender acciones para proteger su parte del ciberespacio.

V.B.6 Fortalecer las actividades de ciencia y tecnología (S&T) y de investigación y desarrollo (I+D).

1) En la medida en que los gobiernos apoyen las actividades de ciencia y tecnología y de investigación y desarrollo, habrá que centrar ciertos esfuerzos en torno a las infraestructuras de la seguridad de la información. Mediante la identificación de prioridades de la I+D en lo que respecta al ciberespacio, los países pueden ayudar a dar forma a la creación de productos con seguridad integrada y a afrontar difíciles problemas técnicos. El hecho de que la I+D se realice en instituciones académicas puede brindar posibilidades para que los estudiantes participen en iniciativas de ciberseguridad.

V.B.7 Examinar el régimen de privacidad vigente y actualizarlo para incluir el entorno virtual.

1) Habrá que considerar los mecanismos sobre privacidad adoptados por diversos países y organizaciones internacionales como la OCDE. Las directrices de la OCDE sobre la protección de la privacidad y el flujo transfronterizo de información personal adoptadas el 23 de septiembre de 1980, siguen reflejando el consenso internacional respecto a las orientaciones generales sobre la forma en que la información personal se recoge y se administra. Al formular los principios fundamentales, las directrices desempeñan un papel importante puesto que ayudan a los gobiernos, al sector comercial y a los representantes de los consumidores a proteger la privacidad y la información personal y a evitar restricciones innecesarias a la comunicación, tanto virtual (en línea) como real, de datos a través de las fronteras.

V.B.8 Sensibilizar acerca del ciberriesgo y soluciones disponibles.

1) La solución de los problemas técnicos exige que los gobiernos, las empresas, la sociedad civil y los particulares usuarios colaboren para idear y aplicar medidas en las cuales se tome en consideración componentes tecnológicos (normas), procesos (directrices voluntarias o reglamentos obligatorios) y de personal (prácticas óptimas).

2) Un ejemplo de amenaza es el correo electrónico basura y los peligros que éste apareja, por ejemplo, el soporte lógico perjudicial. Una serie de organizaciones, incluida la UIT a través de la Cuestión 4

de la CE 17 del UIT-T, están trabajando sobre asuntos relacionados con el correo basura. El Anexo A proporciona una visión de alto nivel sobre este asunto.

3) La gestión de identidad es un ejemplo de herramienta tecnológica que sirve para responder a varias necesidades en materia de ciberseguridad. Una serie de organizaciones, incluida la UIT a través de la Cuestión 10 de la CE 17 del UIT-T, están trabajando sobre asuntos relacionados con la gestión de identidad. El Anexo B proporciona una visión de alto nivel sobre este asunto.

Apéndice 1

Lista de acrónimos

APECTEL	Grupo de Trabajo sobre Telecomunicaciones e Información de la Cooperación Económica Asia-Pacífico
CAN-SPAM	Ley sobre el control del embate de la pornografía y la publicidad no solicitadas de 2003 (Estados Unidos)
CCIPS	Sección de Ciberdelitos y Propiedad Intelectual (Departamento de Justicia de Estados Unidos)
CERT	Equipo encargado de intervenir ante emergencias informáticas
CERT-CC	Centro de Coordinación del equipo dispuesto a intervenir ante emergencias informáticas (de la Universidad Carnegie-Mellon, Estados Unidos)
CII	Infraestructuras de información esenciales
CIIP	Protección de las infraestructuras de información esenciales
CIRT	Equipo encargado de intervenir ante incidentes informáticos
COE	Consejo de Europa
CPNI	Centro para la Protección de la Infraestructura Nacional (Reino Unido)
CSIRT	Equipo de Intervención en caso de Incidentes de Seguridad Informática
CVE	Lista de vulnerabilidades y riesgos corrientes (Estados Unidos)
DHS	Departamento de Seguridad Nacional (Estados Unidos)
DOJ	Departamento de Justicia (Estados Unidos)
EU	Unión Europea
FAR	Reglamento Federal de Adquisiciones (Estados Unidos)
FCC	Comisión Federal de Comunicaciones (Estados Unidos)
FIRST	Foro de los equipos de intervención en caso de incidentes de seguridad
G8	Grupo de los Ocho (Países)
TIC	Tecnologías de la Comunicación y la Información
IMPACT	Asociación Multilateral Internacional contra las Ciberamenazas
ISAC	Centros de Análisis e Intercambio de Información (varios, tales como IT-ISAC; Estados Unidos)
IT-ISAC	Tecnología de la Información – Centro de Intercambio y Análisis de Información
ITAA	Asociación Estadounidense de Tecnología de la Información
LAP	Programa de Acción de Londres
MSCM	Mensaje comercial del servicio móvil
NIAC	Consejo Nacional sobre Protección de la Información (de la ITAA)
NIATEC	Centro Nacional de Educación y Formación en materia de Protección de la Información (de la Universidad de Idaho, Estados Unidos) (www.niatec.org)
NIST	Instituto Nacional de Normas y Tecnología (Estados Unidos)

NRIC	Consejo de Fiabilidad e Interfuncionamiento de la Red (FCC de Estados Unidos)
NSTAC	Comité Consultivo sobre Telecomunicaciones y Seguridad Nacional (DHS de Estados Unidos)
NVD	Base nacional de datos sobre vulnerabilidades (Estados Unidos) (nvd.nist.gov/nvd.cfm)
OCDE	Organización de Cooperación y Desarrollo Económicos (www.oecd.org)
OVAL	Lenguaje abierto para evaluación de la vulnerabilidad (www.oval.mitre.org)
RTPC	Red telefónica pública conmutada
I+D	Investigación y Desarrollo
S&T	Ciencia y Tecnología
PYME	Pequeña y mediana empresa
SMS	Servicio de mensajes cortos
SOP	Procedimientos normalizados de operación
TCPA	Ley de protección del abonado telefónico (Estados Unidos)
UNGA	Asamblea General de las Naciones Unidas

Apéndice 2

Estrategia para hacer efectiva la cooperación en materia de ciberseguridad y medición de su eficacia

El enfoque descrito a continuación emplea una metodología de trabajo diseñada para que, con prioridad nacional, los países establezcan sólidos sistemas de ciberseguridad. La metodología se divide en tres etapas diferentes que harán que los países pasen de la evaluación inicial de su capacidad a la puesta en marcha y evaluación de un programa de trabajo. A continuación se presenta esta metodología por etapas:

Estrategia para hacer efectiva la cooperación en materia de ciberseguridad y medición de su eficacia

Etapa 1 – Analizar, evaluar y recomendar un programa de colaboración.

- **Analizar:** En el primer paso el país realiza un análisis del estado actual de su programa de seguridad. Dicho análisis corre a cargo de un equipo de expertos, que utiliza un instrumento de análisis normalizado.
- **Evaluar:** Gracias a la información recogida durante el análisis se prepara un panorama de los puntos fuertes y las insuficiencias del programa sobre ciberseguridad del país y puede determinarse dónde deben centrarse los esfuerzos.
- **Recomendar:** El entendimiento producto de la evaluación permite sentar las bases de un plan para satisfacer las necesidades del país.

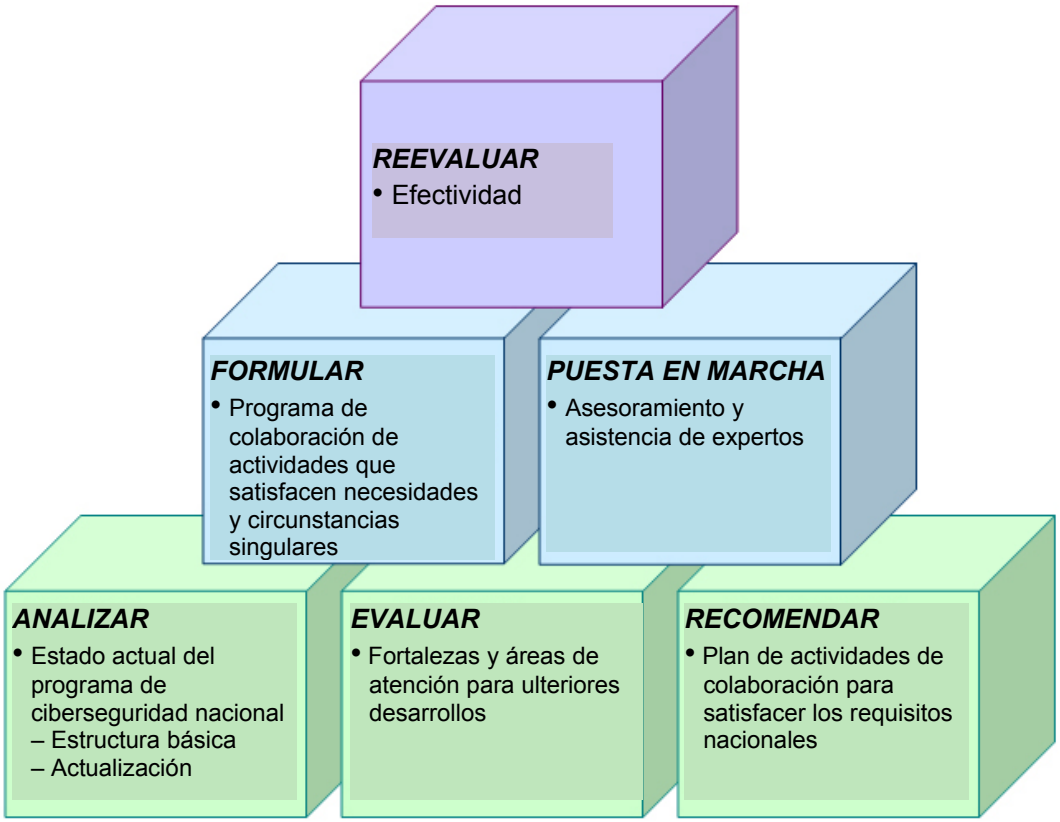
Etapa 2 – Formulación y puesta en marcha de un programa de colaboración.

- **Formulación de un programa de colaboración:** Los expertos nacionales se reúnen entre sí o con sus interlocutores internacionales para diseñar, definir y ajustar las actividades que permitan satisfacer las necesidades peculiares del país en particular. Las actividades pueden abarcar diversas actividades de colaboración y la identificación de necesidades materiales a largo plazo.
- **Puesta en marcha del programa de colaboración:** Los expertos nacionales y, en su caso, internacionales ejecutan el programa de colaboración y ofrecen asesoría concreta.

Etapa 3 – Evaluación del programa de colaboración para medir la eficacia y complementarlo.

- **Programa de colaboración evaluado:** Periódicamente, la eficacia del programa de colaboración se evalúa internamente o con países interlocutores. Los aspectos que se consideren deficientes pueden someterse a otros intercambios de colaboración y el proceso se inicia nuevamente. Si algún país colabora con otros, puede reducirse gradualmente su colaboración, si se considera que el programa del país es eficaz.

Figura 1: Metología del programa para constituir capacidades en materia de ciberseguridad



Medición de la eficacia

El siguiente esquema permite medir la evolución de la eficacia en este campo y demostrar los avances a los funcionarios superiores. El esquema plantea la construcción de una secuencia lógica que permite vincular las entradas básicas (programas del país y/o de la región que tienen asignados tiempo, dinero y recursos humanos) con el resultado final deseado (aumento de la ciberseguridad). A continuación se ilustra la secuencia:

Categoría de la medición:	**Elemento de ejecución:**
Entrada básica:	**Programas de país:** • Tiempo • Dinero • Personal
Procesos básicos de trabajo:	**Actividades, incluidos posibles intercambios cooperativos respecto a:** • La elaboración de la estrategia nacional • La formulación jurídica y reglamentaria • La gestión de incidentes

- Colaboración entre los ámbitos público-privado-personal
- La cultura de la ciberseguridad

Salidas básicas:

Número de:

- Reuniones o intercambios de cooperación
- Contactos con altos funcionarios técnicos y políticos

Resultados intermedios:

Resultados nacionales:

- Nuevas leyes y reglamentos sobre ciberdelito
- Acciones de cumplimiento
- Creación de un CSIRT
- Programas de sensibilización del gobierno y la industria
- Investigaciones sobre respuesta ante incidentes
- Participación en actividades de organizaciones internacionales relacionadas con la ciberseguridad
- Cumplimiento de convenios y directrices internacionales

Resultado posterior: Disminución del riesgo en materia de ciberseguridad como consecuencia del marco jurídico y político, de la respuesta a incidencias y de los esfuerzos en pos de una mayor concienciación.

Resultado final: Un aumento de la ciberseguridad nacional y de la seguridad en general.

Anexo A

Estudio de Caso: Spam

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Serie X

Suplemento 6
(09/2009)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Suplemento sobre la lucha contra el correo basura y amenazas afines

¡PRECAUCIÓN!

RECOMENDACIÓN PREPUBLICADA

Esta prepublicación es una versión no editada de una Recomendación aprobada recientemente. Será sustituida por la versión publicada una vez ésta sea editada. Por lo tanto, existirán diferencias entre esta prepublicación y la versión publicada.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT [ha/no ha] recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección www.itu.int/ITU-T/ipr/

Suplemento 6 a las Recomendaciones UIT-T de las Serie X

Recomendaciones de la Serie UIT-T X.1240 – Suplemento sobre la lucha contra el correo basura y amenazas afines

Resumen

En este Suplemento se establece que para luchar con eficacia contra el correo basura, los Estados han de aplicar un conjunto diverso de enfoques, incluyendo un marco jurídico efectivo, herramientas tecnológicas y la educación tanto del consumidor como de las empresas. Se analizan los foros internacionales en los que se aborda el asunto del correo basura. Como caso de estudio, y con fines ilustrativos, se proporciona información sobre cómo se ha abordado el problema del correo basura en los Estados Unidos de América y Japón.

Origen

El Suplemento 6 de las Recomendaciones UIT-T de la Serie X fue acordado el 25 de septiembre de 2009 por la Comisión de Estudio 17 del UIT-T (2009-1012).

ÍNDICE

Página

1 Alcance 39

2 Referencias 39

3 Definiciones 39

4 Abreviaturas y acrónimos 39

5 Convenios 40

6 Antecedentes 40

7 Enfoques nacionales para abordar de forma efectiva el correo basura y las amenazas afines 40
- 7.1 Estrategia nacional y correo basura 40
- 7.2 Fundamentos jurídicos y reglamentarios y correo basura 40
- 7.3 Colaboración entre gobierno e industria y promoción de la sensibilización nacional respecto al correo basura 41

8 Iniciativas internacionales (multilaterales) contra el correo basura 41
- 8.1 Plan de Acción de Londres 41
- 8.2 Conjunto de herramientas de la OCDE contra el correo basura y recomendación del Consejo sobre cooperación para la aplicación de las leyes contra el correo basura 42
- 8.3 Simposio de APEC TEL sobre correo basura 42

9 Caso de estudio sobre algunas actividades en los Estados Unidos contra el correo basura 42
- 9.1 Estados Unidos 43
  - 9.1.1 Leyes que establecen determinados requisitos a quienes envían correos electrónicos comerciales (Ley CAN-SPAM) 43
  - 9.1.2 Reglamentación que prohíbe el envío de correo electrónico comercial a dispositivos inalámbricos 43
  - 9.1.3 Métodos para limitar el hurto de identidades y credenciales financieras (phishing) 44
- 9.2 Japón 44
  - 9.2.1 Observancia de la ley 44
  - 9.2.2 Consejo para la promoción de la adopción de medidas contra el correo basura 45
  - 9.2.3 Centro de Ciberlimpieza (Cyber Clean Center, CCC) 45
  - 9.2.4 Bloqueo del puerto de salida 25 (OP25B) 45
  - 9.2.5 Tecnologías para la autentificación del remitente 46
  - 9.2.6 Intercambio de información sobre remitentes de correo basura entre operadores de comunicaciones móviles 46

Bibliografía 47

Suplemento 6 a las Recomendaciones UIT-T de las Serie X

Recomendaciones de la Serie UIT-T X.1240 – Suplemento sobre la lucha contra el correo basura y amenazas afines

1 Alcance

Este Suplemento trata sobre el correo basura y amenazas afines y está dirigido a funcionarios nacionales para los que el correo basura es un concepto nuevo y precisan información básica al respecto.

El Suplemento analiza las herramientas necesarias para combatir eficazmente el correo basura y describe los estudios que sobre el mismo están realizando determinados foros internacionales. Con fines ilustrativos, incluye como caso de estudio una descripción de lo que se está haciendo en los Estados Unidos de América y Japón para combatir el correo basura.

2 Referencias

Ninguna.

3 Definiciones

3.1 Peska o hurto de identidades y credenciales financieras (*phishing*) – intento de engaño dirigido a una persona para que acceda a un sitio web falso destinado a sustraer información privada de dicha persona.

3.2 correo basura (*spam*) – aunque no existe una definición acordada con carácter universal del correo basura, el término se utiliza para describir comunicaciones electrónicas masivas no solicitadas a través de correo electrónico o de mensajería móvil (SMS, MMS).

4 Abreviaturas y acrónimos

Este Suplemento utiliza las siguientes abreviaturas:

ADSP	Prácticas de envío de dominio de autor
APEC TEL	Grupo de Trabajo sobre Telecomunicaciones e Información de la Cooperación Económica Asia-Pacífico
CAN-SPAM	Ley sobre el control del embate de la pornografía y la publicidad no solicitadas de 2003 (Estados Unidos)
CNSA	Red de contactos de autoridades contra el correo basura (Unión Europea)
DKIM	Correo identificado claves de dominio
FCC	Comisión Federal de Comunicaciones (Estados Unidos)
FTC	Comisión Federal de Comercio (Estados Unidos)
ISP	Proveedor de servicios Internet
JEAG	Grupo contra los abusos del correo electrónico en Japón
LAP	Programa de Acción de Londres
MAAWG	Grupo de trabajo contra el abuso en el servicio de mensajería
MMS	Servicio de Mensajes Multimedia
MSCM	Servicio Móvil de Mensajes Comerciales del servicio móvil
OCDE	Organización de Cooperación y Desarrollo Económicos

OP25B Bloqueo del puerto de salida 25

SMS Servicio de mensajes cortos

SPF Marco de política del remitente

5 Convenios

Ninguno.

6 Antecedentes

6.1 El **correo basura (*spam*)** ha pasado de ser una fuente de comunicaciones molestas con publicidad a un medio que puede generar un grave problema de ciberseguridad. Así, por ejemplo, el correo basura puede ser un vehículo para el engaño, la difusión de soporte lógico perjudicial tales como virus y soportes lógico espías, y una forma de inducir a los consumidores a proporcionar información confidencial que puede ser utilizada posteriormente para la usurpación de la identidad (es decir, la peska o *phishing*). Los generadores de correo basura aprovechan que pueden mandar sus mensajes desde cualquier lugar del mundo a cualquier persona con un costo extremadamente bajo. Ello convierte al correo basura en un problema internacional que debe ser abordado mediante la cooperación internacional.

6.2 La **peska (*phishing*)** se aprovecha de que debido a una característica básica del sistema de correo de Internet[16], cualquier persona puede enviar un correo electrónico a otra prácticamente sin forma alguna de autenticación. La peska constituye un intento de engañar a alguien para que acceda a una página web falsa con la intención de hurtar información privada a dicha persona. Dicha práctica existe en buena medida debido a que en algunas ocasiones las personas esperan recibir correos electrónicos desde sitios web conocidos y sencillamente no se percatan que el correo electrónico no procede del sitio web legítimo. Debido a la escasa autenticación que ofrece un correo electrónico, es difícil determinar si el mensaje es legítimo sin hacer una cuidadosa inspección del mismo. Dicho examen cuidadoso requiere un conocimiento sustancial de los mecanismos subyacentes de la red.

La *peska* también existe porque para muchas personas resulta difícil verificar que los sitios web a los que acceden son legítimos. En ocasiones no se examina cuidadosamente la URL de una página web antes de introducir información sensible, y en ocasiones, no se conoce cuál es la URL correcta.

Los servidores web utilizados para la peska son frecuentemente victimas de soporte lógico perjudicial, haciendo que sea extremadamente difícil realizar el seguimiento de quienes realizan el hurto de identidades.

6.3 El **soporte lógico prejudicial (*malware*)** o malicioso, se hace ejecutar en un dispositivo sin el conocimiento o autorización del propietario, es asimismo un grave problema.

7 Enfoques nacionales para abordar de forma efectiva el correo basura y las amenazas afines

7.1 Estrategia nacional y correo basura

En relación con la estrategia nacional a adoptar, para conseguir una lucha efectiva contra el correo basura los países deben diseñar y mantener un combinación de elementos que incluya un sistema legal eficiente, autoridades y herramientas para velar por el cumplimiento de la ley, herramientas tecnológicas y prácticas óptimas, así como la educación del consumidor y las empresas para luchar contra el correo basura.

7.2 Fundamentos jurídicos y reglamentarios y correo basura

En cuanto a los fundamentos jurídicos y el marco reglamentario, las autoridades facultadas para abordar el correo basura deben contar con la autoridad necesaria para investigar y emprender acciones contra la

---

[16] El sistema de correo electrónico por Internet fue diseñado en los años 70 cuando el acceso a Internet estaba limitado a grupos reducidos de investigadores y a miembros de los Estados. No era necesaria la autenticación de la identidad de quienes remitían los correos electrónicos y, por tanto, no se hicieron esfuerzos para diseñar un sistema que contara con dichas medidas. Aunque el sistema de correo electrónico ha evolucionado desde entonces, esta omisión básica ha perdurado desde entonces.

violación de las leyes relativas al correo basura originado en su propio país o que afecte otros países. Dichas autoridades deberían disponer de mecanismos para colaborar con autoridades de otros países y priorizar las solicitudes de ayuda de éstas en base a aspectos de interés común o cuando sus efectos perjudiciales sean importantes.

7.3 Colaboración entre gobierno e industria y promoción de la sensibilización nacional respecto al correo basura

Todos los interesados, incluidas las autoridades responsables de la observancia, los comerciantes, los grupos de industria y los grupos de consumidores deben cooperar para combatir las violaciones a las leyes sobre correo basura. Los organismos de control oficiales deben aliarse con la industria y los grupos de consumidores para formar a los usuarios y promover el intercambio de información. Los organismos encargados de aplicar la ley deben cooperar con el sector privado a fin de promocionar el desarrollo de herramientas tecnológicas para combatir el correo basura, incluidas herramientas que faciliten la localización e identificación de quienes lo originan.

El hurto de identidades y credenciales financieras (*phishing*) suele ser un delito que puede prevenirse. Los gobiernos deberían colaborar con el sector privado para hacer más eficaces las medidas existentes para proteger a los ciudadanos contra el mismo, y educar a consumidores y empresas sobre métodos seguros de autenticación.

Asimismo, los gobiernos pueden jugar un papel importante en la educación del público sobre la necesidad de mantener una vigilancia permanente sobre el soporte lógico perjudicial mediante la utilización de herramientas tales como software antivirus y la aplicación de los parches más recientes de los sistemas operativos y las últimas técnicas de computación confiable.

8 Iniciativas internacionales (multilaterales) contra el correo basura

Existen varios foros multilaterales al seno de los cuales se desarrollan iniciativas de lucha contra el correo basura:

8.1 Plan de Acción de Londres

En 2004, la FTC (Comisión Federal de Comercio) y la Oficina del Reino Unido para el Comercio Equitativo organizaron en Londres una conferencia internacional sobre observancia de las leyes de correo basura, que llevó a la creación del Plan de Acción de Londres (LAP) sobre cooperación internacional para la observancia de las leyes de *correo basura*. Desde agosto de 2008, organismos gubernamentales y representantes del sector privado de más de 25 países se han adherido al plan. El LAP alienta a las partes interesadas, incluidos los organismos encargados de la observancia de las leyes sobre *correo basura* y los representantes del sector privado a que se incorporen como miembros de la organización.

El propósito del LAP consiste en promocionar la cooperación internacional para la aplicación de las leyes sobre *correo basura* y abordar los problemas relativos a este tipo de correo, como el fraude y engaño en línea, la usurpación de identidad y la diseminación de virus. A través del LAP se establecen relaciones entre estas entidades que se formalizan mediante un breve documento que formula un plan de trabajo básico para mejorar la aplicación a nivel internacional y la cooperación contra el correo basura ilegal. El documento no es de carácter vinculante y mediante él las partes se comprometen únicamente a hacer lo que les sea posible para que avance el plan de trabajo. Véase www.londonactionplan.org/

Desde su creación, el LAP ha organizado talleres todos los años, generalmente en colaboración con la Red de contacto de las Autoridades que combaten el correo basura (CNSA, *Contact Network of Spam Authorities*) de la Unión Europea. En octubre de 2007, el LAP y la CNSA celebraron su taller mixto anual simultáneamente con la Conferencia del Grupo de Trabajo contra el abuso en mensajería, en Arlington, Virginia, lo cual permitió una mayor cooperación con el sector privado en lo que concierne a la observancia de las leyes. En octubre de 2008, el LAP y la CNSA celebraron su taller mixto anual simultáneamente con la Sexta Cumbre Alemana contra el correo basura de Eco (Asociación alemana de empresas de Internet) en Wiesbaden, Alemania.

8.2 Conjunto de herramientas de la OCDE contra el correo basura y recomendación del Consejo sobre cooperación para la aplicación de las leyes contra el correo basura

En abril de 2006, el Grupo Especial de Trabajo contra el correo basura de la OCDE publicó un "conjunto de herramientas" contra el mismo, que contiene recomendaciones para ayudar a los encargados de formular políticas, reguladores y agentes de la industria a orientar sus políticas respecto a este tipo de correo y a restablecer la confianza en Internet y el correo electrónico. El conjunto de herramientas contiene ocho elementos, entre los que se incluye reglamentación contra el correo basura, soluciones impulsadas por la industria y tecnologías para combatir el correo basura, educación y sensibilización y cooperación/divulgación general. Al reconocer que la cooperación internacional es clave para combatir el correo basura, los gobiernos miembros de la OCDE aprobaron una "Recomendación sobre cooperación transfronteriza para la aplicación de las leyes contra el correo basura", que insta a los gobiernos a asegurarse de que sus leyes permitan a las autoridades de control intercambiar información con otros países y a hacerlo rápida y eficazmente. Véase www.oecd-antispam.org/sommaire.php3

8.3 Simposio de APEC TEL sobre correo basura

En abril de 2006, APEC TEL realizó un simposio sobre "Correo basura y amenazas afines" que reunió a 30 oradores y panelistas para debatir la evolución del problema del correo basura y formular un programa de trabajo común para el grupo de trabajo sobre telecomunicaciones y información. Los principales temas tratados incluyeron:

1) la formulación y aplicación de regímenes reglamentarios nacionales contra el correo basura, incluidas la observancia y las normas de conducta;
2) el papel desempeñado por la industria en la lucha contra el correo basura, incluidas la colaboración entre gobierno e industria;
3) respuesta técnica ante el correo basura;
4) cooperación y observancia transfronteriza, incluido el Convenio del Consejo de Europa sobre ciberdelito y la Recomendación del Consejo de la OCDE sobre cooperación para la observancia, como herramientas fundamentales para reforzar la cooperación; y
5) la necesidad de educación del consumidor y de aumento de la sensibilización.

Los siguientes son algunos pasos concretos que el Grupo sobre telecomunicaciones e informática acordó seguir:

1) alentar el intercambio de información sobre reglamentación y políticas, recurriendo a recursos como el Conjunto de herramientas de la OCDE contra el correo basura;
2) elaborar una lista de personas de contacto para las autoridades contra el correo basura de APEC, a fin de ampliar los recursos similares creados por la OCDE y la UIT;
3) alentar a las economías a unirse voluntariamente a foros de cooperación como el Plan de Acción de Londres o el Acuerdo de Seúl-Melbourne;
4) cooperar con la OCDE en iniciativas relativas al intercambio de información y la orientación; y
5) apoyar la creación de capacidades de las economías en desarrollo para favorecer la lucha contra el correo basura.

9 Caso de estudio sobre algunas actividades en los Estados Unidos contra el correo basura

A continuación se presenta un resumen de las leyes contra el correo basura existentes en algunos países.

9.1 Estados Unidos

9.1.1 Leyes que establecen determinados requisitos a quienes envían correos electrónicos comerciales (Ley CAN-SPAM)

En 2003, Estados Unidos promulgó la Ley CAN-SPAM, que formula exigencias para quienes envíen correo electrónico con fines comerciales, se detallan las penalizaciones para quienes originen el correo basura y para las compañías cuyos productos se publiciten ilegalmente mediante correo basura y faculta al consumidor para que pueda solicitar a quien origina este tipo de correo que deje de enviárselo.

Entre las disposiciones principales de la Ley CAN-SPAM, cabe citar las siguientes:

- **Se prohíben encabezamientos de correo engañosos**. La información de encaminamiento de los correos, "De:" y "Para:", incluidos el nombre de dominio y dirección electrónica de origen, deben ser correctos y deben identificar a la persona que envía el correo.
- **Se prohíben líneas de "asunto:" engañosas.** La línea del asunto no debe confundir al receptor sobre el asunto contenido en el mensaje.
- **Se exige que el correo indique a los destinatarios un método de exclusión voluntaria.** Quien remite el correo debe proporcionar una dirección de correo electrónico u otro mecanismo de respuesta por Internet a través del cual el destinatario pueda solicitar que no se le sigan enviando correos a su dirección de correo electrónico, y el remitente del correo debe aceptar y cumplir dicha solicitud. El remitente debe diseñar una "lista" de posibilidades que permita al destinatario excluirse voluntariamente del envío de cierto tipo de correo comercial del remitente, y en todo caso, se debe incluir la opción de dejar de recibir cualquier mensaje del remitente. Todo mecanismo de exclusión voluntaria debe procesar solicitudes de exclusión durante al menos 30 días después de enviado el correo electrónico comercial. Una vez reciba una solicitud de exclusión voluntaria, la ley otorga un plazo de 10 días hábiles al remitente para que suspenda el envío de correo a quien solicitó la exclusión. El remitente no puede colaborar con otra entidad para enviar correo a una dirección electrónica ni hacer que otra entidad envíe a su nombre correos a dicha dirección. Por último, es ilegal que el remitente venda o comunique las direcciones electrónicas de personas que hayan elegido no recibir su correo, ni siquiera en la forma de lista de correos, salvo que el remitente las comunique para que otra entidad pueda cumplir la ley.
- **Se exige que el correo electrónico comercial sea identificado como publicitario e incluya la dirección postal válida del remitente.** El mensaje del remitente debe advertir claramente y de forma visible que se trata de un mensaje publicitario o solicitación y que el destinatario tiene la posibilidad de dejar de recibir voluntariamente este tipo de mensajes del remitente. El mensaje también debe incluir la dirección postal válida del remitente.

La Comisión Federal de Comercio (FTC), en calidad de organismo autorizado para la observancia de los principios y normas del derecho civil, tiene facultad para aplicar la Ley CAN-SPAM y establecer sanciones administrativas de hasta 11 000 USD cada vez que tenga lugar una violación de la misma. Desde que en 1997 adoptó su primera acción de cumplimiento de la ley aplicada al correo basura, la FTC ha combatido las prácticas engañosas y desleales en materia de correo basura mediante 94 acciones de este tipo, 31 de las cuales se aplicaron a violaciones de la Ley CAN-SPAM.

La Ley CAN-SPAM también faculta al Departamento de Justicia (DOJ) para aplicar las sanciones penales. Esta Ley estipula penas considerables, incluida la prisión, a quien envíe correo basura. Otros organismos federales o estatales pueden hacer que organizaciones bajo su jurisdicción cumplan la ley y las empresas proveedoras de acceso a Internet también pueden multar a los infractores.

9.1.2 Reglamentación que prohíbe el envío de correo electrónico comercial a dispositivos inalámbricos

Estados Unidos también ha adoptado reglas para proteger a los consumidores contra el correo basura recibido en dispositivos inalámbricos. Salvo algunas excepciones, las reglas prohíben el envío de mensajes de correo electrónico comerciales, incluidos el correo electrónico y ciertos mensajes de texto, a dispositivos inalámbricos, como teléfonos celulares. Las reglas son válidas únicamente para los mensajes considerados

"comerciales" según la Ley CAN-SPAM y para los mensajes cuyo propósito principal sea la publicidad comercial o la promoción de un producto o servicio comercial. Los mensajes que no sean de índole comercial, como los de los candidatos a ejercer cargos públicos o los que informan a los clientes del estado de su cuenta, no están sujetos a estas reglas.

Los mensajes comerciales del servicio móvil (MSCM, *mobile service commercial messages*) incluyen cualquier mensaje comercial enviado a una dirección electrónica suministrada por un proveedor de servicios móviles del dispositivo inalámbrico de un abonado. Los MSCM están prohibidos salvo que el destinatario individual haya dado al remitente autorización previa (denominada requisito de "inclusión voluntaria"). Las normas prohíben el envío de mensajes comerciales a direcciones que contengan nombres de dominio que hayan estado figurando en la lista de la FCC durante al menos 30 días, o en cualquier momento antes de esos 30 días si el remitente tiene conocimiento por cualquier otra fuente de que el mensaje se dirige a un dispositivo inalámbrico. Para ayudar a los remitentes de mensajes comerciales conozcan qué direcciones pertenecen a abonados inalámbricos, las reglas exigen que los proveedores de servicios inalámbricos proporcionen a la FCC los nombres de los nombres de dominio pertinentes. Esta protección no abarca los mensajes del servicio de mensajes cortos (SMS) transmitidos exclusivamente a números telefónicos. Las llamadas de marcación automática ya están cubiertas por otras leyes.

Las normas de la FCC estipulan que la FCC puede imponer a quienes envíen correo basura multas que pueden llegar a 11 000 USD por infracción si no se trata de un concesionario de licencia y a 130 000 USD por infracción en el caso de concesionarios de licencias de operador. Además de la penalización monetaria, la FCC puede emitir un mandamiento de cese de la práctica comercial contra el remitente de correo basura que viole cualquier disposición de la Ley de comunicaciones o cualquier norma de la FCC autorizada por la Ley. Adicionalmente, de conformidad con la Ley de comunicaciones, el infractor de cualquier disposición de la Ley está sujeto a enjuiciamiento penal por parte del Departamento de Justicia (además de la pena monetaria), y puede incurrir en prisión de hasta 1 año (o de hasta 2 años en caso de reincidencia). A la fecha, la FCC no ha iniciado ningún proceso ejecutorio en relación con este tipo de mensajes comerciales.

9.1.3 Métodos para limitar el hurto de identidades y credenciales financieras (*phishing*)

Como se dijo antes, quienes cursan correo basura y cometen hurto de identidades y credenciales financieras (*phishing*) cuentan con el hecho de que no se conoce quién envía un mensaje. Actualmente, los participantes en el Grupo Especial sobre Ingeniería de Internet (IETF) han divulgado dos normas, a saber: Domain Keys Identified Mail (DKIM) [b-IETF RFC 4871] y Author Domain Sending Practices (ADSP) [b-IETF RFC 5617] que mejoran la capacidad de los receptores para identificar a quienes les envían correos electrónicos. Los vendedores han comenzado a poner las implementaciones a disposición de los usuarios. Hay al menos una implementación gratuita[17] de dicha norma. Una fuente de asistencia es el Grupo de Trabajo contra la peska (APWG, *Anti-Phishing Working Group*), asociación de la industria que se dedica esencialmente a eliminar el robo y la utilización fraudulenta de identidades a que da lugar el creciente problema que suponen la peska y la falsificación del correo electrónico (*spoofing*). Dicho foro permite discutir los diferentes aspectos de la peska, realizar pruebas y evaluaciones de las posibles soluciones tecnológicas y acceder a un inventario centralizado de incidentes del mismo (www.antiphishing.org).

Así pues, esta norma permite "validar con arreglo a una lista blanca", o la capacidad de verificar que quienes intentan entrar en contacto con ellas son realmente sus amigos o asociados. Esta norma mencionada limita, por su propia índole, algunas formas de *phishing*, pero no todas ellas.

9.2 Japón

9.2.1 Observancia de la ley

En Japón hay dos leyes que restringen el envío de correo electrónico con miras a suprimir el correo basura, cuyos principales elementos son los siguientes:

---

[17] Por "gratuito" se entiende aquí la posibilidad de implementar esta característica sin el pago de regalías y en las condiciones especificadas por el titular de la correspondiente patente.

– Las siguientes reglas se aplican al envío de mensajes publicitarios por correo electrónico (Opt-in).
  – Está prohibido enviar mensajes publicitarios por correo electrónico sin el consentimiento del destinatario a recibirlo.
  – Al enviar el mensaje publicitario, la entidad remitente debe guardar pruebas del consentimiento del destinatario a recibirlo.
  – Los mensajes publicitarios deben contener información sobre la manera de poner término al envío de la publicidad, el nombre del remitente, etc.
  – Si el destinatario utiliza el procedimiento correcto para notificar al remitente que no desea seguir recibiendo mensajes publicitarios, la entidad no puede enviar ningún nuevo mensaje a ese destinatario.
– Está prohibido enviar mensajes electrónicos con falsa información sobre el remitente, por ejemplo correo electrónico, dirección IP y nombre de dominio falsos.
– Está prohibido enviar mensajes electrónicos a direcciones de destinatario ficticio generadas automáticamente por un programa informático.

9.2.2 Consejo para la promoción de la adopción de medidas contra el correo basura

En 2008 una diversidad de partes interesadas como PSI, empresas publicitarias, ASP para la entrega de anuncios publicitarios, vendedores de dispositivos de seguridad, organizaciones de consumidores, administraciones, etc., crearon el Consejo para la promoción de la adopción de medidas contra el correo basura. En noviembre de ese mismo año el Consejo adoptó una "Declaración a favor de la erradicación del correo basura".

9.2.3 Centro de Ciberlimpieza (Cyber Clean Center, CCC)

Este Centro, establecido como resultado de la estrecha colaboración entre el Gobierno japonés, las organizaciones relacionadas con los PSI y los principales PSI, detecta los PC que han sido infectados por redes robot (bot) o programas informáticos dañinos y funciona según se indica a continuación.

– El CCC gestiona un sistema de señuelos en gran escala, que detecta actividades de infección de PC por programas informáticos dañinos (en general redes robot). El sistema de señuelos compila las direcciones IP de los PC infecciosos y los códigos de los programas informáticos dañinos (bot).
– Se envía a todos los PSI listas de las direcciones IP y las fechas/horas en que éstas se detectaron. Cada uno de los PSI identifica las direcciones IP que corresponden a sus abonados y les informa que su PC podría estar infectado por software maliciosos. El PSI también les envía información sobre el CCC (enlace con la página web) y el software de desinfección.
– El CCC analiza los códigos de programas compilados. Cuando se trata de un código programático previamente no identificado, se fabrica y distribuye un nuevo software de desinfección capaz de destruir ese nuevo programa malicioso.

Este procedimiento contribuye a reprimir las actividades de infección por redes robot en Japón, y puesto que la mayoría de los mensajes de correo basura se envían desde PC infectados, también contribuye a reducir el volumen de correo basura enviado desde Japón.

9.2.4 Bloqueo del puerto de salida 25 (OP25B)

Cuando los abonados a un PSI envían y reciben mensajes de correo electrónico, en general utilizan un servicio de correo electrónico proporcionado por el PSI, de modo que ellos envían su mensaje al servidor de correo del PSI y éste retransmite el mensaje a los servidores de correo electrónico de destino. Normalmente los abonados a un PSI no envían sus mensajes directamente a los servidores de correo electrónico de destino. Dado que los PC infectados por virus o redes robot envían correo basura directamente a los servidores de correo electrónico de la dirección de destino, esos mensajes no pasan a través de los servidores de correo del PSI. Ahora bien, si se logra frenar las comunicaciones procedentes de PC de abonados que eluden la red del PSI utilizando SMTP (TCP con número de puerto de destino 25), se pueden bloquear muchos mensajes de

correo indeseable. Por lo tanto el Gobierno de Japón, los PSI y las organizaciones conexas estudiaron en estrecha cooperación:

– el efecto que tiene en los abonados la introducción del TCP de bloqueo del puerto de salida 25 (OP25B) (b-MAAWG MP25);

– las restricciones que impone la legislación en vigor en Japón al bloqueo de ciertas comunicaciones específicas.

Como resultado de esos estudios, actualmente numerosos PSI aplican el OP25B. El Grupo contra el abuso del correo electrónico en Japón (Japan Email Anti-abuse Group, JEAG) ha desempeñado una importante función en este proceso, sobre todo mediante la publicación de una recomendación por la que se insta a los PSI a introducir el OP25B.

– Aunque la introducción del OP25B no tiene carácter obligatorio para los PSI japoneses, en julio de 2009, 52 de ellos (incluidos los más importantes) lo habían adoptado.

– Muchos de los PSI que introducen el OP25B proporcionan TCP puerto 587 con SMTP AUTH, como una alternativa para comunicarse y no degradar la calidad del servicio. Los usuarios pueden presentar sus mensajes de correo procedentes de otro PSI adaptando el OP25B al servidor de correo de ese PSI.

9.2.5 Tecnologías para la autentificación del remitente

Se trata de técnicas concebidas para detectar la fuente de la simulación de direcciones de correo electrónico. El JEAG publicó una recomendación favorable a la introducción de estas técnicas, y el Ministerio de Comunicaciones y Asuntos Internos publicó un documento titulado "Importantes aspectos jurídicos de la introducción, por un PSI, de técnicas para la autentificación del remitente en el extremo receptor". Actualmente casi todos los operadores de comunicaciones móviles más importantes y algunos PSI han adoptado el Marco de Política del Remitente (SPF) (b-IETF RFC 4408), una de las tecnologías de autentificación del remitente, y sus abonados pueden utilizar el resultado de la autentificación para filtrar. La tasa más alta de SPF publicados para dominios "jp" fue del 35,99% en agosto de 2009. Además, varios PSI han comenzado a introducir DKIM (b-IETF RFC 4871) para la autentificación adicional del remitente.

9.2.6 Intercambio de información sobre remitentes de correo basura entre operadores de comunicaciones móviles

En Japón casi todos los teléfonos celulares tienen la capacidad de admitir mensajes generales de correo electrónico. Y dado que numerosos mensajes de correo basura se envían desde teléfonos móviles celulares, en Japón todos los operadores de comunicaciones móviles intercambian información sobre los remitentes de mensajes no deseados, conforme a los siguientes pasos.

– El ID de cualquier particular que desee hacer un contrato relacionado con teléfonos móviles se somete a verificación a tenor de la Ley para la prevención del uso inadecuado de teléfonos móviles.

– Si un operador de comunicaciones móviles determina que un usuario de teléfono celular envía mensajes de correo basura, en violación de la Ley sobre reglamentación de las transmisiones de correos electrónicos especificados, transmite los datos de ese usuario a todos los otros operadores de comunicaciones móviles.

Así pues, los usuarios que envíen mensajes de correo basura desde un teléfono celular tropezarán con dificultades para concertar un contrato relacionado con teléfonos móviles.

Además, una organización que funciona sin fines lucrativos instala detectores, compila mensajes de correo basura y los analiza. Posteriormente transmite información sobre los remitentes de esos mensajes a los PSI originadores en Japón e intercambia dicha información con algunas entidades de países extranjeros.

Bibliografía

[b-IETF RFC 4871] IETF RFC 4871 (2007), **Domainkeys** *Identified Mail (DKIM) Signatures*. www.ietf.org/rfc/rfc4871.txt

[b-IETF RFC 5617] IETF RFC 5617 (2009), *DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)*. www.ietf.org/rfc/rfc5617.txt

[b-MAAWG MP25] MAAWG Recommendation (2005), *Managing Port 25 for Residential or Dynamic IP Space Benefits of Adoption and Risks of Inaction*. www.maawg.org/port25

[b-IETF RFC 4408] IETF RFC 4408 (2007), *Sender Policy Framework (SPF) fo Authorizing Use of Domains in E-*Mail*, Version 1*. www.ietf.org/rfc/rfc4408.txt

[b-contr-spam] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (United States Code). This Act is documented in the following laws: 15 U.S.C. §§ 7701-7713; 18 U.S.C. § 1037; 28 U.S.C. § 994; 47 U.S.C. § 227. www.gpsaccess.gov/uscode/index.html

[b-ITU-T cyb] Messaging Anti-Abuse Working Group Conference reports: www.itu.int/ITU-D/cyb/cybersecurity/spam.html

Anexo B

Gestión de Identidades

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Serie X

Suplemento 7

(02/2009)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Suplemento sobre la visión general de la gestión de identidad en el contexto de la ciberseguridad

¡PRECAUCIÓN!
RECOMENDACIÓN PREPUBLICADA

Esta prepublicación es una versión no editada de una Recomendación aprobada recientemente. Será sustituida por la versión publicada una vez ésta sea editada. Por lo tanto, existirán diferencias entre esta prepublicación y la versión publicada.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección www.itu.int/ITU-T/ipr/

Suplemento 7 a las Recomendaciones UIT-T de las Serie X – Recomendaciones de la Serie UIT-T X.1250

Suplemento sobre la visión general de la gestión de identidad en el contexto de la ciberseguridad

Resumen

Aunque durante los muchos decenios de explotación de la red telefónica pública conmutada (RTPC) se han atendido a los problemas planteados por su seguridad, no puede decirse lo mismo de las redes IP públicas distribuidas con múltiples proveedores de servicios, tales como la Internet y las redes de la próxima generación (NGN). Dichas redes utilizan una plataforma de transporte común para el tráfico de control y para el tráfico de usuario que, además del posible carácter anónimo de dicho tráfico y la posibilidad de generación de tráficos unidireccionales, hace que dichas redes sean vulnerables ante un uso indebido. Todos los servicios electrónicos (cibernegocio, cibercomercio, cibersalud, cibergobierno, etc.) pueden ser objeto de ataques. Este problema puede resolverse en parte identificando a usuarios, especialmente cuando los usuarios son personas físicas, que pueden ser autenticadas, beneficiarse de acceso y ser auditadas. Debido a que la gestión de identidad proporciona mayores garantías y confianza en el usuario, en el proveedor de servicio y en las identidades de los dispositivos de la red, consigue mejorar la seguridad reduciendo la exposición a riesgos de seguridad. Este aspecto de la ciberseguridad es algo que los proveedores de servicio deben tomar en consideración en los planos comercial y técnico, y que los gobiernos deben considerar a nivel nacional como parte del plan de ciberseguridad nacional.

Introducción

La gestión de identidad (IdM) es una forma de gestionar y controlar la información utilizada en los procesos de comunicación para representar entidades (tales como proveedores de servicio, organizaciones que sean usuarios finales, personas, dispositivos de red, aplicación y servicios basados en software). Una entidad individual puede tener varias identidades digitales para acceder a varios servicios con distintos requisitos, que pueden estar presentes en varias localizaciones.

La IdM es un componente fundamental en la ciberseguridad ya que aporta la capacidad de establecer y mantener comunicaciones fiables entre entidades. La gestión de identidad no sólo soporta la autenticación de la identidad de una entidad, sino que también permite autorizar una gama de privilegios de acceso (en lugar de recurrir a la alternativa todo o nada en cuestión de accesos) y facilitar el cambio de los privilegios de acceso cuando se modifica la función que desempeña una entidad. La IdM hace posible también que una organización se cerciore de que sus políticas de seguridad se están aplicando adecuadamente, mediante la supervisión y auditoría de la actividad en la red de una entidad dada. La IdM puede proporcionar acceso a entidades dentro y fuera de una organización. Así pues, una buena solución IdM proporciona las capacidades fiables necesarias para autenticar identidades, proveer y gestionar identidades y auditar las actividades de una entidad.

La IdM es un factor esencial a la hora de gestionar la seguridad y hacer posible el acceso nómada y a petición a redes y ciberservicios. Junto con otros mecanismos de defensa (por ejemplo, murallas de fuego, sistemas de detección de intrusión y protección de virus), la IdM desempeña un importante cometido en lo que concierne a proteger las redes y servicios de información y comunicación contra ciberdelitos tales como el uso fraudulento y el robo de identidades. Esto, a su vez, aumenta la confianza de los usuarios en que las cibertransacciones serán seguras y fiables, lo que, a su vez, facilita la predisposición de los usuarios para utilizar redes IP para ciberservicios.

En la implementación de un sistema IdM, deben resolverse ciertas cuestiones fundamentales en materia de privacidad. Ello implica la elaboración de métodos que garanticen la exactitud de la información obtenida e impidan que sea utilizada con una finalidad distinta a la prevista.

1 Alcance

La gestión de identidad surge como un componente esencial que mejorará la seguridad, proporcionando una mayor garantía mediante la verificación de la validez de la información de identidad. Este Suplemento ofrece una visión general de este nuevo servicio.

La utilización en este Suplemento del término "identidad" en relación con la IdM no es indicativo de su significado absoluto. En particular, no constituye ningún tipo de validación positiva.

2 Referencias

Ninguna.

3 Definiciones

Las definiciones figuran en otras Recomendaciones de la Serie X.1250 del UIT-T.

4 Abreviaturas y acrónimos

IdM – Gestión de identidad (*identity management*)

IP – Protocolo Internet

RTPC – Red telefónica pública conmutada

5 Convenios

Ninguno.

6 Importancia de la gestión de identidad para la protección de la infraestructura de red global y la coordinación multinacional para la seguridad

La adecuada implementación y utilización de las capacidades y buenas prácticas de la gestión de identidad en las redes nacionales, regionales e internacionales reforzarán la seguridad de la infraestructura de red global. La implementación y aplicación de prácticas óptimas son factores importantes y necesarios para proporcionar garantías sobre la información de identidad y de la integridad y disponibilidad de la infraestructura de red global.

Las capacidades IdM pueden emplearse para soportar servicios nacionales e internacionales de telecomunicaciones de emergencia, identificando usuarios autorizados para recurrir a servicios especiales.

Por otra parte, estas capacidades sirven para prevenir, detectar y soportar la coordinación de las intervenciones ante incidentes de ciberseguridad nacionales e internacionales. En determinados casos, la IdM puede ayudar a las autoridades y entidades a coordinar sus esfuerzos para seguir y localizar los orígenes de dichos incidentes.

7 La gestión de identidad como facilitador de comunicaciones fiables entre dos entidades

Una función importante de la IdM es la autenticación de usuarios, redes o servicios. En un proceso de autenticación que implique a dos entidades, una hace aseveraciones acerca de su identidad a la otra. En función de los requisitos de seguridad de la segunda entidad, dichas aseveraciones pueden tener que ser validadas antes de que la segunda entidad tenga la suficiente confianza en la primera como para concederle privilegios. Este proceso puede ser necesario en ambos sentidos.

Existen varios niveles de confianza en la autenticación, desde poca o ninguna, débil (por ejemplo, nombre de usuario y contraseña) hasta fuerte (por ejemplo, infraestructura de clave pública (UIT-T X.509)). Una evaluación del riesgo puede identificar el nivel de autenticación adecuado. Una de las dos entidades puede requerir un nivel más alto de autenticación, por ejemplo, porque una de ellas controle recursos esenciales.

8 Protección, mantenimiento, revocación y control de datos de identidad

Otras funciones importantes de la IdM son la protección, el mantenimiento y el control de los datos de identidad fiables, incluida la capacidad de afirmar el estado actual de una identidad.

El marco legal o político puede requerir que la información de identificación personal se proteja y que la información sobre la identidad no pueda ser utilizada para fines distintos a aquellos por los que fue

recopilada. Otro aspecto que es necesario vigilar es la garantía de que los datos de la identidad siguen siendo válidos. Para aquellos servicios cuya viabilidad exige la utilización de datos de identidad, éstos deben ser mantenidos adecuadamente de forma que sean precisos, oportunos y consistentes.

Cuando sea pertinente, la gestión de los atributos de los datos de identidad incluyen la capacidad de verifica los datos de identidad para comprobar si han sido revocados.

En muchos casos, las entidades desearán controlar la utilización de sus propios datos e información privada.

9 "Descubrimiento" de fuentes fiables de datos de identidad

La IdM también conlleva el concepto de "descubrimiento" de datos de identidad confiables. En un entorno multiproveedor muy distribuido (como es el caso de Internet y de las redes de la próxima generación), los datos de identidad necesarios para que exista fiabilidad en la identidad y aseveraciones conexas de un entidad, pueden ser localizados en diferentes lugares de la red. Las entidades pueden tener múltiples identidades digitales con diferentes fuentes de información de identidad en lugares distintos. Cuando una de las dos entidades de un proceso de autenticación es nómada, la otra necesita localizar y establecer una relación de confianza con una fuente adecuada de información de identidad con el fin de completar el proceso de autenticación con la entidad nómada. El concepto de descubrimiento de fuentes de información fiables es similar a lo que ocurre actualmente cuando se utiliza el teléfono móvil.

10 Servicios del cibergobierno

Las ventajas que para una entidad conlleva la implementación de IdM incluyen la reducción del riesgo, el reforzamiento de la confianza, una mayor funcionalidad y una potencial reducción de los costos. Los motivos para la implementación de la IdM son igualmente válidos cuando la entidad es un gobierno. En los servicios del cibergobierno, los principales objetivos son asimismo la reducción de costos y proporcionar servicios más eficientes y de forma más eficaz a los ciudadanos y a las empresas.

Al igual que otras entidades, los gobiernos se enfrentan al desafío de cómo utilizar la identidad de una forma eficaz y eficiente en un mundo interconectado. Para que los servicios del cibergobierno sean una realidad, los gobiernos deben realizar análisis de riesgos en relación con los ciberservicios que intenta ofrecer e implementar los servicios de protección adecuados. La naturaleza sensible de muchos servicios del cibergobierno (por ejemplo, la cibersalud), pueden requerir al gobierno exigir una autenticación reforzada.

11 Consideraciones regulatorias sobre la gestión de identidad

Las administraciones nacionales y los grupos regionales deben tomar en consideración una serie de potenciales aspectos de carácter regulatorio en relación con la implementación de la gestión de identidad, tales como privacidad y protección de los datos, seguridad nacional y preparación para hacer frente a emergencias, así como acuerdos de carácter obligatorio entre operadores de telecomunicaciones. Los gobiernos no solo utilizan técnicas de gestión de identidad, sino que también pueden imponerlas a otras entidades con el fin de que se cumplan un amplio conjunto de objetivos de seguridad y política nacional.

Bibliografía

Entre los foros que trabajan sobre diferentes aspectos de la gestión de identidad, cabe citar:

ARK (Biblioteca Digital de California, clave de recursos de archivo): www.cdlib.org/inside/diglib/ark/

3GPP SA3: www.3gpp.org/SA3-Security?page=type_urls

ETSI TISPAN WG7: www.etsi.org/tispan/

Hoja de ruta de la Unión Europea en materia de ciberidentidad (eID): ec.europa.eu/information_society/activities/ict_psp/documents/eidm_roadmap_paper.pdf

Tarjeta del ciudadano europeo: europa.eu.int/idabc/servlets/Doc?id=19132

FIDIS (Futuro de la identidad en la sociedad de la información, UE): www.fidis.net/

FIRST (Forum of Incident Response and Security Teams): www.first.org/

Guía (Identidad del usuario gubernamental para Europa, UE): www.ist-world.org/ProjectDetails.aspx?ProjectId=4ddb2e61c84343f0acd370607e5a8499&SourceDatabaseId=7cff9226e582440894200b751bab883f

Handle: www.handle.net/

Higgins: www.eclipse.org/higgins/index.php

IDSP (Grupo Especial de Normas para la Prevención de Robos y la Gestión de Identidad, Instituto Estadounidense de Normas Nacionales): www.ansi.org/standards_activities/standards_boards_panels/idsp/overview.aspx?menuid=3

IGF (Marco de Gobernanza de Identidad, ORACLE): www.oracle.com/technology/tech/standards/idm/igf/index.html; véase Liberty Alliance

ITRC (Centro de Recursos contra el Robo de Identidad): www.idtheftcenter.org/

Grupo Especial de Ingeniería de Internet (IETF): sec.ietf.org/

UIT-T Comisión de Estudio 17 (Seguridad), Grupo Temático de Gestión de Identidad: www.itu.int/ITU-T/studygroups/com17/fgidm/index.html

UIT-T Comisión de Estudio 17, Cuestión 10: www.itu.int/ITU-T/studygroups/com17/index.asp

UIT-T Comisión de Estudio 13 (Redes Futuras) Cuestión 13: www.itu.int/ITU-T/studygroups/com13/index.asp

Proyecto de Alianza para la Libertad (*Liberty Alliance Project*): www.projectliberty.org/

Identidad Ligera (*Light Weight Identity*): lid.netmesh.org/wiki/Main_Page

Consorcio MODINIS-IDM: www.egov-goodpractice.org y www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/ProjectConsortium

Planes de tarjetas de identidad nacionales: por ejemplo www.homeoffice.gov.uk/passports-and-immigration/id-cards/; http://en.wikipedia.org/wiki/Identity_document

OASIS (Organización para el Fomento de Normas de Información Estructuradas, *Organization for the Advancement of Structured Information Standards*): www.oasis-open.org/home/index.php

OCDE (Organización para la Cooperación y el Desarrollo Económicos), Taller sobre gestión de identidad digital, Trondheim, Noruega, 8 y 9 de mayo de 2007: www.oecd.org/sti/security-privacy/idm

OMA (Alianza Móvil Abierta, *Open Mobile Alliance*): www.openmobilealliance.org/

The Open Group: www.opengroup.org

OSIS (Sistema de identidad de fuente abierta, *Open Source Identity System*): osis.idcommons.net/wiki/Main_Page

PAMPAS (Promoción de la privacidad y seguridad móviles avanzadas): www.pampas.eu.org/

PERMIS (Validación de infraestructuras de gestión de privilegios y papeles, Iniciativa de la Sociedad de Información en materia de Normalización (ISIS), Unión Europea, *EU Information Society Initiative in Standardization (ISIS) PrivilEge and Role* Prime (Gestión de privacidad e identidad para Europa, Unión Europea, E*U Privacy and Identity Management for Europe*): https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/ProjectConsortium – PRIME

PERMIS (EU Information Society Initiative in Standardization (ISIS) PrivilEge and Role Prime (EU Privacy and Identity Management for Europe):

www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/ProjectConsortium

W3C (Consorcio World Wide Web): www.w3.org/

Yadis: yadis.org/wiki/Main_Page

Anexo C

Enlaces y referencias

Esta lista de referencias se actualizará periódicamente tomando en consideración los resultados de la Agenda sobre Ciberseguridad Global de la UIT, así como los resultados de la ejecución del proyecto previsto en la Resolución 45 (CMDT-06), el trabajo efectuado por la Comisión de Estudio 17 del UIT-T (Comisión que lidera los temas sobre seguridad del UIT-T), y las Resoluciones pertinentes de la AMNT, así como las actividades de seguimiento relativas a la Línea de Acción C5 de la CMSI sobre ciberseguridad y los resultados de las actividades emprendidas para dar aplicación a las correspondientes Resoluciones de la PP-06 (por ejemplo, las Resoluciones 130, 131 y 149).

Parte I: Formulación y obtención de un acuerdo sobre la estrategia nacional de ciberseguridad

I.C.1 Sensibilización (I.B.1, I.B.2)

Internacional

- Asamblea General de las Naciones Unidas: Resolución 55/63, "Lucha contra la utilización de la tecnología de la información con fines delictivos": www.un.org/Depts/dhl/resguide/r55.htm
- Asamblea General de las Naciones Unidas: Resolución 56/121, "Lucha contra la utilización de la tecnología de la información con fines delictivos": www.un.org/Depts/dhl/resguide/r56.htm
- Asamblea General de las Naciones Unidas: Resolución 57/239, "Creación de una cultura mundial de seguridad cibernética": www.un.org/Depts/dhl/resguide/r57.htm
- Asamblea General de las Naciones Unidas: Resolución 58/199, "Creación de una cultura mundial de seguridad cibernética y protección de las infraestructuras de información esenciales": www.un.org/Depts/dhl/resguide/r58.htm
- Declaración de Principios y Plan de Acción de Ginebra de la Cumbre Mundial sobre la Sociedad de la Información de las Naciones Unidas y Compromiso y Plan de Acción de Túnez para la Sociedad de la Información: www.itu.int/WSIS/index.html
- OCDE: Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de seguridad (2005): www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html
- International CIIP Handbook 2006 (Vol. 1): www.isn.ethz.ch/pubs/ph/details.cfm?id=250
- Recursos de la UIT en materia de ciberseguridad: www.itu.int/cybersecurity/
- Agenda sobre Ciberseguridad Global de la UIT: www.itu.int/cybersecurity/gca/
- Pasarela de ciberseguridad de la UIT: www.itu.int/cybersecurity/gateway/
- Página web sobre ciberseguridad del Sector de Desarrollo de la UIT: www.itu.int/ITU-D/cyb/
- Iniciativa de la UIT sobre Protección de la infancia en línea y directrices conexas: www.itu.int/cop/

I.C.2 Estrategias naciones, regionales e internacionales (I.B.2, I.B.3, I.B.4, I.B.5, I.B.7)

Internacional

- Colección de herramientas de la UIT para la autoevaluación de la ciberseguridad nacional/protección de las infraestructuras de información esenciales (CIIP): www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html
- UIT y ETH Zurich – Marco nacional genérico para la protección de las infraestructuras de información esenciales (CIIP): www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf

- Cuestión 22/1 de la Comisión de Estudio 1 del Sector de Desarrollo de las Telecomunicaciones de la UIT: Garantía de seguridad en las redes de información y comunicación: prácticas óptimas para el desarrollo de una cultura de ciberseguridad: www.itu.int/ITU-D/study_groups/SGP_2006-2010/documents/DEFQUEST-SG1/DEFQUEST-Q22-1-E.pdf
- Agenda sobre Ciberseguridad Global de la UIT: www.itu.int/cybersecurity/gca/
- Guía de la UIT sobre ciberseguridad para los países en desarrollo, Rev. 2009: www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf
- Resolución 45 de la CMDT de la UIT – Mecanismos para aumentar la cooperación en materia de ciberseguridad, incluida la lucha contra el correo basura (Doha, 2006): www.itu.int/ITU-D/cyb/cybersecurity/docs/WTDC06_resolution_45-e.pdf
- Compendio de la Cuestión 4 de la Comisión de Estudio 17 del Sector de Normalización de las Telecomunicaciones – Catálogo de Recomendaciones UIT-T aprobadas relacionadas con la seguridad de las telecomunicaciones: www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D0000090003MSWE.doc
- Cuestión 4 de la Comisión de Estudio 17 del Sector de Normalización de las Telecomunicaciones de la UIT – Seguridad en la esfera de las tecnologías de la información y la comunicación: www.itu.int/pub/T-HDB-SEC.03-2006/en/
- Estudio de la BDT de la UIT sobre aspectos financieros de la seguridad de las redes: soporte lógico perjudicial y correo electrónico basura: www.itu.int/ITU-D/cyb/presentations/2008/bauer-financial-aspects-spam-malware-april-2008.pdf
- OCDE: Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security: www.oecd.org/document/42/0,3343,en_21571361_36139259_15582250_1_1_1_1,00.html
- OCDE: Implementation Plan for co-ordinated national online security policies: www.oecd.org/dataoecd/23/11/31670189.pdf
- Informe del Banco Mundial sobre "Ciberseguridad: un nuevo modelo para la protección de la red": www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2006/12/12/000020953_20061212113151/Rendered/PDF/381170CyberSec1uly0250200601PUBLIC1.pdf
- Documento blanco sobre seguridad de la información de la Asociación Estadounidense de Tecnología de la Información (ITAA): www.itaa.org/eweb/upload/ITAA%20Infosec%20White%20Paper.pdf

Regional

- Grupo de Trabajo sobre Telecomunicaciones e Información de la Cooperación Económica Asia-Pacífico (APECTEL) – APEC Cybersecurity Strategy (2002): unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN012298.pdf
- Libro Azul de CITEL: Políticas de Telecomunicaciones para las Américas (2005) secciones 8.4-8.5 www.citel.oas.org/publications/azul-fin-r1c1_i.pdf
- Resolución del Consejo de la Unión Europea: Estrategia para una sociedad de la información segura en Europa – Diálogo, asociación y potenciación (2007): eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_068/c_06820070324en00010004.pdf
- Declaración de Doha sobre ciberseguridad (2008): www.itu.int/ITU-D/cyb/events/2008/doha/docs/doha-regional-cybersecurity-forum-output-20-feb-08.pdf
- Comunicación de la Unión Europea sobre una estrategia para una sociedad de la información segura (2006): ec.europa.eu/information_society/doc/com2006251.pdf
- Programa de la Unión Europea para una Internet más segura: europa.eu.int/information_society/activities/sip/index_en.htm

- Estudio realizado por la Agencia Europea de Seguridad de las Redes y de la Información (ENISA): "Security Economics and the Internal Market" (2008): www.enisa.europa.eu/pages/analys_barr_incent_for_nis_20080306.htm
- OEA: Inter-American Strategy to Combat Threats to Cybersecurity (2004): www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm

Nacional

- Australia: Programa para el establecimiento de un modelo de protección de infraestructuras esenciales y su análisis (CIPMA): www.csiro.au/partnerships/CIPMA.html
- Crisis and Risk Network (CRN) International CIIP Handbook: An Inventory and Analysis of National Protection Policies: www.crn.ethz.ch/publications/crn_team/detail.cfm?id=250
- Alemania: Plan nacional de protección de la infraestructura de la información: www.en.bmi.bund.de/cln_028/nn_148138/Internet/Content/Common/Anlagen/Nachrichten/Pressemitteilungen/2005/08/National__Plan__for__Information__Infrastructure__Protection,templateId=raw,property=publicationFile.pdf/National_Plan_for_Information_Infrastructure_Protection.pdf
- Japón: Estrategia nacional para la infraestructura de la información: www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf
- Estrategias de aplicación nacional de los 11 Miembros de la OCDE: www.oecd.org/document/63/0,2340,en_21571361_36139259_36306559_1_1_1_1,00.html
- Nueva Zelandia: Estrategia digital: www.digitalstrategy.govt.nz
- Singapur: Plan rector 2 sobre seguridad de las infocomunicaciones: www.ida.gov.sg/doc/News%20and%20Events/News_and_Events_Level2/20080417090044/MR17Apr08MP2.pdf
- Singapur: Estrategia en materia de protección del ciberespacio: www.ida.gov.sg/News%20and%20Events/20050717164621.aspx?getPagetype=21
- Reino Unido: Centro de protección de la infraestructura nacional (CPNI): www.cpni.gov.uk/
- Estados Unidos: Estrategia nacional en materia de protección del ciberespacio: www.whitehouse.gov/

I.C.3 Evaluación y formulación de programas (I.B.5, I.B.7, I.B.8)

- Objetivos de control para la información y la tecnología relacionada (COBIT) 4.1: www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981 (resumen de conclusiones: teledescarga libre; para teledescargar la versión completa: inscripción obligatoria)
- Biblioteca de Infraestructura de Tecnología de la Información (ITIL), Gestión de la seguridad: www.itil-itsm-world.com/ (pago de tasa necesario)
- Organización Internacional de Normalización/Comisión Electrotécnica Internacional (ISO/CEI), 27000 Series, Information technology-Security techniques-Information security management systems: www.iso27001security.com/index.html
- ISO/IEC 13335, Information technology-Security techniques-Management of information and communications technology security-Part 1: Concepts and models for information and communications technology security management: www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue detail.htm?csnumber=39066 (fee required)
- ISO/IEC 17799, 2005 Information technology-Security techniques-Code of practice for information security management: www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612 (fee required)
- ISO/IEC 21827, Systems Security Engineering—Capability Maturity Model (SSE-CMM®): www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=34731 (fee required)

- Estudio de la BDT de la UIT sobre aspectos financieros de la seguridad de las redes: soporte lógico perjudicial y correo electrónico basura: www.itu.int/ITU-D/cyb/presentations/2008/bauer-financial-aspects-spam-malware-april-2008.pdf
- Resolución 50 de la AMNT de la UIT sobre "Ciberseguridad" (Rev. Johannesburgo, 2008): www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf
- Resolución 52 de la AMNT de la UIT – Respuesta y lucha contra el correo basura (Rev. Johannesburgo, 2008): www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf
- Resolución 58 de la AMNT de la UIT – Fomento de la creación de equipos nacionales de respuesta frente a incidentes informáticos, en particular en los países en desarrollo (Johannesburgo, 2008): www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.58-2008-PDF-E.pdf
- NIST Special Publication (SP) 800-12, An Introduction to Computer Security: The NIST Handbook (febrero de 1996): csrc.nist.gov/publications/nistpubs/800-12/
- NIST SP 800-30, Risk Management Guide for Information Technology Systems (julio de 2002): csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- NIST SP 800-53, Recommended Security Controls for Federal Information Systems (diciembre de 2007): csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf
- NIST Draft Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems (diciembre de 2007): csrc.nist.gov/publications/PubsDrafts.html#SP-800-53-A
- NIST SP 800-50 Building an Information Technology Security Awareness and Training Program (octubre de 2003): csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf
- NIST SP 800-30 Risk Management Guide for Information Technology Systems, (julio de 2002): csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVESM): www.cert.org/octave/

I.C.4 Puntos de contacto en relación con la asistencia internacional (I.B.6)

- Grupo de Trabajo contra el phishing (APWG): www.antiphishing.org
- Foro de los equipos de intervención en caso de incidentes de seguridad (FIRST): www.first.org
- Instituto de Ingenieros Eléctricos y Electrónicos: www.ieee.org
- Grupo Especial de Ingeniería de Internet: www.ietf.org
- Grupo de Trabajo contra el abuso en mensajería: www.maawg.org
- Alianza Mundial de Servicios de Tecnología de la Información: www.witsa.org
- Consorcio World Wide Web: www.w3c.org

Parte II: Establecimiento de relaciones de colaboración entre el Estado y la industria de un país

II.C.1 Estructuras de colaboración entre el Estado y la industria

Internacional

- Alianza del sector industrial para la ciberseguridad: www.csialliance.org/about_csia/index.html
- Conjunto de herramientas de la OCDE contra el *spam* – Alianzas de cooperación para combatir el *spam*: www.oecd-antispam.org/article.php3?id_article=243
- StopSpamAlliance.org: stopspamalliance.org/

Regional

- Oriente Medio: Informe del 14º Foro de cibergobierno y ciberservicios GCC: www.zawya.com/Story.cfm/sidZAWYA20080529073202/SecMain/pagHomepage/chnAll%20Regional%20News/obj2A17E941-F5E0-11D4-867D00D0B74A0D7C/

Nacional

- Asociación entre el gobierno y las empresas de Australia: Red de intercambio de información fiable para la protección de la infraestructura esencial: www.tisn.gov.au/www/tisn/tisn.nsf/Page/CIPPrograms_CriticalInfrastructureProtectionModellingandAnalysis(CIPMA)
- Centros de Intercambio de Información y Análisis (ISAC) y Consejos de Coordinación de Estados Unidos:
  - Servicios financieros de los ISAC: www.fsisac.com/
  - Sector eléctrico de los ISAC: www.esisac.com/
  - Tecnología de información de los ISAC: www.it-isac.org
  - Telecomunicaciones de los ISAC: www.ncs.gov/ncc/
  - Consejo sobre Fiabilidad e Interoperabilidad de la Red (NRIC): www.nric.org/
  - Comité Consultivo sobre Telecomunicaciones y Seguridad Nacional (NSTAC): www.ncs.gov/nstac/nstac.html
- Cooperación entre el Estado y la industria en materia de normas: Instituto Nacional de Normas, Estados Unidos – Grupo Especial sobre Normalización de la Seguridad Nacional: www.ansi.org/standards_activities/standards_boards_panels/hssp/overview.aspx?menuid=3
- Documento Blanco sobre seguridad de la información de la sociedad de tecnología de la información de Estados Unidos: www.itaa.org/eweb/upload/ITAA%20Infosec%20White%20Paper.pdf
- Consejo de Coordinación del Sector IT (SCC): www.it-scc.org
- Alianza Nacional para la Ciberseguridad de los Estados Unidos: www.cyberpartnership.org/
- Consejo Nacional sobre Protección de la Información (NIAC), Informes del Grupo de Trabajo sobre un modelo de asociación sectorial: itaa.org/eweb/upload/NIAC_SectorPartModelWorkingGrp_July05.pdf
- Plan de protección de la infraestructura nacional de Estados Unidos: www.dhs.gov/xprevprot/programs/editorial_0827.shtm
- Planes destinados específicamente a diferentes sectores de Estados Unidos: www.dhs.gov/xprevprot/programs/gc_1179866197607.shtm
- Plan destinado específicamente al sector IT de Estados Unidos: www.dhs.gov/xlibrary/assets/IT_SSP_5_21_07.pdf
- Administración Nacional de Telecomunicaciones e Información de Estados Unidos: www.ntia.doc.gov/

II.C.2 Intercambio de información sobre ciberseguridad

Internacional

- Grupo de Trabajo contra el abuso en mensajería: www.maawg.org

Nacional

- Instituto Nacional de Normas y Tecnología (NIST) de los Estados Unidos, Centro de Investigación y Seguridad Informática: csrc.nist.gov/
- Sistema Nacional de Ciberalertas US-CERT (Estados Unidos): www.us-cert.gov/cas/

II.C.3 Sensibilización e información: Herramientas para utilización en las empresas y los hogares

Internacional

- Creación de un programa de sensibilización en materia de seguridad: www.gideonrasmussen.com/article-01.html
- Centro de recursos para la seguridad de Internet y de publicaciones sobre seguridad en las empresas: www.cisecurity.org/resources.html

- Estrategias en materia de seguridad de las empresas: articles.techrepublic.com.com/5100-10878_11-5193710.html
- Guía sobre ciberseguridad deliberadamente adaptada a las pequeñas empresas: www.uschamber.com/publications/reports/0409_hs_cybersecurity.htm
- Recursos destinados a la sensibilización de las autoridades públicas y empresas en materia de seguridad (EDUCAUSE): www.educause.edu/Security%20Task%20Force/CybersecurityAwarenessResource/BrowseSecurityAwarenessResourc/8770?time=1215527945
- Iniciativas de ENISA sobre sensibilización en la seguridad de la información (disponible en numerosos idiomas): www.enisa.europa.eu/Pages/05_01.htm
- Métodos de seguridad de las tecnologías de la información y de prevención de delitos (en empresas) (Interpol): www.interpol.int/Public/TechnologyCrime/CrimePrev/ITSecurity.asp
- Lista de elementos para la prevención de delitos contra las tecnologías de la información en las empresas (Interpol): www.interpol.int/Public/TechnologyCrime/CrimePrev/companyChecklist.asp
- Afiches sobre sensibilización en materia de seguridad (NoticeBored): www.noticebored.com/html/posters.html
- Conjunto de herramientas de la OCDE contra el *spam* – Educación y sensibilización: www.oecd-antispam.org/article.php3?id_article=242
- Recursos sobre una política en materia de seguridad (SANS): www.sans.org/resources/policies/
- Colección de herramientas para la sensibilización en materia de seguridad – The Information Warfare Site: www.iwar.org.uk/comsec/resources/sa-tools/
- Alianza Nacional para la Ciberseguridad de los Estados Unidos – Centro de Recursos para la sensibilización en pequeñas empresas y hogares: www.cyberpartnership.org/init-aware.html

Nacional

- Comisión Federal de Comercio de Estados Unidos: www.ftc.gov/infosecurity
- NIST 800-50, Programa de capacitación y sensibilización en materia de seguridad: csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

Parte III: Disuasión del ciberdelito/fundamentos jurídicos y cumplimiento

Internacional

- Consejo de Europa: Convenio sobre el ciberdelito (2001): www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Default_en.asp
- Principios respecto a los delitos de alta tecnología del G8: www.usdoj.gov/criminal/cybercrime/g82004/g8_background.html
- Material básico de la UIT relativo a la armonización de los enfoques jurídicos nacionales, la coordinación jurídica internacional y el cumplimiento de las leyes: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html
- UIT/InfoDev – Conjunto de herramientas para la reglamentación de las TIC: www.ictregulationtoolkit.org/
- Publicación de la UIT sobre Comprensión del ciberdelito: Guía para los países en desarrollo: www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html
- Conjunto de herramientas de la UIT para la legislación sobre el ciberdelito: www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html
- Recursos en materia de delitos contra las tecnologías de la información (Interpol): www.interpol.com/Public/TechnologyCrime/

- Enfoques reglamentarios de la OCDE contra el *spam*: www.oecd-antispam.org/article.php3?id_article=1
- Conjunto de herramientas de la OCDE contra el *spam*: www.oecd-antispam.org/article.php3?id_article=265
- Asamblea General de las Naciones Unidas: Resolución 55/63, "Lucha contra la utilización de la tecnología de la información con fines delictivos": www.un.org/Depts/dhl/resguide/r55.htm
- Asamblea General de las Naciones Unidas: Resolución 56/121, "Lucha contra la utilización de la tecnología de la información con fines delictivos": www.un.org/Depts/dhl/resguide/r56.htm
- Recursos del Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia (UNICRI) para aumentar los conocimientos y crear nuevas alianzas destinadas a combatir el ciberdelito: www.unicri.it/
- Leyes Modelo de la CNUDMI (Comisión de las Naciones Unidas para el Derecho Mercantil Internacional) sobre Comercio Electrónico y Firmas Electrónicas: www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html
- Recursos de la Oficina de las Naciones Unidas contra las Drogas y el Delito: www.unodc.org/

Regional

- Documentos relacionados con el ciberdelito de la APEC, presentaciones y declaraciones ministeriales: www.apectelwg.org/
- Declaración de la Conferencia sobre Ciberdelito de El Cairo: www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Cairo/CairoDeclarationAgainstCC2007_EN.pdf
- Commonwealth Model Law on Computer and Computer Related Crime: www.thecommonwealth.org/Internal/38061/documents/
- Consejo de Europa: Convenio sobre Ciberdelincuencia (2001): www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Default_en.asp
- Portal Interamericano de Cooperación en Materia de Delito Cibernético (OEA): www.oas.org/juridico/english/cyber.htm

Nacional

- CERT/CC: Cómo el FBI investiga el ciberdelito: www.cert.org/tech_tips/FBI_investigates_crime.html
- Cybercrimelaw: Estudio de la legislación contra el ciberdelito en todo el mundo: www.cybercrimelaw.net/index.html
- Consejo de Europa: Estudio de la legislación nacional en materia de ciberdelito: www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technicalcooperation/CYBER/Legprofiles.asp#TopOfPage
- Microsoft: "Asia Pacific Legislative Analysis: Current and Pending Online Safety and Cybercrime Laws": www.itu.int/ITU-D/cyb/cybersecurity/docs/microsoft_asia_pacific_legislative_analysis.pdf
- Leyes contra el *spam* en los Estados Miembros de la OCDE: www.oecd-antispam.org/countrylaws.php3
- Naciones Unidas: "Modelos de ciberlegislación en los Países Miembros de la Comisión Económica y Social para Asia Occidental (CESPAO)": www.escwa.un.org/information/publications/edit/upload/ictd-07-8-e.pdf
- Departamento de Justicia de los Estados Unidos (USDOJ): Sección Ciberdelito y Propiedad Intelectual: www.cybercrime.gov
- Departamento de Justicia de los Estados Unidos (USDOJ): Manual on Prosecuting Computer Crime (Chapter 1 – Computer Fraud and Abuse Act): www.cybercrime.gov/ccmanual/

- Servicio Secreto de los Estados Unidos – Best Practices for Seizing Electronic Evidence: www.forwardedge2.com/pdf/bestPractices.pdf

Parte IV: Creación de capacidades nacionales de gestión de incidentes: vigilancia, advertencia, respuesta y recuperación

IV.C.1 Plan de intervención nacional y CSIRT nacional

Internacional

- Centro de Coordinación del equipo dispuesto a intervenir ante emergencias informáticas (de la Universidad Carnegie-Mellon, Estados Unidos) (CERT/CC): www.cert.org/csirts/
- CERT/CC: Action List for Developing a CSIRT: www.cert.org/csirts/action_list.html
- CERT/CC: Creating a CSIRT: A Process for Getting Started: www.cert.org/csirts/Creating-A-CSIRT.html
- CERT/CC: Defining Incident Management Processes for CSIRTs: A Work in Progress: www.cert.org/archive/pdf/04tr015.pdf
- CERT/CC: CSIRT Frequently Asked Questions: www.cert.org/csirts/csirt_faq.html
- CERT/CC: Handbook for CSIRTs: www.cert.org/archive/pdf/csirt-handbook.pdf
- CERT/CC: Incident Management Capability Metrics Version 0.1: www.cert.org/archive/pdf/07tr008.pdf
- CERT/CC: Organizational Models for CSIRT: www.cert.org/archive/pdf/03hb001.pdf
- CERT/CC: CSIRT Services: www.cert.org/csirts/services.html
- CERT/CC: Staffing Your CSIRT – What Basic Skills Are Needed?: www.cert.org/csirts/csirt-staffing.html
- CERT/CC: State of the Practice of CSIRT: www.cert.org/archive/pdf/03tr001.pdf
- CERT/CC: Steps for Creating National CSIRTs: www.cert.org/archive/pdf/NationalCSIRTs.pdf
- CERT/CC Virtual Training Environment (VTE): www.vte.cert.org/
- ENISA: A Step-by-Step Approach on How to Set Up a CSIRT: www.enisa.europa.eu/pages/05_01.htm
- Colaboración entre la UIT e IMPACT y recursos conexos: www.itu.int/ITU-D/cyb/cybersecurity/impact.html
- GOVCERT.nl: CSIRT in a Box – Information on Setting up a CSIRT: www.govcert.nl/render.html?it=69
- CPNI del Reino Unido: The Warning, Advice and Reporting Point (WARP) Toolbox: www.warp.gov.uk/

Regional

- CERT, Asia-Pacífico: www.apcert.org/index.html
- CSIRT, Recursos de red europeos: www.ecsirt.net/
- Grupo Europeo de CERT gubernamentales (EGC): www.egc-group.org/

Nacional

- Australia: AusCERT: www.auscert.org.au
- Austria: CERT.at: www.cert.at
- Brasil: CERT.br: www.cert.br/
- Chile: CLCERT: www.clcert.cl/
- China: CNCERT/CC: www.cert.org.cn/

- Finlandia: CERT-FI: www.cert.fi
- Hungría: CERT-Hungary: www.cert-hungary.hu
- India: CERT-In: www.cert-in.org.in
- Italia: CERT-IT: security.dico.unimi.it/
- Japón: JPCERT/CC: www.jpcert.or.jp/
- Corea: KrCERT/CC: www.krcert.or.kr/
- Malasia: MyCERT: www.cybersecurity.org.my
- Países Bajos: www.csirt.dk/
- Polonia: CERT POLSKA: www.cert.pl/
- Eslovenia: SI-CERT: www.arnes.si/en/si-cert/
- Singapur: SingCERT: www.singcert.org.sg/
- Suecia: SITIC: www.sitic.se
- Suiza: MELANI: www.melani.admin.ch
- Tailandia: ThaiCERT: www.thaicert.nectec.or.th/
- Túnez: CERT-TCC: www.ansi.tn/en/about_cert-tcc.htm
- Qatar: www.qcert.org
- Emiratos Árabes Unidos: aecert.ae/
- Estados Unidos: Plan de intervención nacional: www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml
- Estados Unidos: US-CERT: www.us-cert.gov/
- Y otras páginas web de CERT/CSIRT nacionales

IV.C.2 Cooperación e intercambio de información

Internacional

- CERT/CC: Security vulnerabilities and fixes: www.cert.org/nav/index_red.html
- Clearing House for Incident Handling Tools (CHIHT): chiht.dfn-cert.de/
- Recursos del Foro de los equipos de intervención en caso de incidentes de seguridad (FIRST): www.first.org/
- Recursos del Servicio de apoyo a la seguridad para los proveedores de servicios Internet (ISP): www.donelan.com/ispsupport.html
- Portal de la ciberseguridad de la UIT: Material básico sobre vigilancia, advertencia y respuesta a los incidentes: www.itu.int/cybersecurity/gateway/watch_warning.html
- ITsafe warning system for small businesses and individuals: www.itsafe.gov.uk/
- Conjunto de herramientas de la OCDE contra el *spam*: www.oecd-antispam.org/article.php3?id_article=265

Regional

- Asociación Transeuropea de Redes de Investigación y Educación (TERENA): www.terena.org/

Nacional

- Servicio de alerta nacional (Países Bajos): www.waarschuwingsdienst.nl/render.html?cid=106
- CPNI del Reino Unido: The Warning, Advice and Reporting Point (WARP) Toolbox: www.warp.gov.uk/
- IT-ISAC de Estados Unidos: https://www.it-isac.org/

- Consejo de Coordinación del Sector de las TI (ISCC) de los Estados Unidos: Tecnologías de la información: Plan específico del sector para la protección de la infraestructura esencial y los recursos básicos: www.it-scc.org/documents/itscc/Information_Technology_SSP_2007.pdf
- Instituto Nacional de Normas y Tecnología (NIST) de Estados Unidos: csrc.nist.gov/

IV.C.3 Información sobre vulnerabilidad/herramientas y técnicas

- Build Security In – Colección de información sobre protección y seguridad del soporte lógico para ayudar a crear sistemas seguros: buildsecurityin.us-cert.gov/daisy/bsi/home.html
- Lista común de vulnerabilidades y exposición (CVE): www.cve.mitre.org/about/
- Lenguaje abierto de evaluación de vulnerabilidades (OVAL): oval.mitre.org/
- Base nacional de datos sobre vulnerabilidades (NVD) de los Estados Unidos (para soporte lógico): nvd.nist.gov/nvd.cfm

Parte V: Promoción de una cultura nacional de ciberseguridad

V.C.1 Sistemas y redes oficiales (V.B.1, V.B.2, V.B.7)

Internacional

- Línea de Acción C5 del Plan de Acción de la CMSI: www.itu.int/wsis/implementation/index.html
- Agenda sobre Ciberseguridad Global de la UIT: www.itu.int/osg/csd/cybersecurity/gca/
- Reunión temática de la CMSI de la UIT contra el correo basura: www.itu.int/osg/spu/spam/meeting7-9-04/index.html
- Línea de Acción C5 de la CMSI – Primera reunión: Informe del Presidente www.itu.int/osg/spu/cybersecurity/2006/chairmansreport.pdf
- Línea de Acción C5 de la CMSI – Segunda reunión: Plan de Acción www.itu.int/wsis/docs/geneva/official/poa.html
- Segunda reunión: Agenda, con enlaces a las presentaciones: www.itu.int/osg/csd/cybersecurity/WSIS/meetingAgenda.html
- Línea de Acción C5 de la CMSI – Informe de la tercera reunión: www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/WSIS_Action_Line_C5_Meeting_Report_June_2008.pdf
- Tercera reunión: Agenda, con enlaces a las presentaciones: www.itu.int/osg/csd/cybersecurity/WSIS/agenda-3_new.html
- Microsoft: Computing Privacy, Internet Safety and Security Information for Policymakers Worldwide: www.microsoft.com/mscorp/twc/policymakers_us.mspx
- OCDE: Culture of Security portal with resources: ww.oecd.org/sti/cultureofsecurity
- OCDE: "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" (2002): www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html
- OCDE: "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (1980): www.oecd.org/document/20/0,2340,en_2649_34255_15589524_1_1_1_1,00.html
- Informe de la OCDE: "The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries" (2005): www.oecd.org/dataoecd/16/27/35884541.pdf
- Manual del Banco Mundial sobre seguridad de las tecnologías de la información – Políticas oficiales y seguridad de la información: www.infodev-security.net/handbook/part4.pdf
- Resolución 57/239 (Anexos a) y b)) de la Asamblea General de las Naciones Unidas: www.un.org/Depts/dhl/resguide/r57.htm

Regional

- ENISA: "Information Security Awareness Initiatives: Current practice and the measurement of success" (2007): www.enisa.europa.eu/doc/pdf/deliverables/enisa_measuring_awareness.pdf
- ENISA: "A Users' Guide: How to Raise Information Security Awareness" (2006): www.enisa.europa.eu/doc/pdf/deliverables/enisa_a_users_guide_how_to_raise_IS_awareness.pdf
- Europe's Internet Safety Information Source (InSafe): www.saferinternet.org/ww/en/pub/insafe/index.htm
- OEA: Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity (en particular, los Apéndices) (2004):| www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm

Nacional

- Brasil: recursos Antispam.br: antispam.br/
- Brasil: Directrices sobre seguridad de Internet, Comité Directivo sobre Internet de Brasil, CGI.br: cartilha.cert.br/
- Iniciativas de la OCDE para fomentar una cultura de ciberseguridad (por países): www.oecd.org/document/63/0,3343,en_21571361_36139259_36306559_1_1_1_1,00.html
- US-CERT (Estados Unidos): www.us-cert.gov/
- Departamento de Seguridad Nacional (DHS) de Estados Unidos: Plan nacional de I+D para la protección de la infraestructura esencial: www.dhs.gov/xres/programs/gc_1159207732327.shtm
- Prácticas de seguridad de la Agencia Federal (FASP) (Estados Unidos): csrc.nist.gov/fasp/
- Partes 1, 2, 7, 11 y 39 del Reglamento Federal de Adquisiciones (FAR) (Estados Unidos): www.acqnet.gov/FAR/
- Plan Federal de I+D en ciberseguridad y protección de la información (Estados Unidos): www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf
- Junta Asesora en seguridad de la información y privacidad (Estados Unidos): csrc.nist.gov/ispab/
- Directiva Presidencial sobre Seguridad Nacional/HSPD-7, "Infraestructura esencial: identificación, prioridad y protección" (Estados Unidos): www.whitehouse.gov/news/releases/2003/12/20031217-5.html
- Centro multiestatal para el análisis e intercambio de información (Estados Unidos): www.msisac.org/
- Estrategia nacional para garantizar la seguridad del ciberespacio (Estados Unidos): www.whitehouse.gov/pcipb/
- Informe al Presidente de los Estados Unidos del Comité Consultivo sobre Tecnología de la Información respecto a las prioridades de la investigación en materia de ciberseguridad: www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

V.C.2 Empresas y otras organizaciones del sector privado (V.B.3, V.B.5, V.B.7)

- Movimiento a favor de una Internet segura en Brasil: www.internetsegura.org/
- Centro de Seguridad de Cisco (Sección: Prácticas más idóneas): tools.cisco.com/security/center/home.x
- Microsoft Trustworthy Computing: www.microsoft.com/mscorp/twc/default.mspx
- NIATEC – Material pedagógico: niatec.info/index.aspx?page=105
- Manual de seguridad de las tecnologías de la información – Seguridad en organizaciones (Banco Mundial): www.infodev-security.net/handbook/part3.pdf

- US-CERT – Afiches y hojas de información para lugares de trabajo (Estados Unidos): www.uscert.gov/reading_room/distributable.html
- Ejercicios de simulacro "*Cyber Storm*" del DHS/industria: www.dhs.gov/xnews/releases/pr_1158340980371.shtm

V.C.3 Particulares y sociedad civil (V.B.4, V.B.6, V.B.7)

- Brasil: SaferNet Brazil: www.safernet.org.br/site/
- Be Safe Online (SUSI – Uso más seguro de los servicios de Internet): www.besafeonline.org/
- CASEScontact security tips: casescontact.org/tips_list.php
- Recursos de Childnet International destinados a los niños: www.childnet-int.org
- Iniciativa Cyber Peace: www.cyberpeaceinitiative.org/
- CyberTipline: Enseñar a los adolescentes a proteger su seguridad en Internet: tcs.cybertipline.com/
- Zona de seguridad de Internet – Recursos para padres e hijos: www.internetsafetyzone.co.uk/
- Métodos de seguridad de las tecnologías de la información y de prevención de delitos (para particulares) (Interpol): www.interpol.int/Public/TechnologyCrime/CrimePrev/privateChecklist.asp
- Iniciativa de la UIT sobre Protección de la infancia en línea y directrices conexas: www.itu.int/cop/
- GetNetWise – herramientas para familias: kids.getnetwise.org/tools/
- OnGuard Online – recomendaciones contra el fraude: onguardonline.gov/index.html
- MakeItSecure – información sobre peligros comunes en Internet: www.makeitsecure.org/en/index.html
- Malasia – Iniciativas sobre ciberseguridad: www.esecurity.org.my/
- NetSmartz: recursos para padres y tutores: www.netsmartz.org/netparents.htm
- Nueva Zelandia - Netsafe: ww.netsafe.org.nz
- SafeLine - hotline para comunicar contenidos ilícitos: www.safeline.gr/
- Security Cartoon: www.securitycartoon.com/
- Stay Safe Online: www.staysafeonline.info/
- WiredSafety.org: www.wiredsafety.org/
- Banco Mundial: Manual de seguridad de las tecnologías de la información – Seguridad para particulares: www.infodev-security.net/handbook/part2.pdf
- Recursos del Centro contra la Explotación Infantil y de la Protección en Línea del Reino Unido: www.ceop.gov.uk/
- Get Safe Online del Reino Unido: www.getsafeonline.org/
- CERT de los Estados Unidos para usuarios no técnicos: www.us-cert.gov/nav/nt01/

Y otras iniciativas internacionales, regionales y nacionales de sensibilización destinadas a los usuarios.

Impreso en Suiza
Ginebra, 2010