S2 GRUPO

# S2Grupo
# *Carmen v.7.2.4*
# *Common Criteria EAL2 + ALC_FLR.1*

*ASE_DS*

*24/03/2021*

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
IQNet CERTIFIED MANAGEMENT SYSTEM

| | |
|---|---|
| **Tipo de Documento:** | Common Criteria. Declaración de seguridad |
| **Descripción:** | *carmen: Declaración de Seguridad* |
| **Fecha de creación:** | 24/03/2021 |
| **Nombre del documento:** | CARMEN_ASE_DS_v1.11 |

## CONTROL DE VERSIONES

| Versión | Realizado por | Descripción de versión | Fecha |
|---|---|---|---|
| 1.0 | S2 Grupo | Versión inicial | 21/11/2017 |
| 1.1 | S2 Grupo | Finalización Revisión OR | 10/06/2018 |
| 1.2 | S2 Grupo | Finalización Comentarios | 01/08/2018 |
| 1,3 | S2 Grupo | Revisión Comentarios | 24/09/2018 |
| 1.4 | S2 Grupo | Revisión Comentarios | 05/10/2018 |
| 1.5 | S2 Grupo | Revisión Comentarios | 04/03/2019 |
| 1.6 | S2 Grupo | Revisión Comentarios | 09/03/2020 |
| 1.7 | S2 Grupo | Revisión Comentarios | 27/09/2019 |
| 1.8 | S2 Grupo | Revisión Comentarios | 28/10/2019 |
| 1.9 | S2 Grupo | Revisión Comentarios | 04/02/2020 |
| 1.10 | S2 Grupo | Revisión Comentarios | 30/10/2020 |
| 1.11 | S2 Grupo | Revisión Comentarios | 24/03/2021 |

# Índice de Contenidos

# Índice de Ilustraciones

# 1 Introduction

## 1.1 ST Reference

**Título:** CARMEN_ASE_DS_v1.11

**Versión:** v.1.11

**Fecha**: 24/03/2021

**Autor:** S2 Grupo

## 1.2 TOE Reference

**Nombre del TOE:** carmen

**Versión del TOE:** v 7.2.4

**Desarrollador del TOE:** S2 Grupo

## 1.3 TOE Overview

### *1.3.1 TOE Usage*

**CARMEN**, Centro de Análisis de Registros y Minería de EveNtos, es un desarrollo de S2 Grupo en colaboración con el Centro Criptológico Nacional para la identificación del compromiso por parte de amenazas persistentes avanzadas (APT), constituyendo la primera capacidad española, basada en conocimiento y tecnología nacionales, en este sentido.

El proceso de identificación de una amenaza de este tipo (APT) depende de las aptitudes de un analista y de la información de la que dispone. CARMEN permite adquirir información de diferentes protocolos de red (http/s, tls, smtp, dns, netbios, icmp, netflows y la información del endpoint Claudia).

La información adquirida se analiza dando indicios al analista para poder investigar si esas pistas constituyen una amenaza real. Cada analista tiene asignados unos roles concretos en la aplicación que le permiten ver sólo las pantallas asociadas a este, con lo que sólo verá la información asociada a dichas pantallas.

### *1.3.2 TOE Type*

**carmen** es una solución software de adquisición, procesamiento y análisis de información para soportar el proceso de identificación de amenazas a partir de los tráficos de una red.

### *1.3.3 Principal Security functionality*

Además, el TOE provee mecanismos de seguridad para garantizar que únicamente el personal autorizado puede utilizar el TOE.

Las características de seguridad son:

- **Autenticación**: no es posible realizar ninguna acción en el TOE sin haber realizado previamente una autenticación.
- **Identificación**: se almacenan registros de identificación para cada intento de autenticación por parte de un usuario. Los registros se almacenan en la base de datos de la aplicación y pueden ser consultados a través de la interfaz de **carmen**.
- **Control de acceso**: el acceso a la información recolectada y analizada de la organización sólo es posible a través de la interfaz de **carmen**.
- **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.

### *1.3.4 NON-TOE Hardware/Software/Firmware*

**carmen** se sirve preinstalado en un servidor (en modo appliance), para rack de tamaño 2U.


**Ilustración 1 – Appliance de carmen**

El equipo estándar dispone de las siguientes características:

- 2 CPU de 8 núcleos cada uno
- 64 GB RAM
- 2 HDD en RAID10 de 300GB cada uno y 2 HDD de 600GB para el almacenamiento
- Fuente de alimentación redundante
- 8 interfaces de red en dos tarjetas de cuatro interfaces

Adicionalmente, existen una serie de elementos software como son el sistema operativo o productos Open Source que son empleados por el TOE que son necesarias para su ejecución que forman parte de las condiciones de contorno de la aplicación:

- Sistema Operativo: centOS 7, versión 7.5.1804
- Gestor de colas: RabbitMQ, versión 3.5.1
- Gestor de Base de datos: PostgreSQL, versión 9.2.24
- Gestor de Documentos: ElasticSearch, versión 6.3.0
- Máquina virtual Java, versión 1.8.0_191
- Interprete Python, versión 2.7.5
- Servidor de aplicaciones Apache Tomcat, versión 8.5.35

El TOE expone varias interfaces de red, más una interfaz de gestión propietaria del fabricante del dispositivo físico (DELL) denominada iDrac. El appliance de Carmen que aplica en la configuración evaluada tiene un total de 8 interfaces físicas Ethernet 10/100/1000, cuatro de ellas en la placa base del sistema y cuatro más en una tarjeta de red adicional.

En algunos casos, si el cliente lo solicita, se puede dotar a Carmen de una tarjeta de fibra que amplía en 2 las interfaces de red, llegando hasta 10/100/1000/10000.

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 carmen 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.

Por último, para la actualización y verificación del TOE, se necesitarán los siguientes ficheros:

- Un fichero llamado **“update.sh”** utilizado para la actualización del TOE en el appliance físico.
- Un fichero llamado **“spec.json”** usado para la verificación de la integridad del TOE.
- Un fichero llamado **“checker.py” e**ncargado de confirmar que tanto los elementos de control definidos en el sistema, como los permisos asociados a cada uno de ellos son los correspondientes a la versión que ha sido liberada e instalada.

### 1.3.5 Functionality Excluded From the Evaluation

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

- Activación/Desactivación de fuentes de recolección
- Configuración de expresiones regulares para la adquisición y procesamiento del tráfico de red.
- Incorporación de nuevas capacidades de inteligencia mediante el desarrollo de plugins.
- Integración con un sistema central que permite distribuir inteligencia a las instancias de carmen que se suscriban al servicio.
- Integración con un sistema de análisis de ficheros dinámico.

## 1.4 TOE Description

### 1.4.1 Logical Scope

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

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. Pasado un tiempo de inactividad, la sesión de Carmen se cerrara automáticamente, sin poder acceder de nuevo a la información, ni navegar por la interfaz web, para ello será necesario volver a realizar el login.

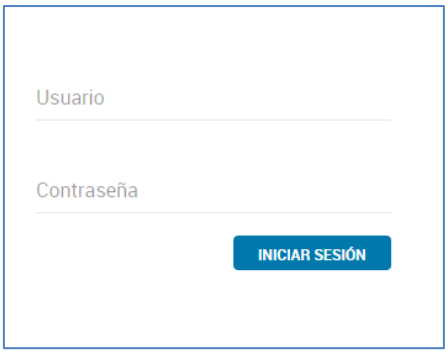


**Ilustración 2 – Autenticación**

- **Identificación**: cada intento de acceso (fallido o no) se almacena en la base de datos de la aplicación y pueden ser consultados a través de la interfaz. De este

modo se puede saber si se está intentado acceder sin credenciales o simplemente se ha cometido un error en la clave de acceso.


Ilustración 3 - Listado de accesos

- **Control de acceso**: el acceso a la información recolectada y analizada de la organización sólo es posible a través de la interfaz de carmen. En función de los roles que tenga el usuario podrá ver la información relacionada con su rol, dado que estos bloquean los permisos por pantalla, y cada origen de datos está separado en una pantalla diferente.

- **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.

### *1.4.2 Physical Scope*

El ámbito físico de CARMEN v7.2.4 es el siguiente:

- Un fichero ".war" llamado **"ROOT.war"** que viene desplegado en el appliance físico, en el servidor de aplicaciones Tomcat.

Las guías de usuario y de administrador, que son accesibles a través de la compartición del repositorio de S2 Grupo albergado en "https://minube.s2grupo.es".

- Una guía de usuario llamada "**u7.3_ccn.pdf**", en formato ".pdf". Esta guía también puede ser descargada tras una autenticación exitosa en la aplicación web de CARMEN y hace referencia a **CARMEN_AGD_OPE_v7.3**. Su hash sha-256 es 43fa1256a1c9ee773961ab6887b5a39bcf90e2354b076b42b4d945834006878f.
- Una guía de administrador llamada "**a7.3_ccn.pdf**" en formato ".pdf" Esta guía también puede ser descargada tras una autenticación exitosa en la aplicación web de CARMEN y hace referencia a **CARMEN_AGD_PRE_v7.3**. Su hash sha-256 es 1d46393a4624bfa032355342cb0285ae4449489996b963b56a195bdf6f61cb3c.

### 1.4.3 TOE Evaluated configuration

Para realizar la evaluación del TOE se ha desplegado un entorno con los siguientes elementos:

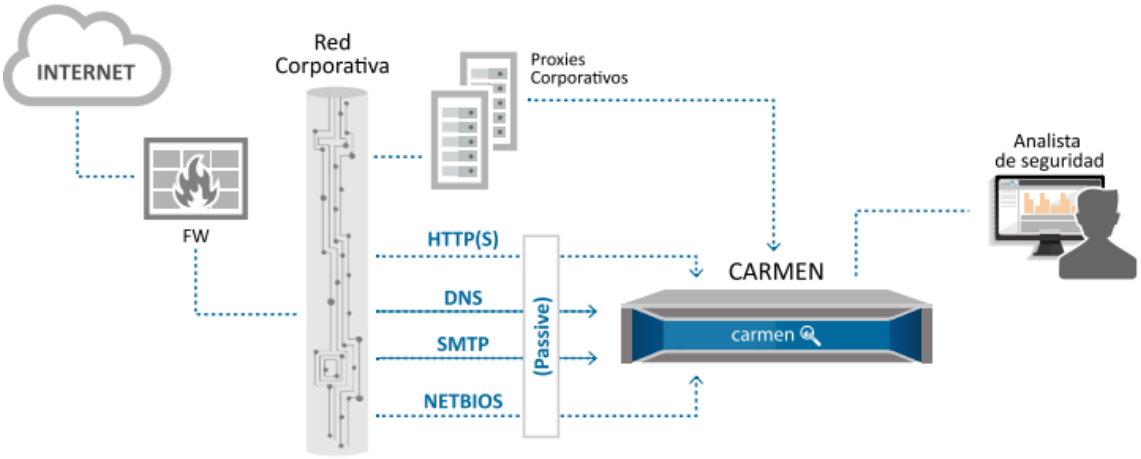


Ilustración 4 – TOE Evaluated configuration

En este diagrama se observa que CARMEN 7.2.4 se encuentra conectada a la red corporativa de la organización para recibir el tráfico HTTP, HTTPS, DNS, SMTP y NETBIOS (IPC) y un analista de seguridad se conecta directamente a CARMEN 7.2.4 para realizar el análisis.

El puesto del analista de seguridad utilizado en la evaluación, dispone de las siguientes características:

- Ubuntu 18.04.2
- 8 CPU
- 16 GB de RAM
- 1 TB HDD
- Navegador Google Chrome 75.0.3770.100

## 1.5 Product description

**Carmen** es una herramienta de apoyo al analista de seguridad para la búsqueda de amenazadas persistentes avanzadas en la organización en la que se encuentra desplegado. Para poder realizar dicha tarea, es necesaria la adquisición, procesamiento y análisis de su tráfico de red de varios protocolos. En función de que protocolos se estén capturando, las capacidades para encontrar usos indebidos, la detección de anomalías o los intentos de intrusión mejorarán. Estos elementos son organizados e interpretados para facilitar la búsqueda de anomalías, que el equipo de analistas de seguridad analizará e investigará.

**carmen** protege a las organizaciones mediante la adquisición, procesamiento y análisis de su tráfico de red: la aparición de usos indebidos, la detección de anomalías o los

intentos de intrusión son identificados, organizados e interpretados para facilitar el desempeño del equipo de analistas de seguridad soportando el proceso de investigación.

Se compone de agentes que recopilan los flujos de tráfico (elementos de adquisición), un motor de almacenamiento en el que se inserta la información, un sistema de detección de anomalías que se encarga de procesar la información almacenada para la identificación de posibles amenazas que puedan afectar a la organización y una aplicación web que permite la representación y consulta tanto de la información obtenida como de la procesada.

**carmen** permite al equipo de analistas de seguridad de la organización abordar el proceso de identificación de amenazas de una forma eficiente y les ayuda en la toma de decisiones a partir de la información generada y procesada por la propia herramienta. Permite un período de retención aproximado de 30 días para el caso de una organización en la que se estima una adquisición equivalente a 1Gb de log de navegación diario.

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

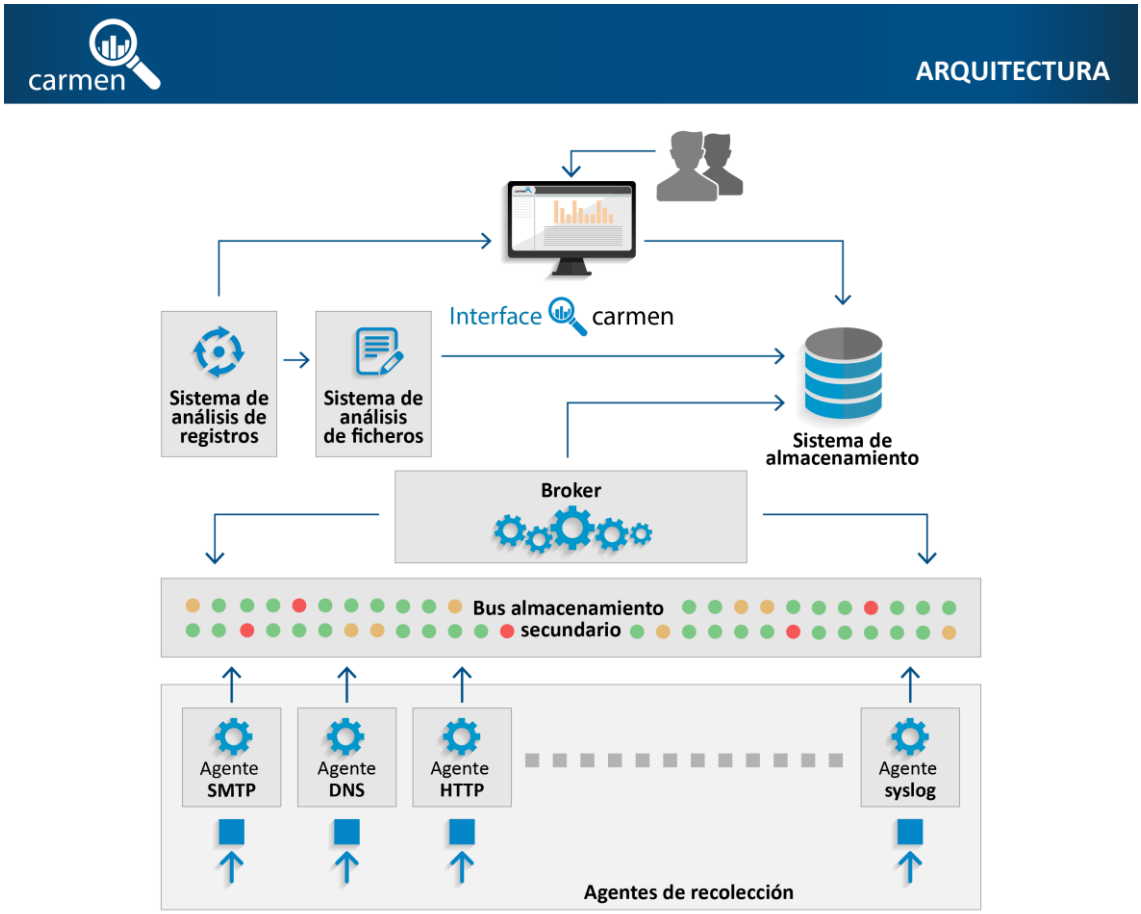


**Ilustración 5 – Arquitectura de carmen**

### 1.5.1 Consola de carmen

Se trata de una aplicación web, desplegada como un war en un servidor de aplicaciones tomcat, que posibilita al usuario del sistema acceder a la información registrada, realizar las diferentes acciones que facilitan las acciones de los analistas de seguridad en la búsqueda de amenazas avanzadas persistentes y lanzar la ejecución de los elementos de análisis, tanto de forma instantánea como programada.

Además, permite realizar el acceso a las opciones de configuración de la herramienta, entre las que destacan el control de acceso a la información, a la identificación y autenticación de los usuarios y el control de acceso a estos datos.

### 1.5.2 Agentes de recolección

Se encargan de procesar, normalizar y preparar para su almacenamiento los registros relacionados con las comunicaciones de la organización.

Los agentes de recolección recolectores consisten en ficheros ejecutables desarrollados en tecnología java, golang y python que cargan y procesan, mediante la aplicación de expresiones regulares, un fichero de registros de navegación o procesan el tráfico recibido a través de una interfaz promiscua para extraer los atributos que identifican cada uno de los elementos de la navegación.

Los orígenes de datos que actualmente soportan los agentes de recolección de **carmen** son los siguientes

- HTTP, mediante la carga de ficheros de log de navegación HTTP (por ejemplo SQUID o similar) o mediante la adquisición y procesamiento del tráfico de red. En concreto los siguientes RFC: RFC 1945, RFC 2616 y RFC 2774.
- HTTPS, mediante la adquisición y procesamiento del tráfico de red obteniendo la información intercambiada durante la fase de negociación. En concreto los siguientes RFC: RFC 1945, RFC 2616 y RFC 2774.
- DNS, mediante la carga de ficheros de log con un formato adaptable y configurable o mediante la adquisición y procesamiento del tráfico de red. En concreto los siguientes RFC: RFC 1034, RFC 1035, RFC 1123, RFC 1995, RFC 1996, RFC 2136, RFC 2181, RFC 2308, RFC 2672, RFC 2845, RFC 3225, RFC 3226, RFC 3596, RFC 3597, RFC 4343, RFC 4592, RFC 4635, RFC 5001, RFC 5011, RFC 5452, RFC 5890, RFC 5891, RFC 5892, RFC 5893, RFC 6891 y RFC 7766.
- SMTP, mediante la adquisición y procesamiento del tráfico de red. En concreto los siguientes RFC: RFC 821, RFC 2821 y RFC 5321.
- IPC, mediante la adquisición y procesamiento del tráfico de red. En concreto los estándares de Microsoft: [MS-MAIL] Remote Mailslot Protocol] [MS-CIFS] Common Internet File System Protocol y [MS-SMB] Server Message Block Protocol.

### 1.5.3 Bus de almacenamiento secundario

Se encarga de recibir cada uno de los mensajes generados por los agentes de recolección para almacenar esta información temporalmente permitiendo disponer de un nivel óptimo de escalado.

El uso de este bus de almacenamiento, que se encuentra desplegado como un servicio del sistema operativo en **carmen**, facilita la comunicación de forma asíncrona entre los diferentes componentes involucrados en la adquisición, procesamiento y almacenamiento de la información.

### 1.5.4 Broker

Se encarga de procesar los diferentes mensajes disponibles en el sistema de almacenamiento secundario para incluir información de contexto y optimizar las consultas sobre la información que será almacenada.

Este componente software, consistente en un fichero ejecutable desarrollado en tecnología java, permite un nivel óptimo de escalado facilitando las tareas de procesamiento y posterior almacenamiento de la información.

### 1.5.5 Sistema de Almacenamiento

Se encarga de registrar y almacenar la información para su posterior tratamiento por los elementos de análisis de **carmen**, y se encuentra desplegado como un servicio del sistema operativo.

### 1.5.6 Sistema de análisis de registros

Se encarga de realizar las tareas de procesamiento y búsqueda de anomalías tanto automáticas como solicitadas por los usuarios de la aplicación sobre los datos recolectados.

Este componente software, consistente en un fichero ejecutable desarrollado en tecnología java y python, consulta la información del sistema de almacenamiento, procesa los datos obtenidos y registra las situaciones relevantes.

Estas situaciones son gestionadas mediante alertas en la consola de **carmen** y deben ser atendidas por el equipo de analistas de seguridad de la organización.

### 1.5.7 Sistema de análisis de ficheros

Se encarga de realizar el procesamiento de ficheros en los que se trata de identificar la posible aparición de patrones que puedan indicar un intento de intrusión.

Este componente software, consistente en un fichero ejecutable desarrollado en lenguaje Python, es configurable y permite seleccionar los patrones y reglas que deben ser aplicados para analizar ficheros.

En caso de identificar alguna situación de riesgo en este análisis, ésta se reportada a la consola de **carmen** mediante la generación de una alerta que debe ser atendida por el equipo de analistas de seguridad de la organización.

# 2 Conformance Claim

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, siendo extendida la incorporación del requisito ALC_FLR.1.

En concreto, se consideran la siguientes condiciones:

- CC Part 2 conformant: la parte 2 de la norma (ccpart2v3.1r5) se considera de forma estricta 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, sino que refleja las propiedades y soluciones de seguridad del producto **carmen**.

# 3 Security Problem Definition

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

- Las supuestas amenazas conocidas que serán contrarrestadas por el TOE.
- Las políticas de seguridad de la organización que el TOE debe cumplir.
- Las suposiciones de uso de TOE en el entorno operativo sugerido.

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

## 3.1 TOE Scope

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

1) Control de acceso al TOE, incluyendo la definición de roles y políticas de control de accesos.
2) Identificación y autenticación.
3) Control de acceso.
4) Gestión securizada de los puntos anteriores.

## 3.2 TOE Assets

Nuestros principales activos a proteger son:

- **A.LOGS_PROCESADOS**: Confidencialidad e integridad de los logs de navegación tratados adquiridos, procesados, normalizados y almacenados en **carmen**.
- **A.ANOMALIAS**: Confidencialidad e integridad de los resultados de las ejecuciones de cada uno de los diferentes elementos de inteligencia de **carmen** a partir de los logs de navegación.
- **A.USUARIOS**: Confidencialidad de la información personal de los usuarios, las credenciales de acceso y el listado de roles asociados a cada persona.
- **A.ROLES**: Confidencialidad de la información de pantallas / funcionalidades a las que tendrá acceso cada usuario que se encuentre relacionado con cada uno de ellos.

## 3.3 Assumptions

Este es el principal supuesto:

- **AS.ENTORNO: carmen** se entrega en modo appliance de forma que se encuentra bastionada, siguiendo las recomendaciones de la guía STIC de bastionado de equipos UNIX.
- **AS.ACCESO:** El acceso a **carmen** través de la interfaz web se realiza empleando SSL/TLS.
- **AS.ADMINISTRADOR:** Se considera que los administradores de **carmen** son competentes y confiables en el uso de la aplicación, por lo que no va a atentar contra la integridad del TOE.
- **AS.GESTION:** La comunicación con la interfaz de gestión está cifrada mediante SSH que solicita la apropiada autenticación.
- **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.INSTALACION:** La instalación y configuración del TOE se realizará de acuerdo a las instrucciones de instalación proporcionadas.
- **AS.OPERATIVO:** La paquetería interna del sistema operativo depende únicamente de la versión de este (Centos7). En cada actualización del TOE se actualizan los elementos de la paquetería. Si existe algún paquete obsoleto o con algún tipo de vulnerabilidad, éste será actualizado cuando la versión esté disponible en los repositorios oficiales, pudiendo pasar varios meses hasta que los paquetes afectados se actualicen.

- **AS.LOCALIZACION:** El appliance donde se ejecuta el TOE se encuentra situado dentro de una instalación segura y controlada donde no se permite el acceso. Se consideran dentro de este entorno la red corporativa, los proxies corporativos y el firewall dela organización.
- **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.

## 3.4 Threats

Las amenazas identificadas en **carmen** son:

- **T.ACCESO**: un atacante consigue acceder a datos de logs procesados (**A.LOGS_PROCESADOS**) o anomalías (**A.ANOMALIAS**) identificadas a los que no tiene concedido permiso de consulta.
- **T.FALSIFICACION**: un atacante consigue, a través de los interfaces de **carmen** modificar los logs almacenados (**A.LOGS_PROCESADOS**) o las anomalías identificadas (**A.ANOMALIAS**).
- **T.SUPLANTACION**: un atacante consigue acceder al perfil de otro usuario (**A.USUARIOS**) o con unos roles (**A.ROLES**) distintos a los de su usuario.

# 4 Security Objectives

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

Estos se dividen en dos tipos:

- Los objetivos de seguridad para el TOE.
- Los objetivos de seguridad para el entorno operativo.

## 4.1 Security Objectives for the TOE

Los objetivos de seguridad para el TOE son:

- **O.AUTENTICACION**: el TOE no permitirá el acceso a sus interfaces sin que se haya realizado antes una autenticación exitosa.
- **O.ACCESO**: el TOE permitirá la definición de usuarios y sus correspondientes políticas de acceso.

## 4.2 Security Objectives for the Operational Environment.

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

- **OE.ENTREGA**: **carmen** se entrega en modo appliance de forma que se encuentra bastionada, siguiendo las recomendaciones de la guía STIC de bastionado de equipos UNIX.
- **OE.DESPLIEGUE**: el TOE está directamente desplegado en el appliance físico y la instalación y configuración se realiza de acuerdo a las instrucciones proporcionadas en los manuales de usuario y administrador.
- **OE.SSL**: el acceso a **carmen** a través de la interfaz web se realiza empleando SSL/TLS, TLS versión 1.2 y en particular los siguientes cifrados:
    - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
    - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- **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 genera timestamps que son confiables, el TOE obtiene las referencias temporales del sistema operativo (Centos7).
- **OE.OPERATIVO:** La paquetería interna del sistema operativo depende únicamente de la versión de éste (Centos7). 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 garantiza que carmen se encuentra dentro de una instalación segura y controlada en la que no se permite el acceso en la que se considerará incorporada la red corporativa, los proxies corporativos y el firewall de la organización.
- **OE.ADMINISTRADOR:** Se considera que el usuario con rol de administrador de la interfaz web de **carmen** es competente y confiable en el uso de la aplicación, por lo que no va a atentar contra la integridad del TOE.
- **OE.GESTION:** El sistema operativo donde reside **carmen** 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.

## 4.3 Security Objectives rationale

### 4.3.1 Objetivos para carmen

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

| | | Amenazas | | |
|---|---|---|---|---|
| | | **T.ACCESO** | **T.FALSIFICACION** | **T.SUPLANTACION** |
| **Objetivos de seguridad** | **O.AUTENTICACION** | X | X | X |
| | **O.ACCESO** | X | X | X |

**Ilustración 6 – 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**).

### 4.3.2 Objetivos para el entorno operacional de carmen

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.

| | | Objetivos de seguridad del entorno operacional | | | |
|---|---|---|---|---|---|
| | | OE.ENTREGA | OE.DESPLIEGUE | OE.SSL | OE.ADMINISTRADOR |
| **Hipótesis** | **AS.ENTORNO** | x | | | |
| | **AS.ACCESO** | | | x | |
| | **AS.INSTALACION** | | x | | |
| | **AS.OPERATIVO** | | | | |
| | **AS.ADMINISTRADOR** | | | | x |
| | **AS.GESTION** | | | | |
| | **AS.CONFIGURADOR** | | | | |
| | **AS.LOCALIZACION** | | | | |
| | **AS.TIME** | | | | |

| Objetivos de seguridad del entorno operacional |
|---|

| | | OE.TIME | OE.OPERATIVO | OE.LOCALIZACION | OE.CONFIGURADOR | OE.GESTION |
|---|---|---|---|---|---|---|
| Hipótesis | **AS.ENTORNO** | | | | | |
| | **AS.ACCESO** | | | | | |
| | **AS.INSTALACION** | | | | | |
| | **AS.OPERATIVO** | | x | | | |
| | **AS.ADMINISTRADOR** | | | | | |
| | **AS.GESTION** | | | | | x |
| | **AS.CONFIGURADOR** | | | | x | |
| | **AS.LOCALIZACION** | | | x | | |
| | **AS.TIME** | x | | | | |

**Ilustración 7 – 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: carmen** será desplegado en un entorno seguro y adecuadamente configurado, por tanto se consideran automáticamente cubierto el objetivos de seguridad del entorno operacional relacionado con el appliance del TOE (**OE.ENTREGA**).
- **AS.ACCESO:** el acceso a **carmen** través de la interfaz web es seguro debido a que se realiza empleando SSL/TLS (**OE.SSL**), TLS versión 1.2 y en particular los siguientes cifrados:
    - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
    - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- **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 appliance físico dónde se encuentra el TOE sólo ejecutará este en un entorno controlado (**OE.LOCALIZACIÓN**).
- **AS.CONFIGURADOR:** Sólo el operador de S2Grupo encargado de la configuración e instalación (**OE.CONFIGURADOR**) del appliance físico accederá a la interfaz ssh y escalará con permisos de root para realizar dichas tareas.
- **AS.ADMINISTRADOR:** Los administradores de la interfaz web de carmen son competentes y confiables en el uso de la aplicación por lo que no van a actuar maliciosamente y por lo tanto no son una amenaza para el TOE **(OE.ADMINISTRADOR)**.

- **AS.TIME:** El TOE será provisto de fuentes de tiempo fiable obtenidas del sistema operativo donde reside (**OE.TIME)**.
- **AS.GESTION:** el acceso a **carmen** 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 Security Requirements for the TOE

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

| Functional Class | Functional Components | |
|---|---|---|
| FDP: User data protección | FDP_ACC | FDP_ACC.2 |
| | FDP_ACF | FDP_ACF.1 |
| FIA: Identification and autehntication | FIA_AFL | FIA_AFL.1 |
| | FIA_ATD | FIA_ATD.1 |
| | FIA_UAU | FIA_UAU.2 |
| | FIA_UID | FIA_UID.2 |
| FMT: Security Management | FMT_MSA | FMT_MSA.1 |
| | | FMT_MSA.3 |
| | FMT_SMF | FMT_SMF.1 |
| | FMT_SMR | FMT_SMR.1 |
| FTA: TOE Access | FTA_SSL | FTA_SSL.1 |
| | | FTA_SSL.2 |
| | | FTA_SSL.4 |
| | FTA_TSE | FTA_TSE.1 |

Ilustración 8 – Requisitos funcionales relacionados con el alcance

## 5.1 Functional Security Requirements.

### *5.1.1 Class FDP: User data protection*

#### 5.1.1.1 Access control policy (FDP_ACC)

Esta familia cubre los siguientes requisitos funcionales de seguridad:

- FDP_ACC.2 con las siguientes características:
  - Hierarchical to: FDP_ACC.1 Subset access control
  - Dependencies: FDP_ACF.1 Security attribute based access control

##### *5.1.1.1.1 FDP_ACC.2.1*

The TSF shall enforce the **[assignment**: **access control SFP]** on:

**[assignment:**

**Sujetos: los usuarios creados en la interfaz web.**

**Objetos: pantallas de la interfaz web]**

, and all operations among subjects and objects covered by the SFP.

##### *5.1.1.1.2 FDP_ACC.2.2*

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

#### 5.1.1.2 Access control functions (FDP_ACF)

Esta familia cubre los siguientes requisitos funcionales de seguridad:

- FDP_ACF.1 con las siguientes características:
  - Hierarchical to: No other components.
  - Dependencies: FMT_MSA.3 Static attribute initialisation
  - Dependencies: FDP_ACC.1 Subset access control

##### *5.1.1.2.1 FDP_ACF.1.1*

The TSF shall enforce the **[assignment: access control SFP]** to objects based on the following:

**[assignment:**

**Sujetos: los usuarios creados en la interfaz web.**

**Atributos de seguridad de los sujetos: el identificador y los roles asociados a cada usuario.**

**Objetos: pantallas de la interfaz web.**

**Atributos de seguridad de los objetos: roles asociados a cada pantalla].**

##### *5.1.1.2.2 FDP_ACF.1.2*

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

**[assignment:**

**Si un rol está relacionado con una pantalla:**

- **Cualquier usuario que disponga del rol puede acceder a la pantalla.**
- **Cualquier usuario que disponga del rol puede acceder a los datos y funciones de seguridad relacionados con la pantalla.**

**Si un rol no está relacionado con una pantalla:**

- **Si el usuario no dispone de algún otro rol que esté asociado no puede acceder a la pantalla.**
- **Si el usuario no dispone de algún otro rol que esté asociado no puede acceder a los datos y funciones de seguridad relacionados con la pantalla.]**

##### *5.1.1.2.3 FDP_ACF.1.3*

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

**[ assignment:**

**Cualquier usuario puede acceder al dashboard de la aplicación con una visibilidad limitada a sus roles asignados una vez autenticado en el sistema.**

**Cualquier usuario dispone de acceso a la pantalla de Mis investigaciones en la que se muestra información específica del usuario en su tarea de analista de seguridad una vez autenticado en el sistema.**

**Cualquier usuario dispone de acceso al listado de investigaciones una vez autenticado en el sistema.**

**Cualquier usuario dispone de acceso a los manuales del TOE una vez autenticado en el sistema.**

**Cualquier usuario dispone de acceso a la sección de 'Acerca De' de la aplicación una vez autenticado en el sistema].**

#### *5.1.1.2.4 FDP_ACF.1.4*

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

**[assignment: No existen reglas adicionales].**

## *5.1.2 Class FIA: Identification and authentication*

### 5.1.2.1 Authentication failures (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

#### *5.1.2.1.1 FIA_AFL.1.1*

The TSF shall detect when **[selection: [assignment: 5]]** unsuccessful authentication attempts occur related to **[assignment: login and relogin].**

#### *5.1.2.1.2 FIA_AFL.1.2*

When the defined number of unsuccessful authentication attempts has been **[selection: met]**, the TSF shall **[assignment: bloquear de forma transparente a cualquier usuario durante 60 minutos]**.

### 5.1.2.2 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

#### *5.1.2.2.1 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].**

### 5.1.2.3 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

#### *5.1.2.3.1 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.

### 5.1.2.4 User identification (FIA_UID)

Esta familia cubre los siguientes requisitos funcionales de seguridad:

- FTA_UID.2 con las siguientes características:
  - Hierarchical to: FIA_UID.1 Timing of identification
  - Dependencies: No other components.

#### *5.1.2.4.1 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.

## *5.1.3 Class FMT: Security Management*

### 5.1.3.1 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

#### *5.1.3.1.1 FMT_SMF.1.1*

The TSF shall be capable of performing the following management functions: **[assignment: ver/crear/editar/eliminar usuarios y roles y realizar la asignación de roles a usuarios y asignación de pantallas a roles]**.

#### 5.1.3.2 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

##### *5.1.3.2.1 FMT_SMR.1.1*

The TSF shall maintain the roles **[assignment**: **que pueden ser gestionados a través de la interfaz de carmen, por defecto se especifican los siguientes roles: Administrador, Cívil Analista de Malware y Trabajador, y es posible crear Custom roles personalizados]**.

##### *5.1.3.2.2 FMT_SMR.1.2*

The TSF shall be able to associate users with roles.

#### 5.1.3.3 Management of security attributes (FMT_MSA)

Esta familia cubre los siguientes requisitos funcionales de seguridad:

- FMT_MSA.1 con las siguientes características:
  - Hierarchical to: No other components.
  - Dependencies: FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control
  - Dependencies: FMT_SMR.1 Security roles
  - Dependencies: FMT_SMF.1 Specification of Management Functions
- FMT_MSA.3 con las siguientes características:
  - Hierarchical to: No other components.
  - Dependencies: FMT_MSA.1 Management of security attributes
  - Dependencies: FMT_SMR.1 Security roles

##### *5.1.3.3.1 FMT_MSA.1.1*

The TSF shall enforce the **[assignment**: **access control SFP]** to restrict the ability to **[selection**: **change_default, query, modify, delete]** the security attributes **[assignment**: **de roles asignados a un usuario]** to **[assignment**: **los usuarios con el rol Administrador].**

#### *5.1.3.3.2 FMT_MSA.3.1*

The TSF shall enforce the **[assignment: access control SFP]** to provide **[selection**: **restrictive]**, default values for security attributes that are used to enforce the SFP.

#### *5.1.3.3.3 FMT_MSA.3.2*

The TSF shall allow the **[assignment**: **none]** to specify alternative initial values to override the default values when an object or information is created.

Application note: The administrator shall assign the minimum necessary privileges to each new user for their required role.

## *5.1.4 Class FTA: TOE Access*

### 5.1.4.1 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.2 con las siguientes características:
  - Hierarchical to: No other components
  - Dependencies: FIA_UAU.1 Timing of authentication
- FTA_SSL.4 User initiated termination
  - Hierarchical to: No other components
  - Dependencies: No dependencies

#### *5.1.4.1.1 FTA_SSL.1.1*

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

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

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

#### *5.1.4.1.2 FTA_SSL.1.2*

The TSF shall require the following events to occur prior to unlocking the session: **[assignment**: **mostrar una ventana indicando que ha caducado la sesión pudiendo volver a autenticarse o cerrar la sesión]**.

#### *5.1.4.1.3 FTA_SSL.2.1*

The TSF shall allow user-initiated locking of the user's own interactive session, by:

a) Clearing or overwriting display devices, making the current contents unreadable;

b) Disabling any activity of the user's data access/display devices other than unlocking the session

#### *5.1.4.1.4 FTA_SSL.2.2*

The TSF shall require the following events to occur prior to unlocking the session: **[assignment: mostrar una ventana indicando que ha caducado la sesión pudiendo volver a autenticarse o cerrar la sesión].**

#### *5.1.4.1.5 FTA_SSL.4.1*

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

### 5.1.4.2 TOE sesión 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

#### *5.1.4.2.1 FTA_TSE.1.1*

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

## 5.2 Security Functional Requirements rationale

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.AUTENTICACIÓN | O.ACCESO |
| Requisitos Funcionales | **FDP_ACC.2** | | X |
| | **FDP_ACF.1** | | X |
| | **FIA_AFL.1** | X | |
| | **FIA_ATD.1** | X | X |
| | **FIA_UAU.2** | X | |
| | **FIA_UID.2** | | X |
| | **FMT_MSA.1** | | X |
| | **FMT_MSA.3** | | X |
| | **FMT_SMF.1** | | X |
| | **FMT_SMR.1** | | X |
| | **FTA_SSL.1** | X | |
| | **FTA_SSL.2** | X | |
| | **FTA_SSL.4** | X | |
| | **FTA_TSE.1** | X | |

**Ilustración 9 – Relación de objetivos de seguridad y requisitos funcionales**

El objetivo **O.AUTENTICACION** indica que el TOE no permitirá el acceso a sus interfaces 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

- FIA_AFL.1: carmen se encuentra configurada para bloquear de forma transparente a cualquier usuario tras 5 intentos de autenticación fallidos durante 60 minutos.
- FIA_ATD.1: asignando de forma permanente un identificador de usuario único que no puede ser modificado en la creación relacionado con el usuario autenticado.
- FIA_UAU.2: incorporando un sistema de autenticación que comprueba si un usuario se encuentra logado y con una sesión válida antes de realizar cualquier acción en el sistema.
- FTA_SSL.1: mediante la configuración de un período de timeout para la sesión de los usuarios.
- FTA_SSL.2: mediante una ventana que indica que la sesión ha caducado permitiendo volver a logarse o cerrar sesión.
- FTA_SSL4: 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:

- FDP_ACC.2: relacionando el usuario autenticado y las pantallas a las que tiene autorización de acceso.
- FDP_ACF.1: mediante un sistema de autorización propietario (ACL) que únicamente permite el acceso al os componentes según los roles asignados al sujeto.
- FIA_ATD.1: registrando los intentos de autenticación, tanto exitosos como fallidos que pueden ser consultados en la interfaz.
- FIA_UID.2: mediante un sistema de gestión de personas y roles en las que se asigna de forma unívoca los roles que debe tener una persona y las pantallas a las que tiene acceso cada uno de los roles.
- FMT_MSA.1: mediante la habilidad de gestionar por parte de los roles autorizados, los atributos de seguridad de los usuarios del TOE.
- FMT_MSA.3: proporcionando por defecto valores restrictivos.
- FMT_SMF.1: mediante la existencia de las pantallas de gestión de roles en las que se asignan de forma unívoca las funciones de administración.
- FMT_SMR.1: mediante la existencia de las pantallas de gestión de personas y roles definidos, en las que se asignan de forma unívoca las relaciones entre éstos.

## 5.3 Assurance Security Requirements.

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**:

### *5.3.1 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 assesment** | AVA_VAN.2 Vulnerability analysis |

**Ilustración 10 – 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.

## 5.4 Justification of the assurance requirements

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.

# 6 TOE Summary Specification

## 6.1 Security Functions

### *6.1.1 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.

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 puede tener acceso.

Los requisitos relevantes asociados son los siguientes: FIA_AFL.1, FTA_SSL.1, FTA_SSL.2, FTA_SSL.4 y FIA_UAU.2.

**carmen** asegura el requisito FIA_AFL.1, mediante la configuración de un bloqueo de forma transparente a cualquier usuario tras 5 intentos de autenticación fallidos durante 60 minutos.

**carmen** asegura los requisitos FTA_SSL.1.1 y FTA_SSL.2.1 mediante la configuración de un periodo de timeout para la sesión de los usuarios y la monitorización de dicha caducidad.

**carmen** asegura los requisitos FTA_SSL.1.2 y FTA_SSL.2.2 puesto que en el momento en el que identifica que la sesión ha caducado muestra una ventana al usuario para que vuelva a autenticarse o cierre la sesión sin permitirle realizar ninguna acción adicional.

**carmen** asegura el requisito FTA_SSL.4 mediante un botón para cerrar la sesión por parte del usuario.

**carmen** asegura el requisito FIA_UAU.2.1 mediante la incorporación de un sistema de autenticación que comprueba si un usuario se encuentra logeado y con una sesión válida antes de realizar cualquier acción en el sistema.

### *6.1.2 Identificación*

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 la confidencialidad de la información mostrada en la interfaz.

Los requisitos relevantes asociados son los siguientes: FIA_AFL.1, FIA_ATD.1, FIA_UAU.2, FIA_UID.2.1 FTA_SSL.1, FTA_SSL.2 y FTA_SSL.4

**carmen** asegura el requisito FIA_UID.2.1 mediante las pantallas de gestión de personas y roles en las que se asignan de forma unívoca los roles que debe tener una persona y las pantallas a las que tiene acceso cada uno de los roles, además un usuario no puede realizar ninguna acción en su nombre si no ha sido autenticado en el sistema.

**carmen** asegura el requisito FIA_AFL.1, mediante la configuración de un bloqueao de forma transparente a cualquier usuario tras 5 intentos de autenticación fallidos durante 60 minutos.

**carmen** asegura el requisito FIA_ATD.1, a través de vincular un conjunto de funcionalidad de la TSF a determinados usuarios.

**carmen** asegura los requisitos FTA_SSL.1.1 y FTA_SSL.2.1 mediante la configuración de un periodo de timeout para la sesión de los usuarios y la monitorización de dicha caducidad.

**carmen** asegura los requisitos FTA_SSL.1.2 y FTA_SSL.2.2 puesto que en el momento en el que identifica que la sesión ha caducado muestra una ventana al usuario para que vuelva a autenticarse o cierre la sesión sin permitirle realizar ninguna acción adicional.

**carmen** asegura el requisito FTA_SSL.4 mediante un botón para cerrar la sesión por parte del usuario.

### *6.1.3 Control de acceso*

El TOE es el único modo de acceder a la información recolectada y analizada de la organización en la que se despliega. Ningún tipo de información sensible puede ser consultado de otro modo, siendo siempre necesario estar autenticado en el sistema para acceder a la información y autorizado para acceder a dicha información.

El TOE dispone de un mecanismo de gestión de personas y roles en la que se asignan de forma unívoca las relaciones entre éstos garantizando que la información únicamente es accesible para los usuarios habilitados para ello.

Los requisitos relevantes asociados son los siguientes: FMT_SMF.1, FMT_MSA.1, FMT_MSA.3, FTA_TSE.1 y FMT_SMR.1.

**carmen** asegura los requisitos FMT_SMF.1.1 mediante las pantallas de gestión de personas y roles en las que se asignan de forma unívoca los roles que debe tener una persona y las pantallas a las que tiene acceso cada uno de los roles.

**carmen** asegura los requisitos FMT_MSA.1.1, FMT_MSA.3.1 y FMT_MSA.3.2 mediante las pantallas de gestión de personas y roles en las que se asignan de forma unívoca los roles que debe tener una persona y las funciones a las que tiene acceso cada uno de los roles.

**carmen** asegura el requisito FTA_TSE.1.1 mediante la comprobación de las credenciales de los usuarios para asegurar la correcta autenticación de éstos y dispone de la posibilidad de seleccionar la opción de cuenta bloqueada en el perfil de los usuarios, bien porque un usuario con privilegios considera que debe ser bloqueado, bien porque se encuentren intentos reiterados de acceso incorrecto en la pantalla de control

de resultados de autenticación. Cualquier usuario puede ser bloqueado, independientemente de su tipo o rol en carmen.

**carmen** asegura el requisito FMT_SMR.1 mediante las pantallas de gestión de personas y roles en las que se asignan de forma unívoca los roles que debe tener una persona y las pantallas a las que tiene acceso cada uno de los roles.

### 6.1.4 Autorización

El TOE permite realizar una gestión de roles a los que se les asocia el control de acceso a cada una de las pantallas y datos recolectados y generados por la aplicación.

Estos roles son relacionados con cada uno de los usuarios de **carmen** permitiendo asignar los permisos adecuados para acceder a los logs recolectados

La gestión de roles de carmen 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: FDP_ACC.2, FDP_ACF.1, FIA_UID.2, FMT_SMR.1, FTA_SSL.1 y FTA_SSL.2.

**carmen** asegura el requisito FDP_ACC.2, mediante la relación entre el usuario autenticado y las pantallas a las que tiene autorización para acceder. Esta relación se realiza a mediante la asignación de roles a un usuario para permitir el acceso a estas pantallas.

**carmen** asegura el requisito FDP_ACF.1, a través de un sistema de autorización propietario (ACL) que únicamente permite el acceso a los componentes según los roles asignados a sujeto.

**carmen** asegura el requisito FIA_UID.2.1 mediante las pantallas de gestión de personas y roles en las que se asignan de forma unívoca los roles que debe tener una persona y las pantallas a las que tiene acceso cada uno de los roles, además un usuario no puede realizar ninguna acción en su nombre si no ha sido autenticado en el sistema.

**carmen** asegura los requisitos FMT_SMR.1 mediante las pantallas de gestión de personas y roles en las que se asignan de forma unívoca los roles que debe tener una persona y las pantallas a las que tiene acceso cada uno de los roles.

**carmen** asegura los requisitos FTA_SSL.1.1 y FTA_SSL.2.1 mediante la configuración de un periodo de timeout para la sesión de los usuarios y la monitorización de dicha caducidad.

**carmen** asegura los requisitos FTA_SSL.1.2 y FTA_SSL.2.2 puesto que en el momento en el que identifica que la sesión ha caducado muestra una ventana al usuario para que vuelva a autenticarse o cierre la sesión sin permitirle realizar ninguna acción adicional.

**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**