

Unión Internacional de Telecomunicaciones

**UIT-T**

SECTOR DE NORMALIZACIÓN  
DE LAS TELECOMUNICACIONES  
DE LA UIT

**X.1500**

(04/2011)

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

Intercambio de información de ciberseguridad –  
Aspectos generales de la ciberseguridad

---

**Aspectos generales del intercambio de  
información de ciberseguridad**

Recomendación UIT-T X.1500

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.1500

### Aspectos generales del intercambio de información de ciberseguridad

#### Resumen

En esta Recomendación se describen técnicas para el intercambio de información de ciberseguridad. Estas técnicas pueden utilizarse individualmente o combinadas, según se prefiera o sea adecuado, para mejorar la ciberseguridad mediante el intercambio de información coherente, completa, global, oportuna y asegurada. No existen obligaciones implícitas de intercambio de información, ni se aborda cómo se adquiere o, en última instancia, se utiliza la información. El intercambio de información de ciberseguridad (CYBEX) es uno de los elementos que aporta confianza y seguridad en la utilización de las TIC.

#### Historia

Edición	Recomendación	Aprobación	Comisión de Estudio
1.0	ITU-T X.1500	2011-04-20	17
1.1	ITU-T X.1500 (2011) Amd. 1	2012-03-02	17
1.2	ITU-T X.1500 (2011) Amd. 2	2012-09-07	17

## 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/>.

© UIT 2012

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

## ÍNDICE

	<b>Página</b>
1 Alcance .....	1
2 Referencias .....	1
3 Definiciones.....	1
3.1    Términos definidos en otros documentos.....	1
3.2    Términos definidos en esta Recomendación .....	2
4 Abreviaturas y acrónimos .....	2
5 Convenios .....	3
6 Conceptos básicos – Intercambio de información de ciberseguridad (CYBEX) .....	3
7 Técnicas de intercambio estructurado de información de ciberseguridad.....	5
7.1    Agrupación de intercambio de debilidades, vulnerabilidades y estado.....	6
7.2    Agrupación de intercambio: eventos, incidentes y observaciones heurísticas .....	6
7.3    Agrupación de intercambio: políticas de intercambio de información .....	6
7.4    Agrupación de identificación, descubrimiento y consulta .....	6
7.5    Agrupación de garantía de la identidad .....	7
7.6    Agrupación de protocolo de intercambio .....	7
Apéndice I – Técnicas de intercambio estructurado de información de ciberseguridad .....	8
Apéndice II – Ontología del intercambio de información de ciberseguridad .....	18
II.1    Dominios de operación.....	19
II.2    Entidades de ciberseguridad .....	19
II.3    Información operacional de ciberseguridad .....	20
Apéndice III – Ejemplos de esquemas de automatización de la seguridad mediante CYBEX.....	23
III.1    Ejemplo: USA Federal Desktop Core Configuration/United States Government Configuration Baseline.....	24
III.2    Ejemplo: Japan Vulnerability Information Portal Site, JVN.....	25
Bibliografía .....	28

## Introducción

Esta Recomendación tiene por objetivo ser adaptable, susceptible ser ampliada y no prescriptiva a fin de permitir la aplicación de una amplia variedad de técnicas (algunas de las cuales están en permanente evolución y en diversas etapas de compleción) en diferentes implementaciones para mejorar el intercambio de información de ciberseguridad relativa a infraestructura, dispositivos y servicios de telecomunicaciones/TIC. La Recomendación será revisada periódicamente según evolucionen dichas técnicas y las que se consideren convenientes se publicarán como Recomendaciones de la serie X.1500 del UIT-T.

Las técnicas descritas en esta Recomendación tienen por objetivo permitir que organizaciones de telecomunicaciones/TIC, incluyendo equipos encargados de los incidentes informáticos (CIRT), tanto en sus propios ámbitos de actuación como en sus relaciones con otros distintos:

- a) dispongan de información para poder tomar decisiones y llevar a cabo actuaciones que mejoren sustancialmente la confidencialidad, integridad y disponibilidad de facilidades y servicios de telecomunicaciones/TIC globales;
- b) dispongan de información que facilite procesos de colaboración seguros y controles que mejoren el nivel de garantía del intercambio de información entre organizaciones;
- c) permitan un enfoque coherente de la gestión e intercambio de información de ciberseguridad sobre una base global;
- d) mejoren la concienciación y colaboración en materia de seguridad para disminuir las ciberamenazas, los ataques y el software maligno.

Las técnicas incluyen:

- estructurar la información de seguridad para la realización de intercambios;
- identificar y descubrir información y entidades de ciberseguridad;
- establecer confianza y acuerdos sobre la política entre entidades que realicen intercambios;
- realizar peticiones y respuestas con información de ciberseguridad;
- garantizar la integridad del intercambio de información de ciberseguridad;

y se organizan en las "agrupaciones" siguientes:

- debilidad, vulnerabilidad y estado;
- eventos, incidentes y observaciones heurísticas;
- política de intercambio de información;
- identificación, descubrimiento y consulta;
- garantía de identidad;
- protocolos de intercambio.

## Recomendación UIT-T X.1500

### Aspectos generales del intercambio de información de ciberseguridad

#### 1 Alcance

En esta Recomendación se presenta un modelo de intercambio de información de ciberseguridad (CYBEX) y se analizan técnicas para facilitar el intercambio de información de ciberseguridad. Dichas técnicas pueden utilizarse individualmente o combinadas, según sea adecuado, para mejorar la ciberseguridad mediante el intercambio de información coherente, completa, global, oportuna y asegurada. No existen obligaciones implícitas de intercambio de información, ni se aborda cómo adquirir o utilizar la información. Las técnicas incluyen el descubrimiento e interoperabilidad global y estructurada de información de ciberseguridad de forma que se permita una evolución permanente de la misma para acomodar las actividades relevantes y la evolución de las especificaciones realizadas en numerosos foros sobre ciberseguridad. CYBEX es uno de los elementos que aporta confianza y seguridad en la utilización de las TIC.

Esta Recomendación incluye las funciones básicas siguientes que pueden utilizarse de forma separada o conjuntamente según proceda:

- estructurar la información de ciberseguridad para la realización de intercambios;
- identificar y descubrir información y entidades de ciberseguridad;
- establecer confianza y acuerdos sobre la política entre entidades que realicen intercambios;
- realizar peticiones y respuestas con información de ciberseguridad;
- garantizar la integridad del intercambio de información de ciberseguridad.

En función de las políticas acordadas y la legislación y reglamentación aplicables, la forma de adquirir información y el uso que se haga de la misma quedan específicamente fuera del alcance de esta Recomendación y no se tratan en la misma. Algunas reglamentaciones y legislaciones nacionales y regionales pueden requerir la implementación de mecanismos para proteger la información identificable de carácter personal. Esta Recomendación no impone la obligatoriedad de las técnicas ni del intercambio de información de ciberseguridad conexas descritas en la misma.

#### 2 Referencias

Ninguna.

#### 3 Definiciones

##### 3.1 Términos definidos en otros documentos

Esta Recomendación utiliza los términos siguientes que se definen en otros documentos:

**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 multimedia, 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 la disponibilidad, integridad (que puede incluir la autenticidad y el no repudio) y la confidencialidad.

NOTA – Determinadas legislaciones y reglamentaciones nacionales pueden exigir la implementación de mecanismos para la protección de información de identificación personal.

**3.1.2 incidente de seguridad** [b-UIT-T E.409]: cualquier evento adverso que podría amenazar algún aspecto relacionado con la seguridad.

## 3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los términos siguientes:

**3.2.1 garantía:** grado de confianza con que el proceso o los resultados cumplen sus objetivos de seguridad.

**3.2.2 protocolo de intercambio:** conjunto de reglas técnicas y formatos que rige el intercambio de información entre dos o más entidades.

**3.2.3 política de intercambio de información:** términos y condiciones asociados a la utilización e intercambio de información de ciberseguridad.

**3.2.4 estado del sistema:** estado actual de un sistema o una entidad, incluida información tal como configuración, utilización de memoria u otros datos relevantes para la ciberseguridad.

**3.2.5 vulnerabilidad** (armonizado con [b-UIT-T X.800]): toda debilidad que puede explotarse para violar un sistema o la información que contiene.

**3.2.6 debilidad:** carencia o imperfección que, aunque en sí no pueden considerarse una vulnerabilidad, podrían en determinado punto convertirse en vulnerabilidad o contribuir a la creación de otras vulnerabilidades.

## 4 Abreviaturas y acrónimos

Esta Recomendación utiliza las abreviaturas y acrónimos siguientes:

ARF	Formato de resultados de evaluación o formato de resultados de activos (en función del contexto) ( <i>assessment results format or asset reporting format</i> )
BEEP	Protocolo de intercambio extensible de bloques ( <i>blocks extensible exchange protocol</i> )
CA	Autoridad de certificación ( <i>certification authority</i> )
CAPEC	Enumeración y clasificación de pautas de ataques comunes ( <i>common attack pattern enumeration and classification</i> )
CCE	Enumeración común de configuraciones ( <i>common configuration enumeration</i> )
CEE	Expresión común de eventos ( <i>common event expression</i> )
CEEE	Intercambio común de expresiones de eventos ( <i>common event expression exchange</i> )
CIRT	Equipos encargados de incidentes informáticos ( <i>computer incident response team</i> )
CPE	Enumeración común de plataformas ( <i>common platform enumeration</i> )
CVE	Vulnerabilidades y exposiciones comunes ( <i>common vulnerabilities and exposures</i> )
CVSS	Sistema común de puntuación de vulnerabilidades ( <i>common vulnerability scoring system</i> )
CWE	Enumeración común de debilidades ( <i>common weakness enumeration</i> )
CWSS	Sistema común de puntuación de debilidades ( <i>common weakness scoring system</i> )
CYBEX	Intercambio de información de ciberseguridad ( <i>cybersecurity information exchange</i> )
CYIQL	Lenguaje de consulta de información de ciberseguridad ( <i>cybersecurity information query language</i> )

DDoS	Ataque de denegación de servicio distribuido ( <i>distributed denial of service</i> )
EVC	Certificados de validación extendida ( <i>extended validation certificates</i> )
EVCERT	Certificado de validación extendida ( <i>extended validation certificate</i> )
HTTP	Protocolo de transferencia de hipertexto ( <i>hypertext transfer protocol</i> )
IC	Circuito integrado ( <i>integrated circuit</i> )
IDS	Sistema de detección de intrusiones ( <i>intrusion detection system</i> )
IODEF	Formato de intercambio de descripciones de objetos incidentes ( <i>incident object description exchange format</i> )
IPS	Sistema de prevención de intrusiones ( <i>intrusion prevention system</i> )
MAEC	Enumeración y caracterización de atributos de software maligno ( <i>malware attribute enumeration and characterization</i> )
OID	Identificador de objeto ( <i>object identifier</i> )
OS	Sistema operativo ( <i>operating system</i> )
OVAL	Vulnerabilidad abierta y lenguaje de evaluación ( <i>open vulnerability and assessment language</i> )
RID	Defensa entre redes en tiempo real ( <i>real-time inter-network defense</i> )
SCAP	Protocolo de automatización de contenidos de seguridad ( <i>security content automation protocol</i> )
SOAP	Protocolo simple de acceso a objetos ( <i>simple object access protocol</i> )
TI	Tecnologías de la información ( <i>information technology</i> )
TIC	Tecnologías de la información y las comunicaciones ( <i>information and communication technology</i> )
TLP	Protocolo ligero de tráfico ( <i>traffic light protocol</i> )
TLS	Seguridad de la capa de transporte ( <i>transport layer security</i> )
TNC	Conexión fiable a la red ( <i>trusted network connect</i> )
TPM	Módulo de plataforma fiable ( <i>trusted platform module</i> )
XCCDF	Formato extensible de descripción de lista de verificación de configuración ( <i>extensible configuration checklist description format</i> )

## 5 Convenios

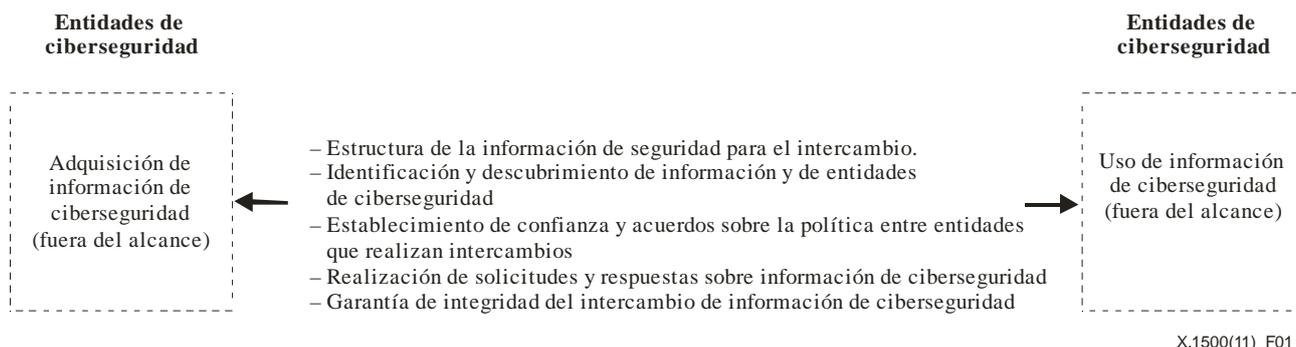
En esta Recomendación se emplean los términos "norma" y "normas" de manera genérica y ha de entenderse que comprenden las normas, las especificaciones y las Recomendaciones.

## 6 Conceptos básicos – Intercambio de información de ciberseguridad (CYBEX)

Esta Recomendación sobre el intercambio de información de ciberseguridad (CYBEX) tiene un objetivo simple y limitado, a saber, describir técnicas mediante las que entidades de ciberseguridad puedan intercambiar información de ciberseguridad empleando métodos que ofrecen un nivel de garantía adecuado. Dichas entidades son típicamente organizaciones, personas, dispositivos o procesos que tiene o buscan información de ciberseguridad. Con frecuencia, dichas organizaciones son equipos encargados de incidentes informáticos (CIRT), operadores o vendedores de equipos, software o sistemas basados en la red.

El intercambio de información de ciberseguridad es una herramienta valiosa para lograr una protección reforzada de las infraestructuras y la ciberseguridad, así como para apoyar las principales funciones realizadas por los CIRT.

El intercambio de información de ciberseguridad puede tener lugar tanto en el seno de comunidades de confianza muy segmentadas con controles estrictos de acceso a la información basados en políticas preestablecidas, como en el dominio público. El conocimiento de amenazas, vulnerabilidades, incidentes, riesgos y técnicas de mitigación, así como sus remedios asociados, son ejemplos del tipo de información de ciberseguridad habitualmente intercambiada entre entidades. Las técnicas incluidas en esta Recomendación tienen por objeto facilitar dicho intercambio de información y, por ende, mejorar la ciberseguridad.



**Figura 1 – Modelo CYBEX**

El modelo general de intercambio de información de ciberseguridad utilizado en esta Recomendación consta, tal como se muestra en la figura 1, de funciones básicas que pueden utilizarse de forma separada o conjuntamente, según sea adecuado, y ampliarse, según sea necesario para permitir un intercambio de información de ciberseguridad con garantías. Dichas funciones son las siguientes:

- Estructurar la información de ciberseguridad para la realización de intercambios.
- Identificar y descubrir información y entidades de ciberseguridad.
- Establecer confianza y acuerdos sobre la política entre entidades que realicen intercambios.
- Realizar peticiones y respuestas con información de ciberseguridad.
- Garantizar la integridad del intercambio de información de ciberseguridad.

En la cláusula 7 se describen técnicas para llevar a cabo dichas funciones.

El intercambio de información de ciberseguridad puede ser bidireccional. Dicha bidireccionalidad permite realizar peticiones y respuestas verificadas de información a fin de alcanzar los niveles de garantía requeridos entre las partes o para certificar la entrega.

La forma de adquirir información y de utilizarla está sujeta a políticas y disposiciones legales y reglamentarias aplicables en cada caso, que quedan fuera del alcance de esta Recomendación y no se abordan en la misma. Por ejemplo, algunas implementaciones de intercambio de información de ciberseguridad, tales como el rastreo de fuentes de ataques, pueden requerir mecanismos específicos en función de la aplicación que permitan establecer conjuntos de preguntas y respuestas recursivas para obtener la información requerida. Sin embargo, otras características de la implementación, tales como utilizar capacidades para la automatización de la seguridad para que ésta sea mensurable y gestionable, están en el ámbito de esta Recomendación. Las técnicas incluidas en la misma permiten estos y otros tipos de casos de uso. Esta Recomendación no impone la obligatoriedad de las técnicas ni del intercambio de información de ciberseguridad conexas descritas en la misma, pudiendo ser adecuada la utilización de otras técnicas.

## **7 Técnicas de intercambio estructurado de información de ciberseguridad**

El intercambio de información de ciberseguridad entre dos entidades cualesquiera debe estar estructurado y descrito de forma consistente para que sea comprensible por ambas entidades. El objetivo de CYBEX es hacer más fácil el intercambio de información de ciberseguridad, al incluir "enumeraciones comunes", es decir, listas ordenadas de valores de información bien establecidos en el sector para el mismo tipo de datos. La enumeración común permite vincular bases de datos y otras capacidades, y facilita las comparaciones relativas a la ciberseguridad.

Con el fin de realizar dichos intercambios, la información de ciberseguridad incluye información estructurada o conocimientos sobre:

- el "estado" del equipo, el software o los sistemas de red con respecto a la ciberseguridad, en particular las vulnerabilidades;
- informes forenses de incidentes o eventos;
- heurística y conocimientos extraídos de la experiencia;
- entidades de ciberseguridad involucradas;
- especificaciones para el intercambio de información de ciberseguridad, incluidos módulos, esquemas, términos y condiciones, y números asignados;
- identidades y atributos de garantía de toda la información de ciberseguridad;
- requisitos, directrices y prácticas de aplicación.

Para describir a nivel general los atributos deseados del intercambio de información de ciberseguridad, las capacidades de información estructuradas se organizan en seis agrupaciones de técnicas para distintos conjuntos de intercambios de información de ciberseguridad. Dichas agrupaciones son las siguientes:

- debilidad, vulnerabilidad y estado;
- eventos, incidencias y prácticas heurísticas;
- política de intercambio de información.
- identificación, descubrimiento y consulta;
- garantía de la identidad;
- protocolos de intercambio.

Dichas agrupaciones son clasificaciones amplias, pudiendo utilizarse las capacidades de una agrupación en alguna de las restantes agrupaciones en función de la aplicación.

Las agrupaciones anteriores se describen con detalle en las subcláusulas siguientes. La descripción de cada agrupación proporciona una visión general de su papel en el CYBEX y enumera técnicas para su realización. Ninguna de las técnicas identificadas se consideran prescriptivas, sino técnicas consistentes con los objetivos de la agrupaciones pertinente. La elección del tratamiento está básicamente relacionada con el grado de especialización de la comunicad de usuarios "propietaria" y con los beneficios derivados de su utilización.

Las técnicas CYBEX de esta Recomendación identifican un conjunto de técnicas complementarias que permiten y facilitan estas y otras implementaciones.

En el resto de esta cláusula y en el apéndice I conexo se describe cada agrupación, incluye una visión general del papel de cada una en el CYBEX y enumera técnicas para la implementación de cada una. Las referencias no son normativas y se detallan en la bibliografía.

Los implementadores y usuarios de las técnicas de las agrupaciones cumplirán todas las leyes, reglamentos y políticas nacionales y regionales aplicables.

### **7.1 Agrupación de intercambio de debilidades, vulnerabilidades y estado**

Las capacidades habilitadoras asociadas a la agrupación de intercambio de debilidades, vulnerabilidades y estado permite el intercambio de información sobre debilidades y vulnerabilidades y/o la evaluación del estado del sistema y las aplicaciones.

En el cuadro I.1 se enumeran las capacidades habilitadoras representativas de los tipos que pueden facilitar el soporte del intercambio de debilidades, vulnerabilidades e información de estado.

### **7.2 Agrupación de intercambio: eventos, incidentes y observaciones heurísticas**

Las capacidades habilitadoras asociadas a la agrupación de intercambio de eventos, incidentes y observaciones heurísticas permiten el intercambio de información de eventos, incidentes y otras observaciones heurísticas.

En el cuadro I.2 se enumeran las capacidades habilitadoras representativas de los tipos que pueden facilitar el intercambio de eventos, incidentes y observaciones heurísticas de forma estructurada entre CIRT y otras entidades. Esta información intercambiada puede utilizarse para crear respuestas globales a ataques y reducir las debilidades y vulnerabilidades existentes.

### **7.3 Agrupación de intercambio: políticas de intercambio de información**

Las capacidades habilitadoras asociadas a la agrupación de intercambio de políticas de intercambio de información permiten la compartición y utilización entre entidades de información de ciberseguridad relativa a los términos y condiciones asociadas a la información compartida entre las mismas. Puede estar ligado a la información específica compartida, o a la clase amplia de información a la que ésta pertenece, o estar asociada a las entidades involucradas. En la medida en que sea necesario por las circunstancias, es deseable proporcionar una indicación de dichas políticas a las entidades involucradas. Dicha indicación puede tomar muchas formas, y transportarse junto con la información o de forma independiente, través de mecanismos pregunta-respuesta.

En el cuadro I.3 se enumeran las capacidades habilitadoras representativas de los tipos que pueden facilitar el intercambio de información política entre entidades de ciberseguridad. Téngase en cuenta que en los foros de intercambio de información de seguridad se continúan generando protocolos y requisitos para el intercambio de políticas entre entidades de ciberseguridad, por lo que es necesario tomar las precauciones necesarias para asegurar su correcta implementación.

### **7.4 Agrupación de identificación, descubrimiento y consulta**

Las capacidades habilitadoras asociadas a la agrupación de identificación, descubrimiento y consulta soportan los procesos de identificación, descubrimiento y consulta.

Existen intereses comunes entre comunidades de ciberseguridad en relación con los identificadores de ciberseguridad, su creación, administración, descubrimiento, verificación y uso. Algunos de dichos intereses son los siguientes:

- Mejora del valor de la información de ciberseguridad al permitir una amplia difusión de la información relacionada con eventos y el análisis de eventos a lo largo de periodos de tiempo prolongados
- Mejora de la seguridad de los intercambios de información de ciberseguridad al permitir que se pueda obtener información del identificador para la verificación y conocimiento de las políticas conexas.
- Mejora de la flexibilidad de los intercambios de información de ciberseguridad al permitir que pueda obtenerse información nueva o adicional asociada con el mensaje, por ejemplo, estado de la información.

Las organizaciones de seguridad pueden desear implementar en aplicaciones operacionales protocolos de ciberseguridad comunes para la captura e intercambio de información de estado del sistema, vulnerabilidades, análisis forense y análisis heurístico de incidentes. Dado que este tipo de información procede de diferentes fuentes, los implementadores deberían armonizar la forma de identificar las organizaciones de ciberseguridad, las políticas de confianza e intercambio de información y la información en sí misma que se intercambia o distribuye. La existencia de un identificador único a nivel global para el intercambio de información de ciberseguridad implica necesariamente que tenga las características siguientes:

- simplicidad, usabilidad, flexibilidad, extensibilidad, escalabilidad y despleabilidad;
- gestión distribuida de diversos esquemas de identificadores;
- fiabilidad a largo plazo de registradores de identificadores y disponibilidad de herramientas de altas prestaciones para el descubrimiento de información asociada a cualquier identificador.

En el cuadro I.4 se enumeran las capacidades habilitadoras representativas de los tipos que pueden facilitar la identificación de organizaciones de ciberseguridad y los procesos de descubrimiento y consulta de información de ciberseguridad.

### **7.5 Agrupación de garantía de la identidad**

Las capacidades habilitadoras asociadas a la agrupación de garantía de la identidad soportan la garantía de la identidad.

En el CYBEX, el intercambio real de información estructurada puede tener lugar de diferentes formas, a través de una red o transportado físicamente. Un elemento fundamental de dicho intercambio es la confianza, tanto en la identidad de las partes como en la información transportada.

En el cuadro I.5 se enumeran las capacidades habilitadoras representativas de tipos que pueden soportar la garantía de la identidad.

### **7.6 Agrupación de protocolo de intercambio**

Las capacidades habilitadoras de la agrupación de protocolo de intercambio comprenden los protocolos de intercambio que pueden emplearse en diversos contextos de intercambio de información de ciberseguridad. El intercambio seguro de información exige una combinación de los protocolos que se indican a continuación. La defensa entre redes en tiempo real (RID) ofrece un marco de mensajería para comunicar información sobre incidentes y las políticas asociadas a esa información. El protocolo de transporte para los mensajes RID que encapsulan los documentos de incidentes IODEF (y todas las extensiones de IODEF) incluye las opciones de transporte BEEP, SOAP y HTTPS enumeradas. El transporte de mensajes RID (el protocolo inicial creado para el transporte de RID) puede sustituirse por SOAP, BEEP y los protocolos que se creen en el futuro. Las consideraciones de seguridad y privacidad están contenidas en RID a fin de poder separar la mensajería del transporte.

En el cuadro I.6 se enumeran las capacidades habilitadoras representativas de los tipos de protocolos de intercambio que pueden utilizarse como para el intercambio de información.

## Apéndice I

### Técnicas de intercambio estructurado de información de ciberseguridad

(Este apéndice no forma parte integrante de la presente Recomendación)

**Cuadro I.1 – Técnicas de la agrupación de intercambio de debilidades, vulnerabilidades y estados**

Técnica	Descripción	Referencias
<b>Vulnerabilidades y exposiciones comunes (CVE)</b>	Las vulnerabilidades y exposiciones comunes (CVE) constituyen un método para identificar e intercambiar información sobre vulnerabilidades y exposiciones de la información con el fin de proporcionar identificadores comunes para problemas que son conocidos públicamente. El objetivo de la CVE es facilitar el intercambio de datos entre distintas capacidades contra vulnerabilidades (herramientas, repositorios y servicios) gracias a dicha "enumeración común". La CVE está diseñada para vincular bases de datos y otros recursos y facilitar la comparación de herramientas y servicios de seguridad. La CVE no contiene información del tipo riesgo, impacto, remedios o información técnica detallada. La CVE sólo contiene el número identificador normalizado con indicación de estado, una breve descripción y referencias a informes y consejos sobre vulnerabilidades conexas. La CVE pretende ser completa para abarcar todas las vulnerabilidades y exposiciones conocidas públicamente. Si bien está diseñada para que contenga información madura, el objetivo principal es identificar las vulnerabilidades y exposiciones detectadas mediante herramientas de seguridad, así como identificar nuevos problemas que sean conocidos públicamente y abordar, cuando sea necesario, la revisión de cualquier problema de seguridad antiguo.	[b-UIT-T X.1520]
<b>Sistema común de puntuación de vulnerabilidades (CVSS)</b>	El sistema común de puntuación de vulnerabilidades (CVSS) proporciona un marco abierto para la comunicación de las características e impactos de las vulnerabilidades de las TIC. El CVSS consta de tres grupos: base, temporal y del entorno. Cada grupo asigna una puntuación numérica que varía entre 0 y 10, y un vector, que es una representación textual comprimida que refleja los valores utilizados para obtener la puntuación. El grupo base representa las características intrínsecas de una vulnerabilidad. El grupo temporal refleja las características de una vulnerabilidad que cambian con el tiempo. El grupo del entorno refleja las características de una vulnerabilidad que son específicas del entorno del usuario. El CVSS permite a los gestores de las TIC, proveedores de boletines de vulnerabilidades, vendedores de aplicaciones e investigadores, beneficiarse de la adopción de un lenguaje común para valorar numéricamente las vulnerabilidades de las TIC.	[b-UIT-T X.1521]

**Cuadro I.1 – Técnicas de la agrupación de intercambio de debilidades, vulnerabilidades y estados**

Técnica	Descripción	Referencias
<b>Enumeración común de debilidades (CWE)</b>	<p>La enumeración común de debilidades (CWE) es un proceso para la identificación e intercambio de conjuntos unificados y medibles de debilidades del software. La CWE permite analizar, describir, seleccionar y utilizar más eficazmente herramientas y servicios de seguridad del software que pueden detectar dichas debilidades en códigos fuente y en sistemas operativos. También proporciona una mejor comprensión y capacidad de gestión de las debilidades del software relacionadas con la arquitectura y el diseño. Las implementaciones de la CWE son compiladas y actualizadas por un grupo heterogéneo de expertos internacionales de empresas, universidades y agencias gubernamentales, lo que asegura la amplitud y profundidad de las mismas. La CWE proporciona terminología normalizada, permite a los proveedores de servicios informar a los usuarios de debilidades potenciales concretas y de las soluciones propuestas para las mismas, de forma que los compradores de software puedan comparar productos similares ofrecidos por diversos vendedores.</p>	[b-CWE]
<b>Sistema común de puntuación de debilidades (CWSS)</b>	<p>El sistema común de puntuación de debilidades proporciona un marco abierto para la comunicación de las características e impactos de las debilidades del software.</p>	[b-CWSS]
<b>Lenguaje abierto de vulnerabilidades y evaluación (OVAL)</b>	<p>El lenguaje abierto de vulnerabilidades y evaluación (OVAL) es un esfuerzo de especificación internacional para promover contenidos de seguridad abiertos y públicamente disponibles, así como para normalizar la transferencia de dicha información a través de cualquier herramienta y servicio de seguridad. OVAL incluye un lenguaje para codificar el detalle de los sistemas y un conjunto de repositorios de contenidos diversos mantenidos por la comunidad. El lenguaje normaliza los tres principales pasos del proceso de evaluación: representación de la información de configuración de los sistemas en prueba, análisis del sistema para la detección de los estados de máquina especificados (vulnerabilidad, configuración, parche...) e información de los resultados de la evaluación. Los repositorios son conjuntos de contenidos abiertos y públicamente disponibles que utilizan dicho lenguaje.</p> <p>Los esquemas OVAL escritos en XML se han desarrollado para servir como marco y vocabulario del lenguaje OVAL. Estos esquemas se corresponden con los tres pasos del proceso de evaluación: un esquema OVAL de Características del sistema para representar la información del mismo, un esquema OVAL de Definición para expresar un estado de máquina específico y un esquema OVAL de Resultados para informar de los resultados de una evaluación.</p>	[b-OVAL]

**Cuadro I.1 – Técnicas de la agrupación de intercambio de debilidades, vulnerabilidades y estados**

Técnica	Descripción	Referencias
<b>Formato eXtensible de descripción de la lista de verificación de la configuración (XCCDF)</b>	<p>El formato eXtensible de descripción de la lista de verificación de configuración (XCCDF) es un lenguaje que especifica la escritura de listas de verificación de seguridad, comparaciones competitivas y tipos de documentos conexos. Un documento XCCDF representa un conjunto estructurado de reglas de configuración de seguridad para un conjunto de sistemas objetivo. La especificación tiene por objeto permitir el intercambio de información, la generación de documentos, el diseño a medida de aspectos organizacionales y situacionales, las pruebas de conformación automáticas y la puntuación de la conformidad. La especificación también define un modelo y formato de datos para almacenar los resultados de comparativas de pruebas de conformidad. El propósito de XCCDF es proporcionar bases homogéneas para la expresión de listas de verificación de seguridad, comparativas y otras directrices de configuración, promoviendo así una aplicación más extendida de buenas prácticas de seguridad. Los documentos XCCDF se expresan en XML.</p>	[b-XCCDF]
<b>Enumeración común plataformas (CPE)</b>	<p>La enumeración común de plataformas (CPE) es un método normalizado de identificar y describir sistemas software y dispositivos hardware del inventario de activos informáticos de una empresa. El CPE proporciona: una especificación de nombres a utilizar, incluyendo la estructura lógica de nombres CPE correctamente formados y los procedimientos para asociar y desasociar dichos nombres a codificaciones legibles por las máquinas; una especificación de concordancias, que define procedimientos para comparar nombres de CPE a fin de determinar si se refieren a todos o algunos de los productos o plataformas; y un diccionario de identificadores que define el concepto de diccionario de identificadores y prescribe reglas de alto nivel para los responsables del mantenimiento del diccionario.</p>	[b-CPE]
<b>Enumeración común de configuraciones (CCE)</b>	<p>La enumeración común de configuraciones (CCE) proporciona identificadores únicos de aspectos de la configuración de un sistema para permitir una correlación rápida y exacta entre los datos de configuración de diferentes fuentes de información y herramientas. Por ejemplo, los identificadores CCE pueden utilizarse para asociar verificaciones realizadas por herramientas de evaluación de configuraciones con declaraciones que figuren en documentos que describen prácticas idóneas para el establecimiento de configuraciones.</p>	[b-CCE]

**Cuadro I.1 – Técnicas de la agrupación de intercambio de debilidades, vulnerabilidades y estados**

Técnica	Descripción	Referencias
<b>Formato de evaluación de resultados (ARF)</b>	El formato de resultados de evaluación (ARF) es una especificación abierta que proporciona un lenguaje estructurado para el intercambio de datos de resultados de evaluaciones de dispositivos entre distintas herramientas de evaluación, bases de datos de activos y otros productos que gestionan información de activos. Está concebido para ser utilizado por las herramientas que recopilan datos detallados de la configuración de activos de tecnologías de la información. El ARF también incluye una especificación de informe agregado para reportar información de múltiples activos, y un lenguaje de tareas y consultas para consultar los resultados de evaluaciones. Las especificaciones de la automatización de la seguridad describen un proceso extremo a extremo para distribuir el contenido de evaluaciones a almacenes de datos, consultar las evaluaciones recogidas en dichos contenidos, informar de los resultados de las evaluaciones y agregar los resultados de las evaluaciones a nivel de empresa.	[b-ARF]

**Cuadro I.2 – Técnicas relevantes de la agrupación de intercambio de eventos, incidentes y observaciones heurísticas**

Técnica	Descripción	Referencias
<b>Expresión común de eventos (CEE)</b>	La expresión común de eventos (CEE) normaliza la descripción de eventos, su registro e intercambio. Utilizando el lenguaje y la sintaxis común CEE, se pueden gestionar de forma más eficiente y con mejores resultados los registros de conexión, su correlación, agregación, auditoría y gestión a nivel de la empresa. El objetivo básico es normalizar la representación e intercambio de los registros de conexión de sistemas electrónicos. La CEE descompone el almacenamiento e intercambio de registros de conexión en cuatro (4) componentes: taxonomía de eventos, sintaxis de registros de conexión, transporte de registros de conexión y recomendaciones sobre el registro.	[b-CEE]
<b>Formato de intercambio de descripción de objetos de incidentes (IODEF)</b>	El formato de intercambio de descripciones de objetos incidentes (IODEF) define una representación de datos que proporciona un marco para el intercambio de información que normalmente intercambian los CIRT sobre incidentes de seguridad. El IODEF describe un modelo de información y proporciona un modelo de datos asociado especificado mediante un esquema XML.	[b-IETF RFC 5070]

**Cuadro I.2 – Técnicas relevantes de la agrupación de intercambio de eventos, incidentes y observaciones heurísticas**

Técnica	Descripción	Referencias
<b>Formato de información de suplantación de identidad, fraude y uso indebido</b>	<p>El formato de información sobre suplantación de identidad, fraude y uso indebido amplía el formato de intercambio de descripciones de objetos de incidentes (IODEF) para soportar la suplantación de identidad, el fraude y otros tipos de usos indebidos. Estas ampliaciones también soportan el intercambio de información sobre incidentes de correo basura de gran difusión. Las ampliaciones son suficientemente flexibles como para admitir información procedente de actividades ocurridas durante todo el ciclo electrónico del fraude o del correo basura. Es posible utilizar informes sencillos e informes forensicos completos, así como consolidar múltiples incidentes.</p> <p>NOTA – Esta Recomendación sólo describe técnicas aplicables a medios cuyo entendimiento sea generalizado y su uso esté garantizado para el intercambio de información de ciberseguridad entre entidades, pero no aborda los posibles usos de dicha información.</p>	[b-IETF RFC 5901]
<b>Enumeración y clasificación de pautas de ataques comunes (CAPEC)</b>	<p>CAPEC es un método para especificar la identificación, descripción y enumeración de pautas de ataques. Las pautas de ataques son un poderoso mecanismo para determinar y comunicar la perspectiva del agresor. Son descripciones de métodos comunes para la explotación maliciosa del software. Se derivan de pautas de diseño aplicadas de forma destructiva, en lugar de constructiva, y se generan a partir de un análisis profundo de casos reales de programas maliciosos. El objetivo del CAPEC es hacer público un catálogo de pautas de ataque junto con un esquema XML completo y una taxonomía de las mismas.</p>	[b-CAPEC]
<b>Formato de enumeración y caracterización de atributos del software maligno</b>	<p>El formato de enumeración y caracterización de atributos del software maligno (MAEC) es un lenguaje formal que incluye un esquema que proporciona una sintaxis para el vocabulario común de atributos y comportamientos y un formato de intercambio de información estructurada sobre dichos elementos de datos. La enumeración se realiza a distintos niveles de abstracción: actuaciones de bajo nivel, comportamientos de nivel medio y mecanismos de alto nivel. Al nivel más bajo, MAEC describe atributos ligados a la funcionalidad básica y la operación a bajo nivel del software maligno. A nivel medio, el lenguaje MAEC organiza las actuaciones de bajo nivel antes mencionadas en grupos con el objetivo de definir comportamientos de nivel medio. Al nivel más conceptual y alto, el vocabulario MAEC permite la construcción de mecanismos que realizan abstracciones de agrupaciones de comportamientos de software maligno de nivel medio en base a lo conseguido mediante una clasificación de orden superior.</p>	[b-MAEC]

**Cuadro I.3 – Técnicas relevantes de la agrupación de intercambio de política**

Técnica	Descripción	Referencias
<b>Protocolo ligero de tráfico (TLP)</b>	<p>El protocolo ligero de tráfico (TLP) se creó para fomentar el intercambio de información sensible. El origen de la comunicación señala el grado de distribución que desea para la información concernida más allá de quien la recibe directamente. Para ello, el TLP proporciona un método sencillo. Está diseñado para mejorar el flujo de información entre individuos, organizaciones o comunidades de forma controlada y fiable. El TLP se basa en que el origen de la información la etiqueta con uno de entre cuatro colores para indicar el grado de difusión que el receptor puede darle. El receptor debe consultar al origen si desea una difusión mayor. El TLP se considera un modelo de intercambio de información fiable entre comunidades de seguridad en más de 30 países. Los cuatro "niveles de compartición de la información" son los siguientes:</p> <p>ROJO – Personal. La información sólo es para los receptores indicados por sus propios nombres. En el contexto de una reunión, la información ROJA se limita a los presentes. En la mayoría de los casos, la información ROJA se transmite verbalmente o en persona.</p> <p>ÁMBAR – Distribución limitada. El receptor sólo puede compartir la información ÁMBAR con miembros de su organización, pero sólo de conformidad con un proceso de acceso restringido a la misma.</p> <p>VERDE – A nivel de comunidad. La información de esta categoría puede ser circulada ampliamente en el seno de una comunidad concreta. Sin embargo, la información puede no estar autorizada para ser difundida en Internet o liberada fuera de la comunidad.</p> <p>BLANCO – Ilimitado. La información BLANCA puede ser distribuida libremente, sin restricciones, sujeta a lo establecido en materia de derechos de autor.</p>	[b-TLP]

**Cuadro I.4 – Técnicas relevantes de la agrupación de identificación, descubrimiento y consulta**

Técnica	Descripción	Referencias
<b>Mecanismos de descubrimiento aplicables al intercambio de información de ciberseguridad</b>	<p>Estas técnicas incluyen métodos y mecanismos que pueden utilizarse para identificar y localizar fuentes de información de ciberseguridad, tipos de información de ciberseguridad, instancias específicas de información de ciberseguridad, métodos existentes para acceder a información de ciberseguridad, así como políticas que pueden aplicarse al acceso a información de ciberseguridad.</p>	
<b>Directrices para la administración del arco OID para el intercambio de información de ciberseguridad</b>	<p>Se describe un nombre de espacio común de identificadores de ciberseguridad global, junto con requisitos administrativos, como parte de un arco OID coherente, e incluye identificadores para:</p> <ul style="list-style-type: none"> <li>• información de ciberseguridad;</li> <li>• organización de ciberseguridad;</li> <li>• política de ciberseguridad.</li> </ul>	

**Cuadro I.4 – Técnicas relevantes de la agrupación de identificación, descubrimiento y consulta**

Técnica	Descripción	Referencias
<b>Lenguaje de consulta de información de ciberseguridad</b>	El lenguaje de consulta de información de ciberseguridad (CYIQL) define una representación flexible de datos que proporciona un marco para solicitar información sobre incidentes de seguridad informática que normalmente intercambian los equipos encargados de incidentes informáticos (CIRT). Esta especificación describe el modelo de información del CYIQL y proporciona un modelo de datos asociado especificado mediante un esquema XML.	

**Cuadro I.5 – Técnicas relevantes de la agrupación de garantía de identidad**

Técnica	Descripción	Referencias
<b>Plataformas fiables</b>	<p>Los productos informáticos y de comunicaciones con módulos de plataformas fiables (TPM, <i>trusted platform modules</i>) integrados potencian la capacidad de las empresas, instituciones, agencias gubernamentales y consumidores de realizar intercambios de información fiables; por tanto, los TPM son relevantes para la mayoría de las implementaciones de CYBEX. Los TPM son circuitos integrados de propósito especial integrados en una serie de plataformas para permitir que la autenticación de usuario y la verificación de máquinas sean potentes, aspecto fundamental para prevenir el acceso indebido a información confidencial y sensible y para la protección de redes en situación de riesgo.</p> <p>La tecnología de módulos de plataformas fiables se basa en normas abiertas que aseguran la interoperabilidad de un conjunto de productos en entornos con varios proveedores. La norma TPM más extendida consta de un conjunto de especificaciones desarrolladas y mantenidas por el Trusted Computing Group (TCG), junto con un perfil de protección para evaluaciones de seguridad según criterios comunes.</p> <p>Los principios de diseño ofrecen conceptos básicos del TPM e información genérica sobre la funcionalidad TPM. Un diseñador TPM debe analizar e implementar la información en la especificación principal del TPM (partes 1-3) y analizar el documento específico de la plataforma de interés. El documento específico de la plataforma contiene consideraciones normativas que afectan al diseño e implementación del TPM. El diseñador del TPM debe analizar e implementar los requerimientos, incluida la prueba y evaluación, tal como establece el Grupo de trabajo de conformidad de TCG. El TPM debe cumplir los requisitos y superar las evaluaciones que realice el Grupo de trabajo. Igualmente, el TPM puede ser sometido a pruebas y evaluaciones más exigentes.</p>	[b-TPM]

**Cuadro I.5 – Técnicas relevantes de la agrupación de garantía de identidad**

Técnica	Descripción	Referencias
<p><b>Conexión de red fiable</b></p>	<p>Las operaciones de seguridad de las TIC a menudo tienen por objeto detectar la situación del sistema operativo y del software de aplicación utilizado por la red utilizada. Por ejemplo, cuando un sistema carece de parches de seguridad o antivirus, es esencial una notificación fiable para limitar el daño por ataques realizados desde la red. Para poder realizar este análisis es necesario contar con información fiable sobre el estado en que se encuentra un sistema conectado.</p> <p>Para proteger los sistemas (por ejemplo, sistemas pirateados) de información falsa, una evaluación exitosa requiere que el hardware del sistema a evaluar cumpla unas premisas básicas. Las plataformas fiables (<i>trusted platforms</i>) están integradas en el hardware para registrar sucesos del proceso de arranque y distribuirlos digitalmente. Además, la mayor parte de los fabricantes de chips complementan actualmente las plataformas fiables con una capacidad de "arranque tardío" que permite la ejecución de código confiable al final de la secuencia de arranque. Ello, a su vez, permite registrar con fiabilidad eventos después del proceso de arranque del hardware.</p> <p>La gestión de la configuración de la red constituye un despliegue efectivo de elementos de control del sistema: agentes software en máquinas de la empresa que periódicamente envían informes de configuración a un repositorio central que evalúa e identifica los sistemas no conformes. Los datos de dichos agentes software, aunque de gran valor, pueden ser fácilmente modificados por un agresor. Un amplio despliegue de plataformas confiables para evaluar con fiabilidad el estado del sistema, incrementa la confianza de una empresa en sus datos de gestión de la configuración.</p> <p>La conexión de red fiable (TNC, <i>trusted network connect</i>) es una arquitectura abierta para controlar el acceso a la red. Su objetivo es proporcionar a los operadores de redes la integridad de los puntos extremos de cada conexión de red, permitiendo la interoperabilidad entre puntos extremos de red de distintos proveedores.</p>	<p>[b-TNC]</p>
<p><b>Garantía de autenticación de entidad</b></p>	<p>Esta norma proporciona un marco del ciclo de vida de la autenticación para gestionar la garantía de la identidad de una entidad y su información de identidad asociada en un contexto determinado. En concreto, proporciona métodos para:</p> <ol style="list-style-type: none"> <li>1) la medición cualitativa y asignación de niveles de garantía sobre la autenticación de las identidades de una entidad y su información de identidad asociada, y</li> <li>2) comunicar niveles relativos de garantía de autenticación.</li> </ol>	<p>[b-NIST EAA]</p>

**Cuadro I.5 – Técnicas relevantes de la agrupación de garantía de identidad**

<b>Técnica</b>	<b>Descripción</b>	<b>Referencias</b>
<b>Marco del Certificado de validación ampliada</b>	El marco del certificado de validación extendida consta de una combinación integrada de tecnologías, protocolos, verificación de identidad, gestión del ciclo de vida y prácticas de auditoria que constituyen los requisitos mínimos necesarios para emitir y mantener certificados de validación ampliada ("Certificados EV") de una organización en particular. El marco incluye una amplia gama de requisitos de seguridad, localización y notificación.	[b-EVCERT]
<b>Requisitos de política para autoridades de certificación que emiten certificados de clave pública</b>	Este documento especifica los requisitos de la política relativa a las autoridades de certificación (AC) que emiten certificados de clave pública, incluidos certificados de validación ampliada. Define requisitos de la política relativa a prácticas de operación y gestión de autoridades de certificación que emiten y gestionan certificados de forma que los abonados, sujetos certificados por la AC y partes que utilizan la certificación puedan tener confianza en la capacidad del certificado para soportar mecanismos criptográficos.	[b-ETSI TS 102 042]

**Cuadro I.6 – Técnicas relevantes de la agrupación de protocolos de intercambio**

<b>Técnica</b>	<b>Descripción</b>	<b>Referencias</b>
<b>Defensa entre redes en tiempo real (RID)</b>	La defensa entre redes en tiempo real (RID) ofrece un marco para el intercambio de información de incidentes. La norma RID estipula el conjunto de mensajes de coordinación de incidentes necesarios para comunicar de manera segura documentos IODEF entre entidades. RID sirve de envoltorio a los documentos IODEF, incluidas todas sus extensiones. Los mensajes normalizados y los formatos de intercambio comprenden opciones/consideraciones de seguridad, privacidad y política, necesarias dentro de un esquema global de coordinación de incidentes. RID es la capa de seguridad entre los documentos IODEF y el protocolo de transporte. Las entidades que comunican la información de incidentes deciden el tipo de transporte seleccionado, que puede ser el transporte RID especificado (HTTP/TLS), BEEP, SOAP o un protocolo que se defina en el futuro.	[b-IETF RFC 6045]
<b>Transporte de mensajes de Defensa entre redes en tiempo real (RID)</b>	Este mecanismo especifica el transporte de mensajes de defensa entre redes en tiempo real (mensajes RID) en mensajes HTTP Request y HTTP Response transportados sobre TLS.	[b-IETF RFC 6046]

**Cuadro I.6 – Técnicas relevantes de la agrupación de protocolos de intercambio**

Técnica	Descripción	Referencias
<p><b>Perfil para CYBEX del protocolo extensible de intercambio de bloques (BEEP)</b></p>	<p>Un perfil BEEP para Técnicas de intercambio de información de ciberseguridad especifica el perfil BEEP a utilizar en el CYBEX. BEEP es un kernel o núcleo de un protocolo de aplicación para interacciones asíncronas con conexión descrito en la [b-IETF RFC 3080]. Un núcleo BEEP es un mecanismo que permite el intercambio independiente y simultáneo de mensajes entre pares. Todos los intercambios se producen en el contexto de un canal (un vínculo o conexión con un aspecto bien definido de la aplicación, tal como la seguridad del transporte, la autenticación de usuario o el intercambio de datos). Cada canal tiene un "perfil" asociado que define la sintaxis y la semántica de los mensajes intercambiados.</p>	<p>[b-IETF RFC 3080]</p>
<p><b>Protocolo simple de acceso a objetos (SOAP) para CYBEX</b></p>	<p>SOAP es un protocolo ligero para el intercambio de información en un entorno descentralizado y distribuido. Está basado en XML y consta de tres partes: una envoltura que define un marco para describir el contenido de un mensaje y cómo procesarlo; un conjunto de reglas de codificación para expresar instancias de tipos de datos definidos para una aplicación; y un convenio para representar un procedimiento a distancia de llamadas y respuestas. Potencialmente SOAP puede utilizarse combinado con una gran variedad de protocolos, sin embargo los únicos vínculos definidos en este documento describen cómo utilizar SOAP con HTTP y con el marco de extensión de HTTP.</p>	<p>[b-W3C SOAP]</p>

## Apéndice II

### Ontología del intercambio de información de ciberseguridad

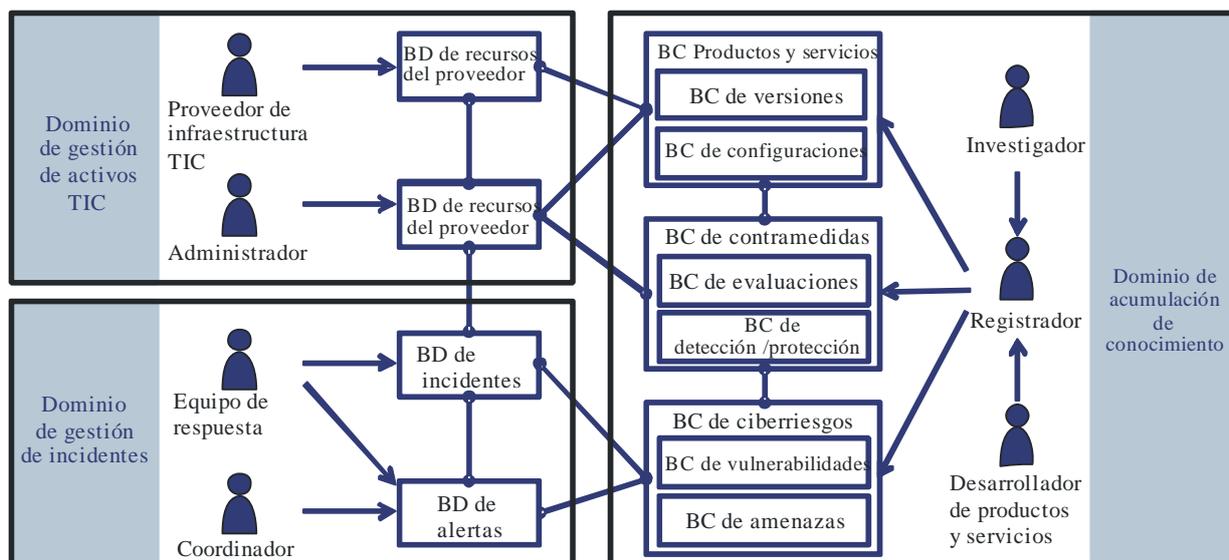
(Este apéndice no forma parte integrante de esta Recomendación)

El apéndice II presenta una ontología o descripción de las propiedades esenciales del intercambio de información de ciberseguridad. Ilustra un contexto operacional de CYBEX y ofrece un ecosistema de ciberseguridad efectivo en el que el conocimiento obtenido a través de informes, pruebas y experiencias se utiliza para crear y evolucionar la información sobre debilidades y vulnerabilidades que puede utilizarse junto con información sobre el estado del sistema a fin de medir y mejorar su seguridad.

La ontología CYBEX define los siguientes términos:

- 1) **Operaciones de ciberseguridad:** métodos y procesos para la supervisión y gestión de la seguridad en límites operacionales definidos, incluyendo:
  - recopilación y análisis de información que puede tener impacto en la seguridad;
  - detección de comportamientos o eventos que afecten negativamente a la seguridad o que permitan determinar la probabilidad de futuros impactos adversos;
  - actuaciones tomadas como consecuencia de un comportamiento o evento adverso destinadas a limitar, mitigar y/o prevenir incidentes futuros;
  - comunicaciones relacionadas con la seguridad y relativas al estado y condiciones del sistema.
- 2) **Entidad de ciberseguridad:** cualquier entidad que participe en un intercambio de información de ciberseguridad, incluida la información del propio objeto.
- 3) **Información operacional de ciberseguridad:** cualquier información necesaria para que entidades de ciberseguridad ejecuten operaciones de ciberseguridad.

En esta ontología del CYBEX se describen con más detalle técnicas de seguridad del mismo, es decir, es un modelo que describe el mundo abstracto de las operaciones de ciberseguridad. La ontología consta de un conjunto de tipos, propiedades y relaciones (véase la figura II.1). Las líneas continuas indican las relaciones entre tipos de información y las flechas indican las entradas de información desde una entidad funcional a una base de datos o a una base de conocimiento. Las entidades funcionales que se muestran a la derecha son genéricas y las entidades como los CIRT pueden abarcar una o más de dichas funciones.



BD Base de datos  
BC Base de conocimiento

X.1500(11)\_FIL-01

**Figura II.1 – Modelo de la ontología de CYBEX**

En esta ontología se utiliza un modelo para definir dominios de operaciones de ciberseguridad que, a su vez, se utiliza para identificar las entidades de ciberseguridad necesarias para las operaciones en cada dominio. En los apartados siguientes se describe en detalle la ontología y se ilustra cómo pueden utilizarse las técnicas CYBEX para soportar dicha ontología.

## II.1 Dominios de operación

Las operaciones de ciberseguridad constan básicamente de tres dominios: gestión de incidentes, gestión de activos tic y acumulación de conocimiento.

El dominio de gestión de incidentes abarca la detección y respuesta a incidentes de ciberseguridad mediante la supervisión de incidentes, de eventos informáticos que constituyen los incidentes y de comportamientos típicos de ataque identificados en los incidentes. Por ejemplo, detecta anomalías mediante alarmas de detectores y agrega información detallada mediante la recopilación de registros de acceso. En ocasiones también proporciona alertas y avisos, por ejemplo, alertas tempranas por posibles amenazas a organizaciones de usuarios.

El dominio de gestión de activos TIC abarca operaciones de ciberseguridad en cada organización de usuario, como la instalación, configuración y gestión de activos TIC en la organización. Incluye operaciones de prevención de incidentes y operaciones de control de daños en cada organización.

El dominio de acumulación de conocimiento incluye información sobre ciberseguridad. Permite generar y acumular conocimiento reutilizable por otras organizaciones.

## II.2 Entidades de ciberseguridad

En base a los dominios de operación descritos, pueden identificarse las entidades funcionales de ciberseguridad necesarias para la realización de las operaciones de ciberseguridad en cada dominio.

En el dominio de gestión de incidentes existen dos entidades operativas: el equipo de respuesta y el coordinador. El equipo de respuesta es una entidad que supervisa y analiza diversos tipos de incidentes, por ejemplo, accesos no autorizados, ataques DDoS y suplantación de identidad, y acumula la información de los incidentes. En base a dicha información, un Equipo de respuesta puede adoptar contramedidas, por ejemplo, registrar en listas negras las direcciones de los sitios desde los que se realiza la suplantación de identidad. Un Coordinador es la entidad que realiza la

coordinación con otras entidades y aborda amenazas potenciales en base a información de incidentes conocidos.

En el dominio de gestión de activos TIC existen dos entidades operativas: el administrador y el proveedor de infraestructuras TIC. El administrador administra los sistemas de su organización y posee información de sus propios activos TIC. Un administrador es una instancia típica en una organización. El proveedor de infraestructuras TIC proporciona las infraestructuras TIC que precisa la organización, incluyendo la conectividad de red, los servicios de computación en la nube, tales como los denominados software como servicio (SaaS), plataforma como servicio (PaaS) e infraestructura como servicio (IaaS) e identifica servicios. Un proveedor de servicios de Internet (ISP) y un proveedor de servicios de aplicaciones (ASP) son instancias típicas.

En el dominio de acumulación de conocimiento existen tres entidades operativas: investigador, desarrollador de productos y servicios y registrador. Un investigador investiga información de ciberseguridad, extrayendo y acumulando conocimiento. Un desarrollador de productos y servicios posee información de productos y servicios, por ejemplo, denominaciones, versiones, vulnerabilidades, parches e información de configuración. Los vendedores de software, los ASP y los programadores individuales de software son instancias típicas. Un registrador es la entidad que clasifica y organiza el conocimiento sobre ciberseguridad que proporcionan los investigadores, desarrolladores y vendedores, de forma que el mismo pueda ser utilizado por otras organizaciones.

### **II.3 Información operacional de ciberseguridad**

En este apartado se describe, en base a los dominios y entidades operativas, la información operacional de ciberseguridad que proporcionan las entidades funcionales para cada dominio operativo.

#### **II.3.1 Dominio de gestión de incidentes**

En el dominio de gestión de incidentes existe una base de datos de incidentes y una base de datos de alertas. La base de datos de incidentes contiene información sobre incidentes proporcionados por un equipo de respuesta. Incluye tres tipos de registros: eventos, incidentes y ataques. Un registro de eventos incluye los eventos informáticos, tales como registros de acceso de usuarios a un sistema. También incluye información sobre paquetes, ficheros y transacciones relacionadas con los incidentes. Normalmente, la mayoría de los registros son proporcionados automáticamente por los sistemas informáticos. Un registro de incidentes incluye eventos candidatos a ser considerados como incidentes. Este registro normalmente se obtiene de varios registros de eventos y sus conjeturas, creados de forma automática y/o manual. Un registro de ataques se basa en el análisis de incidentes e incluye la fecha y hora exacta de los ataques así como su secuencia.

La base de datos de alertas incluye información de alertas de ciberseguridad proporcionadas por un equipo de respuesta y un coordinador. Las alertas se basan en la base de datos de incidentes así como en la base de conocimiento de ciberriesgos.

#### **II.3.2 ICT Dominio de gestión de activos**

En el dominio de gestión de activos TIC existen dos bases de datos: la base de datos de recursos de usuarios y la base de datos de recursos de proveedores.

La base de datos de recursos de usuarios agrega información sobre activos de una organización determinada e incluye información tal como la lista de software, el hardware, sus configuraciones, estado de uso de los recursos, política de seguridad, incluyendo políticas de control de acceso, resultados de evaluaciones del nivel de seguridad y topología de la intranet. El administrador proporciona la información.

La base de datos de recursos de proveedores agrega información sobre activos ajenos a la organización. Esencialmente contiene información de recursos y redes externas. La información de recursos externos consta de información sobre recursos ajenos utilizados por una organización, tales como la lista y estado de los servicios en la nube (por ejemplo, centros de datos y SaaS). La información de redes externas incluye información de las redes que conectan entre sí organizaciones, como topología, información de encaminamiento, política de control de acceso, estado del tráfico y nivel de seguridad. El proveedor de infraestructura TIC proporciona la información.

### **II.3.3 Dominio de acumulación de conocimiento**

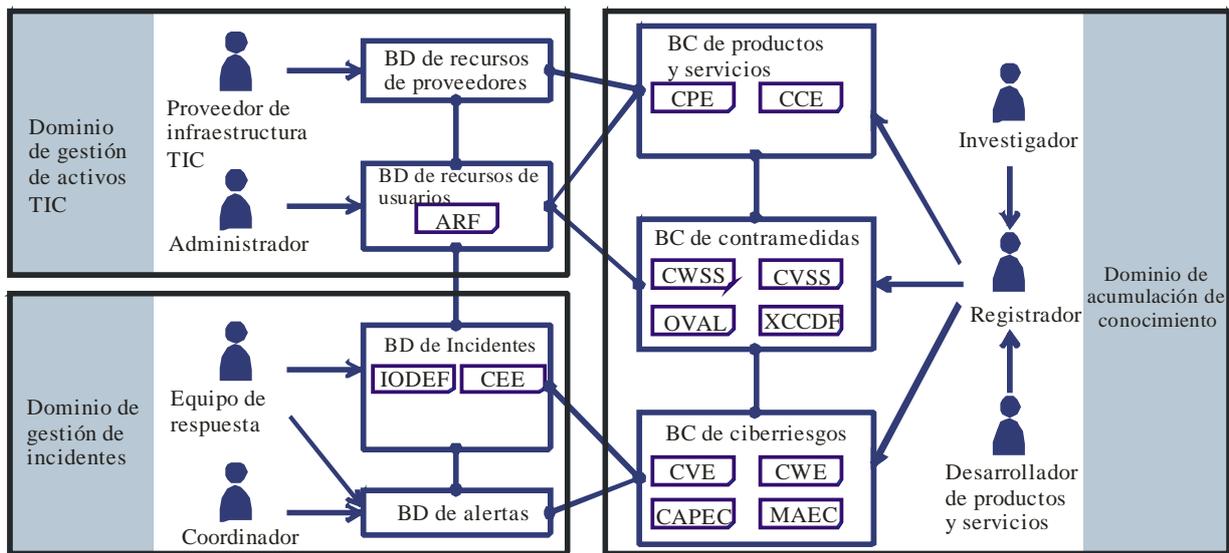
El dominio de acumulación de conocimiento dispone de tres bases de conocimiento: ciberriesgos, contramedidas y productos y servicios. Agregan el conocimiento sobre ciberseguridad que proporcionan el investigador y el desarrollador de productos y servicios, y que el registrador ordena y clasifica.

La base de conocimiento de ciberriesgos agrega información de riesgos de ciberseguridad e incluye conocimiento de vulnerabilidades y conocimiento de amenazas. La base de conocimiento de vulnerabilidades agrega información de vulnerabilidades, incluyendo denominación, taxonomía y enumeración de vulnerabilidades conocidas. También incluye vulnerabilidades humanas que generan los usuarios de las TIC. La base de conocimiento de amenazas agrega información de amenazas conocidas que incluyen ataques y de usos indebidos. El conocimiento de los ataques incluye información sobre patrones de ataques, herramientas de ataque (por ejemplo, software maligno) y sus tendencias, tales como información sobre el ámbito geográfico y el objetivo de ataques previos. También incluye información estadística sobre ataques anteriores. El conocimiento del uso indebido incluye información sobre usos indebidos de las TIC por el ser humano sin intención maliciosa. Ello incluye errores en la escritura, obtenida a través de trampas de suplantación de identidad, y violaciones de la conformidad.

La base de conocimiento de contramedidas agrega información sobre contramedidas frente a riesgos de la ciberseguridad y contiene dos bases de conocimiento: evaluación y detección/protección. La base de conocimiento de evaluación agrega reglas y criterios conocidos para evaluar el nivel de seguridad de activos TIC, así como la lista de verificación de configuraciones. La base de conocimiento de detección/protección agrega conocimiento sobre reglas y criterios para la detección/protección frente a amenazas de seguridad, por ejemplo, firmas IDS/IPS y reglas de detección/protección conexas.

La base de conocimiento de productos y servicios acumula información sobre productos y servicios. Incluye dos bases de conocimiento: conocimiento de versión y conocimiento de configuración. La base de conocimiento de versión agrega información de las versiones de los productos y servicios, incluyendo denominación y enumeración de versiones. En relación con la versión del producto, los parches de seguridad también están incluidos en esta base de conocimiento. La base de conocimiento de configuración agrega información de configuración de productos y servicios. En relación con la configuración de productos, incluye la denominación, taxonomía y enumeración de las configuraciones conocidas.

Cada una de las bases de datos y bases de conocimiento mencionadas pueden utilizar diversas técnicas de descripción de la información, tal como se muestra en la figura II.2.



BD Base de datos  
 BC Base de conocimientos

X.1500(11)\_FI-02

**Figura II.2 – Representación detallada del modelo de ontología CYBEX y sus técnicas**

Para más información sobre la ontología CYBEX, véase la Referencia [b-Takahashi].

## Apéndice III

### Ejemplos de esquemas de automatización de la seguridad mediante CYBEX

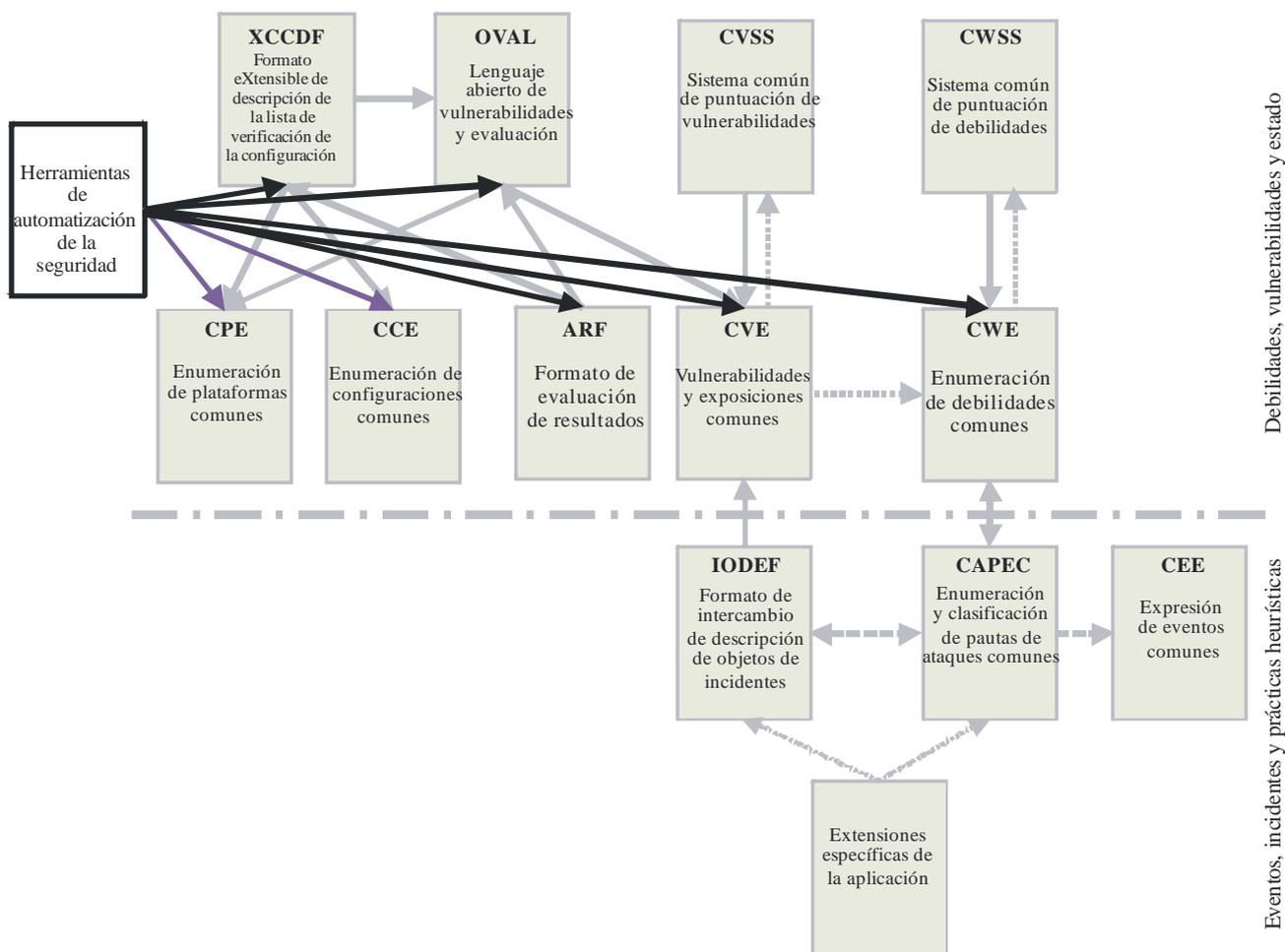
(Este apéndice no forma parte integrante de la presente Recomendación)

El apéndice III proporciona dos ejemplos de esquemas de automatización de la seguridad. Dichas capacidades pueden utilizarse para crear instancias específicas de CYBEX que incluyan la automatización de "estados" conocidos o fiables de software, servicios y sistemas, detección de software maligno, captura de incidentes e información derivada de la experiencia.

Es previsible que surjan gran número de implementaciones, particularmente esquemas de automatización de la seguridad para garantizar que los sistemas TIC estén adecuadamente configurados y cuenten con los parches adecuados. Dos de los ejemplos más destacados son los siguientes:

- 1) El protocolo para la automatización de contenidos de seguridad (SCAP) del Instituto Nacional de Normalización y Tecnología (NIST) de los Estados Unidos de América para la implementación de la *Federal Desktop Core Configuration* (FDCC) y su sustituto la *United States Government Configuration Baseline* (USGCB).
- 2) El marco de automatización de contenidos de seguridad JVN de Japón (*Japan JVN Security Content Automation Framework*).

En este apéndice se describe brevemente ambos ejemplos. En general, dichas implementaciones de herramientas de automatización de la seguridad adoptan la forma que se muestra en la figura III.1 e incluyen un conjunto de plataformas de intercambio de información CYBEX representadas por los punteros solapados del diagrama.



X.1500(11)\_FIII-01

**Figura III.1 – Garantía y automatización de la integridad de la ciberseguridad**

### III.1 Ejemplo: USA Federal Desktop Core Configuration/United States Government Configuration Baseline

La Federal Desktop Core Configuration (FDCC) y sus sustituto la United States Government Configuration Baseline (USGCB), utiliza el protocolo de automatización de contenidos de seguridad (SCAP, *security content automation protocol*) del NIST e incluye las especificaciones para organizar y expresar la información sobre seguridad de varias formas normalizadas, así como datos de referencia conexos tales como identificadores únicos de vulnerabilidades. El objetivo de estas dos iniciativas es crear configuraciones de referencia para productos TIC ampliamente desplegados por las agencias federales del gobierno. La configuración de referencia USGCB ha evolucionado a partir del mandato emanado de la Federal Desktop Core Configuration. La USGCB es una iniciativa del gobierno Federal que proporciona directrices a las agencias sobre lo que deben hacer para mejorar y mantener configuraciones efectivas desde el punto de vista de la seguridad.

La especificación técnica USGCB describe los requisitos y convenios que deben utilizarse para asegurar un intercambio consistente y exacto del contenido de SCAP, así como la capacidad del contenido para utilizar de forma fiable las herramientas validadas por la SCAP. La versión inicial se compone de seis especificaciones: XCCDF, OVAL, CPE, CCE, CVE y CVSS. Estas especificaciones se agrupan en tres categorías: lenguajes, enumeraciones, y sistemas de medición y puntuación de vulnerabilidades.

El protocolo SCAP implementa 1) un formato y nomenclatura especificados que permiten a los productos de seguridad la comunicación de errores de software y configuraciones de seguridad, y 2) errores del software y datos de referencia normalizados de configuraciones de seguridad conocidos como contenido SCAP. Los objetivos del protocolo SCAP incluyen la normalización de la gestión de la seguridad de los sistemas, la promoción de la interoperabilidad entre productos de seguridad y el impulso de la utilización de expresiones normalizadas de contenidos de seguridad. El etiquetado estructurado, el descubrimiento y la verificación de garantías de los actuales esquemas son requisitos importantes a la luz de la previsible aparición de numerosos contenidos de SCAP para distintos sistemas y niveles de seguridad. La iniciativa USGCB crea contenidos y directrices basadas en las especificaciones SCAP.

### III.2 Ejemplo: Japan Vulnerability Information Portal Site, JVN

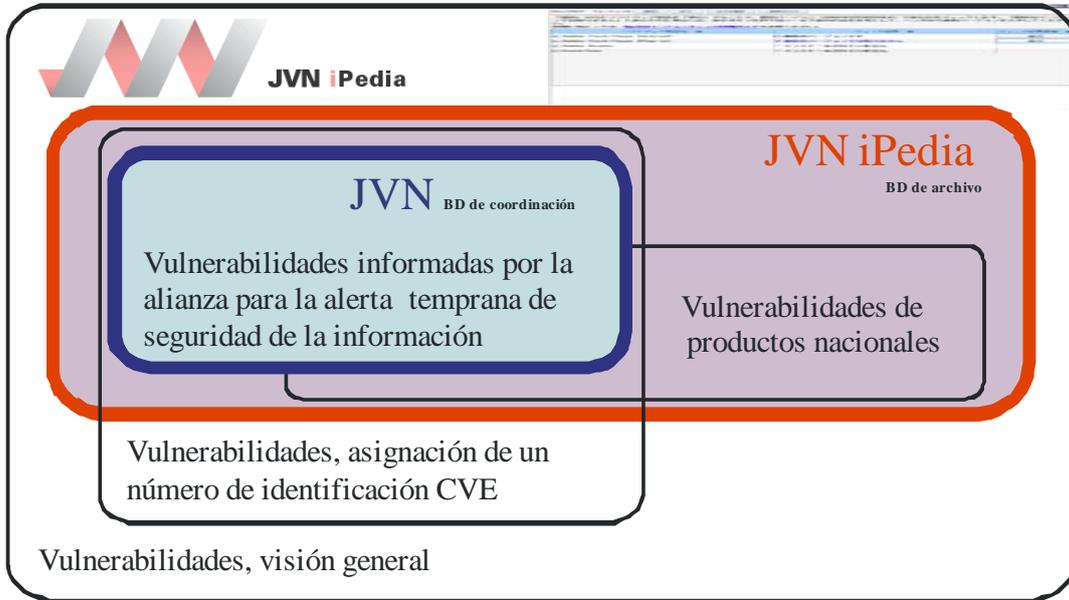
El término JVN, que significa "*Japan Vulnerability Notes*", y es una herramienta que proporciona información sobre vulnerabilidades y aspectos conexos del software utilizado en Japón, siendo su objetivo contribuir a la creación de contramedidas frente a ciberamenazas. Para permitir que los desarrolladores de aplicaciones utilicen datos a través de una interfaz normalizada, la JVN ha adoptado el SCAP y contiene información local (nacional) e internacional que conjuntamente constituyen el marco de automatización de contenidos de seguridad JVN (*JVN security content automation framework*). Al igual que la base de datos nacional de vulnerabilidades (NVD, *national vulnerability database*), todas la información sobre vulnerabilidades incluye un número CVE, una puntuación CVSS y un número CWS. Además, también se suministra el nombre CPE del producto afectado.

El marco consta de tres componentes, MyJVN, JVN y JVN iPedia (véase la figura III.2), cada uno de los cuales se explica a continuación:

MyJVN proporciona información de contramedidas frente a vulnerabilidades mediante un API MyJVN, una interfaz legible por máquina incluyendo APIs Web y herramientas MyJVN tales como el verificador de versiones (*version checker*). Mejora la utilización de información de contramedidas frente a vulnerabilidades almacenada en JVN y JVM iPedia al hacer más fácil y eficiente para los usuarios recopilar información de su interés mediante servicios tales como el filtrado a medida, la auto búsqueda y la creación de listas de verificación. Asimismo, el "MyJVN Version Checker", que es una herramienta basada en SCAP, permite a cualquier persona verificar fácilmente si el software instalado en su PC es la última versión.

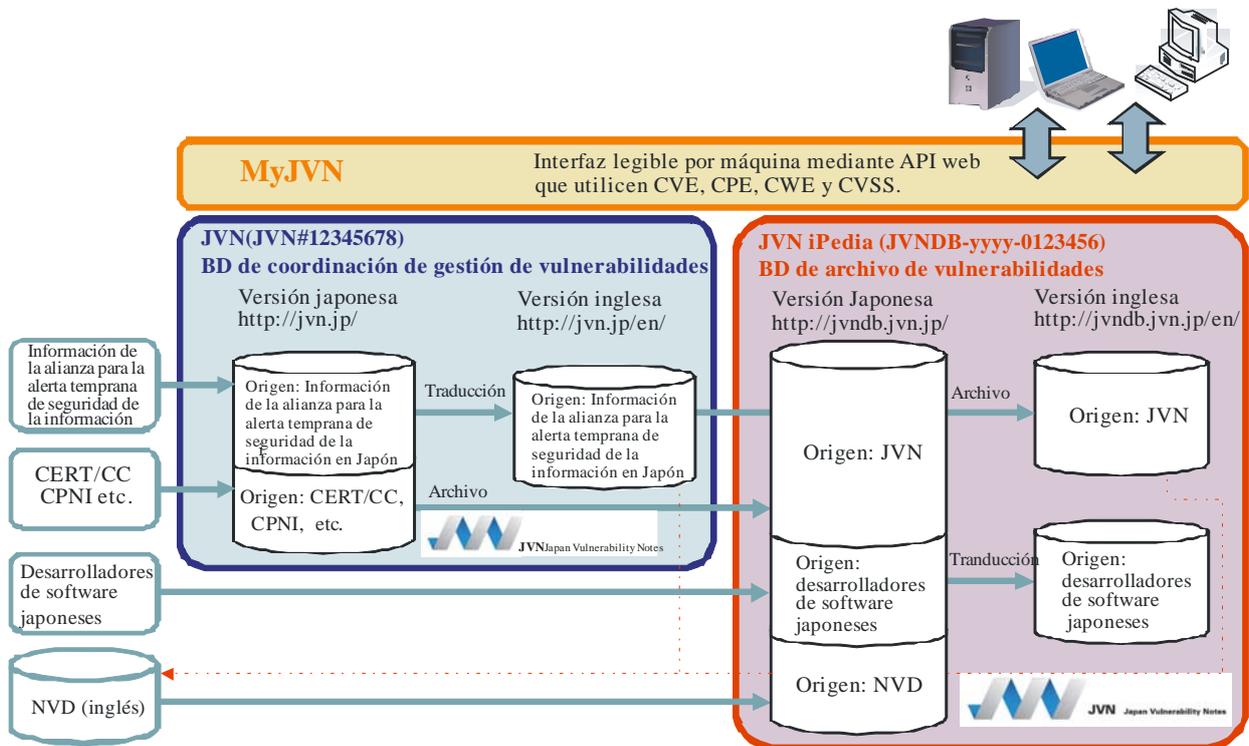
JVN proporciona información de contramedidas frente a vulnerabilidades y la situación en que se encuentran los suministradores japoneses en relación con vulnerabilidades reportadas a través de la Alianza para la alerta temprana de seguridad de la información ("*information security early warning partnership*") que es una alianza público-privada establecida para promover la seguridad de productos software y sitios web y prevenir que la acción dañina se extienda a una amplia gama de computadoras mediante virus o accesos no autorizados. Cuando la IPA (Agencia de promoción de la tecnología de la información de Japón), en su papel de entidad depositaria de dicha alianza, es informada de una vulnerabilidad, ésta se pasa al JPCERT/CC, que es el órgano coordinador. El JPCERT/CC especifica los productos de software afectados y coordina a los desarrolladores. Cuando existen soluciones a vulnerabilidades tales como parches o actualizaciones software, la información detallada de la vulnerabilidad se publica en la JVN.

La JVN iPedia proporciona información sobre contramedidas de vulnerabilidades para productos software, como sistemas operativos, aplicaciones, bibliotecas y sistemas integrados utilizados en Japón. La JVN tiene por objeto ofrecer al público información de vulnerabilidades y contramedidas tan pronto como sea posible. Un órgano de coordinación interactúa con los vendedores en relación con la detección de nuevas vulnerabilidades. Por su parte, la misión de la JVN iPedia es recopilar información adicional de vulnerabilidades y contramedidas que se detectan a diario en los productos de software japoneses y que se publican en la JVN.



X.1500(11)\_FIII-02

**Figura III.2 – Estructura conceptual del marco de automatización de contenidos de seguridad de la JVN**



X.1500(11)\_FIII-03

**Figura III.3 – Base de datos con información local e Internacional**

Los usuarios que adoptan formatos normalizados, tales como RSS, disponen de una base de datos con información internacional y local (véase la figura III.3). Entre los tres componentes, el MyJVN actúa como interfaz de usuario cuya usabilidad es posible gracias a las herramientas y APIs descritas en el apartado siguiente.

### **Herramientas MyJVN y API**

MyJVN es un conjunto de herramientas de seguridad basadas en el protocolo SCAP que mejoran la utilización de contramedidas frente a vulnerabilidades y el entorno de intercambio de información de los usuarios. Actualmente, las principales herramientas ofrecidas son las siguientes:

- **Herramienta de información de filtrado de contramedidas frente a vulnerabilidades** – Esta herramienta mejora la utilización de la información de contramedidas frente a vulnerabilidades almacenadas en la JVN y la JVN iPedia al permitir que los usuarios puedan recuperar más fácil y eficientemente información de interés mediante servicios como el filtrado a medida utilizando el CPE.
- **Verificador de versión** – Es un sistema de exploración en línea basado en OVAL que permite a una persona verificar fácilmente si el software instalado en sus PC es la última versión. Con un solo clic del ratón es posible verificar las versiones de un conjunto de programas informáticos. Los resultados son fácilmente comprensibles: una marca significa que se trata de la versión más reciente y una cruz significa una versión obsoleta. Si el software no es la última versión, los usuarios pueden acceder fácilmente con unos pocos clics al sitio web de descargas del suministrador. El Verificador de versión de MyJVN soporta productos software relacionados con Internet gracias a la colaboración de los vendedores de software.
- **Verificador de configuración de seguridad de MyJVN** – Se trata de un sistema de exploración en línea basado en XCCDF y OVAL. Es una herramienta gratuita y fácil de usar para la evaluación de la configuración de seguridad de Windows, e incluye políticas tales como longitud mínima de contraseña, periodo de expiración de la contraseña, activación automática de salvapantallas, arranque automático de dispositivo USB, etc.
- **API de MyJVN** – Es una interfaz software que permite acceder y utilizar información de contramedidas frente a vulnerabilidades almacenadas en JVN y JVN iPedia. Para que los desarrolladores de aplicaciones puedan utilizar datos a través de una interfaz abierta, la JVN iPedia ha adoptado SCAP, un conjunto de normas para describir la información de contramedidas frente a vulnerabilidades. La utilización del API de MyJVN permite a cualquier aplicación a medida acceder a los datos de la JVN iPedia, siendo actualmente varios los servicios de gestión de vulnerabilidades que utilizan eficientemente la información de contramedidas frente a vulnerabilidades.

Las funciones básicas del API de MyJVN son un API del servicio de información filtrada y un API del servicio de colaboración SCAP. El primer API soporta las opciones "Get list of products" (Obtener lista de productos), "Get list of vulnerability overviews" (Obtener lista de análisis general de vulnerabilidades) etc., utilizadas por la Herramienta de información filtrada de contramedidas frente a vulnerabilidades. La segunda API soporta "Get list of OVAL definitions" (obtener lista de definiciones OVAL), "Get data of OVAL definition" (obtener datos de la definición OVAL) etc., utilizadas por el Verificador de versiones de MyJVN y el Verificador de configuración de seguridad de MyJVN.

Para más información sobre la JVN véase el artículo de referencia [b-Terada].

## Bibliografía

- [b-UIT-T E.409] Recomendación UIT-T E.409 (2004), *Estructura para organizar los incidentes y solucionar los incidentes de seguridad: Directrices para las organizaciones de telecomunicaciones.*
- [b-UIT-T X.800] Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT.*
- [b-UIT-T X.1205] Recomendación UIT-T X.1205 (2008), *Aspectos generales de la ciberseguridad.*
- [b-UIT-T X.1520] Recomendación UIT-T X.1520 (2011), *Vulnerabilidades y exposiciones comunes.*
- [b-UIT-T X.1521] Recomendación UIT-T X.1521 (2011), *Sistema común de puntuación de vulnerabilidades.*
- [b-ETSI TS 102 042] ETSI TS 102 042 (2011), *Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.*
- [b-IETF RFC 3080] IETF RFC 3080 (2001), *The Blocks Extensible Exchange Protocol Core.*  
<http://datatracker.ietf.org/doc/rfc3080/>
- [b-IETF RFC 5070] IETF RFC 5070 (2007), *The Incident Object Description Exchange Format.*  
<http://datatracker.ietf.org/doc/rfc5070/>
- [b-IETF RFC 5901] IETF RFC 5901 (2010), *Extensions to the IODEF-Document Class for Reporting Phishing.*  
<http://datatracker.ietf.org/doc/rfc5901/>
- [b-IETF RFC 6045] IETF RFC 6045 (2010), *Real-time Inter-network Defense (RID).*  
<http://datatracker.ietf.org/doc/rfc6045/>
- [b-IETF RFC 6046] IETF RFC 6046 (2010), *Transport of Real-time Inter-network Defense (RID) Messages.*  
<http://datatracker.ietf.org/doc/rfc6046/>
- [b-ARF] Assessment Results Format.  
<https://measurablesecurity.mitre.org/incubator/arf/>
- [b-CAPEC] Common Attack Pattern Enumeration and Classification.  
<https://capec.mitre.org/>
- [b-CCE] Common Configuration Enumeration. <https://cce.mitre.org/>
- [b-CEE] Common Event Expression. <https://cee.mitre.org/>
- [b-CPE] Common Platform Enumeration. <https://cpe.mitre.org/>
- [b-CWE] Common Weakness Enumeration. <https://cwe.mitre.org/>
- [b-CWSS] Common Weakness Scoring System. <https://cwe.mitre.org/cwss/>
- [b-EVCERT] CA/Browser Forum, *Guidelines for the Issuance and Management of Extended Validation Certificates*, Ver. 1.3.
- [b-MAEC] Malware Attribute Enumeration and Characterization. <https://maec.mitre.org/>
- [b-NIST EAA] *Electronic Authentication Guideline*, NIST Special Publication 800-63 Version 1.0.2, April 2006.
- [b-OVAL] *Open Vulnerability and Assessment Language.* <https://maec.mitre.org/>

- [b-Takahashi] Takahashi, T., Kadobayashi, Y., and Fujiwara, H. (2010), *Ontological Approach toward Cybersecurity in Cloud Computing*, International Conference on Security of Information and Networks, September.
- [b-Terada] Terada, Masato, et al. (2009), *Proposal of MyJVN (Web Service APIs) for Security Information Exchange infrastructure*, 21st Annual FIRST Conference on Computer Security Incident Handling, June.  
[http://jvnrss.ise.chuo-u.ac.jp/jtg/doc/21thFirstConference\\_paper.pdf](http://jvnrss.ise.chuo-u.ac.jp/jtg/doc/21thFirstConference_paper.pdf)
- [b-TLP] *CPNI Traffic Light Protocol*. (2010), Information Sharing Levels, CPNI Information Exchange, UK, April.
- [b-TNC] Trusted Computing Group, *Trusted Network Connect*.  
Integrity Measurement Collectors – TCG Version (IF-IMC, Specification Ver. 1.2 Rev. 8, 5 Feb. 2007).  
Integrity Measurement Verifiers – TCG Version (IF-IMV Specification Ver. 1.2 Rev. 8, 5 Feb. 2007).  
Trusted Network Connect Client-Server – TCG Version (IF-TNCCS TLV Binding Specification Ver. 2.0 Rev. 16, 22 Jan. 2010).  
Trusted Network Connect Client-Server Statement of Health – TCG Version (IF-TNCCS-SOH TLV Binding Specification Ver. 2.0 Rev. 10, 23 Jan. 2008).  
Policy Enforcement Point – TCG Version (IF-PEP Protocol Bindings for RADIUS Specification Ver. 1.1 Rev. 0.7, 5 Feb. 2007).  
Binding for SOAP – TCG Version (IF-MAP Specification Ver. 2.0 Rev. 36, 30 July 2010).  
Platform Trust Services Interface – TCG Version (IF-PTS Specification Ver. 1.0 Rev. 1.0, 17 Nov. 2006).  
Clientless Endpoint Support Profile – TCG Version (CESP Specification Ver. 1.0 Rev. 13, 18 May 2009).
- [b-TPM] Trusted Computing Group, *Trusted Platform Modules*.  
Design Principles – TCG Version (TPM Main, Part 1, Specification Ver. 1.2, Level 2 Rev. 103, 9 July 2007), ISO/IEC Version (11889-2, 2009-05-15, Information technology – TPM – Part 2).  
TPM Structures – TCG Version (TPM Main, Part 2, Specification Ver. 1.2, Level 2 Rev. 103, 9 July 2007), ISO/IEC Version (11889-3, 2009-05-15, Information technology – TPM – Part 3).  
Commands – TCG Version (TPM Main, Part 3, Specification Ver. 1.2, Level 2 Rev. 103, 9 July 2007), ISO/IEC Version (11889-4, 2009-05-15, Information technology – TPM – Part 4).  
The TPM 1.2 specifications have also been adopted as ISO/IEC 11889. Overview – TCG Version (N/A), ISO/IEC Version (11889-1, 2009-05-15, Information technology – TPM – Part 1).
- [b-W3C SOAP] W3C Recommendation Simple Object Access Protocol (SOAP), 2007.  
*SOAP Version 1.2 Part 1: Messaging Framework*.  
*SOAP Version 1.2 Part 2: Adjuncts*.
- [b-XCCDF] The eXtensible Configuration Checklist Description Format.  
<http://scap.nist.gov/specifications/xccdf/>





## 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
<b>Serie X</b>	<b>Redes de datos, comunicaciones de sistemas abiertos y seguridad</b>
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