Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1541

(09/2012)

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

Intercambio de información de ciberseguridad – Intercambio de eventos/incidentes/heurística

Formato para el intercambio de descripciones de objetos de incidentes

Recomendación UIT-T X.1541

Unión Internacional de Telecomunicaciones

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/heurística	**X.1540–X.1549**
Intercambio de políticas	X.1550–X.1559
Petición de heurística 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.1541

Formato para el intercambio de descripciones de objetos de incidentes

Resumen

La Recomendación UIT-T X.1541 describe el modelo de información para el formato de intercambio de descripciones de objetos de incidentes (IODEF) y proporciona un modelo de datos asociado especificado en lenguaje XML. El IODEF especifica una representación de modelo de datos para compartir información que suele intercambiarse en caso de incidentes de seguridad informática o de otro tipo. A tal efecto se ha establecido una lista de las secciones pertinentes de IETF RFC 5070 y se indica si son normativas o informativas.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio
1.0	ITU-T X.1541	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 2013

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

ÍNDICE

Introducción

En la Recomendación UIT-T X.1500, "Aspectos generales del intercambio de información de ciberseguridad" se dan orientaciones para el intercambio de información de seguridad, en particular la relativa a incidentes e indicadores que se indican en la presente Recomendación UIT-T. El formato de intercambio de descripciones de objetos de incidentes (IODEF) es un modelo de datos para representar la información que suele intercambiarse en caso de incidentes de seguridad informática. Se especifica un modelo de datos XML para comunicar información sobre incidentes entre las entidades que tienen la responsabilidad operativa de tomar medidas proactivas defensivas, paliativas y de observancia y alerta a una comunidad determinada. El modelo de datos proporciona un método para codificar la información acerca de las computadoras centrales, las redes y los servicios que corren en estos sistemas; la metodología de explotación y los datos conexos; las repercusiones del incidente; y procedimientos limitados para documentar el flujo de trabajo.

La finalidad principal del IODEF es desarrollar las capacidades operativas y aumentar el conocimiento de la situación. La adopción de IODEF por parte de la comunidad mejora su capacidad para resolver incidentes y comunicar la situación general de las amenazas, gracias a que simplifica la colaboración y el intercambio de información. El formato estructurado de IODEF permite:

- una mayor automatización en el procesamiento de la información sobre incidentes a través del intercambio de información estructural sobre el incidente, eliminando así la necesidad de recurrir a analistas de seguridad para analizar documentos de texto exentos de formato;
- un menor esfuerzo para establecer la correlación entre datos similares (incluso cuando están muy estructurados) procedentes de distintas fuentes, lo que permite conocer mejor la situación; y
- un formato común que hace posible la compatibilidad de herramientas para el tratamiento y análisis de los incidentes, especialmente cuando la información procede de distintas entidades.

Hay numerosas consideraciones de procedimiento, fiabilidad, políticas y legales que pueden limitar o impedir el intercambio de información. El IODEF es una especificación técnica y no trata de resolver estos problemas. Sin embargo, al elaborar los acuerdos de intercambio de información, habrá que considerar este contexto más amplio a efectos de la aplicación práctica del IODEF y de los formatos y protocolos asociados.

Recomendación UIT-T X.1541

Formato para el intercambio de descripciones de objetos de incidentes

1 Alcance

El formato de intercambio de descripciones de objetos de incidentes (IODEF) especifica una representación del modelo de datos para compartir información que suele intercambiarse en caso de incidentes de seguridad informática o de otro tipo. En esta Recomendación se describe el modelo de información para el IODEF y el modelo de datos correspondiente especificado en lenguaje XML.

Toda representación de modelo de datos o todo marco que permita el intercambio de información sobre seguridad informática o incidentes de otro tipo de ofrecer las capacidades necesarias para cumplir con todas las políticas, reglamentaciones y legislaciones regionales y nacionales aplicables.

Los encargados de la aplicación y los usuarios de todas las Recomendaciones UIT-T, incluidas la Recomendación UIT-T X.1541 y las técnicas subyacentes, deberán cumplir con todas las políticas, reglamentaciones y legislaciones regionales y nacionales aplicables.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de esta Recomendación. A la fecha de esta publicación, las ediciones citadas están en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios a que estudien la posibilidad de utilizar la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente en vigor. En la presente Recomendación, la referencia a un documento no confiere a este último, como documento autónomo, la categoría de una Recomendación.

[IETF RFC 5070] IETF RFC 5070 (2007), *Incident Object Description Exchange Format*. <http://datatracker.ietf.org/doc/RFC 5070/>.

3 Definiciones

3.1 Términos definidos en otros documentos

Ninguno.

3.2 Términos definidos en esta Recomendación

Ninguno.

4 Abreviaturas y acrónimos

Esta Recomendación utiliza las abreviaturas y acrónimos siguientes:

IANA Autoridad de asignación de números Internet (*Internet assigned numbers authority*)

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

5 Convenios

Los siguientes términos se consideran equivalentes:

- En la UIT, los requisitos obligatorios se expresan con el futuro simple del verbo principal (futuro de mandato) u otras expresiones con significado de obligación y sus equivalentes negativos.
- En la UIT, el uso de la palabra inglesa "shall" es equivalente al uso que se hace en el IETF de la palabra "MUST".
- En la UIT, el uso de la expresión inglesa "shall not" es equivalente al uso que se hace en el IETF de la expresión "MUST NOT".

NOTA – En el IETF las palabras inglesas "shall" y "must" (en minúsculas) se utilizan para textos de carácter informativo.

6 Descripción de objetos de incidentes y formato de intercambio

En la cláusula 6 se define el formato de intercambio de descripciones de objetos de incidentes (IODEF). Esta cláusula ofrece referencias directas a [IETF RFC 5070] mediante el alineamiento de las cláusulas con los números de la sección, de modo que la cláusula 6.x se alinea con la sección x de [IETF RFC 5070] con títulos idénticos.

NOTA – En [b-Errata ID3333] se corrige una errata de [b-IETF RFC 5070].

6.1 Introducción

La sección 1 de [b-IETF RFC 5070] es informativa.

6.1.1 Terminología

La sección 1.1 [b-IETF RFC 5070] es informativa.

6.1.2 Notaciones

La sección 1.2 de [b-IETF RFC 5070] es informativa.

6.1.3 Sobre el modelo de datos IODEF

La sección 1.3 de [b-IETF RFC 5070] es informativa.

6.1.4 Acerca de la implementación del IODEF

La sección 1.4 de [b-IETF RFC 5070] es informativa.

6.2 Tipos de datos IODEF

La sección 2 de [b-IETF RFC 5070] es informativa.

6.2.1 Enteros

La sección 2.1 de [IETF RFC 5070] es normativa.

6.2.2 Números reales

La sección 2.2 de [IETF RFC 5070] es normativa.

6.2.3 Caracteres y cadenas

La sección 2.3 de [IETF RFC 5070] es normativa.

6.2.4 Cadenas multilingües

La sección 2.4 de [IETF RFC 5070] es normativa.

6.2.5 Bytes

La sección 2.5 de [IETF RFC 5070] es normativa.

6.2.6 Bytes hexadecimales

La sección 2.6 de [IETF RFC 5070] es normativa.

6.2.7 Tipos enumerados

La sección 2.7 de [IETF RFC 5070] es normativa.

6.2.8 Cadenas fecha-hora

La sección 2.8 de [IETF RFC 5070] es normativa.

6.2.9 Cadena de zona horaria

La sección 2.9 de [IETF RFC 5070] es normativa.

6.2.10 Listas de puertos

La sección 2.10 de [IETF RFC 5070] es normativa.

6.2.11 Dirección postal

La sección 2.11 de [IETF RFC 5070] es normativa.

6.2.12 Persona u organización

La sección 2.12 de [IETF RFC 5070] es normativa.

6.2.13 Números de teléfono y fax

La sección 2.13 de [IETF RFC 5070] es normativa.

6.2.14 Cadena de correo-e

La sección 2.14 de [IETF RFC 5070] es normativa.

6.2.15 Cadenas de localizador uniforme de recursos

La sección 2.15 de [IETF RFC 5070] es normativa.

6.3 El modelo de datos IODEF

La sección 3 de [b-IETF RFC 5070] es informativa.

6.3.1 Clase de documento IODEF

La sección 3.1 de [IETF RFC 5070] es normativa.

6.3.2 Clase de incidente

La sección 3.2 de [IETF RFC 5070] es normativa.

6.3.3 Clase de IncidentID

La sección 3.3 de [IETF RFC 5070] es normativa.

6.3.4 Clase de AlternativeID

La sección 3.4 de [IETF RFC 5070] es normativa.

6.3.5 Clase de RelatedActivity

La sección 3.5 de [IETF RFC 5070] es normativa.

6.3.6 Clase de AdditionalData

La sección 3.6 de [IETF RFC 5070] es normativa.

6.3.7 Clase de contacto

La sección 3.7 de [IETF RFC 5070] es normativa.

6.3.7.1 Clase de RegistryHandle

La sección 3.7.1 de [IETF RFC 5070] es normativa.

6.3.7.2 Clase de PostalAddress

La sección 3.7.2 de [IETF RFC 5070] es normativa.

6.3.7.3 Clase de correo-e

La sección 3.7.3 de [IETF RFC 5070] es normativa.

6.3.7.4 Clases de teléfono y fax

La sección 3.7.4 de [IETF RFC 5070] es normativa.

6.3.8 Clases de tiempo

La sección 3.8 de [IETF RFC 5070] es normativa.

6.3.8.1 StartTime

La sección 3.8.1 de [IETF RFC 5070] es normativa.

6.3.8.2 EndTime

La sección 3.8.2 de [IETF RFC 5070] es normativa.

6.3.8.3 DetectTime

La sección 3.8.3 de [IETF RFC 5070] es normativa.

6.3.8.4 ReportTime

La sección 3.8.4 de [IETF RFC 5070] es normativa.

6.3.8.5 DateTime

La sección 3.8.5 de [IETF RFC 5070] es normativa.

6.3.9 Clase de método

La sección 3.9 de [IETF RFC 5070] es normativa.

6.3.9.1 Clase de referencia

La sección 3.9.1 de [IETF RFC 5070] es normativa.

6.3.10 Clase de evaluación

La sección 3.10 de [IETF RFC 5070] es normativa.

6.3.10.1 Clase de repercusión

La sección 3.10.1 de [IETF RFC 5070] es normativa.

6.3.10.2 Clase de TimeImpact

La sección 3.10.2 de [IETF RFC 5070] es normativa.

6.3.10.3 Clase de MonetaryImpact

La sección 3.10.3 de [IETF RFC 5070] es normativa.

6.3.10.4 Clase de confianza

La sección 3.10.4 de [IETF RFC 5070] es normativa.

6.3.11 Clase histórica

La sección 3.11 de [IETF RFC 5070] es normativa.

6.3.11.1 Clase de HistoryItem

La sección 3.11.1 de [IETF RFC 5070] es normativa.

6.3.12 Clase de EventData

La sección 3.12 de [IETF RFC 5070] es normativa.

6.3.12.1 Relacionar las clases de incidente y EventData

La sección 3.12.1 de [IETF RFC 5070] es normativa.

6.3.12.2 Cardinalidad de EventData

La sección 3.12.2 de [IETF RFC 5070] es normativa.

6.3.13 Clase de expectativa

La sección 3.13 de [IETF RFC 5070] es normativa.

6.3.14 Clase de flujo

La sección 3.14 de [IETF RFC 5070] es normativa.

6.3.15 Clase de sistema

La sección 3.15 de [IETF RFC 5070] es normativa.

6.3.16 Clase de nodo

La sección 3.16 de [IETF RFC 5070] es normativa.

6.3.16.1 Clase de cómputo

La sección 3.16.1 de [IETF RFC 5070] es normativa.

6.3.16.2 Clase de dirección

La sección 3.16.2 de [IETF RFC 5070] es normativa.

6.3.16.3 Clase de NodeRole

La sección 3.16.3 de [IETF RFC 5070] es normativa.

6.3.17 Clase de servicio

La sección 3.17 de [IETF RFC 5070] es normativa.

6.3.17.1 Clase de aplicación

La sección 3.17.1 de [IETF RFC 5070] es normativa.

6.3.18 Clase de OperatingSystem

La sección 3.18 de [IETF RFC 5070] es normativa.

6.3.19 Clase de registro

La sección 3.19 de [IETF RFC 5070] es normativa.

6.3.19.1 Clase de RecordData

La sección 3.19.1 de [IETF RFC 5070] es normativa.

6.3.19.2 Clase de RecordPattern

La sección 3.19.2 de [IETF RFC 5070] es normativa.

6.3.19.3 Clase de RecordItem

La sección 3.19.3 de [IETF RFC 5070] es normativa.

6.4 Consideraciones de procesamiento

La sección 4 de [b-IETF RFC 5070] es informativa.

6.4.1 Codificación

La sección 4.1 de [IETF RFC 5070] es normativa.

6.4.2 IODEF namespace

La sección 4.2 de [IETF RFC 5070] es normativa.

6.4.3 Validación

La sección 4.3 de [IETF RFC 5070] es normativa.

6.5 Ampliar el IODEF

La sección 5 de [b-IETF RFC 5070] es informativa.

En la Recomendación UIT-T X.1500, "Aspectos generales del intercambio de información de ciberseguridad" se dan orientaciones para el intercambio de información de seguridad, en particular la relativa a incidentes e indicadores que se indican en la presente Recomendación UIT-T. Esta Recomendación describe el formato básico para el intercambio de información sobre incidentes, pero no comprende todos los casos de utilización con arreglo a la Recomendación UIT-T X.1500. Podrían ser necesarias extensiones para satisfacer la necesidades de ciertos casos de utilización.

6.5.1 Ampliar los valores enumerados de los atributos

La sección 5.1 de [IETF RFC 5070] es normativa.

6.5.2 Ampliar las clases

La sección 5.2 de [IETF RFC 5070] es normativa.

6.6 Cuestiones de internacionalización

La sección 6 de [IETF RFC 5070] es normativa.

6.7 Ejemplos

La sección 7 de [b-IETF RFC 5070] es informativa.

6.7.1 Gusano

La sección 7.1 de [b-IETF RFC 5070] es informativa.

6.7.2 Reconocimiento

La sección 7.2 de [b-IETF RFC 5070] es informativa.

6.7.3 Denuncia de Bot-net

La sección 7.3 de [b-IETF RFC 5070] es informativa.

6.7.4 Lista de vigilancia

La sección 7.4 de [b-IETF RFC 5070] es informativa.

6.8 El esquema IODEF

La sección 8 de [IETF RFC 5070] es normativa.

6.9 Consideraciones de seguridad

La sección 9 de [IETF RFC 5070] es normativa.

En las implementaciones acordes con el UIT-T, el formato y protocolo de mensaje subyacentes utilizados para el intercambio de ejemplos del IODEF deberán prever garantías apropiadas de confidencialidad, integridad y autenticidad.

NOTA – En el IETF la palabra "must" (en minúsculas) se utiliza para el texto informativo.

6.10 Consideraciones IANA

La sección 10 de [IETF RFC 5070] es normativa.

6.11 Acuses de recibo

La sección 11 de [b-IETF RFC 5070] es informativa.

6.12 Referencias

6.12.1 Normativa

La sección 12.1 de [b-IETF RFC 5070] es informativa.

Esta Recomendación UIT-T ha identificado la sección 12 de [IETF RFC 5070] como informativa, ya que el UIT-T no elaboró ninguna posición respecto de ninguna de estas referencias en lo que respecta a esta Recomendación. No obstante, se reconoce que el IETF ha identificado una serie de referencias normativas para [IETF RFC 5070].

6.12.2 Informativo

La sección 12.2 de [b-IETF RFC 5070] es informativa.

Bibliografía

[b-ITU-T X.1500] Recomendación UIT-T X.1500 (2011), *Aspectos generales del intercambio de información de ciberseguridad*.

[b-Errata ID3333] IETF RFC Errata ID: 3333, *IETF RFC5070, "The Incident Object Description Exchange Format", December 2007; Status: Held for Document Update; Type: Editorial; Date Reported: 2012-09-02.* <http://www.rfc-editor.org/errata_search.php?eid=3333>.

[b-IETF RFC 5070] IETF RFC 5070 (2007), *The Incident Object Description Exchange Format (IODEF)*. <https://datatracker.ietf.org/doc/RFC 5070/>.

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, 2013