PÚBLICO

POLÍTICA GENERAL DEL TSP MEDIACERT

AUTOR(ES)	:	F. Da Silva
NÚMERO DE DOCUMENTO	:	WLM-TSP-F094
VERSIÓN	:	1.4
ESTADO	:	Final
FUENTE	:	Worldline
FECHA DEL DOCUMENTO	:	14 de noviembre de 2017
NÚMERO DE PÁGINAS	:	51

TSP MediaCert

Digitally signed by TSP MediaCert
DN: CN=TSP MediaCert, O=Worldline, E=dl-mediacert-tsp@worldline.com, C=FR
Reason: I am approving this document
Location:
Date: 2019-05-23 09:36:22

Papel	Nombre	Firma	Fecha
Corrector 1 - Jefe Adjunto del TSP	Fanny Lesecq	Fanny Lesecq	23/04/2019
Corrector 2 - CISO	Didier Sobkowiak	Didier Sobkowiak	23/04/2019
Función de aseguramiento de la calidad	Franck Da Silva	Franck Da Silva	23/04/2019
Propietario del documento	Comité MediaCert	Guillaume Bailleul	23/04/2019
Autorizador - TSP Resp.	Guillaume Bailleul	Guillaume Bailleul	23/04/2019

Tabla de contenidos

Lista de cambios

Versión	Fecha	Descripción	Autor(es)
0.1	14/11/2017	Inicialización del documento	F. Da Silva V. Dumond
1.0	30/03/2017	Validación del documento por el Comité de Seguridad	Comité de Seguridad
1.1	05/07/2018	Integración de observaciones post-auditoría internas a la plataforma de timestamping: Modificación del plazo de publicación de la documentación de TSP MediaCert Modificación del esquema de presentación del TSP MediaCert	F. Da Silva C. Lootvoet
1.2	18/09/2018	Integración del Servicio de Archivo Electrónico en el ámbito del TSP MediaCert Consideración de la integración de una nueva CA (la CA LCP OTU) que sólo conduce a un cambio en el ámbito funcional del PG.	F. Da Silva
1.3	12/10/2018	Consideración de las observaciones/desviaciones detectadas durante la auditoría de certificación 2018 de la AC OTU LCP: • separación de tareas para la revisión/validación y aprobación de documentos	F. Da Silva
1.4	23/04/2019	Aclaración del punto de contacto del TSP MediaCert: se refiere no sólo a la documentación, sino también a todas las formas de solicitud. Consideración de posibles prestadores de servicios extranjeros en la verificación de los antecedentes penales, ya que el boletín n°3 es específicamente francés. Evolución de las versiones de los estándares del repositorio.	F. Da Silva

1 Prefacio

1.1 Referencias

1.1.1 Reglamentos y normas

Referencia	Descripción
[CNIL]	Ley n°78-17 del 6 de enero de 1978 relativa a la informática, a los ficheros y a las libertades, modificada por la ley n°2004-801 del 6 de agosto de 2004 (Francia)
[EIDAS]	REGLAMENTO (UE) No 910 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 sobre identificación electrónica y servicios fiables en el mercado interior y por el que se deroga la Directiva 1999/93/CE
[SIAF]	Código del Patrimonio Decreto n°2011-574 del 24 de mayo de 2011 Libro 2
[RGPD]	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

1.1.2 Referencias técnicas reglamentarias

Referencia	Descripción
[ETSI 119 312]	ETSI EN 119 312 v1.2.2 (2018-09) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
[ETSI 319 401]	ETSI EN 319 401 v2.2.1 (2018-04) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ISO 27001]	ISO/IEC 27001 : 2013 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos
[ISO 27002]	ISO/IEC 27002 : 2013 Código de buenas prácticas para la gestión de la seguridad de datos
[Higiene]	Guía de higiene informática - Refuerce la seguridad del sonido de su sistema de información en 42 pasos Agencia Nacional de Seguridad de los Sistemas de Información (ANSSI - Francia)
[Calificación ANSSI]	Proveedores de servicios cualificados y de confianza Criterios para evaluar el cumplimiento del Reglamento eIDAS v1.1 Agencia Nacional de Seguridad de los Sistemas de Información (ANSSI)
[RGS B1]	Norma General de Seguridad v2.0 - Apéndice B1 (2014-02) Agencia Nacional de Seguridad de los Sistemas de Información (ANSSI) Mecanismos criptográficos: normas y recomendaciones para la selección y dimensionamiento de los mecanismos criptográficos

Referencia	Descripción
[SOGIS_CRYPTO]	Esquema de criptografía SOG-IS - Mecanismos criptográficos acordados - Versión en vigor. Disponible en http://sogis.org

1.2 Definiciones de los términos

A continuación se presenta una lista de las principales definiciones de los términos técnicos utilizados en este PG:

Suscriptor: una entidad/organización que se beneficia de uno o más servicios de confianza proporcionados por TSP MediaCert.

Bi-clave: par compuesto por una clave privada (a mantener en secreto) y una clave pública, necesarias para la implementación de un servicio de criptografía basado en algoritmos asimétricos (RSA por ejemplo).

Certificado: Elemento de datos estándar X509 utilizado para asociar una clave pública a su titular. Un certificado contiene datos como la identidad del titular, su clave pública, la identidad de la organización que emitió el certificado, el período de validez, un número de serie, una huella dactilar (*resumen*) o los criterios de uso. El conjunto está firmado por la clave privada de la autoridad de certificación que emitió el certificado.

Servicio de archivado: servicio que incluye un conjunto de acciones destinadas a identificar, recoger, clasificar, almacenar, comunicar y devolver documentos electrónicos, durante el tiempo necesario para cumplir con las obligaciones legales o para satisfacer las necesidades de información o para propósitos de propiedad.

Servicio de Certificación: servicio que produce Certificados y, en general, los gestiona (creación, entrega, revocación, publicación, registro, archivado) de acuerdo con una política de certificación.

Servicio de Fideicomiso: un servicio de confianza es un servicio electrónico que consiste en:

- la expedición de certificados de firma electrónica, sello electrónico y autenticación de sitios web; o
- la validación de firmas electrónicas y sellos; o
- el almacenamiento de firmas electrónicas y sellos electrónicos;
- sellado de tiempo electrónico;
- correo electrónico certificado.

El archivado electrónico de información (distinto del almacenamiento de firmas y sellos electrónicos) no se considera un servicio de confianza en el sentido del Reglamento [eIDAS]. Sin embargo, dado que funciona en condiciones similares a las de los servicios de emisión de certificados y sellado de tiempo proporcionados por TSP MediaCert, el archivado electrónico se considerará un servicio de confianza dentro de TSP MediaCert y, por lo tanto, dentro de este documento.

Servicio de marca de tiempo: servicio que produce marcas de tiempo y, de forma más general, garantiza su gestión de acuerdo con una política de marca de tiempo.

1.3 Acrónimos

A continuación se incluye una lista de los acrónimos utilizados en este PG:

- **CA:** Autoridad de certificación;
- **AFNOR:** Asociación Francesa de Normalización;
- **AH** : Autoridad de marcas de tiempo;
- **DTPG:** Documentación Técnica de Prácticas Generales;
- **EIDAS:** Identificación y firma electrónica;
- **HSM :** *Módulo Hardware de seguridad* ;
- **CIG :** *Infraestructura de clave pública*;
- **CRL (LCR)**: Lista de certificados revocados ;
- **OID :** Identificador de objeto;
- **PC-DPC :** Política de certificación - Declaración de prácticas de certificación;
- **PH-DPH:** Política de Time-Stamp - Declaración de Prácticas de Time-Stamping;
- **PA:** Política de archivo;
- **PCRA**: Plan de Continuidad y Reanudación de Negocio;
- **PG:** Política General de TSP MediaCert;
- **ERP:** Política de Gestión de Incidentes;
- **PSI:** Política de Seguridad de la Información de Worldline;
- **DGPS:** Normativa General de Protección de Datos;
- **SAE :** Servicio de archivo electrónico;
- **SIAF:** Servicio Interministerial de Archivos de Francia;
- **SIEM:** Información de Seguridad y Gestión de Eventos;
- **SOC:** Centro de operaciones de seguridad;
- **ISS**: Seguridad de los Sistemas de Información;
- **TSP**: *Proveedor de Servicios de Confianza*;
- **UH (TSU)**: Unidad de marca de Tiempo.

2 Introducción

2.1 Objeto

El *proveedor de servicios de confianza* MediaCert, establecido por Worldline, proporciona un conjunto de servicios de confianza y, por lo tanto, está sujeto a un conjunto de reglamentos (véase el capítulo 1.1.1), como el Reglamento "eIDAS" nº 910/2017 del Parlamento Europeo y del Consejo Europeo sobre servicios de identificación electrónica y servicios de confianza para transacciones electrónicas en el mercado interior.

Este documento describe la política general del TSP MediaCert. En este contexto, presenta:

- los requisitos generales a los que está sujeta la TSP MediaCert;
- la organización creada para garantizar la prestación de servicios;
- las medidas generales de seguridad aplicadas.

2.2 Identificación de documentos

Elementos	Valor
Título	Política General del TSP MediaCert
Referencia del documento	WLM-TSP-F094
OID	1.2.250.1.111.20.1.1
Versión	1.4
Autor	F. Da Silva

La definición de OID de este documento se presenta en el Capítulo 5.3.2.1.

Este documento se denominará "PG" en todo el documento.

2.3 Estructura de la Política General

Con el fin de facilitar la interoperabilidad con los estándares aplicables, esta PG está estructurada de acuerdo con:

- las cláusulas de la norma[ETSI 319 401];
- las principales cláusulas de la norma [ISO 27002].

3 Ámbito de aplicación de la política general

3.1 Ámbito funcional

Tal como se define en la introducción, este documento describe la política general adoptada y aplicada por todos los servicios de confianza de TSP MediaCert, independientemente de su nivel de cualificación, de acuerdo con el reglamento eIDAS.

Entre los servicios de confianza que se ofrecen se encuentran los siguientes:

la expedición de certificados de firma electrónica y de sello electrónico;

sellado de tiempo electrónico;

archivo electrónico (véase el capítulo 1.2).

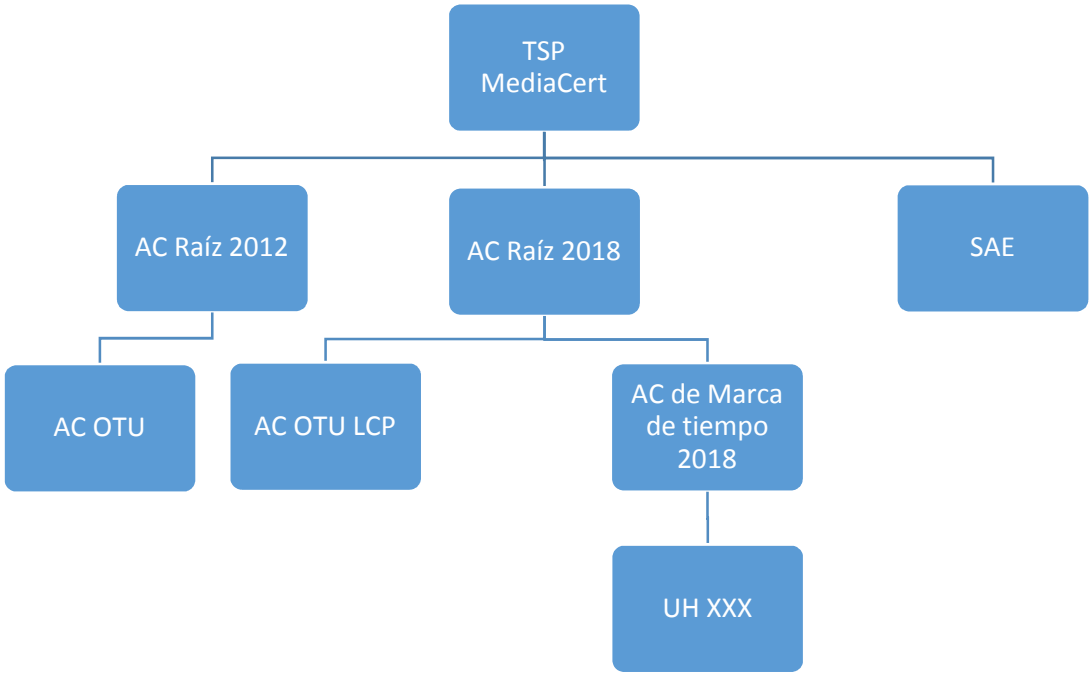

Figura 1 - Alcance funcional del TSP MediaCert

3.2 Ámbito técnico

Este PG se aplica a todo el alcance de TSP MediaCert. Estos componentes se presentan en el DTPG así como en la documentación técnica específica de cada servicio TSP MediaCert Trust.

4 Análisis de riesgos de seguridad

Como parte de las actividades de TSP MediaCert, el gerente de seguridad de TSP MediaCert lleva a cabo un análisis de riesgos en el marco de los servicios fiduciarios.

Su objetivo es permitir la identificación, el análisis y la evaluación de los riesgos funcionales y empresariales del SI, así como la definición de las medidas adecuadas aplicadas para hacerles frente, teniendo en cuenta los resultados de la evaluación.
Las medidas de gestión de riesgos garantizan que el nivel de seguridad aplicado es proporcional a los riesgos que pesan sobre el SI.
Garantiza que el DTPG (véase el capítulo5.4) sea coherente con el nivel de riesgo determinando todos los requisitos de seguridad y procedimientos operativos necesarios.

Este documento permite identificar la depreciación de los algoritmos, activos y sus necesidades de seguridad aplicables a los sistemas TSP MediaCert. Tiene en cuenta el estado actual de la técnica en este ámbito y está sujeta a revisión periódica, al menos una vez al año, y en caso de que se produzcan cambios importantes en la infraestructura o los servicios. Es validado por el Comité MediaCert, que acepta los riesgos residuales expuestos, tras su revisión periódica (véase el capítulo 6.7).

En el caso de un servicio cualificado, la TSP MediaCert procederá a la aprobación del servicio de acuerdo con las recomendaciones de la ANSSI[ANSSI Qualification] antes de prestar el servicio de Qualified Trust. Esta aprobación se revisa cada dos (2) años.

El análisis de riesgos también permite identificar datos sensibles. Como tales, están sujetos a medidas de seguridad específicas que pueden incluir copias de seguridad, registro, acceso, etc.

5 Políticas y Prácticas

5.1 Gestión de la documentación de TSP MediaCert

5.1.1 Entidad gestora de la documentación del TSP MediaCert

Worldline es responsable del desarrollo, aprobación, monitoreo y revisión, según sea necesario, de la documentación de TSP MediaCert. Para eso, se crea un comité denominado "MediaCert Committee", tal y como se define en el capítulo 6.7 este documento.
En particular, para cada Servicio de Confianza operado por MediaCert, se desarrolla y documenta una Política de Servicios de Confianza, así como las prácticas que respaldan esta política.
Este documento define y documenta los requisitos y prácticas comunes a todos los servicios de confianza de MediaCert, los requisitos y prácticas adicionales específicos se detallan en la documentación específica de cada uno de los servicios de confianza.

Entre la documentación relevante de TSP MediaCert se encuentran las siguientes:

- esta Política General;
- Política de Certificación - Declaración de Prácticas de Certificación;
- Política de Time-Stamp - Declaración de Prácticas de Time-Stamping;
- Política de archivado;
- Análisis de riesgos.

Todos estos documentos, así como este documento, están sujetos a la aprobación del Jefe del MediaCert TSP durante una reunión de seguridad del Comité MediaCert. Después de la aprobación, se publican y se comunican a los empleados y a terceros según sea necesario (véase el capítulo 5.3.1).

Todos estos documentos también están sujetos a un proceso de revisión. Este proceso de revisión se inicia después de cada adición o cambio importante de un Servicio de Confianza y al menos una vez al año. El proceso de revisión es responsabilidad del Comité MediaCert.

La Política de Seguridad de los Sistemas de Información (PSSI o PSI) aplicada por TSP MediaCert es gestionada (redacción, revisión, aprobación, publicación) por el Comité de Seguridad de Worldline France (ver Capítulo 5.5). Además, cualquier cambio significativo en dicha PSSI que dé lugar a un cambio en este PG dará lugar a una notificación a la ANSSI (véase el capítulo 5.3.1).

5.1.2 Contacto

El contacto autorizado para cualquier comentario, solicitud de información adicional, quejas o archivos de disputa, en particular en relación con la documentación de TSP MediaCert es:

Comité de MediaCert
Worldline
23 rue de la Pointe
Zona Industrial A
59113 SECLIN
Francia
dl-mediacert-tsp@worldline.com

5.1.3 Entidad que determina la conformidad de una declaración de práctica con su política asociada

La coherencia de una declaración de prácticas con su política asociada es determinada por el Comité de MediaCert al validar la política.

La coherencia de la documentación técnica con la política asociada es determinada por el Comité MediaCert en el momento de la validación de la política.

5.1.4 Procedimiento para aprobar la conformidad de una declaración de prácticas con su política asociada

El proceso de verificación de la conformidad de una declaración de prácticas con la política asociada está garantizado por la unicidad del documento. El Comité MediaCert revisa y valida cualquier cambio importante (ver Capítulo 6.7).
El Comité MediaCert es responsable de la implementación y aplicación efectiva de las prácticas descritas.

La conformidad de una documentación técnica con la política asociada - declaración de prácticas está garantizada por el redactor de la documentación técnica. De hecho, cualquier modificación de una documentación técnica se realiza en paralelo con la política - declaración de prácticas en cuestión. El Comité MediaCert revisa y valida cualquier cambio importante (ver Capítulo 6.7).

En caso de que se produzca un cambio significativo en la prestación de sus servicios de confianza cualificados, el TSP MediaCert informará a la ANSSI de conformidad con los procedimientos recomendados por esta última en el marco de[Cualificación de la ANSSI]. En particular en los siguientes casos (no limitados):

- cambios inducidos por un cambio en la política de servicio o en los términos y condiciones de uso asociados;
- cambios en los subcontratistas;
- cambios en las condiciones de alojamiento;
- cambios en el equipo criptográfico;
- cambios en la arquitectura técnica;
- cambios en los procedimientos de registro e identificación;
- cambios en el gobierno de TSP MediaCert Trust Services.

Los cambios que den lugar a cambios en la lista de confianza publicada por la ANSSI también se notificarán lo antes posible.
Además, el TSP MediaCert envía anualmente a la ANSSI un resumen de todos los cambios introducidos en la prestación de sus servicios de confianza cualificados, que afectan a las conclusiones presentadas en el informe de evaluación de la conformidad.

5.2 Suministro de información

5.2.1 Entidad responsable de la puesta a disposición de la información

El Comité MediaCert es la entidad responsable de poner a disposición la información que se va a publicar.

5.2.2 Información que debe ponerse a disposición

La definición de la información a publicar es específica para cada Servicio de confianza y, por lo tanto, está disponible en las políticas específicas de los distintos Servicios de confianza.

Sin embargo, algunos elementos se publican necesariamente en el sitio especificado en el punto 5.2.3:

- la presente Política General, común a todos los Servicios de confianza;
- los Términos y Condiciones de cada uno de los Servicios de confianza.

Los T&C de un Servicio de Confianza se ponen a disposición de los Usuarios y Suscriptores antes de cualquier uso del servicio.

5.2.3 Lugar de disponibilidad de la información

La información que se publicará está disponible en el sitio web de TSP MediaCert, disponible los 7 días de la semana, las 24 horas del día, en https://www.mediacert.com
Este sitio web tiene por objeto satisfacer un requisito de alta disponibilidad.

5.2.4 Plazos y frecuencia de publicación

Los plazos y frecuencias de publicación de la información son específicos de cada servicio de confianza de TSP MediaCert y, por lo tanto, están disponibles en las políticas pertinentes, - excepto en el caso de la documentación que debe publicarse inmediatamente, independientemente del servicio fiduciario pertinente.

Se especifica que las versiones anteriores de los documentos contractuales (políticas, condiciones generales, etc.) regulan exclusivamente los períodos de tiempo cubiertos por estas versiones, es decir, hasta su sustitución notificada a los Suscriptores. En efecto, tan pronto como una nueva versión sea notificada a los Suscriptores y publicada, será inmediatamente aplicable para el futuro, los cambios que se han producido con respecto a las aclaraciones editoriales, los cambios relacionados con el estado de la técnica y las regulaciones, sin afectar a las cláusulas del contrato entre el Suscriptor y TSP MediaCert, pero necesario para la supervisión cualitativa de los servicios de confianza. No obstante, si tuvieran un impacto en la economía del contrato entre el Suscriptor y TSP MediaCert, las partes se remitirán a los términos y condiciones previstos en las condiciones generales aplicables.

5.2.5 Control de acceso a la información disponible

Toda la información publicada en el sitio web de TSP MediaCert es accesible a los usuarios de lectura. Además, los documentos archivados en este sitio web están firmados electrónicamente para certificar su autenticidad.

El acceso a la información publicada en el sitio web de TSP MediaCert con fines de modificación se limita estrictamente a las funciones administrativas internas autorizadas. El control de acceso es realizado por servidores dedicados a esta función.

Además, podrán aplicarse medidas adicionales específicas a los servicios de confianza, tal como se definen en los siguientes subpárrafos.

5.2.5.1 Servicios de certificación

El acceso a los sistemas de publicación de información sobre el estado de los Certificados (adición, eliminación, modificación de la información publicada) se limita estrictamente a las funciones autorizadas del TSP MediaCert y se realiza mediante autenticación fuerte en servidores dedicados al control de acceso.

5.2.5.2 Servicios de marca de tiempo

Los servicios de marca de tiempo no están sujetos a ninguna medida adicional aparte de las descritas en el Capítulo 5.2.5.

5.2.5.3 Servicios de archivado

Los servicios de archivo no están sujetos a ninguna medida adicional aparte de las descritas en el capítulo 5.2.5.

5.3 Enmiendas al PG, PC-DPC, PH-DPH y PA

5.3.1 Procedimientos de modificación

El Comité MediaCert revisa periódicamente los documentos de los que es responsable.

Cuando se modifica uno de estos documentos, generalmente se revisa y valida. La aprobación de la enmienda es responsabilidad del Jefe del TSP MediaCert, que no realiza ningún cambio documental. Todas estas acciones se llevan a cabo durante una reunión del Comité MediaCert. Los miembros del Comité MediaCert notifican previamente las modificaciones a los Suscriptores y Usuarios afectados.

Sin embargo, no siempre es necesario modificar los documentos revisados. En efecto, los cambios de forma (ortografía, etc.) o las aclaraciones editoriales no están sujetos a validación y los documentos sujetos a notificación previa a los Suscriptores y Usuarios pueden ser actualizados sin notificación previa.

En el caso de un cambio importante en estos documentos, las siguientes entidades también pueden ser notificadas del cambio:

- el organismo encargado de la evaluación de la conformidad;
- ANSSI, como organismo nacional de control de los servicios de confianza;
- el SIAF, como organismo nacional de control de los archivos de Francia.

5.3.2 Gestión de OID

5.3.2.1 Construcción del OID

El OID de los documentos del TSP MediaCert se basa en el OID "**1.2.250.1.111**" asignado por AFNOR a Worldline y se construye de la siguiente manera: 1.2.250.1.1.1.111.**x**. **y**. **z**. **w** donde :

- **x**: Actividad Worldline. Aquí está el TSP MediaCert (Trust Service Provider → 20);
- **y:** número asignado a la política del Servicio de confianza correspondiente;

- **z :** número mayor de la versión del documento (por ejemplo: v3.1 → 3) ;
- **w:** específico para cada Servicio de confianza.

5.3.2.2 Circunstancias en las que debe modificarse el OID

Si el Comité MediaCert considera que un cambio en estos documentos repercute en el nivel de seguridad o confianza en el servicio de confianza pertinente, podrá definir una nueva versión del documento y asignarle un nuevo OID.

Si es probable que el OID de este documento evolucione, el Comité MediaCert tendrá en cuenta esta evolución en los documentos de referencia (PC-DPC, PH-DPH, PA, etc.).

5.4 Documentación Técnica de Prácticas Generales

TSP MediaCert cuenta con una Documentación Técnica de Prácticas Generales para su propio uso. Este documento detalla las medidas legales y de seguridad comunes a los diversos Servicios Fiduciarios implementados por Worldline. Estas medidas pueden ser organizativas, funcionales o técnicas.

5.5 Políticas de seguridad de la información aplicables

Las medidas definidas en la Política de Seguridad de la Información de Worldline se aplican en el ámbito de TSP MediaCert durante todas las fases de su ciclo de vida. Esta política define los objetivos de disponibilidad, integridad y confidencialidad de la información a través de una serie de normas de seguridad. Demuestra el compromiso de Worldline con la seguridad de la información. Debe considerarse como una referencia para todas las decisiones de seguridad. Esto se basa, en particular, en normas de seguridad reconocidas, como la norma[ISO 27001] y la guía de higiene de TI ANSSI[Higiene] para el nivel estándar.

Las medidas de seguridad de la información específicas de cada servicio de confianza podrán definirse en la documentación técnica pertinente para satisfacer sus necesidades específicas de seguridad.

La certificación TSP MediaCert garantiza que Worldline documenta y mantiene el PSI de Worldline y que se implementa dentro del alcance de todos los servicios de confianza. Esto incluye la responsabilidad de implementar controles de seguridad y procedimientos operativos para todos los sitios, sistemas, información y activos involucrados en la prestación del Servicio de Confianza. La PSI de Worldline se publica y se comunica a todos los empleados afectados por su alcance.

El Comité MediaCert es responsable de la correcta aplicación del PSI de Worldline en todos los Servicios de confianza. En particular, el Comité MediaCert vela por su correcta aplicación, incluso en caso de subcontratación de una función de servicio de confianza a un tercero. Para ello, en caso de subcontratación, el TSP MediaCert define, en su caso, las responsabilidades de sus subcontratistas y garantiza que los subcontratistas cumplan con todos los controles necesarios (véase el capítulo6.6) y la obligación de formar a sus empleados (véanse los capítulos7.3 y 7.4).

Las medidas de seguridad aplicadas a los Servicios de confianza son definidas y validadas por el Comité MediaCert. Se revisan periódicamente y en caso de cambios importantes, en particular en el caso de cambios que puedan tener un impacto en el cumplimiento, la adecuación o la eficacia del servicio. Cualquier cambio que afecte al nivel de seguridad deberá ser aprobado por el Comité MediaCert.

6 Organización de la gestión de los Servicios de confianza

6.1 Funciones y responsabilidades relacionadas con los servicios de confianza

La TSP MediaCert define explícitamente las funciones de confianza necesarias para garantizar su funcionamiento y seguridad. Las definiciones de las funciones de confianza se ponen a disposición de todo el personal interesado.
Las funciones realizadas en todos los componentes de los servicios de TSP MediaCert se distribuyen entre varios tipos de partes interesadas para garantizar la separación del conocimiento para tareas o funciones sensibles. Los roles de confianza involucrados en la organización de TSP MediaCert son los siguientes:

- Administrador de HSM: está a cargo de las instalaciones y configuraciones de las cajas criptográficas (HSM) del TSP MediaCert;
- Administrador de sistemas: está a cargo de la instalación, configuración y mantenimiento de los sistemas de confianza de TSP MediaCert para la gestión de servicios. Está autorizado para restaurar estos sistemas; también actúa como operador del sistema, siendo responsable de la operación diaria de los sistemas confiables de TSP MediaCert.
- Auditor del sistema: está autorizado a consultar los archivos y todos los registros de eventos de los sistemas de confianza de TSP MediaCert;
- Maestro de Ceremonias: es el encargado de dirigir la preparación y realización de las ceremonias de clave;
- Responsable de seguridad: se encarga de administrar la implementación de las prácticas de seguridad y de aplicar las restricciones técnicas definidas en el análisis de riesgos;
- Operador de registro: es el encargado de intervenir en el proceso de creación de Certificados;
- Portador secreto: garantiza la confidencialidad, integridad y disponibilidad de los secretos. Es el custodio de los secretos y llaves físicas para acceder a sus cajas fuertes. Es miembro de un equipo cuyos miembros tienen los mismos derechos para acceder a los repositorios ;
- Gestor de aplicaciones: es el encargado de monitorizar el servicio y su rendimiento. Coordina y/o realiza el mantenimiento correctivo y evolutivo de la aplicación;
- Jefe de TSP MediaCert: está a cargo de la implementación de este PG, PC-DPC y PH-DPH así como de la verificación de su aplicación. En particular, es el encargado de revocar un Certificado emitido por las autoridades de certificación de la TSP MediaCert. Como miembro del Comité MediaCert, también es el encargado de aprobar este documento, las políticas (PC-DPC, PH-DPH y PA) y los análisis de riesgo del TSP MediaCert;
- Subdirector de TSP MediaCert: está a cargo de las mismas funciones con el apoyo del Director de TSP MediaCert;
- Responsable de seguridad: es el encargado de definir las reglas de seguridad en torno al TSP MediaCert.

Cuando un nuevo miembro se inscribe en un puesto de confianza dentro del TSP MediaCert, la persona interesada debe firmar un documento en el que se reconozca su nombramiento, para que acepte el puesto, por el gerente de recursos humanos y por la persona a cargo del TSP MediaCert o uno de sus asistentes. Este documento se refiere al DTPG para que el futuro miembro del personal de confianza sea consciente de la descripción de su función y de las responsabilidades que se le han asignado. En particular, especifica:

- los compromisos del firmante y su correcta comprensión;
- en caso de modificación del documento DTPG, se informará al firmante.

Del mismo modo, cuando se pone fin a una función de confianza dentro de la certificación TSP MediaCert, la persona interesada debe firmar un documento en el que conste dicha terminación.

6.2 Número de personas necesarias

6.2.1 Número de personas necesarias por tarea

Dependiendo del tipo de operación realizada, el número y las funciones de las personas que estarán presentes, como actores o testigos, pueden ser diferentes. De hecho, algunas tareas delicadas, como la generación de un certificado de CA, requieren más de una persona en un puesto de confianza dentro del TSP MediaCert por razones de seguridad.

6.2.2 Número de personas necesarias por función

Algunas funciones de confianza están en manos de varias personas, de modo que TSP MediaCert puede garantizar la continuidad de sus servicios sin comprometer la seguridad de los servicios ofrecidos.

Se comprueba regularmente que se hayan cumplido todas las funciones de confianza definidas anteriormente.

6.3 Identificación y autenticación para cada función

Cada uno de los empleados en un puesto de confianza está claramente identificado por el TSP MediaCert a través de un inventario de funciones.

Cada entidad que opera un componente de un servicio TSP MediaCert comprueba, para cada uno de sus componentes, la identidad y las autorizaciones de cualquier miembro del personal, así como de cualquier persona externa involucrada en tareas sensibles.

Antes de utilizar una aplicación crítica que contribuya a un Servicio de Confianza, todo el personal debe ser identificado y autenticado con antelación. Todas las operaciones realizadas en los sistemas por el personal son trazables (véase el capítulo 12.5) y garantizan la responsabilidad de las acciones.

Cada asignación de una función de confianza a un miembro del personal de TSP MediaCert se notifica y documenta por escrito.

6.4 Separación de funciones

Por la presente, este PG autoriza que varias funciones sean desempeñadas por la misma persona. Sin embargo, como parte de las actividades de TSP MediaCert y por razones de seguridad,

algunas funciones no pueden ser realizadas por la misma persona. La separación de las funciones identificadas anteriormente se especifica en el DTPG.
En general, las funciones y responsabilidades se asignan sobre la base del principio del menor privilegio a fin de limitar el riesgo de conflicto de intereses y las oportunidades de acciones no autorizadas o de uso indebido de los activos que aplica el servicio fiduciario.

6.5 Relaciones con las autoridades

Las relaciones con las autoridades legales y reguladoras están aseguradas por los gerentes de TSP MediaCert como se define en el capítulo 6.1 de este documento, apoyándose si es necesario en los diversos departamentos apropiados de Worldline (departamento administrativo y legal, etc.).

En particular, son responsables de informar a las autoridades competentes en caso de que se produzca un incidente de seguridad , tal como se especifica en el DTPG.

6.6 Relaciones con los proveedores

La PSI Worldline define las medidas a aplicar a los proveedores para garantizar la aplicación de un nivel de seguridad al menos equivalente al definido en la PSI Worldline, para las actividades que se les confían. Las medidas integran los conceptos de formación y control.

Las relaciones con proveedores externos se formalizan sistemáticamente mediante un acuerdo contractual con el proveedor. Este acuerdo especifica las responsabilidades de cada parte.

En cualquier caso, el TSP MediaCert, en su fase inicial, evalúa los riesgos específicos de la externalización (control de los sistemas de información, acciones remotas, alojamiento compartido, etc.) con el fin de tener en cuenta, en cuanto se elaboren los requisitos aplicables al futuro prestador de servicios, las necesidades y medidas de seguridad adaptadas.
TSP MediaCert requiere que sus proveedores de servicios externos tengan un plan de garantía de seguridad (SAP) que formalice sus compromisos o imponga los requisitos de seguridad adecuados en el contrato de servicio.

6.7 Órganos de gobierno

La TSP MediaCert crea un único órgano de gobierno, denominado "MediaCert Committee", cuyas misiones son múltiples (validación de la documentación, revisión de los análisis de riesgo, etc.). Las personas presentes en las reuniones de este comité difieren según el tema de la reunión. Sin embargo, el responsable del TSP MediaCert, o uno de sus suplentes, está presente sistemáticamente. Los detalles están disponibles en el DTPG asociado.

6.8 Independencia de las partes y no discriminación

La organización creada en el marco del TSP MediaCert, dedicada a sus actividades con una función hermética, permite preservar la imparcialidad de las operaciones. Además, el TSP MediaCert asegura que las actividades del de confianza se lleven a cabo de manera equivalente para todos los beneficiarios que hayan aceptado los términos del servicio y cumplan con sus obligaciones.

En la medida de lo posible, TSP MediaCert implementará los enfoques apropiados para hacer su servicio accesible a cualquier persona con una discapacidad, teniendo en cuenta, caso por caso, las especificidades de cada solicitante.

En general, los servicios prestados por TSP MediaCert, como la generación de Certificados, la gestión de la revocación de Certificados, el archivo electrónico o la emisión de marcas de Tiempo, se realizan de forma independiente y, por lo tanto, no están sujetos a ninguna presión comercial que pueda perjudicar la ética y la conducta profesional de estos servicios de confianza prestados por TSP MediaCert. Esto está garantizado por el hecho de que la TSP MediaCert está centralizada dentro de una *Línea de Negocio Global*, una unidad que es transversal a las otras unidades de Worldline (ver Figura 2 - Diagrama de organización~~Figura 2 - Diagrama de organización~~).

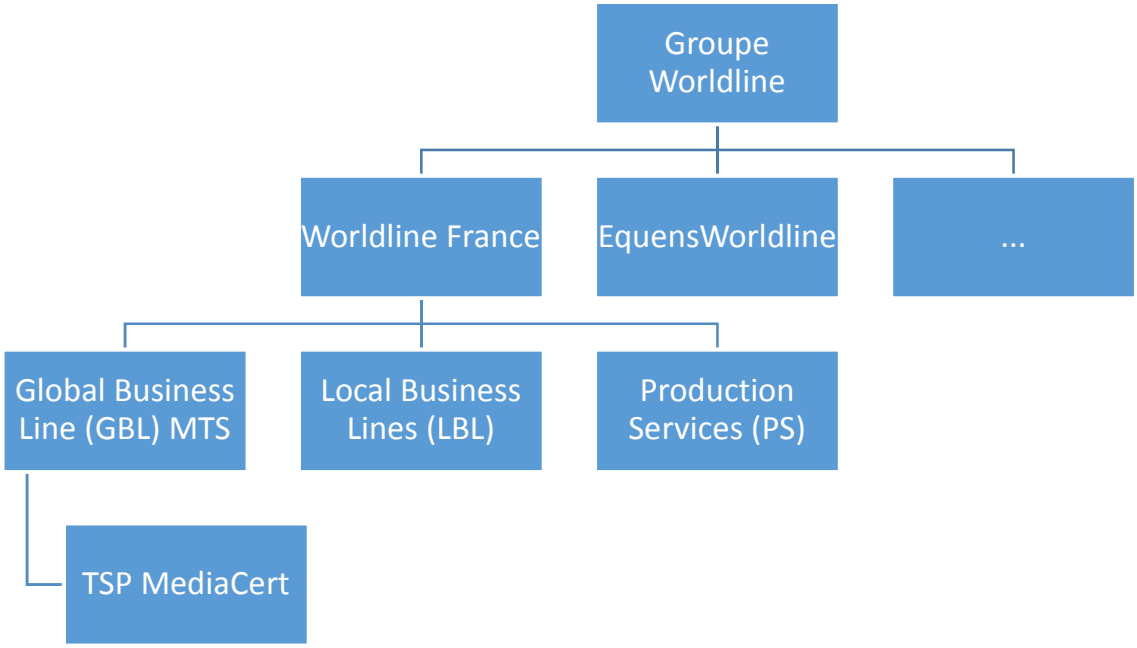

Figura 2 - Diagrama de organización

7 Seguridad de los recursos humanos

TSP MediaCert implementa una política de recursos humanos que contribuye a la confianza en las operaciones del servicio de confianza. En particular, la TSP MediaCert implementa los medios legales a su disposición para asegurar la honestidad del personal que impacta los servicios de confianza.

Además, los derechos y el acceso al sistema de información se actualizan en función de los cambios de personal (llegada, salida, cambios). En particular, todos los derechos asignados a una persona son revocados en el momento de su partida o en caso de cambio de función. Los procedimientos de llegada y salida se definen conjuntamente con la función de recursos humanos. Se tienen en cuenta:

- la creación y eliminación de cuentas de ordenador y buzones de correo asociados;
- los derechos y el acceso que debe concederse y retirarse a una persona cuya función cambia;
- la gestión del acceso físico a los locales (asignación, devolución de credenciales y llaves, etc.);
- la asignación de equipos móviles (ordenador portátil, llave USB, disco duro, smartphone, etc.);
- la gestión de documentos e información sensibles (transferencia de contraseñas, cambio de contraseñas o códigos en sistemas existentes).

Estos procedimientos se formalizan.

7.1 Cualificaciones, habilidades y autorizaciones requeridas

TSP MediaCert emplea personal y, cuando corresponde, proveedores con la experiencia, habilidades, calificaciones y conocimientos necesarios para operar un Servicio de Confianza.

El personal que desempeña funciones de confianza dentro del TSP MediaCert está informado de sus responsabilidades y de los procedimientos relacionados con la seguridad del sistema y el control del personal que deben cumplir.

El personal directivo está capacitado y es consciente de la seguridad y la gestión de riesgos, está familiarizado con los procedimientos de seguridad existentes y tiene suficiente experiencia en seguridad de TI para asumir plenamente sus responsabilidades en relación con los servicios prestados por TSP MediaCert.
Los procedimientos administrativos y de gestión de personal se diseñan y mantienen de acuerdo con los procedimientos de gestión de la seguridad de la información.

TSP MediaCert garantiza la cualificación y competencia de su personal que desempeña un papel de confianza.

7.2 Procedimientos de verificación de antecedentes

Existen procedimientos de verificación de antecedentes penales para las personas a las que se les pide que asuman un papel de confianza dentro de la Certificación de medios de TSP. En particular, estas personas no deben haber sido condenadas por un tribunal por ningún delito que pueda comprometer su participación en las actividades de TSP MediaCert, ni estar en conflicto de

intereses con sus deberes. En Francia, por ejemplo, las personas interesadas deben proporcionar una copia de su boletín de antecedentes penales nº 3 a Worldline Human Resources al firmar el documento (véase el capítulo 6.1) en el que aceptan su papel, obligaciones y responsabilidades en relación con su participación en estas actividades. En particular, las personas que actúan en un papel de confianza en nombre de TSP MediaCert son responsables de comunicar cualquier cambio en esta área. Sin embargo, el TSP MediaCert establece una verificación regular de la idoneidad de los antecedentes penales de sus miembros con el papel que desempeñan en su nombre.

El expediente de candidatura del candidato se envía al departamento de Recursos Humanos para su validación y al responsable del MediaCert TSP (véase el capítulo 6.3). No se conceden derechos de acceso hasta que se valida el expediente.

El personal responsable de la gestión de los servicios de confianza de TSP MediaCert no es responsable de los aspectos comerciales de estos servicios y está libre de cualquier conflicto de intereses que pueda influir en la forma en que se llevan a cabo las operaciones de las que es responsable y socavar la confianza (véase el capítulo 6.8). A este respecto, se comprometen a confirmar por escrito, una vez aceptada la función de confianza en el seno de TSP MediaCert, la ausencia de cualquier conflicto de intereses relacionado con el ejercicio de esta nueva actividad.
Cualquier personal con una situación conocida por TSP MediaCert que pudiera crear un conflicto de intereses considerado incompatible o que pudiera perjudicar la imparcialidad de las operaciones de servicios de confianza:

- no se le puede asignar un papel de confianza;
- puede ser eliminado de una función de confianza asignada previamente.

7.3 Requisitos de formación inicial

El personal está capacitado en el software, hardware y procedimientos operativos de TSP MediaCert. También es consciente de la seguridad de la información y, en particular:

- a cuestiones de seguridad;
- las normas que deben respetarse;
- el comportamiento correcto a adoptar en términos de seguridad de los sistemas de información.

Este personal ha tomado la medida y el conocimiento de las operaciones de las que es responsable.

Todo el personal de confianza recibe una formación típica sobre:

- seguridad y protección de datos personales;
- la legislación vigente;
- los principales riesgos y amenazas;
- el mantenimiento en condiciones seguras;
- autenticación y control de acceso;
- la configuración fina y el endurecimiento de los sistemas;
- partición de red;

- registro de actividad.

Esta formación puede ser adaptada en función del departamento y del puesto ocupado. Puede adoptar la forma de formación teórica, formación práctica con el apoyo de personal formado o una combinación de ambos.

7.4 Requisitos y frecuencias de la educación continua

El personal deberá recibir la formación necesaria antes de realizar cualquier cambio en los sistemas, procedimientos, organización u otros, en función de la naturaleza de dichos cambios. En particular, está capacitado en temas de seguridad de sistemas de información y se le informa sobre el manejo de incidentes.

En particular, las personas reciben formación periódica para mantener su nivel de experiencia, conocimientos y cualificaciones.

Además, se llevan a cabo periódicamente acciones de sensibilización dirigidas a todos los empleados. Estos cubren temas como:

- los objetivos y retos a los que se enfrenta TSP MediaCert en materia de seguridad de los sistemas de información (nuevas amenazas y prácticas de seguridad actuales);
- información considerada delicada;
- reglamentos y obligaciones legales;
- las normas e instrucciones de seguridad que rigen la actividad diaria: cumplimiento de la política de seguridad, no conexión de equipos personales a la red de la entidad, no divulgación de contraseñas a terceros, no uso de contraseñas profesionales en el ámbito privado y viceversa, denuncia de hechos sospechosos, etc;
- los medios disponibles y que contribuyen a la seguridad del sistema: bloqueo sistemático de la sesión cuando el usuario abandona su puesto de trabajo, herramienta de protección de contraseña, etc.

7.5 Frecuencia y secuencia de rotación entre las distintas atribuciones

No existe una rotación definida dentro de esta GL entre las diferentes asignaciones.

7.6 Sanciones en caso de acciones no autorizadas

Las reglas internas de Worldline establecen que se aplicarán las sanciones disciplinarias administrativas apropiadas en caso de mala conducta (incumplimiento de este PG,...). En particular, al personal se le recuerda esto en el compromiso de las responsabilidades que aceptan al aceptar su papel dentro del TSP MediaCert.

Las entidades fuera de Worldline que participen en las actividades de TSP MediaCert están sujetas a las sanciones definidas durante la contractualización en caso de mala conducta (incumplimiento de este PG,...).

7.7 Requisitos para el personal de los proveedores de servicios externos

El personal de cualquier proveedor de servicios externo que trabaje en las instalaciones y/o componentes del TSP MediaCert debe cumplir con los requisitos establecidos en los capítulos 7.1 a 7.4 este documento.

7.8 Documentación proporcionada al personal

Como mínimo, cada persona tiene documentación relacionada con los procedimientos operativos y las herramientas específicas que implementa, así como las políticas y prácticas generales del componente del servicio en el que trabaja.

8 Gestión de Activos

8.1 Responsabilidades de los activos

De acuerdo con las reglas definidas en la PSI Worldline, la TSP MediaCert:

- realiza regularmente un inventario de todos los activos de los Servicios de confianza que presta;
- designa a un propietario/responsable de los activos en cuestión.

8.2 Clasificación de la información

Los datos de TSP MediaCert se clasifican de acuerdo con la Política de clasificación de datos de Worldline. Además, sigue las reglas para el manejo de la información de acuerdo con su sensibilidad, tal como se define en el Estándar de Protección de la Información de Worldline.

Esta clasificación de la información se deriva del análisis de riesgos y se mantiene de acuerdo con sus resultados (véase el capítulo 4).

Esta clasificación permite aplicar un nivel de protección adecuado. Todos los activos se manejan de acuerdo con este documento de clasificación de información y procedimientos asociados. En particular, se establecen medidas para el final de la vida útil, de modo que los activos al final de su vida útil que contengan información sensible puedan ser destruidos o desmantelados de forma segura (véase el capítulo11.5).

9 Control de acceso

9.1 Acceso físico

Los sitios y locales que albergan TSP MediaCert garantizan la seguridad física de los medios implementados para la prestación de los Servicios de Confianza. Todos los medios puestos en marcha para garantizarlo se especifican en la DTPG.

Se establecen medidas de control de acceso físico para garantizar que las personas no autorizadas no puedan acceder a los sistemas de servicios de confianza críticos. Estos controles minimizan los riesgos asociados con la seguridad física de los activos. En particular:

- Los componentes críticos[1] están aislados dentro de perímetros de seguridad claramente definidos y sólo son accesibles a personas autorizadas;
- Los perímetros de seguridad están sujetos a medidas de protección contra intrusiones físicas, medidas de control de acceso y alarmas de intrusión;
- se han adoptado medidas para evitar el robo, la destrucción o el deterioro de los componentes, así como la interrupción del servicio;
- se han establecido medidas contra el compromiso o el robo de información confidencial;
- existen medidas para evitar que el equipo, la información, los medios y el software relacionados con los servicios de TSP MediaCert sean retirados del sitio sin autorización.

9.2 Acceso lógico

El acceso lógico a los servidores de TSP MediaCert, a las herramientas de desarrollo colaborativo y a las aplicaciones, se supervisa y verifica regularmente (véase el capítulo 9.4).

9.3 Acceso a la red

Las medidas de control de acceso a la red se presentan en el Capítulo 13.1 de este documento. En particular, las conexiones de equipos personales están prohibidas en la red de TSP MediaCert.

9.4 Gestión de los derechos de acceso

La TSP MediaCert establece una gestión de los derechos de acceso sobre la base del principio del mínimo privilegio y revisa periódicamente la asignación de estos derechos de acceso.

Esta gestión de los derechos de acceso a los sistemas e información de TSP MediaCert es interna y se especifica en el documento DTPG.

9.5 Administrar cuentas, contraseñas y sesiones

[1] La criticidad se define por la clasificación de la información derivada del análisis de riesgos.

Las reglas de administración de cuentas, las contraseñas y las sesiones de acceso a los sistemas TSP MediaCert están establecidas para garantizar una solidez de identificación con mínima información de identificación y acceso al sistema.

Estas reglas son internas y se especifican en el documento DTPG.

10 Mediciones criptográficas

Existen medidas de seguridad y procedimientos de control adecuados para la gestión de claves criptográficas y módulos criptográficos (HSM) a lo largo de su ciclo de vida.

10.1 Estándares y medidas de seguridad para módulos criptográficos

Los HSMs utilizados por el TSP MediaCert, para la generación de CA, TSU Key Twins y los correspondientes a los diferentes Certificados emitidos por las CAs, son HSMs que cumplen con los requisitos definidos en las políticas asociadas a cada servicio de confianza relevante.

Estos HSM están dedicados a los servicios proporcionados por TSP MediaCert.

TSP MediaCert garantiza la seguridad de los HSM que utiliza a lo largo de su ciclo de vida. En particular, se han establecido procedimientos para:

- garantizar la integridad de estos HSM durante el transporte;
- garantizar la integridad de estos HSM durante el almacenamiento;
- garantizar la integridad de estos HSM durante su funcionamiento;
- garantizar el correcto funcionamiento de estos HSMs.

Para los servicios cualificados en el sentido del Reglamento eIDAS, TSP MediaCert utiliza únicamente HSM que han sido cualificados en el nivel reforzado por la ANSSI.

10.2 Gestión de pares de claves

10.2.1 Generaciones de pares de claves

10.2.1.1 Pares de claves CA y TSU

La generación de los pares de claves CA o TSU se lleva a cabo durante una Ceremonia de Claves. Estas ceremonias de claves están teniendo lugar:

- utilizando un HSM físicamente aislado que cumpla los requisitos definidos en el capítulo 10.1 de este documento;
- en los locales seguros de TSP MediaCert (ver Capítulo 11);
- bajo el control permanente de al menos dos (2) personas que ocupen un puesto de confianza dentro del TSP MediaCert entre: el titular secreto, el maestro de ceremonias, el administrador de HSM y el administrador de la aplicación (ver capítulo 6.1);
- de acuerdo con un documento de organización y un documento técnico, ambos firmados por todos los participantes, en particular por el maestro de ceremonias.

La clave privada de cada CA y TSU se implementa y permanece en las instalaciones seguras de TSP MediaCert.

10.2.1.2 Claves de autenticación para un componente de un servicio TSP MediaCert

Las claves de autenticación de un componente de un servicio TSP MediaCert se generan durante una ceremonia de claves. Esto se puede hacer al mismo tiempo que para las claves CA o TSU. Esta ceremonia tiene lugar en las mismas condiciones que las descritas en el capítulo 10.2.1.1

10.2.1.3 Otros

Cada servicio de TSP MediaCert puede definir sus propios requisitos en términos de generación de pares de claves para otros usos de acuerdo con los requisitos criptográficos aplicables.

10.2.2 Transmisión de la clave pública a los usuarios

El medio de transmisión de la clave pública a los Usuarios es específico para cada servicio de TSP MediaCert. Por lo tanto, esta información se encuentra en las políticas asociadas a cada servicio de confianza.

10.2.3 Tamaño del par de claves y algoritmo

El tamaño de las Dos Llaves y los algoritmos utilizados por el TSP MediaCert cumplen con los requisitos[ETSI 119 312], los requisitos[RGS B1] y las recomendaciones de la ANSSI[SOGIS_CRYPTO].

10.2.4 Comprobación de la clave privada

El control de las claves privadas de CA, las copias de seguridad correspondientes y las claves privadas de las TSUs lo lleva a cabo personal de confianza: titulares de secretos y administradores de HSM (véase el capítulo 6.1); en un entorno protegido. Este control se realiza mediante datos de activación, denominados "secretos", distribuidos entre varias personas identificadas como portadoras secretas.

10.2.5 Fideicomiso de clave privada

TSP MediaCert no ofrece un servicio de custodia de clave privada con fines de cobro.

10.2.6 Copia de seguridad de la clave privada

Esta operación se realiza bajo el control de varias personas durante una Ceremonia de Claves. De hecho, las copias de seguridad de las claves privadas se realizan en las mismas condiciones que las presentadas en el capítulo 10.2.1.1.

Los procedimientos de respaldo se realizan de acuerdo con las especificaciones del proveedor de TSP MediaCert HSM.

El número de copias se limita al mínimo necesario para garantizar la continuidad de los servicios de TSP MediaCert.

10.2.7 Archivado de la clave privada

TSP MediaCert no ofrece un servicio de archivado de claves privadas.

10.2.8 Transferencia de la clave privada desde/hacia el módulo criptográfico

Las claves privadas de CA se generan dentro de un HSM (véase el capítulo 10.2.1.1) y sólo se transfieren a otro HSM en el caso de copias de seguridad (véase el capítulo 10.2.6).

Durante una transferencia, la clave privada se cifra con un algoritmo recomendado por el fabricante de HSM para garantizar la seguridad de la información. La clave privada cifrada no puede ser descifrada sin el uso de componentes criptográficos de hardware y la acción de personas identificadas en las funciones de confianza necesarias.

10.2.9 Almacenamiento de la clave privada

Las claves privadas de CA y TSU se almacenan en un HSM físicamente seguro que cumple los requisitos definidos en el capítulo 10.1 de este documento. Lo mismo se aplica al almacenamiento de copias de seguridad de claves privadas de CA.

Existen procedimientos en torno a estos HSM para garantizar la confidencialidad de su contenido.

10.2.10 Método de activación de la clave privada

Las claves privadas de CA sólo pueden activarse con datos de activación en poder de dos (2) personas en un puesto de confianza dentro de TSP MediaCert.

La activación de una clave privada de CA sólo puede realizarse durante una Ceremonia de Claves documentada y rastreada.

10.2.11 Método de desactivación de la clave privada

La desactivación de las claves privadas de CA en el HSM es automática en cuanto se detiene.

10.2.12 Método de destrucción de las claves privadas

Las claves privadas de CA, las copias de seguridad correspondientes y las claves privadas de las TSU se eliminarán del recurso criptográfico de acuerdo con los procedimientos del fabricante. Las operaciones de destrucción se llevan a cabo durante un procedimiento auditado como la Ceremonia de Claves.

Al final de su vida normal o anticipada (por revocación) de una clave privada de CA o TSU, se destruye sistemáticamente, así como cualquier copia y cualquier elemento que permita su reconstitución. Además, si el recurso criptográfico de hardware que alberga las claves privadas antes mencionadas debe ser desmantelado, entonces ellas también deben serlo.

10.3 Datos de activación de la clave privada de CA

10.3.1 Generación e instalación

Los datos de activación de clave privada de CA se generan en un HSM durante ceremonias de llave bajo el control de dos (2) personas en funciones de confianza, se almacenan en tarjetas inteligentes y luego se entregan a los poseedores secretos que conservan los datos de activación (véase el capítulo 10.2.10). Estos datos de activación sólo los conocen los responsables que se identifican por su nombre en el contexto de la función de confianza que se les ha asignado.

10.3.2 Protección

Los datos de activación están protegidos por mecanismos criptográficos y de control de acceso físico. Los portadores de secretos son responsables de proteger los secretos de los que son responsables. Un poseedor de un secreto no posee más de un dato de activación por CA.

11 Seguridad física y ambiental

TSP MediaCert ha puesto en marcha un conjunto de medidas de seguridad física para garantizarlo:

- los medios, sistemas de información y datos utilizados en la implementación operativa del TSP MediaCert están instalados en locales seguros, cuyo acceso está controlado y restringido a personal estrictamente autorizado. El sistema de control de acceso físico permite garantizar la trazabilidad nominativa del acceso a los locales que albergan los medios y la información del TSP MediaCert (véase el capítulo 9.1);

- la aplicación de estos controles permite respetar la separación de funciones fiduciarias prevista en las presentes OGM (véase el capítulo 6.4).

A continuación se muestra una lista de medidas ambientales implementadas para garantizar la disponibilidad de equipos alojados y la continuidad de los servicios proporcionados por TSP MediaCert. En el documento DTPG se ofrecen detalles al respecto.

11.1 Ubicación geográfica y construcción del sitio

Los entornos TSP MediaCert se instalan en ubicaciones de producción de TI europeos seguros de Worldline. Estas localizaciones están diseñados para alojar sistemas de TI y telecomunicaciones. Los equipos administrativos y operativos de TSP MediaCert operan en las localizaciones europeos de Worldline.

11.2 Suministro de energía y aire acondicionado

Existen una serie de medidas (generadores de emergencia, etc.) para prevenir los cortes de energía y simplificar las operaciones de mantenimiento. Del mismo modo, se aplican medidas (redundancia del sistema, etc.) para evitar fallos en el sistema de aire acondicionado. Estas medidas preventivas se mantienen y prueban regularmente.

11.3 Vulnerabilidad a los daños causados por el agua

Los medios de monitoreo (sensores, monitoreo,...) están en su lugar para prevenir daños causados por el agua. Estos sistemas de monitoreo son mantenidos y probados regularmente.

11.4 Prevención y protección contra incendios

Las medidas de prevención y control de incendios (detectores, puertas cortafuegos, etc.) se aplican para prevenir cualquier riesgo de incendio y para proteger los sistemas de TSP MediaCert en caso necesario. Estas medidas preventivas y de protección se mantienen y prueban regularmente.

11.5 Desmantelamiento de las ayudas

Todos los documentos en papel que contengan datos confidenciales (código PIN, contraseña,...) que ya no sean necesarios o estén obsoletos se destruyen físicamente.

Para los medios físicos (discos, HSM,...) se establece un procedimiento especial de almacenamiento intermedio para la destrucción. Esta destrucción da lugar a la elaboración de un Acta.
En particular, si un HSM está desactivado, las teclas se borran de antemano mediante las funciones de "puesta a cero" del HSM.

El equipo, los datos, los medios y el software operados en el área segura no pueden ser retirados del sitio sin autorización.

12 Gestión operativa

12.1 Medidas de seguridad del sistema informático

12.1.1 Requisitos técnicos de seguridad específicos de los sistemas informáticos

Los requisitos mínimos de seguridad técnica implementados por TSP MediaCert cumplen los siguientes objetivos:

- identificación de usuario y autenticación fuertes para el acceso al sistema (ver capítulo 9.2);
- protección de la red contra el acceso no autorizado (véase el capítulo 9.3);
- la gestión de los derechos de usuario y de cuenta (véanse los capítulos 9.4 y 9.5);
- gestión de las sesiones de usuario: desconexión tras un período de inactividad, acceso a los archivos controlados por función y nombre de usuario (véase el capítulo 9.5);
- funciones de auditoría: no repudio, responsabilidad y naturaleza de las acciones realizadas (véase el capítulo 15);
- aplicación de procedimientos de cambio para la entrega, modificación y resolución urgente de problemas de software (ver capítulo 12.2);
- protección contra virus, software malicioso o no autorizado y actualizaciones de software (ver capítulo 12.3);
- aplicación de procedimientos de cambio para cualquier modificación de las configuraciones de software (véase el capítulo 12.8);
- protección de la red para garantizar la confidencialidad e integridad de los datos transmitidos a través de ella (véase el capítulo 13);
- redundancia de las conexiones de red para garantizar la accesibilidad en caso de un simple fallo.

Existen dispositivos de monitoreo, con registro y alarma automáticos, así como procedimientos para auditar la configuración del sistema, en particular los elementos de enrutamiento y los procedimientos de respuesta a incidentes.

12.1.2 Nivel de cualificación de los sistemas informáticos

TSP MediaCert utiliza sistemas fiables para almacenar los datos que se le proporcionan en una forma verificable para que:

- los datos sólo se pongan a disposición del público para su tratamiento después de haber obtenido el consentimiento de la persona afectada por los datos;
- sólo las personas autorizadas pueden introducir y modificar los datos almacenados;
- la autenticidad de estos datos puede ser verificada.

Los detalles se proporcionan cuando es necesario en las políticas asociadas a cada servicio.

12.1.3 Manipulación y seguridad de los soportes

Los medios utilizados por TSP MediaCert se manejan de forma segura, de acuerdo con procedimientos definidos, para protegerlos de daños, robos, accesos no autorizados y obsolescencia.

Las medidas se refieren específicamente a la reutilización de los medios de comunicación que han contenido información en otro contexto, de modo que las personas no autorizadas no puedan acceder a ella.

Los soportes que contengan datos sensibles se eliminarán de acuerdo con la definición del capítulo 11.5 este documento.

Los soportes de copia de seguridad están sujetos a las medidas específicas descritas en el 12.4.1.

12.2 Procedimientos y responsabilidades operativas

Los procedimientos operativos del TSP MediaCert se documentan y se ponen a disposición de los equipos interesados, en particular de todo el personal administrativo o del personal que desempeña una función de confianza que pueda tener un impacto en la prestación del Servicio de Confianza.

En particular, se han establecido procedimientos de supervisión de cambios para controlar las implementaciones de software, las actualizaciones y las soluciones de emergencia, así como los cambios en las configuraciones de los sistemas que intervienen en la prestación de servicios fiduciarios. TSP MediaCert se basa en una herramienta interna de Worldline para realizar un seguimiento de los cambios e incidentes relacionados con el funcionamiento de sus servicios. La herramienta se utiliza para documentar todos los cambios realizados.

TSP MediaCert garantiza que los diferentes entornos del entorno de producción se distinguen para todos los sistemas de Trusted Services operados.

12.3 Protección contra el malware

TSP MediaCert implementa un conjunto de soluciones para proteger sus plataformas de producción y estaciones de administración contra virus y software malicioso o no autorizado. Estas soluciones se especifican en el DTPG.

12.4 Copias de seguridad

12.4.1 Conservación de los soportes

Como parte de las actividades de TSP MediaCert, se realizan copias de seguridad de diferente naturaleza. A continuación, se establecen medidas para garantizar la disponibilidad, confidencialidad e integridad de los medios de copia de seguridad utilizados. Estas medidas se describen en la DTPG. Estas medidas podrán abordar, cuando proceda, los problemas de obsolescencia y deterioro de los medios de comunicación, en particular cuando sea necesario conservar los datos durante largos períodos.

12.4.2 Copias de seguridad externas

Como parte de este PG, TSP MediaCert está implementando copias de seguridad externas de acuerdo con los procedimientos definidos por Worldline.

12.5 Registro y monitoreo

12.5.1 Registro de actividades

Las medidas de registración de actividad implementadas se describen en el 15.1 de este documento.

12.5.2 Monitorización de registros de eventos

Los registros de eventos se inspeccionan cuando son emitidos por herramientas especificadas en el DTPG. Estas herramientas permiten, en particular, activar automáticamente alarmas para notificar al gestor de eventos un posible incidente detectado, en particular un incidente de seguridad crítica.

12.5.3 Supervisión de la capacidad

Periódicamente se realiza una proyección de las futuras necesidades de capacidad de las plataformas del TSP MediaCert, generalmente en reuniones organizadas por el Comité MediaCert. En particular, se supervisa la capacidad de estas plataformas (disponibilidad y uso de servicios) para garantizar una capacidad adecuada de procesamiento y almacenamiento.

12.5.4 Control de seguridad

Se implementa una herramienta (SIEM) para procesar registros de eventos (análisis, correlación) con el fin de identificar y reportar alertas de seguridad. La TSP MediaCert se apoya especialmente en un equipo dedicado a estas actividades (SOC) para informar de las alertas de seguridad y así cumplir con los requisitos a los que está sujeta.

En particular, se supervisan los siguientes eventos:

- funciones de parada e inicio de la generación de trazas;
- actividad anormal en la red.

El TSP procesa las alertas de acuerdo con los procedimientos descritos en el Capítulo 14.

Se lleva a cabo una revisión regular con este equipo para revisar los eventos anormales y prevenir cambios de configuración.

12.5.5 Monitorización de la instalación

Los sistemas de TSP MediaCert son monitoreados usando varias herramientas para asegurar que estén funcionando correctamente.

12.6 Dominio del software en funcionamiento

TSP MediaCert domina el software (inventario, versiones,...) instalado en sus sistemas. Además, sólo se instala el software necesario en los sistemas en producción. Estos productos de software han sido seleccionados por su fiabilidad y capacidad para garantizar la seguridad y continuidad de

los servicios que proporcionan. Están sujetos a medidas de seguridad para protegerlos de cualquier modificación o alteración.

Los sistemas se endurecen eliminando las cuentas, aplicaciones, servicios, protocolos y puertos no utilizados.

Los derechos de instalación en los distintos entornos de los servicios de confianza de TSP MediaCert Trust Services son limitados y están sujetos a procedimientos de cambio (véase el capítulo12.2).

12.7 Gestión técnica de vulnerabilidades

La TSP MediaCert proporciona gestión de vulnerabilidades técnicas a través de:

- la implementación de procesos de gestión de parches;
- la realización de un seguimiento técnico;
- de exploraciones de vulnerabilidades.

Estos procesos están disponibles en el documento DTPG.
Estos procesos permiten detectar posibles vulnerabilidades y crear planes de corrección de vulnerabilidades para mantener el sistema de información en óptimas condiciones de seguridad. Es posible que una vulnerabilidad no sea objeto de un plan de corrección, sin embargo, el TSP MediaCert documenta los elementos que justifican este arbitraje.

Cualquier vulnerabilidad crítica debe ser tratada dentro de las cuarenta y ocho (48) horas de su descubrimiento.
Estos procesos también aseguran que:

- Los parches se aplican dentro de un tiempo razonable después de que están disponibles;
- no se aplican parches si introducen vulnerabilidades o inestabilidades que compensan sus beneficios teóricos;
- si no se aplica un parche, se documentan las razones de esta decisión.

Las exploraciones de vulnerabilidades son realizadas regularmente por personal con las habilidades, herramientas, ética e independencia necesarias para producir un informe fiable.

12.8 Adquisición, desarrollo y mantenimiento de sistemas de información

La implementación, configuración y cualquier modificación o actualización de un sistema para implementar los componentes de un servicio TSP MediaCert está documentada y controlada (ver Capítulo 12.6). Cualquier cambio que afecte al nivel de seguridad deberá ser aprobado por el Comité de Certificación de Medios de Comunicación.

Los desarrollos se realizan de acuerdo con la política de desarrollo seguro de Worldline. Esto cubre el diseño, desarrollo, pruebas y despliegue en la producción. Se basa en buenas prácticas de seguridad reconocidas. Se realiza un análisis de los requisitos de seguridad en el momento del diseño o selección de cada uno de los componentes de la arquitectura para garantizar que la seguridad se tiene en cuenta en los sistemas de TI.

TSP MediaCert no utiliza desarrollos subcontratados para servicios de confianza.

Los desarrollos se pasan sistemáticamente a una herramienta de análisis automático para controlar la calidad del código.

Los desarrollos están sujetos a pruebas de funcionamiento y aceptación antes de su entrega a producción.

Los datos de producción no se copian en entornos de preproducción, prueba o desarrollo. Para las pruebas y desarrollos se utilizan datos anónimos o de pruebas.

13 Seguridad de las comunicaciones

13.1 Gestión de acceso a la red

TSP MediaCert está implementando medidas para proteger su red contra posibles ataques.

13.1.1 Partición de red

Las plataformas de TSP MediaCert están alojadas en áreas de red separadas, dependiendo de su función y sensibilidad. Los componentes críticos de la red se mantienen en un entorno seguro. La sensibilidad de los distintos elementos se determina en función de los resultados del análisis de riesgos. TSP MediaCert aplica los mismos controles de seguridad a todos los componentes de un área de red.

En particular, se supervisan los flujos de red hacia el TSP MediaCert, así como entre las distintas zonas de la red (véase el capítulo 13.2) para evitar cualquier flujo no autorizado (incluidos los flujos procedentes de usuarios o abonados al servicio). En particular, los dispositivos de control de red están configurados para prohibir todos los protocolos y los accesos que no son necesarios para las operaciones de servicio de confianza.
Las configuraciones están sujetas a revisiones periódicas.

Los entornos de producción y de pruebas/desarrollo también están compartimentados.

Para documentar la partición, el TSP MediaCert crea y mantiene un esquema de red simplificado (o mapeo) que representa las diferentes zonas IP y el plan de direccionamiento asociado, los equipos de enrutamiento y seguridad (cortafuegos, relés de aplicación, etc.) y las interconexiones con el mundo exterior (Internet, redes privadas, etc.) y los socios. Este esquema permite localizar los servidores que contienen la información sensible de la entidad.

13.1.2 Acceso a plataformas

Las plataformas TSP MediaCert están sujetas a restricciones de acceso lógico (véase el capítulo 9.3) y no son directamente accesibles. El proceso para el acceso lógico a las plataformas TSP MediaCert es interno y se describe en el DTPG. La gestión del control de acceso está bajo el control de TSP MediaCert. Esta gestión incluye la gestión de cuentas y le permite modificar o eliminar los accesos sin demora. Los derechos y privilegios de acceso a las plataformas se asignan de acuerdo con la política de acceso lógico definida por TSP MediaCert.

El sistema de control de acceso existente permite, en particular, una gestión eficaz y adecuada de los accesos:

- permite una separación de funciones, en particular entre las operaciones de administración y otras operaciones a nivel de empresa, utilizando redes dedicadas a cada uno de los usos;
- permite controlar y restringir el uso de diferentes aplicaciones y utilidades.

Los sistemas utilizados para la administración están dedicados a este propósito.

Las pruebas de penetración se llevan a cabo cuando se configura la infraestructura de servicio y luego en cada cambio o modificación importante. Debido a su criticidad y a la importancia de proporcionar un informe fiable, las pruebas de penetración sólo pueden ser realizadas por

personal seleccionado en base a criterios tales como sus habilidades, conocimientos, efectividad, ética e independencia.

13.1.3 Acceso a los servicios

Los servicios de TSP MediaCert no están en contacto directo con redes abiertas a Internet. Los gateways que permiten el acceso están protegidas contra intrusiones o intentos de ataque.

Estos gateways limitan los servicios y protocolos abiertos sólo a aquellos servicios esenciales para la operación de los servicios proporcionados por TSP MediaCert. Se actualizan periódicamente para tener en cuenta la evolución de los sistemas de lucha contra las intrusiones y colmar las posibles lagunas en materia de seguridad.

13.2 Transferencia de información

En el caso de que no estén ubicados en una red dedicada, todos los flujos de comunicación entre los equipos de TSP MediaCert son exclusivamente a través de protocolos de comunicación de red seguros que garantizan la confidencialidad e integridad de la comunicación.

13.3 Redundancia

La conexión externa es redundante para proporcionar un alto nivel de disponibilidad del servicio.

14 Gestión de incidentes

En el caso de una escalada de alertas, TSP MediaCert ha establecido un sistema de gestión de incidencias para responder de forma coordinada y rápida a los incidentes con el fin de limitar su impacto.

14.1 Gestión de incidentes de seguridad

Se han establecido procesos de gestión de incidentes para limitar las consecuencias de tales incidentes e informar a las partes interesadas de manera oportuna. En particular, el seguimiento de las alertas que puedan estar relacionadas con un incidente de seguridad lo lleva a cabo el personal con un rol de confianza. Este personal se asegura de que la notificación y el procesamiento de estos incidentes se lleve a cabo de acuerdo con los procedimientos de gestión de incidentes establecidos por TSP MediaCert.

Además, en caso de compromiso de los Servicios de confianza, se notifica a las autoridades legales competentes si la naturaleza del compromiso así lo requiere. En particular, un incidente de seguridad comprobado que afecte a la integridad del servicio de confianza o que comprometa los datos personales deberá notificarse en un plazo de veinticuatro (24) horas:

- a la ANSSI en todos los casos, siguiendo el procedimiento recomendado por la ANSSI;
- a la CNIL en caso de que el incidente afecte a los datos personales.

TSP MediaCert también notificará a los suscriptores afectados.

Estos procesos incluyen la revisión de incidentes para asegurar el seguimiento de los planes de acción correctivos y preventivos para prevenir la repetición de tales incidentes.

También prevén el establecimiento de una vigilancia para detectar los incidentes de seguridad lo antes posible (véase el capítulo 12.5.4).

14.2 Procedimientos de gestión de incidentes de seguridad

Se establecen procedimientos para garantizar una respuesta adecuada a los incidentes propuestos. Para ello, TSP MediaCert se basa en la Política de Gestión de Incidentes de Worldline, que se ocupa en particular de la clasificación y notificación de incidentes de seguridad. A este respecto, la TSP MediaCert tiene su propio procedimiento de notificación, descrito en la DTPG.

Estos procedimientos abordan, en particular, el caso de compromiso de los Servicios de confianza y las interrupciones del servicio. Además, en caso de corrupción de los recursos de TI o de incidentes técnicos, TSP MediaCert ha implementado un Plan de Continuidad y Reanudación del Negocio para cada uno de los servicios de confianza que presta (ver Capítulo 16.2).

15 Recopilación de pruebas

15.1 Registro de actividades

Los eventos que intervienen en la vida de la TSP MediaCert se registran como archivos de generaciones automatizadas por software y se complementan, si es necesario, con entradas manuales. La finalidad de estos ficheros es garantizar la trazabilidad y responsabilidad de las operaciones realizadas (autores, sellos de tiempo, etc.).

Los registros de eventos incluyen explícitamente el identificador del ejecutante (software o humano), la fecha y hora de la operación y la naturaleza del evento.

Podrán ponerse a disposición de los tribunales a petición legal de los solicitantes.

15.1.1 Tipo de eventos registrados

La TSP MediaCert registra los eventos relacionados:

- seguridad (incluido el acceso o el intento de acceso);
- las actividades y el ciclo de vida de los sistemas de los servicios de confianza que presta.

Estos registros de eventos pueden ser electrónicos o manuscritos. Todos estos eventos se enumeran en la documentación técnica de DTPG relativa a este documento.

15.1.2 Frecuencia de procesamiento del registro de eventos

Los sistemas de monitorización implementados (véase el capítulo 12.5.2) registran los procesos tan pronto como se recogen.

15.1.3 Frecuencia de almacenamiento de los registros de eventos

Los registros de eventos se exportan con el tiempo a un servidor remoto.

15.1.4 Período de retención del registro de eventos

Los registros de eventos se mantienen durante diferentes períodos de tiempo dependiendo del tipo de evento y del servicio de confianza involucrado. Estos períodos de retención se especifican en las políticas asociadas con los diversos servicios de fideicomiso de TSP MediaCert.

15.1.5 Protección de registros de eventos

Los registros electrónicos de eventos se recogen a través del sistema descrito en el capítulo 15.1.7 de este documento y luego se externalizan a dos tipos de entornos (supervisión y protocolización) cuyas administraciones son diferentes. Por lo tanto, el acceso a estos elementos sólo es posible para el personal autorizado por TSP MediaCert, tal y como se define en el documento DTPG, y no puede modificarse o eliminarse sin autorización.

Los registros de eventos escritos a mano están protegidos por sistemas físicos seguros como cajas fuertes o gabinetes cuyos accesos son controlados por el TSP MediaCert.
Estos sistemas garantizan la integridad y confidencialidad de los registros de eventos.

15.1.6 Procedimiento para realizar copias de seguridad de los registros de eventos

El procedimiento para realizar copias de seguridad de los registros de eventos de TSP MediaCert es interno y se especifica en el documento DTPG.

15.1.7 Sistema de recogida de datos de registro de eventos

El sistema de recopilación de registros de eventos de TSP MediaCert es interno y se especifica en el documento DTPG.
Esto tiene en cuenta la sensibilidad de la información recogida y analizada.

15.1.8 Notificación de la inscripción de un evento al gestor de eventos

No hay notificación sistemática de la grabación de un evento al gestor de eventos.

15.2 Archivo

15.2.1 Protección de los archivos

La confidencialidad de los archivos está garantizada por una gestión adecuada de los accesos físicos, de sistemas y de redes. Garantiza la integridad y confidencialidad de los archivos.

Durante su período de retención en las instalaciones seguras de TSP MediaCert, los archivos están protegidos en integridad y son accesibles sólo a personas autorizadas. En efecto, la solicitud de acceso a un archivo sólo puede ser realizada por el jefe de la TSP MediaCert, un jefe adjunto de la TSP MediaCert o el responsable de seguridad de la TSP MediaCert con el fin de garantizar la confidencialidad de la información.

Se han establecido procedimientos para evitar la obsolescencia y el deterioro de los archivos. En particular, se almacenan en locales sujetos a medidas de protección contra las amenazas naturales.

15.2.2 Procedimiento de copia de seguridad de archivo

El nivel de protección del archivo comprimido es equivalente al nivel de protección de la copia de seguridad. Los procedimientos de copia de seguridad de archivo son internos y se especifican en el documento DTPG.

15.2.3 Requisitos de marca de tiempo de los datos

Todos los eventos tienen una fecha precisa con la hora del sistema de los servidores MediaCert de TSP. Los servidores de TSP MediaCert sincronizan su reloj interno regularmente (al menos cada 24 horas) en los servidores de referencia para asegurar la consistencia de la hora (UTC) indicada en los distintos registros electrónicos.

15.2.4 Sistema de recogida de archivos

El sistema de recopilación de archivos de eventos de TSP MediaCert es interno y se especifica en el documento DTPG.

15.2.5 Procedimiento de recuperación y verificación de archivos

Los archivos podrán ser recuperados en un plazo inferior a dos (2) días hábiles desde el registro de la solicitud. El acceso a los archivos está sujeto a restricciones (véase el capítulo 15.2.1).

Los archivos estarán disponibles en caso de requisa judicial.

16 Continuidad del negocio

16.1 Compromisos de disponibilidad

El objetivo de disponibilidad del sitio web de TSP MediaCert se especifica en el capítulo 5.2.3 de este documento.

Además, TSP MediaCert tiene compromisos de disponibilidad específicos para cada servicio de confianza que proporciona.

16.1.1 Servicios de certificación

La función de información sobre el estado del certificado está disponible los 7 días de la semana, las 24 horas del día. TSP MediaCert busca el nivel más bajo posible de indisponibilidad.

16.1.2 Servicios de marca de tiempo

La disponibilidad específica para la prestación del servicio se define en la política correspondiente.

16.1.3 Servicios de archivo

La disponibilidad específica tanto para el servicio de captura como para el servicio de consulta de archivos se define en las distintas políticas de archivo.

16.2 Continuidad y recuperación del negocio

En caso de interrupción o corrupción de los recursos informáticos (hardware, software y/o datos), en particular en caso de comprometer la clave privada de un componente, el TSP MediaCert aplicará el Plan de Continuidad y Reanudación de Negocio del servicio en cuestión con el fin de garantizar la continuidad y/o restauración del servicio lo antes posible.
Se establecen medidas correctivas para limitar el riesgo de que ocurra un nuevo incidente.

Los PGI y PCRA son actualizados regularmente por los equipos de seguridad de Worldline y los equipos a cargo de TSP MediaCert respectivamente.

17 Fin de las actividades

TSP MediaCert está implementando un plan de interrupción de negocios para minimizar el impacto de una interrupción de negocios en los suscriptores y usuarios.

En caso de que TSP MediaCert decida interrumpir la prestación de uno de sus servicios de confianza, se aplicará el plan de terminación del servicio en cuestión. Cada uno de los planes para la terminación de los servicios de confianza incluye los siguientes puntos:

- información de la decisión de la TSP MediaCert a los interesados (organismos de control como la ANSSI, los socios, los abonados y los usuarios) antes del cese de las actividades del servicio, previa notificación;
- la derogación de las autorizaciones concedidas a posibles subcontratistas para que actúen en su nombre en el desempeño de cualquier función relacionada con el proceso de prestación de servicios;
- transferir a Worldline sus obligaciones de mantener los registros de eventos y archivos necesarios para demostrar el correcto funcionamiento del servicio durante un período de tiempo razonable;
- destrucción de las claves privadas (nominales y de reserva) afectadas por el servicio de forma que no puedan ser recuperadas;
- mantener o transferir a Worldline sus obligaciones de poner a disposición sus claves públicas y los Certificados afectados por el Servicio al Usuario durante un período de tiempo razonable.

Los planes de terminación de los diversos servicios de confianza de TSP MediaCert se revisan y actualizan periódicamente de acuerdo con el estado actual de la técnica.

En el caso de que TSP MediaCert quiebre, se aferrará a Worldline para cubrir las obligaciones al final de la vida útil de los servicios de confianza que proporciona.

Cada política de un servicio fiduciario de TSP MediaCert puede complementar estos puntos con disposiciones específicas para el tipo de servicio de confianza implementado.

18 Conformidad

18.1 Seguros

18.1.1 Cobertura de seguro

Worldline tiene, con una compañía conocida por ser solvente, una póliza de seguro que garantiza los daños que puedan ocurrir a su propiedad, a su personal, así como una póliza que cubre su responsabilidad profesional en relación con los servicios prestados.

18.1.2 Otros recursos

Worldline tiene los recursos financieros para proporcionar los servicios de TSP MediaCert.

18.1.3 Cobertura y garantía para las entidades usuarias

TSP MediaCert no se hace responsable del uso no autorizado o no conforme de los servicios que proporciona (certificados, contadores).
De hecho, TSP MediaCert sólo puede ser considerada responsable en el caso de que se demuestre el incumplimiento de sus obligaciones.

Además, en la medida de las limitaciones de la ley, TSP MediaCert no será responsable:

- ninguna pérdida financiera;
- sin pérdida de datos;
- cualquier daño indirecto relacionado con el uso de un certificado o una marca de tiempo.
- de cualquier otro daño.

TSP MediaCert generalmente no es responsable de los documentos e información proporcionados por el suscriptor y no garantiza su exactitud ni las consecuencias de hechos dañinos, acciones, negligencia u omisiones por parte del suscriptor.

En cualquier caso, la responsabilidad de TSP MediaCert estará limitada, para todos los eventos y para todos los daños combinados, al importe del acceso al servicio de confianza correspondiente, tal como se especifica en particular en el contrato de servicio asociado, de conformidad con la legislación aplicable y dentro de los límites de la misma.

18.2 Confidencialidad de los datos profesionales

18.2.1 Alcance de la información confidencial

La siguiente información se considera confidencial:

- información técnica relativa a la seguridad de las operaciones de los HSM y de determinados componentes de los servicios de TSP MediaCert;
- claves privadas de las autoridades competentes, sus componentes y los certificados expedidos;
- las claves privadas de las TSUs;

- datos de activación de claves privadas de CA y TSU;
- la documentación técnica relativa a las políticas de los distintos servicios de confianza;
- los procedimientos operativos internos;
- el plan de continuidad y recuperación en caso de desastre para los diversos servicios de confianza;
- el plan de cese de actividad de los distintos servicios de confianza;
- archivos de registro;
- informes de auditoría.

Sólo las personas autorizadas por Worldline y que tengan la necesidad o autorización de conocer su contenido pueden consultar, previa solicitud, la información antes mencionada. Esta solicitud debe ser enviada a la persona a cargo de TSP MediaCert o a uno de sus asistentes.

18.2.2 Información fuera del ámbito de la información confidencial

La información de la TSP MediaCert considerada pública y por lo tanto no confidencial es la que se define en el capítulo 5.2.2 este documento.

18.2.3 Responsabilidad de la protección de la información confidencial

TSP MediaCert se compromete a tratar la información confidencial recopilada de conformidad con las leyes y reglamentos vigentes.

18.3 Protección de datos de carácter personal

18.3.1 Política de protección de datos personales

Worldline garantiza la protección de los datos personales que posee o puede poseer, de conformidad con las normas relativas a la protección de datos personales vigentes en el territorio desde el que presta sus servicios.

Estos datos están protegidos de acuerdo con la legislación nacional francesa aplicable a sus servicios, que en Francia es conforme a la normativa europea tanto de eIDAS como de la RGPD (véase el capítulo 18.7).

Así, de acuerdo con el Reglamento eIDAS, TSP MediaCert adopta las medidas técnicas y organizativas adecuadas para gestionar los riesgos de seguridad asociados a los servicios de confianza que presta. Teniendo en cuenta los últimos avances tecnológicos, estas medidas garantizarán que el nivel de seguridad sea proporcional al grado de riesgo. En particular, se adoptarán medidas para prevenir y limitar las consecuencias de los incidentes de seguridad e informar a las partes interesadas de sus efectos adversos.

En caso de violación de datos personales, TSP MediaCert se remite al Procedimiento de Tratamiento de Datos Personales de Worldline puesto a su disposición.

TSP MediaCert actúa de acuerdo con las obligaciones tipo LRC (Regulatory and Contractual Legal).

18.3.2 Responsabilidad de la protección de datos personales

Worldline procesa los datos personales de acuerdo con las leyes y reglamentos definidos en el capítulo 18.7 este documento, que están en línea con los vigentes en Europa en materia de protección de datos personales.

18.3.3 Derecho de acceso a los datos

De conformidad con el artículo 40 de la Ley de protección de datos modificada por la Ley francesa nº 2016-1321 de 7 de octubre de 2016 - artículo 63, cualquier persona física que demuestre su identidad podrá exigir al responsable del tratamiento que rectifique, complete, actualice, bloquee o borre, según el caso, los datos personales que le conciernan, que sean inexactos, incompletos, ambiguos, obsoletos o cuya recogida, utilización, comunicación o almacenamiento esté prohibido. Cuando el interesado lo solicite, el responsable del tratamiento deberá aportar la prueba, sin coste alguno para el solicitante, de que ha llevado a cabo dichas operaciones.

El derecho de acceso puede ejercerse por escrito: por correo postal al punto de contacto de TSP MediaCert, en la dirección indicada en el capítulo 5.1.2 este documento o en el sitio web de TSP MediaCert (véase el capítulo 5.2.3), acompañado de una copia de un documento de identidad. Idealmente, por correo certificado con acuse de recibo.

18.3.4 Condiciones para la divulgación de información personal a las autoridades judiciales o administrativas

Es posible que Worldline tenga que poner a disposición de terceros autorizados la información personal recopilada en relación con procedimientos legales o auditorías para verificar la validez del funcionamiento de los servicios de TSP MediaCert. Este último dispone de procedimientos seguros para permitir estos accesos, que se rastrean por nombre y se almacenan.

18.4 Derechos de propiedad intelectual e industrial

TSP MediaCert actúa de acuerdo con la legislación y los reglamentos definidos en el Capítulo 18.7 este documento. Los documentos públicos, fuera del alcance de la información confidencial, siguen siendo propiedad de Worldline.

18.5 Disposiciones relativas a la resolución de conflictos

En caso de litigio, es aconsejable ponerse en contacto con el TSP MediaCert en el punto de contacto descrito en el punto 5.1.2.
Las partes se esforzarán por resolver amistosamente y lo antes posible cualquier controversia relativa a la interpretación o ejecución del contrato. En ausencia de conciliación, cualquier disputa relacionada con la validez, interpretación o ejecución de esta Política General, las Políticas de Servicios o los T&Cs se someterá a los tribunales competentes indicados en 18.6

Las disposiciones adicionales de resolución de disputas específicas para cada Servicio de confianza de TSP MediaCert se pueden establecer en las políticas y TyC de dichos servicios. Por lo tanto, se definen en las políticas asociadas y/o en las condiciones generales.

18.6 Jurisdicciones competentes

En caso de litigio relativo a los servicios de confianza prestados por TSP MediaCert, incluida la documentación relacionada y la imposibilidad de llegar a un acuerdo amistoso, cualquier litigio se someterá a los tribunales competentes de París.

18.7 Cumplimiento de las leyes y reglamentos

La TSP MediaCert, en todos sus componentes e incluyendo los documentales, se rige por la legislación y reglamentación francesa que le es aplicable, generalmente basada en textos europeos, aunque sus actividades resultantes de este PG pueden tener efectos legales fuera del territorio francés.

Se lleva a cabo un seguimiento regular para verificar el cumplimiento de estas obligaciones legales.

Además, sólo la versión francesa de los documentos contractuales (incluyendo este PG) es ejecutable contra las partes, incluso en presencia de traducciones. En efecto, las traducciones de los acuerdos expresos se proporcionan por mera conveniencia y no pueden tener ningún efecto jurídico, en particular sobre la interpretación del Contrato de Suscripción o sobre la intención común de las partes.

18.8 Fuerza mayor

Se consideran casos de fuerza mayor todos los que suelen ser retenidos por la jurisprudencia de las cortes y tribunales franceses, incluyendo el caso de un evento imprevisible, insuperable e impredecible. Como tal, TSP MediaCert no puede ser considerada responsable de cualquier daño indirecto o interrupción de sus servicios por causas de fuerza mayor.

18.9 Auditorías

TSP MediaCert somete sus servicios a auditorías de cumplimiento u otros medios de evaluación. Cada departamento proporciona detalles sobre el tema dentro de su política específica.

18.9.1 Frecuencia y/o circunstancias de las evaluaciones

Worldline audita el cumplimiento de sus diversos servicios de confianza (Servicio de Certificación, Servicio de Time-Stamp y Servicio de Archivado) con las políticas actuales durante la implementación operativa de un componente de un servicio de confianza y durante cualquier cambio significativo dentro de un componente por parte de una organización acreditada.

Worldline puede tener que llevar a cabo una auditoría de vigilancia (interna o externa) entre dos auditorías de certificación externa según las normas vigentes en el servicio de confianza de la TSP MediaCert en cuestión.

18.9.2 Identidades / cualificaciones de los evaluadores

18.9.2.1 Auditoría de certificación

La auditoría del componente de servicios de confianza es realizada por un equipo de auditores que forman parte de un organismo de auditoría autorizado y acreditado para realizar evaluaciones de acuerdo con las especificaciones de las normas aplicables al servicio de confianza de la evaluada TSP MediaCert.

18.9.2.2 Auditoría de vigilancia

El control del componente de servicio de fideicomiso es realizado por un equipo de control de cumplimiento que es independiente del servicio de confianza evaluado de TSP MediaCert.

18.9.3 Relaciones entre los evaluadores y las entidades evaluadas

18.9.3.1 Auditoría de certificación

El(los) evaluador(es) que lleve(n) a cabo la auditoría de los componentes del servicio de confianza que se está evaluando será(n) independiente(s) y estará(n) libre(s) de cualquier conflicto de intereses.

18.9.3.2 Auditoría de vigilancia

Los evaluadores que realizan la auditoría de los componentes del servicio de confianza que se está evaluando no tienen ningún rol de confianza dentro de la certificación MediaCert de TSP.

18.9.4 Temas cubiertos por las evaluaciones

Las auditorías realizadas por los auditores cubren algunos o todos los componentes de un servicio de fideicomiso de TSP MediaCert con el fin de monitorear el cumplimiento de la implementación de este PG y la conformidad de los procedimientos y prácticas del servicio de confianza con los requisitos a los que está sujeto.

En este sentido, antes de cada auditoría, el evaluador responsable de la misma envía al TSP MediaCert un plan de auditoría, especificando los componentes y procedimientos que desea auditar durante la auditoría con su(s) colega(s), así como el programa detallado de auditoría.

18.9.5 Medidas adoptadas en respuesta a las conclusiones de la evaluación

Tras una evaluación, el equipo de auditoría proporciona a Worldline su opinión sobre las siguientes opciones:

- Éxito: la auditoría no ha detectado ningún incumplimiento y no se requiere ninguna otra medida. Worldline confirma el cumplimiento del componente auditado con los compromisos de este documento y las prácticas anunciadas;
- Pendiente de confirmación: la auditoría identificó una o más no conformidades no bloqueadoras. Worldline debe entonces presentar un plan de acción correctiva con una fecha límite para su finalización. Podrá efectuarse un nuevo control para comprobar la aplicación de las correcciones;
- fallo: la auditoría detectó una o más no conformidades de bloqueo. El equipo de auditoría hace recomendaciones a Worldline, que pueden incluir el cese temporal o permanente de la actividad, etc. La elección de la medida a aplicar corresponde a Worldline.

18.9.6 Comunicación de resultados

Los resultados de las auditorías de cumplimiento se ponen a disposición del organismo de encargado de certificar el servicio de confianza evaluado de la TSP MediaCert.