25 años Impulsando
la innovación

Sistema de Gestión de Eventos SIEM
Suite LogICA v3.0-SP2 Patch11
Security Target

Diciembre, 2009
Informática y Comunicaciones Avanzadas S.L
Alejandro Rodríguez, 32
28039 Madrid

CONTROL DE VERSIONES

TÍTULO DEL DOCUMENTO	Sistema de Gestión de Eventos SIEM Suite LogICA v3.0-SP2 Patch11 Security Target

Versión	Fecha	Descripción	Realizado por	Revisado por
1.0	17-12-2009	Versión inicial	ICA Seguridad	ICA
1.1	22-12-2009	Cambio de estructura para adaptación a CCV3.1R3	ICA Seguridad	ICA
1.2	23-04-2010	Descripción de estructura física del TOE Descripción de componentes Desarrollo de objetivos y requisitos de seguridad Adecuación de términos	ICA Seguridad	ICA
1.3	12/05/2010	Justificación de objetivos Requisitos de seguridad funcional	ICA Seguridad	ICA
1.4	16/07/2010	Corrección de los siguientes OR: OR1_LOGI002 M0 OR2_LOGI002 M0 OR3_LOGI002 M0 OR4_LOGI002 M0 OR5_LOGI002 M0 OR6_LOGI002 M0 OR7_LOGI002 M0 OR8_LOGI002 M0 OR9_LOGI002 M0	ICA Seguridad	ICA
1.5	27/10/2010	Corrección de los siguientes OR: OR3_LOGI002 M1 OR5_LOGI002 M1 OR6_LOGI002 M1 OR12_LOGI002 M0	ICA Seguridad	ICA
1.6	21/03/2011	Cambio de nomenclatura y versionado TOE	ICA Seguridad	ICA

ÍNDICE DE CONTENIDOS

1.ST Introduction

1.1.ST Reference

Titulo: Sistema de Gestión de Eventos SIEM Suite LogICA v3.0-SP2 Patch11 Security Target
Versión: 1.6
Autor: ICA
Fecha: 21 de marzo de 2011

1.2.TOE Reference

Sistema de Gestión de Eventos (SIEM) Suite LogICA, versión 3.0-SP2 Patch11[1]

Componentes:

- LogAgent, versión 3.0
- LogServer, versión 3.0
- EventCorrelator, versión 3.0
- Console, versión 3.0
- LogHost, versión 3.0
- LogAgentManager, versión 3.0
- LogHostManager, versión 3.0
- LogSpaces, versión 3.0
- LogReports, versión 3.0
- Achilles, versión 3.0
- Activos, versión 3.0
- LISM, versión 3.0
- CuadICA, versión 3.0

1.3.TOE Overview

1.3.1.Tipo de TOE

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 cinco 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.
- Establecimiento de indicadores de cumplimiento legal y normativo en aspectos de seguridad IT.

La herramienta se ha concebida 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.

1.3.2.Componentes del TOE

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.
- Normaliza la información.

[1] Cualquier referencia a LogICA, a lo largo de la documentación desarrollada, se refiere a la versión aquí declarada.

- Realiza el transporte de información a LogServer y LogHost.
- Permite correlación distribuida en agentes mediante procesadores

LogServer

- Event Collector recoge los logs previamente filtrados por LogAgent y genera eventos de primer nivel mediante reglas de correlación, realiza la clasificación y almacenamiento, y permite la notificación y gestión de eventos e incidentes.
- Permite la integración de plugins.
- Realiza acciones asociadas a plugins integradas en paralelo con el sistema.

EventCorrelator

- Recoge los eventos del bus generados por EventCollector y genera eventos de segundo nivel o incidencias mediante reglas de correlación y detecta patrones a través del seguimiento de actividad.

Console

- Permite la monitorización de eventos y módulos en tiempo real.
- Gestiona incidentes.
- Realiza la representación estadística.
- Permite la generación de informes y consultas.
- Permite la consulta sobre logs consolidados.
- Incorpora la administración centralizada del sistema.
- Permite la integración de plugins.

LogHost

- Recoge y recibe los logs de cualquier fuente.
- Almacena los logs recibidos en una base de datos.
- Realiza la protección de integridad y establece la cadena de custodia digital a través de rutinas de LogHostManager.
- Motor estadístico con capacidad para el establecimiento de bandas de normalidad.
- Motor de consultas que permite el acceso a la información en bruto para la generación de casos forenses.

LogAgentManager

- Gestionar y configura los agentes remotamente.
- Distribuye las configuraciones.
- Monitoriza y controla el funcionamiento de los agentes.
- Gestiona la configuración de vigilancia de configuraciones y auditoria de actividad de usuarios sobre archivos.

LogHostManager

- Permite la configuración de LogHost remotamente.
- Gestiona las rutinas de comunicación para la recopilación remota de información.
- Permite generar nuevas reglas del filtrado.
- Muestra información y estadísticas sobre los logs recogidos.

LogSpaces

- Permite el acceso al espacio de logs desde un cliente http (Console).
- Gestiona las consultas de log y creación de casos forenses.

LogReports

- Gestión y creación de informes sobre eventos, incidentes, recomendaciones y activos.
- Subsistema EIS (Enterprise Information System) de LogICA.

Achilles

- Permite la gestión de vulnerabilidades a través de autodescubrimiento.
- Permite la generación de avisos en forma de eventos.
- Incorpora la capacidad para generación de recomendaciones.
- Integración con bases de datos de vulnerabilidades de terceros.

Activos

- Permite la gestión del inventario de activos con orientación CMDB.
- Realiza el autodescubrimiento de activos.
- Incorpora motor para la importación e integración automática de activos de otras fuentes de almacenamiento.
- Extracción de la información de vigilancia de configuraciones y auditoria de actividad de usuarios sobre archivos asociados a cada activo.

LISM

- Realiza la gestión de autenticaciones y autorizaciones.
- Suministro de funciones de rol.
- Gestión de licencias.

CuadICA

- Permite la definición de indicadores asociado a estructura organizativa y en relación con el cumplimiento de normativas de seguridad mediante la composición de cuadros de mando.
- Recopila y centraliza información.
- Generación de informes.
- Permite consulta sobre indicadores según filtros predefinidos.

1.4.TOE Description

1.4.1.Entorno operativo

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

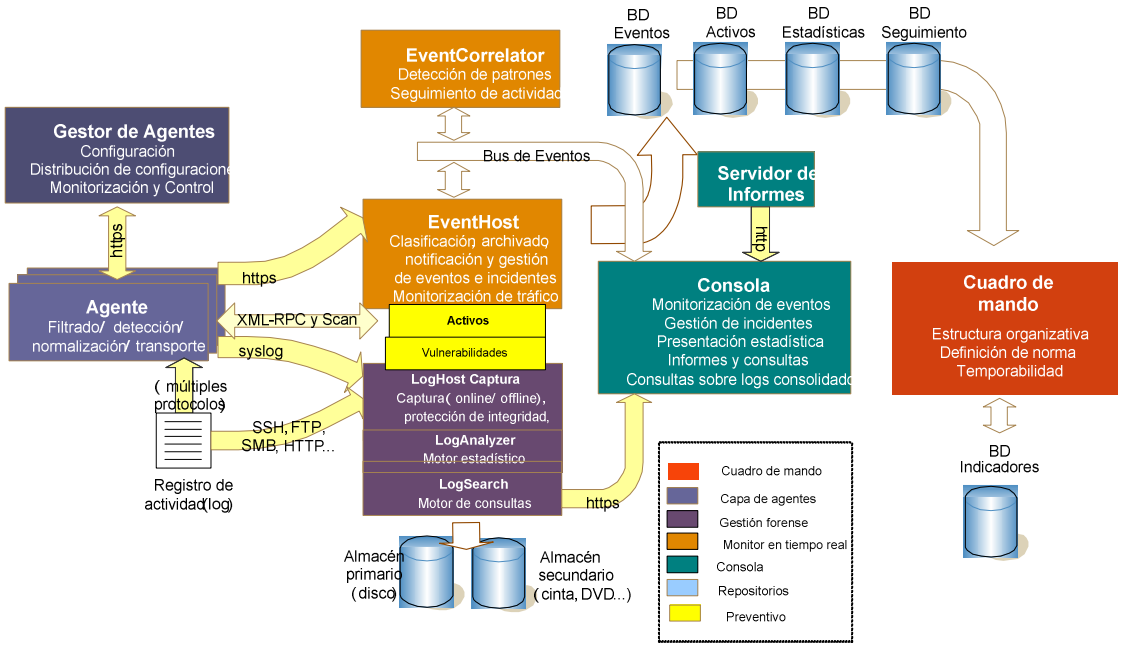

Imagen 1: Arquitectura modular del TOE

Desde el punto de vista de tecnología los componentes necesarios para que el entorno operativo sea adecuado para el correcto funcionamiento del TOE son:

- Sistema Operativo:
  - CentOS 5.3
- Servidor de aplicaciones:
  - Apache Tomcat 5.2.20 o superior.
- Sistemas Gestores de Base de Datos :
  - Oracle Database 10g Enterprise Edition
- JMS Broker BUS
  - ActiveMQ v4 o v5
- JRE 1.6.0.5 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.*

El TOE se instala en un servidor Appliance que permite ser ejecutado íntegramente, aunque por la estructura operativa que implementa LogICA v3.0 totalmente modular, el sistema puede ser ejecutado en modo distribuido. Con ello se consigue separar las deferentes partes, LogAgent, LogServer, EventCorrelator, Console, LogHost, LogAgentManager, LogHostManager, Achilles, Activos, Lism, CuadICA.

Aunque las características del Appliance pueden ser diversas en función de las necesidades de capacidad y rendimiento de la instalación y del estado del arte tecnológico, las características mínimas recomendadas del servidor se ajustan a la siguiente descripción y que pueden ser escaladas para ajustarse a las necesidades y versiones de distribución del producto.

Datos	Detalle
CPU	Quad Core 64 bits
RAM	16 Gb
Almacenamiento interno	1 Tb SATA II
Chasis	1 U. Rack
Alimentación	2x Redundante
Interfaces de red	2x 10/100/1000
Gestión	Consola gráfica
Almacenamiento secundario	Capacidad de volcado
Entradas de eventos/seg (EPS)	500
Cantidad de dispositivos	50
Cantidad de fuentes	5
Ratio de compresión	20:1 - 50:1

Tabla 1 - Características mínimas appliance

Los dispositivos disponibles en base a las necesidades y capacidad se versionan según se refleja en la siguiente tabla:

	LogICA AF				LogICA TR-AF				
	FQ2	FQ3	FQ4	FQ5	FQC2	FQC3	FQC4	FQC5	FQC6
Tiempo real									
Gestión de Alertas					x	x	x	x	x

	LogICA AF				LogICA TR-AF				
Gestión de Vulnerabilidades					x	x	x	x	
Consulta BBDD Vulnerabilidades					x	x	x	x	
Inventariado de Activos					x	x	x	x	
Motor de correlación					x	x	x	x	x
Gestión de Incidencias					x	x	x	x	x
Cuadro Resumen de seguridad					x	x	x	x	x
Vigilancia de configuraciones					x	x	x	x	x
Gestión de Anomalías					x	x	x	x	x
Trazabilidad de usuarios					x	x	x	x	x
Análisis Forense									
Almacenamiento de log	x	x	x	x	x	x	x	x	x
Motor de Consultas	x	x	x	x	x	x	x	x	x
Casos Forenses	x	x	x	x	x	x	x	x	x
Motor estadístico	x	x	x	x	x	x	x	x	x
Licenciamiento									
Nº máximo de Dispositivos	50	200	500	1000	50	150	300	500	1000
Nº Máximo de Fuentes					5	15	30	40	60
Capacidades									
Eventos/seg					500	1500	3000	5000	10000
Almacenamiento de Información	1 Tb	2 Tb	4 Tb	8 Tb	1 TB	1 TB	3 TB	3 TB	7 TB
Líneas/seg	5.000	10.000	20.000	100.000	5.000	15.000	30.000	50.000	100.000
Usuarios Simultáneos	4	4	8	8	4	4	10	10	20
Cuadro de mando									
Mononorma		Opcional	Opcional	Opcional		Opcional	Opcional	x	x
Multinorma		Opcional	Opcional	Opcional		Opcional	Opcional	x	x

Tabla 2 - Versiones de distribución

El sistema sometido a evaluación, cumple con las características FQC3.

1.4.2.Características

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

1.4.2.1.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.

1.4.2.2.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.

1.4.2.3.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.

1.4.2.4.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, de mismo nombre que el original, consiste en la firma electrónica generada a partir del log y un certificado autofirmado con algoritmo de firma **SHA1 with RSA.**

1.4.2.5.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. Entre los diferentes componentes se intercambian, además, objetos serializados y documentos xml bajo protocolo HTTPS.

2.Conformance claims

2.1.CC Conformance claim

Esta declaración de seguridad cumple Common Criteria v3.1, edición 3, de julio de 2009, según los requisitos establecidos de contenido y presentación.

Todos los requisitos funcionales y de garantía de seguridad establecidos en esta declaración de seguridad cumplen con las partes 1, 2 y 3 establecidos en la versión de referencia.

No existen extensiones de requisitos de seguridad.

El nivel de evaluación para el TOE es Evaluation Assurance Level 2 (EAL2).

2.2.PP Claim. Package claim

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

2.3.Conformance rationale

N/A

3.Security problem definition

3.1.Threats

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.

3.2.Organisational security policies

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.

3.3.Assumptions

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

3.3.1.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.

3.3.2.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.

4.Security objectives

4.1.Security objetives 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, eventos y datos de usuario desde las fuentes de logs externas e internas utilizadas por LogICA y exportarlos a las unidades de almacenamiento.

4.2.Security objetives for the operational 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.

4.3.Security objetives 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.

Security objetives rationale		Amenazas				Políticas de seguridad organizativas		Asumpciones operacionales				Asumpciones de usuarios
		T.IDENTITY_SPOOFING	T.FORENSIC_EVENT_MODIFIED	T.UNAUTHORIZED_ACCESS	T.SNIFFING	P.LOGACCESS	P.USERLEVEL	A.IDENTIFICATION_&_AUTHENTICATION	A.DBINTEGRITY	A.INSTALLATION	A.TIME	A.NO_EVIL_ADMIN
Objetivos Seguridad TOE	O.LOG	x	x	x								
	O.ROLE	x		x		x						
	O.AUTHENTICITY		x				x					
	O.SECURECOM				x	x						
	O.INDATA				x	x						
Objetivos Seguridad Entorno Operativo	O.E.OSAUTH	x		x			x	x				
	O.E.DBAUTH	x		x			x	x				
	O.E.ADMIN_TRUST											x
	O.E.BAST									x		
	O.E.TIME										x	
	O.E.DBINT								x			

Security objetives rationale justifica que los objetivos de seguridad, tanto del TOE como del entorno operativo, abarcan todas las amenazas, políticas de seguridad organizativas y las asumpciones operacionales y de usuarios.

O.LOG
Contraresta de forma directa las amenazas: T.IDENTITY_SPOOFING, T.FORENSIC_EVENT_MODIFIED y T.UNAUTHORIZED_ACCESS.
O.ROLE
Contraresta de forma directa las amenazas: T.IDENTITY_SPOOFING, y T.UNAUTHORIZED_ACCESS; y hace cumplir de forma directa las políticas de seguridad organizativas: P.LOGACCESS.
O.AUTHENTICITY
Contraresta de forma directa las amenazas: T.FORENSIC_EVENT_MODIFIED; y hace cumplir de forma directa las políticas de seguridad organizativas: P.USERLEVEL
O.SECURECOM
Contraresta de forma directa las amenazas: T.SNIFFING; y hace cumplir de forma directa las políticas de seguridad organizativas: P. P.LOGACCESS.
O.INDATA
Contraresta de forma directa las amenazas: T.SNIFFING; y hace cumplir de forma directa las políticas de seguridad organizativas: P. P.LOGACCESS.
O.E.OSAUTH
Contraresta de forma directa las amenazas: T.IDENTITY_SPOOFING y T.SNIFFING; hace cumplir de forma directa las políticas de seguridad organizativas: P.USERLEVEL; y hace cumplir de forma directa y razonable las asumpciones operacionales: A.IDENTIFICATION_&_AUTHENTICATION.
O.E.DBAUTH

Contraresta de forma directa las amenazas: T.IDENTITY_SPOOFING y T.SNIFFING; hace cumplir de forma directa las políticas de seguridad organizativas: P.USERLEVEL; y hace cumplir de forma directa y razonable: A.IDENTIFICATION_&_AUTHENTICATION.

O.E.ADMIN_TRUST

Hace cumplir de forma directa y razonable las asumpciones de usuarios: A.NO_EVIL_ADMIN.

O.E.BAST

Hace cumplir de forma directa y razonable las asumpciones operacionales: A.INSTALLATION.

O.E.TIME

Hace cumplir de forma directa y razonable las asumpciones operacionales: A.TIME.

O.E.DBINT

Hace cumplir de forma directa y razonable las asumpciones operacionales: A.DBINTEGRITY.

5.Security requirements

5.1.Security functional requirements

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 3 de la Declaración de Seguridad. Estos requisitos han sido extraídos de la parte 2 de CCV3.1.

5.1.1. LogAgent y LogAgentManager

5.1.1.1.FAU_GEN.1/ LogICA 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 (if applicable), 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.

5.1.1.3.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.

5.1.1.4.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.

5.1.1.5.FDP_ACF.1/LogAgent and LogAgentManager Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [LISM Access Control Policy] to objects based on the following: [login process to get access to LogAgentManager and LogAgent managed by LISM Control Access Module, 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]

5.1.1.6.FDP_ACC.1/LogAgent and LogAgentManager Subset access control

FDP_ACC.1.1 The TSF shall enforce the [LISM Access Control Policy] on [users and all user data managed and kept inside LogAgent and LogAgentManager].

5.1.1.7.FDP_IFC.1/LogAgent and LogAgentManager Subset information flow control

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

5.1.1.8.FDP_IFF.1/LogAgent and LogAgentManager 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: [logagent's sections, log capture based on the following security attributes – log properties: Facility, Level, Host, Mask and Program].

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

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [N/A].

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

5.1.1.9.FIA_UAU.2 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.

5.1.1.10.FIA_UID.1Timing of identification

FIA_UID.1.1 The TSF shall allow [Insert user login and password] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.1.11.FIA_UID.2 User identification before any action

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

5.1.1.12.FMT_MSA.3 /LogICA Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [LISM Access Control Policy and information flow policy] to provide [permissive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2 The TSF shall allow the [any role assigned to the sec-adm section e.g. administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.1.13.FMT_SMF.1 / LogAgent and LogAgentManager Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [Management of agents based on LISM Access Control Policy].

5.1.1.14.FPT_TDC.1/LogAgent and LogAgentManager Inter-TSF basic TSF data consistency

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

FPT_TDC.1.2 The TSF shall use [de-serialization of objects, SETP protocol and syslog header in logs] when interpreting the TSF data from another trusted IT product.

5.1.1.15.FTP_ITC.1/LogAgent and LogAgentManager Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another 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 TSF, another trusted IT product] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [LogAgentManager, LogAgent and LISM to authenticate and validate policies via LISM, Administration/Visualization from Console to LogAgentManager, LogAgent, and sending events via SETP to LogServer and bus JMS under SSL protocol.]

5.1.2.LogServer

5.1.2.1.FAU_GEN.1 / LogICA 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 (if applicable), 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.FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.1.2.3.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.

5.1.2.4.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.

5.1.2.5.FDP_ACF.1 /LogServer Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [LISM Access Control Policy] to objects based on the following: [login process to get access to LogServer managed by LISM Control Access Module, 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, then the LISM policy depending on user's role determine if access 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]

5.1.2.6.FDP_ACC.1 / LogServer Subset access control

FDP_ACC.1.1 The TSF shall enforce the [LISM Access Control Policy] on [users and all user data managed and kept inside LogServer].

5.1.2.7.FDP_IFC.1 /LogServer Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [information flow policy] on [logserver and events]

5.1.2.8.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 events 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: [event capture based on security attributes – standard event properties, logserver's sections]

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

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [N/A].

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

5.1.2.9.FMT_MSA.3 /LogICA Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [LISM Access Control Policy and information flow policy] to provide [permissive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2 The TSF shall allow the [any role assigned to the sec-adm section e.g. administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.2.10.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 logserver engine based on LISM Access Control Policy].

5.1.2.11.FPT_TDC.1 /LogServer Inter-TSF basic TSF data consistency

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

FPT_TDC.1.2 The TSF shall use [de-serialization of objects and SETP protocol] data when interpreting the TSF data from another trusted IT product.

5.1.2.12.FTP_ITC.1/LogServer 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 TSF, another trusted IT product] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [LogServer and LISM to authenticate and validate policies via LISM, and Administration/Visualization from Console to LogServer and sending events via bus JMS to EventCorrelator under SSL protocol.]

5.1.3.EventCorrelator

5.1.3.1.FAU_GEN.1/ LogICA 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 (if applicable), 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.FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.1.3.3.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.

5.1.3.4.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.

5.1.3.5.FDP_ACF.1 /EventCorrelator Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [LISM Access Control Policy] to objects based on the following: [login process to get access to EventCorrelationEngine managed by LISM Control Access Module, 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, then the LISM policy depending on user's role determine if access is allowed.]

FDP_ACF.1.3 The TSF shall explicitly authorise 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]

5.1.3.6.FDP_ACC.1/ EventCorrelator Subset access control

FDP_ACC.1.1 The TSF shall enforce the [LISM Access Control Policy] on [users and all user data managed and kept inside EventCorrelator].

5.1.3.7.FDP_IFC.1 /EventCorrelator Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [information flow policy] on [eventcorrelator and correlated events]

5.1.3.8.FDP_IFF.1 /EventCorrelator 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: [eventcorrelator and events 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: [event capture via JMS bus based on security attributes – standard event properties, eventcorrelator's sections]

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

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [N/A].

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

5.1.3.9.FIA_UAU.2 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.

5.1.3.10.FIA_UID.1Timing of identification

FIA_UID.1.1 The TSF shall allow [Insert user login and password] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.3.11.FIA_UID.2 User identification before any action

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

5.1.3.12.FMT_MSA.3 /LogICA Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [LISM Access Control Policy and information flow policy] to provide [permissive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2 The TSF shall allow the [any role assigned to the sec-adm section e.g. administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.3.13.FMT_SMF.1 /EventCorrelator Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [Management of eventcorrelator engine based on LISM Access Control Policy].

5.1.3.14.FPT_TDC.1/EventCorrelator Inter-TSF basic TSF data consistency

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

FPT_TDC.1.2 The TSF shall use [de-serialization of objects and SETP protocol] when interpreting the TSF data from another trusted IT product.

5.1.3.15.FTP_ITC.1/EventCorrelator 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 TSF, another trusted IT product] to initiate communication via the trusted channel.
FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [EventCorrelator and LISM to authenticate and validate policies via LISM, Administration/Visualization from Console to EventCorrelator, sending and receiving events via bus JMS to LogServer under SSL protocol and to LogServer for managing incidents.]

5.1.4.Console

5.1.4.1.FDP_ACF.1 /Console Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [LISM Access Control Policy] to objects based on the following: [login process to get access to Console managed by LISM Control Access Module for each component, 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, then the LISM policy depending on user's role determine if access is allowed.]

FDP_ACF.1.3 The TSF shall explicitly authorise 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]

5.1.4.2.FDP_ACC.1/Console Subset access control

FDP_ACC.1.1 The TSF shall enforce the [LISM Access Control Policy] on [users and all user data managed and kept inside Console].

5.1.4.3.FDP_IFC.1/Console Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [information flow policy] on [Console and imported events]

5.1.4.4.FDP_IFF.1/Console 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: [imported events controlled under the indicated SFP, and for each, standard event properties, LogICA' sections].

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: [event

capture via JMS bus based on security attributes – standard event properties, LogICA' s sections (sections belonging to each component)]

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

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [N/A].

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

5.1.4.5.FIA_UAU.2 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.

5.1.4.6.FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [Insert user login and password] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.4.7.FIA_UID.2 User identification before any action

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

5.1.4.8.FTP_ITC.1/Console Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another 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 TSF, another trusted IT product] to initiate communication via the trusted channel.
FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [Console, Achilles, Assets, LogAgentManager, EventCorrelationEngine, LogServer, LogSpaces, LogReports, LogHostManager and LISM, to authenticate and validate policies via LISM, and Administration/Visualization from Console to LISM, Achilles, Assets, LogAgentManager, EventCorrelationEngine, LogServer, LogSpaces, LogReports, LogHostmanager, Cuadica, JMS bus, Ntop and several utilities as: nmap, and nessus under SSL protocol.]

5.1.5.LogHost y LogHostManager

5.1.5.1.FAU_GEN.1/ LogICA 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 (if applicable), 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].

5.1.5.2.FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.1.5.3.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.

5.1.5.4.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.

5.1.5.5.FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the [LISM Control Access Policy] on [subject with read/write permissions on LogHost directories] and all operations among subjects and objects covered by the SFP.

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

5.1.5.6.FDP_ACF.1 /LogHost and LogHostManager Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [LISM Control Access Policy] to objects based on the following: [login process to get access to LogHostManager managed by LISM Control Access Module, 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 authorise 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]

5.1.5.7.FDP_DAU.1/LogHost and LogHostManager 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.

5.1.5.8.FDP_IFC.2 Complete information flow control

FDP_IFC.2.1 The TSF shall enforce the [information flow policy] on [subject with read/write permissions on LogHost directories] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

5.1.5.9.FDP_IFF.1/LogHost and LogHostManager 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: [loghostmanager 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: [logs capture without security attributes and logs export with security attributes, Sha1 with RSA; loghostmanager's sections]

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

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [N/A].

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

5.1.5.10.FIA_UAU.2 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.

5.1.5.11.FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [Insert user login and password] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.5.12.FIA_UID.2 User identification before any action

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.

5.1.5.13.FMT_MSA.3 /LogICA Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [LISM Access Control Policy and information flow policy] to provide [permissive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [any role assigned to the sec-adm section e.g. administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.5.14.FMT_SMF.1 /LogHost and LogHostManager Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [Syslog configuration and management of scheduled tasks performed by LogCapture based on LISM Access Control Policy].

5.1.5.15.FPT_TDC.1/LogHost and LogHostManager 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 and logs] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [SHA-1withRSA and syslog header in logs] when interpreting the TSF data from another trusted IT product.

5.1.5.16.FTP_ITC.1/LogHost and LogHostManager Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another 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 TSF] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [LogHostManager and LISM to authenticate and validate policies via LISM, and Administration/Visualization from Console to LogHostManager under SSL protocol.]

5.1.6.LogSpaces

5.1.6.1.FAU_GEN.1/ LogICA 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 (if applicable), 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].

5.1.6.2.FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.1.6.3.FAU_SAR.1Audit 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.

5.1.6.4.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.

5.1.6.5.FDP_ACF.1 /LogSpaces Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [LISM Access Control Policy] to objects based on the following: [login process to get access to LogSpaces by LISM Control Access Module, 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, then the LISM policy depending on user's role determine if access 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]

5.1.6.6.FDP_ACC.1 /LogSpaces Subset access control

FDP_ACC.1.1 The TSF shall enforce the [LISM Access Control Policy] on [users and all user data managed and kept inside LogSpaces].

5.1.6.7.FMT_MSA.3 /LogICA Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [LISM Access Control Policy and information flow policy] to provide [permissive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [any role assigned to the sec-adm section e.g. administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.6.8.FDP_IFC.1 /LogSpaces Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [information flow control SFP] on [logspaces, logs searching criteria].

5.1.6.9.FDP_IFF.1/LogSpaces 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: [logspaces and serialized objects]

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: [serialized objects and logspaces' sections .]

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

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [N/A].

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

5.1.6.10.FIA_UAU.2 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.

5.1.6.11.FIA_UID.1Timing of identification

FIA_UID.1.1 The TSF shall allow [Insert user login and password] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.6.12.FIA_UID.2 User identification before any action

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

5.1.6.13.FMT_SMF.1/LogSpaces Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [management of forensic cases based on the LISM access control SFP].

5.1.6.14.FPT_TDC.1/LogSpaces Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [xml documents and serialized objects] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2 The TSF shall use [XML-RPC protocol, DTD for specific xml documents and de-serialization of objects] when interpreting the TSF data from another trusted IT product.

5.1.6.15.FTP_ITC.1/LogSpaces Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another 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 TSF] to initiate communication via the trusted channel.
FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [LogSpaces and LISM to authenticate and validate policies via LISM, and Administration/Visualization from Console to LogSpaces under SSL protocol.]

5.1.7.LogReports

5.1.7.1.FAU_GEN.1 / LogICA 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 (if applicable), 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].

5.1.7.2.FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.1.7.3.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.

5.1.7.4.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.

5.1.7.5.FDP_ACF.1/LogReports Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [LISM Access Control Policy] to objects based on the following: [login process to get access to LogReports managed by LISM Control Access Module, 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, then the LISM policy depending on user's role determine if access 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]

5.1.7.6.FDP_ACC.1/LogReports Subset access control

FDP_ACC.1.1 The TSF shall enforce the [LISM Access Control Policy] on [users and all user data managed and kept inside LogReports].

5.1.7.7.FMT_MSA.3 /LogICA Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [LISM Access Control Policy and information flow policy] to provide [permissive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [any role assigned to the sec-adm section e.g. administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.7.8.FDP_IFC.1 /LogReports Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [information flow control SFP] on [LogReports, reporting functions on events].

5.1.7.9.FDP_IFF.1 /LogReports 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: [LogReports]

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: [LogReport's sections]

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

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [N/A].

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

5.1.7.10.FIA_UAU.2 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.

5.1.7.11.FIA_UID.1Timing of identification

FIA_UID.1.1 The TSF shall allow [Insert user login and password] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.7.12.FIA_UID.2 User identification before any action

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

5.1.7.13.FMT_SMF.1 /LogReports Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [management of report groups based on the LISM access control SFP].

5.1.7.14.FPT_TDC.1/LogReports Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [setp and serialized objects] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2 The TSF shall use [SETP protocol and de-serialization of objects] when interpreting the TSF data from another trusted IT product.

5.1.7.15.FTP_ITC.1/LogReports Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another 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 TSF] to initiate communication via the trusted channel.
FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel [for LogReports and LISM to authenticate and validate policies via LISM, and Administration/Visualization from Console to LogReports under SSL protocol.]

5.1.8.Achilles

5.1.8.1.FAU_GEN.1/ LogICA 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 (if applicable), 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].

5.1.8.2.FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.1.8.3.FAU_SAR.1Audit 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.

5.1.8.4.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.

5.1.8.5.FDP_ACF.1 /Achilles Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [LISM Access Control Policy] to objects based on the following: [login process to get access to Achilles managed by LISM Control Access Module, 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 is allowed: [If password hashed equals password stored in password file, then the LISM policy depending on user's role determine if access is allowed.]

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [none]
FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the: [N/A]

5.1.8.6.FDP_ACC.1 /Achilles Subset access control

FDP_ACC.1.1 The TSF shall enforce the [LISM Access Control Policy] on [users and all user data managed and kept inside Achilles].

5.1.8.7.FMT_MSA.3/LogICA Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [LISM Access Control Policy and information flow policy] to provide [permissive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [any role assigned to the sec-adm section e.g. administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.8.8.FDP_IFC.1 /Achilles Subset information flow control

FDP_IFC.1.1 The TSF shall enforce [the information flow control SFP] on [Achilles, vulnerability selection and analisis]

5.1.8.9.FDP_IFF.1 /Achilles 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: [Achilles and serialized objets]

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: [Achille's sections and serialized objects]

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

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [N/A].

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

5.1.8.10.FIA_UAU.2 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.

5.1.8.11.FIA_UID.1Timing of identification

FIA_UID.1.1 The TSF shall allow [Insert user login and password] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.8.12.FIA_UID.2 User identification before any action

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

5.1.8.13.FMT_SMF.1/Achilles Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [update vulnerabilities database based on LISM Access Control Policy].

5.1.8.14.FPT_TDC.1/Achilles Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [xml documents and serialized objects] between the TSF and another trusted IT product.
FPT_TDC.1.2 The TSF shall use [XML-RPC protocol, DTD for specific xml documents and de-serialization of objects] when interpreting the TSF data from another trusted IT product.

5.1.8.15.FTP_ITC.1/Achilles Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another 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 TSF] to initiate communication via the trusted channel.
FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [Achilles and LISM to authenticate and validate policies via LISM, and Administration/Visualization from Console to Achilles under SSL protocol.]

5.1.9.Activos

5.1.9.1.FAU_GEN.1/ LogICA 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 (if applicable), 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].

5.1.9.2.FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.1.9.3.FAU_SAR.1/LogAssets 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.

5.1.9.4.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.

5.1.9.5.FDP_ACF.1 /LogAssets Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [LISM Access Control Policy] to objects based on the following: [login process to get access to LogAssets managed by LISM Control Access Module, 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, then the LISM policy depending on user's role determine if access 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]

5.1.9.6.FDP_ACC.1 /LogAssets Subset access control

FDP_ACC.1.1 The TSF shall enforce the [LISM Access Control Policy] on [users and all user data managed and kept inside LogAssets].

5.1.9.7.FMT_MSA.3 /LogICA Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [LISM Access Control Policy and information flow policy] to provide [permissive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [any role assigned to the sec-adm section e.g. administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.9.8.FDP_IFC.1 /LogAssets Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [information flow control SFP] on [LogAssets, management and selection of assets]

5.1.9.9.FDP_IFF.1 /LogAssets 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: [LogAssets and serialized objects].

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: [LogAssets's sections and serialized objects]

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

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [N/A].

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

5.1.9.10.FIA_UAU.2 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.

5.1.9.11.FIA_UID.1Timing of identification

FIA_UID.1.1 The TSF shall allow [Insert user login and password] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.9.12.FIA_UID.2 User identification before any action

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

5.1.9.13.FMT_SMF.1 /LogAssets Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [management of assets based on LISM Access Control Policy].

5.1.9.14.FPT_TDC.1/LogAssets Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [xml documents and serialized objects] between the TSF and another trusted IT product.
FPT_TDC.1.2 The TSF shall use [XML-RPC protocol, DTD for specific xml documents and de-serialization of objects] when interpreting the TSF data from another trusted IT product.

5.1.9.15.FTP_ITC.1/LogAssets Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another 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 TSF] to initiate communication via the trusted channel.
FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [LogAssets and LISM to authenticate and validate policies via LISM, and Administration/Visualization from Console to LogAssets under SSL protocol.]

5.1.10.LISM

5.1.10.1.FAU_GEN.1/ LogICA 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 (if applicable), 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].

5.1.10.2.FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.1.10.3.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.

5.1.10.4.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.

5.1.10.5.FDP_ACC.1 /LISM Subset access control

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

5.1.10.6.FDP_ACF.1 / LISM Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [LISM Access Control Policy] to objects based on the following: [login process to get access to LISM managed by LISM Control Access Module, 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, then the LISM policy depending on user's role determine if access 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]

5.1.10.7.FDP_ETC.1 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 TOE.

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

5.1.10.8.FDP_ETC.2 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 TOE.
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 TOE, 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 TOE: [None].

5.1.10.9.FDP_IFC.1 / LISM Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [information flow control SFP] on [LISM, management of roles and users]

5.1.10.10.FDP_IFF.1 / LISM 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: [LISM and serialized objects]

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: [LISM's sections and serialized objects]

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

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [N/A].

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

5.1.10.11.FIA_UAU.2 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.

5.1.10.12.FIA_UID.1Timing of identification

FIA_UID.1.1 The TSF shall allow [Insert user login and password] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.10.13.FIA_UID.2 User identification before any action

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

5.1.10.14.FDP_ITC.1 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 TOE.
FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [None]

5.1.10.15.FDP_ITC.2 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 TOE.
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 TOE: [None].

5.1.10.16.FIA_ATD.1/LISM User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [Name, Full name, password, role, email and company].

5.1.10.17.FMT_MSA.1/LISM Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [LISM Access Control Policy] to restrict the ability to [change_default, query, modify, delete] the security attributes [user name, user full name, user password, user role, user email, user company, role name, role's assigned users, role's assigned sections, role's assigned queues, role's assigned file patterns, role's actions, role's assigned group reports] to [role Administrator – a role assigned the sec-adm section].

5.1.10.18.FMT_MSA.3 /LogiCA Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [LISM Access Control Policy and information flow policy] to provide [permissive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [any role assigned to the sec-adm section e.g. administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.10.19.FMT_SMF.1 /LISM Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [management of users and roles based on LISM Access Control Policy].

5.1.10.20.FMT_SMR.1/LISM Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [administrator and operator].
FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.10.21.FPT_TDC.1/LISM Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [property files, LDAP LogICA schema and serialized objects] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2 The TSF shall use [specific property files, specific LDAP LogICA schema and de-serialization of objects] when interpreting the TSF data from another trusted IT product.

5.1.10.22.FTP_ITC.1/LISM Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another 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 TSF] to initiate communication via the trusted channel.
FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel [for LISM, Console, LogAgent, LogAgentManager, LogServer, EventCorrelationEngine, LogReports, LogHostManager, LogSpaces, LogAssetts, Achilles to authenticate and validate policies via LISM, and Administration/Visualization from Console to LISM under SSL protocol].

5.1.11.CuadICA

5.1.11.1.FAU_GEN.1/Cuadica 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 [detailed] 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 (if applicable), 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].

5.1.11.2.FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.1.11.3.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.

5.1.11.4.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.

5.1.11.5.FDP_ACC.1 /Cuadica Subset access control

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

5.1.11.6.FDP_ACF.1 /Cuadica Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [CuadICA Access Control Policy] to objects based on the following: [Login process to get access to CuadICA through web browser or LogICA plugin 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 database field, then the CuadICA policy depending on user's role determine if access is allowed]
FDP_ACF.1.3 The TSF shall explicitly authorise 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]

5.1.11.7.FDP_DAU.1 Cuadica 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 [Reports].
FDP_DAU.1.2 The TSF shall provide [Administration, Reading] with the ability to verify evidence of the validity of the indicated information.

5.1.11.8.FDP_IFC.1 / Cuadica Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [pause, restart, stop] on [CuadICA agent].

5.1.11.9.FDP_IFF.1 / Cuadica 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: [CuadICA agent status].
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: [pause, restart, stop CuadICA agent for information recollection and relay of messages].
FDP_IFF.1.3 The TSF shall enforce the [N/A].
FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [N/A].
FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [N/A].

5.1.11.10.FIA_ATD.1 /Cuadica User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [password, role, rights].

5.1.11.11.FIA_UAU.2 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.

5.1.11.12.FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [Insert user login and password] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.11.13.FIA_UID.2 User identification before any action

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

5.1.11.14.FMT_MSA.1 / Cuadica Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [access control policy] to restrict the ability to [change_default, query, modify, delete] the security attributes [user role] to [Reading, Writing, Administration].

5.1.11.15.FMT_MSA.3 /Cuadica Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [access control policy and information flow policy] to provide [restrictive [role]] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2 The TSF shall allow the [existing authorized roles] to specify alternative initial values to override the default values when an object or information is created.

5.1.11.16.FMT_SMF.1 /Cuadica Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [management of users, roles, companies, standards, metrics and config tools based on access control policy].

5.1.11.17.FMT_SMR.1 /Cuadica Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [administrator].
FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.11.18.FPT_TDC.1 /Cuadica Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [INDI_VALOR – this field represents a bridge between CuadICA database and foreign data sources] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2 The TSF shall use [The field INDI_VALOR of the table indicadores] when interpreting the TSF data from another trusted IT product.

5.1.11.19.FTP_ITC.1/Cuadica Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another 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 TSF] to initiate communication via the trusted channel.
FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [user functions].

5.2. 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 CCV3.1.

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	DEPENDENCIAS
Development	ADV_ARC.1	Security architecture description	ADV_FSP.1 Basic functional specification ADV_TDS.1 Basic design
Development	ADV_FSP.2	Security-enforcing functional specification	ADV_TDS.1 Basic design
Development	ADV_TDS.1	Basic design	ADV_FSP.2 Security-enforcing functional specification
Guidance documents	AGD_OPE.1	Operational user guidance	ADV_FSP.1 Basic functional specification
Guidance documents	AGD_PRE.1	Preparative procedures	No dependencies
Life-Cycle support	ALC_CMC.2	Use of a CM system	ALC_CMS.1 TOE CM coverage
Life-Cycle support	ALC_CMS.2	Parts of the TOE CM coverage	No dependencies
Life-Cycle support	ALC_DEL.1	Delivery procedures	No dependencies
Security Target Evaluation	ASE_CCL.1	Conformance claims	ASE_INT.1 ST introduction ASE_ECD.1 Extended components definition ASE_REQ.1 Stated security requirements
Security Target Evaluation	ASE_ECD.1	Extended components definition	No dependencies
Security Target Evaluation	ASE_INT.1	ST introduction	No dependencies
Security Target Evaluation	ASE_OBJ.2	Security objectives	ASE_SPD.1 Security problem definition
Security Target Evaluation	ASE_REQ.2	Derived security requirements	ASE_OBJ.2 Security objectives ASE_ECD.1 Extended components definition
Security Target Evaluation	ASE_SPD.1	Security problem definition	No dependencies
Security Target Evaluation	ASE_TSS.1	TOE summary specification	ASE_INT.1 ST introduction ASE_REQ.1 Stated security requirements ADV_FSP.1 Basic functional specification
Test	ATE_COV.1	Evidence of coverage	ADV_FSP.2 Security-enforcing functional specification ATE_FUN.1 Functional testing
Test	ATE_FUN.1	Functional testing	ATE_COV.1 Evidence of coverage
Test	ATE_IND.2	Independent testing - sample	ADV_FSP.2 Security-enforcing functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures ATE_COV.1 Evidence of coverage ATE_FUN.1 Functional testing
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis	ADV_ARC.1 Security architecture description ADV_FSP.1 Basic functional specification ADV_TDS.1 Basic design AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures

Tabla 3 - Security Assurance Requirements for EAL2

5.3. Security requirements rationale

El razonamiento de los requisitos de seguridad necesarios, se encuentra detallado en el apartado 6.1 de esta Declaración de Seguridad.

6.TOE Summary specification

6.1.TOE summary specification

En este apartado se expone por qué 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.

6.1.1.Justificación para los SFRs

6.1.1.1.Justificación para la iteración LogICA

FAU_GEN.1/ LogICA Audit data generation, cubierto por la generación de datos de auditoría para LogAgent, LogAgentManager, LogServer, EventCorrelator, LogHost, LogHostManager, LogSpaces, LogReports, Achilles, Activos y LISM.

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

6.1.1.2.Justificación para la iteración LogAgent LogAgentManager

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

FDP_ACC.1/LogAgent and LogAgentManager Subset access control, política LISM de acceso al TOE.

FDP_IFC.1/LogAgent and LogAgentManager Subset information flow control, permite la importar y exportar la información recogida por las fuentes de logs, y el envío y recepción de objetos serializados entre el LogAgent, LogAgentManager, Console y LISM.

FDP_IFF.1/LogAgent and LogAgentManager Simple security attributes, permite la posibilidad de configurar las reglas de adquisición de logs desde las fuentes de log, y la ejecución de las diferentes funcionalidades basándose en las políticas de acceso del Lism.

FMT_SMF.1/LogAgent and LogAgentManager Specification of Management Functions, el TOE proporciona capacidad de administración de los agentes para cada usuario basándose en las políticas de acceso del LISM.

FPT_TDC.1/LogAgent and LogAgentManager Inter-TSF basic TSF data consistency, el TOE es capaz de identificar e interpretar eventos basados en fuentes de log.

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

6.1.1.3.Justificación para la iteración LogServer

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

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

FDP_IFC.1/LogServer Subset information flow control permite importar y exportar la eventos recogidos por Logserver, y el envío y recepción de objetos serializados entre el LogServer, Console y LISM.

FDP_IFF.1/LogServer Simple security attributes permite la posibilidad de configurar las reglas de adquisición de eventos desde el LogServer y la ejecución de las diferentes funcionalidades basándose en las políticas de acceso del LISM.

FMT_SMF.1/LogServer Specification of Management Functions, el TOE proporciona capacidad de administración del motor del Logserver basándose en las políticas de acceso del LISM.

FPT_TDC.1/LogServer Inter-TSF basic TSF data consistency, el TOE es capaz de identificar e interpretar eventos basados en fuentes de log y objetos serializados para el tratamiento de incidentes y recomendaciones.

FTP_ITC.1/LogServer Inter-TSF trusted channel, el canal seguro entre los módulos LogServer, EventCorrelator, bus JMS y LISM se asegura mediante el establecimiento de una conexión SSL.

6.1.1.4.Justificación para la iteración EventCorrelator

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

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

FDP_IFC.1/EventCorrelator Subset information flow control permite importar y exportar la eventos recogidos por EventCorrelator, y el envío y recepción de objetos serializados entre el EventCorrelator, LogServer, Console y LISM.

FDP_IFF.1/EventCorrelator Simple security attributes permite la posibilidad de configurar las reglas de adquisición de eventos desde el EventCorrelator y la ejecución de las diferentes funcionalidades basándose en las políticas de acceso del LISM.

FMT_SMF.1/EventCorrelator Specification of Management Functions, el TOE proporciona capacidad de administración del motor del EventCorrelator basándose en las políticas de acceso del Lism.

FPT_TDC.1/EventCorrelator Inter-TSF basic TSF data consistency, el TOE es capaz de identificar e interpretar eventos basados en fuentes de log y objetos serializados para el tratamiento de incidentes.

FTP_ITC.1/EventCorrelator Inter-TSF trusted channel, el canal seguro entre los módulos LogServer, EventCorrelator, bus JMS y LISM se asegura mediante el establecimiento de una conexión SSL.

6.1.1.5.Justificación para la iteración Console

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

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

FDP_IFC.1/Console Subset information flow control permite importar y exportar la eventos recogidos por EventCorrelator y LogServer, y el envío y recepción de objetos serializados entre el LogAssets, LogSpaces, EventCorrelator, LogServer, LogReports, Achilles y LISM.

FDP_IFF.1/Console Simple security attributes permite la posibilidad de configurar las reglas de adquisición de eventos desde el EventCorrelator y LogServer via JMS, y la ejecución de las diferentes funcionalidades, de cada módulo, basándose en las políticas de acceso del LISM.

FTP_ITC.1/ Console Inter-TSF trusted channel, el canal seguro entre los módulos Console, LISM, Achilles, Assets, LogAgentManager, EventCorrelator, LogServer, LogSpaces, LogReports, Cuadica, JMS bus, Ntop; y utilidades como: nmap and nessus; se asegura mediante el establecimiento de una conexión SSL.

6.1.1.6.Justificación para la iteración LogHost and LogHostManager

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

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

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

FDP_IFF.1/ LogHost and LogHostManager Simple security attributes permite la posibilidad de configurar las reglas de adquisición de logs, desde el Syslog y las fuentes originales, y la ejecución de las diferentes funcionalidades del LogHostManager, basándose en las políticas de acceso del LISM.

FMT_SMF.1/ LogHost and LogHostManager Specification of Management Functions, el TOE proporciona capacidad de administración del Syslog, y las reglas de captura de logs, basándose en las políticas de acceso del LISM.

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

FTP_ITC.1/ LogHost and LogHostManager Inter-TSF trusted channel, el canal seguro entre los módulos LogHostManager, Console y LISM, mediante el establecimiento de una conexión SSL.

6.1.1.7.Justificación para la iteración LogSpaces

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

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

FDP_IFC.1/ LogSpaces Subset information flow control permite el envío y recepción de objetos serializados entre LogSpaces, Console y LISM.

FDP_IFF.1/ LogSpaces Simple security attributes permite la ejecución de las diferentes funcionalidades basándose en las políticas de acceso del LISM.

FMT_SMF.1/ LogSpaces Specification of Management Functions, el TOE proporciona capacidad de administración de casos forenses basándose en las políticas de acceso del LISM.

FPT_TDC.1/ LogSpaces Inter-TSF basic TSF data consistency, el TOE es capaz de identificar e interpretar eventos basados en fuentes de log y objetos serializados para el envío y recepción de consultas de log.

FTP_ITC.1/ LogSpaces Inter-TSF trusted channel, el canal seguro entre los módulos LogSpaces, Console y LISM se asegura mediante el establecimiento de una conexión SSL.

6.1.1.8.Justificación para la iteración LogReports

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

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

FDP_IFC.1/ LogReports Subset information flow control permite el envío y recepción de objetos serializados entre LogReports, Console y LISM.

FDP_IFF.1/ LogReports Simple security attributes permite la ejecución de las diferentes funcionalidades basándose en las políticas de acceso del LISM.

FMT_SMF.1/ LogReports Specification of Management Functions, el TOE proporciona capacidad de administración de grupos de informes basándose en las políticas de acceso del LISM.

FPT_TDC.1/ LogReports Inter-TSF basic TSF data consistency, el TOE es capaz de interpretar objetos serializados para el envío y recepción de eventos sobre fuentes de log, incidentes, recomendaciones y activos.

FTP_ITC.1/ LogReports Inter-TSF trusted channel, el canal seguro entre los módulos LogReports, Console y LISM se asegura mediante el establecimiento de una conexión SSL.

6.1.1.9.Justificación para la iteración Achilles

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

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

FDP_IFC.1/ Achilles Subset information flow control permite el envío y recepción de objetos serializados y documentos xml entre Achilles, Console y LISM.

FDP_IFF.1/ Achilles Simple security attributes permite la ejecución de las diferentes funcionalidades basándose en las políticas de acceso del LISM.

FMT_SMF.1/ Achilles Specification of Management Functions, el TOE proporciona capacidad de administración de bases de datos de vulnerabilidades basándose en las políticas de acceso del LISM.

FPT_TDC.1/ Achilles Inter-TSF basic TSF data consistency, el TOE es capaz de interpretar objetos serializados y documentos xml para el envío/búsqueda de análisis de vulnerabilidades.

FTP_ITC.1/ LogReports Inter-TSF trusted channel, el canal seguro entre los módulos Achilles, Console y LISM se asegura mediante el establecimiento de una conexión SSL.

6.1.1.10.Justificación para la iteración LogAssets

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

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

FDP_IFC.1/ LogAssets Subset information flow control permite el envío y recepción de objetos serializados entre LogAssets, Console y LISM.

FDP_IFF.1/ LogAssets Simple security attributes permite la ejecución de las diferentes funcionalidades basándose en las políticas de acceso del LISM.

FMT_SMF.1/ LogAssets Specification of Management Functions, el TOE proporciona capacidad de administración de activos basándose en las políticas de acceso del LISM.

FPT_TDC.1/ LogAssets Inter-TSF basic TSF data consistency, el TOE es capaz de interpretar objetos serializados para el envío y recepción de activos.

FTP_ITC.1/ LogAssets Inter-TSF trusted channel, el canal seguro entre los módulos LogAssets, Console y LISM se asegura mediante el establecimiento de una conexión SSL.

6.1.1.11.Justificación para la iteración LISM

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

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

FDP_IFC.1/ LISM Subset information flow control permite el envío y recepción de objetos serializados entre Console y LISM.

FDP_IFF.1/ LISM Simple security attributes permite la ejecución de las diferentes funcionalidades basándose en las políticas de acceso del LISM.

FIA_ATD.1/ LISM User attribute definition, el TOE almacena y mantiene los atributos que caracterizan a cada usuario (password y rol) y a cada rol (section, file-pattern, report group, queue y action).

FMT_MSA.1/ LISM Management of security attributes, permite la posibilidad de gestionar (añadir, borrar o modificar) los atributos que caracterizan a los usuarios

(nombre, password, rol, email, company), a los roles (usuarios, secciones, queues, file-patterns, report groups y acciones).

FMT_SMF.1/ LISM Specification of Management Functions, el TOE proporciona capacidad de administración de usuarios y roles basándose en las políticas de acceso del LISM.

FMT_SMR.1/ LISM Security roles, el TOE mantiene los diferentes usuarios (administrador, operador …).

FPT_TDC.1/ LISM Inter-TSF basic TSF data consistency, el TOE es capaz de interpretar ficheros de propiedades, esquemas LDAP de LogICA y objetos serializados para el envío y recepción de usuarios y roles.

FTP_ITC.1/ LogAssets Inter-TSF trusted channel, el canal seguro entre los módulos LISM, Console, LogAgent, LogAgentManager, LogServer, EventCorrelationEngine, LogReports, LogHostManager, LogSpaces, LogAssetts, Achilles se asegura mediante el establecimiento de una conexión SSL.

6.1.1.12.Justificación para la iteración CuadICA

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

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

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

FDP_DAU.1/ CuadICA Basic Data Authentication, el TOE es capaz de aportar evidencias de la integridad de los registros en base de datos correspondiente a los informes generados.

FDP_IFC.1/ CuadICA Subset information flow control permitirá la gestión del agente para la extracción de datos.

FDP_IFF.1/ CuadICA Simple security attributes permite la ejecución de las diferentes funcionalidades del agente basándose en las políticas de acceso de CuadICA.

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

FMT_MSA.1/ CuadICA Management of security attributes, permite la posibilidad de gestionar (añadir, borrar o modificar) los atributos que caracterizan a los usuarios y a los roles.

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

FMT_SMF.1/ CuadICA Specification of Management Functions, el TOE proporciona capacidad de administración de usuarios y roles basándose en las políticas de acceso de CuadICA.

FMT_SMR.1/ CuadICA Security roles, el TOE mantiene los diferentes usuarios (administrador …).

FPT_TDC.1/ CuadICA Inter-TSF basic TSF data consistency, el TOE es capaz de importar fuentes de datos provenientes de otros sistemas externos.

FTP_ITC.1/ CuadICA Inter-TSF trusted channel, el canal seguro de CuadICA se asegura mediante el establecimiento de una conexión SSL.

6.1.2. 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.

6.1.2.1. LogAgent y LogAgentManager

LogAgent y LogAgentManager	O.LOG	O.ROLE	O.AUTHENTICITY	O.SECURECOM	O.INDATA
FAU_GEN.1 Audit data generation	x	o	o	o	o
FPT_STM.1 Reliable time stamps	x	o	o	o	o
FAU_SAR.1 Audit review	x	o	o	o	o
FAU_SAR.2 Restricted audit review	x	o	o	o	o
FDP_ACF.1 Security attribute based access control	o	x	o	o	o
FDP_ACC.1 Subset access control	o	x	o	o	o
FMT_MSA.3 Static attribute initialisation	o	x	o	o	o
FDP_IFC.1 Subset information flow control	o	o	o	o	x
FDP_IFF.1 Simple security attributes	o	x	o	o	o
FIA_UAU.2 User authentication before any action	o	x	o	o	o
FIA_UID.1 Timing of identification	o	x	o	o	o
FIA_UID.2 User identification before any action	o	x	o	o	o
FMT_SMF.1 Specification of Management Functions	o	x	o	o	o
FPT_TDC.1 Inter-TSF basic TSF data consistency	o	o	o	o	x
FTP_ITC.1 Inter-TSF trusted channel	o	o	o	x	o

Tabla 4 - Objetivos vs. SFR's LogAgent y LogAgentManager

6.1.2.2. LogServer

LogServer	O.LOG	O.ROLE	O.AUTHENTICITY	O.SECURECOM	O.INDATA
FAU_GEN.1 Audit data generation	x	o	o	o	o
FPT_STM.1 Reliable time stamps	x	o	o	o	o
FAU_SAR.1 Audit review	x	o	o	o	o
FAU_SAR.2 Restricted audit review	x	o	o	o	o
FDP_ACF.1 Security attribute based access control	o	x	o	o	o
FDP_ACC.1 Subset access control	o	x	o	o	o
FMT_MSA.3 Static attribute initialisation	o	x	o	o	o
FDP_IFC.1 Subset information flow control	o	o	o	o	x
FDP_IFF.1 Simple security attributes	o	x	o	o	o
FMT_SMF.1 Specification of Management Functions	o	x	o	o	o
FPT_TDC.1 Inter-TSF basic TSF data consistency	o	o	o	o	x
FTP_ITC.1 Inter-TSF trusted channel	o	o	o	x	o

Tabla 5 - Objetivos vs. SFR's LogServer

6.1.2.3.EventCorrelator

EventCorrelator	O.LOG	O.ROLE	O.AUTHENTICITY	O.SECURECOM	O.INDATA
FAU_GEN.1 Audit data generation	x	o	o	o	o
FPT_STM.1 Reliable time stamps	x	o	o	o	o
FAU_SAR.1 Audit review	x	o	o	o	o
FDP_ACF.1 Security attribute based access control	o	x	o	o	o
FDP_ACC.1 Subset access control	o	x	o	o	o
FMT_MSA.3 Static attribute initialisation	o	x	o	o	o
FDP_IFC.1 Subset information flow control	o	o	o	o	x
FDP_IFF.1 Simple security attributes	o	x	o	o	o
FIA_UAU.2 User authentication before any action	o	x	o	o	o
FIA_UID.1 Timing of identification	o	x	o	o	o
FIA_UID.2 User identification before any action	o	x	o	o	o
FMT_SMF.1 Specification of Management Functions	o	x	o	o	o
FPT_TDC.1 Inter-TSF basic TSF data consistency	o	o	o	o	x
FTP_ITC.1 Inter-TSF trusted channel	o	o	o	x	o

Tabla 6 - Objetivos vs. SFR's EventCorrelator

6.1.2.4.Console

Console	O.LOG	O.ROLE	O.AUTHENTICITY	O.SECURECOM	O.INDATA
FDP_ACF.1 Security attribute based access control	o	x	o	o	o
FDP_ACC.1 Subset access control	o	x	o	o	o
FMT_MSA.3 Static attribute initialisation	o	x	o	o	o
FDP_IFC.1 Subset information flow control	o	o	o	o	x
FDP_IFF.1 Simple security attributes	o	x	o	o	o
FIA_UAU.2 User authentication before any action	o	x	o	o	o
FIA_UID.1 Timing of identification	o	x	o	o	o
FIA_UID.2 User identification before any action	o	x	o	o	o
FTP_ITC.1 Inter-TSF trusted channel	o	o	o	x	o

Tabla 7 - Objetivos vs. SFR's Console

6.1.2.5.LogHost y LogHostManager

LogHost y LogHostManager	O.LOG	O.ROLE	O.AUTHENTICITY	O.SECURECOM	O.INDATA
FAU_GEN.1 Audit data generation	x	o	o	o	o
FPT_STM.1 Reliable time stamps	x	o	o	o	o
FAU_SAR.1 Audit review	x	o	o	o	o
FAU_SAR.2 Restricted audit review	x	o	o	o	o
FDP_ACC.2 Complete access control	o	x	o	o	o
FDP_ACF.1 Security attribute based access control	o	x	o	o	o
FDP_DAU.1 Basic Data Authentication	o	o	x	o	o
FDP_IFC.2 Complete information flow control	o	o	o	o	x
FDP_IFF.1 Simple security attributes	o	x	o	o	o
FIA_UAU.2 User authentication before any action	o	x	o	o	o
FIA_UID.1 Timing of identification	o	x	o	o	o

FIA_UID.2 User identification before any action	o	x	o	o	o
FIA_UAU.2 User authentication before any action	o	x	o	o	o
FIA_UID.1 Timing of identification	o	x	o	o	o
FIA_UID.2 User identification before any action	o	x	o	o	o
FMT_SMF.1 Specification of Management Functions	o	x	o	o	o
FPT_TDC.1 Inter-TSF basic TSF data consistency	o	o	o	o	x
FTP_ITC.1 Inter-TSF trusted channel	o	o	o	x	o

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

6.1.2.6.LogSpaces

LogSpaces	O.LOG	O.ROLE	O.AUTHENTICITY	O.SECURECOM	O.INDATA
FAU_GEN.1 Audit data generation	x	o	o	o	o
FPT_STM.1 Reliable time stamps	x	o	o	o	o
FAU_SAR.1 Audit review	x	o	o	o	o
FAU_SAR.2 Restricted audit review	x	o	o	o	o
FDP_ACF.1 Security attribute based access control	o	x	o	o	o
FDP_ACC.1 Subset access control	o	x	o	o	o
FMT_MSA.3 Static attribute initialisation	o	x	o	o	o
FDP_IFC.1 Subset information flow control	o	o	o	o	x
FDP_IFF.1 Simple security attributes	o	x	o	o	o
FIA_UAU.2 User authentication before any action	o	x	o	o	o
FIA_UID.1 Timing of identification	o	x	o	o	o
FIA_UID.2 User identification before any action	o	x	o	o	o
FMT_SMF.1 Specification of Management Functions	o	x	o	o	o
FPT_TDC.1 Inter-TSF basic TSF data consistency	o	o	o	o	x
FTP_ITC.1 Inter-TSF trusted channel	o	o	o	x	o

Tabla 9 - Objetivos vs. SFR's LogHost y LogHostManager

6.1.2.7.LogReports

LogReports	O.LOG	O.ROLE	O.AUTHENTICITY	O.SECURECOM	O.INDATA
FAU_GEN.1 Audit data generation	x	o	o	o	o
FPT_STM.1 Reliable time stamps	x	o	o	o	o
FAU_SAR.1 Audit review	x	o	o	o	o
FAU_SAR.2 Restricted audit review	x	o	o	o	o
FDP_ACF.1 Security attribute based access control	o	x	o	o	o
FDP_ACC.1 Subset access control	o	x	o	o	o
FMT_MSA.3 Static attribute initialisation	o	x	o	o	o
FDP_IFC.1 Subset information flow control	o	o	o	o	x
FDP_IFF.1 Simple security attributes	o	x	o	o	o
FIA_UAU.2 User authentication before any action	o	x	o	o	o
FIA_UID.1 Timing of identification	o	x	o	o	o
FIA_UID.2 User identification before any action	o	x	o	o	o
FMT_SMF.1 Specification of Management Functions	o	x	o	o	o
FPT_TDC.1 Inter-TSF basic TSF data consistency	o	o	o	o	x
FTP_ITC.1 Inter-TSF trusted channel	o	o	o	x	o

Tabla 10 - Objetivos vs. SFR's LogHost y LogHostManager

6.1.2.8.Achilles

Achilles	O.LOG	O.ROLE	O.AUTHENTICITY	O.SECURECOM	O.INDATA
FAU_GEN.1 Audit data generation	x	o	o	o	o
FPT_STM.1 Reliable time stamps	x	o	o	o	o
FAU_SAR.1 Audit review	x	o	o	o	o
FAU_SAR.2 Restricted audit review	x	o	o	o	o
FDP_ACF.1 Security attribute based access control	o	x	o	o	o
FDP_ACC.1 Subset access control	o	x	o	o	o
FMT_MSA.3 Static attribute initialisation	o	x	o	o	o
FDP_IFC.1 Subset information flow control	o	o	o	o	x
FDP_IFF.1 Simple security attributes	o	x	o	o	o
FIA_UAU.2 User authentication before any action	o	x	o	o	o
FIA_UID.1 Timing of identification	o	x	o	o	o
FIA_UID.2 User identification before any action	o	x	o	o	o
FMT_SMF.1 Specification of Management Functions	o	x	o	o	o
FPT_TDC.1 Inter-TSF basic TSF data consistency	o	o	o	o	x
FTP_ITC.1 Inter-TSF trusted channel	o	o	o	x	o

Tabla 11 - Objetivos vs. SFR's Achilles

6.1.2.9.Activos

Activos	O.LOG	O.ROLE	O.AUTHENTICITY	O.SECURECOM	O.INDATA
FAU_GEN.1 Audit data generation	x	o	o	o	o
FPT_STM.1 Reliable time stamps	x	o	o	o	o
FAU_SAR.1 Audit review	x	o	o	o	o
FAU_SAR.2 Restricted audit review	x	o	o	o	o
FDP_ACF.1 Security attribute based access control	o	x	o	o	o
FDP_ACC.1 Subset access control	o	x	o	o	o
FMT_MSA.3 Static attribute initialisation	o	x	o	o	o
FDP_IFC.1 Subset information flow control	o	o	o	o	x
FDP_IFF.1 Simple security attributes	o	x	o	o	o
FIA_UAU.2 User authentication before any action	o	x	o	o	o
FIA_UID.1 Timing of identification	o	x	o	o	o
FIA_UID.2 User identification before any action	o	x	o	o	o
FMT_SMF.1 Specification of Management Functions	o	x	o	o	o
FPT_TDC.1 Inter-TSF basic TSF data consistency	o	o	o	o	x
FTP_ITC.1 Inter-TSF trusted channel	o	o	o	x	o

Tabla 12 - Objetivos vs. SFR's Activos

6.1.2.10.LISM

LISM	O.LOG	O.ROLE	O.AUTHENTICITY	O.SECURECOM	O.INDATA
FAU_GEN.1 Audit data generation	x	o	o	o	o
FPT_STM.1 Reliable time stamps	x	o	o	o	o

FAU_SAR.1 Audit review	x	o	o	o	o
FAU_SAR.2 Restricted audit review	x	o	o	o	o
FDP_ACC.1 Subset access control	o	x	o	o	o
FDP_ACF.1 Security attribute based access control	o	x	o	o	o
FDP_ETC.1 Export of user data without security attributes	o	o	o	o	x
FDP_ETC.2 Export of user data with security attributes	o	o	o	o	x
FDP_IFC.1 Subset information flow control	o	o	o	o	x
FDP_IFF.1 Simple security attributes	o	x	o	o	o
FIA_UAU.2 User authentication before any action	o	x	o	o	o
FIA_UID.1 Timing of identification	o	x	o	o	o
FIA_UID.2 User identification before any action	o	x	o	o	o
FDP_ITC.1 Import of user data without security attributes	o	o	o	o	x
FDP_ITC.2 Import of user data with security attributes	o	o	o	o	x
FIA_ATD.1 User attribute definition	o	x	o	o	o
FMT_MSA.1 Management of security attributes	o	x	o	o	o
FMT_MSA.3 Static attribute initialisation	o	x	o	o	o
FMT_SMF.1 Specification of Management Functions	o	x	o	o	o
FMT_SMR.1 Security roles	o	x	o	o	o
FPT_TDC.1 Inter-TSF basic TSF data consistency	o	o	o	o	x
FTP_ITC.1 Inter-TSF trusted channel	o	o	o	x	o

Tabla 13 - Objetivos vs. SFR's LISM

6.1.2.11.CuadICA

CuadICA	O.LOG	O.ROLE	O.AUTHENTICITY	O.SECURECOM	O.INDATA
FAU_GEN.1 Audit data generation	x	o	o	o	o
FPT_STM.1 Reliable time stamps	x	o	o	o	o
FAU_SAR.1 Audit review	x	o	o	o	o
FAU_SAR.2 Restricted audit review	x	o	o	o	o
FDP_ACC.1 Subset access control	o	x	o	o	o
FDP_ACF.1 Security attribute based access control	o	x	o	o	o
FDP_DAU.1 Basic Data Authentication	o	o	x	o	o
FDP_IFC.1 Subset information flow control	o	o	o	o	x
FDP_IFF.1 Simple security attributes	o	X	o	o	o
FIA_ATD.1 User attribute definition	o	X	o	o	o
FIA_UAU.2 User authentication before any action	o	X	o	o	o
FIA_UID.1 Timing of identification	o	X	o	o	o
FIA_UID.2 User identification before any action	o	X	o	o	o
FMT_MSA.1 Management of security attributes	o	X	o	o	o
FMT_MSA.3 Static attribute initialisation	o	X	o	o	o
FMT_SMF.1 Specification of Management Functions	o	X	o	o	o
FMT_SMR.1 Security roles	o	x	o	o	o
FPT_TDC.1 Inter-TSF basic TSF data consistency	o	o	o	o	x
FTP_ITC.1 Inter-TSF trusted channel	o	o	o	x	o

Tabla 14 - Objetivos vs. SFR's CuadICA

6.1.3.Selección de Requisitos Funcionales de Seguridad para el TOE

Para la selección de los requisitos de seguridad del catalogo de CCV3.1 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.

6.1.3.1.LogAgent y LogAgentManager

O.LOG
Cada uno de los módulos audita, generación de ficheros de log, las conexiones realizadas por los diferentes usuarios y los intentos de conexión de accesos al TOE, este objetivo está cubierto por FAU_GEN.1 Audit data generation. La información de auditoria:

- puede ser consultada, objetivo cubierto por FAU_SAR.1 Audit review, por usuarios con permiso de lectura en el directorio de generación de logs, este objetivo está cubierto por FAU_SAR.2 Restricted audit review.

- muestra la fecha y hora, precisa, para el seguimiento de eventos de log, objetivo cubierto por FPT_STM.1 Reliable time stamps.

O.ROLE
La política de control de acceso al TOE, centralizada en el módulo LISM, incluye:

- Autenticación de usuarios, basados en rol y password. La hash de la password, SHA-1, debe coincidir con la almacenada en el LISM, este objetivo está cubierto por FDP_ACF.1 Security attribute based access control. La inserción del identificador de usario y password precederá a cualquier otra acción en el TOE, este objetivo está cubierto por FIA_UAU.2 User authentication before any action, FIA_UID.1 Timing of identification y FIA_UID.2 User authentication before any action.

- Segregación de funciones del TOE. Las políticas de control de acceso, definidas como secciones, pueden asignarse a roles, que a su vez pueden asignarse a usuarios, este objetivo está cubierto FDP_ACC.1. Subset access control. Las asignaciones pueden contar con valores iniciales y por defecto durante la instalación del TOE, dichos valores pueden ser modificados por cualquier rol con la sección sec-adm, normalmente Administrador, objetivo cubierto por FMT_MSA.3 Static attribute initialization.

- Administración de agentes y configuración de atributos de auditoria, objetivo cubierto por FMT_SMF.1 Specification of Management Functions.

- Propiedades de log y determinadas secciones de un rol, que afectan a la política de flujo de información, objetivo cubierto por FDP_IFF.1 Simple security attributes.

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 Inter-TSF trusted channel, el cual asegura la comunicación utilizando el protocolo SSL.

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, eventos bajo protocolo SETP, u otra aplicación externa. Para modelar el input y cubrir el objetivo entrada de datos, se ha utilizado el requisito FDP_IFC.1 Subset information flow control, FPT_TDC.1 Inter-TSF basic TSF data consistency.

6.1.3.2.LogServer

O.LOG
Cada uno de los módulos audita, generación de ficheros de log, las conexiones realizadas por los diferentes usuarios y los intentos de conexión de accesos al TOE, este objetivo está cubierto por FAU_GEN.1 Audit data generation. La información de auditoría:

- puede ser consultada, objetivo cubierto por FAU_SAR.1 Audit review, por usuarios con permiso de lectura en el directorio de generación de logs, este objetivo está cubierto por FAU_SAR.2 Restricted audit review.

- muestra la fecha y hora, precisa, para el seguimiento de eventos de log, objetivo cubierto por FPT_STM.1 Reliable time stamps.

O.ROLE
La política de control de acceso al TOE, centralizada en el módulo LISM, incluye:

- Autenticación de usuarios, basados en rol y password. La hash de la password, SHA-1, debe coincidir con la almacenada en el LISM, este objetivo está cubierto por FDP_ACF.1 Security attribute based access control.

- Segregación de funciones del TOE. Las políticas de control de acceso, definidas como secciones, pueden asignarse a roles, que a su vez pueden asignarse a usuarios, este objetivo está cubierto FDP_ACC.1. Subset access control. Las asignaciones pueden contar con valores iniciales y por defecto durante la instalación del TOE, dichos valores pueden ser modificados por cualquier rol con la sección sec-adm, normalmente Administrador, objetivo cubierto por FMT_MSA.3 Static attribute initialization.

- Administración del motor de colección de eventos y configuración de atributos de auditoría, objetivo cubierto por FMT_SMF.1 Specification of Management Functions.

- Adición de colas, reglas de adquisición de eventos y determinadas secciones de rol, que afectan a la política de flujo de información, objetivo cubierto por FDP_IFF.1 Simple security attributes.

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 Inter-TSF trusted channel, el cual asegura la comunicación utilizando el protocolo SSL.

O.INDATA
En el caso de LogServer los datos de entrada son capturados bajo protocolo SETP, y transmitidos por el bus JMS y por objetos serializados, es por ello que para cubrir O.INDATA se utiliza FDP_IFC.1 Subset information flow control, FPT_TDC.1 Inter-TSF basic TSF data consistency.

6.1.3.3.EventCorrrelator

O.LOG
Cada uno de los módulos audita, generación de ficheros de log, las conexiones realizadas por los diferentes usuarios y los intentos de conexión de accesos al TOE, este objetivo está cubierto por FAU_GEN.1 Audit data generation. La información de auditoría:

- puede ser consultada, objetivo cubierto por FAU_SAR.1 Audit review, por usuarios con permiso de lectura en el directorio de generación de logs, este objetivo está cubierto por FAU_SAR.2 Restricted audit review.

- muestra la fecha y hora, precisa, para el seguimiento de eventos de log, objetivo cubierto por FPT_STM.1 Reliable time stamps.

O.ROLE
La política de control de acceso al TOE, centralizada en el módulo LISM, incluye:

- Autenticación de usuarios, basados en rol y password. La hash de la password, SHA-1, debe coincidir con la almacenada en el LISM, este objetivo está cubierto por FDP_ACF.1 Security attribute based access control. La inserción del identificador de usario y password precederá a cualquier otra acción en el TOE, este objetivo está cubierto por FIA_UAU.2 User authentication before any action, FIA_UID.1 Timing of identification y FIA_UID.2 User authentication before any action.

- Segregación de funciones del TOE. Las políticas de control de acceso, definidas como secciones, pueden asignarse a roles, que a su vez pueden asignarse a usuarios, este objetivo está cubierto FDP_ACC.1. Subset access control. Las asignaciones pueden contar con valores iniciales y por defecto durante la instalación del TOE, dichos valores pueden ser modificados por cualquier rol con la sección sec-adm, normalmente Administrador, objetivo cubierto por FMT_MSA.3 Static attribute initialization.

- Administración del motor de correlación de eventos y configuración de atributos de auditoria, objetivo cubierto por FMT_SMF.1 Specification of Management Functions.

- Adición de reglas de adquisición de eventos y determinadas secciones de rol, que afectan a la política de flujo de información, objetivo cubierto por FDP_IFF.1 Simple security attributes.

O.SECURECOM
Todas las comunicaciones entre módulos del TOE se realizan mediante la asociación de canales seguros. En el caso de EvenCorrelator este objetivo está cubierto por FTP_ITC.1 Inter-TSF trusted channel, el cual asegura la comunicación utilizando el protocolo SSL.

O.INDATA
En el caso de EventCorrelator los datos de entrada son capturados por bus JMS y transmitidos por el bus JMS y por objetos serializados, es por ello que para cubrir O.INDATA se utiliza FDP_IFC.1 Subset information flow control, FPT_TDC.1 Inter-TSF basic TSF data consistency.

6.1.3.4.Console

O.ROLE
La política de control de acceso al TOE, centralizada en el módulo LISM, incluye:

- Autenticación de usuarios, basados en rol y password. La hash de la password, SHA-1, debe coincidir con la almacenada en el LISM, este objetivo está cubierto por FDP_ACF.1 Security attribute based access control. La inserción del identificador de usario y

password precederá a cualquier otra acción en el TOE, este objetivo está cubierto por FIA_UAU.2 User authentication before any action y FIA_UID.1 Timing of identification y FIA_UID.2 User authentication before any action.

- Segregación de funciones del TOE. Las políticas de control de acceso, definidas como secciones, pueden asignarse a roles, que a su vez pueden asignarse a usuarios, este objetivo está cubierto FDP_ACC.1. Subset access control. Las asignaciones pueden contar con valores iniciales y por defecto durante la instalación del TOE, dichos valores pueden ser modificados por cualquier rol con la sección sec-adm, normalmente Administrador, objetivo cubierto por FMT_MSA.3 Static attribute initialization.

- Adición de colas, patrones de log, grupos de informes y secciones de rol, que afectan a la política de flujo de información, objetivo cubierto por FDP_IFF.1 Simple security attributes.

O.SECURECOM
Todas las comunicaciones entre módulos del TOE se realizan mediante la asociación de canales seguros. En el caso de Console este objetivo está cubierto por FTP_ITC.1 Inter-TSF trusted channel, el cual asegura todas las comunicaciones utilizando el protocolo SSL.

O.INDATA
En el caso de Console los datos de entrada son transmitidos por el bus JMS, así como objetos serializados y documentos xml, es por ello que para cubrir O.INDATA se utiliza FDP_IFC.1 Subset information flow control.

6.1.3.5. LogHost y LogHostManager

O.LOG
Cada uno de los módulos audita, generación de ficheros de log, las conexiones realizadas por los diferentes usuarios y los intentos de conexión de accesos al TOE, este objetivo está cubierto por FAU_GEN.1 Audit data generation. La información de auditoría:

- puede ser consultada, objetivo cubierto por FAU_SAR.1 Audit review, por usuarios con permiso de lectura en el directorio de generación de logs, este objetivo está cubierto por FAU_SAR.2 Restricted audit review.

- muestra la fecha y hora, precisa, para el seguimiento de eventos de log, objetivo cubierto por FPT_STM.1 Reliable time stamps.

O.ROLE
La política de control de acceso al TOE, centralizada en el módulo LISM, incluye:

- Autenticación de usuarios, basados en rol y password. La hash de la password, SHA-1, debe coincidir con la almacenada en el LISM, este objetivo está cubierto por FDP_ACF.1 Security attribute based access control. La inserción del identificador de usario y password precederá a cualquier otra acción en el TOE, este objetivo está cubierto por FIA_UAU.2 User authentication before any action y FIA_UID.1 Timing of identification y FIA_UID.2 User authentication before any action.

- Segregación de funciones del TOE. Las políticas de control de acceso, definidas como secciones, pueden asignarse a roles, que a su vez pueden asignarse a usuarios, este objetivo está cubierto FDP_ACC.1. Subset access control. Las asignaciones pueden contar con valores iniciales y por defecto durante la instalación del TOE, dichos valores pueden ser modificados por cualquier rol con la sección sec-adm, normalmente Administrador, objetivo cubierto por FMT_MSA.3 Static attribute initialization.

- Administración del Syslog, reglas de captura de logs y configuración de atributos de auditoría, objetivo cubierto por FMT_SMF.1 Specification of Management Functions.

- Adición de patrones de log y determinadas secciones de rol, que afectan a la política de flujo de información, objetivo cubierto por FDP_IFF.1 Simple security attributes.

O.AUTHENTICITY
Para garantizar que los logs originales recogidos por el LogHost 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, de mismo nombre que el original, consiste en la firma electrónica generada a partir del log y un certificado autofirmado con algoritmo de firma **SHA1 with RSA.** Los requisitos necesarios para asegurar la autenticidad de los logs son FDP_DAU.1 Basic Data Authentication.

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 utilizando el protocolo SSL y FTP_ITC.1 Inter-TSF trusted channel.

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_IFC.2 Complete information flow control, FPT_TDC.1 Inter-TSF basic TSF data consistency.

6.1.3.6.LogSpaces

O.LOG
Cada uno de los módulos audita, generación de ficheros de log, las conexiones realizadas por los diferentes usuarios y los intentos de conexión de accesos al TOE, este objetivo está cubierto por FAU_GEN.1 Audit data generation. La información de auditoría:

- puede ser consultada, objetivo cubierto por FAU_SAR.1 Audit review, por usuarios con permiso de lectura en el directorio de generación de logs, este objetivo está cubierto por FAU_SAR.2 Restricted audit review.

- muestra la fecha y hora, precisa, para el seguimiento de eventos de log, objetivo cubierto por FPT_STM.1 Reliable time stamps.

O.ROLE
La política de control de acceso al TOE, centralizada en el módulo LISM, incluye:

- Autenticación de usuarios, basados en rol y password. La hash de la password, SHA-1, debe coincidir con la almacenada en el LISM, este objetivo está cubierto por FDP_ACF.1 Security attribute based access control. La inserción del identificador de usario y password precederá a cualquier otra acción en el TOE, este objetivo está cubierto por FIA_UAU.2 User authentication before any action y FIA_UID.1 Timing of identification y FIA_UID.2 User authentication before any action.

- Segregación de funciones del TOE. Las políticas de control de acceso, definidas como secciones, pueden asignarse a roles, que a su vez pueden asignarse a usuarios, este objetivo está cubierto FDP_ACC.1. Subset access control. Las asignaciones pueden contar con valores iniciales y por defecto durante la instalación del TOE, dichos valores pueden ser modificados por cualquier rol con la sección sec-adm, normalmente Administrador, objetivo cubierto por FMT_MSA.3 Static attribute initialization.

- Administración de casos forenses y configuración de atributos de auditoria, objetivo cubierto por FMT_SMF.1 Specification of Management Functions.

- Adición de patrones de log y determinadas secciones de rol, que afectan a la política de flujo de información, objetivo cubierto por FDP_IFF.1 Simple security attributes.

O.SECURECOM
Todas las comunicaciones entre módulos del TOE se realizan mediante la asociación de canales seguros. En el caso de LogSpaces este objetivo está cubierto por FTP_ITC.1 Inter-TSF trusted channel, el cual asegura la comunicación utilizando el protocolo SSL

O.INDATA
En el caso de Achilles para cubrir requisitos en comunicación de datos de objetos serializados y documentos xml, se utiliza: FDP_IFC.1 Subset information flow control, FDP_IFC.1 Subset information flow control, FPT_TDC.1 Inter-TSF basic TSF data consistency.

6.1.3.7.LogReports

O.LOG
Cada uno de los módulos audita, generación de ficheros de log, las conexiones realizadas por los diferentes usuarios y los intentos de conexión de accesos al TOE, este objetivo está cubierto por FAU_GEN.1 Audit data generation. La información de auditoría:

- puede ser consultada, objetivo cubierto por FAU_SAR.1 Audit review, por usuarios con permiso de lectura en el directorio de generación de logs, este objetivo está cubierto por FAU_SAR.2 Restricted audit review.

- muestra la fecha y hora, precisa, para el seguimiento de eventos de log, objetivo cubierto por FPT_STM.1 Reliable time stamps.

O.ROLE
La política de control de acceso al TOE, centralizada en el módulo LISM, incluye:

- Autenticación de usuarios, basados en rol y password. La hash de la password, SHA-1, debe coincidir con la almacenada en el LISM, este objetivo está cubierto por FDP_ACF.1 Security attribute based access control. La inserción del identificador de usario y password precederá a cualquier otra acción en el TOE, este objetivo está cubierto por FIA_UAU.2 User authentication before any action y FIA_UID.1 Timing of identification y FIA_UID.2 User authentication before any action.

- Segregación de funciones del TOE. Las políticas de control de acceso, definidas como secciones, pueden asignarse a roles, que a su vez pueden asignarse a usuarios, este objetivo está cubierto FDP_ACC.1. Subset access control. Las asignaciones pueden contar con valores iniciales y por defecto durante la instalación del TOE, dichos valores pueden ser modificados por cualquier rol con la sección sec-adm, normalmente Administrador, objetivo cubierto por FMT_MSA.3 Static attribute initialization.

- Administración de grupos de informes y configuración de atributos de auditoria, objetivo cubierto por FMT_SMF.1 Specification of Management Functions.

- Adición de grupos de informes y determinadas secciones de rol, que afectan a la política de flujo de información, objetivo cubierto por FDP_IFF.1 Simple security attributes.

O.SECURECOM
Todas las comunicaciones entre módulos del TOE se realizan mediante la asociación de canales seguros. En el caso de LogReports este objetivo está cubierto por FTP_ITC.1 Inter-TSF trusted channel, el cual asegura la comunicación utilizando el protocolo SSL.

O.INDATA
En el caso de LogReports para cubrir requisitos en comunicación de datos de objetos serializados y protocolo SETP, se utiliza FDP_IFC.1 Subset information flow control, FDP_IFC.1 Subset information flow control, FPT_TDC.1 Inter-TSF basic TSF data consistency.

6.1.3.8.Achilles

O.LOG
Cada uno de los módulos audita, generación de ficheros de log, las conexiones realizadas por los diferentes usuarios y los intentos de conexión de accesos al TOE, este objetivo está cubierto por FAU_GEN.1 Audit data generation. La información de auditoría:

- puede ser consultada, objetivo cubierto por FAU_SAR.1 Audit review, por usuarios con permiso de lectura en el directorio de generación de logs, este objetivo está cubierto por FAU_SAR.2 Restricted audit review.

- muestra la fecha y hora, precisa, para el seguimiento de eventos de log, objetivo cubierto por FPT_STM.1 Reliable time stamps.

O.ROLE
La política de control de acceso al TOE, centralizada en el módulo LISM, incluye:

- Autenticación de usuarios, basados en rol y password. La hash de la password, SHA-1, debe coincidir con la almacenada en el LISM, este objetivo está cubierto por FDP_ACF.1 Security attribute based access control. La inserción del identificador de usario y password precederá a cualquier otra acción en el TOE, este objetivo está cubierto por FIA_UAU.2 User authentication before any action, FIA_UID.1 Timing of identification y FIA_UID.2 User authentication before any action.

- Segregación de funciones del TOE. Las políticas de control de acceso, definidas como secciones, pueden asignarse a roles, que a su vez pueden asignarse a usuarios, este objetivo está cubierto FDP_ACC.1. Subset access control. Las asignaciones pueden contar con valores iniciales y por defecto durante la instalación del TOE, dichos valores pueden ser modificados por cualquier rol con la sección sec-adm, normalmente Administrador, objetivo cubierto por FMT_MSA.3 Static attribute initialization.

- Administración de la base de datos de vulnerabilidades y configuración de atributos de auditoría, objetivo cubierto por FMT_SMF.1 Specification of Management Functions.

- Adición de determinadas secciones de rol, que afectan a la política de flujo de información, objetivo cubierto por FDP_IFF.1 Simple security attributes.

O.SECURECOM
Todas las comunicaciones entre módulos del TOE se realizan mediante la asociación de canales seguros. En el caso de Achilles este objetivo está cubierto por FTP_ITC.1 Inter-TSF trusted channel, el cual asegura la comunicación utilizando el protocolo SSL.

O.INDATA
En el caso de Achilles para cubrir requisitos en comunicación de datos de objetos serializados y documentos xml, se utiliza FDP_IFC.1 Subset information flow control, FPT_TDC.1 Inter-TSF basic TSF data consistency.

6.1.3.9.Activos

O.LOG
Cada uno de los módulos audita, generación de ficheros de log, las conexiones realizadas por los diferentes usuarios y los intentos de conexión de accesos al TOE, este objetivo está cubierto por FAU_GEN.1 Audit data generation. La información de auditoría:

- puede ser consultada, objetivo cubierto por FAU_SAR.1 Audit review, por usuarios con permiso de lectura en el directorio de generación de logs, este objetivo está cubierto por FAU_SAR.2 Restricted audit review.

- muestra la fecha y hora, precisa, para el seguimiento de eventos de log, objetivo cubierto por FPT_STM.1 Reliable time stamps.

O.ROLE
La política de control de acceso al TOE, centralizada en el módulo LISM, incluye:

- Autenticación de usuarios, basados en rol y password. La hash de la password, SHA-1, debe coincidir con la almacenada en el LISM, este objetivo está cubierto por FDP_ACF.1 Security attribute based access control. La inserción del identificador de usario y password precederá a cualquier otra acción en el TOE, este objetivo está cubierto por FIA_UAU.2 User authentication before any action, FIA_UID.1 Timing of identification y FIA_UID.2 User authentication before any action.

- Segregación de funciones del TOE. Las políticas de control de acceso, definidas como secciones, pueden asignarse a roles, que a su vez pueden asignarse a usuarios, este objetivo está cubierto FDP_ACC.1. Subset access control. Las asignaciones pueden contar con valores iniciales y por defecto durante la instalación del TOE, dichos valores pueden ser modificados por cualquier rol con la sección sec-adm, normalmente Administrador, objetivo cubierto por FMT_MSA.3 Static attribute initialization.

- Administración de la gestión del descubrimiento de activos configuración de atributos de auditoría, objetivo cubierto por FMT_SMF.1 Specification of Management Functions.

- Adición de determinadas secciones de rol, que afectan a la política de flujo de información, objetivo cubierto por FDP_IFF.1 Simple security attributes.

O.SECURECOM
Todas las comunicaciones entre módulos del TOE se realizan mediante la asociación de canales seguros. En el caso de Activos este objetivo está cubierto por FTP_ITC.1 Inter-TSF trusted channel, el cual asegura la comunicación utilizando el protocolo SSL.

O.INDATA
En el caso de Activos para cubrir requisitos en comunicación de datos de objetos serializados y documentos xml se utiliza FDP_IFC.1 Subset information flow control, FPT_TDC.1 Inter-TSF basic TSF data consistency.

6.1.3.10.LISM

O.LOG
Cada uno de los módulos audita, generación de ficheros de log, las conexiones realizadas por los diferentes usuarios y los intentos de conexión de accesos al TOE, este objetivo está cubierto por FAU_GEN.1 Audit data generation. La información de auditoría:

- puede ser consultada, objetivo cubierto por FAU_SAR.1 Audit review, por usuarios con permiso de lectura en el directorio de generación de logs, este objetivo está cubierto por FAU_SAR.2 Restricted audit review.

- muestra la fecha y hora, precisa, para el seguimiento de eventos de log, objetivo cubierto por FPT_STM.1 Reliable time stamps.

O.ROLE
La política de control de acceso al TOE, centralizada en el módulo LISM, incluye:

- Autenticación de usuarios, basados en rol y password. La hash de la password, SHA-1, debe coincidir con la almacenada en el LISM, este objetivo está cubierto por FDP_ACF.1 Security attribute based access control. La inserción del identificador de usario y password precederá a cualquier otra acción en el TOE, este objetivo está cubierto por FIA_UAU.2 User authentication before any action, FIA_UID.1 Timing of identification y FIA_UID.2 User authentication before any action.

- Segregación de funciones del TOE. Las políticas de control de acceso, definidas como secciones, pueden asignarse a roles, que a su vez pueden asignarse a usuarios, este objetivo está cubierto FDP_ACC.1. Subset access control. Las asignaciones pueden contar con valores iniciales y por defecto durante la instalación del TOE, dichos valores pueden ser modificados por cualquier rol con la sección sec-adm, normalmente Administrador, objetivo cubierto por FMT_MSA.3 Static attribute initialization.

- Definición de los atributos de seguridad: nombre, nombre completo, password, role, dirección de correo y compañía, objetivo cubierto por FIA_ATD.1 User attribute definition; administración de usuarios, roles, asignación de usuarios a roles, asignación de roles a secciones, colas, patrones de fichero, grupos de informes y acciones, objetivo cubierto por FMT_MSA.1 Management of security attributes y FMT_SMR.1 Security roles, por usuarios asignados a un rol con la sección 'sec-adm', normalmente Administrador.

- Administración de la gestión usuarios, roles y configuración de atributos de auditoria, objetivo cubierto por FMT_SMF.1 Specification of Management Functions.

- Adición de determinadas secciones de rol, que afectan a la política de flujo de información, objetivo cubierto por FDP_IFF.1 Simple security attributes.

O.SECURECOM
Todas las comunicaciones entre módulos del TOE se realizan mediante la asociación de canales seguros. En el caso de Activos este objetivo está cubierto por FTP_ITC.1 Inter-TSF trusted channel, el cual asegura la comunicación utilizando el protocolo SSL.

O.INDATA
En el caso de LISM para cubrir requisitos en comunicación de datos para la transmission y recepción de objetos serializados y logs, importación y exportación de ficheros de propiedades y de esquemas LDAP de LogICA, se utilize: FDP_ETC.1 Export of user data without security attributes, FDP_ETC.2 Export of user data with security attributes, FDP_IFC.1 Subset information flow control, FDP_ITC.1 Import of user data without security attributes, FDP_ITC.2 Import of user data with security attributes, FPT_TDC.1 Inter-TSF basic TSF data consistency.

6.1.3.11.CuadICA

O.LOG
Cada uno de los módulos audita, generación de ficheros de log, las conexiones realizadas por los diferentes usuarios y los intentos de conexión de accesos al TOE, este

objetivo está cubierto por FAU_GEN.1 Audit data generation. La información de auditoría:

- puede ser consultada, objetivo cubierto por FAU_SAR.1 Audit review, por usuarios con permiso de lectura en el directorio de generación de logs, este objetivo está cubierto por FAU_SAR.2 Restricted audit review.

- muestra la fecha y hora, precisa, para el seguimiento de eventos de log, objetivo cubierto por FPT_STM.1 Reliable time stamps.

O.ROLE
La política de control de acceso al TOE, centralizada en el módulo LISM, incluye:

- Autenticación de usuarios, basados en perfil y password. La hash de la password, SHA-1, debe coincidir con la almacenada en la base de datos, este objetivo está cubierto por FDP_ACF.1 Security attribute based access control. La inserción del identificador de usario y password precederá a cualquier otra acción en el TOE, este objetivo está cubierto por FIA_UAU.2 User authentication before any action, FIA_UID.1 Timing of identification y FIA_UID.2 User authentication before any action.

- Segregación de funciones del TOE. Las políticas de control de acceso, definidas como perfiles_acceso, pueden asignarse a perfiles, que a su vez pueden asignarse a usuarios, este objetivo está cubierto FDP_ACC.1. Subset access control. Las asignaciones pueden contar con valores iniciales y por defecto durante la instalación del TOE, dichos valores pueden ser modificados por cualquier usuario con perfil de Administrador, objetivo cubierto por FMT_MSA.3 Static attribute initialization.

- Definición de los atributos de seguridad: nombre, login, password, perfil, dirección de correo, objetivo cubierto por FIA_ATD.1 User attribute definition; administración de usuarios, perfiles, asignación de usuarios a perfiles, asignación de perfiles a perfiles_acceso, objetivo cubierto por FMT_MSA.1 Management of security attributes y FMT_SMR.1 Security roles, por usuarios asignados a un perfil de Administrador.

- Administración de la gestión usuarios, perfiles y configuración de atributos de auditoría, objetivo cubierto por FMT_SMF.1 Specification of Management Functions.

-Estado del agente de CuadICA, que afecta a la política de flujo de información, objetivo cubierto por FDP_IFF.1 Simple security attributes.

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 Audit data generation, FPT_STM.1 Reliable time stamps, FAU_SAR.1 Audit review, FAU_SAR.2 Restricted audit review.

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 Subset access control, FDP_ACF.1 Security attribute based access control, FDP_IFF.1 Simple security attributes, FIA_ATD.1 User attribute definition, FIA_UAU.2 User authentication before any action, FIA_UID.1 Timing of identification, FIA_UID.2 User identification before any action, FMT_MSA.1 Management of security attributes, FMT_MSA.3 Static attribute initialization, FMT_SMF.1 Specification of Management Functions, FMT_SMR.1 Security roles.

O.SECURECOM
Todas las comunicaciones entre módulos del TOE se realizan mediante la asociación de canales seguros. En el caso de CuadICA este objetivo está cubierto por FTP_ITC.1 Inter-TSF trusted channel, el cual asegura la comunicación utilizando el protocolo SSL.

O.INDATA
En el caso de CuadICA para cubrir requisitos en comunicación de datos entre diferentes esquemas de bases de datos, se utiliza: FDP_IFC.1 Subset information flow control, FPT_TDC.1 Inter-TSF basic TSF data consistency.