MNEMO EVOLUTION & INTEGRATION SERVICES, S.A. “PROCESA Engine v1.7.3”
Declaración de Seguridad para PROCESA Engine v.1.7.3
V1.6

HOJA DE CONTROL DOCUMENTAL

Nombre del documento:	PROCESAEngine_v1.7.3_Declaración_de_seguridad_29062009_v1.6		
Resumen:	Declaración de seguridad para la versión 1.7.x de PROCESA Engine		
Autor:	Juan José Rodríguez Gutiérrez	**Fecha Versión:**	22/03/2010
Revisado por:	Fernando García Vicent	**Fecha Revisión:**	22/03/2010
Aprobado por:	Fernando García Vicent	**Fecha Aprobación:**	22/03/2010
Anexos:	N/A	**Nº de páginas:**	50

CONTROL DE VERSIONES

Versión	Fecha	Autor	Descripción
1.0	29/06/2009	Juan José Rodríguez Gutiérrez	Creación del documento
1.1	17/07/2009	Juan José Rodríguez Gutiérrez	Modificación de los requisitos funcionales, aumentos +ASE_SPD.1, +ASE_OBJ.2, +ASE_REQ.2
1.2	17/08/2009	Juan José Rodríguez Gutiérrez	Modificaciones para corregir errores detectados en auditoria previa
1.3	30/09/2009	Juan José Rodríguez Gutiérrez	Modificaciones para corregir errores de inconsistencia de información relacionada con la identificación y los requisitos de seguridad
1.4	20/10/2009	José Peñalba Morales	Modificaciones para corregir errores de inconsistencia del Componente Auditoria
1.5	15/12/2009	José Peñalba Morales	Modificaciones para corregir las no conformidades con la versión 1.4 del documento
1.6	22/03/2010	José Peñalba Morales	Modificaciones para corregir las no conformidades con la versión 1.5 del documento

ÍNDICE

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

1 Introducción

El presente documento contiene la información relativa a la declaración de seguridad del producto PROCESA Engine aplicable a la versión 1.7.3. En el documento se incluyen los elementos necesarios para determinar el Objeto de Evaluación (en adelante TOE), así como los objetivos de seguridad y los mecanismos para asegurarlos que se han determinado.

1.1 Identificación

En este apartado se resume la información para la identificación de la presente declaración de seguridad (en adelante ST), así como del Objeto de Evaluación (TOE) al que ésta hace referencia.

Identificador	Descripción
Identificador del documento:	PROCESAEngine_v1.7.3_Declaracion_de_seguridad_29062009_v1.6
Versión:	1.6
Título:	Declaración de seguridad para PROCESA Engine v.1.7.3
Autores:	Juan José Rodríguez Gutiérrez José Peñalba Morales
Estado del documento:	Finalizado
Fecha de publicación:	15/03/2010
Identificador del TOE:	PROCESA Engine v1.7.3
Versión Common Criteria:	Common Criteria v 3.1. Revision 3.
EAL:	EAL1+ALC_FLR.1 +ASE_SPD.1 +ASE_OBJ.2 +ASE_REQ.2
Evaluación declaración seguridad:	Epoche & Espri

Tabla 1 - Identificación del TOE

1.2 Glosario

Los siguientes términos y acrónimos son usados a lo largo del documento.

Término/Acrónimo	Descripción
Autorización	El proceso de aprobación de una solicitud
Evento	Cualquier acción o suceso que ocurre dentro del sistema provocado por la intervención de un agente externo.
Modelo	Representación de una secuencia de tareas que pueden ser ejecutas por una serie de personas
Tarea	Agrupación de acciones tanto interactivas como automáticas que se pueden ejecutar en un modelo
Rol de proceso	Papel o funciones que desempeña un usuario o grupo de usuarios encargados de la ejecución de una serie de tareas.
HTTP/HTTPS (HyperText Transfer Protocol)	Protocolos usados en cada transacción de la Web.
LDAP (Lightweight Directory Access Protocol)	Protocolo de red que permite el acceso a un servicio de directorio ordenado y distribuido para buscar información en un entorno de red.
Servicio TOE	Conjunto de servicios del Objeto de Evaluación que se publican al exterior para ofrecer

	funcionalidades.
SOAP (Simple Object Access Protocol)	Protocolo estándar creado por Microsoft, IBM y otros, que define cómo dos objetos en diferentes procesos pueden comunicarse por medio de intercambio de datos XML.
TOE (Target of Evaluation)	Objeto de Evaluación.
Webservice	Colección de protocolos y estándares que sirven para intercambiar datos entre aplicaciones.

Tabla 2- Glosario de términos

1.3 Referencias

La presente Declaración de Seguridad ha sido elaborado siguiendo las especificaciones recogidas dentro del *Common Criteria for Information Technology Security Evaluation,* versión 3.1 Revision 3. Partes 1,2 y 3.

1.4 TOE Overview

PROCESA es un producto BPMS especialmente diseñado para la construcción y ejecución de procesos de Administración Electrónica y de Tramitación Electrónica, sobre la base del concepto de reutilización de servicios. Utiliza lo mejor de las tecnologías BPM y SOA para la construcción de sistemas de información basados en procesos, en los cuales cada tarea es ejecutada por la combinación de la ejecución de los distintos tipos de servicios accesibles desde el servidor que está realizando la ejecución del proceso.

El núcleo de PROCESA, en que consiste precisamente el objeto de evaluación (TOE), es el módulo PROCESA Engine, entre cuyas características destacan las siguientes:

- Es un servicio inteligente de BPM-workflow sobre objetos reutilizables, mediante arquitecturas SOA e invocación de servicios web.

- Permite la construcción de una Plataforma de Servicios para el diseño de sistemas de información basados en flujos de procesos y árboles de tramitación complejos, para los cuales el número de caminos, el volumen de tareas por cada camino y la probabilidad de cambio en las especificaciones funcionales y técnicas asociadas a cada tarea son muy elevados.

- Aplicación práctica de las tecnologías BPM, SOA y utilización de estándares (XML, WebServices, XPDL, BPEL, etc.).

- Diseñado teniendo en cuenta requisitos de construcción de sistemas globales e interoperables (eAdministración).

- Integrable de forma natural en estrategias SOA corporativas en las que se incluyen tecnologías de terceros.

- El producto se identifica por los siguientes puntos:
    - Capacidad real para diseñar sistemas de información complejos en términos manejables de tiempo, coste y capacidad de mantenimiento evolutivo. **La principal característica de PROCESA es su sencillez y rapidez de implantación, así como la inmediata capacidad para la obtención de resultados en términos de desarrollo rápido de aplicaciones, con unos considerables aumentos de productividad**.

- Actualizado a las últimas tecnologías líderes de mercado.
- Adecuación perfecta a requisitos de usuario para los sistemas de información construidos con el producto.
- Orientación completa sobre Reutilización de Servicios, Interoperabilidad y Accesibilidad Web.
- RAD: Rapid Application Development.
- Capacidad para definir modelos de proceso verticales: CMMI, ITIL, eAdministración, etc.
- Compatible con productos BPM de fabricante: BEA AquaLogic BPM, ORACLE BPM, Oracle BPEL, IBM WebSphere, etc.
- Construcción de procesos sobre servicios de PROCESA, corporativos o de terceros.
- Directamente implantable sobre una arquitectura de Bus de Servicios.
- Gestión de Contenidos integrada dentro de los modelos de procesos.

Las principales funciones de seguridad ofrecidas por el TOE para garantizar la seguridad, trazabilidad y auditoría de los procedimientos, tareas y acciones ejecutadas son las siguientes:

- **Autenticación:** Permite la autenticación de los usuarios y aplicaciones remotas. La herramienta utiliza para ello la identificación mediante usuario y contraseña.

- **Trazabilidad:** Almacena información de todos los eventos que ocurren en el sistema permitiendo de ésta forma realizar el seguimiento completo de la ejecución de los procesos.

- **Auditoría:** Asociado a cada evento que se produce en el sistema se almacena información relativa al usuario o aplicación que provocó dicho evento en el sistema.

No forman parte del TOE, aunque si de PROCESA, otros módulos cuyas características principales son:

- Conjunto completo de herramientas de Definición, Diseño y Construcción de los modelos de procesos, y un Motor de Ejecución de Procesos que presenta aplicaciones finales al usuario (Web y Movilidad).

1.4.1 Tipo y uso de TOE

PROCESA Engine es una aplicación basada en una arquitectura orientada a servicios que permite la gestión del ciclo de vida de procesos, tareas y acciones encargadas de ser ejecutadas por ciertas personas o grupo de personas ofreciendo sus funcionalidades en base a servicios web.

PROCESA Engine (TOE) es el encargado de gestionar la ejecución de todos los procesos de negocio definidos, las instancias, la gestión del flujo de ejecución y toda la gestión del ciclo de vida de las tareas de PROCESA. Su Arquitectura Orientada a Servicios (SOA) permite su interconexión y reutilización de servicios ya existentes en una organización, así como su futuro uso en caso de existir en la actualidad. Así mismo, permite que otros sistemas o componentes externos puedan hacer uso de los servicios que ofrece el propio producto de forma estándar para su interacción.

1.4.2 Hardware y software no incluido en el TOE

Los requisitos software y hardware, así como las opciones referidas son los que se indican a continuación. Estos elementos no se incluyen en el TOE, por tanto es necesario disponer de los mismos:

- **Servidor de aplicaciones**. El servidor de aplicaciones ha de soportar una máquina virtual Java J2SE 1.5.0. ó superior. Servidor Aplicaciones compatible J2EE 1.4 o superior (JBoss 5.0.X o superior, Weblogic 9 o superior, Websphere 6.1 o superior, OAS 10g o superior) con mínimo 2 procesadores y 2GB RAM.

- **Servidor de portal**. El servidor de portales ha de soportar una máquina virtual Java J2SE 1.5.0. ó superior. Servidor Portal compatible con el estándar JSR-168 (JBoss Portal 2.7.X +, Weblogic Portal 9.2+, Websphere Portal 6.1+, Oracle Portal 10g+) con mínimo 2 procesadores y 2GB RAM.

- **Servidor base de datos**. El servidor de base de datos ha de tener disponible un driver de tipo JDBC. Entre otros puede ser Oracle 9i,10g,11g . SQLServer 2000, 2005. MySQL 5.x. DB2 8 o superior.

- **Sistema operativo**. El sistema operativo de los equipos puede ser cualquiera sobre el que se puedan instalar de forma certificada los servidores de aplicaciones anteriormente descritos.

- **Java Runtime Enviroment**. Respecto a la versión del runtime Java (J2SE) sobre el que se ejecutará el servidor de aplicaciones es necesario como mínimo que sea J2RE 1.5.0 o superior.

- **Servidor LDAP**. Como servidor LDAP se puede utilizar cualquiera que soporta la especificación LDAP v3. Como por ejemplo, OpenLDAP, Active Directory 2003...

- **Gestor de contenido**. PROCESA utiliza un gestor de contenido para almacenar los documentos asociados a los procesos que se ejecutan dentro del motor de ejecución de procesos (PROCESA Engine). El gestor de contenidos tiene que soportar el estándar JSR170.

- **Navegadores**. Cualquiera de los siguientes es válido:
  - Microsoft Internet Explorer v6.0 Service Pack 2 o superior.
  - Netscape Comunicator v6 o superior.
  - Mozilla v4.1 o superior.
  - Firefox 3.0.x o superior.

El detalle de la configuración tanto lógica como física requerida y seleccionada para la evaluación se encuentra en el apartado 1.6 Configuración evaluada.

1.5 TOE Description

Como se indicó anteriormente, es necesario distinguir entre PROCESA como producto y el objeto de evaluación (TOE):

- PROCESA: un producto basado en SOA que contiene una gestor BPM, los servicios necesarios para su administración y ejecución y herramientas para la creación e interacción con los procesos e instancias.
- TOE: el objeto de evaluación que consiste en el módulo PROCESA Engine, el núcleo principal de PROCESA, y que engloba el motor de BPM y la aplicación SOA junto con todos los servicios de administración y ejecución.

El TOE objeto de la presente Declaración de Seguridad posee como interfaz de cara al exterior una serie de servicios Web agrupados en entidades y publicados para ofrecer sus funcionalidades. En adelante, este conjunto será referido con la denominación **Servicio del TOE. Se incluye, además,** un componente adicional denominado **PROCESA Engine Administrator**, que no forma parte del TOE y que proporciona un interfaz web para el despliegue, configuración, monitorización y gestión del TOE.

Teniendo en cuenta lo anterior, a continuación se presenta una breve descripción de la totalidad de los módulos que componen el producto PROCESA. Dichos módulos a su vez se dividen en componentes, los cuales y para el caso del TOE, ofrecen los servicios y utilidades del TOE.

PROCESA consta de los siguientes módulos principales:

- Herramienta de Modelización de Procesos: **PROCESA Model**
- Herramienta de Diseño y Construcción de Procesos: **PROCESA Builder**
- Servicio Universal de Acceso a Datos de Aplicación: **PROCESA SRDA**
- Diseño de Interfaz de Usuario: **PROCESA Web Designer**
- Presentación de Páginas y Diálogos de Usuario: **PROCESA Painter**
- Motor de Ejecución: **PROCESA Engine (TOE)**
- Administración y Monitorización: **PROCESA Engine Administrator**
- Generador de Informes: **PROCESA Reports**
- API de Integración con PROCESA: **PROCESA Integrator**

Mediante *PROCESA Model*, los analistas de negocio pueden crear los modelos de procesos correspondientes a las funcionalidades requeridas por el sistema de información que se está diseñando, con toda la sencillez que se precisa para esta tarea por parte de usuarios no técnicos, al mismo tiempo que el trabajo realizado sirve para definir el proceso de forma real, almacenándose en un formato estructurado que pueden utilizar posteriormente los técnicos que deben construir las tareas de cada proceso.

Mediante *PROCESA Builder*, los diseñadores de aplicaciones workflow tienen la posibilidad de diseñar y construir las tareas de los modelos de procesos definidos por los analistas de negocio. Los diseñadores pueden construir dichas tareas sin necesidad de programar una sola línea de código, ya que dicha construcción se realiza mediante la invocación de servicios que componen todas las acciones que son necesarias para construir cualquier tarea de un proceso administrativo.

El módulo *PROCESA SRDA* consiste en un servicio de repositorio de datos de aplicación que proporciona acceso para lectura y actualización transaccional de datos y meta-datos de las aplicaciones construidas con PROCESA. De esta forma, se aísla la complejidad de las distintas fuentes de datos de la construcción de los procesos.

El módulo *PROCESA Web Designer* permite el diseño del interfaz gráfico de usuario del sistema mediante la utilización de servicios de diseño sobre estándares de portales web. *Web Designer* permite construir todos los diálogos de usuario que son directamente instalables en el portal que gobierna el proceso.

***PROCESA Painter* es el componente de ejecución que presenta todas las páginas de usuario en el portal de Administración Electrónica, así como los diálogos con el usuario necesarios para la ejecución de las tareas del proceso**. Una vez construidos todos los objetos y reglas que definen el sistema BPM final (Modelo de Aplicación).

***PROCESA Engine* se encarga de interpretar el modelo y presentar las aplicaciones a los usuarios en tiempo real**. Para administrar el sistema y monitorizar los procesos y las tareas que definen el sistema BPM final (Modelo de Aplicación). **Este módulo es el Objeto de Evaluación (TOE) de la presente Declaración de Seguridad.**

***PROCESA Engine Administrator* se encarga de administrar y monitorizar el sistema en tiempo real**.

El módulo *PROCESA Reports* consiste en un generador de informes para perfiles de desarrollo, que permite el diseño y construcción de los informes de las aplicaciones construidas con PROCESA.

El módulo *PROCESA Integrator* proporciona el API (Application Program Interface) completo basado en Java y en Servicios Web, para la integración de cualquier sistema externo con las aplicaciones PROCESA.

Una vez descritos los módulos del producto PROCESA nos centraremos en describir en mayor detalle las características y componentes que incluye el módulo PROCESA Engine (TOE). Como características principales referentes a la seguridad el TOE es capaz de realizar el registro de las operaciones realizadas a los servicios que componen el Servicio del TOE. La generación de las auditorías las realiza un subsistema específico, Componente Auditoría, que registra el comienzo y el fin de la ejecución de un servicio invocado por una aplicación externa.

El TOE dispone igualmente de la capacidad de controlar el acceso de las peticiones a los webservices del TOE por parte de las aplicaciones externas. Para ello, el TOE dispone de manejadores automáticos que verifican las peticiones recibidas y autentican las mismas dentro del sistema.

Por lo que respecta a la aplicación de administración y configuración del TOE, módulo PROCESA Engine Administrator, permite configurar todo lo necesario para el uso del Servicio del TOE, permitiendo extraer información acerca de los procesos que se encuentran en ejecución, los roles de los usuarios, etc. La autenticación para el uso de la aplicación de administración PROCESA Engine Administrator se realiza por usuario/contraseña, utilizando los servicios de control de acceso disponibles en el TOE.

Como se ha indicado anteriormente, las funcionalidades ofrecidas por el TOE se encuentran disponibles a través de un conjunto de componentes que pueden interaccionar entre sí. Estos componentes pueden trabajar de forma independiente y de forma distribuida. Dichos componentes pueden ser distribuidos en diferentes servidores, comunicándose entre sí a través de protocolos seguros SSL con o sin autenticación de cliente.

El TOE ofrece sus servicios a través de interfaces de tipo Webservice (SOAP/XML), es decir, el TOE publica sus funcionalidades de forma que puedan ser invocadas desde cualquier servidor utilizando diferentes tecnologías, lenguajes de programación, o sistemas operativos. La invocación de dichos interfaces es posible realizarse ya sea directamente mediante el fichero de definición del servicio web (Web Service Definition Language – WSDL) o mediante la utilización de un componente cliente que encapsula las invocaciones a los servicios mediante la utilización de un interfaz Java.

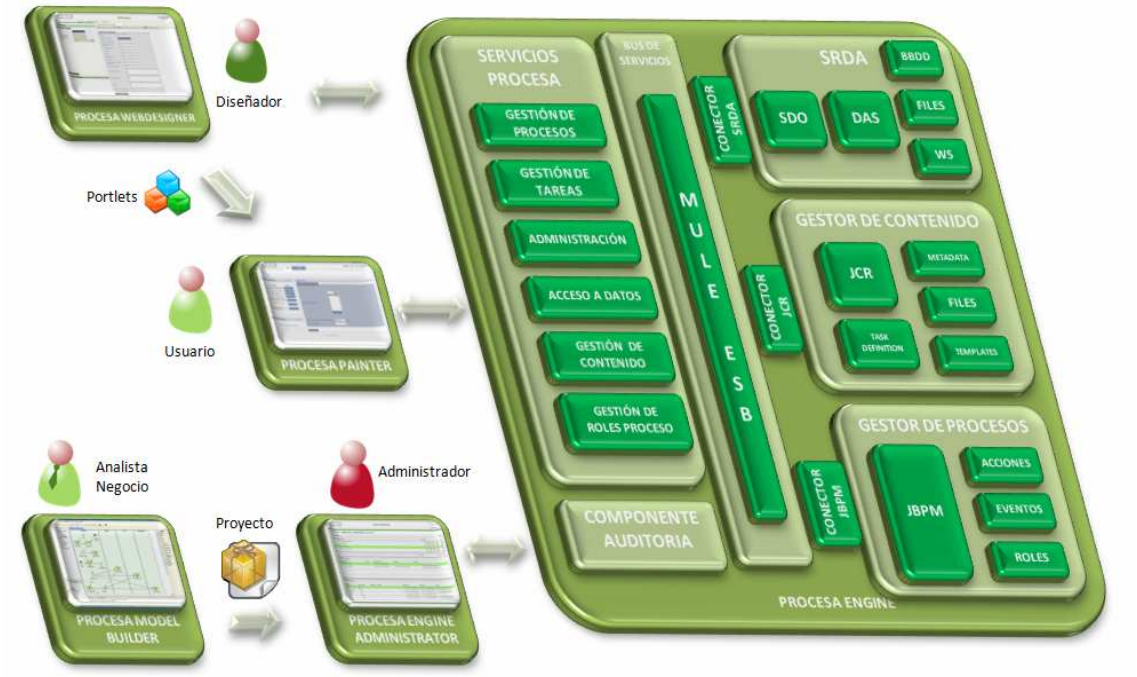
El acceso a dichos servicios puede realizarse utilizando comunicación HTTP o HTTPS, recomendándose únicamente HTTPS para la configuración más segura con el objeto de garantizar la confidencialidad de la información intercambiada. Todos los servicios interactúan con el componente de control de acceso el cual se encarga de la identificación y autenticación de la aplicación llamante, y únicamente en caso de estar correctamente identificada permitir el acceso al servicio.

PROCESA Engine es el encargado de gestionar la ejecución de todos los procesos de negocio definidos, las instancias, la gestión del flujo de ejecución y toda la gestión del ciclo de vida de las tareas de PROCESA. Su Arquitectura Orientada a Servicios (SOA) permite su interconexión y reutilización de servicios ya existentes en una organización, así como su futuro uso en caso de existir en la actualidad. Así mismo, permite que otros sistemas o componentes externos puedan hacer uso de los servicios que ofrece el propio producto de forma estándar para su interacción.

Para conseguir esta Arquitectura Orientada a Servicios, el propio PROCESA Engine incorpora como su espina dorsal un componente clave que es el Intermediador de Servicios (ESB), utilizando para ello la implementación Open Source llamada MULE ESB, sobre el cual se desarrollan e interconectan los restantes componentes y servicios que completan la arquitectura.

En la siguiente figura se aprecia la relación entre los distintos componentes y tecnologías que componen el módulo PROCESA Engine que constituye el núcleo de PROCESA:

Ilustración 1- Arquitectura de PROCESA



1.6 Configuración evaluada

En esta sección se especifican las características y requerimientos de la configuración evaluada del TOE. En particular, se detallan:

1) Detalle de componentes del módulo PROCESA Engine dentro de la configuración evaluada, indicados en el punto 1.6.1 Componentes del TOE.

2) Diagrama de la arquitectura lógica de componentes del TOE, descrito en el apartado 1.6.2 Arquitectura lógica del TOE.

3) Diagrama de arquitectura física de componentes del TOE, descrito en el apartado 1.6.3 Arquitectura física del TOE.

4) Relación de componentes de terceros que deben ser utilizados junto con el TOE en su configuración evaluada, descritos en el apartado 1.6.4 Requisitos de la configuración evaluada.

1.6.1 Componentes del TOE

El conjunto de componentes que integran el TOE se detallan de forma gráfica en la siguiente figura:

Ilustración 2- Componentes del TOE

Todos los componentes que componen el módulo PROCESA Engine serán objeto de evaluación, siendo los componentes denominados **Componente Auditoria** y **Servicios PROCESA (**Servicios del TOE) el interfaz exterior dado que se tratan de los componentes que participan en el acceso a las funcionalidades expuestas por el motor de ejecución de procesos.

Los Servicios del TOE están agrupados de la siguiente manera:

- Servicios de gestión del ciclo de vida de los procesos.
- Servicios de gestión del ciclo de vida de las tareas.
- Servicios de administración
- Servicios de gestión del acceso a datos.
- Servicios de gestión de contenido.
- Servicios de gestión de roles de proceso.

1.6.2 Arquitectura lógica

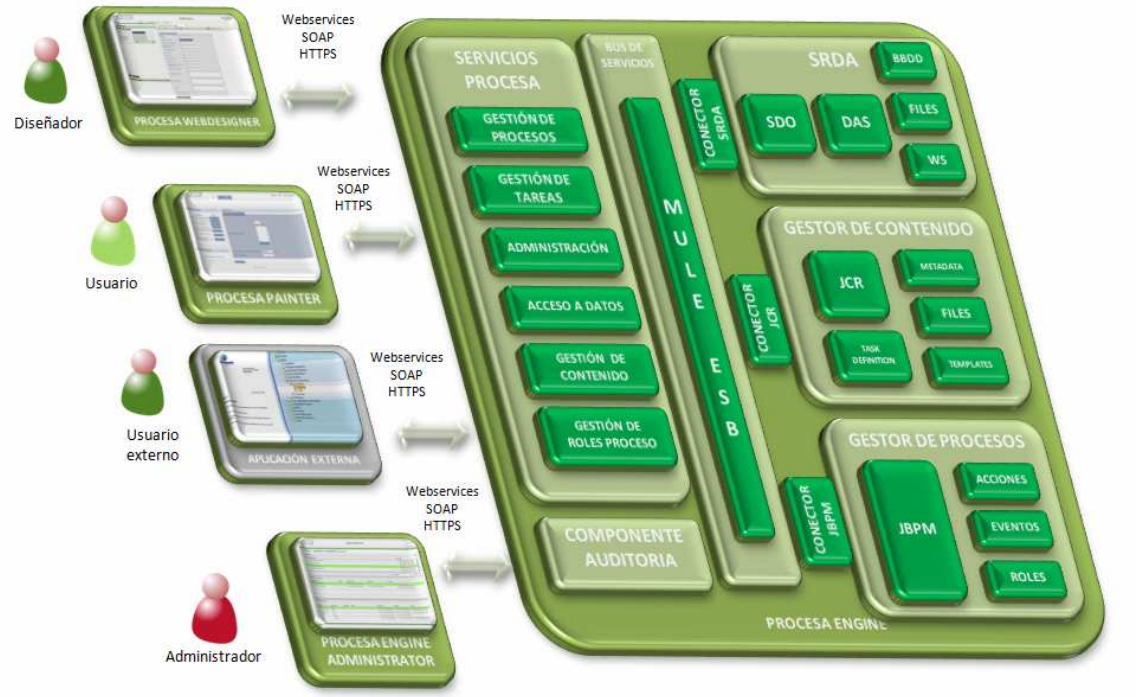
La arquitectura lógica de la configuración evaluada se representa en la **Ilustración 3 – Arquitectura lógica de la configuración evaluada**. En dicha arquitectura se diferencian dos casos, dependiendo de quién invoca los servicios del TOE. Estos son los siguientes:

- **Administrador del sistema:** Para configurar el TOE, el administrador del sistema utiliza el módulo PROCESA Engine Administrator. En la configuración evaluada, la comunicación entre este tipo de usuario y la consola de administración se realiza mediante el protocolo HTTPS. El administrador indica los datos que quiere configurar y la consola de administración invoca a los servicios de administración que son los encargados de almacenar la información suministrada en base de datos. El módulo PROCESA Engine Administrator utiliza siempre los servicios de administración del TOE por lo que se le puede considerar como una aplicación externa más con los mismos requisitos de identificación y seguridad que el resto de las aplicaciones externas.

- **Aplicaciones externas:** Las aplicaciones externas, así como el resto de los módulos que componen PROCESA, pueden interactuar con el Servicio del TOE, pero no con la consola de administración. En la configuración evaluada, los servicios del TOE están desplegados como servicios Web y las invocaciones se realizan vía HTTPS encapsulando mensajes SOAP en formato XML y haciendo uso de las cabeceras de seguridad de servicios Web (UsernameToken y timestamp). Existe la posibilidad igualmente de utilizar el componente cliente de invocación a los Servicios del TOE el cual facilita las labores de integración permitiendo utilizar a las aplicaciones externas un interfaz basado en Java para realizar las invocaciones a los servicios del TOE.

De forma gráfica:

Ilustración 3 – Arquitectura lógica de la configuración evaluada



La comunicación con el TOE, ya que publica sus funcionalidades vía webservices, puede realizarse de dos formas. Una, invocando directamente los servicios por parte de la aplicación usuaria mediante el interfaz de definición de los servicios. Dos, usando el módulo cliente **PROCESA EngineClient** que permite a las aplicaciones usuarias su uso directo como interfaz

Java y que se encarga de la construcción de los mensajes para la invocación a los servicios web. Su utilización es una facilidad que incorpora PROCESA pero no es de obligado uso. La configuración evaluada admite el uso del módulo cliente para agilizar las labores de integración.

1.6.3 Arquitectura física del TOE

Ya se ha mostrado la arquitectura lógica del TOE en el apartado anterior. A nivel físico, el TOE consiste en:

- Por un lado, un único archivo que contiene todos los módulos de PROCESA Engine empaquetados y que es posible desplegar en un servidor de aplicaciones (JBOSS, Weblogic, IBM WebSphere, …)
- Por otro, una serie de archivos de configuración en los que se establecen los parámetros de funcionamiento del PROCESA Engine.

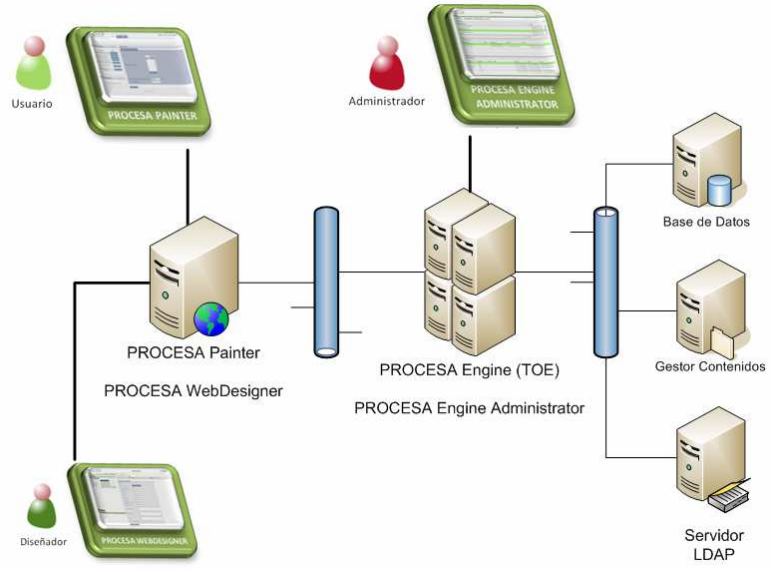
1.6.4 Arquitectura física de la configuración evaluada

La arquitectura física de la configuración evaluada se representa en la **Ilustración 4 – Arquitectura física de la configuración evaluada**. En dicha arquitectura el módulo PROCESA Engine (TOE) y el módulo PROCESA Engine Administrator estarán ubicados en un servidor, la invocación entre ellos se realizará usando el módulo PROCESA EngineClient, el cual encapsula las llamadas a los servicios web del TOE.

Por lo que respecta a las aplicaciones usuarias éstas se alojarán en un equipo diferente al anteriormente citado. Este segundo equipo albergará a los módulos PROCESA WebDesigner y PROCESA Painter los cuales utilizarán también el módulo PROCESA EngineClient para realizar las invocaciones a los servicios del TOE. Lo anterior queda igualmente reflejado en la **Ilustración 4 – Arquitectura física de la configuración evaluada.** De esta forma, la configuración evaluada incluirá únicamente las invocaciones remotas a los servicios del TOE.

El administrador se comunica con el TOE a través de protocolo HTTPS. La interacción entre las aplicaciones usuarias (PROCESA WebDesigner y PROCESA Painter) y el TOE se efectúa mediante la invocación a los servicios web usando protocolo HTTPS y utilizando las cabeceras de seguridad web para la identificación y autenticación de las mismas.

Ilustración 4 - Arquitectura física de la configuración evaluada



La consola de administración (PROCESA Engine Administrator) es el módulo a través del cual se realiza la inserción y/o edición de la información alojada en la base de datos del motor de ejecución PROCESA Engine. El módulo PROCESA Engine Administrator es utilizado únicamente por el administrador del sistema, y se comunica únicamente con el módulo PROCESA Engine (TOE). La autenticación ante la consola de administración se realiza mediante usuario/contraseña pero la validación de la autenticación del usuario se realiza mediante la invocación a los servicios del TOE encargados de la autenticación. Por tanto la consola de administración delega la autenticación del usuario al componente de control de acceso del módulo PROCESA Engine.

De la arquitectura anterior debe tenerse en cuenta que tanto la Base de Datos, como el Gestor de Contenidos y el Servidor LDAP no son componentes que pertenezcan al TOE, sino un software de terceros.

El resto de componentes de terceros requeridos para el funcionamiento de la configuración base (Servidor de Aplicaciones, Servidor de Directorio, Servidor de Portal, Servidor Base de Datos, Gestor de Contenidos, JDK) se instalarán siguiendo las indicaciones recogidas en el apartado 1.6.4 Requisitos de la configuración evaluada.

1.6.5 Requisitos de la configuración evaluada

A continuación se detallan los requisitos necesarios para la instalación en un entorno seguro de la configuración evaluada del TOE presentada en el apartado 1.6 Configuración evaluada.

Los requisitos software y hardware, así como las opciones referidas son los que se indican a continuación. Así, para el funcionamiento de PROCESA es necesario disponer de los siguientes componentes software:

- **Servidor de aplicaciones**. El servidor de aplicaciones ha de soportar una máquina virtual Java J2SE 1.5.0. ó superior. Servidor Aplicaciones compatible J2EE 1.4 o superior (JBoss 5.0.X o superior, Weblogic 9 o superior, Websphere 6.1 o superior, OAS 10g o superior) con mínimo 2 procesadores y 2GB RAM.

- **Servidor de portal**. El servidor de portales ha de soportar una máquina virtual Java J2SE 1.5.0. ó superior. Servidor Portal compatible con el estándar JSR-168 (JBoss Portal

2.7.X +, Weblogic Portal 9.2+, Websphere Portal 6.1+, Oracle Portal 10g+) con mínimo 2 procesadores y 2GB RAM.

- **Servidor base de datos**. El servidor de base de datos ha de tener disponible un driver de tipo JDBC. Entre otros puede ser Oracle 9i, 10g, 11g . SQLServer 2000, 2005. MySQL 5.x. DB2 8 o superior.

- **Sistema operativo**. El sistema operativo de los equipos puede ser cualquiera sobre el que se puedan instalar de forma certificada los servidores de aplicaciones anteriormente descritos.

- **Java Runtime Enviroment**. Respecto a la versión del runtime Java (J2SE) sobre el que se ejecutará el servidor de aplicaciones es necesario como mínimo que sea J2RE 1.5.0 o superior.

- **Servidor LDAP**. Como servidor LDAP se puede utilizar cualquiera que soporta la especificación LDAP v3. Como por ejemplo, OpenLDAP, Active Directory 2003...

- **Gestor de contenido**. PROCESA utiliza un gestor de contenido para almacenar los documentos asociados a los procesos que se ejecutan dentro del motor de ejecución de procesos (PROCESA Engine). El gestor de contenidos tiene que soportar el estándar JSR170.

- **Navegadores**. Cualquiera de los siguientes es válido:
  - Microsoft Internet Explorer v6.0 Service Pack 2 o superior.
  - Netscape Comunicator v6 o superior.
  - Mozilla v4.1 o superior.
  - Firefox 3.0.x o superior.

Dentro de todas las posibilidades que ofrecen estos requisitos software, la configuración que se ha elegido para su evaluación es la siguiente:

- **Servidor de aplicaciones**. JBoss Enterprise Application Platform 5.0.0.

- **Servidor de portal**. JBoss Portal Server 2.7.2

- **Servidor base de datos.** Oracle 10.2.0.5

- **Sistema operativo**: Red Hat Enterprise Linux 5

- **Java Runtime Enviroment**: JRE 1.6u18

- **Navegadores**: Mozilla Firefox 3.0.11.

- **Servidor LDAP**: OpenLDAP

- **Gestor de contenidos**: Jackrabbit 1.4.5

El despliegue de los servicios web del TOE para permitir el acceso a las aplicaciones externas (usuarias) se realizará utilizando la siguiente configuración:

- Conexión mediante protocolo SSL (https)
- SOAP
- Cabeceras de seguridad web (Web Service Secutiry) para la identificación y autenticación de la aplicación externa (UsernameToken + Timestamp)

2 Conformidad

Se declara la conformidad del TOE con las Partes 2 y 3 de *Common Criteria for Information Technology Security Evaluation*, v3.1 Revisión 3 de Junio de 2009.

En concreto, con:

- Requerimientos Funcionales de seguridad de la Parte 2 de CC Version 3.1. Revision 3.

- Requerimientos de Garantía de Seguridad de la Parte 3 de CC Version 3.1 Revision 3 para el Nivel de Certificación EAL1+ (ALC-FLR.1, +ASE_SPD.1, +ASE_OBJ.2, +ASE_REQ.2.).

3 Definición del problema de seguridad

Las principales características que se deben asegurar son:

- **Autenticación**: garantiza la identidad de los usuarios remotos.
- **Control de acceso:** garantiza que solo los usuarios autorizados puedan acceder a los servicios.
- **Capacidad de recuperación**: asegura que la información, así como los procedimientos asociados a su generación y uso, puedan ser recuperados en el momento en el que se necesiten, quedando accesibles a los usuarios autorizados.

3.1 Activos a proteger

Con el objeto de asegurar las características anteriormente descritas se han detectado una serie de activos que es necesario proteger, garantizando el cumplimiento de dichas características para cada uno de ellos. Se presenta a continuación la enumeración y descripción de estos activos.

3.1.1 Activo 01: Confidencialidad de las contraseñas almacenadas en base de datos o ficheros de configuración

Existen varias contraseñas que han de ser almacenadas en base de datos o en ficheros de configuración de manera confidencial (es decir, cifradas), y protegidas de lecturas no permitidas. Éstas son las siguientes:

- Contraseña de acceso a la base de datos interna de PROCESA Engine.
- Contraseñas de acceso para las aplicaciones externas clientes de PROCESA Engine. (Estas aplicaciones clientes envían los datos de su identidad en las cabeceras de seguridad de la invocación de los servicios web del TOE)
- Contraseñas de acceso al repositorio de datos interno y de contenidos.
- Contraseñas de acceso a LDAPs: con ellas se accede al correspondiente repositorio LDAP, en el caso de que el acceso no sea anónimo.
- Contraseñas de acceso servidor de correo: utilizada para establecer la conexión con el servidor de correo corporativo.

3.1.2 Activo 02: Integridad de la gestión de roles de proceso

Para poder ejecutar un proceso previamente modelado es necesario que se realice una asignación segura y confiable de los roles de proceso definidos en los modelos con los usuarios, grupos de usuarios o perfiles concretos de una organización. Esta asociación permite que las tareas queden únicamente accesibles a determinados usuarios o grupos de usuarios por lo tanto tiene que ser gestionada de forma segura.

Es necesario aclarar que no es lo mismo una aplicación externa que un usuario. Las aplicaciones externas son las que hacen uso de los servicios del TOE, los usuarios son los actores que van a participar en los servicios específicos de BPM.

La gestión de los roles de proceso se realiza integrada con el directorio LDAP corporativo, dicha asociación se realiza utilizando la información de usuarios, grupos y perfiles disponibles en un

directorio LDAP corporativo. Solamente las aplicaciones externas autorizadas (por ejemplo, la herramienta Engine Administrator debe serlo) puede hace la gestión de dicha asociación de roles de proceso a usuarios o grupos concretos. Los servicios web del TOE encargados de esta gestión se consideran administrativos y para que una aplicación externa esté autorizada debe poseer el rol “engineAdministrator”. Estos servicios tienen que estar protegidos frente accesos no autorizados debido a que son los encargados establecer la asociación entre los roles de proceso y los usuarios o grupos de usuarios que tienen que ejecutar las tareas.

Como ya se adelantó anteriormente, las aplicaciones externas envían sus datos de identificación en las cabeceras de seguridad de las invocaciones que realizan a los servicios del TOE.

3.1.3 Activo 03: Gestión del ciclo de vida de los procesos

Para poder ejecutar un proceso es necesario previamente su despliegue en motor de ejecución de procesos, de igual forma, es posible el repliegue o versionado de un proceso previamente desplegado dentro del motor de ejecución de procesos. Estos servicios tienen que estar protegidos frente accesos no autorizados debido a que son los encargados de la gestión de los procesos en lo referente a su instanciación y ejecución.

3.1.4 Activo 04: Gestión del ciclo de vida de las tareas

Un proceso desplegado tiene asociada una serie de tareas que es posible ejecutar atendiendo a los diferentes roles de proceso definidos. El motor de ejecución de procesos dispone de una serie de servicios que permiten la ejecución, parada, suspensión o continuación de tareas, por ello sólo las aplicaciones autorizadas pueden acceder a dichos servicios. Estos servicios tienen que estar protegidos frente accesos no autorizados debido a que son los encargados de la gestión de las tareas de los procesos por lo que un uso no autorizado de los mismos podría provocar la ejecución de tareas sin autorización.

3.1.5 Activo 05: Servicios de acceso a datos

El motor de ejecución de procesos permite utilizar una serie de servicios para gestionar el ciclo de vida de los datos asociados a un proceso. Estos servicios tienen que estar protegidos frente accesos no autorizados debido a que son los encargados de la gestión de los datos de los procesos.

3.1.6 Activo 06: Servicios de administración

El motor de ejecución de procesos dispone de una serie de servicios que permiten gestionar los atributos de configuración del mismo. Estos servicios tienen que estar protegidos frente accesos no autorizados debido a que son los encargados de la gestión y configuración de los parámetros del motor de ejecución de procesos.

Para que una aplicación externa esté autorizada a invocar los servicios web de administración del TOE debe poseer el rol “engineAdministrator”

3.1.7 Activo 07: Servicios de gestión documental

El motor de ejecución de procesos dispone de una serie de servicios que permiten gestionar el ciclo de vida de los documentos asociados a procesos que se encuentran en ejecución dentro del motor de procesos. Estos servicios tienen que estar protegidos frente accesos no autorizados debido a que son los encargados de la gestión de los documentos asociados a los procesos.

3.2 Amenazas

Cada uno de los activos a proteger de PROCESA Engine se encuentran expuestos a unas series de amenazas contra una o a varias de las cinco características de seguridad referidas anteriormente.

Cada amenaza tiene asociado un agente responsable de la misma, clasificándose dicho agente en el siguiente tipo:

- **Agente externo**: en este tipo se incluyen todos aquellos agentes o aplicaciones, tanto externos como internos al sistema, que estando o no autorizados a acceder a PROCESA, intentan realizar invocaciones a los servicios web de PROCESA (interfaces del TOE) con el fin de violar algunas de sus características de seguridad.

A continuación se presenta un listado de las amenazas identificadas que pueden afectar a los activos a proteger del sistema.

3.2.1 Amenaza 01: Violación de la confidencialidad de las contraseñas almacenadas en base de datos o ficheros de configuración

Un agente externo podría acceder a las contraseñas almacenadas en base de datos o ficheros de configuración y podría recuperar información de acceso a las fuentes de datos de la aplicación.

3.2.2 Amenaza 02: Violación de la integridad en la gestión de roles de proceso

Un agente externo podría modificar sin autorización la asociación de usuarios, grupos o perfiles con roles de proceso si no se controlase el acceso a los servicios de gestión de roles, de modo que, sólo los usuarios autorizados pueden acceder a dichos servicios.

3.2.3 Amenaza 03: Violación de la integridad en la gestión del ciclo de vida de los procesos

Un agente externo podría realizar sin autorización la ejecución, parada, suspensión o continuación de procesos desplegados, así como el despliegue o repliegue de procesos dentro del motor de ejecución de procesos, sólo los usuarios autorizados pueden acceder a dichos servicios.

3.2.4 Amenaza 04: Violación de la integridad en la gestión del ciclo de vida de las tareas

Un agente externo podría realizar sin autorización la ejecución, parada, suspensión o continuación de tareas asociadas a los procesos desplegados dentro del motor de ejecución de procesos, sólo los usuarios autorizados pueden acceder a dichos servicios.

3.2.5 Amenaza 05: Violación de la integridad de los servicios de acceso a datos

Un agente externo podría realizar sin autorización la ejecución de los servicios que acceden a los datos manejados por los procesos de forma que pudiera crear, alterar, borrar o consultar información de los procesos sin autorización.

3.2.6 Amenaza 06: Violación de la integridad de los servicios de administración

Un agente externo podría realizar sin autorización la ejecución de los servicios de administración de forma que pudiera crear, alterar, borrar o consultar información de los parámetros de configuración del motor de ejecución de procesos sin autorización.

3.2.7 Amenaza 07: Violación de la integridad de los servicios de gestión documental

Un agente externo podría realizar sin autorización la ejecución de los servicios de gestión documental de forma que pudiera crear, alterar, borrar o consultar documentos asociados a los procesos que se encuentran en ejecución.

3.3 Políticas de seguridad organizacional

En esta sección se abordan las políticas de seguridad organizacional que deben aplicarse para asegurar el correcto funcionamiento del TOE.

3.3.1 Política 01: Restricción de acceso al TOE

El propietario del TOE será el responsable de asignar las debidas restricciones de acceso al mismo para cada una de las aplicaciones registradas en el sistema, incluido el acceso físico.

3.3.2 Política 02: Disposición de datos de usuario y privilegios de acceso

El propietario del TOE garantizará la confidencialidad y protección de los datos de autenticación de los usuarios del mismo que, en este caso, son aplicaciones cliente de los servicios del TOE. Ninguna aplicación podrá acceder al sistema sin acreditarse previamente. Asimismo, en el momento en el que una aplicación sea dada de alta se le asignará un rol, en función del cual tendrá unos permisos asociados para realizar determinadas acciones. El propietario del TOE habrá de cerciorarse de que estas acciones corresponden realmente con aquellas operaciones para las que el usuario esté realmente autorizado.

El propietario del TOE se asegurará igualmente de que existan procedimientos apropiados para asegurar la destrucción de los datos de autenticación, así como la eliminación de los privilegios asociados, una vez que el acceso haya sido eliminado o bien en el caso de que las reglas de control de acceso hayan sido redefinidas. Esto se aplica tanto a los administradores como a los aplicaciones clientes del TOE.

3.3.3 Política 03: Configuración segura de conexiones externas del TOE

Todas las conexiones externas que necesite el TOE han de ser configuradas siempre de tal manera que se garantice la seguridad de las mismas. Por ejemplo, en el caso del LDAP, la conexión se realizará basada en SSL.

3.3.4 Política 04: Revisión de auditorías

Existirá un auditor interno del TOE, diferente del administrador del sistema, que será el encargado de revisar periódicamente el archivo de auditoría. Además, el auditor interno del TOE asegurará que los datos auditados se archivan regularmente, para de esta forma prevenir posibles problemas de sobrecarga en los almacenes de registros de auditoría.

3.4 Hipótesis de uso seguro

Para garantizar el uso seguro de PROCESA, se parte de las siguientes hipótesis para su entorno de operación. En caso de que alguna de ellas no pudiera asumirse, no sería posible garantizar el funcionamiento seguro del sistema.

3.4.1 Hipótesis 01: Administrador del sistema confiable

Se supone que el equipo en el que se encuentran instalados tanto los archivos de propiedades utilizados para la configuración del sistema como los archivos de servidor en los que puede aparecer información sensible (por ejemplo, la relativa a las conexiones a bases de datos) tendrá su acceso restringido, de forma que el administrador del sistema será la única entidad que dispondrá de los permisos necesarios para acceder a los mencionados archivos. Además, se supone que dicho administrador no actuará de manera malintencionada ni proporcionará permisos de acceso indebidos.

De la misma manera, se supone que los administradores de la base de datos y LDAP serán confiables, que no otorgará permisos de acceso indebidos (ni de lectura ni de escritura), así como que mantendrá en secreto los datos de las conexiones establecidas.

3.4.2 Hipótesis 02: Administrador de la auditoría

Se supone que existirá un administrador de archivos de auditoría que revisará periódicamente dichos archivos en busca de posibles intentos de ataque al TOE. En el caso de encontrar algún intento de ataque, el administrador de archivos de auditoría realizará las acciones que defina el usuario del producto.

3.5 Hipótesis de entorno

Para garantizar el uso seguro de PROCESA, se parte de las siguientes hipótesis para su entorno de operación. En caso de que alguna de ellas no pudiera asumirse, no sería posible garantizar el funcionamiento seguro del sistema.

3.5.1 Hipótesis de Entorno 01: Entorno seguro y confiable

Se supone que la máquina en la que se instale el producto PROCESA se encuentra correctamente configurada en lo referente al software base, sistema operativo y servidor de aplicaciones, de forma segura y confiable siguiendo las guías y configuraciones seguras en lo referente a su instalación y configuración.

También se supone que el acceso “físico” a la máquina en la que se instale el producto PROCESA está restringido al usuario (o usuarios) administradores. Se supone que este usuario respetará la seguridad y confidencialidad de los datos sensibles que presentes en la máquina (configuración, auditorías…).

3.5.2 Hipótesis de Entorno 02: Conexión entidades externas segura

La interconexión entre el motor de ejecución de procesos PROCESA Engine y las entidades externas se realizará de forma segura y confiable garantizando la integridad de la información intercambiada entre ambas partes.

4 Objetivos de seguridad

Se definen a continuación los objetivos de seguridad que son satisfechos por el sistema. Dichos objetivos se plantean para hacer frente a las posibles amenazas identificadas. Cada amenaza es cubierta por al menos uno de los objetivos de seguridad que se recogen a continuación.

4.1 Objetivos de seguridad para el TOE

4.1.1 Objetivo 01: Confidencialidad de contraseñas almacenadas en BD y en ficheros de configuración

Las contraseñas de acceso a la base de datos del TOE, de acceso a los LDAPs, de las aplicaciones externar, de acceso al servidor de correo, se almacenarán cifradas en la base de datos y en los ficheros de configuración.

4.1.2 Objetivo 02: Registro de las peticiones realizadas

Se efectuará un registro de todas las peticiones realizadas a los servicios publicados por el motor de ejecución de procesos en el archivo de auditoría que corresponda.

4.1.3 Objetivo 03: Identificación y Control de acceso

Se asociarán restricciones de acceso para cada una de las aplicaciones registradas en el sistema de forma que se gestionará la identificación de dichas aplicaciones en base a la asociación de identificador y contraseña garantizando que no es posible la utilización de los servicios de gestión del motor de ejecución de procesos sin autorización. Ciertos servicios (considerados administrativos) requerirán que la aplicación identificada posea, además, el rol “engineAdministrator”.

4.2 Objetivos de seguridad para el entorno

Los objetivos de seguridad para el entorno que se indican a continuación se plantean para contrarrestar las amenazas y/o hacer cumplir las políticas de seguridad organizacional que no hayan sido cubiertas, bien por los objetivos de seguridad del TOE o bien por las hipótesis de uso seguro del mismo.

4.2.1 Objetivo entorno 01: Garantizar el entorno seguro y confiable

El entorno operacional del TOE debe permitir el acceso al TOE o partes del TOE únicamente al personal autorizado al mismo (el administrador del TOE).

4.2.2 Objetivo entorno 02: Garantizar la conexión a entidades externas segura

El entorno operacional del TOE (LDAP) debe asegurar que las conexiones sean seguras a través del uso de cifrado y autenticación en las comunicaciones.

4.2.3 Objetivo entorno 03: Revisión de auditorías

El entorno operacional del TOE debe garantizar la realización de auditorías periódicas que permitan la detección de posibles intentos de violación al TOE, para de esta forma poder tomar las medidas oportunas, definidas por el propietario del TOE, en el caso de que dichos intentos sean identificados.

4.3 Razonamiento de los objetivos de seguridad

En esta sección se demuestra que el problema de seguridad planteado es completo y su solución también lo es, relacionando los objetivos de seguridad definidos con las amenazas, políticas e hipótesis establecidas.

4.3.1 Amenazas

Amenaza 01: Violación de la confidencialidad de las contraseñas almacenadas en base de datos o ficheros de configuración.

Esta amenaza se mitiga a través de un objetivo de seguridad y otro del entorno. El Objetivo 01 contribuye mediante el cifrado de las contraseñas; el Objetivo de entorno 01 contribuye al no permitirse el acceso a personal no autorizado.

Amenaza 02: Violación de la integridad en la gestión de roles de proceso

Contribuyen a mitigar esta amenaza los siguientes objetivos de seguridad:

- Objetivo 02: el registro de las peticiones realizadas ayuda a detectar posibles ataques.
- Objetivo 03: el uso de control de acceso a los servicios limita el uso de los mismos a aplicaciones previamente registradas en el sistema.
- Objetivo de entorno 02: la comunicación segura con las entidades externas involucradas contribuye a garantizar la integridad de los servicios.
- Objetivo de entorno 03: la revisión de los archivos de auditoria ayuda a detectar posibles ataques.

Amenaza 03: Violación de la integridad en la gestión del ciclo de vida de los procesos

Contribuyen a mitigar esta amenaza los siguientes objetivos de seguridad:

- Objetivo 02: el registro de las peticiones realizadas ayuda a detectar posibles ataques.
- Objetivo 03: el uso de control de acceso a los servicios limita el uso de los mismos a aplicaciones previamente registradas en el sistema.
- Objetivo de entorno 02: la comunicación segura con las entidades externas involucradas contribuye a garantizar la integridad de los servicios.
- Objetivo de entorno 03: la revisión de los archivos de auditoria ayuda a detectar posibles ataques.

Amenaza 04: Violación de la integridad en la gestión del ciclo de vida de las tareas

Contribuyen a mitigar esta amenaza los siguientes objetivos de seguridad:

- Objetivo 02: el registro de las peticiones realizadas ayuda a detectar posibles ataques.
- Objetivo 03: el uso de control de acceso a los servicios limita el uso de los mismos a aplicaciones previamente registradas en el sistema.
- Objetivo de entorno 02: la comunicación segura con las entidades externas involucradas contribuye a garantizar la integridad de los servicios.
- Objetivo de entorno 03: la revisión de los archivos de auditoria ayuda a detectar posibles ataques.

Amenaza 05: Violación de la integridad en los servicios de acceso a datos

Contribuyen a mitigar esta amenaza los siguientes objetivos de seguridad:

- Objetivo 02: el registro de las peticiones realizadas ayuda a detectar posibles ataques.
- Objetivo 03: el uso de control de acceso a los servicios limita el uso de los mismos a aplicaciones previamente registradas en el sistema.
- Objetivo de entorno 02: la comunicación segura con las entidades externas involucradas contribuye a garantizar la integridad de los servicios.
- Objetivo de entorno 03: la revisión de los archivos de auditoria ayuda a detectar posibles ataques.

Amenaza 06: Violación de la integridad en los servicios de administración

Contribuyen a mitigar esta amenaza los siguientes objetivos de seguridad:

- Objetivo 02: el registro de las peticiones realizadas ayuda a detectar posibles ataques.
- Objetivo 03: el uso de control de acceso a los servicios limita el uso de los mismos a aplicaciones previamente registradas en el sistema.
- Objetivo de entorno 02: la comunicación segura con las entidades externas involucradas contribuye a garantizar la integridad de los servicios.
- Objetivo de entorno 03: la revisión de los archivos de auditoria ayuda a detectar posibles ataques.

Amenaza 07: Violación de la integridad en los servicios de gestión documental

Contribuyen a mitigar esta amenaza los siguientes objetivos de seguridad:

- Objetivo 02: el registro de las peticiones realizadas ayuda a detectar posibles ataques.
- Objetivo 03: el uso de control de acceso a los servicios limita el uso de los mismos a aplicaciones previamente registradas en el sistema.
- Objetivo de entorno 02: la comunicación segura con las entidades externas involucradas contribuye a garantizar la integridad de los servicios.
- Objetivo de entorno 03: la revisión de los archivos de auditoria ayuda a detectar posibles ataques.

4.3.2 Políticas

Política 01: Restricción de acceso al TOE

El Objetivo de entorno 01 establece el acceso restringido al TOE sólo al administrador del TOE y garantiza así el cumplimiento de esta política.

Política 02: Disposición de datos de usuario y privilegios de acceso a los servicios del TOE

El Objetivo de entorno 01 establece que únicamente el administrador del TOE tiene acceso al mismo. Siendo éste el encargado de establecer los privilegios de acceso a las aplicaciones clientes, se garantiza así el cumplimiento de esta política, no pudiendo aplicaciones no autorizadas hacer uso de los servicios del TOE.

Política 03: Configuración segura de conexiones externas del TOE

El Objetivo de entorno 02 garantiza que la conexión del TOE a las entidades externas se realiza de manera seguro, cumpliendo así esta política.

Política 04: Revisión de auditorías

El Objetivo de entorno 03 establece que el entorno operacional del TOE ha de garantizar la revisión periódica de los archivos de auditoria cumpliéndose así esta política.

4.3.3 Hipótesis

Hipótesis 01: Administrador del sistema confiable

Los siguientes objetivos contribuyen al cumplimiento de esta hipótesis:

- Objetivo de entorno 01: puesto que el acceso al TOE se encuentra restringido únicamente al administrador del TOE, se puede confiar en la labor del mismo.

Hipótesis 02: Administrador de la auditoría

El Objetivo de entorno 03 establece que el entorno operacional del TOE ha de garantizar la revisión periódica de los archivos de auditoria cumpliéndose así esta hipótesis.

Hipótesis de Entorno 01: Entorno seguro y confiable

Los siguientes objetivos contribuyen al cumplimiento de esta hipótesis:

- Objetivo de entorno 01: al no permitirse el acceso a personal no autorizado.

Hipótesis de Entorno 02: Conexión entidades externas segura

Los siguientes objetivos contribuyen al cumplimiento de esta hipótesis:

- Objetivo de entorno 02: la comunicación segura con las entidades externas involucradas contribuye a garantizar la integridad de los servicios.

Como se puede observar, todos los objetivos están relacionados con alguna amenaza o política, quedando patente que todos ellos son necesarios. Igualmente, todas las amenazas, políticas e hipótesis tienen relación con algún objetivo. De esta manera, se concluye que la solución al problema de seguridad planteado es una solución completa.

5 Requisitos de seguridad

5.1 Requisitos funcionales de seguridad

5.1.1 Relación de objetos

Para la definición de los requisitos funcionales de seguridad, se consideran como objetos los siguientes activos del TOE:

- Acceso a contraseñas almacenadas en base de datos y ficheros de configuración
- Servicio TOE. Se entiende por servicio TOE cada uno de los activos detallados anteriormente.

5.1.2 Relación de sujetos y sus atributos

Para la definición de los requisitos funcionales de seguridad, se consideran los siguientes sujetos:

- **Aplicaciones usuarias:** Aplicaciones usuarias que acceden a los servicios que proporciona PROCESA Engine (TOE). El acceso se lleva a cabo a través de servicios web publicados sobre protocolo HTTPS. Sus atributos de seguridad son los que se indican a continuación:
    - La identidad de la aplicación invocante. Código que identifica a la aplicación que realiza la invocación.
    - Para el caso de los servicios que requieran interacción con usuarios se indicará además el identificador del usuario de forma que se compruebe si dicho usuario puede o no ejecutar determinadas tareas.
    - Ciertos servicios administrativos requerirán que la identidad de la aplicación invocante posea, además, el rol de seguridad como aplicación administradora de la plataforma (valor 'engineAdministrator')
    - Una aplicación usuaria puede tener una descripción asociada.
    - Una aplicación usuaria puede estar desactivada, de tal manera que sus datos estén registrados pero sus invocaciones se rechacen.

5.2 Requisitos de control de acceso

5.2.1 FDP_ACC.2 Complete Access control

Hierarchical to: FDP_ACC.1 Subset access control
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.2.1 **The TSF shall enforce the [assignment: PROCESA_ACCESS_CONTROL] on [assignment:**

- *Lista de objetos:*
    - *Acceso a contraseñas almacenadas en base de datos y ficheros de configuración.*
    - *Servicio del TOE*

- *Lista de sujetos*
  - *Aplicaciones usuarias*

] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 **The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP**

5.2.2 FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 **The TSF shall enforce the [assignment:** *PROCESA_ACCESS_CONTROL***] to objects based on the following: [assignment:**

- *Objetos:*
  - *Acceso a contraseñas almacenadas en base de datos y ficheros de configuración.*
  - *Servicio del TOE*
- *Atributos de objetos: ninguno.*
- *Sujetos*
  - *Aplicaciones usuarias*
    - *Atributos para la invocación a un webservice:*
      - *La identidad de la aplicación invocante.*
      - *La contraseña de la aplicación invocante.*

    Si la aplicación usuaria desea hacer uso de los servicios administrativos (o de gestión) deberá poseer el siguiente atributo:

      - *El rol de seguridad, el posible valor es 'engineAdministrator'*

    Además en caso de realizarse la invocación a servicios en los que sea necesaria la identificación del usuario que realiza la invocación, se ven involucrados también los siguientes atributos:

      - *Identificador del usuario.*

]

FDP_ACF.1.2 **The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment:**

- *Acceso de los sujetos (aplicaciones usuarias)*
  - *Invocación a un webservice:*

    Al recibir el TOE una petición a uno de sus servicios web publicados por parte de una entidad externa, éste comprueba que la aplicación invocante existe en el sistema. Si existe, pasa a verificar que la password introducida coincide con la asignada en el sistema en el momento de dar de alta la aplicación desde la consola de administración.

Si todas estas comprobaciones dan un resultado positivo el acceso le será permitido al servicio del TOE (objeto definido para el que se controla el acceso), el cual, para desarrollar las acciones correspondientes para construir la respuesta que se envía al cliente accede a los siguientes objetos:

- *Activo 01. Acceso a contraseñas almacenadas en base de datos y ficheros de configuración. El sistema de control de acceso tiene que comprobar que la contraseña suministrada por la aplicación usuario coincide con la contraseña almacenada en el sistema.*
- *Activos 02 al 07. Servicios del TOE. Cada petición que realiza una aplicación usuaria y que supere el control de acceso definido accede a un servicio del TOE.*

Adicionalmente a la tarea de verificación de la aplicación y la password, comentada anteriormente, para ciertos servicios es necesario proveer el atributo que identifique el usuario que está intentando ejecutar el proceso o la tarea (actor en el BPM). La información del usuario que está ejecutando el servicio se utiliza para comprobar si el usuario pertenece al rol de proceso de la tarea o procedimiento que quiere ejecutar. Esta regla determina la posibilidad o no de ejecutar el servicio por parte del usuario. El concepto de rol de proceso es distinto al del rol de aplicación (rol de seguridad) dentro del TOE. El rol de proceso acota las tareas y acciones dentro de un proceso que puede ejecutar un usuario, un grupo de usuario o un rol de seguridad definido den el TOE. La asociación de un usuario, grupo de usuarios o rol de seguridad a un rol de proceso se realiza desde la consola de administración. Mientras que el rol de seguridad determina las funciones del TOE que se puede ejecutar desde la consola de administración.

].

FDP_ACF.1.3 **The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment:** *no hay ninguna regla adicional***].**

FDP_ACF.1.4 **The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment:** *no hay ninguna regla adicional***].**

5.2.3 FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 **The TSF shall enforce the [assignment:** *PROCESA_ACCESS_CONTROL***] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.**

FMT_MSA.3.2 **The TSF shall allow the [assignment:** *engineAdministrator*] **to specify alternative initial values to override the default values when an object or information is created.**

5.2.4 FMT_MSA.1 Management of security attributes.

Hierarchical to: No other components.
Dependencies: FDP_ACC.2 Complete access control
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 **The TSF shall enforce the [assignment:** *PROCESA_ACCESS_CONTROL*] **to restrict the ability to [selection:** *query, add, modify, delete*] **the security attributes [assignment:** *atributos de los sujetos aplicaciones externas*] **to [assignment:** *engineAdministrator*]**.**

5.2.5 FMT_SMR.1 Security roles

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 **The TSF shall maintain the roles [assignment:** *engineAdministrator*]**.**

FMT_SMR.1.2 **The TSF shall be able to associate users with roles.**

5.2.6 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.
Dependencies: No dependencies.

FMT_SMF.1.1 **The TSF shall be capable of performing the following management functions: [assignment:**

Las funciones de gestión que es posible utilizar son las siguientes:

- *Servicios de administración*
  - *Gestión de Aplicaciones usuarias. Estos servicios permiten añadir, actualizar o eliminar identidades de aplicaciones externas con permisos de ejecución de los servicios de Procesa Engine y asociarles el rol "engineAdministrator" si han de invocar servicios administrativos.*
  - *Gestión de los parámetros de configuración del TOE. Estos servicios permiten recuperar y establecer las propiedades de instalación de Procesa Engine (.ERTC.properties).*
  - *Gestión de Fuentes de identidad. Estos servicios permiten añadir, actualizar o eliminar fuentes de identidades (LDAPs) que podrán ser utilizadas en la gestión de roles o autentificación de usuarios (actores BPM, no aplicaciones cliente).*

Por tanto, una aplicación cliente que deba invocar estos servicios del TOE ha de poseer el rol "engineAdministrator".

].

5.2.7 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies.

FIA_UID.2.1 **The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.**

5.2.8 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 **The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.**

5.2.9 FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UAU.4.1 **The TSF shall prevent reuse of authentication data related to [assignment:** *usuario/contraseña*]**.**

5.3 Requisitos relativos a auditoría de eventos

5.3.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 **The TSF shall be able to generate an audit record of the following auditable events:**

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [*not specified***] level of audit; and**

c) [assignment: *Todas las invocaciones a un servicio web publicado por el TOE*]**.**

FAU_GEN.1.2 **The TSF shall record within each audit record at least the following information:**

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *Parámetros del servicio invocado, Valor de retorno del servicio*]**.**

5.3.2 FAU_GEN.2 User identity association

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 **For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.**

5.4 Requisitos relativos a confidencialidad de las contraseñas

5.4.1 FCS_COP.1 Cryptographic operation.

Hierarchical to: No other components.
Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 **The TSF shall perform [assignment:** *cifrado de contraseñas, descifrado de contraseñas*] **in accordance with a specified cryptographic algorithm [assignment:** *3DES*] **and cryptographic key sizes [assignment:** *192 bits*] **that meet the following: [assignment:** *FIPS 46-2 Data Encryption Standard*]**.**

5.4.2 FCS_CKM.1 Cryptographic key generation.

Hierarchical to: No other components.
Dependencies: FCS_COP.1 Cryptographic operation
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 **The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment:** *3DES*] **and specified cryptographic key sizes [assignment:** *192 bits*] **that meet the following: [assignment:** *La generación de la clave se hace usando una palabra clave secreta (semilla) codificada dentro del TOE a partir de la cual se obtiene la clave simétrica de cifrado/descifrado según lo especificado por la norma FIPS 46-3 Data Encryption Standard. La creación de la clave se hace en el arranque del TOE.*]**.**

5.4.3 FCS_CKM.4 Cryptographic key destruction.

Hierarchical to: No other components.
Dependencies: FCS_CKM.1 Cryptographic key generation

FCS_CKM.4.1 **The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment:** *destrucción de la clave de la memoria*] **that meets the following: [assignment:** *al parar el motor de ejecución de procesos PROCESA Engine (TOE) se realiza el borrado de la memoria de forma pasiva.*
La parada del TOE se realiza por cualquiera de los siguientes motivos:

- *Parada del TOE desde el servidor de aplicaciones*.
- *Repliegue del TOE en el servidor de aplicaciones.*
- *Actualización del TOE en el servidor de aplicaciones.*
- *Parada del servidor de aplicaciones.*

].

En los siguientes apartados se definen los requisitos de garantía de aseguramiento satisfechos por el TOE para la obtención del nivel de certificación EAL1 (Evaluation Assurance Level 1). Todo ello, de acuerdo con los términos especificados en el Catálogo de Componentes de Garantía de Common Criteria Parte 3.

5.5 Requisitos de aseguramiento: Clase ASE – Security Target Evaluation

5.5.1 ASE_INT.1 ST introduction

Dependencies: No dependencies.

Developer action elements:

ASE_INT.1.1D **The developer shall provide an ST introduction.**

Content and presentation elements:

ASE_INT.1.1C **The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.**

ASE_INT.1.2C **The ST reference shall uniquely identify the ST.**

ASE_INT.1.3C **The TOE reference shall identify the TOE.**

ASE_INT.1.4C **The TOE overview shall summarise the usage and major security features of the TOE.**

ASE_INT.1.5C **The TOE overview shall identify the TOE type.**

ASE_INT.1.6C **The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.**

ASE_INT.1.7C **The TOE description shall describe the physical scope of the TOE.**

ASE_INT.1.8C **The TOE description shall describe the logical scope of the TOE.**

5.5.2 ASE_CCL.1 Conformance claims

Dependencies: ASE_INT.1 ST introduction
ASE_ECD.1 Extended components definition
ASE_REQ.1 Stated security requirements

Developer action elements:

ASE_CCL.1.1D **The developer shall provide a conformance claim.**

ASE_CCL.1.2D **The developer shall provide a conformance claim rationale.**

Content and presentation elements:

ASE_CCL.1.1C **The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.**

ASE_CCL.1.2C **The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.**

ASE_CCL.1.3C **The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.**

ASE_CCL.1.4C **The CC conformance claim shall be consistent with the extended components definition.**

ASE_CCL.1.5C **The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.**

ASE_CCL.1.6C **The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.**

ASE_CCL.1.7C **The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.**

ASE_CCL.1.8C **The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.**

ASE_CCL.1.9C **The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.**

ASE_CCL.1.10C **The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.**

5.5.3 ASE_OBJ.2 Security objectives

Dependencies: ASE_SPD.1 Security problem definition

Developer action elements:

ASE_OBJ.2.1D **The developer shall provide a statement of security objectives.**

ASE_OBJ.2.2D **The developer shall provide a security objectives rationale.**

Content and presentation elements:

ASE_OBJ.2.1C **The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.**

ASE_OBJ.2.2C **The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.**

ASE_OBJ.2.3C **The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.**

ASE_OBJ.2.4C **The security objectives rationale shall demonstrate that the security objectives counter all threats.**

ASE_OBJ.2.5C **The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.**

ASE_OBJ.2.6C **The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.**

5.5.4 ASE_SPD.1 Security problem definition

Dependencies: No dependencies.

Developer action elements:

ASE_SPD.1.1D **The developer shall provide a security problem definition.**

Content and presentation elements:

ASE_SPD.1.1C **The security problem definition shall describe the threats.**

ASE_SPD.1.2C **All threats shall be described in terms of a threat agent, an asset, and an adverse action.**

ASE_SPD.1.3C **The security problem definition shall describe the OSPs.**

ASE_SPD.1.4C **The security problem definition shall describe the assumptions about the operational environment of the TOE.**

5.5.5 ASE_ECD.1 Extended components definition

Dependencies: No dependencies.

Developer action elements:

ASE_ECD.1.1D **The developer shall provide a statement of security requirements.**

ASE_ECD.1.2D **The developer shall provide an extended components definition.**

Content and presentation elements:

ASE_ECD.1.1C **The statement of security requirements shall identify all extended security requirements.**

ASE_ECD.1.2C **The extended components definition shall define an extended component for each extended security requirement.**

ASE_ECD.1.3C **The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.**

ASE_ECD.1.4C **The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.**

ASE_ECD.1.5C **The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.**

5.5.6 ASE_REQ.2 Derived security requirements

Dependencies: ASE_OBJ.2 Security objectives
ASE_ECD.1 Extended components definition

Developer action elements:

ASE_REQ.2.1D **The developer shall provide a statement of security requirements.**

ASE_REQ.2.2D **The developer shall provide a security requirements rationale.**

Content and presentation elements:

ASE_REQ.2.1C **The statement of security requirements shall describe the SFRs and the SARs.**

ASE_REQ.2.2C **All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.**

ASE_REQ.2.3C **The statement of security requirements shall identify all operations on the security requirements.**

ASE_REQ.2.4C **All operations shall be performed correctly.**

ASE_REQ.2.5C **Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.**

ASE_REQ.2.6C **The security requirements rationale shall trace each SFR back to the security objectives for the TOE.**

ASE_REQ.2.7C **The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.**

ASE_REQ.2.8C **The security requirements rationale shall explain why the SARs were chosen.**

ASE_REQ.2.9C **The statement of security requirements shall be internally consistent.**

5.5.7 ASE_TSS.1 TOE summary specification

Dependencies: ASE_INT.1 ST introduction
ASE_REQ.1 Stated security requirements
ADV_FSP.1 Basic functional specification

Developer action elements:

ASE_TSS.1.1D **The developer shall provide a TOE summary specification.**

Content and presentation elements:

ASE_TSS.1.1C **The TOE summary specification shall describe how the TOE meets each SFR.**

5.6 Requisitos de aseguramiento: Clase ADV – Development

5.6.1 ADV_FSP.1 Basic functional specification

Dependencies: No dependencies.

Developer action elements:

ADV_FSP.1.1D **The developer shall provide a functional specification.**

ADV_FSP.1.2D **The developer shall provide a tracing from the functional specification to the SFRs.**

Content and presentation elements:

ADV_FSP.1.1C **The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.**

ADV_FSP.1.2C **The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.**

ADV_FSP.1.3C **The functional specification shall provide rationale for the implicit categorisation of interfaces as SFR-non-interfering.**

ADV_FSP.1.4C **The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.**

5.7 Requisitos de aseguramiento: Clase AGD – Guidance documents

5.7.1 AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:

AGD_OPE.1.1D **The developer shall provide operational user guidance.**

Content and presentation elements:

AGD_OPE.1.1C **The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.**

AGD_OPE.1.2C **The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.**

AGD_OPE.1.3C **The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.**

AGD_OPE.1.4C **The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-**

accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C **The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.**

AGD_OPE.1.6C **The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.**

AGD_OPE.1.7C **The operational user guidance shall be clear and reasonable.**

5.7.2 AGD_PRE.1 Preparative procedures

Dependencies: No dependencies.

Developer action elements:

AGD_PRE.1.1D **The developer shall provide the TOE including its preparative procedures.**

Content and presentation elements:

AGD_PRE.1.1C **The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.**

AGD_PRE.1.2C **The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.**

5.8 Requisitos de aseguramiento: Clase ALC - Life-Cycle Support

5.8.1 ALC_CMC.1 Labelling of the TOE

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements:

ALC_CMC.1.1D **The developer shall provide the TOE and a reference for the TOE.**

Content and presentation elements:

ALC_CMC.1.1C **The TOE shall be labelled with its unique reference.**

5.8.2 ALC_CMS.1 TOE CM coverage

Dependencies: No dependencies.

Developer action elements:

ALC_CMS.1.1D **The developer shall provide a configuration list for the TOE.**

Content and presentation elements:

ALC_CMS.1.1C **The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.**

ALC_CMS.1.2C **The configuration list shall uniquely identify the configuration items.**

5.8.3 ALC_FLR.1 Basic flaw remediation

Dependencies: No dependencies.

Developer action elements:

ALC_FLR.1.1D **The developer shall document and provide flaw remediation procedures addressed to TOE developers.**

Content and presentation elements:

ALC_FLR.1.1C **The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.**

ALC_FLR.1.2C **The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.**

ALC_FLR.1.3C **The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.**

ALC_FLR.1.4C **The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.**

5.9 Requisitos de aseguramiento: Clase ATE - Tests

5.9.1 ATE_IND.1 Independent testing - conformance

Dependencies: ADV_FSP.1 Basic functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements:

ATE_IND.1.1D **The developer shall provide the TOE for testing.**

Content and presentation elements:

ATE_IND.1.1C **The TOE shall be suitable for testing.**

5.10 Requisitos de aseguramiento: Clase AVA - Vulnerability Assessment

5.10.1 AVA_VAN.1 Vulnerability survey

Dependencies: ADV_FSP.1 Basic functional specification
AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

Developer action elements:

AVA_VAN.1.1D **The developer shall provide the TOE for testing.**

Content and presentation elements:

AVA_VAN.1.1C **The TOE shall be suitable for testing.**

5.11 Razonamiento de requisitos

5.11.1 Razonamiento de requisitos funcionales

En esta sección se demuestra que todos los requisitos funcionales expuestos son necesarios, pues todos y cada uno de ellos son necesarios para el cumplimiento de un objetivo, y viceversa, que todos los objetivos están cubiertos por al menos un requisito. Asimismo, se expone porque alguna de las dependencias entre los requisitos funcionales detallados no se cumplen.

La dependencia existente entre los requisitos FAU_GEN.1 y FPT_STM.1 no se cumple puesto que la fecha y hora registrada en los ficheros de auditoría no pertenece a la funcionalidad de seguridad del TOE, sino que simplemente es un dato más a registrar en ellos.

Objetivo 01: Confidencialidad de contraseñas almacenadas en BD y en ficheros de configuración

Para este objetivo se asegura que sólo los usuarios que, tras cumplir los requisitos de identificación y autenticación a continuación expuestos, superen las restricciones de acceso impuestas a través de los requisitos (FDP_ACC.2, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1, FMT_SMF.1, FIA_UID.2, FIA_UAU.2 y FIA_UAU.4), podrán leer las contraseñas almacenadas en base de datos y que las deberán descifrar por medio del requisito FCS_COP.1 correspondiente a los de cifrado/descifrado de los impuestos dependiendo de los parámetros de la operación. Para ello deberá utilizar la clave generada para el cifrado (FCS_CKM.1) con los parámetros correspondientes. Esta clave se destruye (FSC_CKM.4) cuando Procesa Engine se para por algún motivo (parada, repliege o actualización del TOE o parada del servidor de aplicaciones).

Los requisitos previos necesarios a cumplir por los usuarios que accedan a las contraseñas almacenadas en base de datos:

- **Entidades externas**: han debido de ser identificadas como exponen los requisitos (FIA_UID.2 y FIA_UAU.2). Así, para su identificación, se ha de comprobar que el identificador de aplicación con el que realizan la petición existe en el sistema.

Objetivo 02: Registro de las peticiones realizadas

Todas las peticiones realizadas a los servicios web se registrarán en el fichero de auditoría (FAU_GEN.1, FAU_GEN.2), los datos necesarios para cada tipo de auditoría.

Objetivo 03: Identificación y control de acceso

Para este objetivo se asegura que sólo las entidades externas que se hayan identificado y autenticado previamente en el TOE (FIA_UID.2, FIA_UAU.4 y FIA_UAU.2) y superado las restricciones de acceso impuestas a través de los requisitos (FDP_ACC.2, FDP_ACF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1, FMT_SMF.1) accederán a los servicios publicados por el TOE.

A continuación, se muestra la correspondencia entre requisitos funcionales y objetivos de seguridad (qué objetivos satisface cada requisito):

Requisito funcional	Objetivos de seguridad

FDP_ACC.2	Objetivo 01, Objetivo 03
FDP_ACF.1	Objetivo 01, Objetivo 03
FMT_MSA.1	Objetivo 01, Objetivo 03
FMT_MSA.3	Objetivo 01, Objetivo 03
FMT_SMR.1	Objetivo 01, Objetivo 03
FMT_SMF.1	Objetivo 01, Objetivo 03
FIA_UID.2	Objetivo 01, Objetivo 03
FIA_UAU.2	Objetivo 01, Objetivo 03.
FIA_UAU.4	Objetivo 01, Objetivo 03.
FAU_GEN.1	Objetivo 02
FAU_GEN.2	Objetivo 02
FCS_COP.1	Objetivo 01
FCS_CKM.1	Objetivo 01
FCS_CKM.4	Objetivo 01

Tabla 3 - Razonamiento de los requisitos funcionales

5.11.2 Razonamiento requisitos de aseguramiento

Los requisitos de aseguramiento se basan en la selección de aquellos necesarios para una evaluación EAL1 (descritos en los apartados 6.5, 6.6, 6.7, 6.8, 6.9 y 6.10 del presente documento), incrementados con ALC_FLR.1 Basic flaw remediation (que describe cómo se gestionan las incidencias, desde su principio hasta su cierre), ASE_SPD.1 Security problem definition (descripción completa del problema de seguridad), ASE_OBJ.2 Security objectives (descripción de los objetivos de seguridad) y ASE_REQ.2 Derived security requirements (descripción de los requisitos de seguridad derivados).

La selección de dichos requisitos de aseguramiento responde a las necesidades del mercado de ofrecer un producto encargado de la gestión de flujos de trabajo y tareas seguro y confiable, que garantice el control de acceso y la trazabilidad de las peticiones realizadas.

6 Especificación resumida

Esta sección define cómo se instancian en el TOE los requisitos de seguridad establecidos en el apartado anterior.

6.1 FDP_ACC.2 Complete access control

El TOE controla el acceso por parte de cualquier tipo de sujeto (ya sea entidad externa con o sin rol de *engineAdministrator*) a los siguientes objetos:

- Acceso a contraseñas almacenadas en base de datos
- Servicio TOE. Se entiende por servicio TOE cada uno de los activos detallados anteriormente.

Asimismo, el TOE asegura que ninguno de los sujetos detallados antes realizará ningún tipo de operación no autorizada mediante las reglas descritas para el requisito presentado a continuación (FDP_ACF.1).

6.2 FDP_ACF.1 Security attribute based access control

El TOE controla el acceso de los sujetos que representan entidades externas realizando una invocación a un Webservice. El servicio del TOE al que se invoca comprueba que la aplicación invocante existe en el sistema y corresponde la tupla identificador/contraseña con la almacenada en el sistema.

En el caso de los servicios relacionados con la gestión de parámetros de configuración del TOE o relacionados por la gestión de roles de proceso se comprueba adicionalmente el identificador del rol de seguridad suministrado. Solamente se permite su invocación si el rol de seguridad coincide con el valor *engineAdministrator.*

Si todas estas comprobaciones dan un resultado positivo el acceso les será permitido a los activos 01 (acceso a contraseñas almacenadas en base de datos) y activos 02 al 07 (servicio del TOE).

6.3 FMT_MSA.1 Management of security attributes

6.3.1 FMT_MSA.1.1

Los atributos de seguridad asociados a los sujetos de tipo aplicación externa pueden ser modificados o borrados por un usuario administrador del TOE desde la consola de administración, la información que se gestiona:

- **Identidad de la aplicación invocante**: al borrar una aplicación se está borrando también el código que correspondería para esa aplicación con este atributo.
- **Contraseña de la aplicación invocante**: al borrar una aplicación se está borrando también el código que correspondería para esa aplicación con este atributo.

Las restricciones de acceso para las aplicaciones usuarias son definidas por un usuario con el rol *engineAdministrator* del TOE desde la consola de administración (o mediante los servicios del TOE a través de una aplicación externa con la autorización necesaria).

6.4 FMT_MSA.3 Static attribute initialisation

Los valores que toman los atributos de seguridad son inicialmente nulos, hasta que un usuario de la consola (o mediante los servicios web administrativos del TOE) los modifica de la siguiente manera:

Invocación de una aplicación externa.

- Identidad de la aplicación invocante: al dar de alta una aplicación se está inicializando este valor.
- Contraseña de la aplicación invocante: al dar de alta una aplicación se está inicializando este valor.

Usuarios de los servicios administrativos

Uno de los atributos de seguridad de los sujetos del TOE es el rol de seguridad que ocupan en el mismo. Las aplicaciones externas con acceso a los servicios web administrativos del TOE (como por ejemplo la consola de administración) tendrán el rol de seguridad *engineAdministrator.*

6.5 FMT_SMR.1 Security roles

Las apliaciones administradoras del TOE, (como, por ejemplo, la consola de administración), deben tener un rol asociado que sólo puede tomar el valor <*engineAdministrator*>.

6.6 FMT_SMF.1 Specification of Management Functions

El TOE proporciona una serie de funciones de gestión que son accesible tanto desde la consola de administración PROCESA EngineAdministrator como directamente a través de servicios web. Las funciones que es posible utilizar son:

- *Servicios de administración*
    - *Gestión de Aplicaciones usuarias. Estos servicios permiten añadir, actualizar o eliminar identidades de aplicaciones externas con permisos de ejecución de los servicios de Procesa Engine y asociarles el rol "engineAdministrator" si han de invocar servicios administrativos.*
    - *Gestión de los parámetros de configuración del TOE. Estos servicios permiten recuperar y establecer las propiedades de instalación de Procesa Engine (.ERTC.properties).*
    - *Gestión de Fuentes de identidad. Estos servicios permiten añadir, actualizar o eliminar fuentes de identidades (LDAPs) que podrán ser utilizadas en la gestión de roles o autentificación de usuarios (actores BPM, no aplicaciones cliente).*

Todas estas funciones están implementadas como servicios web de modo que es posible su invocación de forma externa ya sea a través de la consola de administración PROCESA EngineAdministrator o directamente desde servicio web (sólo aquellas aplicaciones usuarias que posean el rol "engineAdministrator").

Para estas funciones el TOE controla el acceso a su invocación de forma que solamente aquellas aplicaciones que hayan sido registradas previamente el sistema podrán hacer uso de las mismas. Igualmente todas las peticiones realizadas a estas funciones queda registrada por

el componente de auditoría que dispone el TOE. En dicho registro se almacena toda la información referente al mensaje de la petición realizada, el momento en el que se realizó, desde que sistema externo se realizó, qué función se invocó y qué aplicación realizó la petición. Se registra también la respuesta que originó el TOE y el momento de la misma.

6.7 FIA_UID.2 User identification before any action

Los sujetos que solicitan un servicio web del TOE son entidades externas (aplicaciones), las solicitudes deben incluir dos atributos que las identifican (identificador y contraseña). Estos atributos deben comprobarse en el momento de la invocación mediante las reglas de restricción de acceso definidas previamente en la consola. Con todo ello, los sujetos de tipo entidades externas no pueden realizar ninguna acción previa a la identificación.

Adicionalmente cuando los servicios a los que se intentan acceder son los relacionados con la gestión del ciclo de vida de los procesos o de las tareas será necesario además suministrar un atributo adicional que identifique al usuario que está haciendo la petición.

6.8 FIA_UAU.2 User authentication before any action

Una entidad externa ya ha sido identificada debe ser autenticado por medio de la identificación única antes de poder realizar cualquier acción. Esto permitirá determinar si la entidad externa posee el rol necesario (engineAdministrator) en caso de pretender ejecutar servicios administrativos.

6.9 FIA_UAU.4 Single-use authentication mechanisms

La identificación del las entidades externas se realiza mediante identificador/contraseña de forma que cada aplicación disponga de un identificador/contraseña unívoco.

6.10 FCS_CKM.1 Cryptographic key generation

El TOE permite generar claves criptográficas con el propósito de mantener la confidencialidad de las contraseñas almacenadas tanto en ficheros de configuración como en base de datos. Dichas claves se utilizar para cifrar y descifrar las contraseñas almacenadas tanto en base de datos como en ficheros de configuración. La generación de dichas claves se realiza en el momento del arranque del TOE.

6.11 FCS_CKM.4 Cryptographic key destruction

La destrucción de las claves criptográficas usadas para las operaciones de cifrado y descifrado se realiza en el momento de parar el TOE dicha destrucción se realiza borrando la clave de la memoria.

La parada del TOE se realiza por cualquiera de los siguientes motivos:

- Parada del TOE desde el servidor de aplicaciones.
- Repliegue del TOE en el servidor de aplicaciones.
- Actualización del TOE en el servidor de aplicaciones.
- Parada del servidor de aplicaciones.

6.12 FCS_COP.1 Cryptographic operation

El soporte criptográfico requiere que las operaciones criptográficas se realicen de acuerdo a un algoritmo específico y con unas claves criptográficas de tamaños determinados. El TOE realiza las siguientes operaciones criptográficas de cifrado y descifrado de acuerdo a los algoritmos criptográficos y los tamaños de claves que se especifican a continuación de acuerdo al estándar *FIPS 46-2 Data Encryption Standard*:

- **Cifrado simétrico de contraseñas**: Las contraseñas almacenadas en base de datos se cifran utilizando el algoritmo simétrico 3DES (192 bits) de manera que cada vez que se genera una contraseña que va a ser almacenada en base de datos o fichero de configuración, ha de ejecutarse una operación de cifrado.
- **Descifrado simétrico de contraseñas**: Igualmente, las contraseñas almacenadas en base de datos se descifran utilizando el algoritmo simétrico 3DES (192 bits), de manera que cada vez que la aplicación necesita una de ellas, ha de ejecutarse una operación de descifrado.

6.13 FAU_GEN.1 Audit data generation

Existe un único componente de auditoría asociado a los servicios del TOE. Cada vez que un servicio del TOE es invocado registra, antes de realizar cualquier tipo de acción, a través del componente de auditoría la petición antes de realizar cualquier tipo de operación, la fecha en la que se realizó, el tipo de evento, la aplicación responsable de la invocación, el sujeto responsable de la invocación, la operación solicitada y sus parámetros.

El mismo proceso es llevado a cabo al término de la operación del servicio invocado, sólo que en este caso además se registra el estado final de la misma: si ha tenido éxito o ha ocurrido algún error.

6.14 FAU_GEN.2 User identity association

Todos los mensajes de auditoría incluirán información acerca del causante del evento auditado que, en este caso, es la aplicación externa que invoca el servicio web.