Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1209

(12/2010)

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

Seguridad en el ciberespacio – Ciberseguridad

Capacidades e hipótesis contextuales de la comunicación y el intercambio de información sobre ciberseguridad

Recomendación UIT-T X.1209

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	**X.1200–X.1229**
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/eurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de eurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1209

Capacidades e hipótesis contextuales de la comunicación y el intercambio de información sobre ciberseguridad

Resumen

En la presente Recomendación se describen perspectivas y capacidades de apoyo de alto nivel para la comunicación y el intercambio de información sobre ciberseguridad, así como capacidades importantes para facilitar la compatibilidad entre aplicaciones de comunicación e intercambio de información sobre ciberseguridad.

Se describen capacidades que se pueden utilizar en situaciones hipotéticas/reales en las cuales entidades que antes eran independientes participan en diversas actividades coordinadas tales como la prevención o la detención de comportamientos específicos o la coordinación de actividades de análisis y determinación.

Las capacidades enumeradas y descritas tienen por objeto apoyar operaciones de seguridad más eficientes y eficaces mediante la comunicación y el intercambio compatibles de información entre partes de confianza que colaboran para supervisar, mantener y administrar en general la seguridad de sistemas y redes.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio
1.0	ITU-T X.1209	2010-12-17	17

Palabras clave

Comunicación de información, información sobre ciberseguridad, intercambio de información.

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 http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Página

Recomendación UIT-T X.1209

Capacidades e hipótesis contextuales de la comunicación y el intercambio de información sobre ciberseguridad

1 Alcance

En la presente Recomendación se indican capacidades importantes para soportar la compatibilidad entre aplicaciones de comunicación e intercambio de información sobre ciberseguridad. En consecuencia, la cláusula 7 contiene descripciones de hipótesis de capacidades de utilización de alto nivel que se utilizan para fijar el contexto de las capacidades que se encuentran en la cláusula 8. Para aclarar más la finalidad de las capacidades, la cláusula 9 contiene descripciones de las capacidades que se necesitarán con más probabilidad en determinadas situaciones.

La presente Recomendación está destinada a quienes participan en operaciones de seguridad autorizadas.

2 Referencias

Ninguna.

3 Definiciones

3.1 Términos definidos en otras Recomendaciones

En la presente Recomendación se utiliza el siguiente término definido en otras Recomendaciones:

3.1.1 ciberseguridad [b-ITU-T X.1205]: 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 puede incluir la autenticidad y el no repudio;
- confidencialidad.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se define el siguiente término:

3.2.1 información sobre ciberseguridad: Información o conocimientos estructurados que pueden comprender, pero no exclusivamente, el "estado" de equipos, software o sistemas de red, o informes relacionados con incidentes o eventos, partes que aplican capacidades de intercambio de información en términos de ciberseguridad, especificaciones para el intercambio de información en términos de ciberseguridad, incluidos módulos, esquemas y números asignados, identidades y atributos de confianza para todo lo que antecede y requisitos de implementación, directrices y prácticas.

4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan los siguientes acrónimos y abreviaturas:

DDoS Ataque de denegación de servicio distribuido (*distributed denial of service*)

FTP Protocolo de transferencia de ficheros (*file transfer protocol*)

HTTP Protocolo de transferencia hipertexto (*hypertext transfer protocol*)

HTTPS Protocolo de transferencia hipertexto seguro (HTTP por SSL) (*secure-hypertext transfer protocol* (*HTTP over SSL*))

IPS Sistema de prevención de intrusiones (*intrusion prevention system*)

5 Convenciones

Ninguna.

6 Introducción

Los ciberataques por medio de virus, gusanos, etc. reducen la velocidad de propagación de las redes mediante diversas técnicas, y son cada vez más amenazadores. Se han desarrollado varios tipos de soluciones de seguridad tales como antivirus, detección de programas espía, cortafuegos, redes privadas virtuales, detección de intrusiones y protección, etc., a fin de que los incidentes de seguridad debidos a esos ataques amenazadores se puedan contrarrestar con un sistema de respuesta rápida mediante la adopción de contramedidas eficaces.

La defensa más común de los administradores de seguridad contra explotadores, virus, gusanos y redes robot ha consistido principalmente en diversos foros de discusión a los que suscriben muchos profesionales de la seguridad. Normalmente, en un par de días o una semana se tapan agujeros, se suprimen vulnerabilidades y todo vuelve a ser normal.

Lamentablemente, la explotación de vulnerabilidades por virus, gusanos y redes robot puede propagarse muy rápidamente por las redes y, en pocos segundos, éstas pueden verse considerablemente afectadas.

La información sobre ciberseguridad se puede compartir muy rápidamente en una organización. Ahora bien, los métodos actuales no facilitan el intercambio de numerosas informaciones entre organizaciones. La falta de comunicación efectiva puede convertir una organización en un islote de seguridad.

Por consiguiente, es importante compartir información sobre ciberseguridad entre muchas organizaciones y, en particular, operadores de telecomunicaciones, proveedores de servicios de telecomunicaciones y centros de operaciones de seguridad. Para posibilitar ese tipo de intercambio de información se necesita:

- métodos fiables y seguros para que los participantes intercambien información más rápidamente;
- métodos que garanticen la protección de la privacidad.

En la presente Recomendación se recogen las hipótesis estudiadas y las correspondientes capacidades para el intercambio de información sobre ciberseguridad entre participantes de manera segura, fiable y confiable.

7 Capacidades

A fin de examinar las capacidades enumeradas en la cláusula 8 en un contexto apropiado para comprender la presente Recomendación, se presentan hipótesis de utilización de alto nivel en cinco condiciones diferentes para ayudar a explicar los cinco grupos lógicos de capacidades siguientes.

7.1 Hipótesis general

Esta hipótesis general se aplica a todas las hipótesis siguientes.

Hipótesis: Los asociados en el intercambio de información comparten información sobre eventos de seguridad y relacionada con incidentes, que les resulta útil para identificar e impedir ataques nocivos contra sus respectivas redes.

El aspecto importante de esta hipótesis es que ambas partes pueden compilar tipos de datos similares pero de diferentes fuentes y/o en diferentes formatos y/o contenidos ligeramente diferentes de tipos de datos similares.

7.2 Políticas operacionales

En esta hipótesis se describe una situación en la cual diferentes asociados en el intercambio de información tienen restricciones diferentes para el acceso a elementos diferentes de la información compartida.

Hipótesis: Los asociados en el intercambio de información tienen un acuerdo comercial para compartir información sobre eventos de seguridad y relacionada con incidentes.

Un aspecto importante de esta hipótesis es que el acceso a la información de cada asociado en el intercambio de información puede estar limitado con un acceso concedido basado en una relación de confianza preexistente. Otro aspecto importante es que la confianza en la información recibida puede estar asociada con la relación de confianza existente.

7.3 Políticas regionales

En esta hipótesis se describe una situación de múltiples asociados en el intercambio de información, en la cual los diferentes asociados tienen diferentes restricciones legislativas y/o reglamentarias sobre distintos elementos del mismo tipo de información compartida. De manera similar a la hipótesis anterior, en esta hipótesis también se destaca la posibilidad de que se pueda compartir información que no se está autorizado a consultar o visualizar.

La diferencia entre esta hipótesis y la anterior estriba en el origen de las limitaciones impuestas al intercambio de información. Las limitaciones en la hipótesis anterior se deben a políticas operacionales decididas por cada asociado en el intercambio de información, mientras que las limitaciones en esta hipótesis se deben a políticas operacionales externas, tales como jurisdicciones regionales.

Hipótesis: Dos partes que trabajan en regiones diferentes pueden intercambiar información ateniéndose a distintas condiciones impuestas por sus respectivas regiones.

El aspecto importante de esta hipótesis es que además de las partes que tienen políticas operacionales diferentes también puede haber políticas asociadas con la región en la cual se intercambia la información.

7.4 Formato de intercambio

Hipótesis: Un asociado en el intercambio de información entrega a un segundo asociado información que comprende los puertos o la gama de puertos de que se trata, en relación con el comportamiento problemático de un esquema de tráfico. La información compartida se utiliza para identificar casos de ataques específicos.

El aspecto importante de esta hipótesis es que todos los asociados que intervienen en el intercambio de información deben poder comprender y aceptar fácilmente el contenido de la información intercambiada.

Hipótesis: Un asociado en el intercambio de información envía notificaciones y alertas de seguridad por diversos medios y en distintas condiciones. Los datos se pueden telecargar gratuitamente en un directorio consultable, enviar selectivamente por correo electrónico para un nivel de servicio o enviar en formato legible por máquina para otro nivel de servicio.

El aspecto importante de esta hipótesis es que se puede facilitar información del mismo tipo o de tipos diferentes por diversos medios y en distintas condiciones.

7.9 Retrocompatibilidad

Hipótesis: Dos asociados en el intercambio de información ya han intercambiado información específica utilizando formatos y protocolos específicos. Se publica una nueva norma que soporta sus actuales métodos de intercambio y proporciona una nueva funcionalidad adicional.

El aspecto importante de esta hipótesis es que se deben soportar lo más posible las aplicaciones existentes y, al mismo tiempo, ofrecer la posibilidad de actualizarlas si se publica una nueva norma.

8 Capacidades

En las cláusulas siguientes se enumeran varias capacidades que soportan los tipos de hipótesis enumerados en la cláusula 7.

8.1 Capacidades de formateo/codificación

- Ambas partes deben conocer y comprender el formato y la estructura de la información sobre seguridad.
  - La información intercambiada sobre seguridad es heterogénea, como mensajes y firmas de cortafuegos u otros dispositivos de seguridad de red, así como distintos tipos de información específica de aplicaciones, como informes sobre eventos e incidentes, análisis y respuestas, intercambio de datos informativos, etc.
  - La información intercambiada representa varios tipos de información sobre seguridad generada por entornos de sistema heterogéneos y aplicada por los mismos.
- Deben poderse compartir diversos tipos de información relacionada con la seguridad, como por ejemplo, pero no exclusivamente, firmas de comportamiento de tráfico, firmas de acceso a sistema, direcciones IP de origen, gamas de puertos de origen y/o destino, etc.
- Las partes deben poder incluir varios niveles de información, desde el contenido de un solo paquete a todos los paquetes que intervienen en un ataque DDoS a toda la red.
- Ambas partes deben conocer y comprender el contenido de la información sobre seguridad.
- Debe poderse identificar el tema en cuestión, y las posibilidades de utilización y aplicación de la información.

8.2 Capacidades de transferencia/intercambio

- Las partes deben poder transferir, entregar y recibir información sobre seguridad a través de un número no exhaustivo de medios de distribución y transmisión.
- Las aplicaciones pueden tener que soportar intercambios síncronos y asíncronos entre las partes durante la comunicación y el intercambio de información sobre seguridad.
- Las aplicaciones deben poder soportar la entrega de información a discreción, por solicitud y previa suscripción.
- Las aplicaciones deben funcionar de manera estable durante el intercambio y tratamiento de grandes volúmenes de información sobre seguridad.
- Los protocolos de intercambio utilizados deben utilizar y/o basarse en protocolos existentes ampliamente utilizados.

7.5 Protección de la privacidad

En las hipótesis que figuran en esta cláusula destacan diversas cuestiones relacionadas con la privacidad, ya sea de la empresa o personal. Además, se destaca la necesidad de poder garantizar la privacidad de los propios intercambios de información.

- Hipótesis: Un centro de operaciones de seguridad compila información relativa a un ataque malicioso contra uno de sus sistemas, redes o, más generalmente, activos gestionados. Esta información se transmite entonces a un proveedor de servicios de red para que identifique la o las fuentes del ataque malicioso en cuestión.

  El aspecto importante de esta hipótesis es que el proveedor de servicios de red puede identificar personalmente a la o las fuentes sospechadas del ataque pero no necesita divulgar esa información al centro de operaciones de seguridad.
- Hipótesis: La información completa compilada por un asociado en el intercambio de información puede contener elementos que ese asociado desea revelar a asociados en el intercambio dentro de la organización o las operaciones, pero no a entidades ajenas a las operaciones.

  El aspecto importante de esta hipótesis es que las partes interesadas en el intercambio de información pueden decidir compartir toda la información disponible o sólo un subconjunto de la misma, u ocultar de alguna manera parte o la totalidad de la información que comparte.
- Hipótesis: Dos partes intercambien información confidencial por redes "públicas".

  El aspecto importante de esta hipótesis es que se ha de poder garantizar la privacidad de la información intercambiada independientemente del método de comunicación utilizado.

7.6 Granularidad del acceso

En esta hipótesis se destaca el caso en que distintos tipos de información sobre seguridad se pueden compartir en determinadas condiciones y en función de las mismas.

Hipótesis: Un servicio pública avisos y advertencias gratuitamente o previa suscripción y facilita diversos niveles de información en función de la definición de los servicios suscritos.

En esos niveles se pueden distinguir, por ejemplo, sólo datos brutos en un nivel y datos brutos y analizados en otro.

El aspecto importante de este hipótesis es que, si bien toda la información facilitada puede ser de un tipo determinado, puede haber distintos "niveles" de información disponibles para otras partes.

7.7 Verificación de fuentes

En esta hipótesis se destaca la necesidad de autenticar los asociados en el intercambio de información.

Hipótesis: Un asociado en el intercambio de información recibe información de otro asociado y comprueba que la información procede realmente de ese asociado.

El aspecto importante de esta hipótesis es que las partes que intercambian información necesitan comprobar que ésta procede del remitente previsto y que un tercero no trata de hacerse pasar por el mismo.

7.8 Distribución multicanales

En esta hipótesis, que es similar a la "granularidad del acceso", se destaca la situación en que distintos niveles de información pueden estar disponibles por distintos métodos.

8.3 Capacidades de seguridad

- Se debe poder autenticar y verificar la información sobre ciberseguridad que interviene en la comunicación y el intercambio.
- Las aplicaciones deben soportar la fiabilidad, confidencialidad, integridad y disponibilidad de la información y los servicios.
- Se debe poder identificar las partes interesadas de manera autenticada y verificable.
- Las aplicaciones deben impedir los ataques contra la comunicación y el intercambio de información sobre ciberseguridad efectuados mediante la imitación y/o falsificación de la información o del origen/destino de la información.
- Las partes que envían la información deben poder cerciorarse de que sólo acceden a la información confidencial las partes autorizadas. De este modo se garantiza la privacidad de las comunicaciones cuando es necesario para información personal identificable o información privada de la empresa, o cualquier dato que se considere importante mantener privado y sólo esté accesible para las personas autorizadas.
- Las partes que envían la información deben poder controlar el acceso a un nivel granular en el cual sólo las partes autorizadas puedan acceder a elementos específicos de un determinado elemento de información sobre seguridad y no acceder a los elementos a los cuales no están autorizados a acceder.
- Las partes deben poder impedir el acceso a información segura relacionada con la seguridad por partes no autorizadas incluso en un entorno abierto en el cual la información relativa a la seguridad es accesible por todos, incluidas partes no autorizadas.

8.4 Capacidades de política

- Las partes deben poder definir y declarar individualmente la política local y/o regional aplicable en lo que respecta a la divulgación y/o acceso a la información proporcionada sobre ciberseguridad. Podría consistir, por ejemplo, en no revelar información de encaminamiento porque las direcciones de destino podrían dar a entender que se trata de una cuestión de "política".
- Las partes deben poder proporcionar información sobre seguridad y acceder a la misma de manera coherente con sus respectivas políticas aplicables en lo que respecta a la divulgación y/o consulta de información sobre seguridad.
- Las partes deben poder declarar en qué jurisdicción se aplica un determinado conjunto de declaraciones de política.
- Las partes deben poder definir y declarar individualmente posibles exigencias y limitaciones jurisdiccionales en lo que respecta a la divulgación y/o al acceso a información sobre seguridad en sus respectivas jurisdicciones.
- Las partes deben poder proporcionar información sobre seguridad y acceder a ella de manera coherente con sus respectivas exigencias jurisdiccionales.

8.5 Capacidades de neutralidad del vendedor

Para soportar la compartición y el intercambio de la gama más amplia posible de información sobre ciberseguridad, las aplicaciones deben proporcionar servicios que dependan lo menos posible de cualquier sistema específico o datos específicos de vendedor. Al mismo tiempo, es preferible no excluir tampoco los sistemas o datos específicos de vendedor.

9 Aplicabilidad de capacidades

Las hipótesis y capacidades descritas en la presente Recomendación ofrecen un conjunto de "herramientas" discretas que se pueden combinar y mezclar para crear aplicaciones propias.

Algunas aplicaciones menos complejas que una simple agregación de datos y/o búsqueda de información pueden necesitar sólo unas pocas de las capacidades enumeradas, mientras que otras, que tienen numerosas características y ofrecen servicios más extensos, pueden tener que combinar e implementar un mayor número de capacidades.

A continuación se analiza cuándo determinados tipos de capacidades pueden ser más necesarios y cuándo pueden ser más optativos.

9.1 Capacidades de formateo/codificación

Para llevar a cabo cualquier comunicación e intercambio de información sobre ciberseguridad, los que envían y reciben la información deben poder comprender exactamente el contenido de lo que intercambian. En consecuencia, las capacidades de formateo y codificación se aplican a todas las hipótesis en las cuales se han de comunicar y/o intercambiar información sobre ciberseguridad.

9.2 Capacidades de transferencia/intercambio

Igual de importante que las capacidades de formateo y codificación es que dos asociados en el intercambio de información necesitan un método para que la información viaje del que la envía al que la recibe.

9.3 Capacidades de seguridad

No tiene mucho sentido intercambiar información relacionada con la seguridad sin por lo menos ciertas garantías de seguridad en la identificación de los asociados en el intercambio y la obtención de un canal de comunicación entre ellos.

Ahora bien, cada situación y aplicación tiene exigencias de seguridad diferentes, y es pues importante que los que las adopten e implementen tengan en cuenta las necesidades de sus aplicaciones específicas.

Por ejemplo, en una aplicación en la cual dos asociados en un intercambio disponen de una línea de comunicación especializada con medidas de seguridad propias, es prácticamente innecesario tomar medidas de seguridad adicionales a las que ya proporciona el entorno del intercambio.

Por otra parte, si se divulga información en canales de comunicación públicamente accesibles, se necesitarán probablemente numerosas medidas de seguridad.

9.4 Capacidades de política

No todas las aplicaciones que soportan la funcionalidad de comunicación e intercambio de información sobre ciberseguridad necesitarán recurrir a la capacidad de declarar restricciones, limitaciones y/o autorizaciones. No obstante, la capacidad de declarar esos tipos de información relacionada con la política es importante en muchas situaciones comerciales y personales.

Al igual que las capacidades de seguridad, en que las condiciones o las situaciones en las cuales se proporcionan funcionalidades relacionadas con la política son ajenas a la aplicación, debido posiblemente a acuerdos operacionales o contractuales, quizá no se necesite la capacidad de declarar y aplicar una política en la propia aplicación.

9.5 Capacidades de neutralidad del vendedor

La neutralidad del vendedor depende mucho de la situación. Si se comparten o intercambian datos generados por el producto de un determinado vendedor utilizando el formato y/o los protocolos de intercambio de ese vendedor, no se aplica realmente la neutralidad del vendedor.

Por otra parte, si el objetivo de una determinada aplicación es maximizar la aplicación y el apoyo del intercambio de información, se considera importante mantener una actitud neutra con respecto a los métodos y/o información específicos del vendedor.

Apéndice I

Introducción a la comunicación y el intercambio de información sobre ciberseguridad

(El presente apéndice no forma parte integrante de esta Recomendación)

En el presente apéndice se describe la estructura conceptual de un ejemplo de aplicación de información sobre ciberseguridad indicada en las figuras I.1 y I.2. Los dos diagramas representan dos visiones diferentes de la topología de la aplicación que permiten las capacidades enumeradas en la cláusula 7. Si bien son posibles otras topologías, la topología indicada integra la utilización de todas las capacidades, mientras que otras topologías y aplicaciones posibles pueden necesitar solamente un subconjunto de las capacidades descritas.

En el primer diagrama se describe la hipótesis de numerosos asociados en la comunicación de información, que tienen cada uno funcionalidades, aplicaciones e información compartida diferentes. Se muestran distintos métodos de acceso a la información en un nodo determinado por medio de aplicaciones que utilizan la información.

Debe señalarse que en el presente apéndice no se estipula exactamente cómo o para qué se utiliza la información, sólo que se puede acceder a ella por diversos medios. Además, en el primer diagrama se indica que todos los intercambios entre nodos son soportados por la utilización de un formato de mensaje normalizado.

El segundo diagrama es una perspectiva tridimensional del primer diagrama que representa un ejemplo de dos asociados en el intercambio de información y describe las capacidades que necesitará probablemente cada uno de ellos para participar en el proceso de intercambio. Como en el primer diagrama, las implementaciones o aplicaciones reales pueden necesitar todas las funcionalidades soportadas por todas las capacidades enumeradas y pueden elegir libremente las funcionalidades que se integran realmente en una implementación/aplicación determinada.

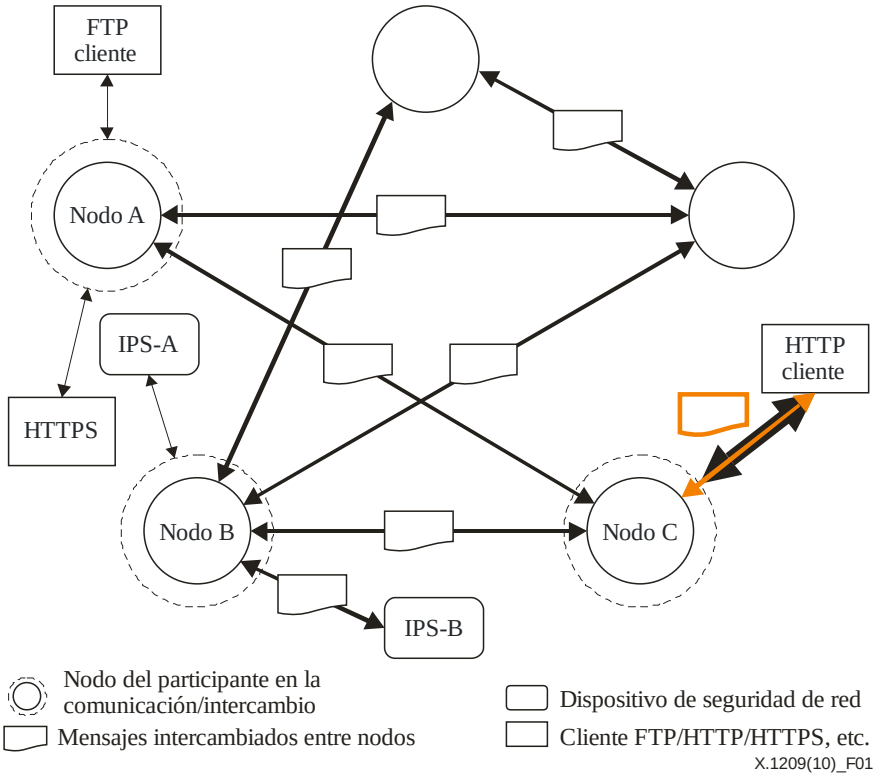

Figura I.1 – Ejemplo de comunicación e intercambio de información sobre ciberseguridad

- Todos los nodos participantes comunican entre sí mediante mensajes normalizados.

  Las siguientes capacidades son importantes para soportar esta funcionalidad:

  – Capacidades de formateo/codificación (cláusula 8.1).
  – Capacidades de transferencia/intercambio (cláusula 8.2).

- Los datos solicitados por un nodo pueden ser proporcionados realmente por otro.

  Las siguientes capacidades son importantes para soportar esta funcionalidad:

  – Capacidades de seguridad (cláusula 8.3).
  – Capacidades de política (cláusula 8.4).

- Un determinado nodo puede implementar protocolos marco únicamente, o puede divulgar datos marco a través de otros protocolos/servicios, como por ejemplo FTP o HTTP, que se utilizan para acceder a datos marco a partir del Nodo A.

  Las siguientes capacidades son importantes para soportar esta funcionalidad:

  – Capacidades de formateo/codificación (cláusula 8.1).
  – Capacidades de transferencia/intercambio (cláusula 8.2).
  – Capacidades de neutralidad del vendedor (cláusula 8.5).

- Los dispositivos de seguridad, como por ejemplo un sistema de prevención de intrusiones (IPS-A) y otro sistema de prevención de intrusiones (IPS-B) que se conectan al Nodo B, pueden acceder a información sobre ciberseguridad ya sea directamente, por ejemplo, IPS-B, o a través de un servicio agrupador, por ejemplo, IPS-A, que permite a los dispositivos utilizar la funcionalidad de comunicación e intercambio, ya sea en la comunicación y el intercambio de información sobre ciberseguridad de manera normalizada o utilizando métodos dependientes del dispositivo/patentados.

  Las siguientes capacidades son importantes para soportar esta funcionalidad:

  – Capacidades de formateo/codificación (cláusula 8.1).
  – Capacidades de transferencia/intercambio (cláusula 8.2).
  – Capacidades de neutralidad del vendedor (cláusula 8.5).

- Un dispositivo de seguridad puede utilizar cualquier protocolo o capa de protocolo que soporta la transmisión de mensajes, por ejemplo, TCP/IP, HTTP, HTTPS, SSL utilizados por clientes que piden servicios al Nodo C.

  Las siguientes capacidades son importantes para soportar esta funcionalidad:

  – Capacidades de formateo/codificación (cláusula 8.1).
  – Capacidades de transferencia/intercambio (cláusula 8.2).
  – Capacidades de neutralidad del vendedor (cláusula 8.5).

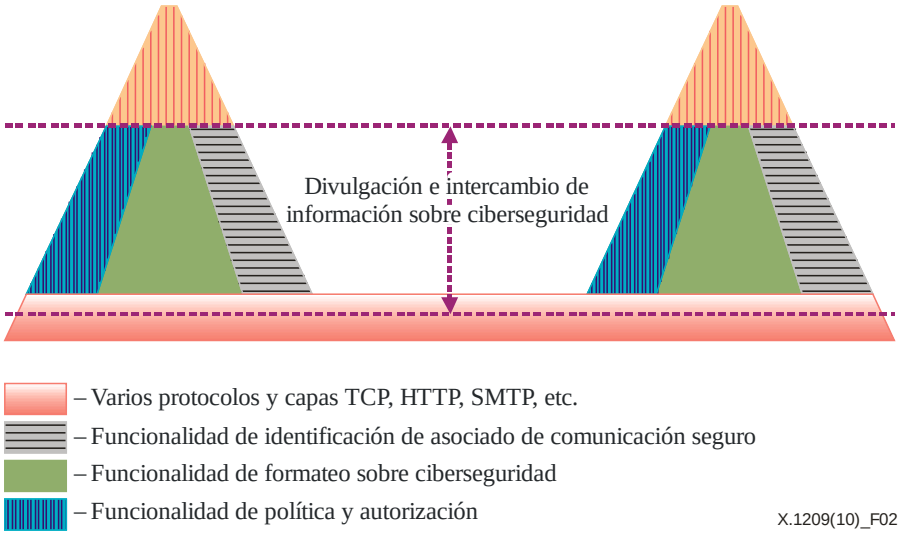

Figura I.2 – Perspectiva de dos nodos

- Los nodos participantes intercambian solicitudes y respuestas mediante varios protocolos y capas de protocolos.

  Las siguientes capacidades son importantes para soportar esta funcionalidad:

  – Capacidades de formateo/codificación (cláusula 8.1).

  – Capacidades de transferencia/intercambio (cláusula 8.2).

- Para muchas aplicaciones se necesitarán métodos confiables para identificar los asociados en una comunicación.

  Las siguientes capacidades son importantes para soportar esta funcionalidad:

  – Capacidades de seguridad (cláusula 8.3).

  – Capacidades de política (cláusula 8.4).

- Los nodos adquieren y utilizan datos proporcionados por otros nodos.

  Las siguientes capacidades son importantes para soportar esta funcionalidad:

  – Capacidades de formateo/codificación (cláusula 8.1).

  – Capacidades de seguridad (cláusula 8.3).

  – Capacidades de política (cláusula 8.4).

  – Capacidades de neutralidad del vendedor (cláusula 8.5).

- Las aplicaciones utilizan varias funcionalidades de verificación de autorización para satisfacer varios requisitos relativos a la seguridad en función de las necesidades, sobre la base de la aplicación.

  Las siguientes capacidades son importantes para soportar esta funcionalidad:

  – Capacidades de política (cláusula 8.4).

- Las aplicaciones en nodos diferentes pueden necesitar utilizar información de identidad de otros nodos por diversos motivos, por ejemplo, el cliente del Nodo A pide acceso a información sobre ciberseguridad disponible en el Nodo B.

  Las siguientes capacidades son importantes para soportar esta funcionalidad:

  – Capacidades de política (cláusula 8.4).

- Las funcionalidades centrales de un nodo participante determinado son:
  - Recibir información sobre ciberseguridad.
  - Almacenar/archivar información sobre ciberseguridad.
  - Atender a solicitudes de información sobre ciberseguridad.

  Las siguientes capacidades son importantes para apoyar las referidas funcionalidades:
  - Capacidades de formateo/codificación (cláusula 8.1).
  - Capacidades de transferencia/intercambio (cláusula 8.2).
  - Capacidades de política (cláusula 8.4).
- Las aplicaciones utilizan herramientas conexas, por ejemplo, verificación de autenticación y autorización para tratar cuestiones relacionadas con el acceso.

  Las siguientes capacidades son importantes para soportar esta funcionalidad:
  - Capacidades de seguridad (cláusula 8.3).
  - Capacidades de política (cláusula 8.4).
- Las aplicaciones utilizan un modelo de datos común para tratar cuestiones relacionadas con el acceso entre nodos.

  Las siguientes capacidades son importantes para soportar esta funcionalidad:
  - Capacidades de formateo/codificación (cláusula 8.1).
  - Capacidades de transferencia/intercambio (cláusula 8.2).
  - Capacidades de neutralidad del vendedor (cláusula 8.5).
- Las aplicaciones utilizan identificadores confiables en las comunicaciones entre nodos y entre nodos y clientes.

  Las siguientes capacidades son importantes para soportar esta funcionalidad:
  - Capacidades de seguridad (cláusula 8.3).
  - Capacidades de política (cláusula 8.4).
- Las solicitudes y respuestas de nodo a nodo se consideran la "norma", mientras que las aplicaciones pueden proporcionar una interfaz de capa de aplicación entre solicitudes y respuestas de nodo a cliente para los clientes que no implementan los métodos y/o protocolos normalizados utilizados entre nodos.

  Las siguientes capacidades son importantes para soportar esta funcionalidad:
  - Capacidades de formateo/codificación (cláusula 8.1).
  - Capacidades de transferencia/intercambio (cláusula 8.2).
  - Capacidades de neutralidad del vendedor (cláusula 8.5).
- El marco soporta los modos de funcionamiento a discreción/por solicitud así como los modos de funcionamiento que dependen o no del estado.

  Las siguientes capacidades son importantes para soportar esta funcionalidad:
  - Capacidades de transferencia/intercambio (cláusula 8.2).
- Las arquitecturas de aplicación pueden proporcionar los "ganchos" hacia modelos de identificación y de datos de identificación que requieren las aplicaciones.

  Las siguientes capacidades son importantes para soportar esta funcionalidad:
  - Capacidades de seguridad (cláusula 8.3).
  - Capacidades de política (cláusula 8.4)

Apéndice II

Actividades conexas

(El presente apéndice no forma parte integrante de esta Recomendación)

II.1 Información común sobre seguridad

La información común sobre seguridad es una información sobre seguridad abierta proporcionada por organizaciones no lucrativas tales como CERT/CC, MITRE o proyecto abierto. Se trata por ejemplo de información sobre vulnerabilidades y exposiciones comunes (CVE, *common vulnerabilities and exposures*), enumeración de debilidades comunes (CWE, *common weakness enumeration*), enumeración de programas malignos comunes (CME, *common malware enumeration*) y enumeración y clasificación de pautas de ataques comunes (CAPEC, *common attack pattern enumeration and classification*), base de datos de vulnerabilidades de fuentes abiertas (OSVDB, *open source vulnerability database*), firmas que [b-Snort] o [b-Bro] proporcionan, etc.

En el caso de MITRE, CVE es un directorio de vulnerabilidades y exposiciones conocidas de seguridad de la información. Se utiliza como base para la base de datos nacional de vulnerabilidades (NVD, *national vulnerability database*) desarrollada por el Instituto Nacional Estadounidense de Normas y Tecnología (*U.S. National Institute of Standards and Technology*). CWE proporciona un conjunto unificado y medible de debilidades informáticas que permite debates, descripciones, selecciones y utilizaciones más eficaces de herramientas y servicios de seguridad informática que pueden detectar esas debilidades en códigos fuente y sistemas operacionales. CME ofrece identificadores únicos comunes de nuevas amenazas virales y de las amenazas virales emergentes más corrientes para limitar las confusiones durante incidentes debidos a software malignos. No se trata de sustituir los nombres de vendedores utilizados para virus y otras formas de software malignos, sino más bien de facilitar la adopción de una capacidad de indización común y neutra de los software malignos. CAPEC proporciona un catálogo público con pautas de ataques junto con una taxonomía completa de esquemas y clasificaciones.

En el caso de OSVDB, este proyecto es una base de datos independiente de fuente abierta creada por y para la comunidad de la seguridad. Su finalidad es proporcionar una información técnica precisa, detallada, actualizada e imparcial sobre vulnerabilidades de seguridad. Además, promoverá una colaboración más amplia y abierta entre empresas y personas físicas, suprimirá la redundancia de los trabajos y limitará los gastos inherentes al desarrollo y al mantenimiento de bases de datos propias sobre vulnerabilidades.

Snort es un sistema de prevención y detención de intrusiones en redes de fuente abierta que utiliza un lenguaje regido por reglas y combina las ventajas de los métodos de inspección basados en firmas, protocolos y anomalías. Las reglas de Snort se han comparado de manera rigurosa con las mismas normas de que utiliza el VRT (*vulnerability research team*) para los clientes.

Por último, Bro es un proyecto de fuente abierta basado en la detección de intrusiones en la red, que supervisa pasivamente el tráfico de la red y busca actividades sospechosas. Las reglas de Bro pueden describir actividades, las actividades que conviene señalar, o actividades que describen ataques conocidos o el acceso a vulnerabilidades conocidas.

II.2 Nueva información sobre seguridad

La nueva información sobre seguridad genera automáticamente firmas para amenazas o ataques nuevos, tráfico anormal, gusanos desconocidos, etc. La generación de firmas de ataques es desde hace poco un tema candente y se han propuesto varias soluciones experimentales tales como "Early bird" y "Polygraph", cuya finalidad principal es detectar ciberataques y capturar secuencias de bytes que representan la identidad del ataque. El FirstLight Signature Service o Active Malware Protection of Endeavor Security y ZASMIN (Zero-day Attack Signature Management

INfrastructure) de ETRI proporcionan nuevas firmas constantemente actualizadas, revisadas y ampliadas. Estas tecnologías avanzadas de generación de pautas nos permiten generar automáticamente firmas basadas en tráfico de ataque. Si bien ha mejorado notablemente la calidad de las firmas, la comunicación de firmas todavía está en mantillas.

II.3 Actividades relacionadas con la comunicación de información sobre seguridad

II.3.1 Equipos encargados de los incidentes informáticos (CIRT)

Los CIRT estudian vulnerabilidades de seguridad de las redes, investigan cambios a largo plazo en los sistemas de red y desarrollan información y capacitación para ayudar a mejorar la seguridad. Siguen respondiendo a grandes incidentes de seguridad y analizan vulnerabilidades de productos. Además del rápido aumento del tamaño de Internet y de la utilización de funciones críticas en la misma, se han observado cambios progresivos en las técnicas de intrusión, un aumento de los daños causados, mayores dificultades para detectar los ataques y un aumento de las dificultades para capturar a los atacantes.

II.3.2 Organismo Europeo de Seguridad de las Redes y la Información

El Organismo Europeo de Seguridad de las Redes y la Información (ENISA) ha presentado el primer estudio de viabilidad de un Sistema Europeo de Comunicación de Información y Alerta (EISAS, *European Information Sharing and Alert System*) para informar a las PYME (pequeñas y medianas empresas) y a los ciudadanos de la Unión Europea sobre amenazas, vulnerabilidades y ataques. En ese estudio se llega la conclusión de que la manera ideal de que la UE facilite la comunicación de información consiste en que asuma el papel de facilitador, moderador de los debates y "custodio de prácticas idóneas" entre comunicación de información nacional y sistema de alerta, en lugar de adoptar una posición operacional central. Para llevar a cabo el estudio, se daba por supuesta la viabilidad de un EISAS, que era necesario verificar. Este sistema sugiere un modelo general que consiste en tres componentes principales y este modelo tenía por objeto identificar áreas funcionales en las cuales un EISAS podría añadir valor a las actividades existentes de comunicación de información en los estados miembros y colmar brechas en la cobertura con información NIS (seguridad de redes e informática). Los tres componentes son IGC (componente de compilación de información, *information gathering component*), IPC (componente de procesamiento de información, *information processing component*) e IDC (componente de divulgación de información, *information dissemination component*).

II.3.3 Forum of Incident Response and Security Teams

El Forum of Incident Response and Security Teams (FIRST) es la principal organización y líder mundial reconocido en la respuesta a incidentes. La participación en el FIRST permite que los equipos de respuesta a incidentes respondan más eficazmente a los incidentes de seguridad – reactivo y proactivo. Este foro reúne a diversos equipos de respuesta a incidentes de seguridad informática de organizaciones públicas, comerciales y docentes. Tiene por objeto fomentar la cooperación y coordinación en la prevención de incidentes, estimular la pronta reacción a incidentes y promover la comunicación de información entre sus miembros y la comunidad en general.

II.3.4 Asia Pacific Computer Emergency Response Team

El Asia Pacific Computer Emergency Response Team (APCERT) coopera con equipos de intervención en caso de emergencia informática (CERT) y equipos encargados de los incidentes informáticos (CSIRT) para velar por la seguridad de Internet en la región de Asia-Pacífico, sobre la base de una auténtica comunicación de información, confianza y cooperación. Facilitan la comunicación de información y los intercambios tecnológicos, incluida información sobre seguridad, virus y códigos maliciosos entre sus miembros. También promueve la colaboración en la investigación y el desarrollo de temas de interés para sus miembros, y formular recomendaciones

para ayudar a tramitar cuestiones legislativas relacionadas con la información sobre seguridad y la respuesta a emergencias a través de fronteras regionales.

II.3.5 Centro de comunicación y análisis de información para telecomunicaciones

Internet y otras redes de telecomunicaciones son la base de una estructura económica social a escala mundial. Garantizar la seguridad de la información se vuelve urgente en la vida económica social. El Centro de comunicación y análisis de información para telecomunicaciones (Telecom-ISAC) tiene por objeto compilar, analizar y comunicar información sobre incidentes y tomar medidas oportunas para garantizar una explotación sin problemas y estable de los servicios de telecomunicaciones. Además, el ISAC crea un foro para que diversos miembros colaboren y compartan sus opiniones y experiencias, incluida información sobre riesgos de seguridad, vulnerabilidades, soluciones de seguridad, etc.

Apéndice III

Actividades conexas

(El presente apéndice no forma parte integrante de esta Recomendación)

[APCERT]	Asia Pacific Computer Emergency Response Team, http://www.apcert.org
[CERT]	Computer Emergency Response Team, http://www.cert.org
[ENDEAVOR]	Endeavor Security, http://www.endeavorsecurity.com
[FIRST]	Forum of Incident Response and Security Team, http://www.first.org
[MITRE]	MITRE, http://makingsecuritymeasurable.mitre.org/
[Telecom-ISAC]	Telecom information sharing and Analysis Center, https://www.telecom-isac.jp
[WIKI]	Wikipedia, http://en.wikipedia.org

Bibliografía

[b-ITU-T X.1205] Recomendación UIT-T X.1205 (2008), *Aspectos generales de la ciberseguridad*.

[b-Bro] Bro (November 2004). *Quick Start Guide Manual*.

[b-EISAS] European information sharing and Alert System (2006/2007), *A feasibility study*.

[b-OSVDB] Open Source Vulnerability DataBase. *Project Aims and Objectives*.

[b-Snort] Snort (May 2008). *Snort User Manual 2.8.2*.

[b-ZASMIN] Information Security Research Division of ETRI, *Zero-day Attack Signature Management Infrastructure*.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Terminales y métodos de evaluación subjetivos y objetivos
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2011