Política de servicios DSS

EADTRUST

(**E**uropean **A**gency of **D**igital **Trust,** S.L.)

Miembro de

Observatorio del Notariado para la Sociedad de la Información

UBL

cen European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

AENOR
Asociación Española de Normalización y Certificación

FORO evidencias electrónicas

Histórico de versiones			
Versión	Fecha	Documentos sustituidos	Descripción / Detalles
2	9/09/09		

Cambios desde la última versión
Maquetación corporate

Difusión	
Propietario:	EADTrust, S.L
Preparado por:	Ivan Basart
Modificado por	
Aprobado por:	
Firma:	
Fecha:	9 de Septiembre 2009
Distribución:	

Referencias de archivo	
Nombre archivo:	Política de Servicios DSS EADTrust

CONTENIDO

A. INTRODUCCIÓN 6

A.1 Presentación 6
A.2 Opciones del servicio 6
A.3 Identificación del Documento 7
A.4 Participantes en los servicios DSS 7
A.4.1 Prestador de Servicios DSS 7
A.4.2 Terceros de confianza 7
A.4.3 Entidades y usuarios finales 7
A.4.4 Suscriptores 8
A.4.5 Terceros 8
A.5 Uso de los servicios DSS 8
A.5.1 Usos permitidos 8
A.5.2 Límites y prohibiciones de uso 8
A.5.3 Límites de uso 8
A.5.4 Prohibiciones de usos 8
A.6 Administración de la política 9
A.6.1 Organización que administra el documento 9
A.6.2 Datos de contacto de la organización 9
A.6.3 Procedimientos de gestión del documento 9

B. PUBLICACIÓN DE INFORMACIÓN 10

B.1 Publicación de información 10
B.2 Frecuencia de publicación 10
B.3 **Control de acceso** 10

C. REQUISITOS DE OPERACIÓN 11

C.1 Solicitud 11
C.1.1 Legitimación suscriptor 11
C.1.2 Procedimiento de alta 11
C.1.2.1 Certificado de Suscriptor 12
C.1.2.1.1 Generación de Claves 12
C.1.2.1.2 Envío de la clave pública el emisor del certificado 12
C.1.2.1.3 Instalación del certificado 12
C.2 Procesamiento de las solicitudes 12
C.3 Respuesta a las solicitudes 12
C.4 Finalización de la suscripción 13

D. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES 14

D.1 Controles de seguridad física 14
D.1.1 Localización y construcción de las instalaciones 15
D.1.2 Acceso físico 15
D.1.3 Electricidad y aire acondicionado 15
D.1.4 Exposición al agua 15
D.1.5 Prevención y protección de incendios 16
D.1.6 Almacenamiento de soportes 16
D.1.7 Tratamiento de residuos 16
D.1.8 Copia de respaldo fuera de las instalaciones 16
D.2 Controles de gestión 16
D.2.1 Funciones fiables 16
D.2.2 Roles que requieren separación de tareas 17
D.3 Controles de personal 17
D.3.1 Requisitos de historial, calificaciones, experiencia y autorización 17

D.3.2 Procedimientos de investigación de historial 18
D.3.3 Requisitos de formación 18
D.3.4 Secuencia y frecuencia de rotación laboral 18
D.3.5 Sanciones para acciones no autorizadas 19
D.3.6 Requisitos de contratación de profesionales externos 19
D.3.7 Suministro de documentación al personal 19
D.4 Procedimientos de auditoría de seguridad 19
D.4.1 Tipos de eventos registrados 19
D.4.2 Frecuencia de tratamiento de registros de auditoría 20
D.4.3 Periodo de conservación de registros de auditoría 20
D.4.4 Protección de los registros de auditoría 20
D.4.5 Procedimientos de copia de respaldo 20
D.4.6 Localización del sistema de acumulación de registros de auditoría 20
D.4.7 Notificación del evento de auditoría al causante del evento 20
D.4.8 Análisis de vulnerabilidades 20
D.5 Archivo de informaciones 21
D.5.1 Tipos de eventos registrados 21
D.5.2 Periodo de conservación de registros 21
D.5.3 Protección del archivo 21
D.5.4 Procedimientos de copia de respaldo 22
D.5.5 Localización del sistema de archivo 22
D.5.6 Procedimientos de obtención y verificación de información de archivo 22
D.6 Renovación de claves 22
D.7 Compromiso de claves y recuperación de desastre 22
D.7.1 Corrupción de recursos, aplicaciones o datos 22
D.7.2 Compromiso de la clave privada de suscriptor 22
D.7.3 Desastre sobre las instalaciones 22
D.8 Terminación del servicio 23

E. CONTROLES DE SEGURIDAD TÉCNICA 24

E.1 Protección de las claves privadas 24
E.1.1 Estándares de módulos criptográficos 24
E.1.2 Control por más de una persona sobre las claves privadas 24
E.1.3 Repositorio de la clave privada 24
E.1.4 Copia de respaldo de la clave privada 24
E.1.5 Archivo de la clave privada 24
E.1.6 Introducción de la clave privada en el módulo criptográfico 24
E.1.7 Método de activación de la clave privada 25
E.1.8 Método de desactivación de la clave privada 25
E.1.9 Método de destrucción de la clave privada 25
E.2 Otros aspectos de gestión de claves 25
E.2.1 Periodos de utilización de las claves pública y privada 25
E.3 Controles de seguridad informática 25
E.3.1 Requisitos técnicos específicos de seguridad informática 25
E.3.2 Evaluación del nivel de seguridad informática 26
E.4 Controles técnicos del ciclo de vida 26
E.4.1 Controles de desarrollo de sistemas 26
E.4.2 Controles de gestión de seguridad 26
E.4.3 Evaluación del nivel de seguridad del ciclo de vida 26
E.5 Controles de seguridad de red 26
E.6 Controles de ingeniería de módulos criptográficos 27

F. AUDITORIA DE CONFORMIDAD 28

F.1 Frecuencia de la auditoria de conformidad 28
F.2 Identificación y calificación del auditor 28
F.3 Relación del auditor con la entidad auditada 28
F.4 Listado de elementos objeto de auditoria 28
F.5 Acciones a emprender como resultado de una falta de conformidad 28

G. REQUISITOS COMERCIALES Y LEGALES 30

G.1 Tarifas 30
G.1.1 Tarifa de servicios 30
G.1.2 Tarifas de otros servicios 30
G.1.3 Política de reintegro 30
G.2 Capacidad financiera 30
G.2.1 Otros activos 30
G.3 Confidencialidad 30
G.3.1 Informaciones confidenciales 30
G.3.2 Informaciones no confidenciales 30
G.3.3 Divulgación legal de información 30
G.3.4 Divulgación de información por petición de su titular 31
G.3.5 Otras circunstancias de divulgación de información 31
G.4 Protección de datos personales 31
G.5 Derechos de propiedad intelectual 31
G.6 Obligaciones y responsabilidad civil 31
G.6.1 Obligaciones de EADTRUST (European Agency of Digital Trust) 31
G.6.2 Garantías ofrecidas a suscriptores y terceros 31
G.6.3 Rechazo de otras garantías 32
G.6.4 Limitación de responsabilidades 32
G.6.5 Caso fortuito y fuerza mayor 32
G.6.6 Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación 32
G.6.7 Cláusula de jurisdicción competente 32
G.6.8 Resolución de conflictos 32

A. INTRODUCCIÓN

EADTRUST (European Agency of Digital Trust, S.L.) en adelante EADTrust es una compañía ubicada en el estado español dedicada a la prestación de servicios relacionados con la seguridad informática y, en concreto, con la firma electrónica.

Dentro de estas prestaciones englobadas en la marca EADTrust, se ofrecen servicios de Prestador de Servicios de Certificación, tal como quedan definidos en el punto 2 del artículo 2 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica:

> *Se denomina **prestador de servicios de certificación** la persona física o jurídica que expide certificados electrónicos o presta **otros servicios en relación con la firma electrónica.***

En este contexto, el presente documento contiene la política de servicios DSS EADTrust de EADTRUST (European Agency of Digital Trust).

A.1 Presentación

EADTrust ofrece una plataforma de servicios de confianza que incluye un conjunto de servicios de seguridad globales y estandarizados como servicios Web.

Basándose en un protocolo de comunicación entre cliente servidor, se podrán enviar documentos al servidor para ser firmados, o documentos firmados para obtener la verificación de una firma.

Los servicios de confianza de EAD Trust corresponden a lo definido por OASIS en el estándar DSS (Digital Signature Services)[1]. Mediante el uso de estos servicios y perfiles determinados se realizarán operaciones como firma remota, verificación de firmas o ampliación de firmas.

A.2 Opciones del servicio

Para cada usuario se definirán unas condiciones de servicio en las que se especificarán que perfiles son aceptados. En general se distinguen dos tipos de casuística:

- ✓ Generación de elementos criptográficos
- ✓ Verificación de elementos criptográficos

Se deberán especificar que elementos criptográficos entran en consideración. En el caso de la generación de elementos criptográficos que requieran el uso de un certificado por parte del cliente se procederá según lo especificado en C.1.2.1.1.

1 OASIS DSS Core v1.0

A.3 Identificación del Documento

Este documento es la "Política de servicios DSS de EADTrust".

Adicionalmente, EADTrust custodiará en su repositorio y publicará a través del sitio web de EADTrust, un documento con los OIDs correspondientes a la política vigente en cada momento.

A.4 Participantes en los servicios DSS

Esta política regula la prestación de servicios DSS al público.

Los participantes en los Servicios de DSS serán los siguientes:

- Prestadores de Servicios DSS.
- Terceros de confianza
- Entidades y usuarios finales.

A.4.1 Prestador de Servicios DSS

EADTrust dispondrá de una o más Servidores DSS para la prestación de los servicios, para ofrecer garantías de alta disponibilidad, continuidad de negocio, u otros criterios de seguridad que lo justifiquen.

A.4.2 Terceros de confianza

EADTrust puede recabar datos de terceros de confianza en caso de que sea necesario para la prestación del servicio. Estos datos serán típicamente información sobre el estado de certificados emitidos por prestadores confiables.

En tales casos EADTrust se regirá por lo expuesto en la política de certificación pertinente. EADTrust no se hace responsable de que dicha información no sea veraz o incumpla lo que el prestador expresa en su propia política.

A.4.3 Entidades y usuarios finales

Las entidades y usuarios finales serán las personas y organizaciones destinatarias de los servicios DSS, entre ellas, las siguientes:

1) Suscriptores de los servicios DSS.
2) Terceros

A.4.4 Suscriptores

Los suscriptores son las personas y las organizaciones que se suscriben a servicios DSS y que podrán hacer solicitudes durante el periodo de suscripción.

A.4.5 Terceros

Se considera en esta categoría a las personas y las organizaciones que reciben los resultados de las solicitudes generadas por los suscriptores.

Dichos resultados pueden ser bien la generación de elementos criptográficos como informes sobre la verificación de los mismos. Es obligación de los terceros realizar las verificaciones oportunas, tal como se establece en este documento de política y en las correspondientes condiciones generales de uso.

A.5 Uso de los servicios DSS

Esta sección lista las aplicaciones para las que pueden emplearse los servicios DSS, establece limitaciones a determinadas aplicaciones y prohíbe ciertas aplicaciones.

A.5.1 Usos permitidos

Se podrán realizar solicitudes de los servicios DSS según lo establecido por OASIS[2]. Las respuestas serán con arreglo a lo estandarizado por OASIS

A.5.2 Límites y prohibiciones de uso

A.5.3 Límites de uso

Los servicios DSS se emplearán para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.

En el caso que el acceso a los datos de los terceros de confianza[3] incurra en algún coste dicho coste será asumido por el suscriptor del servicio

A.5.4 Prohibiciones de usos

Los servicios DSS no se han diseñado, no se pueden destinar y no se autoriza su uso en equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Todas las responsabilidades legales, contractuales o extra contractuales, daños directos o indirectos que puedan derivarse de usos limitados y/o

2 OASIS DSS Core v1.0

3 Sección 1.3.2

prohibidos quedan a cargo del suscriptor. En ningún caso podrán el suscriptor o los terceros perjudicados reclamar a EADTrust compensación o indemnización alguna por daños o responsabilidades provenientes del uso del servicio para los usos limitados y/o prohibidos.

A.6 Administración de la política

A.6.1 Organización que administra el documento

EADTRUST (European Agency of Digital Trust, S.L.)

A.6.2 Datos de contacto de la organización

EADTRUST (European Agency of Digital Trust, S.L.)

http://www.eadtrust.net

A.6.3 Procedimientos de gestión del documento

EADTrust debe disponer de un comité de aprobación de procedimientos y prácticas de los sistemas que proveen los servicios DSS, formado por miembros de la alta dirección, que vele porque esta política se implante adecuadamente.

Se deben practicar análisis de riesgos periódicamente, para evaluar los activos implicados, las vulnerabilidades y amenazas a dichos activos que puedan producir un impacto en el negocio, con la finalidad de determinar la idoneidad de los controles y procedimientos establecidos por esta política, o la necesidad de cambios en dichos controles y procedimientos.

B. PUBLICACIÓN DE INFORMACIÓN

B.1 Publicación de información

EADTrust publicará las siguientes informaciones, de sus Repositorios:

- La política de servicios DSS
- Los documentos de condiciones generales vinculantes con suscriptores y terceros
- Las modificaciones de los documentos anteriormente indicados.

B.2 Frecuencia de publicación

La información anteriormente indicada se publicará inmediatamente tras su aprobación.

B.3 Control de acceso

EADTrust no limitará el acceso de lectura a las informaciones establecidas en la sección B.1, pero establecerá controles para impedir que personas no autorizadas puedan añadir, modificar o borrar datos, para proteger la integridad y autenticidad de la información publicada.

C. REQUISITOS DE OPERACIÓN

C.1 Solicitud

C.1.1 Legitimación suscriptor

Antes de proceder a procesar ninguna solicitud, debe existir un procedimiento de alta de suscriptor al servicio, en el que se determinarán las personas y sistemas que podrán realizar solicitudes y bajo qué condiciones.

C.1.2 Procedimiento de alta

Antes del alta como suscriptor, EADTrust debe informar al suscriptor de los términos y condiciones aplicables al servicio.

La citada información se comunicará en soporte duradero, en papel o electrónicamente y en lenguaje fácilmente comprensible, y tendrá los siguientes contenidos mínimos:

- ✓ La información de contacto.
- ✓ La política aplicable.
- ✓ La disponibilidad del servicio, incluyendo los tiempos previstos de recuperación y de parada programados.
- ✓ Cualesquiera limitaciones en el uso del servicio.
- ✓ Las obligaciones del suscriptor del servicio.
- ✓ Las obligaciones del tercero que confía.
- ✓ El sistema jurídico que resulte aplicable a la prestación del servicio, incluyendo el cumplimiento de los requisitos establecidos por la legislación aplicable.
- ✓ Limitaciones de responsabilidad.
- ✓ Procedimientos de reclamaciones y resolución de disputas.

En el caso que los servicios contratados requieran del uso de un certificado electrónico del suscriptor para la generación de firmas se procederá según lo expresado en la sección C.1.2.1.

Tras la adhesión a las condiciones generales del servicio por el suscriptor, EADTrust procederá a su alta en el sistema, habilitando los medios técnicos para recibir solicitudes.

EADTrust soportará protocolos de transporte[4] de las solicitudes de servicio, y entre ellos, al menos dispondrá de la posibilidad de solicitar el servicio empleando HTTP[5].

[4] OASIS DSS Core v1.0, sección 6
[5] OASIS DSS Core v1.0, sección 6.1

C.1.2.1 Certificado de Suscriptor

En el caso de que para la prestación del servicio sea necesario un certificado de suscriptor el procedimiento a seguir será el especificado en esta sección

C.1.2.1.1 Generación de Claves

Las claves para el certificado de suscriptor de los servicios serán generadas por EADTrust. EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar que las claves sean generadas de acuerdo a los estándares.

C.1.2.1.2 Envío de la clave pública el emisor del certificado

El método de remisión de la clave pública del suscriptor será PKCS #10, otra prueba criptográfica equivalente o cualquier otro método aprobado por EADTrust.

C.1.2.1.3 Instalación del certificado

El certificado emitido por el prestador de certificación del suscriptor será enviado a EADTrust que realizará las comprobaciones pertinentes y en concreto verificará que se corresponde con las claves generadas.

El certificado será alojado y custodiado por EADTrust para su uso con los fines establecidos en las condiciones generales con el suscriptor. EADTrust deberá realizar los esfuerzos que razonablemente estén a su alcance para proteger el certificado y claves de suscriptor.

C.2 Procesamiento de las solicitudes

Una vez recibida una solicitud EADTrust debe verificar los siguientes aspectos:

- La procedencia y la autenticidad de la solicitud, mediante el protocolo de seguridad apropiado al medio de transporte empleado.
- La corrección técnica de la solicitud. En concreto se validará que la solicitud sea conforme al esquema especificado por OASIS.

En caso de verificación incorrecta de la solicitud, se devolverán los mensajes de error apropiados.

C.3 Respuesta a las solicitudes

Una vez recibida y verificada una solicitud EADTrust procederá a la ejecución de las operaciones necesarias según se indique en la petición y conforme a lo especificado por OASIS. El resultado será una respuesta con arreglo a lo especificado por OASIS.

EADTrust deberá utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de las operaciones que se realicen.

C.4 Finalización de la suscripción

Transcurrido el plazo contractualmente establecido, finalizará la suscripción al servicio, y no se podrán seguir realizando solicitudes.

D. CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES

EADTrust deberá implantar los siguientes controles:

- Seguridad física.
- Gestión de la seguridad.
- Personal
- Auditoría de seguridad.
- Archivo de operaciones.
- Compromiso de claves y recuperación de desastre.
- Terminación del servicio.

D.1 Controles de seguridad física

EADTrust debe disponer de instalaciones que protejan físicamente la prestación del servicio del compromiso causado por acceso no autorizado a los sistemas o a los datos.

La protección física se logrará mediante la creación de perímetros de seguridad claramente definidos en torno al servicio, pudiendo compartirse estos espacios con los restantes servicios que presta EADTrust

EADTrust establecerá controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones.

La política de seguridad física y ambiental aplicable al servicio deberá establecer prescripciones para las siguientes contingencias

- Controles de acceso físico.
- Protección frente a desastres naturales.
- Medidas de protección frente a incendios.
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura.
- Inundaciones.
- Protección antirrobos.
- Allanamiento y entrada no autorizada.
- Recuperación del desastre.

D.1.1 Localización y construcción de las instalaciones

La localización de las instalaciones debe permitir la presencia de fuerzas de seguridad en un plazo de tiempo razonablemente inmediato desde que una incidencia fuera notificada a los mismos (en el caso de no contar con presencia física permanente de personal de seguridad)

La calidad y solidez de los materiales de construcción de las instalaciones deberá garantizar unos adecuados niveles de protección frente a intrusiones por la fuerza bruta.

D.1.2 Acceso físico

EADTrust deberá establecer al menos cuatro (4) niveles de seguridad con restricción de acceso a los diferentes perímetros y barreras físicas definidas.

Para el acceso a las dependencias donde se lleven a cabo procesos relacionados con el servicio, será necesaria la autorización previa, identificación en el momento del acceso y registro del mismo.

Esta identificación, ante el sistema de control de accesos, deberá realizarse mediante reconocimiento de algún parámetro biométrico del individuo, excepto en caso de visitas escoltadas.

La generación de claves criptográficas según lo expuesto en la sección C.1.2.1.1, así como su almacenamiento, deberá realizarse en dependencias específicas para estos fines, y requerirán de acceso y permanencia duales.

D.1.3 Electricidad y aire acondicionado

Los equipos informáticos deberán estar convenientemente protegidos ante fluctuaciones o cortes del suministro eléctrico, que pudieran dañarlos o interrumpir el servicio.

Las instalaciones contarán con un sistema de estabilización de la corriente, así como de un sistema de generación propio con autonomía suficiente para mantener el suministro durante el tiempo que requiera el cierre ordenado y completo de todos los sistemas informáticos.

Los equipos informáticos deberán estar ubicados en un entorno donde se garantice una climatización (temperatura y humedad) adecuada a sus condiciones óptimas de trabajo.

D.1.4 Exposición al agua

EADTrust deberá disponer de sistemas de detección de inundaciones adecuados para proteger los equipos y activos ante tal eventualidad, en el caso de que las condiciones de ubicación de las instalaciones lo hagan necesario.

D.1.5 Prevención y protección de incendios

Todas las instalaciones y activos de EADTrust deben contar con sistemas automáticos de detección y extinción de incendios.

En concreto, los dispositivos criptográficos y los soportes que almacenen claves, deberán contar con un sistema específico y adicional al resto de la instalación, para la protección frente al fuego.

D.1.6 Almacenamiento de soportes

El almacenamiento de soportes de información debe realizarse de forma que se garantice tanto su integridad como su confidencialidad, de acuerdo con la clasificación de la información que se haya establecido.

Deberá contarse para ellos con dependencias o armarios ignífugos.

El acceso a estos soportes, incluso para su eliminación, deberá estar restringido a personas específicamente autorizadas.

D.1.7 Tratamiento de residuos

La eliminación de soportes, tanto papel como magnéticos, se deberá realizar mediante mecanismos que garanticen la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se procederá al formateo, borrado permanente, o destrucción física del soporte.

En el caso de documentación en papel, éste deberá someterse a un tratamiento físico de destrucción.

D.1.8 Copia de respaldo fuera de las instalaciones

Periódicamente, EADTrust almacenará copia de respaldo de los sistemas de información, en dependencias físicamente separadas de aquellas en las que se encuentran los equipos.

D.2 Controles de gestión

EADTrust debe garantizar que sus sistemas se operan de forma segura, para lo cual deberá establecer e implantar procedimientos para las funciones que afecten a la provisión de sus servicios.

D.2.1 Funciones fiables

EADTrust deberá identificar funciones o roles con la condición de fiables.

Las personas que deban ocupar tales puestos deberán ser formalmente nombrados por la alta dirección EADTrust.

Las funciones fiables deberán incluir:

✓ Personal responsable de la seguridad.
✓ Administradores del sistema.
✓ Operadores del sistema.
✓ Auditores del sistema.

Las funciones fiables deberán realizarse teniendo en cuenta que debe existir una separación de funciones sensibles, así como una concesión de mínimo privilegio, cuando sea posible.

Para determinar la sensibilidad de la función, se tendrán en cuenta los siguientes elementos:

✓ Deberes asociados a la función.
✓ Nivel de acceso.
✓ Monitorización de la función.
✓ Formación y concienciación.
✓ Habilidades requeridas.

EADTrust deberá identificar y autenticar al personal antes de acceder a la correspondiente función fiable.

D.2.2 Roles que requieren separación de tareas

Las siguientes tareas deberán ser realizadas, al menos, por dos personas:

✓ Gestión del acceso físico.
✓ Gestión de aplicaciones informáticas relacionadas con el servicio.
✓ Gestión de bienes de equipo criptográfico.
✓ Gestión de claves.
✓ Gestión de configuración y control de cambios.
✓ Gestión del archivo.

D.3 Controles de personal

D.3.1 Requisitos de historial, calificaciones, experiencia y autorización

EADTrust deberá emplear personal cualificado y con la experiencia necesaria, para la prestación de los servicios ofrecidos, en el ámbito de la presente política.

Este requisito se aplicará al personal de gestión, especialmente en relación con procedimientos de personal de seguridad.

La calificación y la experiencia podrán suplirse mediante una formación y entrenamiento apropiados.

El personal en puestos fiables deberá encontrarse libre de intereses personales que entre en conflicto con el desarrollo de la función que tenga encomendada.

No se podrá asignar a un puesto fiable o de gestión a una persona que no sea idóneo para el puesto, especialmente por haber sido condenada por delito o falta que afecte a su idoneidad para el puesto. Por este motivo, se deberá realizar una investigación, de acuerdo con lo establecido en la sección siguiente, relativa a los siguientes aspectos:

- ✓ Estudios, incluyendo titulación alegada.
- ✓ Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales y comprobación de que realmente se hizo el trabajo alegado.

D.3.2 Procedimientos de investigación de historial

EADTrust deberá realizar la investigación antes de que la persona sea contratada y/o acceda al puesto de trabajo.

En la solicitud para el puesto de trabajo se informará acerca de la necesidad de someterse a una investigación previa.

Se deberá advertir de que la negativa a someterse a la investigación implicará el rechazo de la solicitud.

Se deberá obtener consentimiento inequívoco del afectado por la investigación previa y procesar y proteger todos sus datos personales de acuerdo con la LOPD y el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos.

D.3.3 Requisitos de formación

EADTrust deberá formar al personal en puestos fiables y de gestión, hasta que alcancen la cualificación necesaria, de acuerdo con lo establecido en la sección D.3.1 de esta política.

La formación deberá incluir los siguientes contenidos:

- ✓ Principios y mecanismos de seguridad de la jerarquía de certificación, así como el entorno de usuario de la persona a formar.
- ✓ Versiones de maquinaria y aplicaciones en uso.
- ✓ Tareas que debe realizar la persona.
- ✓ Gestión y tramitación de incidentes y compromisos de seguridad.
- ✓ Procedimientos de continuidad de negocio y emergencia.

EADTrust deberá realizar una actualización en la formación del personal al menos cada dos años.

D.3.4 Secuencia y frecuencia de rotación laboral

EADTrust podrá establecer métodos de rotación laboral para la prestación del servicio en turnos, con el objeto de cubrir las necesidades de 24x7 del servicio.

D.3.5 Sanciones para acciones no autorizadas

EADTrust deberá disponer de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, que deberá encontrarse adecuado a la legislación laboral aplicable y, en especial, coordinado con el sistema sancionador del convenio colectivo que resulte de aplicación al personal.

Las acciones disciplinarias podrán incluir la suspensión y el despido de la persona responsable de la acción dañina.

D.3.6 Requisitos de contratación de profesionales externos

EADTrust podrá contratar profesionales externos a EADTrust para cualquier función, incluso para un puesto fiable, en cuyo caso deberá someterse a los mismos controles que los restantes empleados.

En el caso de que el profesional no deba someterse a tales controles, deberá estar constantemente acompañado por un empleado fiable, cuando se encuentre en las instalaciones de EADTrust.

D.3.7 Suministro de documentación al personal

EADTrust suministrará la documentación que estrictamente precise su personal en cada momento, al objeto de que sea suficientemente competente a tenor de lo establecido en la sección D.3.1 de esta política.

D.4 Procedimientos de auditoría de seguridad

D.4.1 Tipos de eventos registrados

EADTrust debe guardar registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- ✓ Encendido y apagado de los sistemas.
- ✓ Inicio y terminación de la aplicación relacionadas con el servicio.
- ✓ Intentos de crear, borrar, cambiar contraseñas o permisos de los usuarios dentro del sistema.
- ✓ Cambios en las políticas de los servicios DSS.
- ✓ Intentos de entrada y salida del sistema.
- ✓ Intentos no autorizados de entrada en la red.
- ✓ Intentos no autorizados de acceso a los ficheros del sistema.
- ✓ Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación del mismo.

EADTrust debe también guardar, ya sea manual o electrónicamente, la siguiente información:

- ✓ La ceremonia de generación de claves y las bases de datos de gestión de claves expuestas en el apartado C.1.2.1.1.
- ✓ Los registros de acceso físico.
- ✓ Mantenimientos y cambios de configuración del sistema.
- ✓ Cambios en el personal.

✓ Informes de compromisos y discrepancias.

D.4.2 Frecuencia de tratamiento de registros de auditoría

Los registros de auditoría se examinarán por lo menos una vez a la semana en busca de actividad sospechosa o no habitual.

El procesamiento de los registros de auditoría consistirá en una revisión de los registros la cual incluye la verificación de que los registros no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros.

Las acciones llevadas a cabo a partir de la revisión de auditoría también deben ser documentadas.

D.4.3 Periodo de conservación de registros de auditoría

Los registros de auditoría se deben retener en el recinto durante por lo menos dos meses después de procesarlos y a partir de ese momento se archivarán de acuerdo con la sección D.5.2 de esta política.

D.4.4 Protección de los registros de auditoría

Los ficheros de registros, tanto manuales como electrónicos, deben protegerse de lecturas, modificaciones, borrados o cualquier otro tipo de manipulación no autorizada usando controles de acceso lógico y físico.

D.4.5 Procedimientos de copia de respaldo

Se deberán generar, al menos, copias incrementales de respaldo de registros de auditoría diariamente y copias completas semanalmente.

D.4.6 Localización del sistema de acumulación de registros de auditoría

El sistema de acumulación de registros de auditoría deberá ser, al menos, un sistema interno de EADTrust, compuesto por los registros de la aplicación, por los registros de red y por los registros del sistema operativo, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado.

D.4.7 Notificación del evento de auditoría al causante del evento

Cuando el sistema de acumulación de registros de auditoría registre un evento, no será preciso enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

Se podrá comunicar si el resultado de su acción ha tenido éxito o no, pero no que se ha auditado la acción.

D.4.8 Análisis de vulnerabilidades

Los eventos en el proceso de auditoría deberán ser guardados, en parte, para monitorizar las vulnerabilidades del sistema.

Los análisis de vulnerabilidad deben ser ejecutados, repasados y revisados a través de un examen de esos eventos monitorizados.

Estos análisis deben ser ejecutados diariamente, mensualmente y anualmente de acuerdo con su definición en el plan de auditoría o documento que lo sustituya, de EADTrust.

D.5 Archivo de informaciones

EADTrust debe garantizar que toda la información relativa al servicio se guarda durante un período de tiempo apropiado, según lo establecido en la sección D.5.2 de esta política.

D.5.1 Tipos de eventos registrados

EADTrust debe guardar todos los eventos que tengan lugar en relación a las operaciones de los servicios DSS.

Se debe guardar un registro de lo siguiente:

✓ Altas y bajas de suscriptores.
✓ Operaciones realizadas.

D.5.2 Periodo de conservación de registros

EADTrust debe guardar los registros especificados en la sección anterior de esta política de forma permanente, con un mínimo de quince (15) años.

D.5.3 Protección del archivo

EADTrust debe:

✓ Archivar los datos de forma completa y confidencial.
✓ Mantener la privacidad de los datos del suscriptor.

D.5.4 Procedimientos de copia de respaldo

EADTrust debe realizar copias de respaldo incrementales diarias de todos sus documentos electrónicos, según la sección D.5.1 de esta política. Debe, además, realizar copias de respaldo completas semanalmente para casos de recuperación de datos, de acuerdo con la sección D.7 de esta política.

D.5.5 Localización del sistema de archivo

EADTrust debe disponer de un sistema de mantenimiento de datos de archivo tal y como se especifica en la sección D.5.4 de esta política.

D.5.6 Procedimientos de obtención y verificación de información de archivo

Sólo personas autorizadas por EADTrust podrán tener acceso a los datos de archivo, ya sea en las mismas instalaciones de EADTrust o en su ubicación externa.

D.6 Renovación de claves

EADTrust informará a los suscriptores con antelación cuando las claves generadas según lo expuesto en C.1.2.1.1 estén próximas a expirar.

Se procederá a la creación de un nuevo par de claves, previa aprobación del suscriptor, repitiendo el proceso detallado en la sección C.1.2.1

D.7 Compromiso de claves y recuperación de desastre

D.7.1 Corrupción de recursos, aplicaciones o datos

Cuando tenga lugar un evento de corrupción de recursos, aplicaciones o datos, EADTrust debe iniciar las gestiones necesarias, de acuerdo con el plan de seguridad, el plan de emergencia y el plan de auditoría, o documentos que los sustituyan, para hacer que el sistema vuelva a su estado normal de funcionamiento.

D.7.2 Compromiso de la clave privada de suscriptor

EADTrust debe considerar el compromiso o la sospecha de compromiso de la clave privada de suscriptor como un desastre.

En caso de compromiso, EADTrust debe realizar como mínimo las siguientes acciones:

- ✓ Informar a todos los suscriptores y terceros del compromiso.
- ✓ Indicar que operaciones han sido realizadas usando la clave comprometida.

D.7.3 Desastre sobre las instalaciones

EADTrust debe desarrollar, mantener, probar y, si es necesario, ejecutar un plan de emergencia para el caso de que ocurra un desastre, ya sea por causas naturales o causado por el hombre, sobre las instalaciones, el cual indique cómo restaurar los servicios de los sistemas de información.

La ubicación de los sistemas de recuperación de desastres debe disponer de las protecciones físicas de seguridad detalladas en el plan de seguridad.

EADTrust debe ser capaz de restaurar la operación normal de los servicios, en las 24 horas siguientes al desastre.

La base de datos de recuperación de desastres utilizada por EADTrust debe estar sincronizada con la base de datos de producción, dentro de los límites temporales especificados en el plan de seguridad.

D.8 Terminación del servicio

EADTrust debe asegurar que las posibles interrupciones a los suscriptores y a terceras partes son mínimas como consecuencia del cese de los servicios Antes de terminar sus servicios, EADTrust debe ejecutar, como mínimo, los siguientes procedimientos:

- Informar a todos los suscriptores y tercero.
- Ejecutar las tareas necesarias para transferir las obligaciones de mantenimiento de los archivos de registro de eventos durante los períodos de tiempo respectivos indicados al suscriptor y a los terceros
- Facilitar las claves privadas a los suscriptores de forma fiable y proceder posteriormente a su destrucción.

EADTrust debe declarar en sus prácticas las previsiones que tiene para el caso de terminación del servicio. Estas deben incluir:

- Notificación a las entidades afectadas.
- Transferencia de sus obligaciones a otras personas.

E. CONTROLES DE SEGURIDAD TÉCNICA

EADTrust deberá emplear sistemas y productos fiables, que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica.

E.1 Protección de las claves privadas

E.1.1 Estándares de módulos criptográficos

Para los módulos que gestionan claves se deberá asegurar el nivel exigido por los estándares indicados en las secciones anteriores.

E.1.2 Control por más de una persona sobre las claves privadas

El acceso de operación a las claves privadas de los suscriptores deberá requerir necesariamente del concurso sucesivo de más de una persona que tendrá el role o bien de custodio de un dispositivo criptográfico o bien de conocedor de una clave de acceso

Los dispositivos criptográficos quedarán almacenados en las dependencias de EADTrust, y para su acceso será necesaria una persona adicional.

E.1.3 Repositorio de la clave privada

Las claves privadas de los suscriptores se almacenarán en espacios ignífugos y protegidos por controles de acceso físico dual.

E.1.4 Copia de respaldo de la clave privada

No se podrán realizar copias de respaldo de las claves privadas de los suscriptores.

Cuando las claves se almacenen en un módulo hardware de proceso dedicado, deberán proveerse los controles oportunos para que éstas nunca puedan abandonar el dispositivo.

E.1.5 Archivo de la clave privada

No se archivarán claves privadas.

E.1.6 Introducción de la clave privada en el módulo criptográfico

Las claves privadas se podrán generar directamente en los módulos criptográficos o en módulos criptográficos externos, de los que se exportarán las claves cifradas para su introducción en los módulos de producción.

En este caso, las claves privadas quedarán almacenadas en ficheros cifrados con claves fragmentadas y en dispositivos criptográficos (de las que no podrán ser extraídas).

Dichos dispositivos serán empleados para introducir la clave privada en el módulo criptográfico.

E.1.7 Método de activación de la clave privada

La clave privada de cada suscriptor se activará mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección E.3.2E.4.3.

E.1.8 Método de desactivación de la clave privada

La desactivación de la clave privada se producirá en los casos de apagado del módulo criptográfico, o mediante los procedimientos soportados por el módulo criptográfico.

E.1.9 Método de destrucción de la clave privada

Las claves privadas serán destruidas en una forma que impida su robo, modificación, divulgación no autorizada o uso no autorizado.

E.2 Otros aspectos de gestión de claves

E.2.1 Periodos de utilización de las claves pública y privada

Los periodos de utilización de las claves serán los determinados por la duración del certificado según lo establecido por el prestador emisor del mismo. Transcurrido el cual no se podrá continuar utilizando.

E.3 Controles de seguridad informática

E.3.1 Requisitos técnicos específicos de seguridad informática

Se deberá garantizar que el acceso los sistemas está limitado a individuos debidamente autorizados. En particular:

- ✓ Se debe garantizar una administración efectiva del nivel de acceso de los usuarios (operadores, administradores, así como cualquier usuario con acceso directo al sistema) para mantener la seguridad del sistema, incluyendo gestión de cuentas de usuarios, auditoría y modificaciones o denegación de acceso oportunas.
- ✓ Se debe garantizar que el acceso a los sistemas de información y aplicaciones se restringe de acuerdo a lo establecido en la política de control de acceso, así como que los sistemas proporcionan los controles de seguridad suficientes para implementar la segregación de funciones identificada en las prácticas, incluyendo la separación de funciones de administración de los sistemas de seguridad y de los operadores. En concreto, el uso de programas de utilidades del sistema estará restringido y estrechamente controlado.
- ✓ El personal deberá ser identificado y reconocido antes de utilizar aplicaciones críticas
- ✓ El personal será responsable y deberá poder justificar sus actividades, por ejemplo mediante un archivo de eventos.
- ✓ Deberá evitarse la posibilidad de revelación de datos sensibles mediante la reutilización de objetos de almacenamiento (por ejemplo ficheros borrados) que queden accesibles a usuarios no autorizados.

- ✓ Los sistemas de seguridad y monitorización deben permitir una rápida detección, registro y actuación ante intentos de acceso irregular o no autorizado a sus recursos (por ejemplo, mediante sistema de detección de intrusiones, monitorización y alarma)
- ✓ El acceso a los repositorios públicos de la información deberá contar con un control de accesos para modificaciones o borrado de datos.

E.3.2 Evaluación del nivel de seguridad informática

Las aplicaciones usadas para el desempeño de los servicios DSS por EADTrust deberán ser fiables

E.4 Controles técnicos del ciclo de vida

E.4.1 Controles de desarrollo de sistemas

Se deberá realizar un análisis de requisitos de seguridad durante las fases de diseño y especificación de requisitos de cualquier componente empleado en las aplicaciones, para garantizar que los sistemas son seguros.

Se emplearán procedimientos de control de cambios para las nuevas versiones, actualizaciones y parches de emergencia, de dichos componentes.

E.4.2 Controles de gestión de seguridad

EADTrust deberá mantener un inventario de todos los activos informativos y realizará una clasificación de los mismos, de acuerdo con sus necesidades de protección, coherente con el análisis de riesgos efectuado.

La configuración de los sistemas se auditará de forma periódica, de acuerdo con lo establecido en la sección G.1.1 de esta política.

Se realizará un seguimiento de las necesidades de capacidad, y se planificarán procedimientos para garantizar suficiente disponibilidad electrónica y de almacenamiento para los activos informativos.

E.4.3 Evaluación del nivel de seguridad del ciclo de vida

EADTrust se someterá a evaluaciones independientes, auditorías y, en su caso, certificaciones de seguridad del ciclo de vida de los productos que emplea.

E.5 Controles de seguridad de red

Se deberá garantizar que el acceso a las diferentes redes de EADTrust está limitado a individuos debidamente autorizados. En particular:

- ➢ Deben implementarse controles para proteger la red interna de dominios externos accesibles por terceras partes. Los cortafuegos deberán configurarse de forma que se impidan accesos y protocolos que no sean necesarios para la operación de las aplicaciones relacionadas con el servicio.

- Los datos sensibles deberán protegerse cuando se intercambien a través de redes no seguras (incluyendo como tales los datos de registro del suscriptor)
- Se debe garantizar que los componentes locales de red se encuentran ubicados en entornos seguros, así como la auditoría periódica de sus configuraciones.

E.6 Controles de ingeniería de módulos criptográficos

Se debe garantizar que las claves de los suscriptores son generadas en equipamientos criptográficos, que cumplan los estándares criptográficos de seguridad que se han indicado en las secciones anteriores.

F. AUDITORIA DE CONFORMIDAD

EADTrust debe realizar periódicamente una auditoría de cumplimiento para probar que cumple, una vez ha empezado a funcionar, los requisitos de seguridad y de operación necesarios para cumplir la política de los servicios DSS.

F.1 Frecuencia de la auditoria de conformidad

Se debe llevar a cabo una auditoría de conformidad anualmente o en cualquier momento, a causa de una sospecha de incumplimiento de alguna medida de seguridad o por un compromiso de claves. Estas auditorias podrán ser internas o externas.

F.2 Identificación y calificación del auditor

Si EADTrust dispone de un departamento de auditoría interno, éste podrá encargarse de llevar a cabo la auditoría de conformidad.

En el caso de no poseer ese departamento, o de considerarse oportuno, se deberá acudir a un auditor independiente, el cual debe demostrar experiencia en seguridad informática, en seguridad de sistemas de información y en auditorías de conformidad de servicios de certificación.

F.3 Relación del auditor con la entidad auditada

Las auditorías de conformidad ejecutadas por terceros deben ser llevadas a cabo por una entidad independiente de EADTrust, no debiendo tener ningún conflicto de intereses que menoscabe su capacidad de llevar a cabo servicios de auditoría.

F.4 Listado de elementos objeto de auditoria

Los elementos objeto de auditoría serán los siguientes:

- Servicios DSS.
- Sistemas de información.
- Protección del centro de proceso
- Documentación del servicio.

Los detalles de cómo llevar a cabo la auditoría de cada uno de estos elementos se detallarán en el plan de auditoría de EADTrust.

F.5 Acciones a emprender como resultado de una falta de conformidad

Una vez recibido el informe de la auditoría de cumplimiento llevada a cabo, EADTrust debe discutir, con la entidad que ha ejecutado la auditoría y las deficiencias encontradas y desarrollar y ejecutar un plan correctivo que solvente dichas deficiencias.

Si EADTrust no es capaz de desarrollar y/o ejecutar el mencionado plan o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o

integridad del sistema deberá terminar los servicios, tal y como se describe en la sección D.8 de esta política.

G. REQUISITOS COMERCIALES Y LEGALES

G.1 Tarifas

G.1.1 Tarifa de servicios

EADTrust podrá establecer una tarifa por el uso de los servicios DSS.

G.1.2 Tarifas de otros servicios

Sin estipulación.

G.1.3 Política de reintegro

EADTrust no podrá reintegrar las tarifas del servicio, excepto por funcionamiento erróneo.

G.2 Capacidad financiera

EADTrust deberá disponer de recursos económicos suficientes para mantener sus operaciones y cumplir sus obligaciones, así como para afrontar el riesgo de la responsabilidad por daños y perjuicios.

G.2.1 Otros activos

Sin estipulación.

G.3 Confidencialidad

G.3.1 Informaciones confidenciales

Las siguientes informaciones, como mínimo, serán mantenidas confidenciales por EADTrust:

- ✓ Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- ✓ Registros de auditoría interna y externa, creados y/o mantenidos por EADTrust y sus auditores.
- ✓ Planes de continuidad de negocio y de emergencia.
- ✓ Política y planes de seguridad.
- ✓ Documentación de operaciones y restantes planes de operación, como archivo, monitorización y otros análogos.
- ✓ Toda otra información identificada como "Confidencial".

G.3.2 Informaciones no confidenciales

La siguiente información será considerada no confidencial:

- ✓ Toda otra información que no esté indicada en la sección anterior de esta política.

G.3.3 Divulgación legal de información

EADTrust divulgará la información confidencial en los casos legalmente previstos para ello.

G.3.4 Divulgación de información por petición de su titular

EADTrust incluirá, en la política de intimidad prevista en la sección G.4 de esta política, prescripciones para permitir la divulgación de la información del suscriptor, directamente a los mismos o a terceros.

G.3.5 Otras circunstancias de divulgación de información

Sin estipulación.

G.4 Protección de datos personales

Para la prestación del servicio, EADTrust precisa recabar y almacenar ciertas informaciones, que incluyen informaciones personales. Tales informaciones serán recabadas directamente de los afectados, con su consentimiento explícito o en los casos es los que la ley permita recabar la información sin consentimiento del afectado.

Se recabarán los datos exclusivamente necesarios para la prestación del servicio.

EADTrust no divulgará ni cederá datos personales, excepto en los casos previstos en las secciones G.3.2 a G.3.5 de esta política, y en la sección D.8, en caso de terminación de la Entidad de Certificación.

La información confidencial de acuerdo con la LOPD será protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de acuerdo con las prescripciones establecidas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

G.5 Derechos de propiedad intelectual

EADTrust será propietaria de la Política de Servicios DSS

G.6 Obligaciones y responsabilidad civil

G.6.1 Obligaciones de EADTrust

EADTrust debe garantizar, bajo su plena responsabilidad, que cumple con todos los requisitos establecidos en la política.

Será la única entidad responsable del cumplimiento de los procedimientos descritos en esta política, incluso cuando una parte o la totalidad de las operaciones sean subcontratadas externamente.

Se debe vincular a los suscriptores mediante condiciones del servicio, que deberán estar en lenguaje escrito y comprensible.

G.6.2 Garantías ofrecidas a suscriptores y terceros

EADTrust, en las condiciones generales del servicio, establecerá y rechazará garantías, y limitaciones de responsabilidad aplicables.

G.6.3 Rechazo de otras garantías

EADTrust podrá rechazar toda otra garantía que no sea legalmente exigible, excepto las contempladas en la sección G.6.2.

G.6.4 Limitación de responsabilidades

EADTrust limitará su responsabilidad en las condiciones de esta política y en los acuerdos generales y/o particulares establecidos con los suscriptores.

G.6.5 Caso fortuito y fuerza mayor

EADTrust incluirá cláusulas para limitar su responsabilidad en caso fortuito y en caso de fuerza mayor, en las condiciones generales del servicio.

G.6.6 Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

EADTrust deberá establecer, en las condiciones generales del servicio, cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación:

- ✓ En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afectará al resto del contrato.
- ✓ En virtud de la cláusula de supervivencia, ciertas reglas continuarán vigentes tras la finalización de la relación jurídica reguladora del servicio entre las partes. A este efecto, se velará porque, al menos los requisitos contenidos en las secciones G.6 (Obligaciones y responsabilidad), F.1 (Auditoría de conformidad) y G.3 (Confidencialidad), continúen vigentes tras la terminación de los servicios.
- ✓ En virtud de la cláusula de acuerdo íntegro se entenderá que el documento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.
- ✓ En virtud de la cláusula de notificación se establecerá el procedimiento por el cual las partes se notifican hechos mutuamente.

G.6.7 Cláusula de jurisdicción competente

EADTrust deberá establecer, en las condiciones generales de emisión y uso, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces españoles.

La competencia territorial y funcional se determinará en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.

G.6.8 Resolución de conflictos

EADTrust deberá establecer, en las condiciones generales de emisión y uso, los procedimientos de mediación y resolución de conflictos aplicables.