Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1570

(09/2011)

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

Intercambio de información de ciberseguridad – Identificación y descubrimiento

Mecanismos de descubrimiento en el intercambio de información de ciberseguridad

Recomendación UIT-T X.1570

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.1570

Mecanismos de descubrimiento en el intercambio de información de ciberseguridad

Resumen

En esta Recomendación se facilita un marco para el descubrimiento de información de ciberseguridad y el mecanismo que lo hace posible. El descubrimiento puede considerarse como una fase del ciclo de vida de la información de ciberseguridad adyacente a la publicación y la adquisición de información, que son fases inherentes y necesarias para el descubrimiento. De esta manera, el marco trata de la manera de publicar información de ciberseguridad, de obtener la lista de candidatos y de adquirir la información necesaria. Es posible aplicar un sistema de descubrimiento con mecanismos arbitrarios, siempre que se ajuste al marco, y entre tales mecanismos figuran el descubrimiento basado en los identificadores de objeto (OID) y el descubrimiento basado en los marcos de descripción de recursos (RDF), que también se tratan en esta Recomendación.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio
1.0	ITU-T X.1570	2011-09-02	17

Palabras clave

Descubrimiento de fuente, descubrimiento de información, información de ciberseguridad.

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

Introducción

Se le está asignando más importancia que nunca al intercambio de información de ciberseguridad, y en particular a una norma internacional para el intercambio de información de ciberseguridad denominada CYBEX. Entre las diversas especificaciones técnicas de CYBEX figura el descubrimiento CYBEX, el cual proporciona un esquema para encontrar la fuente de información de ciberseguridad, y en el presente documento se describen su marco y sus técnicas.

Recomendación UIT-T X.1570

Mecanismos de descubrimiento en el intercambio de información de ciberseguridad

1 Alcance

En esta Recomendación se facilita un marco para el descubrimiento de información de ciberseguridad y el mecanismo que lo hace posible. El descubrimiento puede considerarse como una fase del ciclo de vida de la información de ciberseguridad adyacente a la publicación y la adquisición de información, que son fases inherentes y necesarias para el descubrimiento. De esta manera, el marco trata de la manera de publicar información de ciberseguridad, de obtener la lista de candidatos y de adquirir la información necesaria. Es posible aplicar un sistema de descubrimiento con mecanismos arbitrarios, siempre que se ajusten al marco, y entre tales mecanismos figuran el descubrimiento basado en los identificadores de objeto (OID) y el descubrimiento basado en los marcos de descripción de recursos (RDF), que también se tratan en esta Recomendación.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[UIT-T X.660] Recomendación UIT-T X.660 (2011) | ISO/CEI 9834-1:2012, *Tecnología de la información – Procedimientos para el funcionamiento de las autoridades de registro de los identificadores de objeto: Procedimientos generales y arcos superiores del árbol de identificadores de objeto internacionales.*

[W3C RDF] W3C Recommendation (2004), *Resource Description Framework (RDF): Concepts and Abstract Syntax*.
<http://www.w3.org/TR/rdf-concepts/>

3 Definiciones

3.1 Términos definidos en otros documentos

En esta Recomendación se utilizan los siguientes términos definidos en otros sitios:

3.1.1 identificador de objeto [UIT-T X.660]: Lista ordenada de valores enteros primarios de la raíz del árbol de identificador de objeto internacional a un nodo, que inequívocamente identifica dicho nodo.

3.1.2 ontología [b-Gruber]: Especificación explícita de una conceptualización.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los siguientes términos:

3.2.1 información de ciberseguridad: Información estructurada o conocimiento sobre:

1) "estado" del equipo, software o sistemas sobre redes en relación con la ciberseguridad, especialmente con las vulnerabilidades;
2) análisis forense relacionado con incidentes o eventos;
3) observaciones heurísticas y firmas consecuencia de eventos experimentados;
4) entidades de ciberseguridad involucradas;
5) especificaciones para el intercambio de información de ciberseguridad, incluyendo módulos, esquemas, términos y condiciones y números asignados;
6) identidades y atributos de garantía de toda la información de ciberseguridad;
7) requisitos, directrices y aspectos prácticos de la implementación.

NOTA – Esta definición se basa en la descripción de información de seguridad que puede encontrarse en [b-UIT-T X.1500].

3.2.2 intercambio (de información de ciberseguridad): Transferencia de información de ciberseguridad entre dos o más entidades de ciberseguridad. Esta transferencia puede ser unidireccional o bidireccional, multidireccional, es decir, de muchos a muchos.

3.2.3 descubrimiento: Acto o proceso de descubrir el objetivo, es decir de tomar conocimiento del objetivo por primera vez.

3.2.4 extractor: Entidad que extrae la información de ciberseguridad.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan los siguientes acrónimos y abreviaturas:

CCE Enumeración de configuración común (*common configuration enumeration*)

CERT Equipos de intervención ante emergencias informáticas (*computer emergency response teams*)

CIRT Equipos de intervención ante incidentes informáticos (*computer incident response team*)

CPE Enumeración de plataforma común (*common platform enumeration*)

CVE Exposiciones y vulnerabilidades comunes (*common vulnerabilities and exposures*)

CVSS Sistema de puntuación de vulnerabilidades común (*common vulnerability scoring system*)

CWE Enumeración de debilidades comunes (*common weakness enumeration*)

CWSS Sistema de puntuación de debilidades comunes (*common weakness scoring system*)

CYBEX Intercambio de información de ciberseguridad (*CYBersecurity information EXchange*)

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

IODEF Formato de intercambio de descripciones de objetos de incidentes (*incident object description exchange format*)

MAEC Enumeración y caracterización de atributos de programas informáticos dañinos (*malware attribute enumeration and characterization*)

OID Identificador de objeto (*object IDentifier*)

OVAL Lenguaje abierto de vulnerabilidad y evaluación (*open vulnerability and assessment language*)

RDF Marco de descripción de recurso (*resource description framework*)

SCAP Protocolo de automatización de contenidos de seguridad (*security content automation protocol*)

SNMP Protocolo de gestión de red simple (*simple network management protocol*)

XCCDF Formato de descripción de lista de verificación de configuración extensible (*eXtensible configuration checklist description format*)

5 Convenios

Ninguno.

6 Marco para identificar y localizar la fuente de información de ciberseguridad

Diversas organizaciones dedicadas a la ciberseguridad están aplicando protocolos comunes de ciberseguridad para obtener e intercambiar información sobre el estado del sistema, su vulnerabilidad, los análisis forenses y observaciones heurísticas relacionados con incidentes en las aplicaciones operacionales. Puesto que esta información procede de muchas fuentes diferentes, los implementadores deben llegar a un acuerdo sobre la manera de identificar a las organizaciones encargadas de la ciberseguridad, las políticas para el intercambio de información y garantías, así como sobre la propia información que se intercambia o distribuye. Para abordar esta cuestión, en esta cláusula se introduce un marco encaminado a identificar y localizar la fuente de información de ciberseguridad: el marco para el descubrimiento de información de ciberseguridad.

En la obtención de información sobre ciberseguridad intervienen tres entidades: el extractor, la fuente de información y el directorio. El extractor obtiene la información enviando una solicitud, la fuente de información proporciona la información solicitada y el directorio registra los metadatos de la información procedente de la fuente de información y ayuda al extractor a encontrar la fuente de información adecuada.

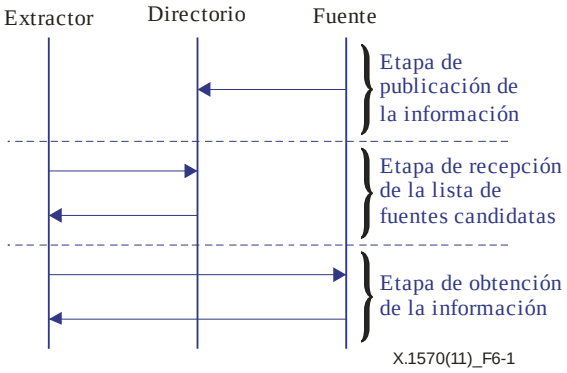
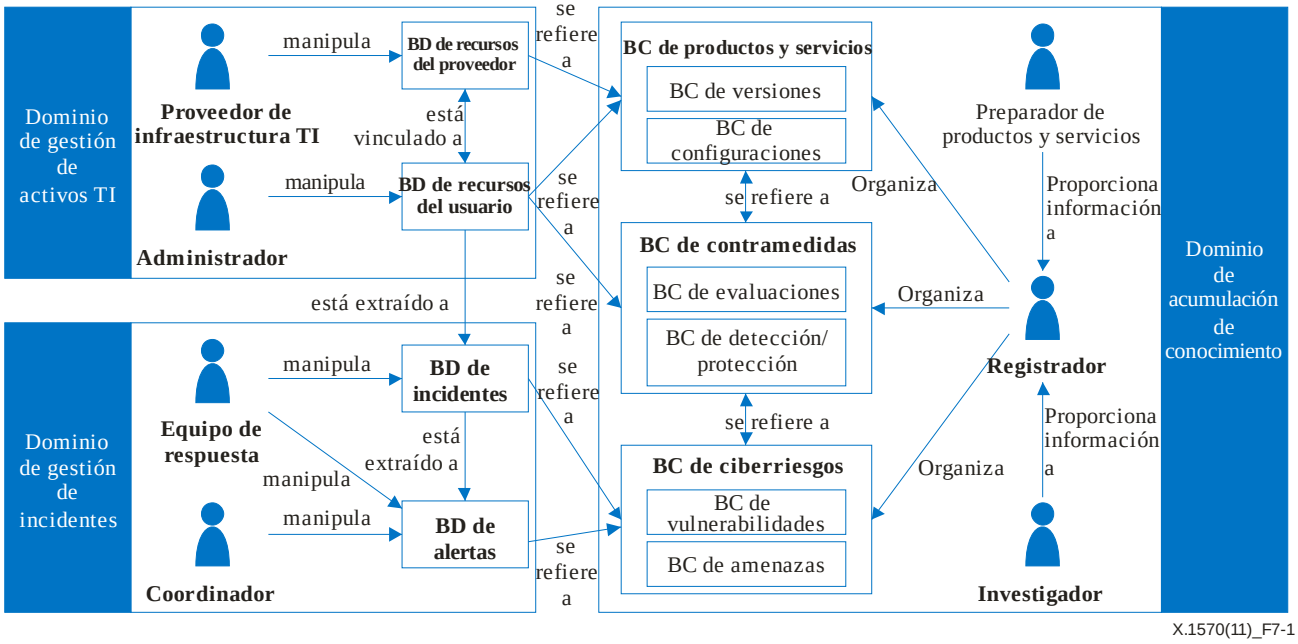


Figura 6-1 – Las tres etapas del descubrimiento

El proceso de descubrimiento es el proceso de comunicación de las tres entidades, según se describe en la figura 6-1, y consta de tres etapas: publicación de la información, recepción de la lista de fuentes candidatas y obtención de la información. La fuente publica su información para la cibersociedad registrando dicha información en el directorio en la etapa de publicación de información. El extractor solicita al directorio registrador la lista de fuentes de información candidatas en la etapa de recepción de la lista de fuentes candidatas. A continuación selecciona la fuente que le parece más adecuada y recibe la información de esa fuente en la etapa de selección de la fuente de información.

7 Tipos y grados de detalle de la información de ciberseguridad descubierta

Los mecanismos de descubrimiento son capaces de descubrir información de ciberseguridad, y están destinados a descubrir los siete tipos de información siguientes: base de datos de recursos de usuario, base de datos de recursos de proveedor, base de datos de incidentes, base de datos de alertas, base de conocimientos sobre productos y servicios, base de conocimientos sobre ciberriesgos, y base de conocimientos sobre contramedidas. En la figura 7-1 se presenta el modelo ontológico utilizado en esta Recomendación y se muestran las relaciones entre los tipos de información que se emplean en el modelo.



BD: Base de datos

BC: Base de conocimientos

Figura 7-1 – Ontología de la información de ciberseguridad operativa

Esta ontología es un modelo para describir la obtención, acumulación y utilización de conocimientos sobre información de ciberseguridad, que consiste en una serie de dominios operativos, funciones y tipos de información. Las funciones, representadas por los iconos humanos en la figura, son genéricas, y ciertas entidades tales como CIRT pueden abarcar una o más de esas funciones. Este modelo se utiliza con el fin de definir dominios para operaciones de ciberseguridad, a efectos de identificar a las entidades de ciberseguridad requeridas para soportar las operaciones en cada dominio. En el apéndice se expone detalladamente esta ontología.

En el cuadro II.1 se indican las especificaciones de ciberseguridad coherentes con los siete tipos de información descritos en este modelo ontológico. El nivel de detalle de la información sobre ciberseguridad descubierta está en consonancia con el nivel de detalle de las normas. Con este método, el nivel de detalle es flexible y, por tanto, pueden elaborarse diversas especificaciones para fines concretos.

8 Identificador de información sobre ciberseguridad

Se necesita un identificador único para identificar la información de ciberseguridad. Todo identificador único que se utilice a escala mundial para el intercambio de información global sobre ciberseguridad debe tener las siguientes características:

- simplicidad, flexibilidad, y capacidades de utilización, extensión, adaptación y despliegue;
- gestión distribuida de diversos esquemas de identificador;

- fiabilidad a largo plazo de los registradores de identificador, y disponibilidad de herramientas de gran rendimiento para descubrir la información relacionada con cualquier identificador dado.

Sólo dos candidatos de identificador único cumplen con los requisitos antes mencionados: el identificador de objeto (OID) y el marco descripción de recurso (RDF). Éstos representan los dos principales paradigmas para el descubrimiento de información y el servicio común, según se examina en la cláusula 9.

9 Tipos de mecanismos de descubrimiento

Los esquemas de descubrimiento pueden implementarse con mecanismos arbitrarios, siempre que éstos respeten el marco. Éstos se clasifican en dos tipos, centralizados y descentralizados, según su modalidad de registro y gestión de los registros de información de ciberseguridad.

Cuando se trata de mecanismos centralizados, los directorios gestionan uno o más registros "centrales", que permiten la fácil localización y el rápido descubrimiento de la información objetivo (en ciertos casos puede omitirse la etapa de recepción de lista de fuentes candidatas). No obstante, la parte que busca la información debe conocer primero la existencia de un registro dado antes de poder utilizarlo. Los diversos recursos y costos que entraña el mantenimiento de un depósito central también pueden hacer que éste resulte prohibitivo para personas con escasos recursos. Entonces el descubrimiento basado en el OID es un mecanismo típico.

Cuando se trata de mecanismos descentralizados, los directorios gestionan múltiples registros "distribuidos". En el marco de este mecanismo, los recursos y costos que exige poner a disposición la información son mínimos, y los que buscan y proporcionan información no necesitan conocer de antemano su existencia recíproca. Sin embargo, para encontrar información partiendo de un conocimiento nulo, el investigador debe arrastrarse literalmente por toda la red Internet. Entonces el descubrimiento basado en el RDF es un mecanismo típico.

9.1 Mecanismos de descubrimiento basados en el OID en el intercambio de información de ciberseguridad

Un mecanismo de descubrimiento basado en OID identifica y localiza fuentes de información de ciberseguridad utilizando OID dentro de una estructura de árbol jerárquica, donde las hojas identifican los objetos. Los OID construyen una denominación jerárquica, es decir, una concatenación de valores en arcos que van desde la raíz del árbol hasta una de sus hojas. Puede llegarse a la información de ciberseguridad registrada siguiendo el árbol desde la raíz hasta una de sus hojas. Téngase en cuenta que la información de ciberseguridad se registra en el arco identificador de objeto Intercambio de información de ciberseguridad {joint-iso-itu-t(2) cybersecurity(48)} [b-UIT-T X.1500.1].

En las cláusulas 9.1.1 a 9.1.3 se describen las etapas de descubrimiento mencionadas en la cláusula 6.

9.1.1 Etapa de publicación de información

Al registrar la información, una fuente proporciona múltiples tipos de metadatos, entre los cuales las principales categorías son: país/región, ID de la organización, tipo de información, y formato de descripción de la información. En país/región se especifica el país de la organización, o la región de la organización si la fuente es una organización transnacional como la UIT. En el ID de la organización se especifica la organización y puede describirse utilizando por ejemplo un número del tablero de cotización o un nombre empresarial único. El tipo de información especifica el tipo de información descrita en la cláusula 7. El formato de descripción de información especifica el formato, como compatible con CVE [b-ITU-T X.1520] o compatible con ARF [b-ARF].

Al recibir la solicitud de registro de la fuente de información, el directorio registra y almacena información basada en los metadatos y construye subárboles OID. Aunque en esta Recomendación no se especifica ninguna estructura normativa para el árbol, en los apéndices I y II se describen algunas posibilidades.

9.1.2 Etapa de recepción de la lista de fuentes candidatas

El extractor no envía forzosamente una petición al directorio que tiene el único registro coherente del árbol OID. Éste puede conocer la estructura del árbol de antemano, y al seguirlo puede identificar la información necesaria sin enviar una petición.

El directorio puede aceptar una petición arbitraria (incluida la de búsqueda de texto) y responder con una lista de fuentes candidatas.

9.1.3 Etapa de obtención de información

Sobre la base de la lista de fuentes candidatas o siguiendo el árbol OID desde la raíz hasta una hoja, el extractor elige una fuente y le envía una solicitud, para que ésta a su vez le proporcione información de ciberseguridad.

En el caso del descubrimiento basado en OID, podría decirse que las etapas de recepción de lista de fuentes candidatas y obtención de información son inseparables, pues la reducción de la lista de candidatos al ir siguiendo el árbol conduce a la selección de una única fuente.

9.2 Mecanismos de descubrimiento basados en el RDF para el intercambio de información sobre ciberseguridad

Un mecanismo de descubrimiento basado en RDF identifica y localiza fuentes de información de ciberseguridad basadas en el RDF. En la figura 9-1 se describe el concepto de este mecanismo. La fuente puede registrarse a sí misma en uno o más directorios (que contienen registros), lo que facilita a los extractores la obtención de información. Durante el proceso de descubrimiento, las entidades se intercambian información sobre las identidades y las capacidades de las entidades de ciberseguridad. Estas últimas envían solicitudes de descubrimiento al directorio, cada una con diferentes fuentes, que se transforman en la gama de la búsqueda para el motor de búsqueda.

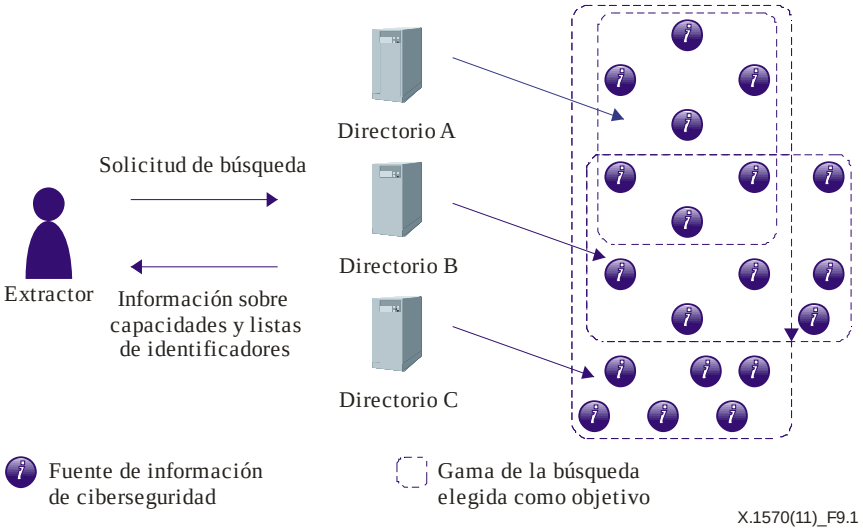


Figura 9-1 – Concepto de descubrimiento basado en el RDF

A diferencia del descubrimiento basado en el OID, el descubrimiento basado en el RDF tiene directorios que constan de múltiples entidades, según se ilustra en la figura 9-2. Desde un punto de vista funcional, un directorio consiste en un agente de descubrimiento y un agente de registro. El agente de descubrimiento se comunica con el extractor (una interfaz del receptor), y el agente de

registro se comunica con la fuente (una interfaz de la fuente). En ciertos casos ambos agentes pueden residir en una computadora. Las cuatro entidades intercambian información sobre las capacidades y los identificadores.

Las etapas del descubrimiento mencionadas en la cláusula 6 se detallan en las cláusulas 9.2.1 a 9.2.3.

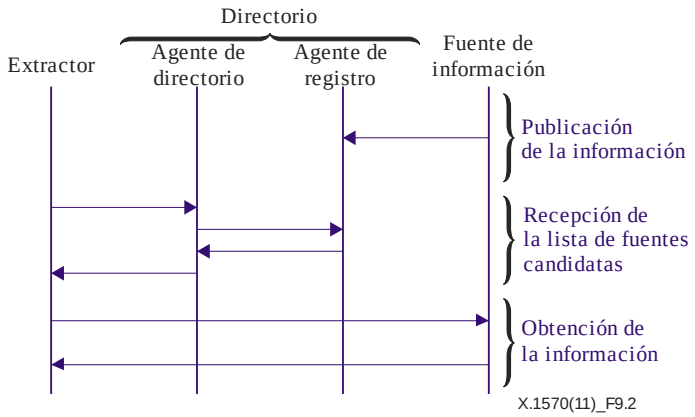


Figura 9-2 – Diagrama de secuencias del descubrimiento basado en el RDF

9.2.1 Etapa de publicación de la información

Una fuente registra su información con un agente de registro, que genera y acomoda metadatos adecuados para los datos en la etapa de publicación de información. Al igual que en el descubrimiento basado en OID, la fuente proporciona múltiples tipos de metadatos al registrar la información de ciberseguridad, entre los cuales las principales categorías son: país/región, ID de la organización, tipo de información, y formato de descripción de información. En país/región se especifica el país de la organización o su región si la fuente es una organización transnacional como la UIT. En el ID de la organización se especifica la organización y puede describirse utilizando por ejemplo un número de tablero de cotización o un nombre empresarial único. En tipo de información se especifica el tipo de información descrita en la cláusula 7. En el formato de descripción de información se especifica el formato, como compatible con CVE o compatible con ARF.

Al recibir la solicitud de registro de la fuente, el directorio registra y almacena información basada en los metadatos y actualiza la base de datos RDF. Puesto que los agentes de registro a menudo utilizan registros distribuidos jerárquicamente, el agente de registro debe identificar en qué registro deben almacenarse los datos.

Aunque en esta Recomendación no se especifica la estructura normativa del formato de metadatos RDF, en los apéndices I y II se describen algunas posibilidades.

9.2.2 Etapa de recepción de la lista de fuentes candidatas

El extractor envía consultas a un agente de descubrimiento, que las retransmite a uno o más agentes de registro adecuados, los cuales recuperan su base de metadatos y responden con una lista de fuentes candidatas en la etapa de recepción de lista de fuentes candidatas. El agente de descubrimiento agrupa la información recibida de múltiples agentes de registro y la envía al extractor.

9.2.3 Etapa de obtención de información

En esta etapa el extractor selecciona de la lista la fuente más adecuada.

10 Métodos disponibles para acceder a la información descubierta

Se puede recurrir a varios protocolos de comunicación para intercambiar información de ciberseguridad, incluidos el HTTP (que utiliza RDF) y el SNMP (que utiliza OID).

Algunos podrían querer imponer una limitación al número de partes que pueden acceder a la información descubierta, mediante la aplicación de políticas de control de acceso. Entre los principales criterios de esas políticas cabe mencionar la dirección IP, el dominio, el protocolo de comunicación, el ID y la contraseña, así como el certificado de identificación.

Toda parte que busca información sobre ciberseguridad intercambia diversos mensajes, incluidos los mensajes de solicitud. Estos métodos se describirán en la familia de Recomendaciones UIT-T X.1500.

Apéndice I

Ontología de la información de ciberseguridad operativa

(Este apéndice no es una parte integrante de la presente Recomendación)

En la cláusula 7 de la presente Recomendación se utiliza una ontología de la información de ciberseguridad operativa, que se muestra en la figura 7-1. A continuación se detalla esa ontología.

La ontología está formada por dominios de operación de ciberseguridad, las funciones necesarias para efectuar las operaciones en los dominios, y la información de ciberseguridad asociada con las funciones. Todos estos conceptos se exponen detalladamente a continuación.

I.1 Dominios de operación de ciberseguridad

El término "operación de ciberseguridad" abarca una serie de operaciones de seguridad en la cibersociedad, pero esta ontología se centra en las operaciones de ciberseguridad que preservan la información de seguridad en la cibersociedad. La seguridad de la información es la preservación de la confidencialidad, la integridad y la disponibilidad de la información, y en ocasiones comprende también la responsabilidad, la autenticidad y la fiabilidad de la información.

A fin de describir el dominio de tales operaciones, la ontología utiliza tres dominios de operación de ciberseguridad: gestión de activos de TI, tratamiento de incidentes y acumulación de conocimientos.

Gestión de activos de TI: Este dominio realiza las operaciones de ciberseguridad dentro de las organizaciones del cliente, por ejemplo, la instalación, la configuración y la gestión de los activos de TI, y comprende tanto la prevención de incidentes como las operaciones de control de daños. Los activos de TI no son sólo los activos de TI propios del usuario, sino también la conectividad de la red, los servicios en nube y los servicios de identidad facilitados por entidades externas al usuario.

Tratamiento de incidentes: Este dominio detecta y responde a los incidentes acaecidos en la cibersociedad mediante la supervisión de eventos informáticos, incidentes compuestos por múltiples eventos informáticos y ataques que causan los incidentes. Más concretamente, supervisa los eventos informático y, cuando detecta una anomalía, elabora un informe de incidente. A partir de ese informe, investiga detalladamente el incidente a fin de aclarar el patrón de ataque y las contramedidas correspondientes. Basándose en el análisis del incidente, puede emitir alertas y avisos, por ejemplo, alertas tempranas contra posibles amenazas a organizaciones de usuario.

Acumulación de conocimientos: Este dominio recopila y genera información de ciberseguridad y extrae conocimiento que pueden reutilizar otras organizaciones. Para facilitar esa reutilización, dispone de una taxonomía y sistema de denominación común con los que organiza y acumula los conocimientos. Este dominio sirve de base para la colaboración mundial más allá de las fronteras de la organización.

I.2 Funciones

Tomando como base los dominios de operación de ciberseguridad definidos más arriba, en esta cláusula se identifican las funciones necesarias para realizar las operaciones de ciberseguridad en cada dominio. El dominio de gestión de activos de TI tiene un administrador y un proveedor de infraestructura de TI. El dominio de tratamiento de incidentes tiene un equipo de intervención y un coordinador. Y el dominio de acumulación de conocimientos tiene un investigador, un creador de productos y servicios y un registrador para sus operaciones. Téngase en cuenta que las funciones están definidas desde el punto de vista de su actividad, por lo que una entidad puede asumir más de una función dependiendo del contexto.

Administrador: Esta función administra el sistema de su organización y mantiene su funcionalidad. Para ello, esta función supervisa la utilización del sistema, diagnostica el sistema mediante verificaciones de integridad, analiza las vulnerabilidades, ejecuta pruebas de penetración y entonces evalúa el nivel de seguridad del sistema. Normalmente el administrador del sistema está dentro de la organización. Si la organización externaliza alguna de las operaciones mencionadas, el administrador también puede ser un proveedor de servicios de seguridad gestionado (MSSP).

Proveedor de infraestructura de TI: Esta función facilita la infraestructura de TI a una organización. La infraestructura comprende la conectividad de la red y los servicios en nube, como el software como servicio (SaaS), la plataforma como servicio (PaaS) y la infraestructura como servicio (IaaS). El proveedor de infraestructura de TI posee información sobre redes entre organizaciones, por ejemplo, información sobre la topología de red y especificaciones de los servicios en nube. Normalmente ejercen esta función los proveedores de servicios Internet (PSI), los proveedores de servicios de aplicación (PSA) y los proveedores de servicios en nube (PSN).

Equipo de intervención: Esta función supervisa y analiza los incidentes acaecidos en la cibersociedad, por ejemplo, acceso no autorizado, ataques de denegación de servicio distribuidos (DDoS) y de peska, y acumula información sobre los incidentes. A partir de esa información, puede aplicar contramedidas, por ejemplo, bloquear el tráfico y registrar las direcciones de sitios de peska en listas negras. El equipo de intervención ante incidentes suele pertenecer al MSSP.

Coordinador: Esta función establece la coordinación con otras funciones y afronta las posibles amenazas de acuerdo con la información de incidentes conocida. Emite alertas a otras organizaciones y, en ocasiones, lidera la colaboración destinada a mitigar ataques devastadores a gran escala, como los ataques DDoS. Esta función suele recaer en el Centro de Coordinación de CERT (CERT/CC), ya sea de carácter comercial o no comercial.

Investigador: Esta función investiga los problemas de ciberseguridad, incluidos los ataques y vulnerabilidades, extrae conocimientos de la investigación y la acumula. Publica gran parte de la información reutilizable a través del registrador a fin de que cada organización pueda aplicar las contramedidas necesarias. De esta función se ocupa X-force dentro de International Business Machines Corp. (IBM); el Risk Research Institute of Cyber Space (RRICS) en la Little eArth Corporation Co., Ltd. (LAC); y el McAfee Lab en McAfee Inc., por ejemplo.

Creador de productos y servicios: Esta función crea productos y servicios y acumula su información, así como sus versiones, configuraciones, vulnerabilidades y parches. Publica mucha información reutilizable a través del registrador, de manera que, al igual que ocurre con el investigador, cada organización pueda aplicar las contramedidas necesarias. Esta función recae normalmente en los fabricantes de software y los programadores de software privados.

Registrador: Esta función clasifica, organiza y acumula conocimientos en material de ciberseguridad facilitados por el investigador y el creador de productos y servicios a fin de que otras organizaciones puedan reutilizar dichos conocimientos. Entidades como NIST y la Agencia de Fomento de la Tecnología de la Información de Japón suelen asumir esta función. En algunos casos, una entidad investigadora o creadora de productos y servicios puede también ejercer de registrador y publicar la información.

I.3 Información de ciberseguridad

De acuerdo con los dominios de operación y las funciones, en esta cláusula se identifica la información de ciberseguridad necesaria para las operaciones. Habida cuenta de la información correspondiente a cada una de las funciones, en esta ontología se definen cuatro bases de datos: recursos de usuario, recursos de proveedor, incidentes y alertas; y tres bases de conocimientos: productos y servicios, contramedidas y ciberriesgos.

I.3.1 Base de datos de recursos de usuario

La base de datos de recursos de usuario acumula información sobre los activos de cada organización y contiene información, como listas de software/hardware, sus configuraciones, el estado de utilización de los recursos, las políticas de seguridad, incluidas las políticas de control de acceso, los resultados de la evaluación del nivel de seguridad y la topología de intranet. También contiene información sobre recursos externos que cada organización usuaria utiliza, como listas de servicios en nube suscritos (por ejemplo, centros de datos y SaaS) y sus registros de utilización. El administrador manipula esa información. ARF y CRF pueden utilizarse para describir los resultados de la evaluación de activos de TI, mientras que las valoraciones CVSS y CWSS sirven para determinar el nivel de seguridad del activo de TI. Las valoraciones resultan útiles al administrador a la hora de establecer prioridades en las operaciones de seguridad de activos de TI.

I.3.2 Base de datos de recursos de proveedor

La base de datos de recursos de proveedor acumula información sobre los activos exteriores a la organización. A fin de realizar eficaz y eficientemente las operaciones de ciberseguridad, la base de datos ha de estar vinculada a una base de datos de recursos de usuario, pues la línea que separa los activos de TI internos y externos es cada vez más tenue, en particular en la computación en nube. El proveedor de infraestructura de TI manipula esta información. La base de datos contiene principalmente información sobre las redes del proveedor y los servicios en nube. La información de red de proveedor, que se encuentra en las redes mediante las cuales cada organización está conectada a otras organizaciones, es la topología, la información de encaminamiento, las políticas de control de acceso, la situación del tráfico y los niveles de seguridad. La información de servicio en nube comprende la especificación del servicio, información sobre la carga de trabajo e información sobre la política de seguridad de cada servicio en nube. Téngase en cuenta que la información propia de las organizaciones usuarias, como la configuración local de cada servicio en nube, se almacena en la base de datos de recursos de usuario.

I.3.3 Base de datos de incidentes

La base de datos de incidentes contiene información sobre los incidentes y se genera a partir del análisis de la información que contiene la base de datos de recursos de usuario. El equipo de intervención manipula esta información. Esta base de datos tiene tres registros: registro de eventos, registro de incidentes y registro de ataques.

El registro de eventos contiene información sobre eventos informáticos, incluidos los acontecidos en paquetes, ficheros y sus transacciones. Normalmente las computadoras generan automáticamente la mayoría de los registros como registros cronológicos, es decir, la hora y fecha de conexión al sistema y la información terminal facilitada cuando los usuarios raíz se conectan al sistema. Estos registros pueden ser de ese tipo. CEE puede utilizarse para describir el registro.

El registro de incidentes contiene información sobre los incidentes de seguridad y facilita información, como el estado actual de los sistemas de usuario y otros riesgos. Se deriva de los análisis de varios registros de eventos y sus condiciones, que se recrean automática o manualmente. Por ejemplo, cuando se detecta un acceso excesivo a una computadora, se han de inscribir en el registro de incidentes el estado de la computadora (acceso excesivo a una computadora) y sus consecuencias previstas (denegación de servicio). La malignidad del incidente, así como la necesidad de aplicar contramedidas, pueden determinarse a partir de este registro. Téngase en cuenta que en un registro de incidentes puede haber inscritos incidentes falsos, es decir, presuntos incidentes que tras una investigación no se consideraron incidentes. Para describir el registro puede emplearse el formato de intercambio de descripciones de objetos de incidentes (IODEF).

El registro de ataques contiene información sobre ataques derivada del análisis del registro de incidentes. Se describe la secuencia del ataque, como la manera en que se inició el ataque, qué parte de los activos de TI fue objeto del ataque, y cómo se propagaron los daños causados por el ataque. Este registro debe estar vinculado al registro de incidentes.

I.3.4 Base de datos de alertas

La base de datos de alertas contiene información sobre alertas de ciberseguridad. La información está diseñada para para el público en general o para una organización concreta. La información para el público en general contiene información estadística y alertas, mientras que la destinada a una organización concreta contiene consejos de seguridad adaptados a la organización. Esta información se genera a partir de la información de la base de datos de incidentes y de la base de conocimientos de ciberriesgos. El coordinador y el equipo de intervención manipulan esta información. A partir de las alertas, las organizaciones usuarias pueden aplicar tomar medidas contra los riesgos de ciberseguridad anunciados.

I.3.5 Base de conocimientos de ciberriesgos

La base de conocimientos de ciberriesgos acumula información sobre los riesgos de ciberseguridad. El investigador y el creador de productos y servicios facilitan la información que organiza y clasifica el registrador. Esta base de conocimientos comprende las bases de conocimientos de vulnerabilidades y amenazas.

Base de conocimientos de vulnerabilidades: Esta base de conocimientos acumula información sobre las vulnerabilidades conocidas, incluida la denominación, taxonomía y enumeración de las vulnerabilidades conocidas del software y el sistema. También contiene información sobre vulnerabilidades humanas, que son aquellas a que se exponen los usuarios humanos de TI. La National Vulnerability Database (NVD) y la Open Source Vulnerability Database (OSVDB) son ejemplos de este tipo de base. CVE y CWE pueden emplearse para describir los contenidos de la base de conocimientos.

Base de conocimientos de amenazas: Esta base de conocimientos acumula información sobre las amenazas de ciberseguridad conocidas. Comprende las bases de conocimientos de ataques y de utilizaciones indebidas. La base de conocimientos de ataques acumula información sobre los ataques, como los patrones, herramientas (por ejemplo, software maligno) y tendencias. La información sobre tendencias comprende, por ejemplo, la tendencia de ataques anteriores en términos geográficos y de objetivos, e información estadística de ataques pasados Pueden utilizarse CAPEC y MAEC para describir los contenidos de la base de conocimientos.

La base de conocimientos de utilizaciones indebidas acumula información sobre las utilizaciones indebidas atribuidas a una utilización inadecuada por parte del usuario, ya sea inocua o maligna. La utilización inocua comprende los errores tipográficos, los errores de lectura por falta de atención, los errores de comprensión y ser víctima de la peska. La utilización maligna supone una infracción de la observancia y puede ser una utilización no autorizada del servicio o el acceso a material inadecuado. Téngase en cuenta que las bases de conocimientos de ataques y de utilizaciones indebidas no aparecen en la figura 7-1 para simplificar.

I.3.6 Base de conocimientos de contramedidas

La base de conocimientos de contramedidas acumula información sobre las contramedidas opuestas a los riesgos de ciberseguridad. El investigador y el creador de productos y servicios alimentan la base, que organiza y clasifica el registrador. La base de conocimientos contiene las bases de conocimientos de evaluación y de detección/protección.

Base de conocimientos de evaluación: Esta base de conocimientos acumula las reglas y criterios conocidos para evaluar el nivel de seguridad de los activos de TI, las listas de verificación de las configuraciones e información heurística, incluidas las prácticas idóneas. Las fórmulas CVSS/CWSS son dos de las prácticas idóneas para evaluar el nivel de seguridad y están incluidas en esta base de conocimientos. Por otra parte, para describir las reglas y establecer las listas de verificación se pueden utilizar XCCDF y OVAL.

Base de conocimientos de detección/protección: Esta base de conocimientos acumula las reglas y criterios conocidos para la detección de amenazas de seguridad y la protección contra las mismas. También contiene información heurística, incluidas las prácticas idóneas.

I.3.7 Base de conocimientos de productos y servicios

La base de conocimientos de productos y servicios acumula información sobre los productos y los servicios. El investigador y el creador de productos y servicios alimentan la base, que organiza y clasifica el registrador. Esta base de conocimientos contiene las bases de conocimientos de versión y de configuración.

Base de conocimientos de versión: Esta base de conocimientos acumula información sobre la versión de los productos y servicios, lo que comprende la denominación y enumeración de cada versión. En lo que respecta a los productos, también se incluyen en la base los parches de seguridad. Puede utilizarse CPE para enumerar las plataformas comunes.

Base de conocimientos de configuración: Esta base de conocimientos acumula información sobre la configuración de productos y servicios, lo que comprende la denominación, taxonomía y enumeración de las configuraciones conocidas de productos y servicios. En lo que respecta a la configuración de los servicios, también se incluyen en la base directrices de utilización de los servicios. Puede emplearse CCE para enumerar las configuraciones de productos comunes.

Puede encontrarse información suplementaria sobre esta ontología en [b-Ontology] y en el apéndice II de [b-ITU-T X.1500].

Apéndice II

Especificaciones de las bases de datos y las bases de conocimientos

(Este apéndice no es una parte integrante de la presente Recomendación)

Los siete tipos de información indicados en la cláusula 7 se describen en una serie de especificaciones de ciberseguridad, incluidas las compatibles con UIT-T X.1500 (por ejemplo, CVE e IODEF), como puede verse en el cuadro II.1. Por consiguiente, el nivel de detalle de la información de ciberseguridad descubierta se ajustará al de las especificaciones. Por consiguiente, el nivel de detalle es flexible, por lo que pueden crearse varias especificaciones para fines específicos.

Cuadro II.1 – Especificaciones que soportan la ontología

Dominios	**BC/BD**		**Especificaciones**
Gestión de activos de TI	BD recursos de usuarios		ARF, AI, valoraciones CVSS/CWSS
	BD recursos de proveedor		---
Tratamiento de incidentes	BD incidentes		CEE, IODEF
	BD alertas		IODEF
Acumulación de conocimientos	BC ciberriesgos	BC vulnerabilidades	CVE, CWE, CVRF
		BC amenazas	CAPEC, MAEC
	BC contramedidas	BC evaluación	Fórmulas CVSS/CWSS
		BC detección/protección	OVAL, XCCDF
	BC productos y servicios	BC versión	CPE
		BC configuración	CCE
BD: Base de datos. BC: Base de conocimientos.			

Apéndice III

Ejemplo de implementación de descubrimiento basado en el RDF

(Este apéndice no es una parte integrante de la presente Recomendación)

III.1 Ejemplo de implementación de descubrimiento basado en el RDF

El concepto ilustrado en la figura 9-1 puede aplicarse poniendo los agentes de descubrimiento y los agentes de registro juntos en los motores de búsqueda del RDF. Las entidades de ciberseguridad envían una solicitud de descubrimiento a un motor de búsqueda RDF, que les responde con la lista de identidades y sus capacidades. Obsérvese que cada motor de búsqueda tiene sus fuentes diferentes, lo que viene a ser su gama de búsqueda.

En un entorno práctico y para garantizar la adaptabilidad, la fuente puede registrarse y gestionarse jerárquicamente, según se ilustra en la figura III.1. La hilera 1 puede ser un motor de búsqueda RDF individual que en realidad funciona como agente de descubrimiento, la hilera 2 puede ser una entidad registrada dentro de las reglas de operación de un registro regional tal como el American Registry for Internet Numbers (ARIN), los Réseaux IP Européens (RIPE), o el Asia Pacific Network Information Centre (APNIC), y se puede introducir una mayor jerarquía dependiendo de la implementación. La fuente puede ser un CERT o cualquier otra entidad de ciberseguridad.

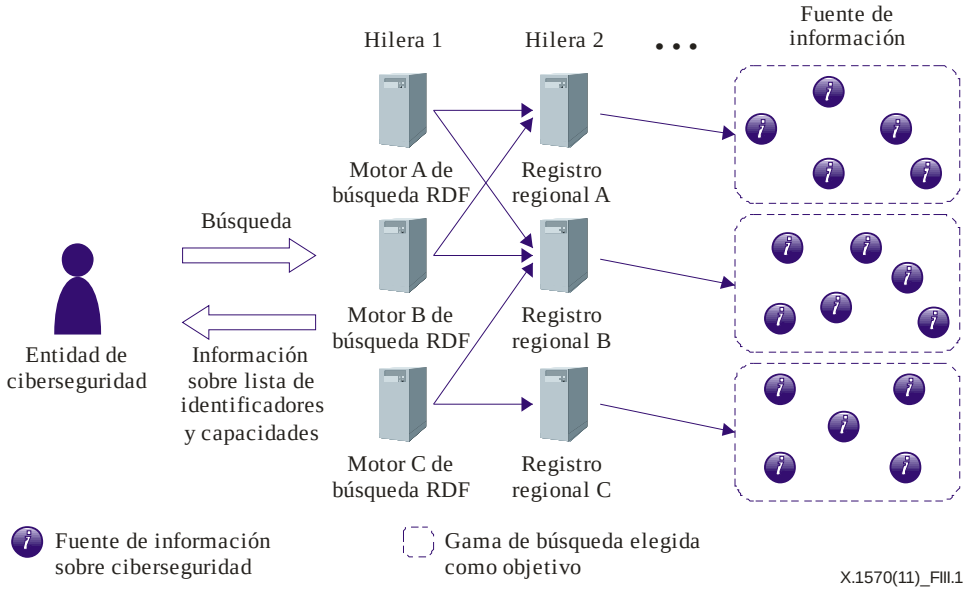


Figura III.1 – Jerarquía del registro de la fuente

III.2 Jerarquía de clase de la información de ciberseguridad

En la figura III.2 se ilustra la jerarquía de clase del mecanismo de descubrimiento. Cada clase representa la categoría introducida en el apéndice II de [b- UIT-T X.1500], así que para mayores detalles véase dicha Recomendación. Obsérvese que se utiliza el espacio de nombre (*namespace*) XML definido por el UIT-T [b-UIT-T X.1500].

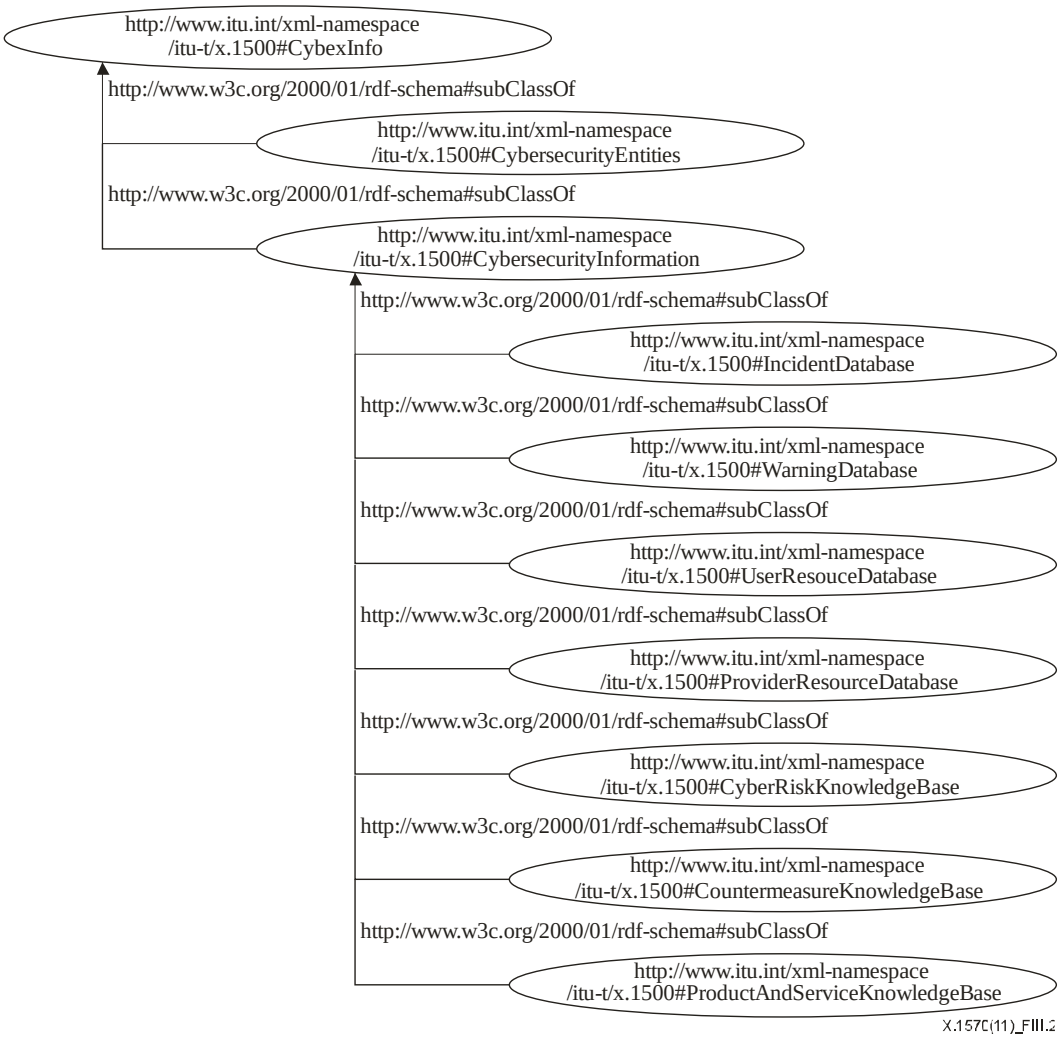


Figura III.2 – Jerarquía de clase de la información de ciberseguridad

NOTA – En la figura III.2 se muestra la utilización de **.int** en el nombre de dominio de nivel superior a título de ejemplo, y no para ser adoptado operacionalmente.

Normalmente cada clase de ciberseguridad contiene los siguientes atributos:

- Fecha de ingreso (entry_date): almacena la fecha de ingreso/modificación de los datos.
- Nombre de expedidor (issuer_name): almacena el nombre del emisor (que puede ser un particular o una empresa).
- Correo electrónico de contacto (contact_email): almacena la dirección de correo electrónico de contacto.
- Recursos (resources): almacena los identificadores, tales como direcciones web.
- Tipo de información (Info_type): almacena los tipos de información tales como CVE, CWSS [b-CWSS], CVSS [b-ITU-T X.1521], OVAL [b-OVAL], SCAP [b-SCAP], XCCDF [b-XCCDF], CPE [b-CPE], CCE [b-CCE] y ARF.

Toda parte que busque información sobre ciberseguridad puede solicitar datos en una unidad de cualquier clase. La información puede buscarse por criterios tales como el nombre de clase, el atributo de clase, o la última hora y fecha de modificación.

La implementación de prueba del esquema de descubrimiento está disponible en línea en http://cybiet.sourceforge.net/.

NOTA – En la implementación se descubre la información de ciberseguridad que está estructurada conforme a la ontología descrita en la figura 7-1.

Bibliografía

[b-UIT-T X.1500] Recomendación UIT-T X.1500 (2011), *Técnicas para el intercambio de información en materia de ciberseguridad.*

[b-UIT-T X.1500.1] Recomendación UIT-T X.1500.1 (2012), *Procedimientos de registro de arcos bajo el arco de identificador de objetos (OID) para el intercambio de información sobre 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-AI] NIST, *The Asset Identification.*
<http://scap.nist.gov/specifications/ai/>

[b-ARF] *Assessment Results Format*
<https://measurablesecurity.mitre.org/incubator/arf/>

[b-CCE] *Common Configuration Enumeration.*
<https://cce.mitre.org/>

[b-CPE] *Common Platform Enumeration.*
<https://cpe.mitre.org/>

[b-CWSS] *Common Weakness Scoring System.*
<https://cwe.mitre.org/cwss/>

[b-Gruber] Gruber T.R. (1993), *Toward principles for the design of ontologies used for knowledge sharing*. International Journal of Human-Computer Studies, Vol. 43, Issues 4-5, noviembre 1995, págs. 907-928.

[b-Ontology] Takahashi T., Kadobayashi Y., Fujiwara H. (2010), *Ontological Approach toward Cybersecurity in Cloud Computing*, International Conference on Security of Information and Networks (SIN), septiembre 2010.

[b-OVAL] *Oval – Open Vulnerability and Assessment Language.*
<https://oval.mitre.org/>

[b-SCAP] *Security Content Automation Protocol (SCAP).*
<http://scap.nist.gov/>

[b-XCCDF] *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
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, 2012