



I.C.A. Informática y Comunicaciones Avanzadas, S.L



Herramienta de Gestión de Eventos LogICA v2.1-SP6 Security Target

Agosto, 2009
Informática y Comunicaciones Avanzadas S.L
La Rábida 27
28039 Madrid

© Copyright Informática y Comunicaciones Avanzadas, S.L., 2008
Este documento es propiedad de **Informática y Comunicaciones Avanzadas** y su contenido es confidencial. Este documento no puede ser reproducido, en su totalidad o parcialmente, ni mostrado a otros, ni utilizado para otros propósitos que los que han originado su entrega, sin el previo permiso escrito de **Informática y Comunicaciones Avanzadas**. En el caso de ser entregado en virtud de un contrato, su utilización estará limitada a lo expresamente autorizado en dicho contrato. **Informática y Comunicaciones Avanzadas** no podrá ser considerada responsable de eventuales errores u omisiones en la edición del documento

CONTROL DE VERSIONES

TÍTULO DEL DOCUMENTO	Herramienta de Gestión de Eventos LogICA v2.1-SP6 Security Target
-----------------------------	---

Versión	Fecha	Descripción	Realizado por	Revisado por
1.1	15-05-2007	Versión borrador del documento	Ernst & Young	ICA Seguridad Lógica
1.2	25-05-2007	Versión borrador del documento	Ernst & Young	ICA Seguridad Lógica
1.3	26-05-2007	Versión borrador del documento	Ernst & Young	ICA Seguridad Lógica
1.4	01-06-2007	Versión inicial del documento	Ernst & Young	ICA Seguridad Lógica
1.5	15-06-2007	Versión evaluada	Ernst & Young	ICA Seguridad Lógica
1.6	14-10-2007	Modificación versiones del software que soporta la herramienta y formato del documento	Ernst & Young	ICA Seguridad Lógica
1.7	12-02-2008	Corrección de ORs	Ernst & Young	ICA Seguridad Lógica
1.9	27-03-2008	Modificación componentes y formato del documento	Ernst & Young	ICA Seguridad Lógica
1.10	15-05-2008			
1.11	12-06-2008	Modificación de versiones de documentos y relación de objetivos	ICA	ICA
1.12	20-06-2008	Modificación de cambios de versionado de documentos, cambios de fecha de referencia, aclaración de funciones.	ICA	ICA
1.13	27-06-2008	Corregir mapeos de objetivos, funciones de seguridad e hipótesis. Revisión general.	Ernst & Young	ICA
1.14	15-12-2008	Nueva Estructura y concepto.	ICA	ICA Seguridad Lógica
1.15	15-04-2009	Definición TSF, justificación modelo .	ICA	ICA Seguridad Lógica
1.16	10-08-2009	Eliminación SPM.1	ICA	ICA Seguridad Lógica

ÍNDICE DE CONTENIDOS

<u>1. ST Introduction.....</u>	<u>7</u>
<u>1.1. ST Reference & Identification.....</u>	<u>7</u>
1.1.1. ST Identification.....	7
1.1.2. TOE identification.....	7
1.1.3. TOE Version Number.....	7
1.1.4. ST Date.....	7
1.1.5. ST Author	7
1.1.6. Assurance Level.....	7
1.1.7. Strength of function.....	7
<u>1.2. ST Overview.....</u>	<u>8</u>
<u>1.3. CC Conformance.....</u>	<u>8</u>
<u>2. TOE description.....</u>	<u>9</u>
<u>2.1. Introduction.....</u>	<u>9</u>
<u>2.2. Objetivos del TOE.....</u>	<u>9</u>
<u>2.3. Componentes del TOE.....</u>	<u>10</u>
2.3.1. Componentes.....	10
<u>2.4. Entorno IT.....</u>	<u>10</u>
<u>2.5. Descripción de la Arquitectura.....</u>	<u>11</u>
2.5.1. Arquitectura Alto Nivel.....	11
2.5.2. Estructura Física del TOE.....	12
<u>2.6. Summary of Security Features.....</u>	<u>12</u>
2.6.1. Auditoría de accesos, registro de accesos.....	12
2.6.2. Identificación y autenticación.....	12
2.6.3. Segregación de funciones mediante mapa de roles de usuario.....	12
2.6.4. Integridad de logs originales.....	12
2.6.5. Canales de comunicación cifrados con protocolos seguros.....	12
<u>3. TOE security environment</u>	<u>14</u>
<u>3.1. Assumptions.....</u>	<u>14</u>
3.1.1. Operational assumptions.....	14
3.1.2. Personnel assumptions.....	14
<u>3.2. Threats to security.....</u>	<u>15</u>
<u>3.3. Organisational security policies (OSPs).....</u>	<u>15</u>
<u>4. Security objectives</u>	<u>16</u>
<u>4.1. Security Objectives for the TOE.....</u>	<u>16</u>
<u>4.2. Security Objectives for the Environment.....</u>	<u>16</u>
4.2.1. Correspondencia entre Objetivos de Seguridad, Amenazas y Políticas Organizativas.....	17
4.2.2. Correspondencia entre Objetivos de Seguridad del entorno e hipótesis de entorno.....	18
<u>5. IT Security Requirements.....</u>	<u>20</u>
<u>5.1. TOE Security Functional Requirements (SFRs).....</u>	<u>20</u>

5.1.1. LOGHOST y LOGHOSTMANAGER.....	20
5.1.1.1. FAU GEN.1/LogHost Audit data generation.....	20
5.1.1.2. FPT STM.1 Reliable time stamps.....	20
5.1.1.3. FDP ACC.1/LogHost Subset access control.....	20
5.1.1.4. FDP ACF.1/LogHost Security attribute based access control.....	20
5.1.1.5. FMT MSA.3/LogHost Static attribute initialization.....	21
5.1.1.6. FMT MSA.1/LogHost Management of security attributes.....	21
5.1.1.7. FMT SMR.1/LogHost Security roles.....	21
5.1.1.8. FMT SMF.1/LogHost Specification of Management Functions.....	21
5.1.1.9. FDP ITC.1/LogHost Import of user data without security attributes.....	21
5.1.1.10. FDP ETC.2/LogDB Export of user data with security attributes.....	22
5.1.1.11. FDP ITC.2/LogDB Import of user data with security attributes.....	22
5.1.1.12. FTP ITC.1/LogDB Inter-TSF trusted channel.....	22
5.1.1.13. FIA ATD.1/LogHost User attribute definition	23
5.1.1.14. FIA UAU.2/LogHost User authentication before any action.....	23
5.1.1.15. FIA UID.2/LogHost Timing of identification.....	23
5.1.1.16. FDP DAU.1 Basic Data Authentication.....	23
5.1.1.17. FTP ITC.1/LogHostManager Inter-TSF trusted channel.....	23
5.1.1.18. FPT TDC.1/LogHost Inter-TSF basic TSF data consistency.....	23
5.1.1.19. FDP IFC.1/LogHost Subset information flow control	24
5.1.1.20. FDP IFF.1/LogHost Simple security attributes	24
5.1.2. LOGAGENT y LOGAGENTMANAGER.....	24
5.1.2.1. FAU GEN.1/LogAgent Audit data generation.....	24
5.1.2.2. FDP ACC.1/LogAgent Subset access control.....	25
5.1.2.3. FDP ACF.1/LogAgent Security attribute based access control.....	25
5.1.2.4. FMT MSA.3/LogAgent Static attribute initialization.....	25
5.1.2.5. FMT MSA.1/LogAgent Management of security attributes.....	25
5.1.2.6. FMT SMR.1/LogAgent Security roles.....	25
5.1.2.7. FMT SMF.1/LogAgent Specification of Management Functions.....	25
5.1.2.8. FDP ITC.1/LogAgent Import of user data without security attributes.....	26
5.1.2.9. FDP ETC.2/LogAgent Export of user data with security attributes.....	26
5.1.2.10. FDP ITC.2/LogAgent Import of user data with security attributes.....	26
5.1.2.11. FPT TDC.1/LogAgent Inter-TSF basic TSF data consistency.....	26
5.1.2.12. FTP ITC.1/LogAgent-JMS Inter-TSF trusted channel.....	27
5.1.2.13. FTP ITC.1/LogAgentManager Inter-TSF trusted channel.....	27
5.1.2.14. FIA ATD.1/LogAgent User attribute definition	27
5.1.2.15. FIA UAU.2/LogAgent User authentication before any action.....	27
5.1.2.16. FIA UID.2/LogAgent Timing of identification.....	27
5.1.2.17. FDP IFC.1/LogAgent Subset information flow control	28
5.1.2.18. FDP IFF.1/LogAgent Simple security attributes	28
5.1.3. LOGSERVER.....	28
5.1.3.1. FAU GEN.1/LogServer Audit data generation.....	28
5.1.3.2. FDP ACC.1/LogServer Subset access control.....	29
5.1.3.3. FDP ACF.1/LogServer Security attribute based access control.....	29
5.1.3.4. FMT MSA.3/LogServer Static attribute initialization.....	29
5.1.3.5. FMT MSA.1/LogServer Management of security attributes.....	29
5.1.3.6. FDP IFF.1/LogAgent Simple security attributes	29
5.1.3.7. FMT SMR.1/LogServer Security roles.....	30
5.1.3.8. FMT SMF.1/LogServer Specification of Management Functions.....	30
5.1.3.9. FIA ATD.1/LogServer User attribute definition	30
5.1.3.10. FIA UAU.2/LogServer User authentication before any action.....	30
5.1.3.11. FIA UID.2/LogServer Timing of identification.....	30
5.1.3.12. FDP ETC.2/LogServer Export of user data with security attributes	31

5.1.3.13. FDP ITC.2/LogServer Import of user data with security attributes	31
5.1.3.14. FPT TDC.1/LogServer Inter-TSF basic TSF data consistency.....	31
5.1.3.15. FTP ITC.1/LogServer-JMS Inter-TSF trusted channel.....	31
5.1.3.16. FTP ITC.1/Console Inter-TSF trusted channel.....	32
5.1.3.17. FDP ITC.1/LogServer Import of user data without security attributes.....	32
5.1.3.18. FDP ETC.1/LogServer Export of user data without security attributes.....	32
5.1.3.19. FAU SAR.2 Restricted audit review	32
5.1.3.20. FAU SAR.1 Audit review	32
5.1.3.21. FDP IFC.1/LogServer Subset information flow control	33
5.1.3.22. FDP IFF.1/LogServer Simple security attributes	33
5.2. TOE Security assurance requirements.....	34
5.3. Strength of Function claimed for the TOE SFRs.....	35
5.4. Security Requirements for IT Environment.....	35
5.4.1.1. FIA ATD.1/OS User attribute definition	35
5.4.1.2. FIA ATD.1/DB User attribute definition	35
5.4.1.3. FIA UAU.2/ENV User authentication before any action.....	35
5.4.1.4. FIA UID.2/ENV User identification before any action.....	35
5.4.1.5. FIA USB.1 User-subject binding.....	35
5.4.1.6. FMT SMR.1/OS Security roles	36
5.4.1.7. FMT SMR.1/DBA Security roles	36
5.4.1.8. FMT MOF.1/OS Management of security functions behaviour.....	36
5.4.1.9. FMT SMF.1/OS Specification of Management Functions.....	36
5.4.1.10. FDP SDI.1 Stored data integrity monitoring.....	36
6. TOE summary specification.....	37
6.1. TOE Security Functions.....	37
6.1.1. TSFs Description.....	37
6.1.2. Trazabilidad TSF Vs. SFRs.....	38
6.1.2.1. Tabla de Trazabilidad con la Iteración LogHost y LogHostManager.....	38
6.1.2.2. Tabla de Trazabilidad con la Iteración LogAgent y LogAgentManager.....	38
6.1.2.3. Tabla de Trazabilidad con la Iteración LogServer.....	39
6.1.3. Justificación TSFs Vs. SFRs.....	40
6.1.3.1. Justificación para la Iteración LOGHOST.....	40
6.1.3.2. LOGAGENT.....	42
6.1.3.3. LOGSERVER.....	44
6.2. Assurance Measures.....	46
7. PP Claims.....	49
8. Rationale.....	50
8.1. Security Objectives Rationale.....	50
8.2. Security Assurance Rationale.....	50
8.3. TOE Summary Specification Rationale.....	50
8.3.1. Mapeo Objetivos de Seguridad del TOE Requisitos Funcionales de Seguridad.....	50
8.3.1.1. LOGHOST y LOGHOSTMANAGER.....	50
8.3.1.2. LOGAGENT y LOGAGENTMANAGER.....	51
8.3.1.3. LOGSERVER.....	52
8.3.2. Selección de Requisitos Funcionales de Seguridad para el TOE.....	52
8.3.2.1. LOGHOST.....	53

8.3.2.2. LOGAGENT.....	53
8.3.2.3. LOGSERVER.....	54
8.3.3. Objetivos de Seguridad del Entorno IT Vs. Requisitos Funcionales de Seguridad.....	56
8.3.4. Selección de Requisitos Funcionales de Seguridad del entorno IT.....	56
8.3.5. Análisis de satisfacción de dependencias funcionales.....	58
8.3.5.1. Satisfacción de dependencias para la iteración LOGHOST y LOGHOSTMANGER.....	58
8.3.5.2. Satisfacción de dependencias para la iteración LOGAGENT y LOGAGENTMANAGER.....	59
8.3.5.3. Satisfacción de dependencias para la iteración LOGSERVER.....	59
8.4. PP Claims Rationale.....	60

1.ST Introduction

1.1. ST Reference & Identification

El presente documento presenta *la Herramienta de Gestión de Eventos LogICA v2.1. Security Target v1.16*

1.1.1.ST Identification

Herramienta de Gestión de Eventos LogICA v2.1 Security Target v1.16

1.1.2.TOE identification

Herramienta de Gestión de Eventos LogICA v2.1 SP6, compuesta de:

- EventCollector^(*), versión 2.0 – Colector de eventos.
- EventCorrelation^(*), versión 2.0 – Correlacionador de eventos
- LogAgent versión, 2.0– Captura y correlación de Logs originales.
- LogHost, versión 1.2 – Módulo de almacenamiento de Logs originales.
- Console, versión 1.1 – Consola de monitorización en tiempo real.
- LogAgentManager versión 1.0 – Módulo de Administración del LogAgent.
- LogHostManager versión 1.1 – Módulo de Administración del LogHost.

^(*) La agrupación de EventCollector y EventCorrelation es conocida como Logserver, al que también se versiona como Logserver versión 2.0

1.1.3.TOE Version Number

Versión 2.1 - SP6

1.1.4.ST Date

15 – Abril - 2009

1.1.5.ST Author

ICA

1.1.6.Assurance Level

EAL2

1.1.7.Strength of function

SOF Basic.

1.2. ST Overview

La presente Declaración de Seguridad (Security Target ST) describe los objetivos y requisitos de seguridad, así como el razonamiento (rationale) de los mismos, aplicados a la Herramienta de Gestión de Eventos LogICA v2.1 SP6. Todo lo expuesto dentro del presente documento está de acuerdo a la *Common Criteria for Information Technology Security Evaluation, versión 2.3*.

LogICA v2.1 SP6 es una herramienta de adquisición de Logs centralizada, con ella es posible obtener registros de eventos ocurridos en máquinas distribuidas, es decir, accede, prepara y centraliza los Logs de diferentes dispositivos.

Por otra parte LogICA v2.1 SP6 aplica reglas de correlación sobre los eventos generados, permitiendo así generar eventos de 2º nivel o incidentes, que aportarán información acerca de las acciones realizadas por los usuarios legítimos e ilegítimos.

1.3. CC Conformance

El TOE da conformidad a:

- Common Criteria Versión 2.3 Parte 1
- Common Criteria Versión 2.3 Parte 2
- Common Criteria Versión 2.3 Parte 3

La presente Declaración de Seguridad ha sido implementada utilizando Common Criteria (CC) Version 2.3 (ISO/IEC 15408 Evaluation Criteria for Information Technology security; Part 1: Introduction and general model, Part 2: Security functional requirements, and Part 3: Security assurance requirements).

El nivel de garantía para esta ST es EAL2.

2. TOE description

2.1. Introduction

El TOE es una herramienta software concebida como una plataforma de gestión de la seguridad lógica de la red sobre la que se implante.

La gestión de la seguridad citada, está enfocada principalmente en cuatro aspectos:

- Gestión centralizada de los logs generados por los sistemas.
- Realización de auditorías forenses.
- Gestión de la seguridad en tiempo real a través de consolas de seguridad.
- Consultas al sistema Gestor de BD que consolida la información en Tiempo Real.

La herramienta se ha concebido para transformar la información en bruto que reside en los logs generados por los sistemas de información, en datos procesados y útiles para la toma de decisiones en materia de seguridad.

2.2. Objetivos del TOE

- a) Establecer los mecanismos y capacidades de captura de datos de auditoría ("logs") en formato nativo y su almacenamiento centralizado con protección de integridad, para su consulta con fines principalmente **FORENSES**.
- b) Disponer de los mecanismos necesarios para la identificación en **TIEMPO REAL** de eventos y alertas de seguridad de manera distribuida mediante agentes.

Transmisión y almacenamiento consolidado de estos eventos y alertas, y de las herramientas que faciliten la monitorización de alertas.

- c) Tratamiento y respuesta ante incidentes, y la obtención de informes tanto operativos como ejecutivos.
- d) Poder realizar un seguimiento de la actividad de los usuarios, de los recursos de la instalación, la detección de actividades sospechosas con miras a la detección de anomalías y facilitar la investigación de estas anomalías (seguimiento de eventos de seguridad).

2.3. Componentes del TOE

2.3.1. Componentes

LogAgent

- Recoge los logs de los diferentes sistemas y filtra los relacionados con la seguridad.
- Aporta un primer nivel de filtrado sobre un mismo tipo de fuente de logs.

LogServer

- Event Collector recoge los logs previamente filtrados por LogAgent y genera eventos de primer nivel mediante reglas de correlación.
- Event Correlator recoge los eventos generados por EventCollector y genera eventos de segundo nivel o **incidencias** mediante reglas de correlación.

Console

- Permite la monitorización de eventos y módulos en tiempo real.

LogHost

- Recoge y recibe los logs de cualquier fuente.
- Almacena los logs recibidos en una base de datos.

LogAgentManager

- Gestionar y configura los agentes remotamente.

LogHostManager

- Configurar LogHost remotamente
- Permite generar nuevas reglas del filtrado.
- Muestra información y estadísticas sobre los logs recogidos.

2.4. Entorno IT

Sistema Operativo:

- Linux Red Hat Enterprise (4 o superior) o
- Suse (9 o superior) o
- Debian (kernel 2.4 o superior) o
- Sun Solaris (9 o superior)

Servidor de aplicaciones:

- Apache Tomcat 5.2.25 o superior.

Sistemas Gestores de Base de Datos :

- Oracle (8, 9 , 10)
- SQL Server (2007 o superior)

- MySQL 4.x o superior

JMS Broker BUS

- ActiveMQ v1.1
- OpenJMS v0.7
- JRE 1.5 o superior. El agente puede ejecutarse en cualquier entorno que soporte un entorno de ejecución de máquina virtual Sun Microsystems Java versión 1,5 o superior. El SSL com.sun.net.ssl.*

2.5. Descripción de la Arquitectura

En este apartado se analizará la arquitectura a alto nivel del modelo que representa el sistema LogICA v2.1.

2.5.1. Arquitectura Alto Nivel

El TOE posee una arquitectura modular (en su estructura lógica) cuyos componentes son los siguientes:

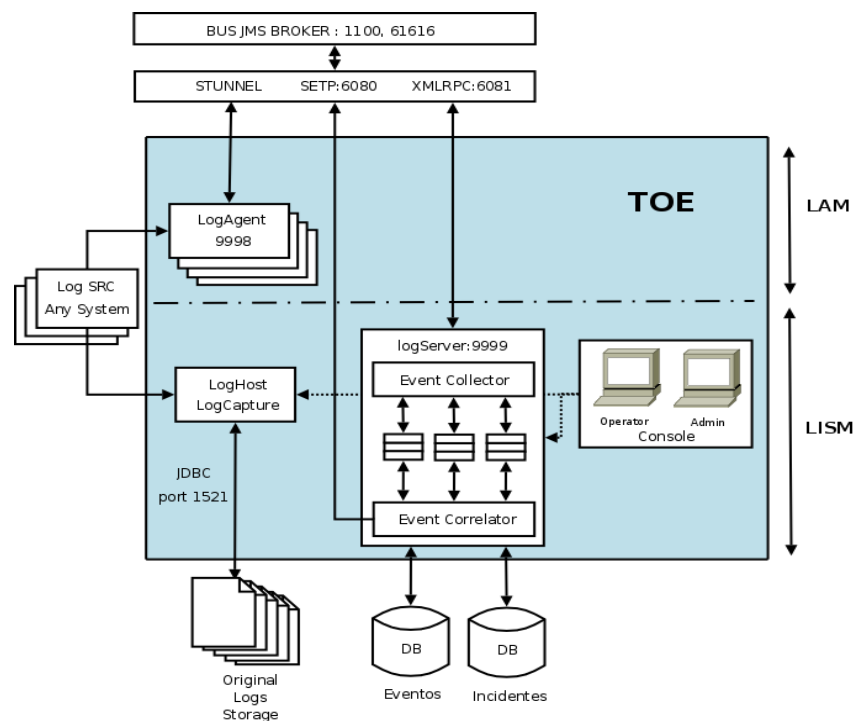


Imagen 1: Arquitectura modular de LogICA

2.5.2.Estructura Física del TOE

LogICA necesita como mínimo un PC para ser ejecutado íntegramente, aunque debido a que la estructura física que implementa LogICA v2.1 es totalmente modular, el sistema puede ser ejecutado de modo distribuido. Con ello se consigue separar las diferentes partes, gestión, monitorización y adquisición de logs.

2.6. Summary of Security Features

Existen varias características de seguridad que la aplicación dispone para asegurar los activos que gestiona. Las citadas características son las siguientes:

2.6.1.Auditoría de accesos, registro de accesos

Todo acceso a la consola de gestión del TOE, generará un evento de seguridad con una serie de datos, disponibles para su monitorización y tratamiento para detectar posibles intrusiones o intentos de intrusión.

2.6.2.Identificación y autenticación

Existirán unas cuentas de usuario (operador) para poder acceder a los recursos del TOE. Estas cuentas estarán asociadas de manera unívoca a aquellos usuarios que realizan operaciones propias del TOE. La autenticación de los citados usuarios estará basada en la utilización de una contraseña asociada a cada cuenta de usuario. **Esta contraseña no deberá ser compartida ni revelada** y es almacenada en el sistema de forma cifrada.

2.6.3.Segregación de funciones mediante mapa de roles de usuario

Para implementar la política P.USERLEVEL se posibilitará el acceso segregado a los recursos del TOE mediante roles de usuario. Esto quiere decir que existirán roles diferentes que realizarán acciones diferentes sobre los activos del TOE, procurando que cada usuario acceda únicamente a aquellos recursos que le sean necesarios para el desempeño de su trabajo.

2.6.4.Integridad de logs originales

Para garantizar que los logs originales recogidos por el sistema forense son íntegros y que toda modificación sobre ellos pueda ser detectada, se añadirá un registro para verificar la integridad de los Logs originales almacenados. Este registro consiste en un fichero asociado .sig con el mismo nombre que el original y que contiene un certificado autofirmado con algoritmo de firma **SHA1 with RSA**.

2.6.5.Canales de comunicación cifrados con protocolos seguros

La securización de las comunicaciones contra la consola de gestión del TOE, se realizará mediante la implantación de protocolos seguros SSL/TLS. De esta manera, la información de gestión que se intercambie en las conexiones realizadas mediante protocolo HTTPS, quedará ininteligible para aquel que quiera capturar el tráfico. El transporte de eventos

desde agente, permite la configuración del protocolo SETP (SETPS) sobre la capa de SSL/TLS. SETP es un protocolo de serialización HTTP utilizado para el intercambio de eventos entre LogAgent y LogServer.

3.TOE security environment

La presente sección describe los aspectos de seguridad del entorno en el cual el TOE ha de ser utilizado así como el método de utilización esperado. Esta declaración se aborda a través de los siguientes puntos:

3.1. Assumptions

En este apartado se incluye información acerca de las **hipótesis de entorno** sobre el que funciona el TOE:

3.1.1.Operational assumptions

A.IDENTIFICATION_&_AUTHENTICATION

Se asume que el entorno IT ha de ser capaz de identificar y autenticar a aquellos usuarios cuyo propósito final sea el de acceder al sistema que almacena el TOE, sus TSFs y las bases de datos de almacenamientos.

A.DBINTEGRITY

Se asume que el Sistema Gestor de Bases de Datos mantendrá la integridad de los datos almacenados.

A.INSTALLATION

Se asume que el Sistema Operativo sobre el que se instala el TOE estará securizado.

A.TIME

Se asume que el Sistema Operativo sobre el que se instala el TOE proporciona una base de tiempo confiable.

3.1.2.Personnel assumptions

A.NO_EVIL_ADMIN

Se asume que los administradores debidamente autorizados serán confiables y no realizarán acciones maliciosas, además estarán debidamente formados para usar, configurar y mantener el TOE.

3.2. Threats to security

En este apartado se aporta información acerca de las amenazas a las cuales va estar expuesto el TOE.

Todas las amenazas hacen referencia a un atacante que puede ser, o no, un usuario autorizado del sistema.

Un atacante puede tener control del host sobre el que funciona el TOE cuando está en producción.

T.IDENTITY_SPOOFING

Un atacante puede realizar operaciones con los TSF's con identidad falsa sin ser detectado por medio de la suplantación de identidad de otro usuario.

T.FORENSIC_EVENT_MODIFIED

Un atacante puede hacer modificaciones no detectadas en los raw logs gestionados por el TOE.

T.UNAUTHORIZED_ACCESS

Un atacante puede acceder, administrar o operar activos del TOE sin estar autorizado a ello y sin ser detectado.

T.SNIFFING

Un atacante puede capturar datos que circulan por el interior del TOE o que se transmiten entre diferentes partes del TOE.

3.3. Organisational security policies (OSPs)

P.LOGACCESS

El TOE deberá importar los logs originales como datos de entrada de la base de datos raw logs. Estos logs estarán firmados mediante RSA y almacenados en una base de datos externa.

P.USERLEVEL

Es necesaria la implantación de una serie de roles de usuario para segregar el acceso a los recursos gestionados por el TOE. Estos roles de usuario estarán de acuerdo al estándar de mínimo privilegio mediante el cual, cada usuario accederá a los recursos que le son precisos para realizar su trabajo.

4. Security objectives

Los objetivos de seguridad están especificados para las siguientes dos categorías:

4.1. Security Objectives for the TOE

O.LOG

El TOE debe proporcionar auditoría de acceso, por medio de generación de logs de todos los accesos que se realizan en él, así como el resultado de los mismos.

O.ROLE

El TOE debe realizar control de acceso a recursos y objetos del propio TOE basándose en usuarios, contraseñas y roles que permitan segregar las funciones a las cuales tenga acceso cada usuario.

O.AUTHENTICITY

El TOE debe proporcionar integridad que aseguren que los logs originales gestionados no han sido modificados por ningún agente externo, mediante mecanismos de firma.

O.SECURECOM

El TOE debe proporcionar canales de comunicación seguros por medio del uso de protocolos basados en SSL/TLS.

O.INDATA

El TOE debe ser capaz de importar los logs y evento desde las fuentes de logs externas e internas utilizadas por LogICA y exportarlos a las unidades de almacenamiento.

4.2. Security Objectives for the Environment

O.E.OSAUTH

El entorno IT requerirá que los usuarios del TOE estén identificados y autenticados antes de permitirles realizar cualquier actividad relacionada con los TSF.

O.E.DBAUTH

El acceso directo a los eventos almacenados en la base de datos sobre la que esté montado el TOE, requerirá de la autenticación previa contra el Sistema Gestor de Base de Datos.

O.E.ADMIN_TRUST

Los administradores del TOE deben ser competentes para el trabajo a desarrollar, confiables y cumplir lo expuesto en las guías de administración.

O.E.BAST

El entorno IT sobre el que se instale el TOE estará suficientemente bastionado de manera que no ofrezca fallos triviales en la su seguridad.

O.E.TIME

El entorno IT sobre el que se instale el TOE debe proporcionar una base de tiempo confiable.

O.E.DBINT

El Sistema Gestor de Base de Datos proporcionará mecanismos que garanticen la integridad de los logs y eventos que almacena.

4.2.1. Correspondencia entre Objetivos de Seguridad, Amenazas y Políticas Organizativas.

	O.LOG	O.ROLE	O.AUTHENTICITY	O.SECURECOM	O.INDATA		
T.IDENTITY_SPOOFING	✓	✓	✗	✗	✗	✓	Matching
T.FORENSIC_EVENT_MODIFIED	✗	✗	✓	✗	✗	✗	No Matching
T.UNAUTHORIZED_ACCESS	✓	✓	✗	✗	✗		
T.SNIFFING	✗	✗	✗	✓	✗		
P.LOGACCESS	✗	✗	✗	✗	✓		
P.USERLEVEL	✗	✓	✗	✗	✗		

Tabla 1 - Mapeo Objetivos de Seguridad, Amenazas y Políticas Organizativas.

T.IDENTITY_SPOOFING

Es necesario modelar un objetivo de seguridad que implemente una adecuada segregación de funciones dentro del TOE mediante la utilización de roles de usuarios O.ROLE y el almacenamiento de todos los accesos al TOE mediante O.LOG.

T.FORENSIC_EVENT_MODIFIED

Es necesario que los eventos de correlación almacenados dentro del TOE permanezcan íntegros. Ante una modificación que pudieran sufrir éstos, sea posible detectarlo, para ello, se implanta un sistema que permite garantizar la integridad de los logs originales, evitando su modificación por algún agente externo O.AUTHENTICITY.

T.UNAUTHORIZED_ACCESS

Todos los accesos al TOE han de estar autorizados, por ello, es necesario que un objetivo de seguridad sea que todos los accesos al sistema sean autorizados por un mecanismo de seguridad O.ROLE y que se establezca un registro de los accesos O.LOG.

T.SNIFFING

Todas las comunicaciones entre diferentes partes del TOE y agentes externos deben realizarse mediante la utilización de canales seguros, es por ello que se establece O.SECURECOM.

P.LOGACCESS

Es necesario que el sistema importe los logs originales como datos de entrada, para ello se establece que el TOE realice importaciones periódicas de los logs mediante O.INDATA.

P.USERLEVEL

El TOE debe implementar una adecuada función de roles para cada usuario, para ello se ha definido el objetivo de seguridad O.ROLE.

4.2.2. Correspondencia entre Objetivos de Seguridad del entorno e hipótesis de entorno.

	O.E.OSAUTH	O.E.DBAUTH	O.E.BAST	O.E.TIME	O.E.DBINTE	O.E.ADMIN_TRUST		
A.IDENTIFICATION_ & AUTHENTICATION	✓	✓	✗	✗	✗	✗	✓	Matching
A.NO_EVIL_ADMIN	✗	✗	✗	✗	✗	✓	✗	No Matching
A.DB_INTEGRITY	✗	✗	✗	✗	✓	✗		
A.INSTALLATION	✗	✗	✓	✗	✗	✗		
A.TIME	✗	✗	✗	✓	✗	✗		

Tabla 2 - Correspondencia entre Objetivos de Seguridad del Entorno y hipótesis de entorno.

A.IDENTIFICATION_ & AUTHENTICATION

Dado que partes del TOE se encuentran accesibles desde el Sistema Operativo y desde la base de datos, es necesario que se establezca como objetivo que el acceso a ambos se realice mediante identificación y autenticación de los usuarios que pretendan acceder a ellos O.E.DBAUTH y O.E.OSAUTH.

A.NO_EVIL_ADMIN

El personal que gestione tanto el TOE como el entorno, han de hacerlo de manera que no se haga un abuso de los mismos, para ello, es un objetivo del entorno que el administrador sea de confianza, competente y no actúe de forma maliciosa. Para ello se establece el objetivo de seguridad del entorno O.E.ADMIN TRUST.

A.DBINTEGRITY

Se asume que el Sistema Gestor de Base de Datos utilizado será totalmente seguro y no esta expuesto a problemas de modificación de registro. Con ello se cubre el objetivo O.E.INTE.

A.INSTALLATION

Todos los entornos que soporten las funcionalidades del TOE han de tener la capacidad de establecer una configuración segura, quedando en un estado bastionado, O.E.BAST.

A.TIME

Todos los entornos que soporten las funcionalidades del TOE han de tener la capacidad de proporcionar una base de tiempo confiable, cubriendo el objetivo O.E.TIME.

5. IT Security Requirements

Se detallan en este apartado todos los requisitos funcionales de seguridad (SFR) y políticas que modelan tanto el TOE como el entorno sobre el que está implantado.

5.1. TOE Security Functional Requirements (SFRs)

Dentro de la presente sección, se ponen de manifiesto los requisitos funcionales de seguridad que el TOE posee para hacer frente a las potenciales amenazas a las que se ve expuesto, así como para dar cumplimiento a las políticas de seguridad organizativas descritas en el apartado 4 de la Declaración de Seguridad. Estos requisitos han sido extraídos de la parte 2 de CC2V3.

5.1.1. LOGHOST y LOGHOSTMANAGER

5.1.1.1. FAU_GEN.1/LogHost Audit data generation

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 **[basic]** level of audit; and
- c) **[User Login]**

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, **[None]**.

5.1.1.2. FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.1.1.3. FDP_ACC.1/LogHost Subset access control

FDP_ACC.1.1 The TSF shall enforce the **[LISM access control SFP]** on **[users and all user data managed and kept inside these modules]**.

5.1.1.4. FDP_ACF.1/LogHost Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **[LISM access control SFP]** to objects based on the following: **[login process into logICA modules managed by LISM Control Access Module, through web browser]**.

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

- **If password hashed equals password stored in password file, then the LISM policy depending on user's role determine if access to both modules is allowed.**

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *[N/A]*.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the *[N/A]*.

5.1.1.5.FMT MSA.3/LogHost Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the *[LISM access control SFP]* to provide *[permissive]* default values for security attributes that are used to enforce the SFP.

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

5.1.1.6.FMT MSA.1/LogHost Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the *[LISM access control SFP]* to *[restrict]* the ability to *[change default, query, modify and delete]* the security attributes *[password and role]* to *[administrator]*.

5.1.1.7.FMT SMR.1/LogHost Security roles

FMT_SMR.1.1 The TSF shall maintain the roles of *[administrator]*.

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

5.1.1.8.FMT SMF.1/LogHost Specification of Management Functions

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

5.1.1.9.FDP ITC.1/LogHost Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the *[Information Flow Policy]* when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: *[N/A]*

5.1.1.10.FDP_ETC.2/LogDB Export of user data with security attributes

FDP_ETC.2.1 The TSF shall enforce the **[Information Flow Policy]** when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TSC: **[N/A]**

5.1.1.11.FDP_ITC.2/LogDB Import of user data with security attributes

FDP_ITC.2.1 The TSF shall enforce the **[Information Flow Policy]** when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **[N/A]**

5.1.1.12.FTP_ITC.1/LogDB Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit **[to communicate LogHost and Raw logs DB]**

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **[store and recover original logs from the raw logs DB]**

5.1.1.13.FIA ATD.1/LogHost User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- **Password.**
- **Role.**

5.1.1.14.FIA UAU.2/LogHost User authentication before any action

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.

5.1.1.15.FIA UID.2/LogHost Timing of identification

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.1.16.FDP DAU.1 Basic Data Authentication

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of the **[original log events from monitored systems stored on the data base.]**

FDP_DAU.1.2 The TSF shall provide **[administrator]** with the ability to verify evidence of the validity of the indicated information.

5.1.1.17.FTP ITC.1/LogHostManager Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit **[the LogHostManager to initiate communication via the trusted channel.]**

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **[Administration from LogHostManager to LogHost under SSL protocol.]**

5.1.1.18.FPT TDC.1/LogHost Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret **[RSA signatures using SHA-1 hash function]** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use **[SHA-1withRSA]** when interpreting the TSF data from another trusted IT product.

5.1.1.19.FDP IFC.1/LogHost Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the **[information flow policy]** on **[loghost sobre la información logs, en la operación captura de logs]**.

5.1.1.20.FDP IFF.1/LogHost Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the **[information flow policy]** based on the following types of subject and information security attributes: **[loghost and logs controlled under the indicated SFP, and for each, log properties]**

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[captura de logs sin atributos de seguridad y exportación de logs con atributos de seguridad, Sha1 con RSA.]**.

FDP_IFF.1.3 The TSF shall enforce the **[N/A]**.

FDP_IFF.1.4 The TSF shall provide the following **[N/A]**.

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: **[N/A]**.

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: **[N/A]**.

5.1.2.LOGAGENT y LOGAGENTMANAGER

5.1.2.1.FAU GEN.1/LogAgent Audit data generation

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 **[basic]** level of audit; and
- c) **[User Login]**

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, **[None]**.

5.1.2.2.FDP ACC.1/LogAgent Subset access control

FDP_ACC.1.1 The TSF shall enforce the **[LAM Access Control Policy]** on **[users and all user data managed and kept inside these modules]**.

5.1.2.3.FDP ACF.1/LogAgent Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **[LAM Access Control Policy]** to objects based on the following: **[Login process to get access to LogAgentManager through web browser based in role and password authentication]**

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

- **If password hashed equals password stored in password file, access to both modules is allowed.**

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[N/A]**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the: **[N/A]**

5.1.2.4.FMT MSA.3/LogAgent Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the **[LAM access control SFP and information flow policy]** to provide **[password, role and log properties]** default values for security attributes that are used to enforce the SFP.

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

5.1.2.5.FMT MSA.1/LogAgent Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **[LAM access control SFP]** to **[restrict]** the ability to **[change default, query, modify and delete]** the security attributes **[password, role and capture information rules]** to **[the Administrator]**.

5.1.2.6.FMT SMR.1/LogAgent Security roles

FMT_SMR.1.1 The TSF shall maintain the roles **[of administrator and operator]**.

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

5.1.2.7.FMT SMF.1/LogAgent Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: **[management of LAM security attributes]**.

5.1.2.8.FDP ITC.1/LogAgent Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the **[Information Flow Policy]** when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **[N/A]**

5.1.2.9.FDP ETC.2/LogAgent Export of user data with security attributes

FDP_ETC.2.1 The TSF shall enforce the **[Information Flow Policy]** when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TSC: **[none]**.

5.1.2.10.FDP ITC.2/LogAgent Import of user data with security attributes

FDP_ITC.2.1 The TSF shall enforce the **[Information Flow Policy]** when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **[none]**.

5.1.2.11.FPT TDC.1/LogAgent Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret **[SETP data]** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use **[SETP]** when interpreting the TSF data from another trusted IT product.

5.1.2.12.FTP ITC.1/LogAgent-JMS Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit the **[LogAgent]** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for:**[Get and send Logica events between LogAgent and JMS bus under SETP protocol.]**

5.1.2.13.FTP ITC.1/LogAgentManager Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit **[LogAgentManager]** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **[Administration/Visualization from LogAgentManager to LogAgent under SSL protocol.]**

5.1.2.14.FIA ATD.1/LogAgent User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- **Password.**
- **Role.**

5.1.2.15.FIA UAU.2/LogAgent User authentication before any action

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.

5.1.2.16.FIA UID.2/LogAgent Timing of identification

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.2.17.FDP IFC.1/LogAgent Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the **[information flow policy]** on **[logagent, logs and the logs capture]**.

5.1.2.18. FDP IFF.1/LogAgent Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the **[information flow policy]** based on the following types of subject and information security attributes: **[logagent and logs controlled under the indicated SFP, and for each, log properties]**.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[captura de logs basado en los atributos de seguridad log properties "Facility, Level, Host, Mask y Program"]**.

FDP_IFF.1.3 The TSF shall enforce the **[N/A]**.

FDP_IFF.1.4 The TSF shall provide the following **[N/A]**.

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: **[N/A]**.

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: **[N/A]**.

5.1.3.LOGSERVER

5.1.3.1.FAU GEN.1/LogServer Audit data generation

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 **[basic]** level of audit; and
- c) **[User Login]**

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, **[None]**.

5.1.3.2.FDP ACC.1/LogServer Subset access control

FDP_ACC.1.1 The TSF shall enforce the **[LAM Access Control Policy]** on **[users and all user data managed and kept inside these modules]**.

5.1.3.3.FDP ACF.1/LogServer Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **[LAM Access Control Policy]** to objects based on the following: **[login process into logICA modules managed by LISM Control Access Module, through web browser]**.

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

- **If password hashed equals password stored in password file, then the LISM policy depending on user's role determine if access to both modules is allowed.**

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[N/A]**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the **[N/A]**.

5.1.3.4.FMT MSA.3/LogServer Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the **[LISM access control SFP , information flow policy]** to provide **[password, role and standard event properties]** default values for security attributes that are used to enforce the SFP.

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

5.1.3.5.FMT MSA.1/LogServer Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **[LISM access control SFP]** to **[restrict]** the ability to **[change default, query, modify and delete]** the security attributes **[standard event properties]** to **[the Administrator]**.

FDP_IFC.1.1 The TSF shall enforce the **[information flow policy]** on **[logagent, logs and the logs capture]**.

5.1.3.6. FDP IFF.1/LogAgent Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the **[information flow policy]** based on the following types of subject and information security attributes: **[logagent and logs controlled under the indicated SFP, and for each, log properties]**.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[captura de logs basado en los atributos de seguridad log properties “Facility, Level, Host, Mask y Program”]**.

FDP_IFF.1.3 The TSF shall enforce the **[N/A]**.

FDP_IFF.1.4 The TSF shall provide the following **[N/A]**.

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: **[N/A]**.

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [N/A].

5.1.3.7.FMT_SMR.1/LogServer Security roles

FMT_SMR.1.1 The TSF shall maintain the roles of **[administrator and operator]**.

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

5.1.3.8.FMT_SMF.1/LogServer Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: **[management of LISM security attributes]**.

5.1.3.9.FIA_ATD.1/LogServer User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- **Password.**
- **Role.**

5.1.3.10.FIA_UAU.2/LogServer User authentication before any action

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.

5.1.3.11.FIA_UID.2/LogServer Timing of identification

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.3.12.FDP ETC.2/LogServer Export of user data with security attributes

FDP_ETC.2.1 The TSF shall enforce the **[Information Flow Policy]** when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TSC: **[N/A]**.

5.1.3.13.FDP ITC.2/LogServer Import of user data with security attributes

FDP_ITC.2.1 The TSF shall enforce the **[Information Flow Policy]** when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **[none]**.

5.1.3.14.FPT TDC.1/LogServer Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret **[SETP data]** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use **[SETP]** when interpreting the TSF data from another trusted IT product.

5.1.3.15.FTP ITC.1/LogServer-JMS Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit **[LogServer]** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for ***[send and receive Logica events between LogServer to JMS bus under SETP protocol.]***

5.1.3.16.FTP ITC.1/Console Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit ***[Console]*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for: ***[Administration/Visualization from Console to LogServer under SSL protocol.]***

5.1.3.17.FDP ITC.1/LogServer Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the ***[Information Flow Policy]*** when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: ***[Logica event and incident properties]***

5.1.3.18.FDP ETC.1/LogServer Export of user data without security attributes

FDP_ETC.1.1 The TSF shall enforce the ***[Information Flow Policy]*** when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes

5.1.3.19.FAU SAR.2 Restricted audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.1.3.20.FAU SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide ***[administrator]*** with the capability to read ***[all audit information]*** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.3.21.FDP IFC.1/LogServer Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the ***[information flow policy]*** on ***[logserver, eventos e importación de eventos correlados]***.

5.1.3.22. FDP IFF.1/LogServer Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the ***[information flow policy]*** based on the following types of subject and information security attributes: ***[logserver and eventos controlled under the indicated SFP, and for each, standard event properties]***.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: ***[captura de eventos basado en los atributos de seguridad standard event properties]***.

FDP_IFF.1.3 The TSF shall enforce the ***[N/A]***.

FDP_IFF.1.4 The TSF shall provide the following ***[N/A]***.

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: ***[N/A]***.

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: ***[N/A]***.

5.2. TOE Security assurance requirements

Los requisitos de garantía de seguridad descritos en la presente sección de la Declaración de Seguridad, se ajustan al **Paquete de requisitos de Garantía EAL2** especificado en la *Parte 3 de la norma Common Criteria versión 2.3*.

Se ha elegido este conjunto de requisitos de garantía porque supone un primer paso, necesario para evolucionar a niveles de certificación superiores y que permite conocer el impacto sobre la empresa y el producto.

En la siguiente tabla están incluidos los requisitos de garantía de seguridad citados:

CLASE	COMPONENTE	NOMBRE DEL COMPONENTE	DEPENDENCIAS
Configuration Management	ACM_CAP.2	Configuration Items	No dependencies
Delivery and Operation	ADO_DEL.1	Delivery Procedures	No dependencies
Delivery and Operation	ADO_IGS.1	Installation, Generation, and Start-Up Procedures	AGD_ADM.1
Development	ADV_FSP.1	Informal Functional Specification	ADV_RCR.1
Development	ADV_HLD.1	Descriptive High-Level Design	ADV_FSP.1, ADV_RCR.1
Development	ADV_RCR.1	Informal Correspondence Demonstration	No dependencies
Guidance Documents	AGD_ADM.1	Administrator Guidance	ADV_FSP.1
Guidance Documents	AGD_USR.1	User Guidance	ADV_FSP.1
Tests	ATE_COV.1	Evidence of Coverage	ADV_FSP.1, ATE_FUN.1
Tests	ATE_FUN.1	Functional Testing	No dependencies
Tests	ATE_IND.2	Independent Testing – Sample	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
Vulnerability Assessment	AVA_SOF.1	Strength of TOE Security Function Evaluation	ADV_FSP.1, ADV_HLD.1
Vulnerability Assessment	AVA_VLA.1	Developer Vulnerability Analysis	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1

Tabla 3 - Security Assurance Requirements for EAL2

Las evidencias documentales dan soporte al cumplimiento del Paquete de requisitos de garantía de seguridad EAL2, están incluidos en los procedimientos operativos, documentación de la aplicación y documentos de desarrollo de software.

5.3. Strength of Function claimed for the TOE SFRs

La Fortaleza de las Funciones de Seguridad reclamadas para el TOE es **básica**, debido a que la naturaleza de los potenciales atacantes a los que el TOE ha de hacer frente, es de carácter **básico**.

5.4. Security Requirements for IT Environment

Dentro de la presente sección, se ponen de manifiesto los requisitos funcionales de seguridad que el entorno del TOE ha de tener implantados para ajustarse a las suposiciones de entorno definidas en la sección 3 del presente documento, así como para aportar funcionalidades de seguridad que el TOE no puede ofrecer.

5.4.1.1.FIA_ATD.1/OS User attribute definition

FIA_ATD.1.1 *[The Operating system]* shall maintain the following list of security attributes belonging to individual users:

- **Password.**
- **Role.**

5.4.1.2.FIA_ATD.1/DB User attribute definition

FIA_ATD.1.1 The *[Database Management System]* shall maintain the following list of security attributes belonging to individual users:

- **Password.**
- **Role.**

5.4.1.3.FIA_UAU.2/ENV User authentication before any action

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

5.4.1.4.FIA_UID.2/ENV User identification before any action

FIA_UID.2.1 The *[IT Environment]* shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.4.1.5.FIA_USB.1 User-subject binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

- **Validation of Password.**

- **Validation of Role**

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

[Create and associate an initial password and user role during TOE installation.]

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: ***[Administrator can change user role and password through TOE facilities.]***

5.4.1.6.FMT SMR.1/OS Security roles

FMT_SMR.1.1 The ***[Operating System]*** shall maintain the role:

- ***Administrator.***
- ***LogICA***

FMT_SMR.1.2 The ***[Operating System]*** shall be able to associate users with roles.

5.4.1.7.FMT SMR.1/DBA Security roles

FMT_SMR.1.1 The ***[Database Management System]*** shall maintain the role:

- ***logicaDBA.***

FMT_SMR.1.2 The ***[Database Management System]*** shall be able to associate users with roles.

5.4.1.8.FMT MOF.1/OS Management of security functions behaviour

FMT_MOF.1.1 The ***[Operating System]*** management functions enable authorized users to set up and control the secure operation of the TOE environment.

5.4.1.9.FMT SMF.1/OS Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: ***[management of security attributes of the OS, validation of users and passwords]***.

5.4.1.10.FDP SDI.1 Stored data integrity monitoring

FDP_SDI.1.1 The IT Environment shall monitor user data stored within the IT Environment Scope of ***[Control for all the integrity errors]*** that DBMS is able to detect on all objects, based on the following attributes: ***[Primary and Foreign Keys and Indexes.]***

6. TOE summary specification

6.1. TOE Security Functions

6.1.1. TSFs Description

TSF 1.- User Management – LISM/LAM Access

Esta funcionalidad aporta la capacidad al TOE de agregar, borrar y modificar usuarios y los atributos que caracterizan a un usuario, nombre de usuario y password. Con esta funcionalidad se generarán los usuarios que después tendrán la capacidad de acceder a las diferentes partes del TOE.

TSF 2.- Role Management – LISM/LAM Role

Role management aporta la capacidad al TOE de crear, borrar y modificar los roles, cada uno de los usuarios estará sujeto a un rol. Los roles otorgan privilegios entre los usuarios y las diferentes partes del TOE.

TSF 3.- Sign

Esta funcionalidad aporta la capacidad al TOE de generar datos que evidencien la integridad total de los logs originales adquiridos desde dispositivos externos una vez hayan sido capturados por el TOE. Por otra parte permite la posibilidad de acceder a ellos y comprobar la validez de los mismos.

TSF 4.- Access Audit

Access Audit capacita al TOE para que genere datos de acceso de los usuarios a las diferentes partes del mismo y el entorno que lo compone. Por otra lado esta funcionalidad nos permitirá importar logs de las fuentes de log y exportar los logs pretatados por los diferentes subsistemas.

TSF 5.- Trusted Channel

Esta funcionalidad de seguridad se encarga de asegurar los canales de comunicación entre módulos del TOE y componentes externos. Todos los accesos que se realicen al TOE deben realizarse mediante canales seguros.

6.1.2. Trazabilidad TSF Vs. SFRs

A continuación se presenta un mapeo y justificación de cobertura de los funciones de seguridad y los requisitos funcionales que caracterizan al TOE.

6.1.2.1. Tabla de Trazabilidad con la Iteración LogHost y LogHostManager

	User Management	Role Management	Sign	Access Audit	Trusted Channel
FAU_GEN.1/LogHost	X	X	X	✓	X
FPT_STM.1	X	X	✓	✓	X
FDP_ACC.1/LogHost	✓	✓	X	X	X
FDP_ACF.1/LogHost	✓	✓	X	X	X
FMT_MSA.3/LogHost	✓	✓	X	X	X
FMT_MSA.1/LogHost	✓	✓	X	X	X
FMT_SMR.1/LogHost	X	✓	X	X	X
FMT_SMF.1/LogHost	✓	✓	X	X	X
FDP_ITC.1/LogHost	X	X	X	X	✓
FDP_ETC.2/LogDB	X	X	X	X	✓
FDP_ITC.2/LogDB	X	X	X	X	✓
FTP_ITC.1/LogDB	X	X	X	X	✓
FIA_ATD.1/LogHost	✓	✓	X	X	X
FIA_UAU.2/LogHost	✓	✓	X	✓	X
FIA_UID.2/LogHost	✓	✓	X	✓	X
FDP_DAU.1	X	X	✓	X	X
FTP_ITC.1/LogHostManager	X	X	X	✓	✓
FPT_TDC.1/LogHost	X	X	✓	X	X
FDP_IFC.1/LogHost	X	X	X	✓	X
FDP_IFF.1/LogHost	X	X	X	✓	X

Tabla 4.-LogHost and LogHostManager TSFs Vs. SFRs

6.1.2.2. Tabla de Trazabilidad con la Iteración LogAgent y LogAgentManager

	User Management	Role Management	Access Audit	Trusted Channel
FAU_GEN.1/LogAgent	X	X	✓	X
FDP_ACC.1/LogAgent	✓	✓	X	X
FDP_ACF.1/LogAgent	✓	✓	X	X
FMT_MSA.3/LogAgent	✓	✓	X	X

	User Management	Role Management	Access Audit	Trusted Channel
FMT_MSA.1/LogAgent	✓	✓	✗	✗
FMT_SMR.1/LogAgent	✗	✓	✗	✗
FMT_SMF.1/LogAgent	✓	✓	✗	✗
FDP_ITC.1/LogAgent	✗	✗	✗	✓
FDP_ETC.2/LogAgent	✗	✗	✓	✓
FDP_ITC.2/LogAgent	✗	✗	✓	✓
FPT_TDC.1/LogAgent	✗	✗	✗	✓
FTP_ITC.1/LogAgent-JMS	✗	✗	✓	✓
FTP_ITC.1/LogAgentManager	✗	✗	✓	✓
FIA_ATD.1/LogAgent	✓	✓	✗	✗
FIA_UAU.2/LogAgent	✓	✓	✗	✗
FIA_UID.2/LogAgent	✓	✓	✗	✗
FDP_IFC.1/LogAgent	✗	✗	✓	✗
FDP_IFF.1/LogAgent	✗	✗	✓	✗

Tabla 5-LogAgent and LogAgentManager TSFs Vs. SFRs

6.1.2.3. Tabla de Trazabilidad con la Iteración LogServer

	User Management	Role Management	Access Audit	Trusted Channel
FAU_GEN.1/LogServer	✗	✗	✓	✗
FDP_ACC.1/LogServer	✓	✓	✗	✗
FDP_ACF.1/LogServer	✓	✓	✗	✗
FMT_MSA.3/LogServer	✓	✓	✗	✗
FMT_MSA.1/LogServer	✓	✓	✗	✗
FMT_SMR.1/LogServer	✗	✓	✗	✗
FMT_SMF.1/LogServer	✓	✓	✗	✗
FIA_ATD.1/LogServer	✓	✓	✗	✗
FIA_UAU.2/LogServer	✓	✓	✗	✗
FIA_UID.2/LogServer	✓	✓	✗	✗
FDP_ETC.2/LogServer	✗	✗	✓	✓
FDP_ITC.2/LogServer	✗	✗	✓	✓
FPT_TDC.1/LogServer	✗	✗	✗	✓

	User Management	Role Management	Access Audit	Trusted Channel
FDP_ITC.1/LogServer	X	X	X	✓
FTP_ITC.1/LogServer-JMS	X	X	X	✓
FTP_ITC.1/Console	X	X	✓	✓
FDP_ITC.1/LogServer	X	X	X	✓
FDP_ETC.1/LogServer	X	X	X	✓
FAU_SAR.2	X	X	✓	X
FAU_SAR.1	X	X	✓	X
FDP_IFC.1/LogServer	X	X	✓	X
FDP_IFF.1/LogServer	X	X	✓	X

Tabla 6-LogServer TSFs Vs. SFRs

6.1.3. Justificación TSFs Vs. SFRs

6.1.3.1. Justificación para la Iteración LOGHOST

TSF 1.- User Management

FDP_ACC.1/LogHost Subset access control, política LISM de acceso al TOE.

FDP_ACF.1/LogHost Security attribute based access control, cubierto por los atributos de seguridad que caracteriza a cada usuario.

FMT_MSA.3/LogHost Static Attribute Inicialization, cuando se instala el producto se definen diferentes atributos de seguridad por defecto, ejemp. User administrator.

FMT_MSA.1/LogHostLogHost Management of Security Attributes, el TOE proporciona capacidades de administración sobre los usuarios y sus atributos de seguridad.

FMT_SMF.1/LogHostLogHost Specification of Management Functions, el TOE proporciona capacidad de administración de los atributos de seguridad de cada usuario desde LogAgentManager

FIA_ATD.1/LogHost User attribute definition, cubierto por la capacidad que tiene el TOE de caracterizar los usuarios mediante: Password and Role.

FIA_UAU.2/LogHost User authentication before any action, para poder realizar acciones sobre el TOE el usuario debe estar autenticado.

FIA_UID.2/LogHost Timing of identification, para poder realizar acciones sobre el TOE el usuario debe de estar identificado.

TSF 2.- Role Management

FDP_ACC.1/LogHost Subset access control, política LISM de acceso al TOE.

FDP_ACF.1/LogHost Security attribute based access control, cubierto por los atributos de seguridad que caracteriza a cada usuario.

FMT_MSA.3/LogHost Static Attribute Inicialization, cuando se instala el producto se definen diferentes atributos de seguridad por defecto, ejemp. User administrator.

FMT_MSA.1/LogHostLogHost Management of Security Attributes, el TOE proporciona capacidades de administración sobre los usuarios y sus atributos de seguridad.

FMT_SMR.1/LogHost Security Roles, el TOE mantiene los roles de administrador y operador, dando la posibilidad al administrador de eliminar o agregar privilegios a cada usuario por separado.

FMT_SMF.1/LogHostLogHost Specification of Management Functions, el TOE proporciona capacidad de administración de los atributos de seguridad de cada usuario desde LogAgentManager

FIA_ATD.1/LogHost User attribute definition, cubierto por la capacidad que tiene el TOE de caracterizar los usuarios mediante: Password and Roles.

FIA_UAU.2/LogHost User authentication before any action, para poder realizar acciones sobre el TOE el usuario debe estar autenticado.

FIA_UID.2/LogHost Timing of identification, para poder realizar acciones sobre el TOE el usuario debe de estar identificado.

TSF 3.- Sign

FPT_TDC.1/LogHost Inter-TSF basic TSF data consistency, el TOE es capaz de realizar test de integridad de los logs originales.

FDP_DAU.1 Basic Data Authentication, el TOE es capaz de aportar evidencias de la integridad de los logs originales.

TSF 4.- Access Audit

FAU_GEN.1/LogHost Audit data generation, cubierto por la generación de datos de auditoría por LogHost.

FDP_ETC.2/LogDB Export of user data with security attributes, los logs originales almacenados en la base de datos van acompañados de una firma **SHA1 con RSA**.

FDP_ITC.2/LogDB Import of user data with security attributes, los logs originales de la base de datos de almacenamiento vienen acompañados de la firma **SHA1 con RSA**.

FDP_IFC.1/LogHost Information flow control, permite importar y exportar la información recogida por las fuentes de logs.

FDP_IFF.1/LogHost Simple Secure attributes, permite la posibilidad de configurar las reglas de adquisición de logs desde las fuentes de log.

TSF 5.- Trusted Channel

FDP_ETC.2/LogDB Export of user data with security attributes, los logs originales almacenados en la base de datos van acompañados de una firma **SHA1 con RSA**.

FDP_ITC.2/LogDB Import of user data with security attributes, los logs originales de la base de datos de almacenamiento vienen acompañados de la firma **SHA1 con RSA**.

FTP_ITC.1/LogDB Inter-TSF trusted channel, para acceder a la base de datos de almacenamiento de los log originales, LogHost utiliza un canal cifrado con **SSL**.

FTP_ITC.1/LoghostManager Inter-TSF trusted channel, para acceder a la parte de la administración el LogHostManager utiliza un canal cifrado mediante **SSL**.

FDP_ITC.1/LogHost Import of user data without security attributes, los datos de entrada de LogHost provienen de syslog-ng u otros componentes externos, estos datos se adquieren en bruto y sin ningún tipo de atributo de seguridad.

6.1.3.2.LOGAGENT

TSF 1.- User Management

FDP_ACC.1/LogAgent Subset access control, politica LAM de acceso al TOE.

FDP_ACF.1/LogAgent Security attribute based access control, cubierto por los atributos de seguridad que validan el acceso a cada usuario.

FMT_MSA.3/LogAgent Static attribute initialization, cuando se instala el producto se definen diferentes atributos de seguridad por defecto, ejemp. User administrator.

FMT_MSA.1/LogAgent Management of security attributes, el TOE proporciona capacidades de administración sobre los usuarios y sus atributos de seguridad.

FMT_SMF.1/LogAgent Specification of Management Functions, el TOE proporciona capacidad de administración de los atributos de seguridad de cada usuario desde LogAgentManager.

FIA_ATD.1/LogAgent User attribute definition, cubierto por la capacidad que tiene el TOE de caracterizar los usuarios mediante: Password y Role.

FIA_UAU.2/LogAgent User authentication before any action, para poder realizar acciones sobre el TOE el usuario debe estar autenticado.

FIA_UID.2/LogAgent Timing of identification, para poder realizar acciones sobre el TOE el usuario debe de estar identificado.

TSF 2.- Role Management

FDP_ACC.1/LogAgent Subset access control, politica LAM de acceso al TOE.

FDP_ACF.1/LogAgent Security attribute based access control, cubierto por los atributos de seguridad que validan el acceso a cada usuario.

FMT_MSA.3/LogAgent Static attribute initialization, cuando se instala el producto se definen diferentes atributos de seguridad por defecto, ejemp. User administrator.

FMT_MSA.1/LogAgent Management of security attributes, el TOE proporciona capacidades de administración sobre los usuarios y sus atributos de seguridad.

FMT_SMR.1/LogAgent Security roles, el TOE mantiene los roles de administrador y operador, dando la posibilidad al administrador de eliminar o agregar privilegios a cada usuario por separado.

FMT_SMF.1/LogAgent Specification of Management Functions, el TOE proporciona capacidad de administración de los atributos de seguridad de cada usuario desde LogAgentManager

FIA_ATD.1/LogAgent User attribute definition, cubierto por la capacidad que tiene el TOE de caracterizar los usuarios mediante: Password y Role.

FIA_UAU.2/LogAgent User authentication before any action, para poder realizar acciones sobre el TOE el usuario debe estar autenticado.

FIA_UID.2/LogAgent Timing of identification, para poder realizar acciones sobre el TOE el usuario debe de estar identificado

TSF 4.- Access Audit

FAU_GEN.1/LogAgent Audit data generation, cubierto por la generación de datos de auditoría por LogAgent.

FDP_ETC.2/LogAgent Export of user data with security attributes, para transferir datos entre LogAgent y LogServer, LogICA implementa un bus JMS, solo los módulos válidos tendrán acceso a enviar paquetes SETP para el bus JMS.

FDP_ITC.2/LogAgent Import of user data with security attributes, para transferir datos entre LogAgent y LogServer, LogICA implementa un bus JMS, solo los modulos validos tendrán acceso a enviar paquetes SETP para el bus JMS.

FTP_ITC.1/LogAgent-JMS Inter-TSF trusted channel, el canal confiable entre los modulos LogAgent y el bus JMS es asegurado mediante el intercambio y validación de certificados.

FDP_IFC.1/LogAgent Information flow control, permite importar y exportar la información recogida por las fuentes de logs.

FDP_IFF.1/LogAgent Simple Secure attributes, permite la posibilidad de configurar las reglas de adquisición de logs desde las fuentes de log.

TSF 5.- Trusted Channel

FDP_ETC.2/LogAgent Export of user data with security attributes, para transferir datos entre LogAgent y LogServer, LogICA implementa un bus JMS, solo los modulos validos tendrán acceso a enviar paquetes SETP para el bus JMS.

FDP_ITC.2/LogAgent Import of user data with security attributes, para transferir datos entre LogAgent y LogServer, LogICA implementa un bus JMS, solo los modulos validos tendrán acceso a enviar paquetes SETP para el bus JMS.

FTP_ITC.1/LogAgent-JMS Inter-TSF trusted channel, el canal confiable entre los modulos LogAgent y el bus JMS es asegurado mediante el intercambio y validación de certificados.

FTP_ITC.1/LogAgentManager Inter-TSF trusted channel, el canal seguro entre los modulos LogAgentManager y LogAgent se asegura mediante el establecimiento de una conexión SSL.

FDP_ITC.1/LogAgent Import of user data without security attributes, los logs en bruto son importados por el modulo LogAgent y representan el input de nuestro sistema.

6.1.3.3.LOGSERVER

TSF 1.- User Management

FDP_ACC.1/LogServer Subset access control, politica LISM de acceso al TOE.

FDP_ACF.1/LogServer Security attribute based access control, cubierto por los atributos de seguridad que validan el acceso a cada usuario.

FMT_MSA.3/LogServerLogServer Static attribute initialization, cuando se instala el sistema se definen diferentes parametros de seguridad por defecto, el administrador tiene la posibilidad de cambiarlos o agregar nuevos.

FMT_MSA.1/LogServerLogServer Management of security attributes, el administrador tiene la posibilidad de gestionar (Agregar, borrar o modificar) los parametros que caracterizan a los usuarios (nombre, password y rol).

FMT_SMF.1/LogServerLogServer Specification of Management Functions, esta cubierto por la capacidad que ofrece el modulo LogServer de modificar los parametros que caracterizan las funciones de seguridad.

FIA_ATD.1/LogServer User attribute definition, el sistema almacena y mantiene los atributos que caracterizan a cada usuario (password y rol).

FIA_UAU.2/LogServer User authentication before any action, para poder realizar cualquier tipo de acción sobre alguna de las partes del TOE, el usuario deberá estar debidamente autenticado.

FIA_UID.2/LogServer Timing of identification, para poder realizar cualquier tipo de acción sobre alguna de las partes del TOE, el usuario deberá estar debidamente identificado.

TSF 2.- Role Management

FDP_ACC.1/LogServer Subset access control, politica LISM de acceso al TOE.

FDP_ACF.1/LogServer Security attribute based access control, cubierto por los atributos de seguridad que validan el acceso a cada usuario.

FMT_MSA.3/LogServerLogServer Static attribute initialization, cuando se instala el sistema se definen diferentes parametros de seguridad por defecto, el administrador tiene la posibilidad de cambiarlos o agregar nuevos.

FMT_MSA.1/LogServerLogServer Management of security attributes, el administrador tiene la posibilidad de gestionar (Agregar, borrar o modificar) los parametros que caracterizan a los usuarios (nombre, password y rol).

FMT_SMR.1/LogServer Security roles, el sistema mantiene los dos tipos de usuarios adminstrador y operador.

FMT_SMF.1/LogServerLogServer Specification of Management Functions, esta cubierto por la capacidad que ofrece el modulo LogServer de modificar los parametros que caracterizan las funciones de seguridad.

FIA_ATD.1/LogServer User attribute definition, el sistema almacena y mantiene los atributos que caracterizan a cada usuario (password and rol).

FIA_UAU.2/LogServer User authentication before any action, para poder realizar cualquier tipo de acción sobre alguna de las partes del TOE, el usuario deberá estar debidamente autenticado.

FIA_UID.2/LogServer Timing of identification, para poder realizar cualquier tipo de acción sobre alguna de las partes del TOE, el usuario deberá estar debidamente identificado.

TSF 4.- Access Audit

FDP_ETC.2/LogServer Export of user data with security attributes, para transferir datos entre LogAgent y LogServer, LogICA implementa un bus JMS, solo los módulos validos tendrán acceso a enviar paquetes SETP para el bus JMS.

FDP_ITC.2/LogServer Import of user data with security attributes, para transferir datos entre LogAgent y LogServer, LogICA implementa un bus JMS, solo los módulos validos tendrán acceso a enviar paquetes SETP para el bus JMS.

FDP_IFC.1/LogServer Information flow control, permite importar y exportar la eventos recogidos por logserver.

FDP_IFF.1/LogServer Simple Secure attributes, permite la posibilidad de configurar las reglas de adquisición de eventos desde logserver.

TSF 5.- Trusted Channel

FDP_ETC.2/LogServer Export of user data with security attributes, para transferir datos entre LogAgent y LogServer, LogICA implementa un bus JMS, solo los módulos validos tendrán acceso a enviar paquetes SETP para el bus JMS.

FDP_ITC.2/LogServer Import of user data with security attributes, para transferir datos entre LogAgent y LogServer, LogICA implementa un bus JMS, solo los módulos validos tendrán acceso a enviar paquetes SETP para el bus JMS.

FTP_ITC.1/LogServer-JMS Inter-TSF trusted channel, el canal confiable entre los módulos LogAgent y el bus JMS es asegurado mediante el intercambio y validación de certificados.

FTP_ITC.1/Console Inter-TSF trusted channel, el acceso remoto entre el módulos Console y LogServer se asegura mediante el establecimiento de una conexión segura SSL.

FDP_ITC.1/LogServer Import of user data without security attributes, LogServer es capaz de entender e importar los eventos e incidentes almacenados en la base de datos.

FDP_ETC.1/LogServer Export of user data without security attributes, LogServer es capaz de entender y exportar los eventos e incidentes almacenados en la base de datos.

6.2. Assurance Measures

En esta sección se especifican las medidas de garantía de seguridad que ha de tener el TOE para satisfacer los requisitos de garantía de seguridad. Las medidas de garantía se

han asociado a los requisitos de garantía, de manera que sea posible trazar la correspondencia entre medidas y requisitos.

Las citadas medidas se encuentran tabuladas a continuación. Éstas son necesarias para la correcta evaluación del TOE.

COMPONENTE DE GARANTÍA	MEDIDA DE GARANTÍA	RAZONAMIENTO
ACM_CAP.2	Procedimiento de Gestión de Configuraciones Configuration Management Plan v.1.3	En el documento se encuentra la relación de elementos de configuración que componen el TOE, las referencias unívocas a los mismos, así como la descripción somera del elemento de configuración.
ADO_DEL.1	Protocolo de Entrega Segura de Software ICA DEL_Secure Delivery Procedure v.1.6	Especificación de cómo se realiza la entrega del TOE de manera que no se vea comprometida su integridad.
ADO_IGS.1	Manual de Instalación general de LogICA 2.1 v.7	Documento en el que se especifica cómo se realiza la instalación, configuración y arranque seguro del TOE, requerimientos de instalación y la gestión de excepciones durante el citado proceso.
ADV_FSP.1	Especificación Funcional LogICA 2.1 v.1.4	En este documento se detallan los TSF a nivel de subsistemas, las interacciones entre ellos así como la especificación de los errores y excepciones que se pueden presentar.
ADV_HLD.1	Diseño de Alto Nivel LogICA 2.1 ADV_HLC - High Level Design Specification- V1.1.doc	Documento de diseño de los diferentes subsistemas de información que componen el TOE.
ADV_RCR.1	Análisis de Correspondencia ST, HLD y FSP v.1.3	Documento de análisis de correspondencia entre la Diseño de Alto Nivel, la Declaración de Seguridad y el Análisis Funcional.
AGD_ADM.1	Manual de Administración LogICA 2.1 v.5	Manual en el que se especifica cómo se ha de realizar la configuración y gestión de los diferentes TSFs que componen el TOE por parte de los usuarios con rol de administrador.
AGD_USR.1	Manual de Operador LogICA 2.1 v.6	Manual en el que se especifica cómo se ha de realizar la configuración y gestión de los diferentes TSFs que componen el TOE por parte de los usuarios operadores.
ATE_COV.1	Manual de Testing de Software Plan de Pruebas v.1.4	Manual de especificación de las pruebas a realizar sobre los TSFs del TOE. En él queda patente la tipología de las pruebas que se van a realizar.
ATE_FUN.1	Documentación de las Pruebas Realizadas	Documentación en la que se muestran los resultados de las pruebas realizadas sobre los TSFs del TOE para que quede patente su

COMPONENTE DE GARANTÍA	MEDIDA DE GARANTÍA	RAZONAMIENTO
		correcto funcionamiento.
ATE_IND.2	Acción del Evaluador.	Acción del Evaluador. Se aporta la distribución de LogICA a evaluar.
AVA_SOF.1	Strength of Function Claim - logICA V2.1-V1.2.pdf	Documento con la evaluación de la fortaleza de los TSFs con comportamiento no criptográfico y con carácter probabilístico y permutacional.
AVA_VLA.1	Análisis de Vulnerabilidades de LogICA 2.1 v.1.5	Documento en el que se encuentra el análisis de vulnerabilidades realizado sobre el TOE para determinar que no existen vulnerabilidades que puedan ser explotadas para comprometer su seguridad.

Tabla 7 - Medidas de Garantía vs. Documentos Correspondientes

7.PP Claims

La presente Declaración de Seguridad no da cumplimiento a ningún Perfil de Protección.

8.Rationale

8.1. Security Objectives Rationale

La consecución de los objetivos de seguridad se aborda desde la perspectiva de casar los objetivos de seguridad, con las amenazas, suposiciones de entorno y políticas de seguridad organizativas.

8.2. Security Assurance Rationale

El razonamiento de los requisitos de seguridad necesarios, se encuentra detallado en el apartado 6.1 del presente documento.

8.3. TOE Summary Specification Rationale

En este apartado se expone porque se han escogido los requisitos de seguridad incluidos en la sección 5 del presente documento. Para ello, se ha utilizado un formato tabular en que se realiza un mapa de requisitos de seguridad, con los objetivos de seguridad a los que dan cumplimiento.

Asimismo, se realizará el análisis de satisfacción de dependencias funcionales de requisitos que se han satisfecho en el modelado de requisitos.

8.3.1.Mapeo Objetivos de Seguridad del TOE Requisitos Funcionales de Seguridad

A continuación se analiza, la trazabilidad de los de los requisitos funcionales de seguridad con los objetivos de seguridad a los que dan cumplimiento. Para ello, se muestra en formato tabular cada instancia de cada requisito cruzado con los diferentes objetivos de seguridad del TOE definidos en la sección 4.

8.3.1.1.LOGHOST y LOGHOSTMANAGER

	O.LOG	O.ROLE	O.AUTHENTICITY	O.SECURECOM	O.INDATA
FAU_GEN.1/LogHost	✓	✗	✗	✗	✗
FDP_ACC.1/LogHost	✗	✓	✗	✗	✗
FDP_ACF.1/LogHost	✗	✓	✗	✗	✗
FMT_MSA.3/LogHost	✗	✓	✗	✗	✗
FMT_MSA.1/LogHost	✗	✓	✗	✗	✗
FMT_SMR.1/LogHost	✗	✓	✗	✗	✗
FMT_SMF.1/LogHost	✗	✓	✗	✗	✗
FDP_ITC.1/LogHost	✗	✗	✗	✗	✓
FDP_ETC.2/LogDB	✗	✗	✗	✗	✓

	O.LOG	O.ROLE	O.AUTHENTICITY	O.SECURECOM	O.INDATA
FDP_ITC.2/LogDB	X	X	X	X	✓
FTP_ITC.1/LogDB	X	X	X	✓	X
FIA_ATD.1/LogHost	X	✓	X	X	X
FIA_UAU.2/LogHost	X	✓	X	X	X
FIA_UID.2/LogHost	X	✓	X	X	X
FDP_DAU.1	X	X	✓	X	X
FTP_ITC.1/LogHostManager	X	X	X	✓	X
FPT_TDC.1/LogHost	X	X	✓	X	X
FDP_IFC.1/LogHost	X	X	X	X	✓
FDP_IFF.1/LogHost	X	X	X	X	✓

Tabla 8 - Objetivos vs. SFR's LogHost y LogHostManager

8.3.1.2.LOGAGENT y LOGAGENTMANAGER

	O.LOG	O.ROLE	O.AUTHENTICITY	O.SECURECOM	O.INDATA
FAU_GEN.1/LogAgent	✓	X	X	X	X
FDP_ACC.1/LogAgent	X	✓	X	X	X
FDP_ACF.1/LogAgent	X	✓	X	X	X
FMT_MSA.3/LogAgent	X	✓	X	X	X
FMT_MSA.1/LogAgent	X	✓	X	X	X
FMT_SMR.1/LogAgent	X	✓	X	X	X
FMT_SMF.1/LogAgent	X	✓	X	X	X
FDP_ITC.1/LogAgent	X	X	X	X	✓
FDP_ETC.2/LogAgent	X	X	X	X	✓
FDP_ITC.2/LogAgent	X	X	X	X	✓
FPT_TDC.1/LogAgent	X	X	X	X	✓
FTP_ITC.1/LogAgent-JMS	X	X	X	✓	X
FTP_ITC.1/LogAgentManager	X	X	X	✓	X
FIA_ATD.1/LogAgent	X	✓	X	X	X
FIA_UAU.2/LogAgent	X	✓	X	X	X
FIA_UID.2/LogAgent	X	✓	X	X	X
FDP_IFC.1/LogAgent	X	X	X	X	✓

	O.LOG	O.ROLE	O.AUTHENTICITY	O.SECURECOM	O.INDATA
FDP_IFF.1/LogAgent	X	X	X	X	✓

Tabla 9 - Objetivos vs. SFR's LogAgent and LogAgentManager

8.3.1.3.LOGSERVER

	O.LOG	O.ROLE	O.AUTHENTICITY	O.SECURECOM	O.INDATA
FAU_GEN.1/LogServer	✓	X	X	X	X
FDP_ACC.1/LogServer	X	✓	X	X	X
FDP_ACF.1/LogServer	X	✓	X	X	X
FMT_MSA.3/LogServer	X	✓	X	X	X
FMT_MSA.1/LogServer	X	✓	X	X	X
FMT_SMR.1/LogServer	X	✓	X	X	X
FMT_SMF.1/LogServer	X	✓	X	X	X
FIA_ATD.1/LogServer	X	✓	X	X	X
FIA_UAU.2/LogServer	X	✓	X	X	X
FIA_UID.2/LogServer	X	✓	X	X	X
FDP_ETC.2/LogServer	X	X	X	X	✓
FPT_TDC.1/LogServer	X	X	X	X	✓
FDP_ITC.1/LogServer	X	X	X	X	✓
FTP_ITC.1/LogServer-JMS	X	X	X	✓	X
FTP_ITC.1/Console	X	X	X	✓	X
FDP_ITC.1/LogServer	X	X	X	X	✓
FDP_ETC.1/LogServer	X	X	X	X	✓
FAU_SAR.2	X	✓	X	X	X
FAU_SAR.1	X	✓	X	X	X
FDP_IFC.1/LogServer	X	X	X	X	✓
FDP_IFF.1/LogServe	X	X	X	X	✓

Tabla 10 - Objetivos vs. SFR's LogServer

8.3.2. Selección de Requisitos Funcionales de Seguridad para el TOE

Para la selección de los requisitos de seguridad del catalogo de Ccv2.3 Parte 2, se ha tomado como referencia el cumplimiento de los objetivos de seguridad definidos en el

apartado 4. A continuación se expone el razonamiento sobre la selección de los citados requisitos por cada uno de los objetivos de seguridad identificados.

8.3.2.1.LOGHOST

O.LOG

Cada uno de los módulos audita las conexiones realizadas por los diferentes usuarios y los intentos de conexión, este objetivo está cubierto por FAU_GEN.1/LogHost, el cual genera eventos de auditoría de accesos al TOE. FAU_GEN.1/LogHost depende de FPT_STM.1 el cual está incluido.

O.ROLE

Para permitir la correcta segregación de funciones por usuario, se agrego el objetivo de seguridad O.ROLE, este objetivo está cubierto FDP_ACC.1/LogHost, FDP_ACF.1/LogHost, FMT_MSA.3, FMT_MSA.1, FMT_SMR.1, FMT_SMF.1, FIA_ATD.1/LogHost, FIA_UAU.2/LogHost y FIA_UID.2/LogHost.

O.AUTHENTICITY

Los requisitos necesarios para asegurar la autenticidad de los logs son FDP_ETC.2/LogDB, FDP_ITC.2/LogDB, FDP_DAU.1 y FPT_TDC.1/LogHost.

O.SECURECOM

Todas las comunicaciones entre módulos del TOE se realizan mediante la asociación de canales seguros. En el caso de LogHost este objetivo está cubierto por FTP_ITC.1/LogHostManager el cual asegura la comunicación entre LogHostManager y LogHost utilizando el protocolo SSL y FTP_ITC.1/LogDB utilizando SSL.

O.INDATA

Los datos de entrada en el cuales se basarán todos los eventos e incidentes generados, son capturados a partir de logs generados por “**syslog-ng**”. Para modelar el input y cubrir el objetivo entrada de datos, se ha utilizado el requisito FDP_ITC.1/LogHost, FDP_IFC.1 y FDP_IFF.1

8.3.2.2.LOGAGENT

O.LOG

Cada uno de los módulos audita las conexiones realizadas por los diferentes usuarios y los intentos de conexión, este objetivo está cubierto por FAU_GEN.1/LogAgent, el cual genera eventos de auditoría de accesos al TOE. FAU_GEN.1/LogAgent depende de FPT_STM.1 el cual no ha sido agregado ya que no se realiza sellado de tiempo en este subsistema.

O.ROLE

Para permitir la correcta segregación de funciones por usuario, se agregó el objetivo de seguridad O.ROLE, este objetivo está cubierto FDP_ACC.1/LogAgent, FDP_ACF.1/LogAgent, FMT_MSA.3/LogAgent, FMT_MSA.1/LogAgent, FMT_SMR.1/LogAgent, FMT_SMF.1/LogAgent, FIA_ATD.1/LogAgent, FIA_UAU.2/LogAgent y FIA_UID.2/LogAgent.

O.AUTHENTICITY

Los requisitos necesarios para asegurar la autenticidad de los logs son FDP_ETC.2/LogAgent, FDP_ITC.2/LogAgent y FPT_TDC.1/LogAgent.

O.SECURECOM

Todas las comunicaciones entre módulos del TOE se realizan mediante la asociación de canales seguros. En el caso de LogAgent este objetivo está cubierto por FTP_ITC.1/LogAgentManager, el cual asegura la comunicación entre LogAgent y Console utilizando el protocolo SSL y por FTP_ITC.1/LogAgent-JMS LogAgent, el cual asegura la comunicación entre LogAgent y el bus JMS utilizando el protocolo SETP.

O.INDATA

Los datos de entrada en el cuales se basaran todos los eventos e incidentes generados, son capturados a partir de logs generados por syslog-ng u otra aplicación externa. Para modelar el input y cubrir el objetivo entrada de datos, se ha utilizado el requisito FDP_ETC.1/LogAgent, FDP_ITC.1/JMS, FDP_IFC.1 y FDP_IFF.1.

8.3.2.3.LOGSERVER

O.LOG

Cada uno de los módulos audita las conexiones realizadas por los diferentes usuarios y los intentos de conexión, este objetivo está cubierto por FAU_GEN.1/LogServer, el cual genera

eventos de auditoría de accesos al TOE. FAU_GEN.1/LogServer depende de FPT_STM.1 el cual no está agregado porque este subsistema no realiza sellado de tiempo.

O.ROLE

Para permitir la correcta segregación de funciones por usuario, se agrego el objetivo de seguridad O.ROLE, este objetivo es cubierto FDP_ACC.1/LogServer, FDP_ACF.1/LogServer, FMT_MSA.3/LogServer, FMT_MSA.1/LogServer, FMT_SMR.1/LogServer, FMT_SMF.1/LogServer, FIA_ATD.1/LogServer, FIA_UAU.2/LogServer, FIA_UID.2/LogServer, FAU_SAR.2 y FAU_SAR.1.

O.AUTHENTICITY

Los requisitos necesarios para asegurar la autenticidad de los logs son FDP_ETC.2/LogServer, FDP_ITC.2/LogServer y FPT_TDC.1/LogServer.

O.SECURECOM

Todas las comunicaciones entre módulos del TOE se realizan mediante la asociación de canales seguros. En el caso de LogServer este objetivo está cubierto por FTP_ITC.1/Console el cual asegura la comunicación entre LogServer y Console utilizando el protocolo SSL y FTP_ITC.1/LogServer-JMS, el cual asegura la comunicación entre LogServer y el bus JMS utilizando el protocolo SETP.

O.INDATA

En el caso de LogServer los datos de entrada son transmitidos por el bus JMS, es por ello que para cubrir O.INDATA se utiliza FDP_ETC.1/LogServer y FDP_ITC.1/LogServer.

8.3.3. Objetivos de Seguridad del Entorno IT Vs. Requisitos Funcionales de Seguridad

Se analiza a continuación, la trazabilidad de los de los requisitos funcionales de seguridad con los objetivos de seguridad del entorno IT a los que dan cumplimiento. Para ello, se muestra en formato tabular cada instancia de cada requisito cruzado con los diferentes objetivos de seguridad entorno IT definidos en la sección 4.

	O.E.OSAUTH	O.E.DBAUTH	O.E.BAST	O.E.TIME	O.E.DBINTE	O.E.ADMIN_TRUST
FIA_ATD.1/OS	✓	✗	✗	✗	✗	✗
FIA_ATD.1/DB	✗	✓	✗	✗	✗	✗
FDP_UAU.2/ENV	✓	✓	✗	✗	✗	✗
FIA_UID.2/ENV	✓	✓	✗	✗	✗	✗
FIA_USB.1	✗	✗	✓	✗	✗	✗
FMT_SMR.1/OS	✓	✗	✗	✗	✗	✗
FMT_SMR.1/DB	✗	✓	✗	✗	✗	✗
FMT_SMF.1/OS	✓	✗	✗	✗	✗	✗
FMT_MOF.1/OS	✗	✗	✓	✗	✗	✓
FPT_STM.1	✗	✗	✗	✓	✓	✗
FDP_SDI.1	✗	✗	✗	✗	✓	✗

Tabla 11 - Correspondencia entre Objetivos de Seguridad de Entorno y Requisitos Funcionales

8.3.4. Selección de Requisitos Funcionales de Seguridad del entorno IT

Para la selección de los requisitos de seguridad de la norma de CC v2.3 Parte 2, se ha tomado como referencia el cumplimiento de los objetivos de seguridad definidos en el apartado 4. A continuación se expone el razonamiento sobre la selección de los citados requisitos por cada uno de los objetivos de seguridad identificados.

O.E.OSAUTH

Para poder gestionar ciertos aspectos del TOE y de su entorno, es necesario realizarlo desde una consola del Sistema Operativo donde éste se encuentre instalado. Se hace necesaria la identificación y autenticación de los usuarios que accedan al sistema y por ello se realiza la selección de los requisitos que modelan este aspecto, FIA_ATD.1/OS, FIA_UAU.2/ENV y FIA_UID.2/ENV, modelado de atributos de Tabla 11 validación y requisitos de identificación y autenticación. Durante la instalación del Sistema Operativo se crea el

usuario "logica", junto con la raíz del sistema, este aspecto se modela en los roles especificados por el requisito FMT_SMR.1/OS y FMT_SMF.1/OS.

O.E.DBAUTH

Para poder gestionar el Sistema Gestor de Base de Datos en el que almacene los eventos LogICA, es necesario realizarlo desde una consola del sistema operativo donde éste se encuentre instalado. Se hace necesaria la identificación y autenticación de los usuarios que accedan a la consola de administración del Sistema Gestor de Bases de Datos y por ello se realiza la selección de los requisitos que modelan este aspecto, FIA_ATD.1/DB, FIA_UAU.2/ENV y FIA_UID.2/ENV, modelado de atributos de validación y requisitos de identificación y autenticación. Como durante la instalación del Sistema Gestor de Bases de Datos se crea el usuario "logicadba", es necesario modelar el rol con el requisito FMT_SMR.1/DBA.

O.E.BAST

La consecución de este objetivo de seguridad, se realiza siguiendo lo indicado dentro de los manuales de bastionado incluidos en los dos siguientes documentos:

1. Manual de Instalación de LogICA 2.1 v.5
2. Manual de Administración de LogICA 2.1 v.5

Para ello se seleccionan los requisitos funcionales FMT_MOF.1/OS y FIA_USB.1

El objetivo final es que las siguientes plataformas queden bastionadas:

1. Sistema Operativo donde se ejecuta el TOE.
2. Servidor de aplicaciones que utiliza el TOE.
3. Sistema Gestor de Bases de Datos utilizado por el TOE.

O.E.TIME

La consecución de este objetivo de seguridad, es necesario instanciar el requisito FPT_STM.1 el cual mantiene una base de tiempo confiable.

O.E.DBINTE

Dado que es necesario que el Sistema Gestor de Bases de Datos sobre el que se instale el TOE ha de garantizar la integridad de los datos que gestiona, es necesario instanciar los requisitos FDP_SDI.1 y FPT_STM.1 el cual mantiene una base de tiempo confiable.

O.E.ADMIN_TRUST

La consecución de este objetivo de seguridad, se realiza siguiendo lo indicado dentro del "Manual del Administrador" y que cumple con el requisito FMT_MOF.1/OS.

8.3.5. Análisis de satisfacción de dependencias funcionales

Tal y como queda definido en el paradigma de la parte 2 de CC v2.3, todo requisito de seguridad puede depender funcionalmente de uno más requisitos diferentes de manera que cubra en su totalidad el objetivo de seguridad que se persigue.

A continuación, se expresa en forma tabular la satisfacción de estas dependencias funcionales para los requisitos funcionales de seguridad que se han escogido para dar cumplimiento a los objetivos de seguridad que se han expuesto en la sección 4 del presente documento.

8.3.5.1. Satisfacción de dependencias para la iteración LOGHOST y LOGHOSTMANGER.

DEPENDENCIAS	ACCIÓN
FDP_IFF.1/LogHost FMT_MSA.3	NO se ha incluido FMT_MSA.3 para este requisito ya que los atributos de seguridad son dinámicos.

Tabla 12.- Satisfacción de Dependencias Funcionales

8.3.5.2. Satisfacción de dependencias para la iteración LOGAGENT y LOGAGENTMANAGER

DEPENDENCIAS	ACCION
FAU_GEN.1/LogAgent FPT_STM.1	No se ha incluido ya que no se realizan sellados de tiempo en este modulo.

Tabla 13.- Satisfacción de Dependencias Funcionales

8.3.5.3. Satisfacción de dependencias para la iteración LOGSERVER

DEPENDENCIAS	ACCION
FAU_GEN.1/LogServer FPT_STM.1	No se ha incluido ya que no se realizan sellados de tiempo en este modulo.
FDP_ACC.1/LogServer FDP_ACF.1	Incluido FDP_ACF.1/LogServer.
FDP_ACF.1/LogServer FDP_ACC.1 FMT_MSA.3 FDP_IFC.1 FDP_IFF.1	Incluidos FDP_ACC.1/LogServer, FMT_MSA.3/LogServer, FDP_IFC.1 y FDP_IFF.1.
FMT_MSA.3/LogServer FMT_MSA.1 FMT_SMR.1	Incluidos FMT_MSA.1/LogServer y FMT_SMR.1/LogServer.
FMT_MSA.1/LogServer FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	Incluidos FDP_ACC.1/LogServer, FMT_SMR.1/LogServer y FMT_SMF.1/LogServer.
FMT_SMR.1/LogServer FIA_UID.1	Incluido FIA_UID.2/LogServer.
FIA_UAU.2/LogServer FIA_UID.1	Incluido FIA_UID.2/LogServer.
FDP_ETC.2/LogServer FDP_ACC.1	Incluido FDP_ACC.1/LogServer.
FDP_ITC.2/LogServer FDP_ACC.1 FTP_ITC.1 FPT_TDC.1	Incluidos FDP_ACC.1/LogServer, FTP_ITC.1/LogServer-JMS y FPT_TDC.1/LogServer.
FDP_ITC.1/LogServer FDP_ACC.1 FMT_MSA.3	Incluidos FDP_ACC.1/LogServer y FMT_MSA.3/LogServer.
FDP_ETC.1/LogServer FDP_ACC.1	Incluido FDP_ACC.1/LogServer
FAU_SAR.2 FAU_SAR.1	Incluido FAU_SAR.1.
FAU_SAR.1 FAU_GEN.1	Incluido FAU_GEN.1/LogServer

Tabla 14.- Satisfacción de Dependencias Funcionales

8.4. PP Claims Rationale

Como se ha expuesto en el apartado 7 del documento, la presente Declaración de Seguridad no da cumplimiento a ningún perfil de protección.