Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1257

(03/2016)

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

Seguridad en el ciberespacio – Gestión de identidades

Taxonomía de la gestión del acceso y de la identidad

Recomendación UIT-T X.1257

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
Recomendaciones relacionadas con la PKI	X.1340–X.1349
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
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699

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

Recomendación UIT-T X.1257

Taxonomía de la gestión del acceso y de la identidad

Resumen

En la Recomendación UIT-T X.1257 se describe una especificación destinada a garantizar que se asigna el significado corporativo necesario a los permisos y roles de IAM (gestión del acceso y de la identidad) y que dicho significado corporativo es trazable y referenciable durante toda la vida útil del proceso IAM, de modo que esos permisos puedan asignarse eficazmente al usuario, que los controles de separación de funciones (SoD, *separation of duties*) se apliquen satisfactoriamente entre aplicaciones y que los procesos de conciliación y revisión del acceso puedan llevarse a cabo con eficiencia.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1257	2016-03-23	17	11.1002/1000/12608

Palabras clave

Función, gestión de acceso, gestión de identidad y acceso, permiso, significado corporativo, tarea corporativa, taxonomía corporativa, vida útil de IAM.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

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

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

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

En la fecha de aprobación de la presente Recomendación, la UIT [ha recibido/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

Recomendación UIT-T X.1257

Taxonomía de la gestión del acceso y de la identidad

1 Alcance

En la presente Recomendación se especifican los requisitos para asignar significado corporativo a roles de gestión de identidad y acceso (IAM) y permisos de usuario a partir de [UIT-T X.1252], [UIT-T X.1254] y [b-UIT-T X.1255] y ampliándolas para proponer lo siguiente:

- Una taxonomía IAM para identificar semánticamente y organizar las fases y procesos IAM a fin de representar una vida útil exhaustiva de los procesos IAM.
- Un modelo ontológico IAM para identificar semánticamente los tipos de permisos y roles IAM, su sintaxis y los correspondientes tipos de relaciones.

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.1252] Recomendación UIT-T X.1252 (2010), *Términos y definiciones sobre gestión de identidad de referencia*.

[UIT-T X.1254] Recomendación UIT-T X.1254 (2012), *Marco de garantía de la autentificación de entidades*.

3 Definiciones

3.1 Términos definidos en otros documentos

3.1.1 control de acceso [UIT-T X.1252]: Procedimiento utilizado para determinar si se debe conceder a una entidad acceso a Recursos, instalaciones, servicios o informaciones, en función de las normas preestablecidas y la autoridad o los derechos específicos de la parte solicitante.

3.1.2 atributo [UIT-T X.1252]: Información relacionada con una entidad que especifica una característica de la entidad.

3.1.3 contexto [UIT-T X.1252]: Entorno con condiciones de contorno definidas en las que existen e interactúan entidades.

3.1.4 credencial [UIT-T X.1252]: Conjunto de datos presentado como evidencia de una identidad y/o unos derechos declarados.

3.1.5 entidad [UIT-T X.1252]: Cualquier cosa que tenga una existencia autónoma y bien definida y pueda ser identificada en contexto.

3.1.6 identificador [UIT-T X.1254]: Uno o varios atributos que caracterizan inequívocamente una entidad en un determinado contexto.

3.1.7 identidad [b-ISO/IEC 24760-1]: Conjunto de atributos relativos a una entidad.

NOTA – Una identidad puede tener uno o varios identificadores que permiten reconocer inequívocamente a la entidad en un determinado contexto.

3.1.8 rol [UIT-T X.1252]: Serie de propiedades o atributos que describen las capacidades o las funciones que puede desempeñar una entidad.

NOTA – Cada entidad puede tener/desempeñar varias funciones. Las capacidades pueden ser inherentes o asignadas.

3.1.9 usuario [UIT-T X.1252]: Entidad que utiliza un Recurso, por ejemplo, sistemas, equipos, terminales, procesos, aplicaciones o redes corporativas.

3.2 Términos definidos en la presente Recomendación

En esta Recomendación se definen los términos siguientes:

3.2.1 asignación de acceso: Proceso de asignar derechos de acceso al usuario.

3.2.2 gestión de solicitudes de cambio de acceso: Proceso para gestionar las solicitudes de cambio de acceso.

3.2.3 restricciones de acceso: Conjunto de restricciones de acceso basadas en la ubicación del usuario, las tareas restringidas temporalmente y los Recursos restringidos temporalmente.

3.2.4 ingeniería de acceso: Proceso de crear y mantener derechos de acceso.

3.2.5 operación de acceso: Proceso de evaluar los derechos de acceso del usuario a los efectos de ejecutar determinadas tareas administrativas.

3.2.6 política de acceso: Mecanismos de restricción del control de acceso (es decir, de qué permisos corporativos puede disfrutar un usuario durante el tiempo de ejecución).

3.2.7 conciliación de acceso: Proceso de modificación de los derechos del usuario con arreglo a los requisitos de acceso estipulados a fin de evitar el acceso de usuarios sobre (o *infra*) privilegiados.

3.2.8 revisión del acceso: Proceso de revisión de los derechos de acceso del usuario a los efectos de la ulterior conciliación y certificación.

3.2.9 política de asignación: Mecanismo de restricción de asignación de permisos (es decir, qué tareas pueden asignarse a cada usuario).

3.2.10 ingeniería de la lógica de autorización: Proceso de desarrollo y mantenimiento de lógica de autorización entre las aplicaciones relacionadas.

3.2.11 navegador: Aplicación que se ejecuta en un dispositivo utilizado por el usuario para interactuar con un proveedor de servicio.

3.2.12 rol corporativo: Conjunto de tareas (con o sin permisos) que un usuario puede tener derecho a realizar.

3.2.13 registro de acceso a tareas corporativas: Proceso de registro de la ejecución de tareas finalizadas satisfactoriamente o de los usuarios no autorizados a realizar ciertas tareas.

3.2.14 autorización para la ejecución de tareas: Proceso de autorización a un usuario para realizar tareas específicas en un determinado Recurso.

3.2.15 ejecución de tareas corporativas: Proceso de ejecutar tareas específicas.

3.2.16 ingeniería de taxonomía corporativa: Proceso de creación y mantenimiento de procesos corporativos y de taxonomía de productos corporativos.

3.2.17 taxonomía de procesos corporativos: Taxonomía que identifica semánticamente y organiza procesos corporativos en subprocesos dentro de una estructura jerárquica.

3.2.18 canal: Método de comunicación que elige el usuario para interactuar con el proveedor de servicio.

3.2.19 dispositivo: Mecanismo al que recurre un usuario para permitir la interacción con el proveedor de servicios.

3.2.20 titularidad: Conjunto de tareas y permisos asignados al usuario.

3.2.21 vida útil del proceso IAM: Vida útil de los procesos y subprocesos de gestión del acceso y de identidades.

3.2.22 ingeniería de roles IAM: Proceso de creación y mantenimiento de permisos y roles IAM.

3.2.23 intención: Motivo o propósito del usuario para iniciar la interacción con el proveedor de servicio.

3.2.24 permiso: Conjunto de tareas que acceden a Recursos restringidos por las correspondientes políticas de control de acceso.

3.2.25 recurso: Nodo extremo de una taxonomía de productos corporativos también denominado producto corporativo.

3.2.26 sesión: Contenedor de atributos de autentificación y autorización en tiempo de ejecución.

3.2.27 tarea: Nodo extremo de una taxonomía de procesos corporativos también denominado tarea corporativa.

3.2.28 equipo: Contenedor de Recursos humanos de roles que tienen en común cada miembro del equipo.

4 Siglas y acrónimos

En esta Recomendación se utilizan los siguientes acrónimos y abreviaturas:

APQC American Productivity and Quality Center

CPC Clasificación central de productos (*central product classification*)

eTOM Mapa de operaciones de telecomunicaciones (*enhanced Telecom Operations Map*)

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

IAM Gestión de acceso y de identidades (*hypertext transfer protocol*)

IP Protocolo Internet (*Internet protocol*)

IT Tecnología de la información (*information technology*)

JSON Notación de objetos JavaScript (*javascript object notation*)

JSON-LD JSON para enlaces de datos (*json-based serialization for linked data*)

MAC Control de acceso a los medios (*media access control*)

PCF Marco de clasificación de procesos (*process classification framework*)

RBAC Control de acceso basado en roles (*role based access control*)

REST Transferencia de estado representativo (*representational state transfer*)

SCIM Sistema para la gestión de identidades entre dominios (*system for cross-domain identity management*)

SDLC Vida útil de desarrollo del software (*software development life cycle*)

SKOS Sistema sencillo de organización de conocimientos (*simple knowledge organization system*)

SOAP Protocolo sencillo de acceso a objetos (*simple object access protocol*)

SoD Separación de funciones (*separation of duties*)

URL Localizador uniforme de Recursos (*uniform resource locator*)

XACML Lenguaje de marcaje de control de acceso extensible (*extensible access control markup language*)

5 Convenios

En la presente Recomendación se utilizan los siguientes convenios:

La mayúscula inicial en el medio de una frase indica que se utiliza un término que forma parte del modelo (es decir, del modelo ontológico IAM o del modelo de taxonomía IAM) como "Rol corporativo" o "Ingeniería de roles IAM" y que también puede encontrase en los diagramas correspondientes. El término "Tarea corporativa" y "Tarea" se utilizan indistintamente en aras de la legibilidad. El término "Recurso corporativo" y "Recurso" también se emplean indistintamente a efectos de legibilidad.

6 Introducción

La falta de significado corporativo en los actuales roles de gestión del acceso y de identidades (IAM) y en los permisos de usuario afecta negativamente a toda la vida útil de la IAM. Si bien los roles IAM tales como "SuperAdmin", "SuperUpdate" y "XYZSystemSpecialAccess" son ambiguos, excesivamente técnicos y crípticos, son no obstante comunes en muchas empresas. Obviamente, en lugar de reutilizar estos ambiguos roles, los ingenieros de roles IAM crean una y otra vez nuevos roles. En última instancia acaba dificultando sobremanera la gestión de los roles IAM específicos del sistema que, además, no se corresponde con el significado corporativo previsto.

Este enorme número de roles y su escasa calidad semántica afecta negativamente a las importantes fases de la vida útil IAM tales como la Asignación de acceso, la Autorización de acceso, la Revisión del acceso y la Conciliación del acceso. Durante la Asignación del acceso, si el experto en este campo no comprende el significado de los roles existentes podría asignar privilegios equivocados al usuario. Para compensar la falta de significado corporativo en la aplicación de los roles IAM los ingenieros disponen de una lógica física de autorización de código en sus aplicaciones. Sincronizar el mantenimiento del código fuente de dicha lógica de autorización entre las aplicaciones es una tarea problemática y propensa a errores. Por otra parte, resulta difícil (si no imposible) aplicar controles de Separación de funciones (SoD) entre las distintas aplicaciones. Durante la Revisión del acceso debido a la falta de significado corporativo en las funciones IAM y a la presión para cumplir los plazos, los encargados de dicha revisión certifican (o rechazan) por error derechos de acceso de los usuarios. La elevada tasa de tales errores de revisión de acceso y la aplicación de la lógica de autorización propensa a errores aumenta el riesgo de dañar la reputación y de pérdidas financieras, plantea problemas reglamentarios, repercute negativamente en la productividad del Equipo de operaciones IAM y, además, dificulta la capacidad de suministrar soluciones corporativas a gran escala, tales como la racionalización de roles, procesos y aplicaciones.

Dado que las actuales especificaciones de control de acceso estándar no definen la semántica de los roles y permisos IAM, es necesario especificar un conjunto complementario de requisitos de gestión del acceso. Dichos requisitos garantizarán que se asigne el significado corporativo necesario a los roles y permisos IAM y que dicho significado sea trazable y referenciable durante la vida útil del proceso IAM, de modo que esos permisos puedan asignarse eficazmente al usuario, los controles de Separación de funciones se apliquen satisfactoriamente entre aplicaciones y que los procesos de conciliación y revisión del acceso puedan llevarse a cabo con eficiencia.

7 Descripción general del método

A continuación se describe en detalle el método, teniendo presente que el cometido de esta Recomendación es desarrollar un conjunto de requisitos para asignar significado corporativo a los roles IAM. Como se indicó en la cláusula 6 – el Equipo de ingería de roles IAM necesita asignar el significado corporativo requerido para los nuevos roles IAM. La cuestión radia determinar cuál es el origen de dicho significado corporativo y quién lo produce. Hoy en día, los arquitectos corporativos reciben una estrategia corporativa y se les encomienda la tarea de desarrollar un proceso corporativo y una taxonomía de productos corporativos.

La taxonomía de procesos corporativos identifica semánticamente y organiza los procesos y subprocesos corporativos en una estructura jerárquica (a los efectos de la navegación por el inventario de procesos) que comienza con la raíz Industria y se descompone en Sector de actividad, Proceso corporativo, Actividad corporativa y Tareas corporativas (para más información, véase el Apéndice VI – normas de la taxonomía de procesos corporativos). La taxonomía corporativa también incluye una jerarquía de productos corporativos y normalmente los arquitectos de productos corporativos se encargan de su mantenimiento en una gran hoja de cálculo u otro tipo de documento.

Durante la vida útil del desarrollo del software (SDLC) los analistas copian y pegan fragmentos de ese contenido jerárquico a fin de crear un documento de requisitos corporativos que luego transmiten al Equipo de ingeniería de roles IAM y al Equipo de desarrollo de aplicaciones para su ulterior implementación. Como el ingeniero de roles no puede hacer referencia a tareas específicas mediante su identificador, suele crear roles IAM con o sin definición en función de su interpretación obsoleta de las Tareas que el usuario puede realizar. Al final, el significado corporativo del rol IAM se pierde o el diseñador de aplicaciones lo malinterpreta. ¿Cómo se puede resolver este problema?

Para resolver este problema, el significado corporativo en los roles IAM debe ser referenciable y trazable respecto de las correspondientes Tareas actuales durante la vida útil de los procesos IAM. Esta es una característica fundamental de calidad que permite mejorar la calidad de toda la vida útil de los procesos IAM. ¿Cómo se puede implementar esta característica de calidad? Existen diversos métodos de representación semántica para implementar una interfaz de programación de aplicaciones para la taxonomía corporativa (véase el Apéndice V – Posibles mecanismos de implementación de la interfaz de taxonomía corporativa).

Ahora bien, no basta con disponer de un significado corporativo referenciable y trazable durante la vida útil de los procesos IAM. También se necesita especificar una sintaxis para los roles IAM.

Actualmente la sintaxis para roles IAM se especifica mediante un mecanismo de control de acceso estándar muy utilizado denominado Control de acceso basado en roles (RBAC) que se ilustra en la Figura 1.

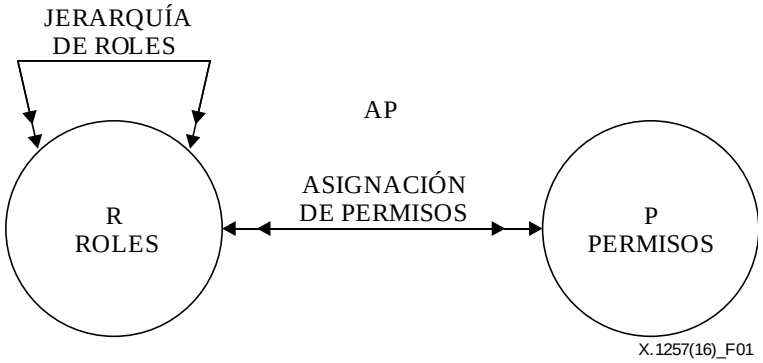

Figura 1 – Modelo RBAC tradicional

Se puede observar la siguiente sintaxis de roles:

- Roles que contienen otros roles – es decir, que forman una jerarquía de roles.
- Los roles se crean a partir de permisos.

Sin embargo, este mecanismo RBAC tradicional tiene limitaciones conocidas: no especifica la semántica de los permisos (es decir, la "naturaleza de los permisos"). En cambio, la especificación dice que la semántica de permisos está abierta a interpretación: "los permisos pueden definirse en términos de operaciones primitivas, tales como leer y escribir, u operaciones abstractas como crédito y débito." [b-NIST-RBAC 2000]. Ahora bien, en la práctica, como se muestra en la cláusula 6, se crean roles IAM ambiguos sin referencia a las correspondientes Tareas.

A fin de asignar significado corporativo a los roles IAM es necesario especificar la sintaxis semántica para los roles IAM. El significado tendrá que proceder de los nodos hoja de taxonomía corporativa más granulares: Tareas y Recursos. En la Figura 2 se muestra la sintaxis del rol IAM.

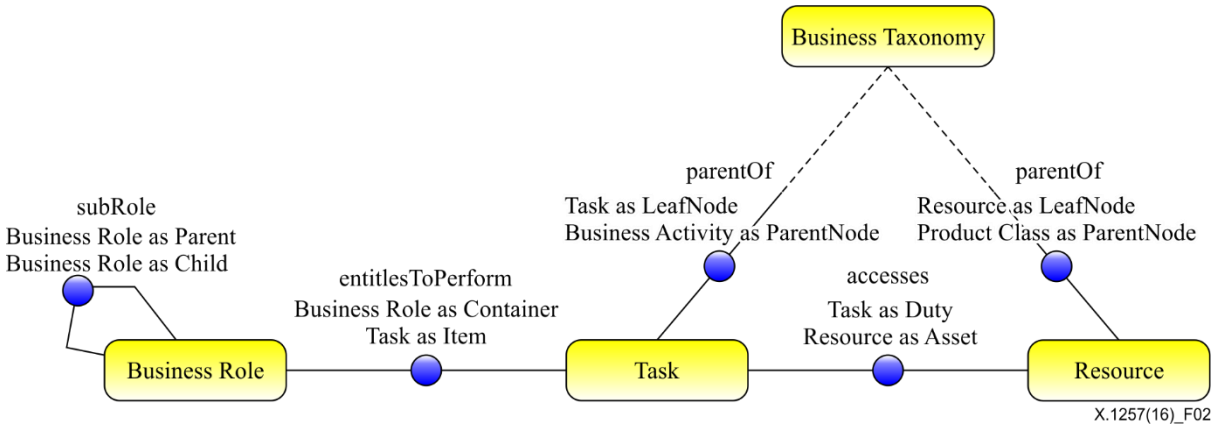

Figura 2 – Diagrama conceptual de la gestión de acceso basado en Tareas

Se puede observar lo siguiente:

- Los roles pueden (aún) contener otros roles mediante la relación "subRole", es decir, formar una jerarquía de roles.
- Sintaxis básica de los roles IAM:
  - El rol corporativo autoriza al usuario a realizar tareas mediante la relación "entitlesToPerform". De esto modo, todo rol IAM hereda implícitamente su significado corporativo de las correspondientes Tareas.
  - La Tarea administrativa (no el usuario o el rol) accede a un recurso específico (es decir "producto corporativo"). La relación "accesos" es optativa y se necesita cuando se requiere un control de acceso con mayor granularidad.
  - Las tareas y los recursos en cuanto nodos hoja de la taxonomía corporativa sirve de componentes indispensables durante la ingeniería de roles IAM y se hace referencia a los mismos durante toda la vida útil de los procesos IAM.

En aras de la simplicidad, en la Figura 2 no se muestran los tipos matrices de tareas y de productos de recursos.

En el Cuadro 1 figuran unos cuantos ejemplos de derechos que ayudan a ilustrar los puntos mencionados:

Cuadro 1 – Ejemplos de derechos

Rol corporativo	Tarea	Recurso
Cajero	Crear cuenta	Cuenta corriente avanzada
Doctor	Examinar historial del paciente	Historial del paciente
Administrador del sistema	Actualizar el entorno del sistema	Entorno del sistema

La sintaxis anterior de los roles IAM permiten obtener nuestra meta principal, a saber, asignar significado corporativo a los roles IAM. En la siguiente cláusula se describe el método propuesto en la forma de requisitos.

8 Requisitos sintácticos y semánticos de los roles IAM

Se formulan las siguientes recomendaciones para roles IAM que tienen el significado corporativo necesario:

1) La taxonomía corporativa sirve de parámetro indispensable en la vida útil del proceso IAM para otorgar significado corporativo a los permisos de usuario y a los roles IAM durante toda la vida útil.

2) El significado corporativo en los roles IAM es referenciable y trazable respecto de las Tareas de la taxonomía corporativa durante toda la vida útil del proceso IAM.

3) Los roles IAM han de obedecer a la siguiente sintaxis:

   3.1) El rol IAM está integrado por las tareas que el usuario tienen derecho a desempeñar.

   3.2) El rol IAM está formado por tareas que opcionalmente acceden a recursos corporativos específicos cuando se requiere un control de acceso con mayor granularidad.

4) La ejecución de tareas realizadas y las solicitudes no autorizadas de ejecución de tareas se han de registrar mediante la referencia a los correspondientes identificadores de tareas.

Anexo A

(Este anexo forma parte integrante de la presente Recomendación.)

Este anexo se deja en blanco y se ha previsto para proporcionar posibles casos de implementación futura de la Gestión de acceso basada en tareas IAM.

Apéndice I

Vida útil de los procesos de taxonomía IAM

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

La Figura I.1 muestra que toda la vida útil de los procesos IAM se ve afectada principalmente por los cambios resultantes de la taxonomía corporativa. Estos cambios en la taxonomía corporativa los realizan y consuman los Equipos de ingeniería lógica de autorización y de ingeniería de roles IAM. Los cambios contendrán identificadores de Tareas corporativas en los correspondientes objetos, tales como roles IAM, código fuente de la Lógica de autorización y ficheros registro de autorización y de ejecución de Tareas.

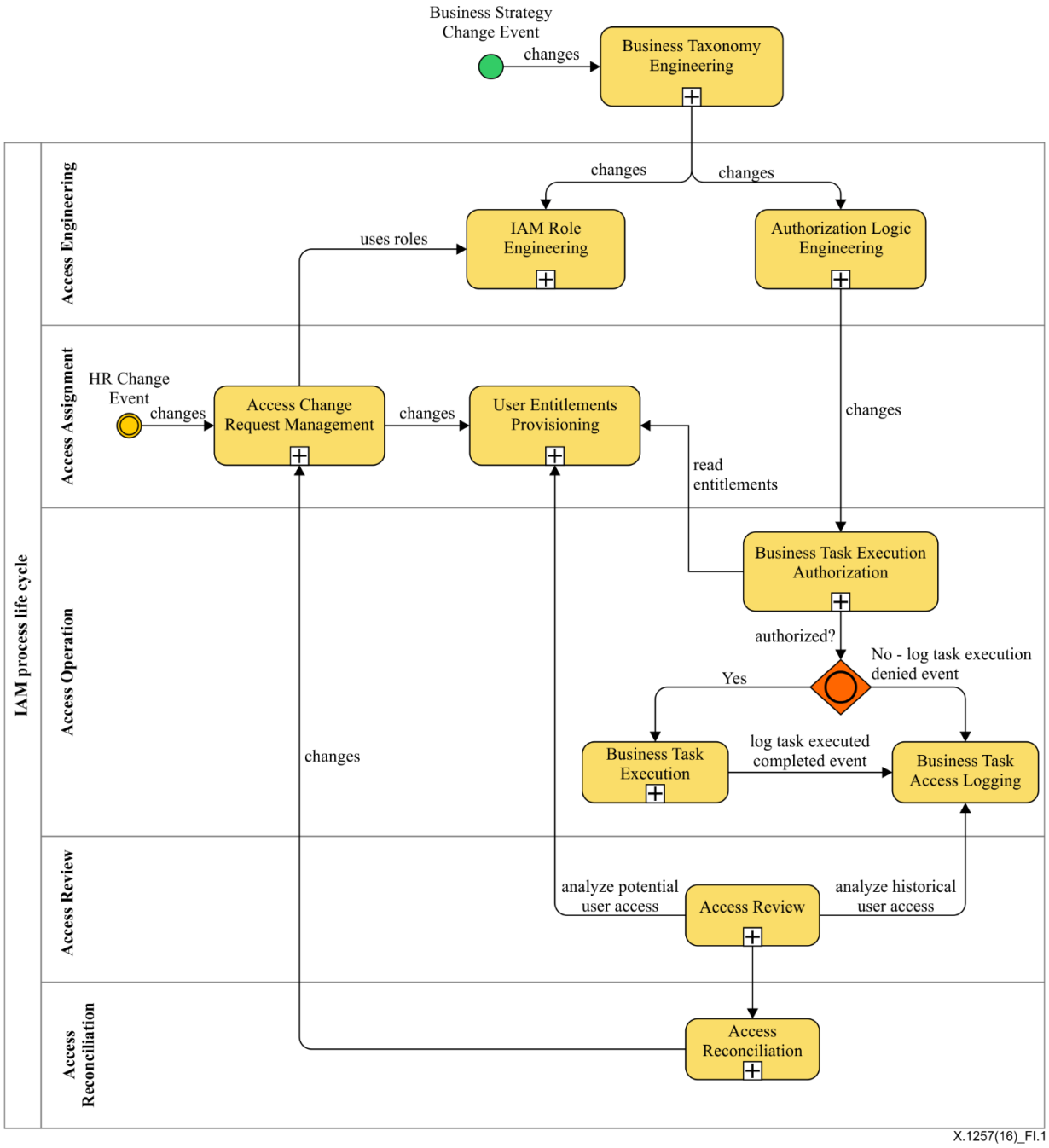

Figura I.1 – Dependencia de la vida útil de los procesos IAM

La segunda fuente de cambios consiste en eventos de recursos humanos, tales como contratación, ausencias, movilidad y otros eventos de este tipo. Estos eventos se tramitan en el proceso de gestión de solicitud de modificación de acceso y los correspondientes derechos de usuario se configuran en directorios de derechos de usuario. En particular, estos derechos contendrán referencias identificadoras a tareas que tienen un significado corporativo y se referenciarán durante la autorización en tiempo de ejecución de la aplicación. Una vez autentificado el usuario (este proceso no se muestra en aras de la simplicidad) los controles SoD preventivos bloquearán la ejecución de Tareas conflictivas durante la autorización en tiempo de ejecución. Durante el proceso de Autorización de ejecución de Tareas el usuario está autorizado a realizar la Tarea y ésta se ejecuta, o bien no está autorizado. En cualquier caso la aplicación registrará estos eventos haciendo referencia a los correspondientes identificadores de Tareas. A continuación se muestra un posible ejemplo de formato del registro:

```
2016-02-08 22:20:02,165 ait:AppID1 192.168.0.1 UserID123 btt:TaskID1 btr:456:355
bttes:200 "Tarea llevada a buen término"

2016-02-08 22:24:02,165 ait:AppID1 192.168.0.1 UserID123 btt:TaskID2 bttes:401
"Usuario no autorizado a ejecutar la Tarea"
```

siendo:

- **btt** – es un espacio de nombres que apunta a un prefijo HTTP URL como **http://example.com/mylob/businesstaxonomy/task/**
- **btt:TaskID1** – es el identificador de la Tarea. Cuando el identificador se añade a un espacio de nombres **btt** puede utilizarse para obtener información sobre la Tarea, como su nombre, descripción y estadísticas de utilización.
- **bttes** – es un espacio de nombres que apunta a un prefijo HTTP URL como **http://example.com/mylob/businesstaxonomy/task/execution/state**
- **bttes:200** – es un código del estado de ejecución de la Tarea, que indica que se ha ejecutado con éxito.
- **bttes:401** – es un código del estado de ejecución de la Tarea que indica que la ejecución no está autorizada.

Dado que las Tareas se referencian semánticamente en los ficheros registro, el examinador de acceso podrá analizar el historial de acceso del usuario y los accesos posibles del usuario en lo que respecta a la ejecución de tareas. Una vez que el acceso del usuario se ha examinado y analizado exhaustivamente, las correspondientes modificaciones resultantes de la conciliación se envían de vuelta a la Gestión de solicitudes de modificación de acceso para corregir cualquier derecho de acceso del usuario con privilegios excesivos o inferiores. Esta conciliación constituye un importante mecanismo de retroalimentación que caracteriza cualquier proceso en la forma de vida útil, es decir, la vida útil de los procesos IAM. Ahora bien, en el caso de pequeñas o medianas empresas, no serán necesarias todas las fases. Por ejemplo, la Ingeniería de lógica de autorización de aplicaciones se deja de lado o se realiza mediante un componente de directorio de usuarios. La Figura I.1 contiene solamente las partes esenciales de toda la vida útil del proceso IAM.

La siguiente lista jerárquica es una representación en texto de la vida útil del proceso IAM. Cada nodo de la taxonomía se define también en la cláusula 3.2. Para una representación codificada véase el esquema SKOS (sistema sencillo de organización de conocimientos) [b-Antonie].

1 Gestión de cambios corporativos

1.1 Ingeniería de taxonomía corporativa

1.1.1 Cambios de procesos corporativos

1.1.2 Cambios de productos corporativos

2 Ingeniería de acceso
- 2.1 Ingeniería de roles IAM
- 2.2 Ingeniería de lógica de autorización

3 Gestión de la identidad de las entidades
- 3.1 UIT-T X.1254 "Fase de inscripción" (Inscripción de entidades)
  - 3.1.1 Aplicación e inicialización
  - 3.1.2 Demostración de la identidad
  - 3.1.3 Verificación de la identidad
  - 3.1.4 Anotación en el registro
  - 3.1.5 Registro
- 3.2 X.1254 "Fase de gestión de credenciales" (Gestión de credenciales)
  - 3.2.1 Creación de la credencial
  - 3.2.2 Precreación de la credencial
  - 3.2.3 Inicialización de la credencial
  - 3.2.4 Vinculación de la credencial
  - 3.2.5 Expedición de la credencial
  - 3.2.6 Activación de la credencial
  - 3.2.7 Almacenamiento de la credencial
  - 3.2.8 Suspensión de la credencial
  - 3.2.9 Revocación de la credencial
  - 3.2.10 Destrucción de la credencial
  - 3.2.11 Renovación de la credencial
  - 3.2.12 Sustitución de la credencial
  - 3.2.13 Anotación en el registro

4 Asignación de acceso
- 4.1 Gestión de la solicitud de modificación de acceso
- 4.2 Gestión de permisos del usuario
- 4.3 Configuración de derechos del usuario

5 Operación de acceso
- 5.1 "Fase de autentificación de la entidad" UIT-T X.1254 (Autentificación)
  - 5.1.1 Anotación en el registro
  - 5.1.2 Autentificación de la sesión
- 5.2 Autorización
  - 5.2.1 Autorización de ejecutar Tareas
- 5.3 Registro de acceso a Tareas

6 Examen del acceso
- 6.1 Análisis
  - 6.1.1 Análisis de los posibles derechos de acceso
  - 6.1.2 Análisis del historial de acceso del usuario
- 6.2 Auditoría de acceso

7 Conciliación de acceso

Apéndice II

Propuesta de perfil de extensión SCIM 2.0

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

Se propone el siguiente perfil de extensión para el sistema de gestión de identidades entre dominios (SCIM), versión 2.0[1], basado en el protocolo de servicio web REST (transferencia de estado representacional) [b-SCIM REST]. En la Figura II.1 se ilustra la extensión propuesta. Las flechas y rectángulos en negro representan el núcleo de la actual especificación SCIM 1.0 [b-IETF SCIM 1.0]. Los dos rectángulos en azul ("roles" y "derechos") son los puntos de la extensión SCIM. Las flechas y rectángulos en línea continua de color naranja representan la extensión propuesta. Dado que la especificación SCIM deja la naturaleza semántica de los "roles" y "derechos" abierta a interpretación y definición por cada implementación[2], es posible especificar más concretamente los puntos de extensión que formarán parte del núcleo de la norma.

Para poder asignar significado corporativo a los roles IAM se formulan las siguientes recomendaciones como perfil de extensión de la actual especificación SCIM:

- El punto de extensión "roles" SCIM sirve de contenedor de los roles y cada rol está formado por una o varias tareas.
- El punto de extensión "derechos" SCIM sirve de contenedor de tareas adicionales que puede realizar el usuario (además de las tareas que puede realizar en virtud de los roles asignados).

---

1 "La especificación SCIM (sistema de gestión de identidades entre dominios) se ha concebido para facilitar la gestión de identidades en aplicaciones y servicios en la nube." Véase http://www.simplecloud.info/.

2 SCIM deja abierto a la interpretación y definición por las implementaciones lo siguiente:

"derechos

Una lista de derechos del usuario que representa algo que el usuario tiene. Es decir, un derecho es un derecho adicional a algo, un objeto o un servicio. No se especifica vocabulario ni sintaxis y cabe esperar que los proveedores de servicio/consumidores codifiquen información suficiente en el valor para poder determinar con exactitud y sin ambigüedades a qué tiene acceso el usuario. Este valor NO tiene tipos canónicos, aunque el tipo puede resultar útil como mecanismo para examinar derechos.

roles

Una lista de roles para el usuario que representan en conjunto quién es el usuario; por ejemplo, "estudiante", "facultad". No se especifica vocabulario o sintaxis, pero se espera que el valor del rol sea una cadena o etiqueta que represente un conjunto de derechos. Este valor NO tiene tipos canónicos." Véase https://tools.ietf.org/html/draft-ietf-scim-core-schema-22.

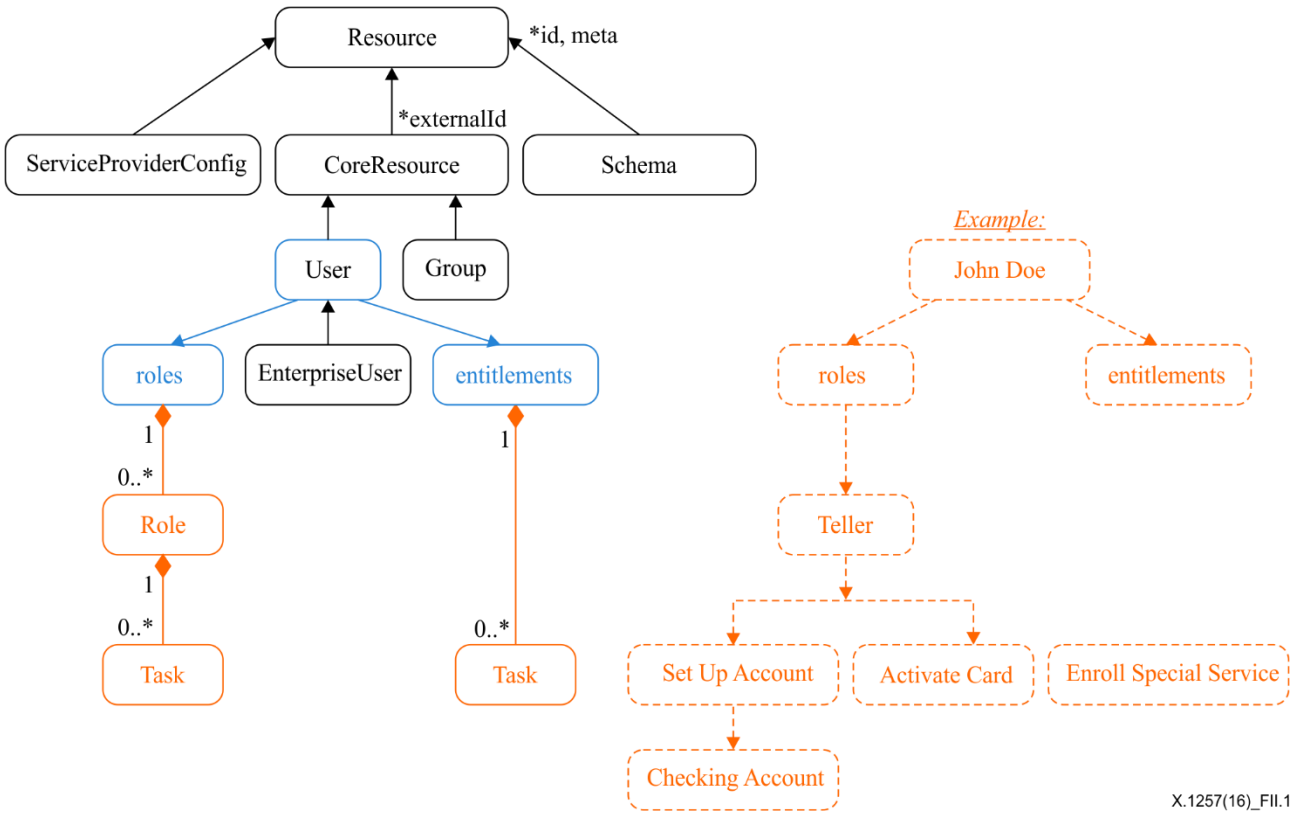

Figura II.1 – Extensión del perfil SCIM

El ejemplo de la derecha en color naranja ilustra cómo un usuario con el rol de "cajero" que consiste en dos tareas: "crear cuenta" y "activar tarjeta". La otra tarea – "inscribir en servicios especiales" es un derecho directo adicional para el que aún no es necesario crear un rol.

Apéndice III

Extensión propuesta al perfil XACML 3.0

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

A fin de alcanzar los objetivos de calidad de datos IAM descritos en el presente documento, se propone el siguiente perfil de extensión.

La propuesta consiste en introducir un nuevo tipo de política XACML 3.0 [b-OASIS XACML 3.0] – Política tipo asignación (marcada con un círculo rojo) – política que se evalúa durante el tiempo de petición de acceso. Como ejemplo puede citarse la política de acceso para aplicar la Separación de funciones (SoD) durante el tiempo de asignación de acceso. Por otra parte, el tipo de política de acceso (rodeado con un círculo rojo en línea discontinua) es una política que se evalúa en tiempo de ejecución y suele ser más compleja (granularidad fina). En la Figura III se muestra un fragmento del esquema IAM en que se insiste en la política de asignación propuesta.

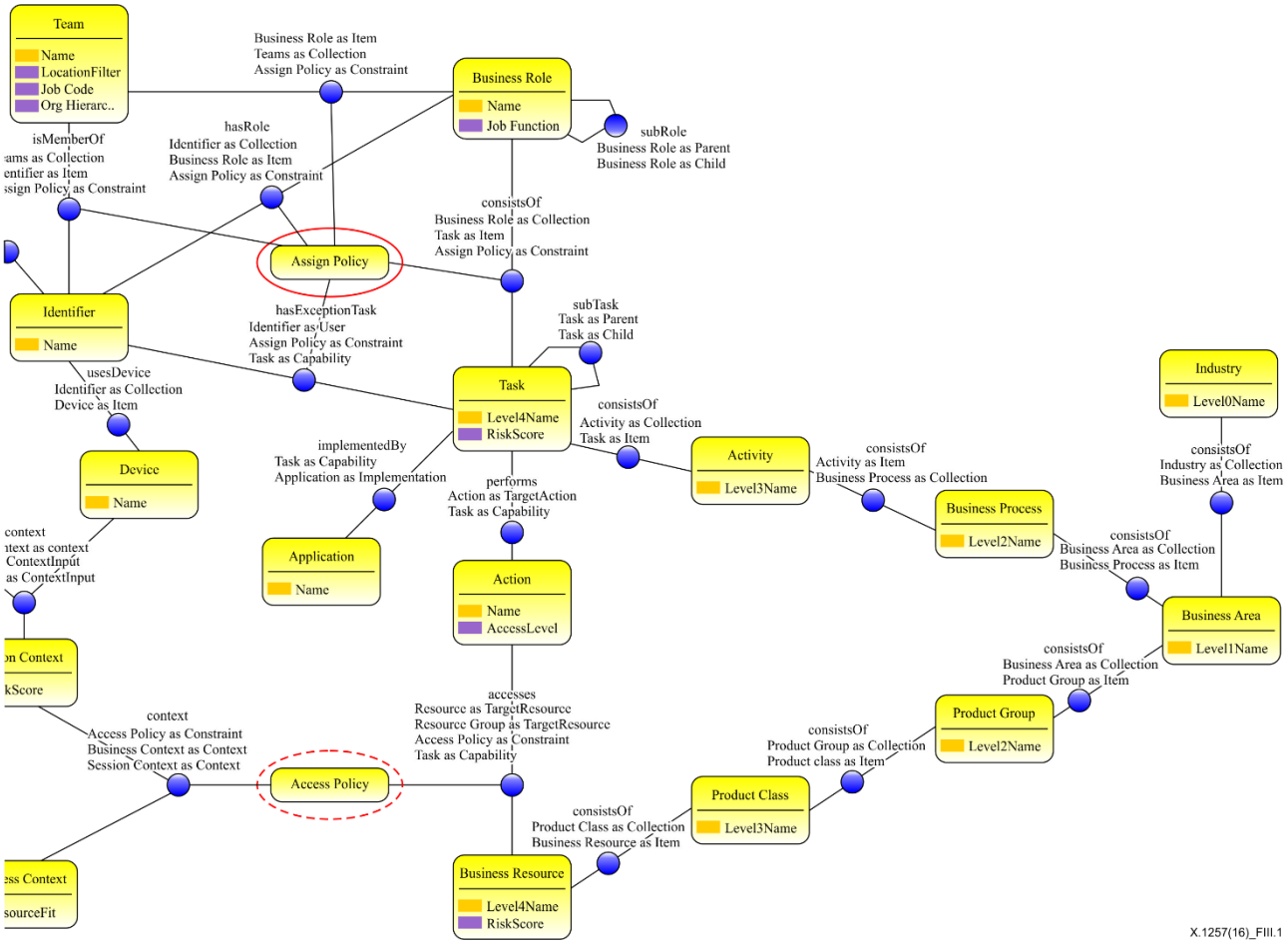

Figura III.1 – Fragmento del esquema IAM donde se indica la Política de Asignación

Semántica corporativa para el modelo XACML:

a) Atributos de recursos de referencia mediante un id concepto de recursos. El recurso es el nodo extremo de la taxonomía de productos.

b) atributos de acción de referencia mediante un id concepto de Tarea y Acción. Tarea es el nodo extremo de la taxonomía de procesos. Acción es la operación realizada por la tarea en el recurso.

c) Atributos del entorno de referencia mediante un id concepto de contexto corporativo y contexto de sesión. El contexto corporativo podría proporcionar atributos corporativos de granularidad fina, tales como un filtro por número de cuenta. El contexto de la sesión que conoce el estado de autentificación (metadatos de dispositivos y credenciales) podría suministrar información como la dirección del protocolo Internet (IP) y la dirección del dispositivo MAC (control de acceso al medio) para la autorización de granularidad fina técnica.

En la Figura III.2 se muestra la extensión semántica propuesta para el modelo XACML.

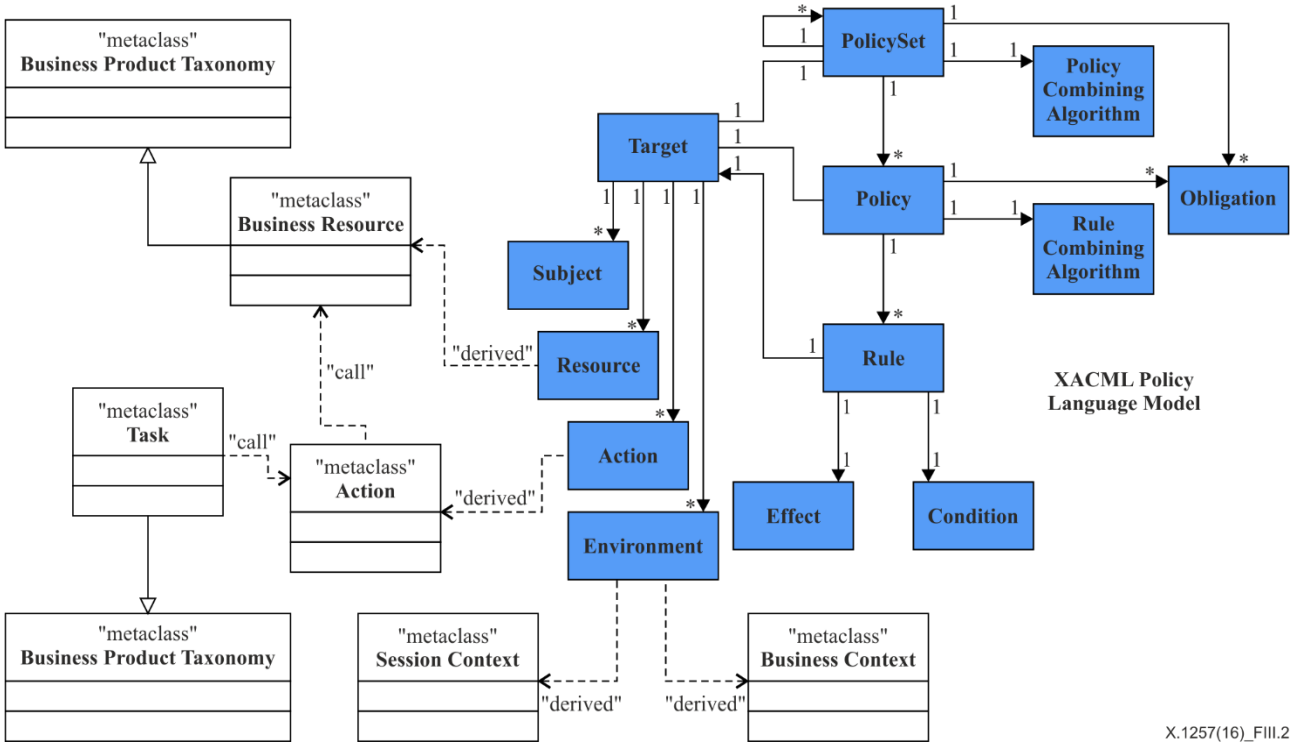

Figura III.2 – Extensión semántica propuesta al modelo XACML

Apéndice IV

Casos de utilización de la gestión de acceso basado en Tareas

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

A continuación figuran casos de utilización pertinentes que ilustran la utilidad de la presente Recomendación:

1 Política de acceso:

a) El usuario A tiene derecho a realizar las tareas A, B y C mediante el rol A.

b) El usuario A también tiene derecho a realizar la tarea D por derecho directo.

c) La política A especifica que las tareas B y D son mutuamente excluyentes para el mismo número de cuenta.

d) Se evalúa la política A y se obtiene la decisión de prohibición para el caso antes mencionado.

2 Notificación de acceso (derechos):

a) Se aprovechan los conceptos de tareas para mejorar la legibilidad y el significado de los esfuerzos para describir los actuales derechos del lenguaje corporativo.

b) Se aprovechan los conceptos de recursos corporativos para mejorar la legibilidad y significado de los esfuerzos para describir los actuales derechos del lenguaje corporativo.

3 Utilización de Tareas

a) Se aprovecha una aplicación web de referencia existente y:

i) se configura la plantilla de registro de la aplicación para utilizar id de tareas;

ii) se generan ficheros registro durante el tiempo de ejecución de la aplicación.

b) Se analizan los ficheros registro de la aplicación con una herramienta analítica para:

i) informar sobre las tareas que se están utilizando durante el tiempo de ejecución de producción;

ii) actualizar la taxonomía con la información estadística anterior.

4 Utilización de derechos

a) Se aprovecha una aplicación web de referencia existente y:

i) se configura la plantilla de registro de la aplicación para utilizar los id de tareas;

ii) se generan ficheros registro durante el tiempo de ejecución.

b) se analizan los ficheros registro de la aplicación con una herramienta analítica para:

i) correlacionar eventos de ejecución de tareas sobre la base del identificador de Tareas;

ii) correlacionar eventos de denegación de autorizaciones sobre la base del identificador de Tareas;

iii) Producir informes sobre situaciones contradictorias de SoD producidas en el pasado.

Apéndice V

Posibles mecanismos para la implementación de la interfaz de taxonomía corporativa

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

Las soluciones basadas en normas, tales como el vocabulario controlado SKOS[3] [b-Antonie] o un mecanismo de registro de metadatos, pueden facilitar el registro e identificación de conceptos de taxonomía corporativa. SKOS resulta especialmente útil para representar relaciones jerárquicas.

Otra posible solución es utilizar la serialización basada en la notación de objetos JavaScript (JSON) para enlaces de datos (JSON-LD) [b-W3C JSON-LD] también denominada Datos vinculados JSON. Aunque JSON-LD permite mezclar varios vocabularios controlados y puede representar relaciones gráficas complejas no existe una norma para la interfaz de taxonomía. Al día de hoy no existen implementaciones REST ni del protocolo sencillo de acceso a objetos (SOAP).

[3] SKOS proporcionar relaciones jerárquicas básicas, tales como mayor o menor, pero no permite especificar relaciones ontológicas más específicas que pudieran ser necesarias para expresar la sintaxis y el significado de elementos de datos IAM.

Apéndice VI

Normas de taxonomía de procesos corporativos

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

En esta Recomendación se hace referencia como mínimo a dos tipos de taxonomías corporativas: taxonomía de procesos corporativos y taxonomía de productos corporativos. Estos términos están acuñados por los organismos de normalización de procesos corporativos como el Foro de TeleManagement del Mapa de Operaciones de Telecomunicaciones (eTOM) y la clasificación central de productos (CPC) [b-CPC].

En el ejemplo de la Figura VI.1 siguiente se muestra un marco de clasificación de procesos (PCF) del American Productivity and Quality Center (APQC) [b-APQC-PCF] y se ilustra cómo se pueden clasificar los procesos.

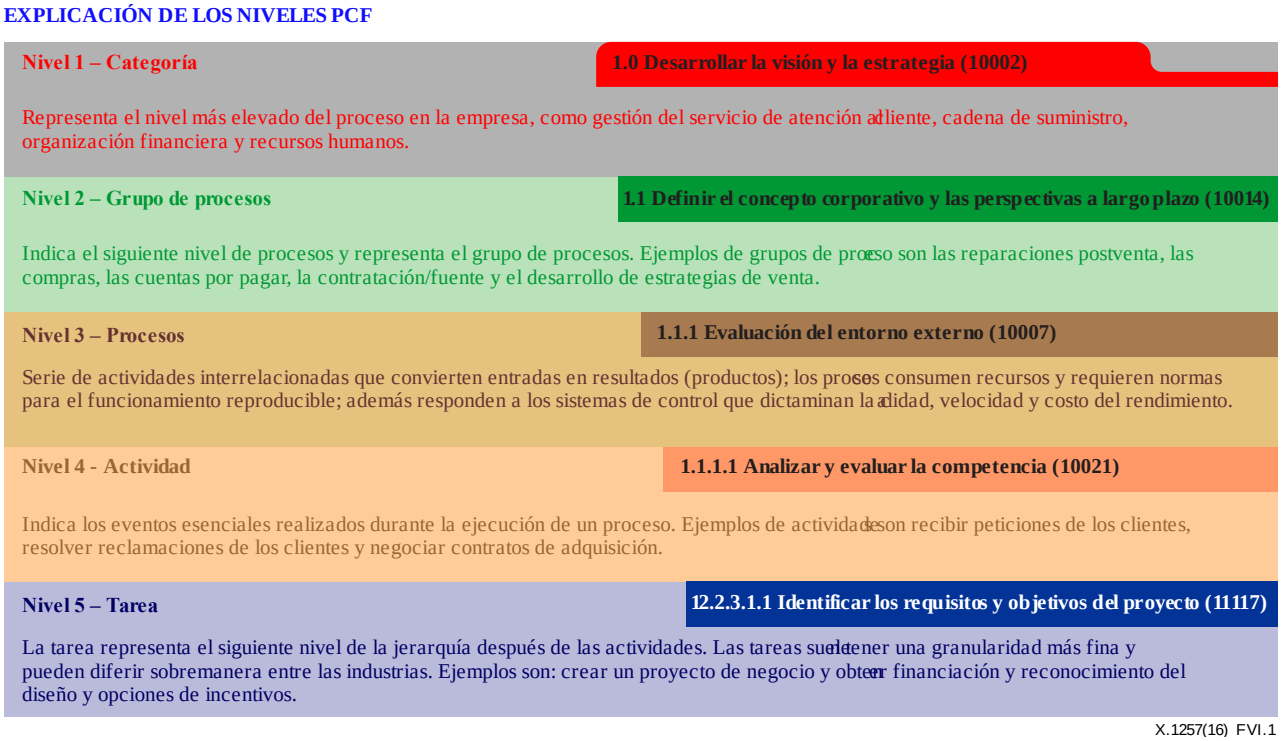

Figura VI.1 – Definiciones de la estructura de la taxonomía de procesos PCF

Apéndice VII

Modelo de dominio de ontología IAM

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

En la Figura VII.5 se muestra todo el modelo del dominio ontológico IAM. Para facilitar la lectura del dominio IAM se presentan en primer lugar las siguientes áreas temáticas de IAM:

- Figura VII.1, modelo del dominio IAM – Área temática de usuario
- Figura VII.2, modelo del dominio IAM – Área temática de asignación de acceso
- Figura VII.3, modelo del dominio IAM – Área temática de control de acceso
- Figura VII.4, modelo del dominio IAM – Área temática de dominio corporativo.

Y por último se fusionan estas áreas temáticas en el modelo íntegro del dominio IAM de la Figura VII.5. Así, la primera área temática trata de los tipos de concepto de usuario. Según [UIT-T X.1252] y [UIT-T X.1254] el usuario se representa mediante una entidad desde algunas perspectivas, como el ser o la existencia de un sujeto. Una entidad tiene una o varias identidades. Una identidad tiene uno o varios identificadores.

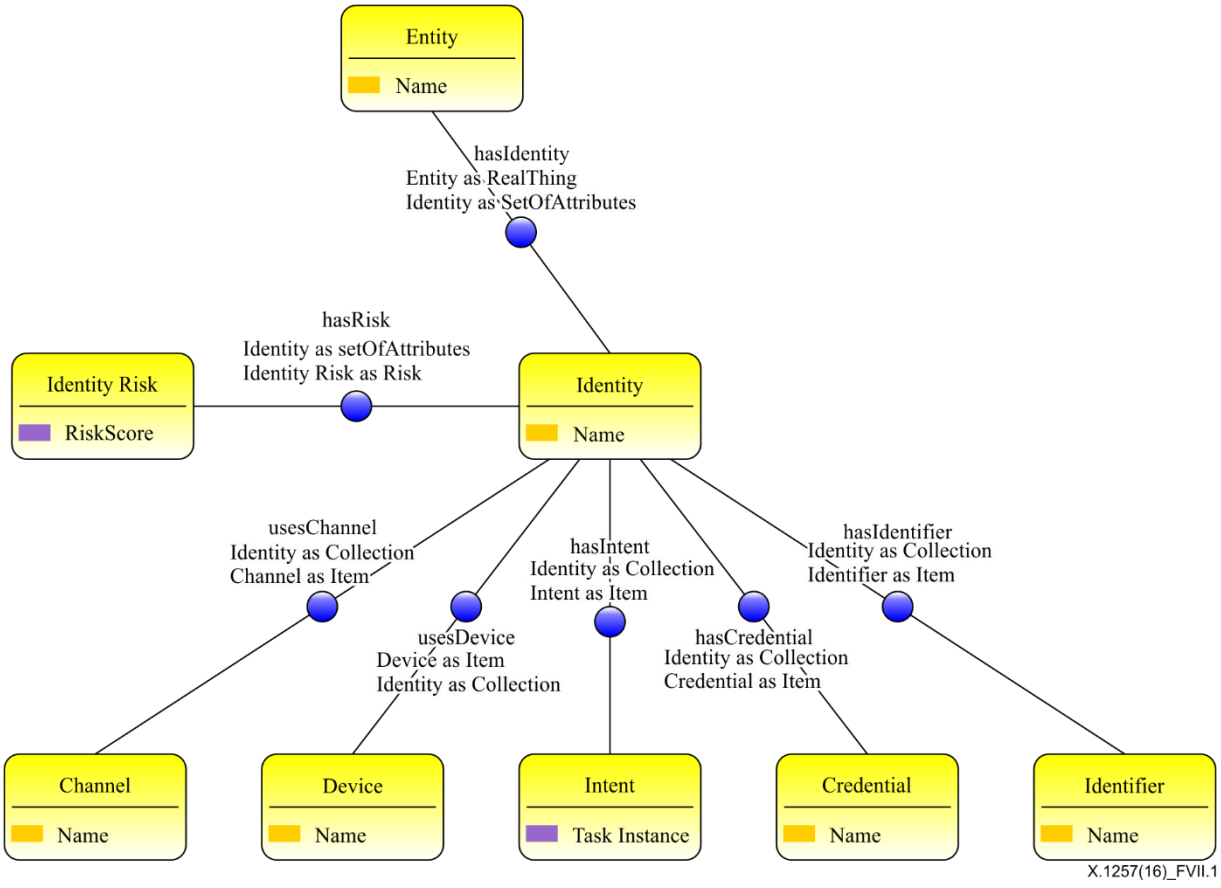

Figura VII.1 – Modelo de dominio IAM – área temática de usuario

Ejemplo: Un ser humano consta de una entidad que se caracteriza por nombre, fecha de nacimiento, etc. Este ser humano puede ser al mismo tiempo un empleado y un cliente y, por tanto, puede tener dos identidades. Además, el empleado tiene un identificador EmployeeID y el cliente tiene un identificador CustomerID.

NOTA – En algunos casos, el rol del ser humano puede desempeñarlo un dispositivo que actúa en su nombre.

En la Figura VII.2 se ilustra el área temática de asignación de acceso, que trata de la Asignación al usuario de derechos de acceso por medio de sus identificadores. Los derechos de acceso pueden asignarse al usuario por medio de los equipos de los cuales es miembro. El Equipo en este contexto es un contenedor de derechos de acceso basados en recursos humanos. El usuario puede obtener sus derechos de acceso por medio del rol que desempeña además de los derechos de acceso de miembro de un equipo. Y por último, el usuario puede excepcionalmente el tener derecho a realizar determinadas tareas. En definitiva, los derechos de acceso son una colección de tareas que el usuario puede realizar. Ahora bien, toda asignación de usuario a tareas se evalúa mediante ciertos derechos aplicables, denominados "Políticas de asignación", que prohíben combinaciones de derechos peligrosas y aplican las reglas de Separación de funciones (SoD).

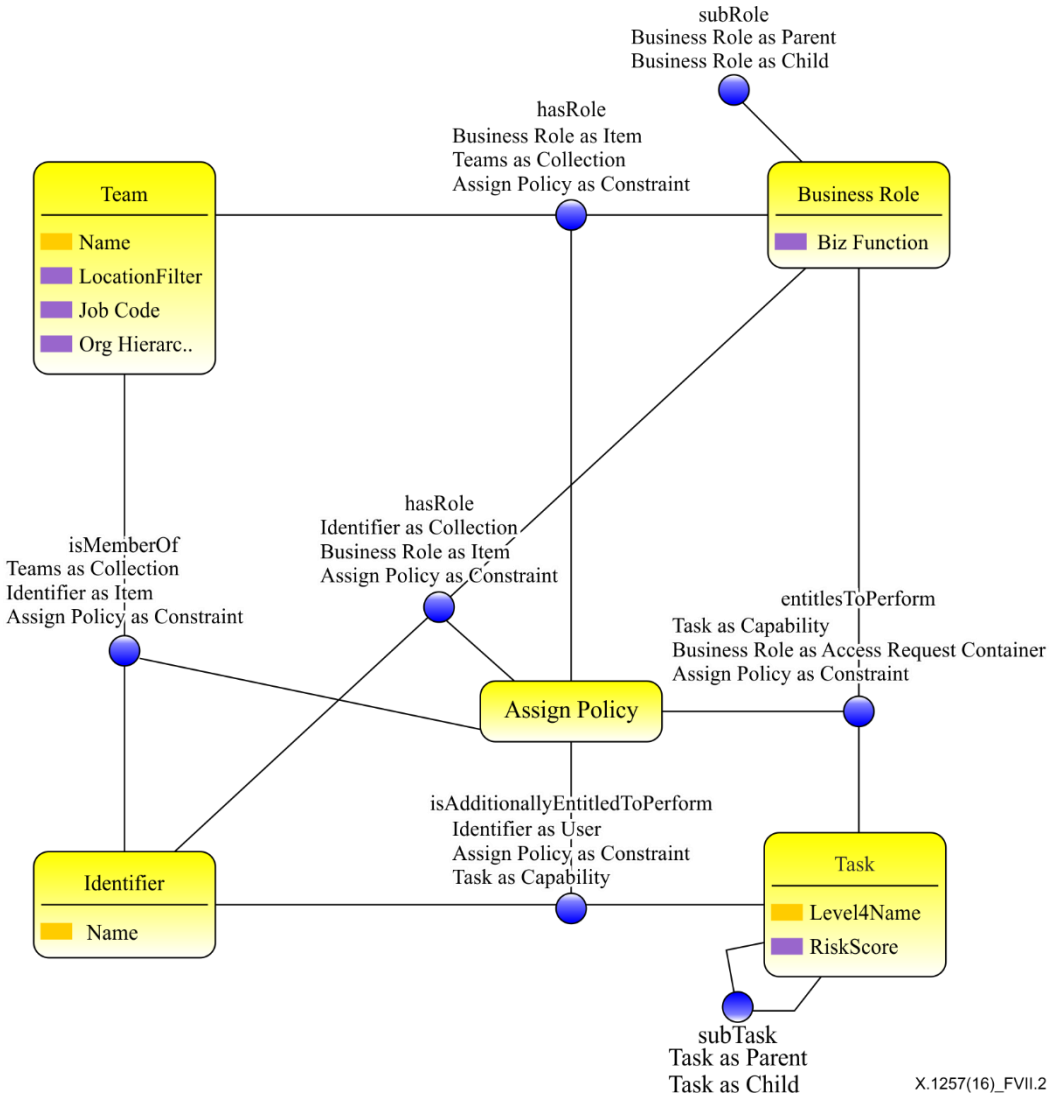

Figura VII.2 – Modelo de dominio IAM – Área temática de asignación de acceso

Ejemplo: El usuario A es miembro del equipo X. Cada miembro del equipo X que se encuentra en la sede (es decir Región=principal, Mostrador=principal) tiene cinco roles y cada rol otorga al usuario el derecho de realizar 10 tareas. Así cualquier miembro del equipo X puede, en principio, realizar 50 tareas. Además, el usuario A tiene asignados tres roles más que le dan derecho a realizar 5 Tareas adicionales. El usuario A también está autorizado excepcionalmente a realizar una tarea más. Al final el usuario A tiene derecho a realizar 66 Tareas distintas. Sin embargo, los miembros del equipo que no están ubicados en la sede tendrán sólo tres roles, es decir, 30 tareas menos.

La siguiente área temática – control de acceso – realiza la autorización basada en políticas y tareas y en los derechos del usuario y el contexto de la sesión. Una determinada tarea accede a ciertos recursos si la correspondiente política de acceso lo permite. La política de acceso evalúa sus reglas con arreglo al contexto de sesión y las correspondientes restricciones de acceso del usuario. El contexto de la sesión dispondrá de metadatos de autentificación del usuario, tales como canal, dispositivo, intención, credencial e identificador.

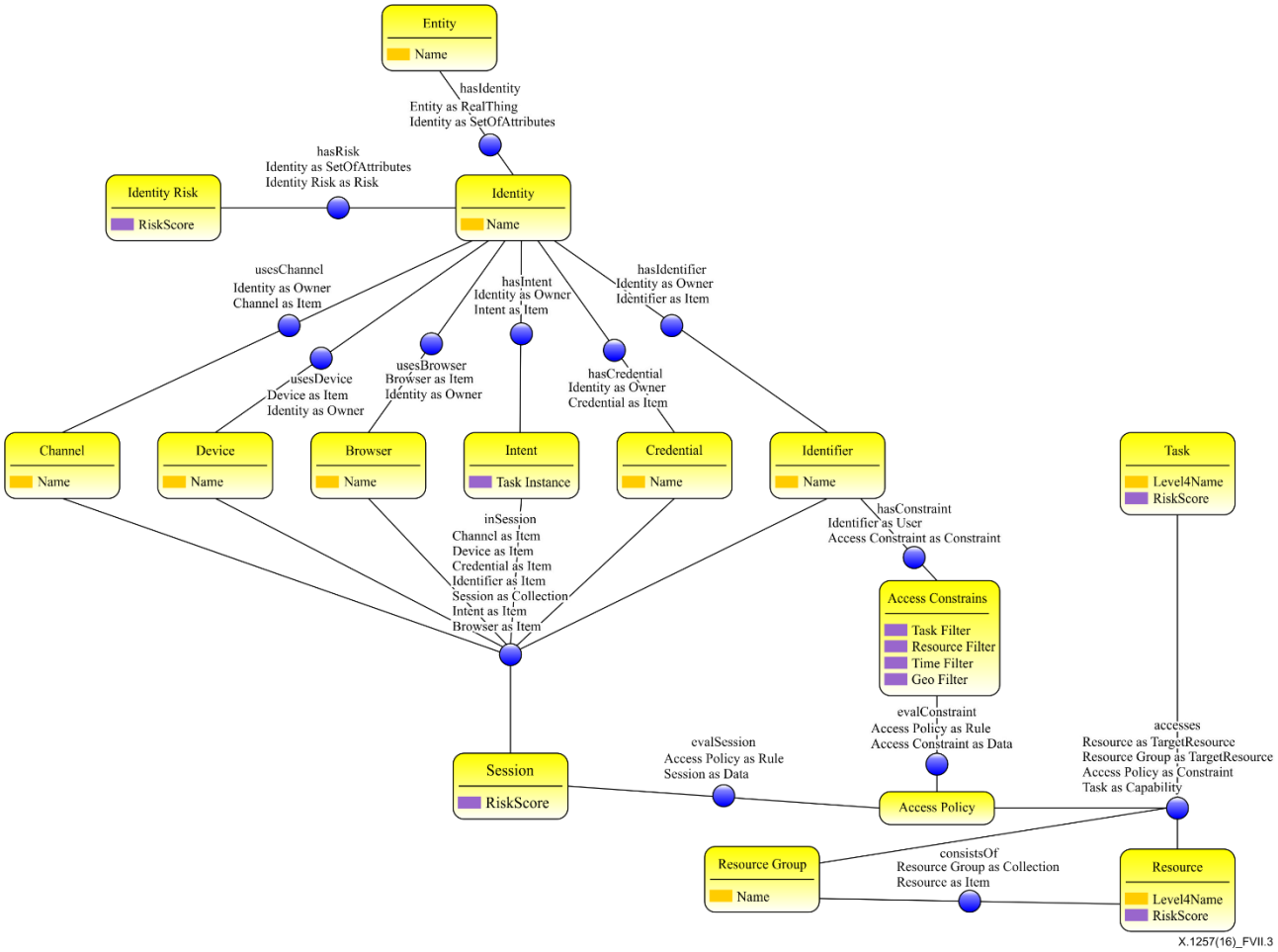

Figura VII.3 – Modelo de dominio IAM – Área temática de control de acceso

Ejemplo: El usuario A intenta realizar la tarea "crear cuenta". Esta tarea accede (es decir, crea) un recurso "cuenta corriente superior". Este acceso se produce si al evaluar la correspondiente política de acceso se obtiene verdadero. La política de acceso garantiza que el usuario del caso utilice un canal adecuado para esta transacción y que la dirección IP se encuentra dentro de la gama válida de direcciones IP. La política también puede consultar un depósito transitorio de tareas no permitidas en ese momento porque ya han pasado las horas de oficina.

La última área temática – taxonomía corporativa – ilustra la interconexión entre el domino IAM y el dominio corporativo. La taxonomía corporativa está formada por procesos y productos. Puede observarse (de derecha a izquierda) que las áreas industria y negocio son los dos primeros niveles de esta taxonomía. A la izquierda del sector de actividad figuran dos estructuras jerárquicas relacionadas – taxonomía de procesos y taxonomía de productos. Por lo general la tarea es un nodo extremo en la taxonomía de procesos y el recurso es un nodo extremo en la taxonomía de productos. La aplicación implementa las correspondientes tareas y accede a los recursos en nombre del usuario.

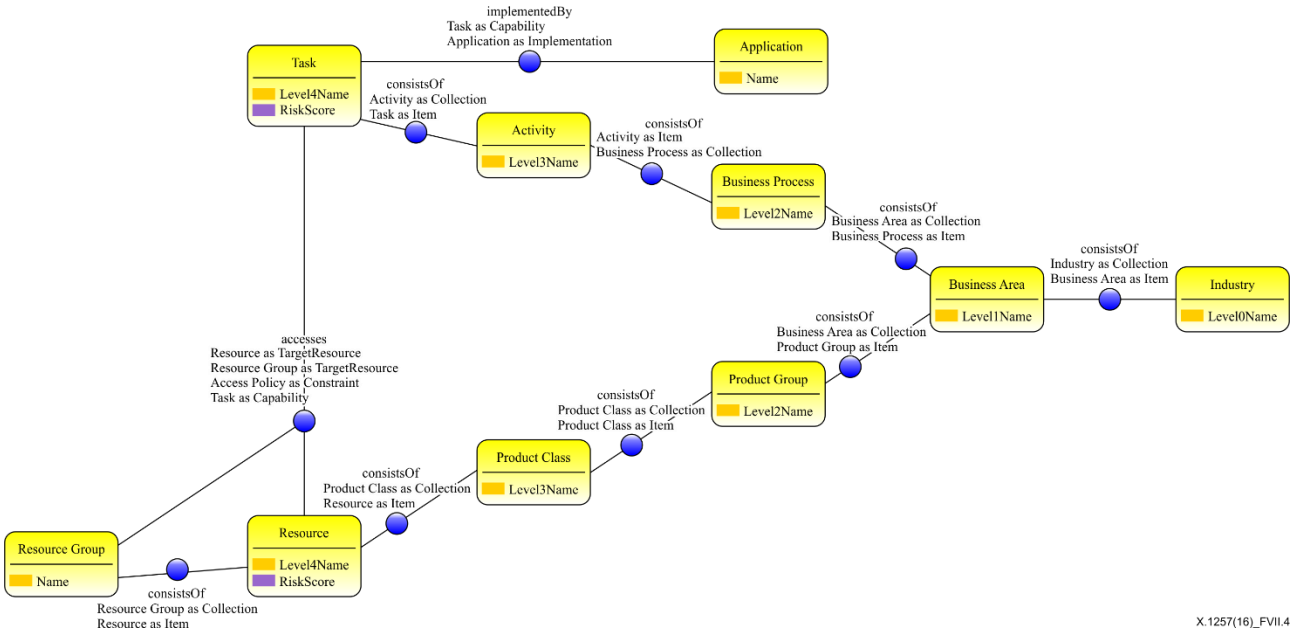

Figura VII.4 – Modelo del dominio IAM – Área temática dominio de actividad

Ejemplo: Industria financiera cuyo sector de actividad es un servicio de atención al cliente. El proceso corporativo es origen. La actividad es actividad de las cuentas. La tarea es "crear cuenta". Desde la perspectiva de la taxonomía de productos – el grupo de productos es cuenta, la clase de producto es cuenta corriente y el recurso es "cuenta corriente superior."

Por último, en la Figura VII.5 siguiente se ilustra el modelo íntegro del dominio IAM en el que se conjugan las cuatro áreas temáticas antes descritas.

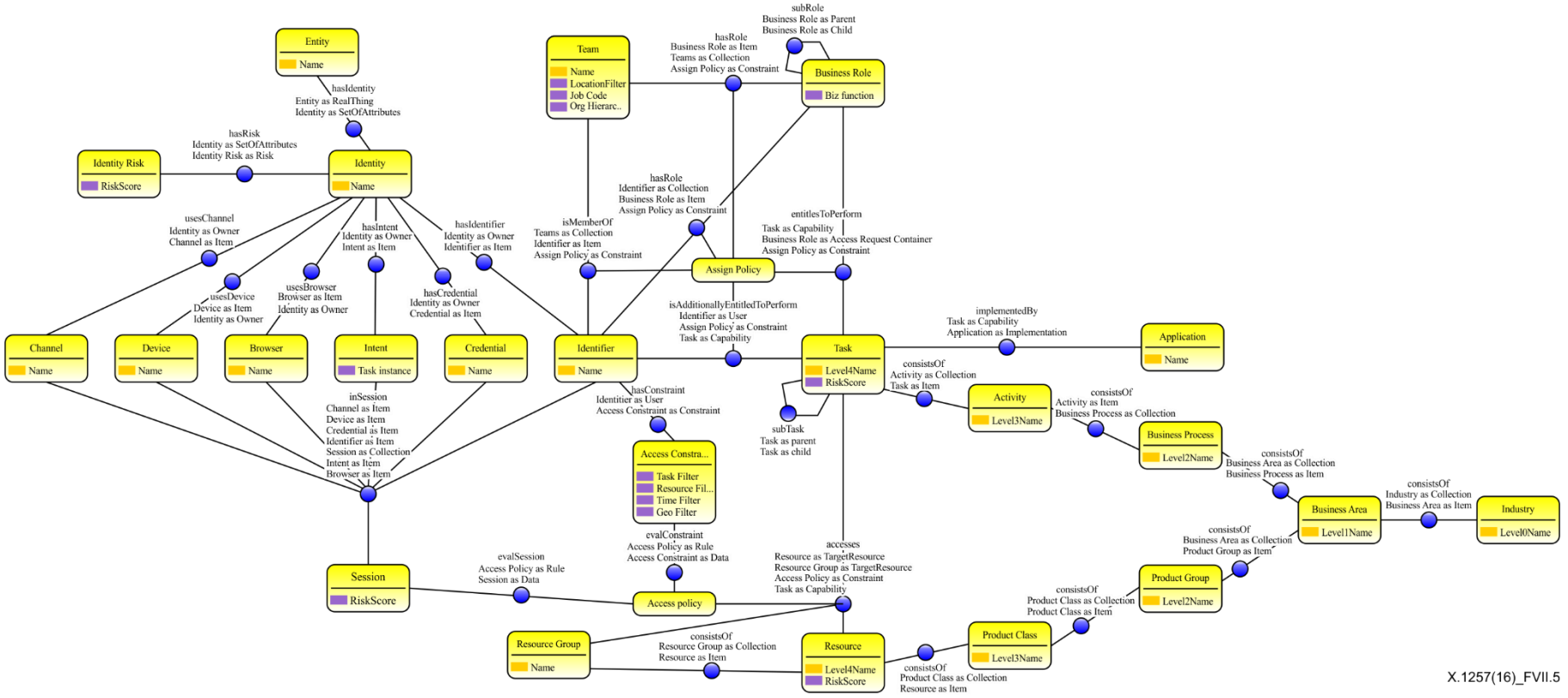

Figura VII.5 – Modelo del dominio IAM

El modelo del dominio IAM de la Figura VII.5 muestra las relaciones entre los conceptos con arreglo a los requisitos estipulados en la correspondiente sección. El diagrama representa los siguientes principios claves:

- El usuario se representa por su entidad, identidad, identificadores y otras características. Durante el proceso de asignación de derechos, el usuario puede tener derecho a realizar tareas específicas derivadas de equipo y rol (normalmente en el 80% de los casos) o se le puede haber asignado directamente una tarea específica (una excepción en el 20% de los casos).
- El Equipo es un contenedor de roles de recursos humanos. La principal finalidad de los tipos de roles y de equipos es acelerar y simplificar la asignación de derechos y el proceso de aprobación.
- Los roles heredan el significado corporativo de las correspondientes tareas.

NOTA – Actualmente los roles IAM son creados y mantenidos por el servicio IT y, por consiguiente, no tienen un significado corporativo directo trazable. En muchos casos, basarse en un nombre de rol solamente para obtener el significado administrativo no es suficiente para examinar debidamente los derechos de acceso.

- Las tareas son nodos extremos de la taxonomía de procesos creados y mantenidos por arquitectos y diseñadores.
    - Las tareas suelen ser más granulares que las aplicaciones que las implementan.
    - Las tareas son implementadas por las correspondientes aplicaciones.
    - Las tareas representan las funciones con arreglo a casos de utilización de Separación de funciones (SoD).

NOTA – Es imposible aplicar la SoD sin las tareas subyacentes.

- El usuario no tiene acceso directo a los recursos. En cambio el usuario tiene derecho a realizar una tarea y la tarea accede a los recursos en nombre del usuario.
- Proceso-Actividad-Tarea es una estructura lógica y forma parte de la taxonomía de procesos para identificar y organizar procesos corporativos de manera normalizada [b-APQC PCF 5.0.1] y su mantenimiento suele estar a cargo de los arquitectos y diseñadores.
- El Recurso Grupo de productos-Clase de productos es una estructura lógica y forma parte de la taxonomía de productos para identificar y organizar productos de manera normalizada [b-CPC Ver 2] y su mantenimiento suele estar a cargo de los arquitectos y diseñadores.
- La política de asignación es un mecanismo de restricción de asignaciones de derechos utilizado durante la fase de asignación de derechos para impedir el fraude y combinaciones estáticas de tareas peligrosas.
- La Política de acceso es un mecanismo de restricción de operaciones de acceso en la fase de acceso en tiempo de ejecución para impedir el fraude y combinaciones dinámicas peligrosas.
- Los Recursos son conceptos tales como historial del paciente, cuenta de préstamos y cuenta corriente. Permiten la asignación de derechos a nivel de recursos con granularidad fina y el control de acceso.
- Los derechos son tareas que el usuario tiene derecho a realizar (es decir, derechos de granularidad gruesa).
- Los permisos son tareas que acceden a recursos específicos y tan restringidos por una política.
- Durante la configuración de derechos del usuario se pueden hacer corresponder esos derechos con los correspondientes permisos del sistema, de ser necesario.
- Los permisos del sistema tratan de recursos del sistema, tales como bases de datos, cuadros, columnas, filas o conjunto de datos del sistema central.

Bibliografía

[b-UIT-T X.1255] Recomendación UIT-T X.1255 (2013), *Marco para la indagación de información de gestión de identidades.*

[b-ISO/IEC 24760-1] ISO/IEC 24760-1:2011, *Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts*.

[b-Antonie] Antoine Isaac, E.S. (2009), *SKOS simple knowledge organization system primer*.
http://www.w3.org/TR/skos-primer/ (extraído el 18 de mayo de 2016)

[b-APQC-PCF] Tesmer, John (2014), *Process Classification Framework 6.1.1*.
http://www.apqc.org/process-classification-framework (extraído el 18 de mayo de 2016)

[b-APQC PCF 5.0.1] APQC PCF. (2011), *Banking Process Classification Framework*.
http://www.apqc.org/knowledge-base/download/33193/PCF_Banking_Ver_5.0.1_2011.pdf
(extraído el 18 de mayo de 2016)

[b-CPC] http://en.wikipedia.org/wiki/Central_Product_Classification.

[b-CPC Ver 2] CPC Workgroup. (2008), *Central Product Classification, Ver.2, Detailed structure and explanatory notes*. http://unstats.un.org/unsd/cr/registry/regcst.asp?Cl=25
(extraído el 18 de mayo de 2016)

[b-example] http://www.apqc.org/knowledge-base/documents/apqc-process-classification-framework-pcf-banking-excel-version-501

[b-IETF SCIM 1.0] C. Mortimore, Ed. (2013), *System for Cross-Domain Identity Management: Core Schema*. http://tools.ietf.org/html/draft-ietf-scim-core-schema-01
(extraído el 18 de mayo de 2016)

[b-IETF SCIM 2.0] Hunt, e.a. (2015), *System for Cross-Domain Identity Management: Core Schema*. https://tools.ietf.org/html/draft-ietf-scim-core-schema-22 (extraído el 18 de mayo de 2016)

[b-NIST-RBAC 2000] Sandhu, R., David, F., & Khun, R. (2000), *The NIST Model for Role-Based Access Control: Towards A Unified Standard*.

[b-OASIS XACML 3.0] Erik Rissanen. (2013), *eXtensible Access Control Markup Language (XACML) Version 3.0*.
http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html (extraído el 18 de mayo de 2016)

[b-OBAC] Mohammad, A. (2011), *Ontology-Based Access Control Model for Semantic Web.*
http://www.worldacademicunion.com/journal/1746-7659JIC/jicvol6no3paper03.pdf (extraído el 18 de mayo de 2016)

[b-schema.org 2011] Google, Yahoo, Bing, Yandex. (2011), *schema.org*.
http://schema.org (extraído el 18 de mayo de 2016)

[b-SCIM REST] SCIM 2.0 REST web service protocol, C. Mortimore, Ed., (2013),
http://www.simplecloud.info/ (extraído el 18 de mayo de 2016)

[b-W3C JSON-LD] Manu Sporny. (2013), *JSON-LD 1.0, A JSON-based* Serialization *for Linked Data*.
http://json-ld.org/spec/latest/json-ld/ (extraído el 18 de mayo de 2016)

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	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás 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, 2016