S2 GRUPO

S2 Grupo

GLORIA v5.6.0

Common Criteria EAL2

ASE_DS

22/06/2021

AENOR ER Empresa Registrada UNE-EN ISO 9001 ER-0343/2008
AENOR ER Seguridad Información UNE-ISO/IEC 27001 SI-0002/2006
AENOR ER Gestión Servicios TI UNE-ISO/IEC 20000-1 STI-0001/2011
AENOR ER Gestión I+D+i UNE 166002 ID-0066/2010
AENOR Gestión Ambiental UNE-EN ISO 14001 GA-2013/0358
CERTIFIED IQNet MANAGEMENT SYSTEM

Tipo de Documento:	*Declaración de Seguridad*
Descripción:	GLORIA_ASE_DS
Fecha de creación:	22/06/2021
Nombre del documento:	GLORIA_ASE_DS_v1.9

CONTROL DE VERSIONES

Versión	Realizado por	Descripción de versión	Fecha
1.0	S2Grupo	Versión inicial	26/06/2019
1.1	S2 Grupo	Revisión	21/01/2020
1.2	S2 Grupo	Revisión	24/01/2020
1.3	S2 Grupo	Revisión	06/03/2020
1.4	S2 Grupo	Revisión	20/03/2020
1.5	S2 Grupo	Revisión	27/03/2020
1.6	S2 Grupo	Revisión	29/07/2020
1.7	S2 Grupo	Revisión	10/09/2020
1.8	S2 Grupo	Revisión	30/04/2021
1.9	S2 Grupo	Revisión	22/06/2021

Índice de Contenidos

1 Introducción

1.1 Referencia ST

Título: GLORIA_ASE_DS

Versión: v1.9

Autor: S2 Grupo

1.2 Referencia TOE

Nombre del TOE: GLORIA

Versión del TOE: v5.6.0

Desarrollador del TOE: S2 Grupo

1.3 Visión general del TOE

1.3.1 Uso del TOE

GLORIA, **G**estor de **LO**gs para **R**esponder ante **I**ncidentes y **A**menazas, es una plataforma para la gestión de incidentes y amenazas de seguridad informática a través de técnicas de correlación compleja de eventos. La solución va un paso más allá de las capacidades de **SIEM** (Security Information and Event Management), proporcionando, además de la monitorización, almacenamiento y procesado de la información, capacidades de gestión de servicios para un centro de operaciones de seguridad.

Los componentes que conforman la plataforma ofrecen las siguientes funcionalidades:

- Monitorización de entornos tecnológicos (IT/OT), recolección de eventos de seguridad y análisis de la información.
- Análisis basado en inteligencia, a través de técnicas de correlación compleja de eventos que sirve de base para el desarrollo y parametrización de los mismos.
- Gestión del servicio mediante una consola única de gestión de alertas e incidentes que recoge todas las incidencias o alertas automáticas generadas por el sistema de correlación.
- Cuadro de mando.

1.3.2 Tipo de 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:

ARGOS: componente de monitorización y recolección de eventos de seguridad

TRITON: componente de inteligencia, correlación

EMAS: componente de gestión del servicio

HERA: componente de cuadro de mando

1.3.3 Funcionalidad principal de seguridad

GLORIA es una plataforma para la gestión de incidentes y amenazas de ciberseguridad que ayuda a identificar, mediante la generación de alertas en la consola de gestión, posibles amenazas a las organizaciones con la aplicación de técnicas de correlación compleja de eventos sobre los registros de seguridad generados por los diferentes dispositivos de seguridad de la organización.

El TOE dispone de mecanismos de seguridad para garantizar que únicamente el personal autorizado puede utilizarlo.

Las características de seguridad son:

Autenticación: no es posible realizar ninguna acción en el TOE sin haber realizado previamente una autenticación. El usuario accede a los componentes a través de la interfaz específica de cada uno, pero basado en un control de la autenticación centralizado en la consola de gestión, EMAS.

Autorización: es posible definir roles de acceso a los diferentes componentes. Cada componente, a su vez, puede disponer de roles específicos internos para su funcionamiento, controlado así de forma detallada qué puede hacer cada usuario. La funcionalidad ofrecida a cada usuario se determina a partir de los roles que tenga asignados, siendo estos roles atributos de seguridad de cada uno de los usuarios.

Aseguramiento: garantiza que, pasado un tiempo de inactividad configurable, la sesión de los componentes de **GLORIA** se cerrarán automáticamente, evitando el acceso a la información.

Comunicaciones: Las comunicaciones entre los componentes de **GLORIA** se realizan en una red interna aislada, mientras que las que se realizan desde fuera del TOE se hacen mediante protocolos seguros.

Auditoría: Todos los intentos de inicios de sesión y accesos a alertas se registran en ficheros de log para su posterior consulta por parte de un usuario con privilegios.

1.3.4 Hardware/Software/Firmware exentos al TOE

Los componentes de **GLORIA** se sirven en imágenes virtuales (.ova) preparadas para su despliegue sobre un hipervisor VMWare ESXi.

Las imágenes se publican en un repositorio privado de S2 Grupo (con acceso cifrado y protegido por contraseña) para la descarga por parte del cliente, preconfiguradas con el direccionamiento acordado previamente con el propio cliente. De este modo, el cliente puede proceder a la descarga de las imágenes y el despliegue en su hipervisor.

Existen una serie de elementos software (como el hipervisor, el sistema operativo o productos Open Source que son empleados por el TOE) que son necesarias para su ejecución y forman parte de las condiciones de entorno de la aplicación:

Hipervisor VMWare ESXi, versión 5.1 o superior

Sistema Operativo máquinas virtuales: CentOS 7, versión 7.9

Servidor de aplicaciones Apache Tomcat: versión 7.0

Servidor de aplicaciones Apache: versión 2.4

Elementos no accesibles desde el exterior de **GLORIA**:

Gestor de colas: RabbitMQ, versión 3.6

Gestor de Base de datos: PostgreSQL, versión 9.2

Gestor de Documentos: ElasticSearch, versión 6.

Máquina virtual Java: versión 1.8

Para acceder a la interfaz web se deberá de disponer de un navegador web en un equipo que esté en la misma red que la interfaz de gestión del TOE. En concreto, los navegadores soportados por GLORIA son los siguientes:

- Chrome: a partir de la versión 74
- Firefox: a partir de la versión 66
- Edge: a partir de la versión 12
- Internet Explorer: a partir de la versión 11

En cualquier otro navegador, no es posible garantizar que la visualización de la interfaz de usuario sea la esperada, sin embargo, los datos visualizados sí serán los mismos en todos los navegadores.

Los recursos recomendados para las máquinas virtuales de los componentes de GLORIA son los siguientes:

Máquina virtual	Requisitos básicos			
	vCPU	RAM	HD (S.O)	HD (datos)
ARGOS	4	6 GB	60 GB	
ARGOS-LogServer	8	8 GB	20 GB	
ARGOS-LogData1	8	16 GB	20 GB	750 GB
ARGOS-LogData2	8	16 GB	20 GB	750 GB
TRITON	8	16 GB	40 GB	
EMAS	4	6 GB	60 GB	

Tabla 2 – Recursos recomendados despliegue componentes GLORIA

Estos recursos básicos aproximados se calculan considerando una volumetría de 500 EPS, un tamaño medio de mensaje de 1 Kb y una retención de 15 días de los registros de las fuentes de seguridad.

El incremento de los valores de estos parámetros supone una ampliación de capacidades de la plataforma. Puede suponer un aumento de recursos en las máquinas virtuales de ARGOS, TRITON o EMAS, o un aumento de recursos y/o instancias de ARGOS-LogServer y ARGOS-LogData.

1.3.5 *Funcionalidad excluida de la evaluación*

La siguiente funcionalidad incluida en **GLORIA** no se encuentra dentro del alcance de la evaluación:

- Activación/Desactivación de fuentes y agentes de recolección
- Configuración de expresiones regulares, patrones y pipelines para la adquisición de logs
- Incorporación de nuevas capacidades de inteligencia mediante el desarrollo de nuevas reglas de correlación
- Integración con un sistema remoto que permita importar inteligencia (ioc, analizadores…)
- Integración con un sistema de restauración y copias de seguridad
- Mecanismo de bloqueo temporal de autenticación en la interfaz de gestión.

1.4 Descripción del TOE

Los componentes de **GLORIA** se pueden observar en el siguiente diagrama explicativo de la arquitectura lógica y son descritos a continuación

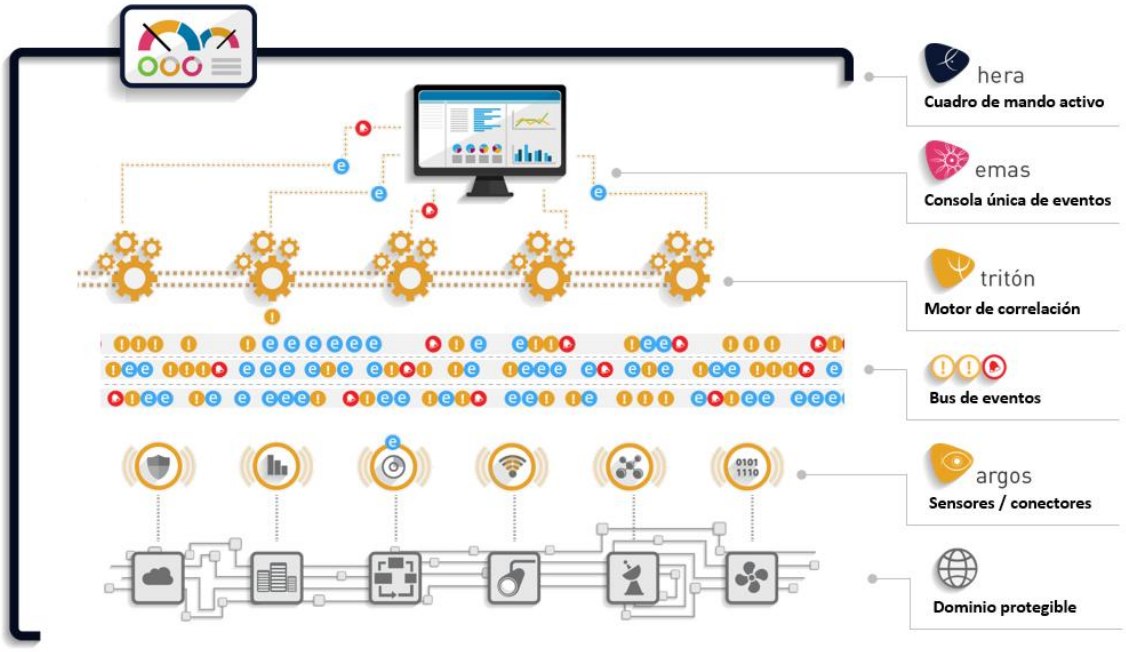


Figura 1. Modelo de operación por niveles de la plataforma GLORIA

1.4.1 Alcance lógico

El ámbito lógico del TOE se define agrupando funcionalidades en las siguientes clases funcionales que se detallarán a continuación en este Objetivo de seguridad.

Las características de seguridad son:

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.

Ilustración 1 Mensaje error tras una autenticación incorrecta en cualquiera de los componentes ARGOS, TRITON, EMAS y HERA

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.

1.4.2 Alcance físico

El ámbito físico del TOE, **GLORIA**, se define como:

- **EMAS:** componente para las tareas de gestión del servicio y el componente HERA de cuadro de mando. Proporcionada en el fichero de plantilla de máquina virtual **GLORIA -EMAS-v 5.6.0 .ova** con el cual se despliega la máquina virtual asociada a estos componentes.
- **TRITON:** componente para realizar las acciones de correlación. Proporcionada en el fichero de plantilla de máquina virtual **GLORIA-TRITON-v5.6.0.ova** con el cual se despliega la máquina virtual asociada a este componente.
- **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** con el cual se despliega la máquina virtual asociada a este componente.
- **ARGOS-LogServer:** subcomponente para el tratamiento de los eventos de seguridad. Proporcionada en el fichero de plantilla de máquina virtual **GLORIA -ARGOS-LogServer-v5.6.0.ova**, con el cual se despliega la máquina virtual asociada a este subcomponente.
- **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 -ARGOS-LogData1-v5.6.0.ova** y **GLORIA-ARGOS-LogData2-v5.6.0.ova**¸ con los cuales se despliegan las dos máquinas virtuales que componen el clúster asociado a este subcomponente.

La distribución de estos entregables se realiza mediante la compartición en el repositorio https://minube.s2grupo.es. Los ficheros OVA que se distribuyen son marcados mediante la

huella SHA256, para asegurar que no son alterados ni modificados antes de su distribución. En el proceso de entrega al cliente, se comunica al cliente via email la URL de descarga, la Contraseña de acceso, la fecha de vigencia del enlace facilitado a partir de la cuál dejará de estar disponible la descarga y el Hash SHA256 de cada fichero ova y los manuales de administración y usuario. Pudiendo garantizar, mediante esta comprobación, que los elementos que se van a desplegar son los que tienen que ser y no han sido manipulados.

La siguiente tabla muestra la lista de elementos que se deben descargar de la ruta de descarga:

Componente	Fichero OVA	SHA256
ARGOS	GLORIA-ARGOS-v5.6.0.ova	GLORIA-ARGOS-v5.6.0.sha
ARGOS-LogServer	GLORIA-ARGOS-LogServer-v5.6.0.ova	GLORIA-ARGOS-LogServer-v5.6.0.sha
ARGOS-LogData1	GLORIA-ARGOS-LogData1-v5.6.0.ova	GLORIA-ARGOS-LogData1-v5.6.0.sha
ARGOS-LogData2	GLORIA-ARGOS-LogData2-v5.6.0.ova	GLORIA-ARGOS-LogData2-v5.6.0.sha
TRITON	GLORIA-TRITON-v5.6.0.ova	GLORIA-TRITON-v5.6.0.sha
EMAS	GLORIA-EMAS-v5.6.0.ova	GLORIA-EMAS-v5.6.0.sha

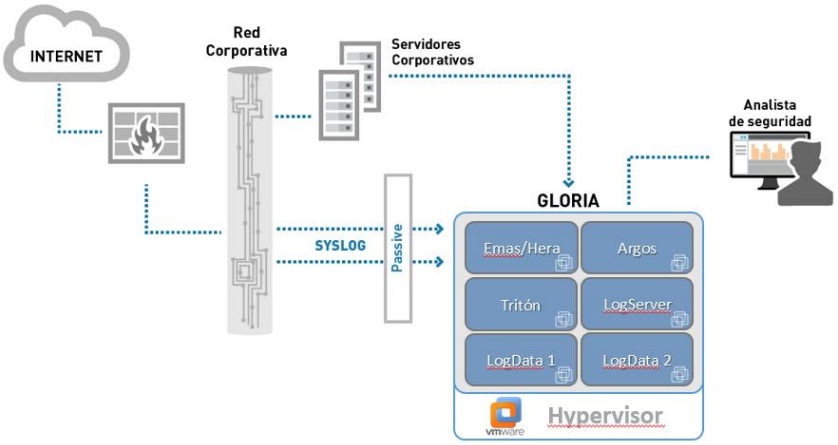
Tabla 1 – Ficheros que se encuentran para la descarga

Las guías de usuario y de administrador son marcados mediante la huella SHA256, Estos archivos son accesibles a través de la compartición del repositorio de S2 Grupo albergado en "https://minube.s2grupo.es". En el repositorio también se ubicarán los ficheros de texto que indican el hash SHA256 de las siguientes guías.

- Una guía de usuario llamada **"GLORIA_AGD_OPE_v 5.6.0 .pdf"**, en formato ".pdf". Esta guía hace referencia a **GLORIA_AGD_OPE_v1.4**.
- Una guía de administrador llamada "**GLORIA_AGD_PRE_v 5.6.0 .pdf**", en formato ".pdf". Esta guía hace referencia a **GLORIA_AGD_PRE_v1.5**.

1.4.3 Configuración evaluación del TOE

Para realizar la evaluación del TOE se ha desplegado un entorno donde se ejecutan todas sus imágenes.



En el diagrama anterior se observa que **GLORIA** 5.6.0 se encuentra conectada a la red corporativa de la organización para recibir el tráfico SYSLOG de la red del cliente y un analista se conecta directamente a **GLORIA** 5.6.0 para realizar el análisis.

Los recursos utilizados para la evaluacion configurada son los siguientes:

Máquina virtual	Requisitos			
	vCPU	RAM	HD (S.O)	HD (datos)
ARGOS	4	6 GB	60 GB	
ARGOS-LogServer	8	8 GB	20 GB	
ARGOS-LogData1	8	16 GB	20 GB	750 GB
ARGOS-LogData2	8	16 GB	20 GB	750 GB
TRITON	8	16 GB	40 GB	
EMAS	4	6 GB	60 GB	

Tabla 2 – Recursos recomendados despliegue componentes GLORIA

Posteriormente, el servidor donde se encuentran las máquinas desplegadas tiene instalado el hipervisor VMWare ESXi, versión 5.1

1.5 Descripción del producto

GLORIA es una herramienta de apoyo al analista de seguridad para la recolección, modelado y centralización de registros y eventos de seguridad tanto de infraestructuras IT como de infraestructuras OT, dentro de la organización en la que se encuentra desplegado.

Para poder realizar dicha tarea, es necesaria la adquisición, centralizado, procesamiento y análisis de los registros de los diferentes sistemas que conforman la plataforma tecnológica dentro del alcance del servicio y almacenarlos en disco para su posterior consulta con un potente motor de indexación y búsqueda. De esta gestión se encarga el componente **ARGOS** y sus subcomponentes asociados.

Así mismo, **GLORIA** permite la correlación y procesamiento de los eventos remitidos por el sistema de monitorización, con capacidad de realizar correlación simple, compleja y multinivel en base a reglas de correlación predefinidas y reglas personalizables de forma sencilla e intuitiva mediante un lenguaje DSL (Domain Specific Language), a través del componente **TRITON**.

Para gestionar de forma unificada las alertas e incidentes anteriores y otras definidas de forma manual independientes de su origen se utiliza el componente de **EMAS**, basado en la gestión del ciclo de vida del incidente (Incident Handling) desde su creación hasta su resolución, y que se apoya en una base de datos de activos (CMDB) que recoge los activos a proteger, y una definición del catálogo de servicios con soporte para asegurar una respuesta basada en procedimientos, y siempre vigilando los marcos de Acuerdos de Nivel de Servicio (ANS o SLA del inglés Service Level Agreement).

Finalmente, como cuadro de mando **GLORIA** utiliza el componente **HERA**, el cual cubre indicadores de disponibilidad, calidad de servicio actividad y riesgo en tiempo procesando los

datos generados por **GLORIA** y otros sistemas de forma automática y permitiendo un posterior análisis histórico.

El TOE, además provee mecanismos de seguridad para garantizar que únicamente el personal autorizado puede hacer uso de él.

2 Declaración de conformidad

Esta declaración de seguridad es conforme, en su estructura y contenido, a los requisitos de la norma **Common Criteria, versión 3.1, revisión 5 y nivel de evaluación EAL2**.

Todos los requisitos de seguridad, tanto funcionales como de garantía, incluidos en esta declaración de seguridad se han extraído de las partes 2 y 3 de la norma Common Criteria, con algunos componentes funcionales extendidos.

En concreto, se consideran las siguientes condiciones:

> CC Part 2 extended: la parte 2 de la norma (ccpart2v3.1r5) se considera de forma extendida en esta declaración de seguridad.
>
> CC Part 3 conformant: la parte 3 de la norma (ccpart3v3.1r5) se considera de forma estricta en esta declaración de seguridad.

Esta declaración de seguridad no satisface ningún perfil de protección.

Esta declaración de seguridad es conforme al paquete de garantía EAL2 aumentado con ALC_FLR.1 cómo se define en el CC, parte 3.

3 Definición del problema de seguridad

Esta sección describe los aspectos de seguridad del entorno operativo de **GLORIA** y su uso esperado en dicho entorno. Incluye la declaración del entorno operativo TOE que identifica y describe:

Las amenazas conocidas que serán contrarrestadas por el TOE;

Las políticas de seguridad de la organización que el TOE debe cumplir;

El uso del TOE en el entorno operativo sugerido.

A continuación se definen los actos, hipótesis y amenazas que son aplicables a esta definición.

3.1 Alcance del TOE

El TOE que se va a proceder a certificar consta del siguiente alcance:

Control de acceso al TOE

Identificación y autenticación

Control de sesiones

Gestión segura de los puntos anteriores

3.2 Activos del TOE

Los principales activos a proteger son:

A.EVENTOS: confidencialidad e integridad de los registros enviados por los dispositivos de seguridad y activos de la organización tratados, adquiridos, procesados, normalizados y almacenados en **GLORIA.**

A.INCIDENCIAS: confidencialidad e integridad de los resultados de las ejecuciones de los diferentes correladores (procesadores inteligentes de logs) a partir de los registros enviados por los dispositivos de seguridad y activos de la organización.

A.USUARIOS: Confidencialidad de la configuración de acceso de los usuarios como son las credenciales de acceso y el listado de roles asociados.

A.ROLES: Confidencialidad de la información de pantallas / funcionalidades / componentes a las que tendrá acceso cada usuario que se encuentre relacionado con cada uno de ellos.

A.AUDITORIA: Confidencialidad e integridad de los registros de auditoría de seguridad del TOE.

A.COMUNICACIONES: Confidencialidad e integridad de los datos en tránsito de las interfaces accesibles por los usuarios (SSH y HTTPS).

3.3 Hipótesis

Este es el principal supuesto:

AS.ENTORNO: GLORIA se entrega en máquinas virtuales que se encuentran bastionadas y configuradas para evitar el acceso directo a la información almacenada.

AS.INSTALACION: La instalación y configuración del TOE se realizará de acuerdo a las instrucciones de instalación proporcionadas.

AS.OPERATIVO: Los sistemas operativos empleados por los diferentes componentes de **GLORIA** (CentOS7) se consideran condición de entorno, por lo que las vulnerabilidades propias de estos deberán ser solucionadas por su fabricante, al igual que los componentes software instalados desde el repositorio oficial del Sistema Operativo (apache, tomcat…). Así mismo, el control de usuarios del sistema y su acceso ssh, lo gestiona también el propio sistema operativo. En cada actualización del TOE se actualizan los elementos de paquetería, con lo cual, en caso de haber algún paquete obsoleto o con una vulnerabilidad, éste se actualizará cuando la versión esté disponible en los repositorios oficiales.

AS.LOCALIZACION: El servidor que aloja el hipervisor donde se ejecuta el TOE se encuentra situado dentro de una instalación segura y controlada donde no se permite el acceso. Se considera dentro de este entorno la red corporativa, el firewall y los dispositivos de seguridad de la organización.

AS.ADMINISTRADOR: Se considera que los usuarios con rol de administrador de la interfaz web (https) son competentes y confiables con el uso de la aplicación, por lo que no van a atentar contra la integridad del TOE.

AS.CONFIGURADOR: Se considera que el configurador de la interfaz de gestión (ssh) es competente y confiable con el uso de la aplicación, por lo que no va a atentar contra la integridad del TOE.

AS.TIME: El entorno operacional garantiza que se entregan timestamps que sean confiables y el TOE obtiene las referencias temporales del sistema operativo donde reside.

AS.GESTION: La comunicación con la interfaz de gestión está cifrada mediante SSH que solicita la apropiada autenticación.

3.4 Amenazas

Las amenazas identificadas en **GLORIA** son:

T.ACCESO: un atacante consigue acceso a los registros de los dispositivos de seguridad de la organización (**A.EVENTOS**), incidencias (**A.INCIDENCIAS**) identificadas, registros de auditoría (**A.AUDITORIA**) a las que no tiene concedido permiso de consulta o al contenido del canal de comunicación (**A.COMUNICACIONES**).

T.FALSIFICACION: un atacante consigue modificar o suprimir los registros de los dispositivos de seguridad almacenados (**A.EVENTOS**), los registros de auditoría (**A.AUDITORIA**), incidencias identificadas (**A.INCIDENCIAS**) o alterar el contenido del canal de comunicación (**A.COMUNICACIONES**).

T.SUPLANTACION: un atacante consigue acceder con el perfil de otro usuario **(A.USUARIOS)** o con unos roles **(A.ROLES)** distintos a los que le corresponden a su propio usuario.

4 Objetivos de Seguridad

Los objetivos de seguridad son declaraciones de alto nivel, concisas y abstractas de la solución al problema expuesto en la sección anterior, que contrarrestan las amenazas y cumplen con las políticas de seguridad y las hipótesis.

Estos se dividen en dos tipos:

objetivos de seguridad para el TOE

objetivos de seguridad para el entorno operacional

4.1 Objetivos de seguridad del TOE

Los objetivos de seguridad para el TOE son:

O.AUTENTICACION: el TOE mostrará la interfaz de autenticación cuando se acceda a alguno de sus componentes y no permitirá el acceso a ninguna otra de sus interfaces sin que se haya realizado antes una autenticación éxitosa.

O.ACCESO: el TOE permitirá la definición de usuarios y sus correspondientes políticas de acceso.

O.AUDITORIA: el TOE registrará los intentos de inicios de sesión en los componentes de GLORIA y los accesos a los eventos de la consola de gestión y no permite la manipulación ni la eliminación de los registros de auditoría. Además, el TOE protege dichos registros de accesos no autorizados.

O.COMUNICACIONES: los componentes del TOE se comunican a través de una red interna aislada y las comunicaciones de los usuarios se realizan mediante el uso de protocolos seguros.

4.2 Objetivos de seguridad para el entorno operacional

Los objetivos de seguridad para el entorno operacional del TOE son:

OE.ENTREGA: GLORIA se entrega en forma de máquinas virtuales de los distintos componentes que la conforman. Cada componente tiene su sistema operativo bastionado siguiendo las recomendaciones detalladas en el apartado *Perfil de seguridad* del documento de especificaciones funcionales, destacando los controles de configuración de:

- *Instalación y Mantenimiento de Software*
- *Permisos y máscaras de ficheros*
- *Política de SELinux*
- *Cuentas y control de Acceso*
- *Red y Firewall*
- *Syslog*
- *Auditoría del Sistema*
- *Servicios*

OE.DESPLIEGUE: El administrador se asegurará de seguir los pasos de los manuales de instalación y uso del producto para realizar el despliegue de forma segura.

OE.ADMINISTRADOR: Los usuarios con el rol de administrador de la interfaz web (https) son competentes y confiables en el uso de la aplicación, por lo que no van a atentar contra la integridad del TOE.

OE.CONFIGURADOR: el configurador de la interfaz de gestión (ssh) se considera competente y confiable con el uso de la aplicación, por lo que no va a atentar contra la integridad del TOE.

OE.TIME: el entorno operacional garantiza que se entregan timestamps que sean confiables y el TOE obtiene las referencias temporales del sistema operativo.

OE.OPERATIVO: La paquetería interna de cada componente que conforma **GLORIA** , depende únicamente de su operativo. En cada actualización del TOE se actualizan los elementos de la paquetería, aunque podría ocurrir que existiese algún paquete obsoleto o con algún tipo de vulnerabilidad que no sea actualizado hasta que se encuentre disponible en los repositorios oficiales, pudiendo pasar varios meses hasta que los paquetes afectados se actualicen.

OE.LOCALIZACION: el entorno operacional garantizará que **GLORIA** se encuentra dentro de una instalación segura y controlada, conectado a la red corporativa y protegido por los dispositivos de seguridad de la organización.

OE.GESTION: El sistema operativo donde reside **GLORIA** cifra mediante SSH la comunicación con la interfaz de gestión. El protocolo SSH esta implementado de tal

manera que solicita automáticamente credenciales para llevar a cabo la autenticación. La configuración del servicio de SSH del sistema operativo ha sido realizada siguiendo las recomendaciones detalladas en el apartado *Perfil de seguridad* del documento de especificaciones funcionales, destacando las siguientes recomendaciones para la protección de los accesos de usuarios:

- *Permitir únicamente protocolo SSHv2*
- *Deshabilitar la autenticación por GSSAPI*
- *Deshabilitar la autenticación por Kerberos*
- *Habilitar el uso de la comprobación de seguridad en modo estricto*
- *Habilitar el uso de separación de privilegios*
- *Establecer el temporizador de inactividad para las sesiones SSH*
- *Deshabilitar el soporte de SSH para ficheros .rhosts*
- *Deshabilitar el soporte de SSH para hosts conocidos por el usuario*
- *Deshabilitar el soporte de SSH para autenticar en base a RSA de hosts*
- *Deshabilitar la autenticación basada en hosts*
- *Deshabilitar el inicio de sesión por SSH para el usuario root*
- *Deshabilitar el inicio de sesión por SSH para cuentas sin clave*
- *Protección de cuentas mediante PAM*
- *Establecer el algoritmo de hashing a SHA-512*

4.3 Justificación de los objetivos de seguridad

4.3.1 Objetivos para GLORIA

La siguiente tabla permite representar la relación entre cada uno de los objetivos de seguridad exigibles y sus correspondientes amenazas identificadas:

		Amenazas		
		T.ACCESO	T.FALSIFICACIÓN	T.SUPLANTACIÓN
Objetivos de Seguridad	O.AUTENTICACIÓN	X	X	X
	O.ACCESO	X	X	X
	O.AUDITORIA	X	X	
	O.COMUNICACIONES	X	X	

Tabla 3 – Relación de objetivos y amenazas

De esta forma, la relación entre cada uno de los objetivos de seguridad que permiten mitigar las amenazas identificadas es la siguiente:

O.AUTENTICACION: el TOE no permitirá el acceso a sus interfaces sin que se haya realizado antes una autenticación exitosa, por lo que no se podrán consultar los datos

almacenados (**T.ACCESO**), ni realizar modificaciones sobre los datos existentes (**T.FALSIFICACIÓN**), ni simular el acceso de un usuario (**T.SUPLANTACION**).

O.ACCESO: el TOE permitirá la definición de usuarios y sus correspondientes políticas de acceso, por lo que no se podrán consultar los datos almacenados sin los permisos de acceso adecuados (**T.ACCESO**), ni realizar modificaciones sobre los datos existentes (**T.FALSIFICACIÓN**), ni obtener el acceso de un usuario distinto al autenticado (**T.SUPLANTACION**).

O.AUDITORIA: el TOE registra todos los accesos, no permite el acceso a los registros de auditoría excepto al usuario administrador (**T.ACCESO**), y no existe funcionalidad ninguna para su manipulación o eliminación (**T.FALSIFICACION**).

O.COMUNICACIONES: el TOE protege las comunicaciones entre él mismo y los usuarios a través de un canal seguro de navegación que impide el acceso a la información (**T.ACCESO**) y su posible manipulación (**T.FALSIFICACIÓN**) por parte de un atacante.

4.3.2 Objetivos para el entorno operacional de GLORIA

La siguiente tabla permite representar la relación entre cada una de las hipótesis de seguridad exigibles en el TOE y sus correspondientes objetivos de seguridad del entorno operacional relacionadas.

		OE.ENTREGA	OE.DESPLIEGUE	OE.TIME	OE.OPERATIVO	OE.LOCALIZACIÓN	OE.ADMINISTRADOR	OE.CONFIGURADOR	OE.GESTION
Suposiciones	AS.ENTORNO	X							
	AS.INSTALACION		X						
	AS.OPERATIVO				X				
	AS.LOCALIZACION					X			
	AS.ADMINISTRADOR						X		
	AS.CONFIGURADOR							X	
	AS.TIME			X					
	AS.GESTION								X

Tabla 4 – Relación entre hipótesis y objetivos de seguridad del entorno operacional

De esta forma, la relación entre cada uno de las hipótesis de seguridad y sus correspondientes objetivos de seguridad del entorno operacional es la siguiente:

AS.ENTORNO: GLORIA será desplegado en un entorno seguro y adecuadamente configurado, por tanto se consideran automáticamente cubiertos las objetivos de seguridad del entorno operacional relacionados con el TOE (**OE.ENTREGA**).

AS.INSTALACION: La instalación y configuración del TOE se realizará de acuerdo a las instrucciones de instalación proporcionadas, por tanto se consideran automáticamente

cubiertos los objetivos de seguridad del entorno operacional relacionados con el modo de configuración del mismo (**OE.DESPLIEGUE).**

AS.OPERATIVO: El sistema operativo (CentOS7) se mantiene actualizado en cada actualización (**OE.OPERATIVO**) solventando los problemas de seguridad que se hayan descubierto desde la última actualización.

AS.LOCALIZACION: El conjunto de máquinas virtuales que componen el TOE sólo ejecutará este en un entorno controlado (**OE.LOCALIZACIÓN**).

AS.ADMINISTRADOR: Los administradores de la interfaz web (**OE.ADMINISTRADOR**) se encargan de las tareas de gestión de usuarios y sus permisos.

AS.CONFIGURADOR: Sólo el operador encargado de la configuración e instalación (**OE.CONFIGURADOR**) de los componentes del TOE accederá a la interfaz ssh y escalará con permisos de superusuario para realizar dichas tareas.

AS.TIME: El TOE será provisto de fuentes de tiempo fiable obtenidas del sistema operativo donde reside (**OE.TIME)**.

AS.GESTION: El acceso a **GLORIA** a través de la interfaz de gestión es seguro debido a que se realiza empleando SSH. El protocolo SSH proporciona mecanismos de autenticación (**OE.GESTION**).

5 Definición de requisitos funcionales extendidos de seguridad

Los requisitos funcionales incluidos en esta sección son derivados de la Parte 2 del Common Criteria para la Seguridad en Tecnologías de Información Parte 2 Versión 3.1 Revisión 5 con algunos componentes funcionales extendidos descritos a continuación.

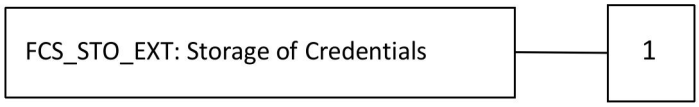
5.1.1 Class FCS: Cryptographic Support

5.1.1.1 FCS_STO_EXT.1: Storage of Credentials

Family Behaviour

Esta declaración de seguridad presenta el requisito extendido **FCS_STO_EXT Storage of credentials** debido a la necesidad de introducir un requisito que garantice que las credenciales persistentes (claves secretas, claves privadas PKI o contraseñas) se almacenen de forma segura.

Component leveling



FCS_STO_EXT.1 Almacenar las credenciales en la memoria no volátil.

Management: FCS_STO_EXT.1

There are no management activities foreseen.

Audit: FCS_STO_EXT.1

There are no auditable events foreseen.

FCS_STO_EXT.1 Storage of Credentials

Hierarchical to: No other components.

Dependencies: No other components.

FCS_STO_EXT.1.1 The application shall [**selection**: not store any credentials, invoke the functionality provided by the platform to securely store [**assignment**: list of credentials], implement functionality to securely store [**assignment**: list of credentials]] to non-volatile memory.

5.1.1.2 FCS_HTTPS_EXT.1: HTTPS Protocol

Family Behaviour

Esta declaración de seguridad presenta el requisito extendido **FCS_HTTPS_EXT HTTPS Protocol** debido a la necesidad de introducir un requisito para proteger las sesiones de administración remota entre el TOE y los usuarios.

Component leveling

FCS_HTTPS_EXT.1: HTTPS requires that HTTPS be implemented according to RFC 2818 and supports TLS.

Management: **FCS_HTTPS_EXT.1**

There are no management activities foreseen.

Audit: FCS_HTTPS_EXT.1

There are no auditable events foreseen.

FCS_HTTPS_EXT.1 HTTPS Protocol

Hierarchical to: No other components

Dependencies: No other components

FCS_HTTPS_EXT.1.1

The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2

The application shall implement HTTPS using TLS (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bits TLS 1.2).

5.1.2 Class FTP: Trusted Path/Channel

5.1.2.1 FTP_DIT_EXT.1: Protection of Data in Transit

Family behaviour

Esta declaración de seguridad presenta el requisito extendido **FTP_DIT_EXT.1** Protection of Data in Transit, el cual se introduce debido a la necesidad de crear un requisito por el cual se cifren los datos que está en tránsito entre el TOE y otro producto IT confiable.

Component leveling

FTP_DIT_EXT: Protection of Data in Transit	1

FTP_DIT_EXT.1 Cifrado de datos a través de un protocolo entre el TOE y otro producto IT confiable.

Management: FTP_DIT_EXT.1

There are no management activities foreseen.

Audit: FTP_DIT_EXT.1

There are no auditable events foreseen,

FTP_DIT_EXT.1 Protection of Data in Transit

Hierarchical to: No other components.

Dependencies: No other components.

FTP_DIT_EXT.1.1 The application shall [**selection**:

- not transmit any [**selection**: data, sensitive data],
- encrypt all transmitted [**selection**: sensitive data, data] with [**selection:** HTTPS in accordance with FCS_HTTPS_EXT.1],
- invoke platform-provided functionality to encrypt all transmitted sensitive data with [**selection**: HTTPS],
- invoke platform-provided functionality to encrypt all transmitted data with [**selection**: HTTPS]

] between itself and another trusted IT product.

5.1.3 Class FDP: User Data Protection

5.1.3.1 FDP_NET_EXT.1: Network Communications

Family behaviour

Esta declaracion de seguridad presenta el requisito extendido **FDP_NET_EXT.1 Network Communications**, el cual se introduce debido a la necesidad de restringir las comunicaciones de red entrantes y salientes solo a aquellas requeridas, o a las comunicaciones de red iniciadas por el usuario.

Component leveling

FDP_NET_EXT Network Communications	1

FDP_NET_EXT.1 Cifrado de datos a través de un protocolo entre el TOE y los usuarios.

Management: FDP_NET_EXT.1

There are no management activities foreseen.

Audit: FDP_NET_EXT.1

There are no auditable events foreseen,

FDP_NET_EXT.1 Network Communications

Hierarchical to: No other components.

Dependencies: No other components.

FDP_NET_EXT.1: The application restrict network communication to [**selection**: no network communication, user-initiated communication for [**assignment**: list of functions for which the user can initiate network communication], respond to [**assignment**: list of remotely initiated communication], [**assignment**: list of application-initiated network communication]].

6 Requisitos de seguridad del TOE

Los requisitos funcionales escogidos para cubrir el alcance del TOE son:

Functional Class	Functional Components	
FAU: Security Audit	FAU_GEN	FAU_GEN.1
	FAU_SAR	FAU_SAR.1
		FAU_SAR.2
	FAU_STG	FAU_STG.2
FCS: Cryptographic Support	FCS_STO_EXT	FCS_STO_EXT.1
	FCS_HTTPS_EXT	FCS_HTTPS_EXT.1
FDP: User Data Protection	FDP_NET_EXT	FDP_NET_EXT.1
FIA:Identification and authentication	FIA_AFL	FIA_AFL.1
	FIA_ATD	FIA_ATD.1
	FIA_UAU	FIA_UAU.2
	FIA_UID	FIA_UID.2
FMT: Security Management	FMT_MOF	FMT_MOF.1
	FMT_MTD	FMT_MTD.1
	FMT_SMF	FMT_SMF.1
	FMT_SMR	FMT_SMR.1
FTA: TOE Access	FTA_SSL	FTA_SSL.1
		FTA_SSL.3
		FTA_SSL.4
	FTA_TSE	FTA_TSE.1
FTP: Trusted Path/Channel	FTP_DIT_EXT	FTP_DIT_EXT.1

Tabla 5 – Requisitos funcionales relacionados con el alcance

6.1 Requisitos funcionales de seguridad

6.1.1 Class FAU: Security Audit

6.1.1.1 Audit data generation (FAU_GEN)

Esta familia cubre los siguientes requisitos funcionales de seguridad:

FAU_GEN.1 con las siguientes características:

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

6.1.1.1.1 FAU_GEN.1.1

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

Start-up and shutdown of the audit functions;

All auditable events for the **[selection: not specified]** level of audit; and

[assignment:

- **Autenticación correcta (inicio y cierre de sesión)**
- **Intento de autenticación fallido**
- **Acceso a los componentes del TOE**
- **Acceso en modo lectura o escritura a las alertas de la consola de gestión**

].

6.1.1.1.2 FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

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

For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST**, [assignment:**

- **en un inicio de sesión satisfactorio, se registra el identificador de sesión y componente al que se accede**
- **en un acceso a una alerta se registra el identificador de la alerta**

].

6.1.1.2 Restricted Audit Review (FAU_SAR)

Esta familia cubre los siguientes requisitos funcionales de seguridad:

FAU_SAR.1 con las siguientes características:

- *Hierarchical to: No other components.*
- *Dependencies: FAU_GEN.1 Audit Data Generation*

FAU_SAR.2 con las siguientes características:

- *Hierarchical to: No other components.*
- *Dependencies: FAU_SAR.1 Audit Review*

6.1.1.2.1 FAU_SAR.1.1

The TSF shall provide **[assignment: usuario con el rol administrador]** with the capability to read **[assignment: toda la información]** from the audit records.

6.1.1.2.2 FAU_SAR.1.2

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

6.1.1.2.3 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.

6.1.1.3 Security Audit Event Storage (FAU_STG)

Esta familia cubre los siguientes requisitos funcionales de seguridad:

FAU_STG.2 con las siguientes características:

- *Hierarchical to: No other components*
- *Dependencies: FAU_GEN.1 Audit data generation*

6.1.1.3.1 FAU_STG.2.1

The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

6.1.1.3.2 FAU_STG.2.2

The TSF shall be able to **[selection: prevent]** unauthorized modifications to the stored audit records in the audit trail.

6.1.1.3.3 FAU_STG.2.3

The TSF shall ensure that **[assignment: 10 ficheros de 10 MB]** stored audit records will be maintained when the following conditions occur: **[selection: audit storage exhaustion]**.

6.1.2 Class FCS: Cryptographic Support

6.1.2.1 Storage of Credentials (FCS_STO_EXT.1)

Esta familia cubre los siguientes requisitos funcionales de seguridad:

FCS_STO_EXT.1 con las siguientes características:

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

6.1.2.1.1 FCS_STO_EXT.1.1

The application shall **[selection: invoke the functionality provided by the platform to securely store [assignment: todas las credenciales de usuario]]** to non-volatile memory.

6.1.2.2 HTTPS Protocol (FCS_HTTPS_EXT.1)

FCS_HTTPS_EXT.1 con las siguientes características:

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

6.1.2.2.1 FCS_HTTPS_EXT.1.1

The application shall implement the HTTPS protocol that complies with RFC 2818.

6.1.2.2.2 FCS_HTTPS_EXT.1.2

The application shall implement HTTPS using TLS (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bits TLS 1.2).

6.1.3 Class FDP: User Data Protection

6.1.3.1 Network Communications (FDP_NET_EXT)

Esta familia cubre los siguientes requisitos funcionales de seguridad:

FDP_NET_EXT.1 con las siguientes características:

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

6.1.3.1.1 FDP_NET_EXT.1.1

The application shall restrict network communication to **[selection: [assignment: a las interfaces de adquisición y procesamiento de tráfico]]**.

6.1.4 Class FIA: Identification and authentication

6.1.4.1 Authentication failure handling (FIA_AFL)

Esta familia cubre los siguientes requisitos funcionales de seguridad:

FIA_AFL.1 con las siguientes características:

- *Hierarchical to: No other components.*
- *Dependencies: FIA_UAU.1 Timing of authentication*

6.1.4.1.1 FIA_AFL.1.1

The TSF shall detect when **[selection: [assignment: 3]]** unsuccessful authentication attempts occur related to **[assignment: login].**

6.1.4.1.2 FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been [**selection: met]**, the TSF shall **[assignment: bloquear el acceso del usuario durante 15 minutos]**.

6.1.4.2 User attribute definition (FIA_ATD)

Esta familia cubre los siguientes requisitos funcionales de seguridad:

FIA_ATD.1 con las siguientes características:

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

6.1.4.2.1 FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: **[assignment: identificador de usuario y lista de roles de acceso a funcionalidades]**

6.1.4.3 User Authentication (FIA_UAU)

Esta familia cubre los siguientes requisitos funcionales de seguridad:

FIA_UAU.2 con las siguientes características:

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

6.1.4.3.1 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.

6.1.4.4 User Identification (FIA_UID)

Esta familia cubre los siguientes requisitos funcionales de seguridad:

FIA_UID.2 con las siguientes características:

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

6.1.4.4.1 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.

6.1.5 Class FMT: Security Management

6.1.5.1 Management of Functions in TSF (FMT_MOF)

Esta familia cubre los siguientes requisitos funcionales de seguridad:

FMT_MOF.1 con las siguientes características:

- *Hierarchical to: No other components.*
- *Dependencies: FMT_SMR.1 Security roles*
  FMT_SMF.1 Specification of Management Functions

6.1.5.1.1 FMT_MOF.1.1

The TSF shall restrict the ability to **[selection: modify the behavior of]** the functions **[assignment: gestionar el control de acceso de los usuarios]** to **[assignment: usuario con rol administrador].**

6.1.5.2 Specification of TSF data (FMT_MTD)

Esta familia cubre los siguientes requisitos funcionales de seguridad:

FMT_MTD.1 con las siguientes características:

- *Hierarchical to: No other components.*
- *Dependencies: FMT_SMR.1 Security roles*
  FMT_SMF.1 Specification of Management Functions

6.1.5.2.1 FMT_MTD.1.1

The TSF shall restrict the ability to **[selection: query, modify, delete, [assignment: create]]** the **[assignment: cuentas de usuario]** to **[assignment: usuario con rol administrador]**.

6.1.5.3 Specification of Management Functions (FMT_SMF)

Esta familia cubre los siguientes requisitos funcionales de seguridad:

FMT_SMF.1 con las siguientes características:

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

6.1.5.3.1 FMT_SMF.1.1

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

- **ver/crear/editar/eliminar usuarios y roles,**
- **realizar la asignación de roles a usuarios,**
- **asignación de pantallas a roles,**
- **modificar las contraseñas de los usuarios,**
- **gestionar el control de acceso de los usuarios**

].

6.1.5.4 Security Roles (FMT_SMR)

Esta familia cubre los siguientes requisitos funcionales de seguridad:

FMT_SMR.1 con las siguientes características:

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

6.1.5.4.1 FMT_SMR.1.1

The TSF shall maintain the roles **[assignment: Administrador, Técnico, Solo Lectura, Dirección N3, Dirección N4, Visor de Identificadores, Acceso Tritón, Acceso Argos y Acceso Hera y roles personalizados].**

6.1.5.4.2 FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.1.6 Class FTA: TOE Access

6.1.6.1 Session locking and termination (FTA_SSL)

Esta familia cubre los siguientes requisitos funcionales de seguridad:

FTA_SSL.1 con las siguientes características:

- *Hierarchical to: No other components.*
- *Dependencies: FIA_UAU.1 Timing of authentication*

FTA_SSL.3 con las siguientes características:

- *Hierarchical to: No other components*
- *Dependencies: No dependencies*

FTA_SSL.4 con las siguientes características:

- *Hierarchical to: No other components*
- *Dependencies: No dependencies*

6.1.6.1.1 FTA_SSL.1.1

The TSF shall lock an interactive session after **[assignment**: **30 minutos de inactividad]** by:

clearing or overwriting display devices, making the current contents unreadable;

disabling any activity of the user's data access/display devices other than unlocking the session.

Application note: Este requisito aplica para el componente emas.

6.1.6.1.2 FTA_SSL.1.2

The TSF shall require the following events to occur prior to unlocking the session: **[assignment: en emas, autenticarse correctamente de nuevo el usuario en la ventana de sesión caducada]**.

6.1.6.1.3 FTA_SSL.3.1

The TSF shall terminate an interactive session after a **[assignment: 30 minutos de inactividad]**.

Application note: Este requisito aplica para los componentes argos, tritón y hera.

6.1.6.1.4 FTA_SSL.4.1

The TSF shall allow user-initiated termination of the user's own interactive session.

6.1.6.2 TOE session establishment (FTA_TSE)

Esta familia cubre los siguientes requisitos funcionales de seguridad:

FTA_TSE.1 con las siguientes características:

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

6.1.6.2.1 FTA_TSE.1.1

The TSF shall be able to deny session establishment based on **[assignment: nombre usuario]**.

6.1.7 Class FTP: Trusted Path/Channel

6.1.7.1 Protection of Data in Transit (FTP_DIT_EXT)

Esta familia cubre los siguientes requisitos funcionales de seguridad:

FTP_DIT_EXT.1 con las siguientes características:

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

6.1.7.1.1 FTP_DIT_EXT.1.1

The application shall **[selection: encrypt all transmitted [selection: sensitive data] with [selection: HTTPS in accordance with FCS_HTTPS_EXT.1]]** between itself and another trusted IT product.

6.2 Justificación de los requisitos funcionales de seguridad

La siguiente tabla proporciona la asignación de objetivos de seguridad TOE a los Requisitos funcionales de seguridad. Se incluye el análisis de necesidad y suficiencia para cumplir con los objetivos de seguridad del TOE.

		Objetivos de seguridad			
		O.AUTENTICACION	O.ACCESO	O.AUDITORIA	O.COMUNICACIONES
Requisitos funcionales	FAU_GEN.1			X	
	FAU_SAR.1			X	
	FAU_SAR.2			X	
	FAU_STG.2			X	
	FCS_STO_EXT.1	X			
	FCS_HTTPS_EXT.1				X
	FDP_NET_EXT.1				X
	FIA_AFL.1	X			
	FIA_ATD.1	X			
	FIA_UAU.2	X			
	FIA_UID.2		X		
	FMT_MOF.1		X		
	FMT_MTD.1		X		
	FMT_SMF.1		X		
	FMT_SMR.1		X		
	FTA_SSL.1	X			
	FTA_SSL.3	X			
	FTA_SSL.4	X			
	FTA_TSE.1	X			
	FTP_DIT_EXT.1				X

Tabla 6 – Relación de objetivos de seguridad y requisitos funcionales

El objetivo **O.AUTENTICACION** indica que el TOE no permitirá el acceso a los componentes del TOE sin que se haya realizado anteriormente una autenticación exitosa, por lo que no se podrán consultar los datos almacenados ni simular el acceso de un usuario.

Este objetivo se encuentra cubierto por los siguientes requisitos funcionales:

FCS_STO_EXT.1: utilizando un mecanismo de cifrado para asegurar que las credenciales ofrecidas no puedan ser descifradas.

FIA_AFL.1: mediante bloqueo temporal del usuario tras reiterados intentos de autenticación fallidos.

FIA_ATD.1: mediante la asignación de un identificador único de usuario y la posibilidad de asignación de roles de acceso.

FIA_UAU.2: mediante la comprobación de que se está accediendo a la interfaz con un usuario autenticado y solicitando autenticación en caso de que no lo esté.

FTA_SSL.1: mediante un control de timeout para bloquear la sesión de los usuarios en emas.

FTA_SSL.3: mediante un control de timeout para cerrar la sesión de los usuarios en argos, tritón y hera.

FTA_SSL.4: mediante la disponibilidad de un método para cerrar la sesión.

FTA_TSE.1: comprobando las credenciales de los usuarios para asegurar una correcta autenticación.

El objetivo **O.ACCESO** indica que el TOE permitirá la definición de usuarios y sus correspondientes políticas de acceso, por lo que no se podrán consultar los datos almacenados sin los permisos de acceso adecuados ni obtener el acceso de un usuario distinto al autenticado.

Este objetivo se encuentra cubierto por los siguientes requisitos funcionales:

FIA_UID.2: mediante la identificación del usuario en el inicio de sesión.

FMT_MOF.1: restringiendo el acceso la gestión del control de acceso a un usuario con el rol administrador.

FMT_MTD.1: restringiendo la gestión de usuarios a un usuario con el rol administrador.

FMT_SMF.1: proporcionando la gestión de las funcionalidades de seguridad.

FMT_SMR.1: proporcionando el listado de roles definidos y su posible asignación a usuarios.

El objetivo **O.AUDITORÍA** indica que el TOE debe proteger los registros de auditoría almacenados de modificaciones o eliminaciones no autorizadas.

FAU_GEN.1: mediante el registro y almacenamiento de los eventos de auditoría.

FAU_SAR.1: garantizando que solo el administrador pueda acceder a los registros de auditoría y registrando la información de auditoría de forma legible.

FAU_SAR.2: garantizando que únicamente los usuarios del entorno operacional con los permisos necesarios pueden acceder a los registros de auditoría.

FAU_STG.2: garantizando que únicamente los usuarios del entorno operacional con los permisos necesarios pueden acceder a los registros de auditoría y se mantienen un número mínimo de ficheros de almacenamiento de los registros de auditoría y no pueden ser modificados ni eliminados por ningún usuario.

El objetivo **O.COMUNICACIONES** indica que el TOE debe proteger las comunicaciones entre los usuarios remotos y este. Este objetivo se satisface por los siguientes requisitos de seguridad:

FCS_HTTPS_EXT.1: garantizando que la comunicación se realiza mediante el protocolo https entre los usuarios y el TOE.

FDP_NET_EXT.1: garantizando que únicamente se realizan conexiones a las interfaces de adquisición y procesamiento de tráfico.

FTP_DIT_EXT.1: garantizando que la comunicación se realiza mediante el cifrado de las comunicaciones entre los diferentes elementos.

6.3 Dependencias requisitos de seguridad

La dependencia de FAU_GEN.1 se satisface con el requisito de entorno OE.TIME que obtiene la hora que proporciona el propio sistema operativo.

Tabla general de dependencias de los requisitos:

SFR	Dependencia	Satisfecha (S, N, NA)
FAU_GEN.1	FPT_STM.1	S (OE.TIME)
FAU_SAR.1	FAU_GEN.1	S
FAU_SAR.2	FAU_SAR.1	S
FAU_STG.2	FAU_GEN.1	S
FCS_STO_EXT.1	NA	NA
FCS_HTTPS_EXT.1	NA	NA
FDP_NET_EXT.1	NA	NA
FIA_AFL.1	FIA_UAU.1	S (FIA_UAU.2)
FIA_ATD.1	NA	NA
FIA_UAU.2	FIA_UID.1	S (FIA_UID.2)
FIA_UID.2	NA	NA
FMT_MOF.1	FMT_SMR.1	S
	FMT_SMF.1	S
FMT_MTD.1	FMT_SMR.1	S
	FMT_SMF.1	S
FMT_SMF.1	NA	NA
FMT_SMR.1	FIA_UID.1	S (FIA_UID.2)
FTA_SSL.1	FIA_UAU.1	S (FIA_UAU.2)
FTA_SSL.3	NA	NA
FTA_SSL.4	NA	NA
FTA_TSE.1	NA	NA
FTP_DIT_EXT.1	NA	NA

Tabla 7 – Dependencias requisitos de seguridad

6.4 Requisitos de garantía de seguridad

El desarrollo y la evaluación del TOE debe realizarse de acuerdo con los siguientes requerimientos de aseguramiento de la seguridad, a nivel EAL 2, para la ampliación de esta certificación se realiza con el requisito **ALC_FLR.1**:

6.4.1 EAL2

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic Design
AGD: Guidance Documents	AGD_OPE.1 Operation user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.1 Flaw remediation procedure
ASE: Security Target Evaluation	ASE_OBJ.2 Security objectives
	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problems definition
	ASE_TSS.1 TOE summary specification
ATE: Test	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – simple
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Tabla 8 – Listado de clases de aseguramiento de la seguridad

Esta es la asignación de clases de aseguramiento de la seguridad necesarias para una obtener una certificación de Common Criteria a nivel EAL 2.

6.5 Justificación de los requisitos de garantía

Los requisitos de seguridad se han seleccionado de acuerdo con el nivel de garantía de evaluación EAL 2 aumentado con el componente ALC_FLR.1.

El nivel de seguridad seleccionado es apropiado para las amenazas especificadas en el problema de seguridad en el entorno operativo descrito.

7 Resumen de especificaciones del TOE

7.1 Funciones de seguridad

7.1.1 Autenticación

Con anterioridad a la realización de cualquier acción, un usuario debe realizar una autenticación exitosa en el sistema.

El TOE requiere al usuario que introduzca correctamente su usuario y contraseña para poder realizar acciones.

Cualquier usuario que desconozca esta combinación de valores no podrá acceder al TOE para realizar ningún tipo de acción. Además, estos datos no son visibles por el administrador, puesto que sólo tiene acceso al atributo del nombre de usuario y no a la contraseña en claro ni puede recuperarse teniendo su valor cifrado.

Los requisitos relevantes asociados son los siguientes: FCS_STO_EXT.1, FIA_UAU.2, FTA_TSE.1, FIA_AFL.1 y FIA_ATD.1.

GLORIA asegura el requisito **FCS_STO_EXT.1** mediante un mecanismo de cifrado no reversible aseguran que las credenciales ofrecidas no puedan ser descifradas. Asimismo, dichas credenciales solo se pueden consultar desde la consola SSH por un usuario configurador.

```
emas=# select idpersona, password from usuario
 idpersona |              password
-----------+------------------------------
     15707 | vcYHqb6LZJZ+IzrDBFJLUKgUSSA=
      2884 | KoCM59XedkhqUYcAsCGEk5fb1iM=
```

GLORIA asegura el requisito **FIA_UAU.2** mediante la incorporación de un sistema de autenticación que comprueba si un usuario se encuentra con sesión iniciada y válida antes de realizar cualquier acción en el sistema.

GLORIA asegura el requisito **FTA_TSE.1** mediante la posibilidad de marcar la cuenta de un usuario como bloqueada desde el perfil del mismo, en caso de que un usuario con el rol de Administrador considere que ésta deba ser bloqueada.

Este bloqueo manual no tiene efecto sobre el usuario administrador inicial (usuario con identificador 1). Cualquier otro usuario puede ser bloqueado en GLORIA, independientemente de su tipo o rol.

GLORIA asegura el requisito **FIA_AFL.1** mediante el control de autenticaciones incorrectas, de forma que tras tres intentos fallidos de autenticación se bloquea al usuario temporalmente por un periodo de 15 minutos, evitando que este pueda iniciar sesión en ese plazo. Este bloqueo se aplica a cualquier usuario de GLORIA.

GLORIA asegura el requisito **FIA_ATD.1.1** mediante la asignación de un identificador único de usuario y la posibilidad de asignación de roles de acceso a este.

7.1.2 Autorización

El TOE permite realizar una gestión de roles a los que se les asocia el control de acceso a cada componente de **GLORIA**.

Estos roles son relacionados con cada uno de los usuarios de **GLORIA** permitiendo asignar los permisos adecuados para acceder a la información.

La gestión de roles de **GLORIA** permite crear tantos roles como sea necesario en la organización en la que se despliega, permitiendo de este modo un alto nivel de granularidad en la definición de la autorización de acceso a los datos.

En el caso de que un usuario disponga de varios roles, la autorización se obtiene como la suma de cada uno de ellos, no siendo necesario que todos los roles tengan acceso a todas las funcionalidades.

El TOE dispone de un mecanismo de detección de inactividad de sesiones que evita que una sesión de un usuario autenticado pueda ser utilizada tras un tiempo de inactividad realizando el bloqueo de dicha sesión de forma automática garantizando que sólo el usuario que conoce los datos de autenticación se encuentra autorizado a visualizar la información.

Los requisitos relevantes asociados son los siguientes: FIA_UID.2, FMT_MOF.1, FMT_MTD.1, FMT_SMF.1 y FMT_SMR.1.

GLORIA asegura el requisito **FIA_UID.2** mediante la identificación unívoca del usuario en el inicio de sesión y su asociación a su identificador único.

GLORIA asegura el requisito **FMT_MOF.1** restringiendo la visibilidad de la pestaña de control de acceso en la pantalla de gestión de personas y personal, a usuarios con el rol administrador. En emas se realiza la gestión de personas, y no todas las personas tienen usuario asociado. Cualquier usuario tiene permisos para ver la información de las personas registradas en la aplicación, pues desde el formulario de evento puede asociar el evento a cualquier persona y, por tanto, debe poder ver la información asociada. Sin embargo, la pestaña de control de acceso está restringida a los usuarios con el rol de administrador.

GLORIA asegura el requisito **FMT_MTD.1** haciendo que sólo usuarios con el rol administrador puedan otorgar/revocar permisos sobre las pantallas y/o componentes.

GLORIA asegura el requisito **FMT_SMF.1** mediante las pantallas:

Gestión de roles: permite su administración.

Gestión de pantallas: permite asignar roles a pantallas e indicar sus permisos.

Gestión de personas y gestión de personal: permiten administrar las personas registradas y habilitarles usuario en la herramienta, asignándoles en tal caso los roles que les correspondan.

GLORIA asegura el requisito **FMT_SMR.1** permitiendo únicamente la asignación a los usuarios de los roles definidos.

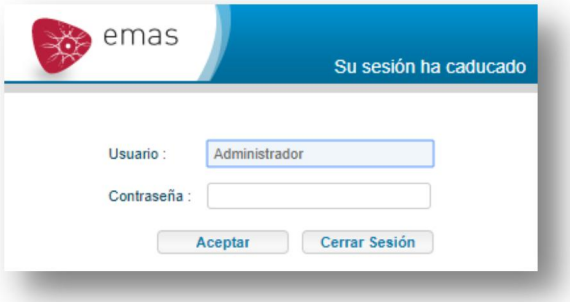
7.1.3 Aseguramiento

El TOE tiene configurado un tiempo de inactividad de la sesión, para que esta tenga una duración determinada en el tiempo si no se está realizando acción alguna sobre la interfaz web. Pasado el tiempo configurado, la sesión se cerrará evitando que se pueda acceder a la interfaz y a sus datos, por lo que será necesario realizar un nuevo inicio de sesión para continuar trabajando con la herramienta.

Los requisitos relevantes asociados son los siguientes: FTA_SSL.1, FTA_SSL.3 y FTA_SSL.4.

GLORIA asegura el requisito **FTA_SSL.1.1:** mediante un periodo de caducidad para bloquear la sesión de los usuarios del componente EMAS.

GLORIA asegura el requisito **FTA_SSL.1.2** en el componente de EMAS mostrando una ventana emergente al usuario para que bien, vuelva a iniciar sesión continuando su trabajo, o bien cierre la sesión sin permitirle realizar ninguna acción adicional.



GLORIA asegura el requisito **FTA_SSL.3.1:** mediante un periodo de caducidad para cerrar la sesión de los usuarios en argos, tritón y hera.

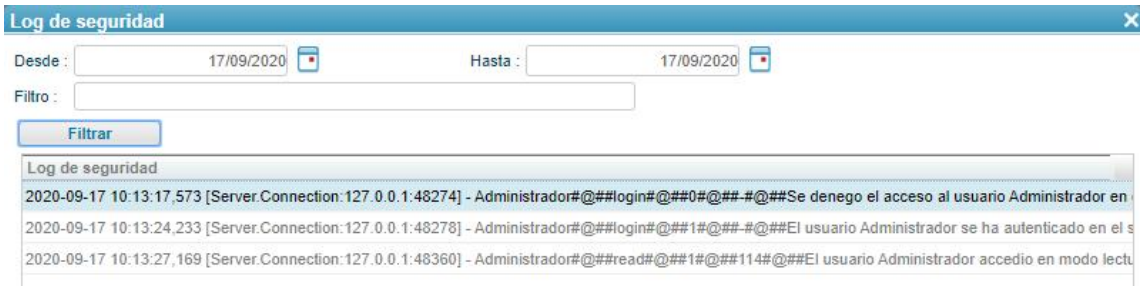
GLORIA asegura el requisito **FTA_SSL.4.1** mediante la disponibilidad de un método para cerrar la sesión, como una opción de menú o bien con un botón de cierre de sesión.

7.1.4 Auditoría

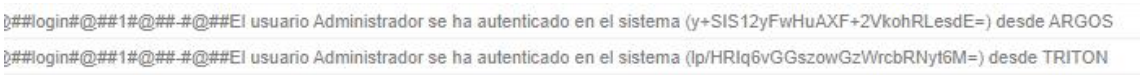
Todos los accesos al TOE mediante la interfaz se registran en ficheros de log para su posterior consulta.

Los requisitos relevantes asociados son los siguientes: FAU_GEN.1, FAU_SAR.1, FAU_SAR.2 y FAU_STG.2.

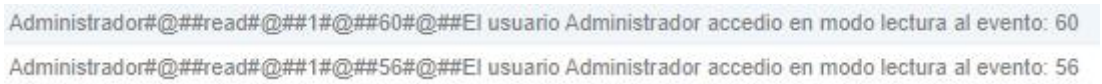
GLORIA asegura el requisito **FAU_GEN.1.1** y **FAU_GEN.1.2** mediante la generación de los registros de auditoría para todos los eventos relevantes relacionados con la seguridad. Estos incluyen la fecha y la hora del evento, el tipo de evento, el sujeto que genera el registro de autoría y el resultado del evento: exitoso (valor 1) o fallido (valor 0).



Adicionalmente, en un inicio de sesión satisfactorio, se registra el identificador de sesión (entre paréntesis) y componente al que se accede:



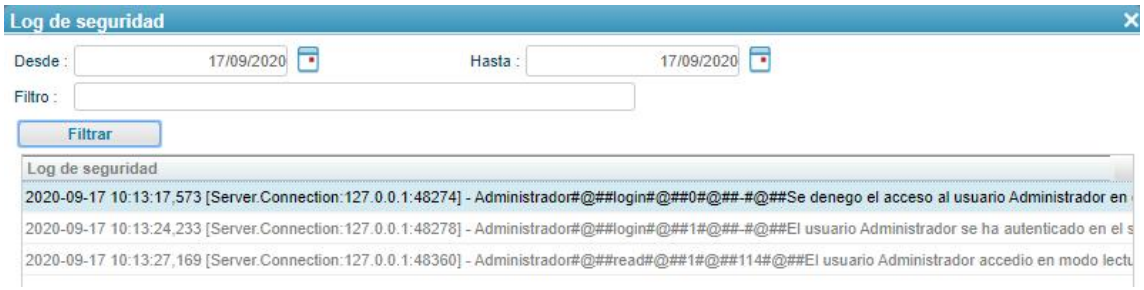
Y en un acceso a una alerta se registra el identificador de la misma:



GLORIA asegura los requisitos **FAU_SAR.1.1 y FAU_SAR.1.2** registrando la información de auditoría de forma legible y permitiendo únicamente su consulta a usuarios con el rol administrador.

GLORIA asegura el requisito **FAU_SAR.2.1** garantizando que únicamente los usuarios con rol administrador del entorno operacional tienen los permisos necesarios para consultar los registros de auditoría.

GLORIA asegura los requisitos **FAU_STG.2.1 y FAU_STG.2.2** mediante la protección de los registros de auditoría almacenados, frente a modificaciones y eliminaciones.



GLORIA asegura el requisito **FAU_STG.2.3** garantizando que se mantienen hasta 10 ficheros con un tamaño máximo de 10Mb cada uno, destinados al almacenamiento de los registros de auditoría. Para mantener este límite de ficheros se realiza un rotado del mismos.

7.1.5 Comunicaciones

Las comunicaciones entre los usuarios y el TOE se realizan mediante el protocolo HTTPS que garantiza que la información que se intercambia entre el TOE y el usuario se realiza de forma cifrada y segura.

Los requisitos relevantes asociados son los siguientes: FCS_HTTPS_EXT.1, FDP_NET_EXT.1 y FTP_DIT_EXT.1.

GLORIA asegura los requisitos **FCS_HTTPS_EXT.1.1 y FCS_HTTPS_EXT.1.2** mediante el uso del protocolo https en todas las comunicaciones que se realizan desde los usuarios hacia el TOE.

GLORIA asegura el requisito **FDP_NET_EXT.1.1** mediante la restricción de comunicaciones del TOE con las interfaces de adquisición y procesamiento de tráfico.

GLORIA asegura el requisito **FTP_DIT_EXT.1.1** mediante el cifrado en todas las comunicaciones que se realizan desde/hacia el TOE.

MADRID
Avda. de Manoteras,
46BIS, 6ºC, 28050
T.(+34) 902 882 992

BARCELONA
Llull, 321 (Edifici Cinc)
08019
T.(+34) 902 882 992

VALENCIA
Ramiro de Maeztu 7,
46022
T.(+34) 902 882 992

BRUSELAS
Rue Belliard, 20
1040
T. (+32) (0) 474532974

LISBOA
Rua Cidade Rabat, 27
1.dto, 1500-159
T.(+35) 1917620918

BOGOTÁ
Carrera 11 Nº 93A-53,
Of. 401
T.(+57 1) 74 5 74 39

MÉXICO D.F.
44-7, México D.F.
06600
T.(+52) 55 2128 068

S2 GRUPO

ANTICIPANDO UN MUNDO CIBERSEGURO