REF:	2009-31-INF-678 v1	Creado:	CERT3
Difusión:	Expediente	Revisado:	TECNICO
Fecha:	16.06.2011	Aprobado:	JEFEAREA

INFORME DE CERTIFICACIÓN

Expediente: 2009-31 LogIca 3.0-SP2 Patch11

Datos del solicitante: B28893139 ICA Informática y Comunicaciones Avanzadas S.L.

Referencias:

- [EXT-871] Solicitud de Certificación de LogIca 3.0-SP2 Patch11.
- [EXT-1291] ETR M0 de LogIca 3.0-SP2 Patch11.
- [CCRA] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, mayo 2000.
- [SOGIS]. European Mutual Recognition Agreement of IT Security Evaluation Certificates v3.0, January 2010.

Informe de certificación del producto “Sistema de Gestión de Eventos (SIEM) Suite LogICA, versión 3.0-SP2 Patch11”, según la solicitud de referencia [EXT-871], de fecha 28.12.2009, y evaluado por el laboratorio LGAI-APPLUS, conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-1291], de acuerdo a [CCRA] y a [SOGIS], recibido el pasado 13.05.2011.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

ÍNDICE

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

RESUMEN

Este documento constituye el Informe de Certificación para el expediente de certificación del producto “Sistema de Gestión de Eventos (SIEM) Suite LogICA, versión 3.0-SP2 Patch11”.

Fabricante: ICA - Informática y Comunicaciones Avanzadas S.L.

Patrocinador: ICA - Informática y Comunicaciones Avanzadas S.L.

Organismo de Certificación: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

Laboratorio de Evaluación: LGAI-APPLUS.

Perfil de Protección: Ninguno.

Nivel de Evaluación: EAL2.

Fecha de término de la evaluación: 28 de abril de 2011.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL2 presentan el veredicto de “PASA”. Por consiguiente, el laboratorio LGAI-APPLUS asigna el VEREDICTO de “PASA” a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL2, definidas por los Criterios Comunes v3.1 [CC-P3] y la Metodología de Evaluación v3.1 [CEM].

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto “Sistema de Gestión de Eventos (SIEM) Suite LogICA, versión 3.0-SP2 Patch11”, se propone la resolución estimatoria de la misma.

Resumen del 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 Base de Datos que consolida la información en tiempo real.
- Establecimiento de indicadores de cumplimiento legal y normativo en aspectos de seguridad IT.

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

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Requisitos de garantía de seguridad

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL2, según la Parte 3 de CC v3.1 r3.

Se enumeran, a continuación, los componentes de garantía satisfechos en esta evaluación:

ASE_CCL.1	AGD_OPE.1
ASE_ECD.1	AGD_PRE.1
ASE_INT.1	ALC_CMC.2
ASE_OBJ.2	ALC_CMS.2
ASE_REQ.2	ALC_DEL.1
ASE_SPD.1	ATE_COV.1
ASE_TSS.1	ATE_FUN.1
ADV_ARC.1	ATE_IND.2
ADV_FSP.2	AVA_VAN.2
ADV_TDS.1	

Requisitos funcionales de seguridad

La funcionalidad de seguridad del producto satisface los siguientes componentes funcionales, extraídos de la Parte 2 de CC v3.1 r3, y agrupados por los componentes del TOE a los que afectan.

LogAgent y LogAgentManager

- FAU_GEN.1 LogICA Audit data generation.
- FPT_STM.1 Reliable time stamps.
- FAU_SAR.1 Audit review.
- FAU_SAR.2 Restricted audit review.
- FDP_ACF.1 LogAgent and LogAgentManager Security attribute based access control.
- FDP_ACC.1 LogAgent and LogAgentManager Subset access control.
- FDP_IFC.1 LogAgent and LogAgentManager Subset information flow control.
- FDP_IFF.1 LogAgent and LogAgentManager Simple security attributes.
- FIA_UAU.2 User authentication before any action.
- FIA_UID.1 Timing of identification.
- FIA_UID.2 User identification before any action.
- FMT_MSA.3 LogICA Static attribute initialisation.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- FMT_SMF.1 LogAgent and LogAgentManager Specification of Management Functions.
- FPT_TDC.1 LogAgent and LogAgentManager Inter-TSF basic TSF data consistency.
- FTP_ITC.1 LogAgent and LogAgentManager Inter-TSF trusted channel.

LogServer

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

EventCorrelator

- FAU_GEN.1 LogICA Audit data generation.
- FPT_STM.1 Reliable time stamps.
- FAU_SAR.1 Audit review.
- FAU_SAR.2 Restricted audit review.
- FDP_ACF.1 EventCorrelator Security attribute based access control.
- FDP_ACC.1 EventCorrelator Subset access control.
- FDP_IFC.1 EventCorrelator Subset information flow control.
- FDP_IFF.1 EventCorrelator Simple security attributes.
- FIA_UAU.2 User authentication before any action.
- FIA_UID.1 Timing of identification.
- FIA_UID.2 User identification before any action.
- FMT_MSA.3 LogICA Static attribute initialisation.
- FMT_SMF.1 EventCorrelator Specification of Management Functions.
- FPT_TDC.1 EventCorrelator Inter-TSF basic TSF data consistency.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- FTP_ITC.1 EventCorrelator Inter-TSF trusted channel.

Console

- FDP_ACF.1 Console Security attribute based access control.
- FDP_ACC.1 Console Subset access control.
- FDP_IFC.1 Console Subset information flow control.
- FDP_IFF.1 Console Simple security attributes.
- FIA_UAU.2 User authentication before any action.
- FIA_UID.1 Timing of identification.
- FIA_UID.2 User identification before any action.
- FTP_ITC.1 Console Inter-TSF trusted channel.

LogHost y LogHostManager

- FAU_GEN.1 LogICA Audit data generation.
- FPT_STM.1 Reliable time stamps.
- FAU_SAR.1 Audit review.
- FAU_SAR.2 Restricted audit review.
- FDP_ACC.2 Complete access control.
- FDP_ACF.1 LogHost and LogHostManager Security attribute based access control.
- FDP_DAU.1 LogHost and LogHostManager Basic Data Authentication.
- FDP_IFC.2 Complete information flow control.
- FDP_IFF.1 LogHost and LogHostManager Simple security attributes.
- FIA_UAU.2 User authentication before any action.
- FIA_UID.1 Timing of identification.
- FIA_UID.2 User identification before any action.
- FMT_MSA.3 LogICA Static attribute initialisation.
- FMT_SMF.1 LogHost and LogHostManager Specification of Management Functions.
- FPT_TDC.1 LogHost and LogHostManager Inter-TSF basic TSF data consistency.
- FTP_ITC.1 LogHost and LogHostManager Inter-TSF trusted channel.

LogSpaces

- FAU_GEN.1 LogICA Audit data generation.
- FPT_STM.1 Reliable time stamps.
- FAU_SAR.1 Audit review.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- FAU_SAR.2 Restricted audit review.
- FDP_ACF.1 LogSpaces Security attribute based access control.
- FDP_ACC.1 LogSpaces Subset access control.
- FMT_MSA.3 LogICA Static attribute initialization.
- FDP_IFC.1 LogSpaces Subset information flow control.
- FDP_IFF.1 LogSpaces Simple security attributes.
- FIA_UAU.2 User authentication before any action.
- FIA_UID.1 Timing of identification.
- FIA_UID.2 User identification before any action.
- FMT_SMF.1 LogSpaces Specification of Management Functions.
- FPT_TDC.1 LogSpaces Inter-TSF basic TSF data consistency.
- FTP_ITC.1 LogSpaces Inter-TSF trusted channel.

LogReports

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

Achilles

- FAU_GEN.1 LogICA Audit data generation.
- FPT_STM.1 Reliable time stamps.
- FAU_SAR.1 Audit review.
- FAU_SAR.2 Restricted audit review.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- FDP_ACF.1 Achilles Security attribute based access control.
- FDP_ACC.1 Achilles Subset access control.
- FMT_MSA.3 LogICA Static attribute initialisation.
- FDP_IFC.1 Achilles Subset information flow control.
- FDP_IFF.1 Achilles Simple security attributes.
- FIA_UAU.2 User authentication before any action.
- FIA_UID.1 Timing of identification.
- FIA_UID.2 User identification before any action.
- FMT_SMF.1 Achilles Specification of Management Functions.
- FPT_TDC.1 Achilles Inter-TSF basic TSF data consistency.
- FTP_ITC.1 Achilles Inter-TSF trusted channel.

Activos

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

LISM

- FAU_GEN.1 LogICA Audit data generation.
- FPT_STM.1 Reliable time stamps.
- FAU_SAR.1 Audit review.
- FAU_SAR.2 Restricted audit review.
- FDP_ACC.1 LISM Subset access control.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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

CuadICA

- FAU_GEN.1 Cuadica Audit data generation.
- FPT_STM.1 Reliable time stamps.
- FAU_SAR.1 Audit review.
- FAU_SAR.2 Restricted audit review.
- FDP_ACC.1 Cuadica Subset access control.
- FDP_ACF.1 Cuadica Security attribute based access control.
- FDP_DAU.1 Cuadica Basic Data Authentication.
- FDP_IFC.1 Cuadica Subset information flow control.
- FDP_IFF.1 Cuadica Simple security attributes.
- FIA_ATD.1 Cuadica 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 Cuadica Management of security attributes.
- FMT_MSA.3 Cuadica Static attribute initialisation.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- FMT_SMF.1 Cuadica Specification of Management Functions.
- FMT_SMR.1 Cuadica Security roles.
- FPT_TDC.1 Cuadica Inter-TSF basic TSF data consistency.
- FTP_ITC.1 Cuadica Inter-TSF trusted channel.

IDENTIFICACIÓN

Producto: "Sistema de Gestión de Eventos (SIEM) Suite LogICA, versión 3.0-SP2 Patch11".

Declaración de Seguridad: "Sistema de Gestión de Eventos SIEM Suite LogICA v3.0-SP2 Patch11 Security Target", versión 1.6, de 21.03.2011.

Perfil de Protección: Ninguno.

Nivel de Evaluación: CC v3.1 r3 EAL2.

POLÍTICA DE SEGURIDAD

Para el correcto uso del producto "Sistema de Gestión de Eventos (SIEM) Suite LogICA, versión 3.0-SP2 Patch11", se deben aplicar una serie de políticas organizativas, que aseguran el cumplimiento de diferentes estándares y exigencias de seguridad.

El detalle de estas políticas se encuentra en la Declaración de Seguridad. En síntesis, se establece la necesidad de aplicar políticas organizativas relativas a los siguientes aspectos.

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 únicamente a los recursos que le son precisos para realizar su trabajo.

HIPÓTESIS Y ENTORNO DE USO

Las siguientes hipótesis restringen las condiciones sobre las cuales se garantizan las propiedades y funcionalidades de seguridad indicadas en la Declaración de Seguridad. Estas mismas hipótesis se han aplicado durante la evaluación en la determinación de la condición de explotables de las vulnerabilidades identificadas.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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

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.

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.

Aclaraciones sobre amenazas no cubiertas

Las siguientes amenazas no suponen un riesgo explotable para el producto “Sistema de Gestión de Eventos (SIEM) Suite LogICA, versión 3.0-SP2 Patch11”, aunque los agentes que realicen ataques tengan un potencial de ataque “Basic”, correspondiente con el nivel de garantía EAL2, y siempre bajo el cumplimiento de las hipótesis de uso y la correcta satisfacción de las políticas de seguridad.

Para cualquier otra amenaza no incluida en esta lista, el resultado de la evaluación de las propiedades del producto, y el correspondiente certificado, no garantizan resistencia alguna.

T.IDENTITY_SPOOFING

Un atacante puede realizar operaciones con las 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 u operar activos del TOE sin estar autorizado a ello y sin ser detectado.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

T.SNIFFING

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

Funcionalidad del entorno

El producto requiere de la colaboración del entorno para la cobertura de algunos objetivos del problema de seguridad definido.

Los objetivos que se deben cubrir por el entorno de uso del producto son los siguientes:

O.E.OSAUTH

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

Los detalles de la definición del entorno del producto (hipótesis, amenazas y políticas de seguridad), o de los requisitos de seguridad del TOE se encuentran en la correspondiente Declaración de Seguridad.

ARQUITECTURA

Arquitectura lógica

El TOE posee una arquitectura modular (en su estructura lógica) cuyos componentes son los descritos a continuación.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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.
- 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

- Gestiona y configura los agentes remotamente.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- Distribuye las configuraciones.
- Monitoriza y controla el funcionamiento de los agentes.
- Gestiona la configuración de vigilancia de configuraciones y auditoría 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 auditoría de actividad de usuarios sobre archivos asociados a cada activo.

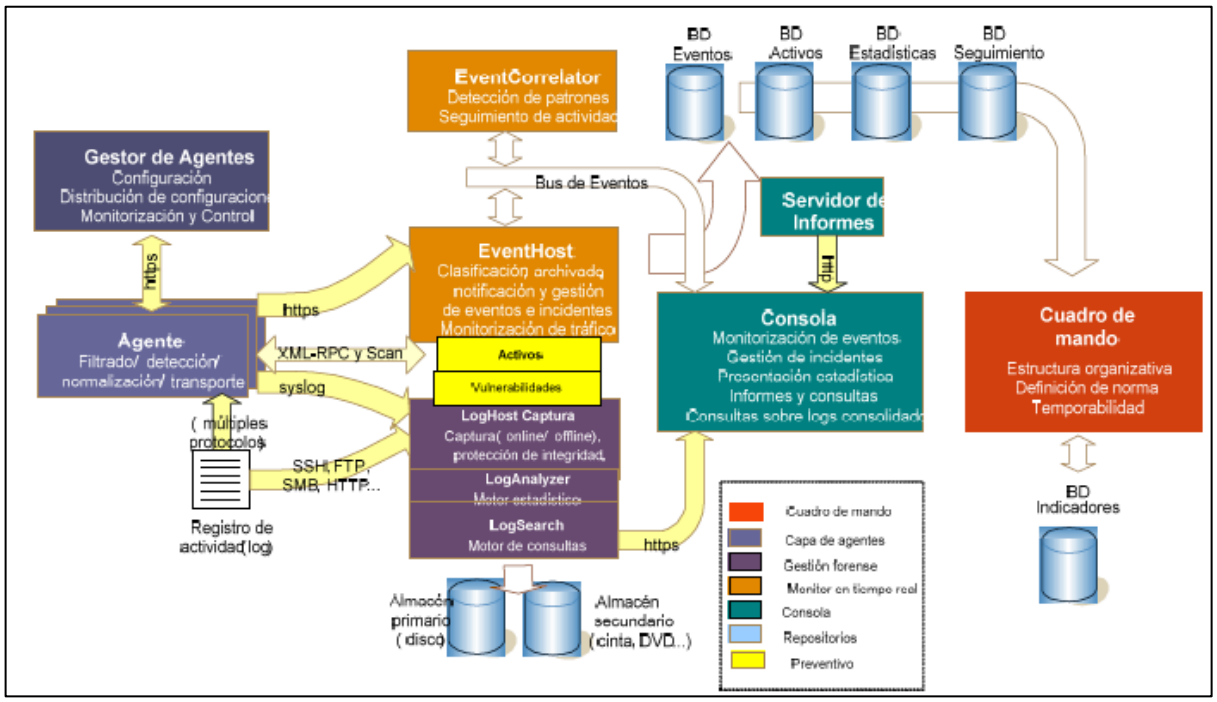
LISM

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

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

CuadICA

- Permite la definición de indicadores asociados 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.



- Arquitectura Modular del TOE -

Arquitectura física

El TOE se instala en un servidor Appliance que permite ejecutarlo 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 diferentes partes, LogAgent, LogServer, EventCorrelator, Console, LogHost, LogAgentManager, LogHostManager, Achilles, Activos, Lism y 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 descripción de la siguiente tabla, que pueden ser escaladas para ajustarse a las necesidades y versiones de distribución del producto.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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

- Características mínimas Appliance -

DOCUMENTOS

El producto incluye los documentos indicados a continuación, y que deberán distribuirse y facilitarse de manera conjunta a los usuarios de la versión evaluada:

- Manual de Administración de LogICA, v1.2.
- Manual de Operador de LogICA, v1.2.
- Manual de Administración de CuadICA, v1.1.
- Manual de Operador de CuadICA, v1.0.
- Manual Kettle de CuadICA, v1.0.
- Manual de Instalación de LogICA, v1.0.

PRUEBAS DEL PRODUCTO

El fabricante ha realizado pruebas para todas las funciones de seguridad. Todas las pruebas han sido realizadas por el fabricante en sus instalaciones con resultado satisfactorio.

En el proceso de evaluación se ha verificado cada una de las pruebas individuales, comprobando que se identifica la función de seguridad que cubre y que la prueba es adecuada a la función de seguridad que se desea cubrir.

Todas las pruebas se han realizado sobre un mismo escenario de pruebas acorde a la arquitectura identificada en la Declaración de Seguridad.

Se ha comprobado que los resultados obtenidos en estas pruebas se ajustan a los resultados esperados.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Para verificar los resultados de las pruebas del fabricante, el laboratorio ha repetido todas estas pruebas funcionales y se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados.

Adicionalmente, y de acuerdo con la información presentada por el fabricante en las evidencias de evaluación, el evaluador ha preparado un conjunto de pruebas independientes que corroboran, y en algunos casos complementan, las pruebas de funcionalidad realizadas por el fabricante.

CONFIGURACIÓN EVALUADA

Los requisitos software y hardware son los que se indican a continuación. Así, para el funcionamiento del producto “Sistema de Gestión de Eventos (SIEM) Suite LogICA, versión 3.0-SP2 Patch11” es necesario disponer de los siguientes componentes software:

- 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.

En cuanto a los componentes hardware, el único requisito es que soporten los elementos software detallados previamente.

Dentro de todas las posibilidades que ofrecen estos requisitos, la configuración elegida para su evaluación fue la siguiente:

- TOE: Sistema de Gestión de Eventos (SIEM) Suite LogICA, versión 3.0-SP2 Patch11.
- Sistema Operativo: CentOS 5.3 - Version 2.6.18-128.el5.
- Servidor de aplicaciones: Apache-Tomcat v.5.5.20.
- Servidor de Bases de Datos: Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 – Prod.
- Bus JMS: Active-MQ v.5.3.
- Sistema IDS: Snort v.2.6.1.2.
- Sistema de adquisición de logs: Syslog-ng v2.0.6.
- Sistema Operativo Agentes:
    - Linux RedHat Enterprise v.4 update 3
    - Windows XP Profesional SP2

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- Java:
    - Java(TM) SE Runtime Environment (build 1.6.0_05-b13)
    - Apache-ant v1.7.1
- Script: Perl v5.8.5 built for i386-linux-thread-multi.
- Tunneling: stunnel 3.x o superior.
- Hardware: se utilizó como plataforma principal de consolidación de LogICA, una máquina servidor con las siguientes características:
    - SUPERSERVER SYS-6016T-URF SUPERMICRO 1U
    - INTEL NEHALEM E5520 2,26GHZ LGA1366 5,86GT/SEC 8M
    - DDR3 1333 4GB ECC
    - ST31000340NS SEAGATE 1.0TB 7200 SATAII 32MB

En términos de versiones de distribución, la configuración evaluada cumple las características de la versión FQC3.

RESULTADOS DE LA EVALUACIÓN

El producto “Sistema de Gestión de Eventos (SIEM) Suite LogICA, versión 3.0-SP2 Patch11” ha sido evaluado frente a la Declaración de Seguridad “Sistema de Gestión de Eventos SIEM Suite LogICA v3.0-SP2 Patch11 Security Target”, versión 1.6, de 21.03.2011.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL2 presentan el veredicto de “PASA”. Por consiguiente, el laboratorio LGAI-APPLUS asigna el VEREDICTO de “PASA” a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL2, definidas por los Criterios Comunes [CC-P3] y por la Metodología de Evaluación [CEM], en su versión 3.1 r3.

RECOMENDACIONES DEL CERTIFICADOR

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto “Sistema de Gestión de Eventos (SIEM) Suite LogICA, versión 3.0-SP2 Patch11”, se propone la resolución estimatoria de la misma.

GLOSARIO DE TÉRMINOS

CC	Criterios Comunes
CCN	Centro Criptológico Nacional
CCRA	Common Criteria Recognition Arrangement

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
OC	Organismo de Certificación
SOGIS	Senior Officials Group for Information Systems Security of the European Commission
TOE	Target Of Evaluation
TSF	TOE Security Function

BIBLIOGRAFÍA

Se han utilizado las siguientes normas y documentos en la evaluación del producto:

[CC-P1] Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, Version 3.1, r3, July 2009.

[CC-P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, r3, July 2009.

[CC-P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, r3, July 2009.

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1, r3, July 2009.

DECLARACIÓN DE SEGURIDAD

Conjuntamente con este Informe de Certificación, se dispone en el Organismo de Certificación de la Declaración de Seguridad completa de la evaluación: “Sistema de Gestión de Eventos SIEM Suite LogICA v3.0-SP2 Patch11 Security Target”, versión 1.6, de 21.03.2011.

ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es