Referencia: 2019-38-INF-3595- v1
Difusión: Limitada al expediente
Fecha: 23.08.2021

Creado por: CERT9
Revisado por: CALIDAD
Aprobado por: TECNICO

INFORME DE CERTIFICACIÓN

Expediente #	**2019-38**
TOE	**GLORIA 5.6.0**
Solicitante	**B96863444 - S2 Grupo**
Referencias	
	[EXT-6991] ETR v1.1 GLORIA

Informe de Certificación del producto GLORIA 5.6.0, según la solicitud de referencia [EXT-5306], de fecha 19/07/2019, evaluado por el laboratorio DEKRA Testing and Certification S.A.U., conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-6991], recibido el pasado 22/06/2021.

CONTENIDOS

RESUMEN

Este documento constituye el Informe de Certificación para el expediente de certificación del producto GLORIA 5.6.0.

GLORIA (Gestor de LOgs para Responder ante Incidentes y Amenazas) es una plataforma para la gestión de incidentes y amenazas de seguridad informática a través de técnicas de correlación compleja de eventos. La solución proporciona la funcionalidad SIEM (*Security Information and Event Management*) y, además, permite la monitorización, almacenamiento y procesado de la información y presenta capacidades de gestión de servicios para un centro de operaciones de seguridad.

Fabricante: S2 Grupo.

Patrocinador: S2 Grupo.

Organismo de Certificación: Centro Criptológico Nacional (CCN).

Laboratorio de Evaluación: DEKRA Testing and Certification S.A.U..

Perfil de Protección: Ninguno.

Nivel de Evaluación: Common Criteria v3.1 R5 EAL2 + ALC_FLR.1.

Fecha de término de la evaluación: 09/07/2021 <fecha de reunión de audiencia previa>.

Fecha de expiración[1]: 20/08/2026

Todos los componentes de garantía requeridos por el nivel de evaluación EAL2 (aumentado con ALC_FLR.1) presentan el veredicto de “PASA”. Por consiguiente, el laboratorio DEKRA Testing and Certification S.A.U. asigna el VEREDICTO de “PASA” a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL2 + ALC_FLR.1, definidas por los Common Criteria v3.1 R5 y la CEM v3.1 R5.

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto GLORIA 5.6.0, se propone la resolución estimatoria de la misma.

RESUMEN DEL TOE

GLORIA es una solución software de monitorización, correlación, gestión y cuadro de mando para facilitar la identificación y respuesta de incidentes y amenazas, así como la consulta de datos históricos de eventos de los elementos de seguridad de la organización.

Está compuesta por los siguientes componentes:

[1] Este campo se refiere a la fecha de expiración del reconocimiento del certificado en el ámbito de los acuerdos de reconocimiento mutuo firmados por este Organismo de Certificación.

- ARGOS: componente de monitorización y recolección de eventos de seguridad.
- TRITON: componente de inteligencia y correlación.
- EMAS: componente de gestión del servicio.
- HERA: componente de cuadro de mando.

REQUISITOS DE GARANTÍA DE SEGURIDAD

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL2, más las requeridas para el componente adicional ALC_FLR.1, según los Common Criteria v3.1 R5.

CLASE DE GARANTÍA	COMPONENTE DE GARANTÍA
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE.TSS.1
ADV	ADV_ARC.1
	ADV_FSP.2
	ADV_TDS.1
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.2
	ALC_CMS.2
	ALC_DEL.1
	ALC_FLR.1
ATE	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.2

REQUISITOS FUNCIONALES DE SEGURIDAD

La funcionalidad de seguridad del producto satisface los siguientes requisitos funcionales, según los Common Criteria v3.1 R5.

REQUISITOS FUNCIONALES DE SEGURIDAD
FAU_GEN.1
FAU_SAR.1
FAU_SAR.2
FAU_STG.2
FCS_STO_EXT.1
FCS_HTTPS_EXT.1
FDP_NET_EXT.1
FIA_AFL.1
FIA_ATD.1
FIA_UAU.2
FIA_UID.2
FMT_MOF.1
FMT_MTD.1
FMT_SMF.1
FMT_SMR.1
FTA_SSL.1
FTA_SSL.3
FTA_SSL.4
FTA_TSE.1
FTP_DIT_EXT.1

IDENTIFICACIÓN

Producto: GLORIA 5.6.0.

Declaración de Seguridad: GLORIA_ASE_DS_v1.9 (22 de junio de 2021).

Perfil de Protección: Ninguno.

Nivel de Evaluación: Common Criteria v3.1 R5 EAL2 + ALC_FLR.1.

POLÍTICA DE SEGURIDAD

La Declaración de Seguridad no incluye ninguna política de seguridad de la organización.

HIPÓTESIS Y ENTORNO DE USO

Las hipótesis descritas en la sección 3.3 ("*Hipótesis*") de la Declaración de Seguridad 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.

Por tanto, para garantizar el uso seguro del TOE, se parte de dichas hipótesis para su entorno de operación. En caso de que alguna de ellas no pudiera asumirse, no sería posible garantizar el funcionamiento seguro del TOE.

ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS

Las amenazas descritas en la sección 3.4 ("*Amenazas*") de la Declaración de Seguridad no suponen un riesgo explotable para el producto GLORIA 5.6.0, aunque los agentes que realicen ataques tengan potencial de ataque correspondiente al nivel Basic de EAL2 + ALC_FLR.1, 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.

FUNCIONALIDAD DEL ENTORNO

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

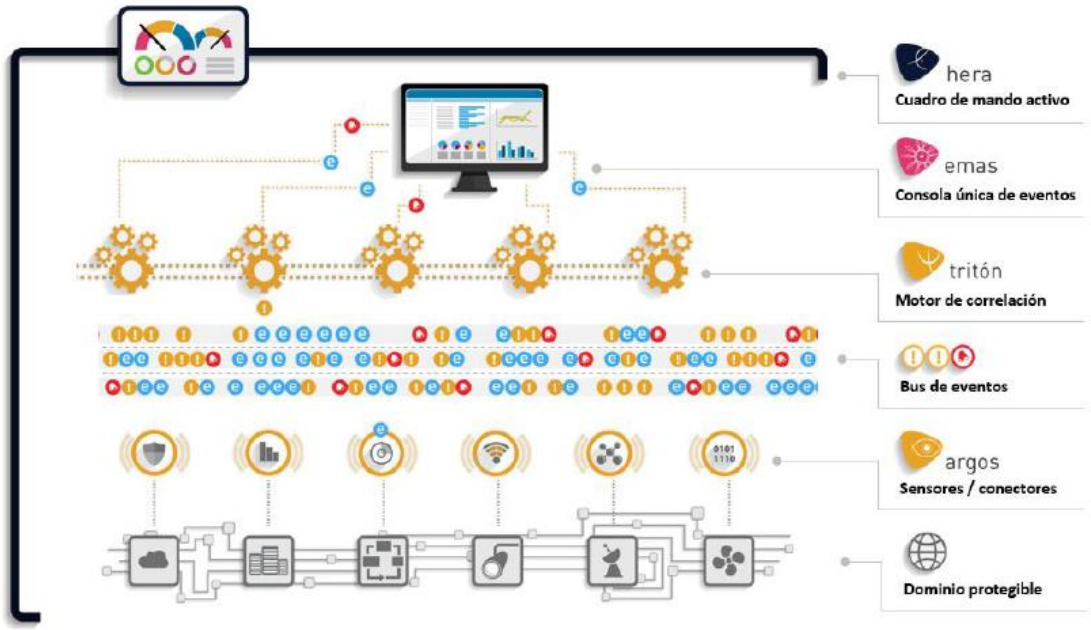
Los objetivos de seguridad para el entorno operacional son los que se detallan en la sección 4.2 ("*Objetivos de seguridad para el entorno operacional*") de la Declaración de Seguridad.

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

La arquitectura lógica del TOE es la que se muestra en la siguiente figura:



Las principales funcionalidades de seguridad que proporciona el TOE son las siguientes:

- **Autenticación**: no es posible realizar ninguna acción en el TOE sin haber realizado previamente una autenticación (a parte de la propia acción). Para ello el TOE muestra una pantalla de acceso dónde se solicitan las credenciales del usuario.
- **Aseguramiento**: pasado un tiempo de inactividad configurado, la sesión de GLORIA se cerrará automáticamente, sin poder acceder de nuevo a la información, ni navegar por la interfaz web, para ello será necesario volver a realizar un inicio de sesión.
- **Autorización**: es posible definir roles específicos y políticas de control de acceso para cada una de las funcionalidades existentes de la interfaz que dan acceso a la información recolectada y analizada de la organización. La funcionalidad ofrecida a cada usuario se determina a partir de los roles asignados a cada usuario, siendo estos roles uno de los atributos de seguridad de cada uno de los usuarios.

- **Auditoría**: Para poder llevar un control de sus accesos, el TOE dispone de la capacidad de generar y almacenar registros de auditoría, exitosos y fallidos. Estos registros están protegidos por el TOE ante la modificación y borrado no autorizado.
- **Comunicaciones**: Las comunicaciones entre los usuarios y el TOE se realizan mediante el protocolo HTTPS y SSH que garantiza que la información que se intercambia entre el TOE y el usuario se realiza de forma cifrada y segura.

ARQUITECTURA FÍSICA

El alcance físico del TOE es el que se describe a continuación:

- **EMAS**: componente para las tareas de gestión del servicio. Proporcionada en el fichero de plantilla de máquina virtual GLORIA-EMAS-v 5.6.0.ova.
- **HERA**: componente de cuadro de mando. Proporcionada en el fichero de plantilla de máquina virtual GLORIA-EMAS-v 5.6.0.ova.
- **TRITÓN**: componente para realizar las acciones de correlación. Proporcionada en el fichero de plantilla de máquina virtual GLORIA-TRITON-v5.6.0.ova.
- **ARGOS**: componente para la monitorización y recolección de eventos de seguridad. Proporcionada en el fichero de plantilla de máquina virtual GLORIA -ARGOS-v 5.6.0.ova.
- **ARGOS-LogServer**: subcomponente para el tratamiento de los eventos de seguridad. Proporcionada en el fichero de plantilla de máquina virtual GLORIA-ARGOS-LogServerv5.6.0.ova.
- **ARGOS-LogData**: subcomponente desplegado en clúster para el almacenamiento de registros de eventos de seguridad recogidos de las fuentes de información. Al tratarse de un clúster se proporciona en los ficheros plantilla de máquinas virtuales GLORIA-ARGOSLogData1-v5.6.0.ova y GLORIA-ARGOS-LogData2-v5.6.0.ova.

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.

- La guía de usuario llamada "*GLORIA_AGD_OPE_v 5.6.0*" (versión 1.4) en formato PDF.
- La guía de administración llamada "*GLORIA_AGD_PRE_v 5.6.0*" (versión 1.5) en formato PDF.

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 satisfactorios.

Durante el proceso de evaluación se han 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 las pruebas se ajustan a los resultados esperados.

Para verificar los resultados de las pruebas del fabricante, el laboratorio ha repetido todas estas pruebas funcionales. Igualmente, ha escogido y repetido todas las pruebas funcionales definidas por el fabricante, en la plataforma de pruebas montada en el laboratorio de evaluación, seleccionando una prueba por cada una de las clases funcionales más relevantes.

Adicionalmente, el laboratorio ha desarrollado una prueba por cada una de las funciones de seguridad del producto, verificando que los resultados, así obtenidos, son consistentes con los resultados obtenidos por el fabricante.

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados, y en aquellos casos en los que se presentó alguna desviación respecto de lo esperado, el evaluador ha constatado que dicha variación no representa un problema para la seguridad, ni supone una merma en la capacidad funcional del producto.

CONFIGURACIÓN EVALUADA

Los requisitos software y hardware, así como las opciones referidas son los que se indican a continuación. Así, para el funcionamiento del producto GLORIA 5.6.0 es necesario disponer de los siguientes componentes software:

- Componente EMAS: fichero "*GLORIA-EMAS-v5.6.0.ova*".
- Componente HERA: fichero "*GLORIA-EMAS-v5.6.0.ova*".
- Componente TRITÓN: fichero "*GLORIA-TRITON-v5.6.0.ova*".
- Componente ARGOS: fichero "*GLORIA-ARGOS-v5.6.0.ova*".
- Subcomponente ARGOS-LogServer: fichero "*GLORIA-ARGOS-LogServer-v5.6.0.ova*".
- Subcomponente ARGOS-LogData: ficheros "*GLORIA-ARGOS-LogData1-v5.6.0.ova*" y "*GLORIA-ARGOS-LogData2-v5.6.0.ova*".

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

RESULTADOS DE LA EVALUACIÓN

El producto GLORIA 5.6.0 ha sido evaluado en base a la Declaración de Seguridad GLORIA_ASE_DS_v1.9 (22 de junio de 2021)..

Todos los componentes de garantía requeridos por el nivel de evaluación EAL2 + ALC_FLR.1 presentan el veredicto de "PASA". Por consiguiente, el laboratorio DEKRA Testing and Certification S.A.U. asigna el **VEREDICTO de "PASA"** a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL2 + ALC_FLR.1, definidas por los Common Criteria v3.1 R5 y la CEM v3.1 R5.

RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES

A continuación, se proporcionan las recomendaciones acerca del uso seguro del producto. Estas recomendaciones han sido recopiladas a lo largo de todo el proceso de evaluación y se detallan para que sean consideradas en la utilización del producto.

- Se recomienda el uso del TOE ya que no presenta vulnerabilidades explotables en su entorno operacional.

RECOMENDACIONES DEL CERTIFICADOR

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto GLORIA 5.6.0, se propone la resolución estimatoria de la misma.

GLOSARIO DE TÉRMINOS

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
TOE	Target Of Evaluation

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, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

DECLARACIÓN DE SEGURIDAD O DECLARACIÓN DE SEGURIDAD LITE (SI APLICA)

Junto con este Informe de Certificación, se dispone en el Organismo de Certificación de la Declaración de Seguridad completa de la evaluación:

- GLORIA_ASE_DS_v1.9 (22 de junio de 2021).

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.org.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.