Security Target Lite

NGSIEM LogICA5 7.1 Security Target Lite

Versión 1.0
03/02/2020

Grupo ICA
La Rábida 27
28039 Madrid

Control de versiones

Versión	Responsable			Modificación
1.0	Autor:	CiberSeguridad	03/02/2020	Versión inicial
	Revisión:	La Dirección	03/02/2020	

Contenido

ILUSTRACIONES

TABLAS

1. Security Target Introduction

Esta sección introduce el TOE, identifica el ST, la versión CC aplicable, las definiciones, y abreviaturas utilizadas a lo largo de la declaración.

Esta declaración contiene las siguientes secciones:

- Conformance Claims (2). Contiene la identificación de la versión CC aplicable y el nivel de evaluación.
- Security Problem Definition (3). Describe las amenazas y las suposiciones que definen el problema de seguridad que debe contemplar el TOE y su entorno operativo.
- Security Objectives (4). Describe los objetivos de seguridad para el TOE y su entorno operativo necesarios para contrarrestar las amenazas y satisfacer los supuestos que definen el problema de seguridad.
- Security Requirements (5). Especifica los requisitos funcionales de seguridad (SFR) y los requisitos de garantía de seguridad (SAR) que debe cumplir el TOE.
- TOE Summary Specification (6). Describe las funciones de seguridad del TOE y cómo satisfacen los requisitos funcionales de seguridad.

1.1 ST reference

Título ST: NGSIEM LogICA5 Security Target Lite

Versión ST: Versión 1.0

Fecha ST: 03/02/2020

1.2 TOE reference[1]

NGSIEM LogICA5 7.1

Identificación TOE:

Subsistemas pertenecientes al entorno de aplicación de NGSIEM LogICA5, proporcionados por los componentes o plugins base core:

- Servidores de front end 1.1.12
- Bus de streaming y procesado en tiempo real 1.1.12

y su extensión en funcionalidad proporcionada por los componentes o plugins de extensión core:

- Gestión de usuarios y roles 1.1.12
- Gestión de auditoría 1.1.12

[1] Cualquier referencia al TOE, NGSIEM LogICA5, y a cualquiera de sus componentes referenciados como, -Servidores de front end, Bus de streaming y procesado en tiempo real, Gestíon de usuarios y roles, Gestión de auditoría, Inventario de activos, Gestión de incidentes, Análisis forense, Análisis en tiempo real y correlación de eventos de seguridad y Planificación de tareas -, a lo largo de la documentación desarrollada, se refiere a la versión aquí declarada.

- Inventario de activos 1.1.12
- Gestión de incidentes 1.1.12
- Análisis forense 1.1.12
- Análisis en tiempo real y correlación de eventos de seguridad 1.1.12
- Planificación de tareas 1.1.12

Todos los componentes anteriormente indicados se empaquetan en un único paquete de instalación LogICA5-core-1.1.12.-Release.x86_64.rpm.

Versión del TOE:

7.1

Fabricante TOE:

I.C.A. Informática y Comunicaciones Avanzadas, S.L.

Esponsor Evaluación:

I.C.A. Informática y Comunicaciones Avanzadas, S.L.

1.3 CC reference

Identificación CC: Common Criteria for Information Technology Security Evaluation, Version v3.1r5.

1.4 Definiciones

- Amenaza. Todo elemento o acción capaz de atentar contra la seguridad de la información.
- Apache Kafka. Plataforma unificada, de alto rendimiento y de baja latencia para la manipulación en tiempo real de fuentes de datos. Sistema distribuido de mensajería para la publicación y subscripción de mensajes.
- Apache Storm. Sistema de computación en tiempo real, distribuido, libre y de código abierto.
- Apache Zookeeper. Servicio para la coordinación de procesos distribuido y altamente confiable que da soluciones a varios problemas de coordinación para grandes sistemas distribuidos.
- Cola (queue). Clasificación de eventos de seguridad según valores de las propiedades del evento de seguridad.
- Colección. Colección de documentos JSON, de forma unificada, en una base de datos NoSQL orientada a documentos JSON. Las colecciones pueden admitir índices para mejorar las búsquedas.
- Componente. Elemento de división de un subsistema de NGSIEM LogICA5. Un componente puede ser un plugin, pero un plugin es siempre un componente. Un componente puede estar constituido de componentes. Ejemplo: el subsistema base del bus de streaming y procesado en tiempo real está basado en un plugin base. Este plugin está constituido de dos componentes: el componente de entrada y el componente de recolección y procesamiento.

- Correlación de eventos de seguridad. Técnica basada en la monitorización en tiempo real de eventos de seguridad para detectar patrones de actividad mediante el uso de funciones de correlación como: ventanas de tiempo, contextos, umbrales, condiciones de acuerdo a expresiones lógicas o complejas sobre modelos entrenados.
- Datos SIEM (SIEM data). Datos transmitidos por los sistemas cedentes: líneas de logs y eventos de seguridad.
- Documento JSON. JSON (acrónimo de JavaScript Object Notation) es un formato de texto sencillo para el intercambio de datos. Se trata de un subconjunto de la notación literal de objetos de JavaScript.
- Entorno IT. Conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de información.
- Evento de seguridad (security event). Tupla de propiedades fijas y extendidas que normalizan uno o varios registros de log.
- HDFS. Sistema de archivos distribuido, escalable y portátil escrito en Java para el framework Hadoop.
- HTTPS. Protocolo seguro de transferencia de hipertexto, es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto.
- Línea de log (log line). Línea de un archivo de log.
- Líneas de logs (log lines). Líneas de varios archivos de log.
- Módulo. Subsistema físico de NGSIEM LogICA5. Despliegue físico de un subsistema lógico de NGSIEM LogICA5.
- MongoDB. Sistema de base de datos NoSQL, orientado a documentos JSON.
- Plugin. Componente constitutivo de NGSIEM LogICA5. Existen plugins base y de extensión. Los subsistemas del TOE se encuentran constituidos de plugins.
- Sección de acceso (access section). Mecanismo de segregación de acceso en el subsistema de front end. Basado en identificadores tipo <acceso>/<componente/plugin>.
- Servicio de front end público. Servicio REST perteneciente al subsistema de servidores de front end que puede ser invocado sin identificación ni autenticación previa. Los servicios de front end públicos son los siguientes:
    - validation-by-email: devuelve si el mecanismo de identificación de usuario de front end es por la dirección de email del usuario o por un nombre de usuario.
    - security-type: devuelve si el almacenado de usuarios de front end es: en el subsistema de almacenamiento primario, en un servidor de LDAP o en el subsistema de almacenamiento primario en modalidad SaaS. (El almacenado de los usuarios de front end en LDAP o en modalidad SaaS no se encuentra incluido en la configuración evaluada del TOE).
- SETP. El protocolo SETP es un protocolo propietario de Grupo ICA que incorpora NGSIEM LogICA5 para el envío de eventos de seguridad serializados java/XML por HTTP/S.
- Sistema cedente (Transferring system). Sistema IT perteneciente a la organización del cliente adjudicatario de la plataforma. Sistema proveedor de registros de log.

El propio TOE puede ser un sistema cedente, al igual que el entorno operacional del TOE.

- Subsistema. Subsistema lógico del sistema NGSIEM LogICA5. Se encuentran constituidos de componentes.
- Tópico. Categorización de mensajes en un sistema distribuido subscriptor/publicador de mensajes.
- Usuarios administradores del TOE:
  - Usuarios del sistema operativo administradores del TOE.
  - Usuarios de front end administradores del TOE.
- Usuarios de bases de datos. Usuarios con acceso a la base de datos del entorno operacional del TOE.
- Usuarios de front end. Usuarios del subsistema de front end del TOE asignados a roles con secciones de acceso.
- Usuarios de front end administradores del TOE. Usuarios del subsistema de front end con roles de administración: roles con secciones de acceso asignadas tipo admin/* (el asterisco denomina el nombre del componente o plugin como admin/cep o admin/security, cada sección de acceso permite realizar acciones de administración sobre cada componente o plugin).
- Usuarios del bus. Usuarios del subsistema del bus de streaming y procesado en tiempo real del TOE encargados de transmitir líneas de logs y eventos de seguridad.
- Usuarios del sistema operativo. Usuarios del sistema operativo de la máquina en la que se ejecuta el TOE.
- Usuarios del sistema operativo administradores del TOE. Usuarios del sistema operativo con privilegios para operar sobre el TOE, autorizados por el propio TOE, con acceso de escritura a todos los archivos desplegados del TOE, incluyendo archivos relacionados como, por ejemplo: archivos de configuración de rotación de archivos de logs o servicios de ejecución, entre otros.
- Usuarios del TOE:
  - Usuarios del sistema operativo
  - Usuarios remotos
- Usuarios remotos. Usuarios que establecen una ruta de confianza basada en TLS 1.2. con el TOE. Usuarios de front end y usuarios del bus.
- XFS. sistema de archivos de 64 bits con registro de bitácora o journaling de alto rendimiento para su implementación de UNIX.

1.5 Abreviaturas y Acrónimos

- AES Advanced Encryption Standard. Sistema criptográfico de clave simétrica.
- CA Certification Authority
- CC Common Criteria
- CMDB Configuration Management Database
- EAL Evaluation Assurance Level
- HDFS Hadoop Distributed File System
- HTTPS Hypertext Transfer Protocol Secure
- IOC Indicator of Compromise
- JSON JavaScript Object Notation

- LDAP Lightweight Directory Access Protocol
- NTP Network Time Protocol
- REST Representational State Transfer
- RSA Sistema criptográfico de clave pública. Sistema criptográfico asimétrico. Creado por Rivest, Shamir y Adleman
- SaaS Software as a Service
- SAR Security Assurance Requirement
- SETP Security Event Transfer Protocol
- SFR Security Functional Requirement
- SFP Securiry Functional Policies
- SHA3 Secure Hash Algorithm 3
- ST Security Target
- TCP Transmission Control Policy
- TLS Transport Layer Security
- TOE Target of Evaluation
- TSF TOE security function
- TSFI TOE security functions interface
- UDP User Datagram Protocol
- UEBA User and Entity Behavior Analytics
- VRRP Virtual Router Redundancy Protocol
- XFS eXtent File System
- XML eXtensible Markup Language
- X509 Estándar para infraestructuras de clave pública. Específica, entre otros estándares, formatos estándar de certificados de clave pública.

1.6 TOE Overview

NGSIEM LogICA5 es una solución NGSIEM (gestión de eventos de seguridad e información de seguridad de nueva generación) modular que integra:

- Recopilación de datos de seguridad para el cómputo de variables técnicas.
- Inventario de activos orientado a repositorio de configuraciones CMDB.
- Mantenimiento de CMDB de activos en estructura e instancias de la propia herramienta.
- Descubrimiento de activos y actualización de información de la CMDB.
- Capacidades de gestión de líneas de logs con fines de auditoría forense, así como la recolección, indexación y control de la información de los dispositivos en un sistema jerárquico forense.
- Detección y tratamiento de eventos de seguridad en tiempo real a través de la capa de agentes que se reciben por el motor de recolección
- Correlación centralizada con una amplia colección de reglas de correlación disponibles.

Y las siguientes funcionalidades no incluidas en el TOE.

- Comparativa de vulnerabilidades de activos en base a BD e histórico de resultados obtenidos desde la misma plataforma.

- Vigilancia de configuraciones de activos. Implementa funcionalidades de detección de cambios en archivos de configuración.
- Descubrimiento de anomalías y análisis predictivo basado en patrones.
- Descubrimiento de amenazas y vulnerabilidades sobre activos almacenados en la CMDB de activos.
- Consulta de BD de vulnerabilidades externas con actualización de información.
- Motor de informes expositivos y analíticos.

A su vez, la plataforma puede ser desplegada en modalidad de servicio, con las funcionalidades expuestas out of the box, o en modo on premise. En el ámbito de esta evaluación se despliega en modo on premise, en un appliance.

Permite la integración con otras soluciones, no incluidas en el TOE, para:

- Almacenamiento externo de incidentes.
- Centralización de usuarios de front end por LDAP.
- Enriquecimiento de la información de seguridad mediante feeds.
- Consulta de hashes, listas de reputación, análisis de vulnerabilidades y otra información relacionada con la seguridad informática.
- Labores de threat hunting y descubrimiento de IOCs.
- Análisis UEBA.
- Motores de análisis predictivo mediante aprendizaje.
- …

Las funciones evaluadas son las siguientes:

- Auditoría de seguridad
- Operaciones con claves criptográficas
- Autenticación e identificación
- Gestión de los datos y funciones de seguridad
    - Gestión de usuarios de front end
    - Asignación de roles a usuarios de front end
    - Políticas de seguridad
    - Gestión de mecanismos de acceso a datos de los sistemas cedentes.
    - Gestión de la configuración de entradas de líneas de log
    - Gestión de la activación de reglas de correlación
    - Gestión de la respuesta – alarmas - debido a funciones de correlación
    - Notificación a destinatarios de correo electrónico ante la respuesta – alarmas -.
- Acceso y Protección
- Rutas confiables

La plataforma se encuentra constituida por varios módulos base o subsistemas, pertenecientes a diferentes entornos de actuación.

El siguiente diagrama muestra los límites del TOE frente al resto de subsistemas de la plataforma NGSIEM LogICA5 que no son parte constituyente del TOE:

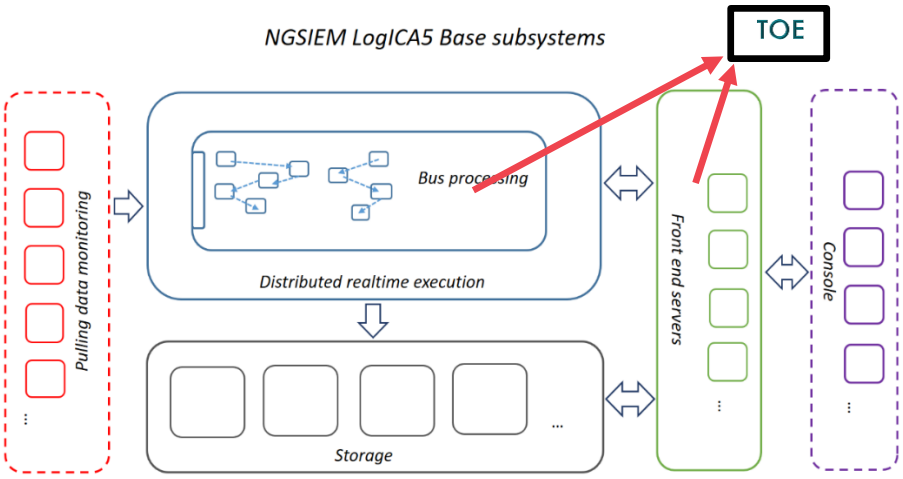

ILUSTRACIÓN 1 NGSIEM LOGICA5 SUBSYSTEMS

Se aprecian los diferentes subsistemas o módulos que forman la plataforma NGSIEM LogICA5:

- Subsistemas base pertenecientes al entorno operacional de NGSIEM LogICA5:
  - Sistema de almacenamiento
  - Sistema distribuido de ejecución en tiempo real
- Subsistemas base pertenecientes al entorno de aplicación de NGSIEM LogICA5:
  - Bus de streaming y procesado en tiempo real
  - Servidores de front end
- Subsistemas base pertenecientes al entorno de integración de NGSIEM LogICA5, subsistemas no pertenecientes al TOE:
  - Monitores de extracción de datos
  - Consola

1.6.1 TOE Type

El TOE es una solución de gestión de eventos de seguridad, solución modular que recolecta y almacena de forma centralizada en dispositivos de alto rendimiento, líneas de logs de sistemas cedentes. Desplegable en formato appliance o formato de plataforma virtualizada - en el ámbito de esta certificación, el TOE se despliega en formato appliance para su validación -. Incorpora capacidad para recolectar datos de cualquier fuente cedente, correlar datos, monitorizar en tiempo real y realizar consultas avanzadas, para desarrollar analítica con objetivos de seguridad.

1.7 TOE Description

En esta sección se describe el TOE y su alcance físico y lógico.

1.7.1 Physical scope

En la Ilustración 1, se muestran los límites del TOE frente al resto de subsistemas de la plataforma que no son parte constituyente del TOE.

El TOE es un producto software constituido por los siguientes subsistemas o módulos base:

- Bus de streaming y procesado en tiempo real
- Servidores de front end

y su extensión en funcionalidad:

- Gestión de usuarios y roles
- Gestión de auditoría
- Gestión de activos
- Gestión de incidentes
- Análisis forense
- Análisis en tiempo real y correlación de eventos de seguridad
- Planificación de tareas

Estos subsistemas o módulos base y su extensión en funcionalidad, proporcionada por los plugins core, se distribuyen como un archivo rpm, LogICA5-core-1.1.12.-Release.x86_64.rpm.

Además, la siguiente documentación es parte del TOE:

- LogICA5-GuiaInstalacion_1.10.pdf
- LogICA5-GuiaOperacion_1.11.pdf
- LogICA5-Distribución_2.5.pdf

La instalación inicial del entorno operacional se efectúa en un Appliance. Se entrega a través de transportistas especializados embalado en cajas o contenedores cerrados junto con albarán de entrega.

La parte constituyente del TOE, se entrega desde servidor de descarga online, firmado electrónicamente, la integridad se verifica a través de la clave pública suministrada, mediante - gpg --verify nombre_fichero.sig nombre_fichero -, para ser instalado en el Appliance, junto con un certificado en Papel/Formato Electrónico de licencia de producto en el cual se incluye, Referencia de producto, clave de licencia y proyecto al que aplica.

La plataforma software se empaqueta:

- Desde servidor de descarga online. Contiene los manuales y el RPM de la parte constituyente del TOE de NGSIEM LogICA5:
  - LogICA5-core-1.1.12.-Release.x86_64.rpm
  - LogICA5-GuiaInstalacion_1.10.pdf
  - LogICA5-GuiaOperacion_1.11.pdf
  - LogICA5-Distribución_2.5.pdf

- Desde servidor de descarga online. Contiene la documentación adicional de entrega. Documentación de soporte no perteneciente al TOE:
  - LogICA5-LicenciaDeUso_1.1.pdf
  - LogICA5-Credenciales.pdf
  - LogICA5-EtiquetaAppliance_1.0.pdf
  - LogICA5-Recepción_1.6.doc
  - NGSIEM-LogICA5-7.1-Resumen.pdf
  - Clave pública.asc
- Desde servidor de descarga online. Contiene los manuales y los RPM de la parte no constituyente del TOE de NGSIEM LogICA5, firmados también electrónicamente con el mismo método de verificación del TOE:
  - LogICA5-add-on-1.1.12.-Release.x86_64.rpm
  - LogICA5-GuiaUsuario_1.1.pdf
  - Monitor-1.1.3.-Release.x86_64.rpm
  - Monitor-1.1.3-release.x86_64.msi
  - LogICA5-GuiaUsuarioMonitor_1.1.pdf

Los subsistemas del entorno operacional y los adicionales de integración de la plataforma NGSIEM LogICA5 del TOE aparecen en la Ilustración 1.

El entorno operacional del TOE es:

- Sistema operativo CentOS7. CentOS Linux 7.x 64-bit
- Base de datos MongoDB 3.6.8
- Plataforma de ejecución de nodejs 8.12.0
- Plataforma de ejecución java 1.8.0_161
- Manejador de cluster Apache Zookeeper 3.4.12
- Broker Kafka 2.12-1.0.0
- Base de datos Redis 0:3.2.12-2.el7
- Plataforma distribuida Apache Storm 1.0.6
- Sistema de auditoria Nmap
- Librerías adicionales

Los mínimos requerimientos hardware del appliance son:

- Arquitectura: x86_64
- CPU:1 x 8C o equivalente (2 x 8C recomendado)
- Memoria: 128 GB (512 GB recomendado)
- Espacio Disco: 2T (mínimo)
- Partición Root: 50 GB (mínimo)
- Dos interfaces de red de 1G.

1.7.2 Logical scope

El alcance lógico del TOE está dividido en clases de seguridad que son descritas en detalle en las secciones 5 y 6. El alcance lógico también proporciona la descripción de seguridad de las características del TOE. Los requisitos funcionales de seguridad implementados por el TOE son agrupados mediante las siguientes funcionalidades de seguridad:

1.7.2.1 Registros de auditoría

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.

1.7.2.2 Claves criptográficas

El TOE emplea claves criptográficas para:

- Soportar el uso de TLS 1.2 durante la comunicación entre los usuarios remotos y los subsistemas del TOE. RSA de 3072 bits, AES 128/256 bits. EL TOE proporciona métodos de generación y destrucción de claves AES 128/256 soportados por TLS 1.2.
- Almacenar contraseñas en el archivo de configuración del subsistema de Servidores de front end. AES 128 bits.

Y las siguientes funciones de hash:

- Almacenado de las contraseñas de los usuarios remotos. SHA3.

1.7.2.3 Identificación y autenticación

El TOE requiere de autenticación e identificación antes de cualquier acción frente al TOE.

1.7.2.4 Gestión de la seguridad

El TOE proporciona un conjunto de funciones y datos de seguridad para la gestión y parametrización de la seguridad.

En el subsistema del bus de streaming y procesado en tiempo real, los usuarios del sistema operativo administradores del TOE son los encargados de la gestión de los datos y funciones de seguridad. Existe un único rol para la transmisión de información al TOE por lo que no hay segregación de funcionalidad en los usuarios del bus. Rol denominado transmisor de información (information sender).

En el subsistema de servidores de front end los usuarios de front end administradores del TOE son los encargados de gestionar los datos y funciones de seguridad:

- Gestión de usuarios de front end.
- Asignación de roles a usuarios de front end.
- Asignación a roles con:
    - Secciones, segregación de acceso por funciones
    - Autorizaciones sobre los mecanismos de acceso a datos de los sistemas cedentes:
        - Colas de clasificación de eventos de seguridad
        - Patrones de ficheros de log/consultas de líneas de log
        - Acciones sobre eventos de seguridad/líneas de log
- Políticas de seguridad.
- Gestión de los propios mecanismos de acceso a datos de los sistemas cedentes.
- Gestión de la configuración de entradas de syslog.

- Gestión de la activación de: reglas de correlación, de la respuesta mediante alarmas y la notificación a destinatarios de correo electrónico ante la respuesta mediante alarmas.

Inicialmente, existe un único usuario de front end administrador del TOE, llamado super root, con todas las secciones de acceso por defecto – acceso autorizado completo. Este usuario puede crear usuarios de front end y roles con un control de permisos jerárquico.

1.7.2.5 Acceso

El TOE permite a los usuarios remotos finalizar su propia sesión interactiva frente al TOE y finalizar la sesión del usuario tras un tiempo de inactividad configurable

1.7.2.6 Ruta de confianza

El TOE obliga a establecer una ruta de confianza a los usuarios remotos del TOE que quieran comunicarse con el TOE. Toda acción frente al TOE requiere el empleo de una ruta de confianza.

En el subsistema del bus de streaming y procesado en tiempo real, el TOE mantiene rutas de confianza frente al TOE:

- Endpoint de syslog: TLS 1.2, certificados X.509, RSA 3072, AES 128/256, hash de SHA-256.
- Endpoint de setp: HTTPS TLS 1.2, certificados X.509, RSA 3072, AES 128/256, hash de SHA-256.

En el subsistema de servidores de front end:

- Endpoint de servicios REST: HTTPS TLS 1.2, certificados X.509, RSA 3072, AES 128/256, hash de SHA-256.
- Endpoint de websockets: HTTPS TLS 1.2, certificados X.509, RSA 3072, AES 128/256, hash de SHA-256.

1.7.3 Evaluated configuration

La parametrización evaluada del entorno operacional del TOE y del TOE es:

- Entorno operacional del TOE:
  - El TOE se instala en un appliance, un único nodo dedicado en exclusiva a la ejecución del TOE:
    - Arquitectura: x86_64
    - CPU:1 x 8C o equivalente (2 x 8C recomendado)
    - Memoria: 128 GB (512 GB recomendado)
    - Espacio Disco: 2T (mínimo)
    - Partición Root: 50 GB (mínimo)
    - Dos interfaces de red de 1G:
      - Red de gestión de acceso al módulo de servidores de front end.
      - Red de producción de acceso a los sistemas cedentes desde el módulo bus de streaming y procesado en tiempo real.

- Sistema operativo CentOS7
  - CentOS Linux 7.x 64-bit, bastionado.
    - No accesible mediante protocolo SSH como usuario del sistema operativo root
    - Tiempo de expiración de sesión SSH a 5 minutos.
    - Contraseñas fuertes.
    - Usuario del sistema operativo administrador del TOE, logica5, para labores de administración del TOE.
      - Acceso de escritura a directorios y archivos de despliegue del TOE, y de ejecución de servicios del TOE mediante sudo.
    - Usuario del sistema operativo administrador del TOE, root, para labores de administración del TOE y del entorno operacional del TOE.
    - Usuario del sistema operativo, ica, con acceso de lectura a directorios y archivos de despliegue del TOE.
    - Rotación de archivos de logs de la plataforma. Ventana de cinco.
  - Reglas de Firewall:
    - Puertos de entrada:
      - Componente de entrada del módulo bus de streaming y procesado en tiempo real. Puertos con acceso seguro TLS 1.2: 6514, 6083. Acceso desde la red de producción.
      - Servidores de front end. Puertos con acceso seguro TLS 1.2: 7000. Acceso desde la red de gestión.
      - Servicio SSH: 22. Acceso desde la red de gestión.
    - Puertos de salida
      - Sin restricciones de acceso.
- Base de datos MongoDB 3.6.8
  - Configurado en modo stand-alone, un único nodo. Acceso por protocolo TLS 1.2. Sesión de conexión previa mediante autenticación por identificación de usuario y contraseña.
- Plataforma de ejecución de nodejs 8.12.0
- Plataforma de ejecución java 1.8.0_161
- Manejador de cluster Apache Zookeeper 3.4.12
  - Configurado en modo stand-alone, un único nodo. Sin acceso desde el exterior. Protegido por el sistema operativo.
- Broker Kafka 2.12-1.0.0
  - Configurado en modo stand-alone, un único nodo. Sin acceso desde el exterior. Protegido por el sistema operativo.
- Base de datos Redis 0:3.2.12-2.el7
  - Configurado en modo stand-alone, un único nodo. Sin acceso desde el exterior. Protegido por el sistema operativo.
- Plataforma distribuida Apache Storm 1.0.6

        - Configurado en modo stand-alone, un único nodo. Sin acceso desde el exterior. Protegido por el sistema operativo.
    - Sistema de auditoria Nmap
    - Librerías adicionales
    - Almacenamiento secundario en XFS.
- TOE:
    - No se emplea modalidad SaaS
    - TLS 1.2: Soportado por RSA 3072 y AES 128/256
    - Bus de streaming y procesado en tiempo real:
        - Un único nodo, un appliance, para el despliegue, por lo que no hay alta disponibilidad, ni necesidad de balanceo, ni protocolo VRRP.
        - Servicio de recepción de líneas de logs. Protocolo TLS 1.2 sobre syslog TCP y certificados x509, incorporando autenticación del certificado del cliente
        - Servicio de recepción de eventos de seguridad. Protocolo SETP HTTPS sobre TLS 1.2 TCP y certificados x509, autenticación mediante identificación de usuario y contraseña.
    - Servidores de front end
        - Todas las conexiones deben ser efectuadas por protocolo seguro TLS 1.2.
        - Un único nodo, un appliance, para el despliegue de un único servidor de front end, por lo que no hay cluster configurado en el bus de coordinación.
        - No se emplea LDAP para el almacenado de usuarios de front end.
        - Cifrado de todas las contraseñas en el archivo de configuración: AES 128.
        - Configurado en modo que no permita crear ni editar acciones sobre eventos de seguridad y líneas de log. Se emplean las acciones preinstaladas (Whois, Whitelist, Blacklist, Integritycheck, Nmap, Ping y Portscan)

1.8 Conventions

CC permite las operaciones de asignación, refinamiento e iteración en los requisitos funcionales de seguridad. Estas operaciones son empleadas en esta ST. Se describen en la Parte 2 de CC:

- Las declaraciones de asignación se identifican usando [*texto en cursiva entre corchetes*].
- Las declaraciones de selección se identifican usando [texto subrayado entre corchetes].
- Los refinamientos se identifican con **texto en negrita**. Cualquier texto eliminado se tacha (Ejemplo: ~~Datos TSF~~) y debe considerarse como un refinamiento.
- Iteración: permite que un componente se use más de una vez con diferentes operaciones. En esta ST, la iteración se identifica con un número entre paréntesis que sigue al identificador del componente base. Por ejemplo, las iteraciones de

FAU_GEN.1 se identifican: FAU_GEN.1 (1) para el componente y FAU_GEN.1.1 (1) para los elementos.

2. Conformance Claims

2.1 CC Conformance claim

Esta declaración de seguridad cumple Common Criteria v3.1r5, según los requisitos establecidos de contenido y presentación.

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

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version v3.1r5
  Part 2 Conformant.
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version v3.1r5
  Part 3 Conformant.

El nivel de evaluación para el TOE es:

- Evaluation Assurance Level 2 (EAL2).

2.2 PP Claim

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

2.3 Package claim

La presente Declaración de seguridad cumple con el paquete EAL 2 Security Assurance Requirements.

2.4 Conformance rationale

N/A

3. Security problem definition

3.1 Threats

En este apartado se aporta información acerca de las amenazas a las cuales va estar expuesto el TOE.

Todas las amenazas hacen referencia a un atacante que puede ser, o no, un usuario autorizado del sistema.

T.HOST_COMPROMISE

Un atacante puede tener control de la máquina sobre el que se ejecuta el TOE cuando está en producción.

T.BRUTE_FORCE
Un usuario no autorizado puede obtener acceso al TOE a través de intentos reiterados de adivinar la contraseña.

T.FORENSIC_EVENT_MODIFIED
Un atacante puede hacer modificaciones no detectadas en los registros de auditoría gestionados por el TOE, eliminando así la evidencia de actividad no autorizada o maliciosa.

T.INAPPROPRIATE_USE
Usuarios administradores del TOE y usuarios del sistema operativo realizan acciones inapropiadas en el TOE debido al desconocimiento de sus responsabilidades o políticas y procedimientos operativos.

T.IDENTITY_SPOOFING
Un atacante puede realizar operaciones con el TOE con identidad falsa sin ser detectado por medio de la suplantación de identidad de otro usuario.

T.NETWORK_COMPROMISE
Un usuario no autorizado puede monitorizar la red de la organización en un intento de obtener datos confidenciales, como contraseñas, o modificar los datos transmitidos.

T.NO_ACCOUNTABILITY
Usuarios del TOE realizan o intentan realizar acciones maliciosas en el TOE que no son detectadas.

T.PASSW_COMPROMISE
Un atacante puede obtener acceso a los contenedores donde se almacenan las contraseñas y claves del TOE.

T.UNATTENDED_SESSION
Un usuario no autorizado obtiene acceso al TOE a través de una sesión de usuario autorizado desatendida.

T.UNAUTHORIZED_ACCESS
Un atacante puede acceder al TOE sin estar autorizado y sin ser detectado.

T.UNAUTHORIZED_ACTIVITY
Los usuarios del TOE realizan acciones no autorizadas en el TOE.

T.UNDETECTED_THREATS
Situaciones de uso indebido, no autorizado o actividad maliciosa no detectables sin hacer uso de técnicas de correlación en tiempo real.

3.2 Organisational security policies
No aplicable.

3.3 Assumptions

En este apartado se incluye información acerca de las hipótesis del entorno operacional del TOE:

3.3.1 Operational assumptions

A.IDENTIFICATION_&_AUTHENTICATION

El entorno IT será capaz de identificar y autenticar a los usuarios del sistema operativo y a los usuarios de la base de datos.

A.DBINTEGRITY

La base de datos del entorno operacional del TOE mantendrá la integridad de los datos almacenados.

A.INSTALLATION

El sistema operativo y la base de datos del entorno operacional del TOE estarán securizados.

A.PROTECT

El entorno operacional del TOE mantendrá un entorno físico confiable.

A.TIME

El sistema operativo del entorno operacional del TOE proporcionará una base de tiempo confiable.

3.3.2 Personnel assumptions

A.NO_EVIL_ADMIN

Los usuarios administradores del TOE serán confiables y no realizarán acciones maliciosas, además estarán debidamente formados para usar, configurar y mantener el TOE.

A.OS_USER

El acceso al sistema operativo donde se ejecuta el TOE, efectuado mediante el uso de usuarios del sistema operativo, solo será realizado por personal administrador del TOE.

4. Security objectives

4.1 Security objectives for the TOE

O.LOG

El TOE debe proporcionar auditoría de actividad, por medio de la generación de registros de auditoría, de todos los accesos que se realizan en él, del resultado de los mismos, y de la actividad de componentes que lo constituyen, para que los usuarios administradores del TOE revisen los registros de auditoría generados.

O.LOG_REVIEW

El TOE debe proporcionar un mecanismo de consulta de registros de auditoría a los usuarios administradores del TOE.

O.LOG_STORAGE
El TOE debe proteger los registros de auditoría almacenados de modificaciones o eliminaciones no autorizadas.

O.LOGIN_ATTEMPTS
El TOE limitará el número de intentos de autenticación sin éxito consecutivos.

O.IDENTIFY_AUTHENTICITY
El TOE debe requerir que todos los usuarios remotos estén identificados y autenticados antes de obtener acceso a los servicios del TOE.

O.PASSWORD_POLICY
El TOE debe proporcionar un mecanismo para reducir la probabilidad de que los usuarios remotos elijan contraseñas débiles.

O.PASSWORD_PROTECT
El TOE debe proporcionar un mecanismo para proteger las contraseñas almacenadas.

O.ROLE
El TOE debe realizar control de acceso a recursos y objetos del propio TOE basándose en los atributos de los usuarios remotos: identificador, contraseña y roles que permitan segregar las funciones a las cuales tenga acceso cada usuario remoto.

O.SECURECOM
El TOE debe proteger las comunicaciones entre los usuarios remotos y el TOE.

O.SESSION_LOGOUT
El TOE debe proporcionar mecanismos para finalizar una sesión de usuario remoto después de un período de inactividad o a petición del usuario remoto.

O.SIEM_COLLECT
El TOE debe proporcionar mecanismos de captura de datos SIEM desde los sistemas cedentes y de la actividad del propio TOE.

O.SIEM_ALERT
El TOE debe proporcionar mecanismos de generación de alertas ante potenciales amenazas de seguridad basadas en la correlación de los eventos de seguridad recibidos.

4.2 Security objetives for the operational environment

OE.ADMIN_TRUST
Los usuarios administradores del TOE deben ser competentes, tener conocimientos para el trabajo a desarrollar, confiables y cumplir lo expuesto en la guía de operación del TOE. LogICA5-GuiaOperacion_1.11.pdf

OE.OS_USER_TRUST
Los usuarios del sistema operativo deben estar asignados únicamente a personal administrador del TOE.

OE.BAST
El entorno IT sobre el que se instale el TOE debe estar suficientemente bastionado de manera que no ofrezca fallos triviales en su seguridad y proteja los componentes y su configuración del acceso no autorizado.

OE.DBAUTH
El acceso directo a los parámetros, líneas de logs y eventos de seguridad almacenados en la base de datos del entorno operacional del TOE, debe requerir de la identificación y autenticación previa contra la base de datos.

OE.DBINT
La base de datos del entorno operacional del TOE debe proporcionar mecanismos que garanticen la integridad de los datos almacenados.

OE.OSAUTH
El entorno IT debe requerir que los usuarios del sistema operativo estén identificados y autenticados antes de permitirles realizar cualquier actividad relacionada con los TSF.

OE.PHYSICAL
El entorno físico donde opera el TOE debe asegurar que los componentes del TOE estén protegidos de cualquier ataque físico.

OE.TIME
El entorno IT sobre el que se instale el TOE debe proporcionar una base de tiempo confiable.

4.3 Security objectives rationale

La consecución de los objetivos de seguridad se aborda desde la perspectiva de casar los objetivos de seguridad, con las amenazas, suposiciones de entorno y políticas de seguridad organizativas.

SECURITY OBJECTIVES RATIONALE		THREATS												OPERATIONAL ASSUMPTIONS					PERSONNEL ASSUMPTIONS	
		T_HOST_COMPROMISE	T.BRUTE_FORCE	T.FORENSIC_EVENT_MODIFIED	T.INAPPROPRIATE_USE	T.IDENTITY_SPOOFING	T.NETWORK_COMPROMISE	T.NO_ACCOUNTABILITY	T.PASSW_COMPROMISE	T.UNATTENDED_SESSION	T.UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_ACTIVITY	T.UNDETECTED_THREATS	A.IDENTIFICATION_&_AUTHENTICATION	A.DBINTEGRITY	A.INSTALLATION	A.PROTECT	A.TIME	A.NO_EVIL_ADMIN	A.OS_USER
SECURITY OBJECTIVES FOR THE TOE	O.LOG							X			X	X								
	O.LOG_REVIEW											X								
	O.LOG_STORAGE			X																
	O.LOGIN_ATTEMPTS		X																	

SECURITY OBJECTIVES RATIONALE		THREATS												OPERATIONAL ASSUMPTIONS					PERSONNEL ASSUMPTIONS	
		T_HOST_COMPROMISE	T.BRUTE_FORCE	T.FORENSIC_EVENT_MODIFIED	T.INAPPROPRIATE_USE	T.IDENTITY_SPOOFING	T.NETWORK_COMPROMISE	T.NO_ACCOUNTABILITY	T.PASSW_COMPROMISE	T.UNATTENDED_SESSION	T.UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_ACTIVITY	T.UNDETECTED_THREATS	A.IDENTIFICATION_&_AUTHENTICATION	A.DBINTEGRITY	A.INSTALLATION	A.PROTECT	A.TIME	A.NO_EVIL_ADMIN	A.OS_USER
	O.IDENTIFY_AUTHENTICITY					X					X									
	O.PASSWORD_POLICY		X																	
	O.PASSWORD_PROTECT								X											
	O.ROLE					X					X	X								
	O.SECURECOM						X													
	O.SESSION_LOGOUT									X										
	O.SIEM_COLLECT												X							
	O.SIEM_ALERT												X							
SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENTOE	OE.ADMIN_TRUST	X	X		X	X						X							X	
	OE.OS_USER_TRUST	X			X	X						X								X
	OE.BAST	X				X			X			X				X				
	OE.DBAUTH								X		X			X		X				
	OE.DBINT														X					
	OE.OSAUTH	X							X		X			X		X				
	OE.PHYSICAL	X							X								X			
	OE.TIME							X										X		

TABLA 1: SECURITY OBJECTIVES RATIONALE

Security objetives rationale justifica que los objetivos de seguridad, tanto del TOE como del entorno operativo, cubren todas las amenazas y las asunciones.

T.HOST_COMPROMISE
Un atacante puede tener control de la máquina sobre el que se ejecuta el TOE cuando está en producción.

Esta amenaza es contrarrestada por los siguientes objetivos de seguridad:

- OE.ADMIN_TRUST – satisface el objetivo suponiendo la garantía de los usuarios administradores del TOE, estén debidamente capacitados para administrar el TOE.
- OE.OS_USER_TRUST – satisface el objetivo suponiendo la garantía de que los usuarios del sistema operativo pertenecen a personal administrador del TOE, los cuales están debidamente capacitados para realizar sus tareas y son confiables.

- OE.BAST – satisface el objetivo suponiendo la garantía de que el sistema operativo de cada componente del TOE proteja el componente y su configuración ante acceso no autorizado.
- OE.OSAUTH – complementa este objetivo suponiendo la garantía de que los usuarios del sistema operativo, estén previamente identificados y autenticados con permisos suficientes y necesarios antes de poder operar en la máquina en la que se ejecuta el TOE.
- OE.PHYSICAL – satisface el objetivo suponiendo la garantía de que el TOE y la infraestructura de operación, esté protegido contra ataques físicos.

T.BRUTE_FORCE
Un usuario no autorizado puede obtener acceso al TOE a través de intentos reiterados de adivinar la contraseña.

Esta amenaza es contrarrestada por los siguientes objetivos de seguridad:
- O.LOGIN_ATTEMPTS – gestiona esta amenaza proporcionando un mecanismo, configurable por un administrador del TOE, para bloquear una cuenta de usuario remoto después de que se haya alcanzado un número específico de intentos de autenticación fallidos consecutivos.
- O.PASSWORD_POLICY – gestiona esta amenaza proporcionando un mecanismo, configurable por un administrador del TOE, que obligue a los usuarios remotos a elegir contraseñas difíciles de adivinar.
- OE.ADMIN_TRUST – satisface el objetivo suponiendo la garantía de que aquellos usuarios administradores del TOE, estén debidamente capacitados para administrar el TOE.

T.FORENSIC_EVENT_MODIFIED
Un atacante puede hacer modificaciones no detectadas en los registros de auditoría gestionados por el TOE, eliminando así la evidencia de actividad no autorizada o maliciosa.

Esta amenaza es contrarrestada por los siguientes objetivos de seguridad:
- O.LOG_STORAGE – gestiona esta amenaza proporcionando un mecanismo de protección de los registros de auditoría almacenados, frente a modificaciones y eliminaciones no autorizadas.

T.INAPPROPRIATE_USE
Usuarios administradores del TOE y del sistema operativo realizan acciones inapropiadas en el TOE debido al desconocimiento de sus responsabilidades o políticas y procedimientos operativos.

Esta amenaza es contrarrestada por los siguientes objetivos de seguridad:
- OE.ADMIN_TRUST – satisface el objetivo suponiendo la garantía de que los usuarios administradores del TOE, estén debidamente capacitados para administrar el TOE y son confiables.

- OE.OS_USER_TRUST – satisface el objetivo suponiendo la garantía de que los usuarios del sistema operativo pertenecen a personal administrador del TOE, los cuales están debidamente capacitados para realizar sus tareas y son confiables.

T.IDENTITY_SPOOFING
Un atacante puede realizar operaciones con el TOE con identidad falsa sin ser detectado por medio de la suplantación de identidad de otro usuario.

Esta amenaza es contrarrestada por los siguientes objetivos de seguridad:

- O.IDENTIFY_AUTHENTICITY – gestiona esta amenaza asegurando que todos los usuarios remotos, estén identificados y autenticados previamente a la obtención de acceso al TOE y a los servicios del TOE.
- O.ROLE – gestiona esta amenaza proporcionando un mecanismo que requiere que los usuarios remotos autorizados, tengan los privilegios adecuados para realizar acciones en el TOE.
- OE.ADMIN_TRUST – satisface el objetivo suponiendo la garantía de que los usuarios administradores del TOE, estén debidamente capacitados para administrar el TOE y son confiables.
- OE.OS_USER_TRUST – satisface el objetivo suponiendo la garantía de que los usuarios del sistema operativo pertenecen a personal administrador del TOE, los cuales están debidamente capacitados para realizar sus tareas y son confiables.
- OE.BAST – satisface el objetivo suponiendo la garantía de que el sistema operativo de cada componente del TOE, proteja el componente y su configuración ante acceso no autorizado.

T.NETWORK_COMPROMISE
Un usuario no autorizado puede monitorizar la red de la organización en un intento de obtener datos confidenciales, como contraseñas, o modificar los datos transmitidos.

Esta amenaza es contrarrestada por el siguiente objetivo de seguridad:

- O.SECURECOM – gestiona esta amenaza proporcionando un mecanismo que asegura que el TOE, proteja las comunicaciones entre los usuarios remotos y el propio TOE.

T.NO_ACCOUNTABILITY
Usuarios del TOE realizan o intentan realizar acciones maliciosas en el TOE que no son detectadas.

Esta amenaza es contrarrestada por los siguientes objetivos de seguridad:

- O.LOG – gestiona esta amenaza asegurando que el TOE genere registros de auditoría de eventos relevantes para la seguridad y estos pueden ser consultados por usuarios administradores del TOE.
- OE.TIME – es complemento de O.LOG y satisface el objetivo suponiendo la garantía de que el entorno TI pueda proporcionar a los componentes del TOE una fuente de tiempo confiable que se pueda usar para generar marcado de tiempo para su inclusión en los registros de auditoría generados.

T.PASSW_COMPROMISE
Un atacante puede obtener acceso a los contenedores donde se almacenan las contraseñas y claves del TOE.

Esta amenaza es contrarrestada por los siguientes objetivos de seguridad:

- O.PASSWORD_PROTECT – gestiona esta amenaza proporcionando el TOE mecanismos que protejan las contraseñas almacenadas.
- OE.BAST – satisface el objetivo suponiendo la garantía de que el sistema operativo de cada componente del TOE, proteja el componente y su configuración ante acceso no autorizado.
- OE.DBAUTH – satisface este objetivo suponiendo la garantía de que los usuarios de base de datos están previamente identificados y autenticados con permisos suficientes y necesarios antes de realizar cualquier actividad con la base de datos.
- OE.OSAUTH – complementa este objetivo suponiendo la garantía de que los usuarios del sistema operativo están previamente identificados y autenticados con permisos suficientes y necesarios antes de poder operar con la máquina en la que se ejecuta el TOE.
- OE.PHYSICAL – satisface el objetivo suponiendo la garantía de que el TOE y el entorno operacional del TOE esté protegido contra ataques físicos.

T.UNATTENDED_SESSION
Un usuario no autorizado obtiene acceso al TOE a través de una sesión de usuario autorizado desatendida.

Esta amenaza es contrarrestada por los siguientes objetivos de seguridad:

- O.SESSION_LOGOUT – gestiona esta amenaza proporcionando a los usuarios remotos un mecanismo para terminar sus sesiones interactivas con el TOE, y asegurando que las sesiones que han estado inactivas durante un período de tiempo, configurable por un usuario administrador del TOE, sean terminadas por el TOE.

T.UNAUTHORIZED_ACCESS
Un atacante puede acceder al TOE sin estar autorizado y sin ser detectado.

Esta amenaza es contrarrestada por los siguientes objetivos de seguridad:

- O.LOG – gestiona esta amenaza asegurando que el TOE genera registros de auditoría de eventos relevantes para la seguridad y estos pueden ser consultados por usuarios administradores del TOE.
- O.IDENTIFY_AUTHENTICITY – gestiona esta amenaza asegurando que todos los usuarios remotos estén identificados y autenticados previamente a la obtención de acceso al TOE y a los servicios del TOE.
- O.ROLE – gestiona esta amenaza proporcionando un mecanismo que requiere que los usuarios remotos tengan los privilegios adecuados para realizar acciones en el TOE.
- OE.DBAUTH – satisface este objetivo suponiendo la garantía de que los usuarios de base de datos, estén previamente identificados y autenticados con permisos suficientes y necesarios antes de realizar cualquier actividad con la base de datos.

- OE.OSAUTH – satisface este objetivo suponiendo la garantía de que los usuarios del sistema operativo, estén previamente identificados y autenticados con permisos suficientes y necesarios antes de poder operar con la máquina en la que se ejecuta el TOE.

T.UNAUTHORIZED_ACTIVITY
Los usuarios del TOE realizan acciones no autorizadas en el TOE.

Esta amenaza es contrarrestada por los siguientes objetivos de seguridad:

- O.LOG – gestiona esta amenaza asegurando que el TOE genere registros de auditoría de eventos relevantes para la seguridad y estos pueden ser consultados por usuarios administradores del TOE.
- O.LOG_REVIEW – gestiona esta amenaza asegurando que el TOE proporciona capacidades para la revisión de los registros de auditoría almacenados.
- O.ROLE – gestiona esta amenaza proporcionando un mecanismo que requiere que los usuarios remotos tengan los privilegios adecuados para realizar acciones en el TOE.
- OE.ADMIN_TRUST – satisface el objetivo suponiendo la garantía de que los usuarios administradores del TOE, estén debidamente capacitados para administrar el TOE y son confiables.
- OE.OS_USER_TRUST – satisface el objetivo suponiendo la garantía de que los usuarios del sistema operativo pertenecen a personal administrador del TOE, los cuales están debidamente capacitados para realizar sus tareas y son confiables.
- OE.BAST – satisface el objetivo suponiendo la garantía de que el sistema operativo de cada componente del TOE, proteja el componente y su configuración ante acceso no autorizado.

T.UNDETECTED_THREATS
Situaciones de uso indebido, no autorizado o actividad maliciosa no detectables sin hacer uso de técnicas de correlación en tiempo real.

Esta amenaza es contrarrestada por los siguientes objetivos de seguridad:

- O.SIEM_COLLECT – gestiona esta amenaza asegurando que el TOE proporciona mecanismos de captura de eventos de seguridad y líneas de logs desde los sistemas cedentes de la organización y del propio TOE (datos SIEM).
- O.SIEM_ALERT – se soporta a partir de O.SIEM_COLLECT para la gestión de esta amenaza asegurando que el TOE proporciona mecanismos para generar alertas ante la detección de actividades sospechosas. Dicha detección se obtiene al aplicar técnicas de correlación en tiempo real sobre los eventos de seguridad recibidos.

A.IDENTIFICATION_&_AUTHENTICATION
El entorno IT será capaz de identificar y autenticar a los usuarios del sistema operativo y a los usuarios de la base de datos.

Este supuesto es satisfecho con el siguiente objetivo de seguridad:

- OE.DBAUTH – satisface este objetivo suponiendo la garantía de que los usuarios de base de datos, estén previamente identificados y autenticados con permisos suficientes y necesarios antes de realizar cualquier actividad con la base de datos.
- OE.OSAUTH – satisface este objetivo suponiendo la garantía de que los usuarios del sistema operativo, estén previamente identificados y autenticados con permisos suficientes y necesarios antes de poder operar con la máquina en la que se ejecuta el TOE.

A.DBINTEGRITY
La base de datos del entorno operacional del TOE mantendrá la integridad de los datos almacenados.

Este supuesto es satisfecho con el siguiente objetivo de seguridad:
- OE.DBINT – satisface este objetivo suponiendo la garantía de la integridad de los datos almacenados en la base de datos: parámetros, líneas de logs y eventos de seguridad.

A.INSTALLATION
El sistema operativo y la base de datos del entorno operacional del TOE estarán securizados.

Este supuesto es satisfecho con los siguientes objetivos de seguridad:
- OE.BAST – satisface el objetivo suponiendo la garantía de que el sistema operativo y base de datos de cada componente del TOE protege el componente y su configuración ante acceso no autorizado.
- OE.DBAUTH – satisface este objetivo suponiendo la garantía de que los usuarios de base de datos, estén previamente identificados y autenticados con permisos suficientes y necesarios antes de realizar cualquier actividad con la base de datos.
- OE.OSAUTH – satisface este objetivo suponiendo la garantía de que los usuarios del sistema operativo, estén previamente identificados y autenticados con permisos suficientes y necesarios antes de poder operar con la máquina en la que se ejecuta el TOE.

A.PROTECT
El entorno operacional del TOE mantendrá un entorno físico confiable.

Este supuesto es satisfecho con el siguiente objetivo de seguridad:
- OE.PHYSICAL – satisface el objetivo suponiendo la garantía de que el TOE y el entorno operacional del TOE está protegido contra ataques físicos.

A.TIME
El sistema operativo del entorno operacional del TOE proporcionará una base de tiempo confiable.

Este supuesto es satisfecho con el siguiente objetivo de seguridad:
- OE.TIME – satisface el objetivo suponiendo la garantía de que el entorno operacional del TOE pueda proporcionar a los componentes del TOE una fuente

de tiempo confiable que se pueda usar para generar marcado de tiempo para su inclusión en los registros de auditoría generados.

A.NO_EVIL_ADMIN
Los administradores debidamente autorizados serán confiables y no realizarán acciones maliciosas, además estarán debidamente formados para usar, configurar y mantener el TOE.

Este supuesto es satisfecho con el siguiente objetivo de seguridad:

- OE.ADMIN_TRUST – satisface el objetivo suponiendo la garantía de que los usuarios administradores del TOE, estén debidamente capacitados para administrar el TOE y son confiables.

A.OS_USER
El acceso al sistema operativo donde se ejecuta el TOE, efectuado mediante el uso de usuarios del sistema operativo, solo será realizado por personal administrador del TOE.

Este supuesto es satisfecho con el siguiente objetivo de seguridad:

- OE.OS_USER_TRUST – satisface el objetivo suponiendo la garantía de que los usuarios del sistema operativo pertenecen a personal administrador del TOE, los cuales están debidamente capacitados para realizar sus tareas y son confiables.

5. Security Requirements

5.1 Security functional requirements

Dentro de la presente sección, se ponen de manifiesto los requisitos funcionales de seguridad que el TOE posee para hacer frente a las potenciales amenazas a las que se ve expuesto. Estos requisitos han sido extraídos de la parte 2 de CC v3.1r5.

CLASE	NOMBRE	REQUISITO	NOMBRE
FAU	SECURITY AUDIT	FAU_ARP.1	Security alarms
		FAU_SAA.1	Potential violation analysis
		FAU_GEN.1	Audit data generation
		FAU_SAR.1	Audit review
		FAU_SAR.2	Restricted audit review
		FAU_SAR.3	Selectable audit review
		FAU_STG.2	Guarantees of audit data availability
		FAU_STG.3	Action in case of possible audit data loss
		FAU_STG.4	Prevention of audit data loss
FCS	CRYPTOGRAPHIC SUPPORT	FCS_CKM.1	Cryptographic key generation
		FCS_CKM.4	Cryptographic key destruction
		FCS_COP.1	Cryptographic operation
FIA	IDENTIFICATION AND AUTHENTICATION	FIA_AFL.1	Authentication failure handling
		FIA_ATD.1	User attribute definition

CLASE	NOMBRE	REQUISITO	NOMBRE
		FIA_SOS.1	Verification of secrets
		FIA_UAU.1	Timing of authentication
		FIA_UAU.6	Re-authenticating
		FIA_UID.1	Timing of identification
FMT	SECURITY MANAGEMENT	FMT_MOF.1	Management of security functions behaviour
		FMT_MTD.1	Management of TSF data
		FMT_SMF.1	Specification of Management Functions
		FMT_SMR.1	Security roles
FTA	TOE ACCESS	FTA_SSL.3	TSF-initiated termination
		FTA_SSL.4	User-initiated termination
FTP	TRUSTED PATH/CHANNELS	FTP_TRP.1	Trusted path

TABLA 2: SECURITY FUNCTIONAL REQUIREMENTS

5.1.1 Security audit (FAU)

FAU_ARP.1 Security alarms

- FAU_ARP.1.1 The TSF shall take [*the generation of alarms (security events) and the notification by email to configurable receivers*] upon detection of a potential security violation.

FAU_SAA.1 Potential violation analysis

- FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

- FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:
  a) Accumulation or combination of [*security events*] known to indicate a potential security violation;
  b) [*none*].

FAU_GEN.1 (1) Audit data generation

- FAU_GEN.1.1(1) The TSF shall be able to generate an audit record of the following auditable events **generated in the Real time streaming and processing bus subsystem**:
  a) Start-up and shutdown of the audit functions;
  b) All auditable events for the [not specified] level of audit; and
  c) [*authentication mechanism,*
  reception of SIEM data.
  ].

- FAU_GEN.1.2 (1) The TSF shall record within each audit record **generated in the Real time streaming and processing bus subsystem** at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*none*].

Application note:
Table 2 shows the SIEM data audit record detail:

	DATE AND TIME	TYPE	SUBJECT	OUTCOME
LOG LINE	*Date and time of the transferring system and date and time inside the TOE*	*Syslog header*	*Originating host (hostname or IP)*	*Contained in the message description, if not explicity specified is success*
SECURITY EVENT	*Date and time of the transferring system and date and time inside the TOE*	*Categorized type of the event by the TOE*	*Originating host (hostname or IP)*	*Contained in the message description, if not explicity specified is success*

TABLA 3 : SIEM DATA AUDIT RECORD

FAU_GEN.1 (2) Audit data generation

- FAU_GEN.1.1(2) The TSF shall be able to generate an audit record of the following auditable events **generated in the Front-end servers subsystem**:
  a) Start-up and shutdown of the audit functions;
  b) All auditable events for the [not specified] level of audit; and
  c) [*identification mechanism,*
  authentication mechanism,
  TSF data and TSF functions management,
  termination of an inactive user session by the TSF,
  80%, 90% and 100% threshold consumed in the size of memory space reserved for audit records,
  modification in the size of reserved memory for audit records.
  ].

- FAU_GEN.1.2 (2) The TSF shall record within each audit record **generated in the Front-End servers subsystem** at least the following information:
  a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
  b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*none*].

FAU_SAR.1 (1) Audit review

- FAU_SAR.1.1 (1) The TSF shall provide [*front end users assigned with a role with the access sections admin/cep (or view/cep) and admin/loghost (or view/cep), and authorized access to event security queues and file/query patterns*] with the capability to read [*SIEM data*] from the audit records **generated in the Real time streaming and processing bus subsystem**.

- FAU_SAR.1.2 (1) The TSF shall provide the audit records **of SIEM data generated in the Real time streaming and processing bus subsystem** in a manner suitable for the user to interpret the information.

FAU_SAR.1 (2) Audit review

- FAU_SAR.1.1 (2) The TSF shall provide [*front end users assigned with a role with the access section view/audit*] with the capability to read [all *audit information*] from the audit records **generated in the Front-end servers subsystem**.

- FAU_SAR.1.2 (2) The TSF shall provide the audit records **generated in the Front end servers subsystem** in a manner suitable for the user to interpret the information.

FAU_SAR.2 (1) Restricted audit review

- FAU_SAR.2.1 (1) The TSF shall prohibit all users read access to the audit records **of SIEM data generated in the Real time streaming and processing bus subsystem** except those users that have been granted explicit read-access.

FAU_SAR.2 (2) Restricted audit review

- FAU_SAR.2.1 (2) The TSF shall prohibit all users read access to the audit records **generated in the Front-end servers subsystem** except those users that have been granted explicit read-access.

FAU_SAR.3 (1) Selectable audit review

- FAU_SAR.3.1 (1) The TSF shall provide the ability to apply [*selection and ordering*] of audit data **of SIEM data generated in the Real time streaming and processing bus subsystem** based on [*selection based on date and time range and, optionally, subject identity and outcome (success or failure); ordering based on date and time, subject identity, or type of event.*
  ].

FAU_SAR.3 (2) Selectable audit review

- FAU_SAR.3.1 (2) The TSF shall provide the ability to apply [*selection and ordering*] of audit data **generated in the Front-end servers subsystem** based on [*selection based on date and time range and, optionally, subject identity and outcome (success or failure); ordering based on date and time, subject identity, or type of event.*
  ].

FAU_STG.2 (1) Guarantees of audit data availability

- FAU_STG.2.1(1) The TSF shall protect the stored audit records **generated in the Real time streaming and processing bus subsystem** in the audit trail from unauthorised deletion.

- FAU_STG.2.2 (1) The TSF shall be able to [prevent] unauthorised modifications to the stored audit records **generated in the Real time streaming and processing bus subsystem** in the audit trail.

- FAU_STG.2.3 (1) The TSF shall ensure that [*as specified in Table 3*] stored audit records **generated in the Real time streaming and processing bus subsystem** will be maintained when the following conditions occur: [audit storage exhaustion].

	THRESHOLD MECHANISM
SIEM DATA	*up to a configurable maximum number of days*
REST OF EVENTS	*up to a configurable maximum number of files*

TABLA 4 : MAXIMUM THRESHOLD – REAL TIME STREAMING AND PROCESSING BUS SUBSYSTEM AUDIT RECORDS

FAU_STG.2 (2) Guarantees of audit data availability

- FAU_STG.2.1(2) The TSF shall protect the stored audit records **generated in the Front-End servers subsystem** in the audit trail from unauthorised deletion.

- FAU_STG.2.2 (2) The TSF shall be able to [prevent] unauthorised modifications to the stored audit records **generated in the Front-End servers subsystem** in the audit trail.

- FAU_STG.2.3 (2) The TSF shall ensure that [*up to a configurable maximun number of*] stored audit records **generated in the Front-End servers subsystem** will be maintained when the following conditions occur: [audit storage exhaustion].

FAU_STG.3 Action in case of possible audit data loss

- FAU_STG.3.1 The TSF, **on the Front-end servers subsystem**, shall [*generate audit records in case of approaching and overcome trail threshold – 80%, 90% and 100%* -] if the audit trail exceeds [*50000000 records – by default*].

FAU_STG.4 Prevention of audit data loss

- FAU_STG.4.1 The TSF shall [overwrite the oldest stored audit records] and [*the TSF shall generate an audit record informing that the trail threshold is overcome*] if the audit trail is full.

5.1.2 Cryptographic key support (FCS)

FCS_CKM.1 Cryptographic key generation

- FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*cryptographic key generation methods supported by TLS 1.2*] and specified cryptographic key sizes [*key sizes supported by TLS 1.2*] that meet the following: [*none*].

  Application note: Specifically AES key generation with 128/256 bits key size.

FCS_CKM.4 Cryptographic key destruction

- FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*cryptographic key destruction methods supported by TLS 1.2*] that meets the following: [*none*].

  Application note: Specifically AES key destruction with 128/256 bits key size.

FCS_COP.1 (1) Cryptographic operation

- FCS_COP.1.1 (1) The TSF shall perform [*encryption/decryption*] in accordance with a specified cryptographic algorithm [*as specified in Table 4*] and cryptographic key sizes [*as specified in Table 4*] that meet the following: [*as specified in Table 4*].

ALGORITHM	KEY SIZE	RFC	FUNCTION
AES (simetric)	*128/256*	*4615*	*TLS 1.2 session-specific shared key*
	128	*4615*	*Passwords storage*
RSA (asimetric)	*3072*	*8017*	*TLS 1.2 handshake*

TABLA 5 : CRIPTOGRAPHY

Application note: The TOE uses RSA and AES in establishing TLS 1.2 session and AES in storing passwords in the front end servers subsystem configuration file.

FCS_COP.1 (2) Cryptographic operation

- FCS_COP.1.1 (2) The TSF shall perform [*hash operations*] in accordance with a specified cryptographic algorithm [*SHA3*] and cryptographic key sizes [*none*] that meet the following: [*FIPS 202*].

Application note: The TOE uses SHA3 in storing remote users passwords.

5.1.3 Identification and authentication (FIA)

FIA_AFL.1 Authentication failure handling

- FIA_AFL.1.1 The TSF shall detect when [an administrator configurable positive integer within [*3 to 5*]] unsuccessful authentication attempts occur related to [*user authentication*].

- FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*disable the user account until a configurable user account blocking time has been reached. By default: three minutes*].

FIA_ATD.1 (1) User attribute definition

- FIA_ATD.1.1 (1) The TSF shall maintain, **on the Real time streaming and processing bus subsystem – endpoint that receives log lines**, the following list of security attributes belonging to individual users: [*Trusted CA*].

FIA_ATD.1 (2) User attribute definition

- FIA_ATD.1.1 (2) The TSF shall maintain, **on the Real time streaming and processing bus subsystem – endpoint that receives security events**, the following list of security attributes belonging to individual users: [*user identity and password*].

FIA_ATD.1 (3) User attribute definition

- FIA_ATD.1.1 (3) The TSF shall maintain, **on the Front End Servers subsystem**, the following list of security attributes belonging to individual users: [*user identity, password, assigned roles with – access sections, queues, queue/file patterns, actions – and email address*].

FIA_SOS.1 (1) Verification of secrets

- FIA_SOS.1.1 (1) The TSF shall provide a mechanism to verify, **on the Real time streaming and processing bus subsystem – endpoint that receives security events,** that secrets meet [*a single policy with a minimum of twelve characters with: at least two non-alphanumeric characters, at least two numeric characters and at least two uppercase characters*].

FIA_SOS.1 (2) Verification of secrets

- FIA_SOS.1.1 (2) The TSF shall provide a mechanism to verify, **on the Front-end servers subsystem,** that secrets meet [*restrictions on the structure of the password, policies based on: a minimum number of characters and the inclusion of character types (uppercase, lowercase, numeric and alphanumeric). By default: twelve characters long and the inclusion of uppercase, lowercase and numeric characters*].

FIA_UAU.1 Timing of authentication

- FIA_UAU.1.1 The TSF shall allow [*public front end services: validation-by-email and security-type*] on behalf of the user to be performed before the user is authenticated.
- FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.6 (1) Re-authenticating

- FIA_UAU.6.1 (1) The TSF shall re-authenticate, **on the Real time streaming and processing bus subsystem,** the user under the conditions [*inactivity user session time has elapsed*].

FIA_UAU.6 (2) Re-authenticating

- FIA_UAU.6.1 (2) The TSF shall re-authenticate, **on the Front End Servers subsystem,** the user under the conditions [*user changes own password, inactivity user session time has elapsed*].

FIA_UID.1 Timing of identification

- FIA_UID.1.1 The TSF shall allow [*public front end services: validation-by-email and security-type*] on behalf of the user to be performed before the user is identified.
- FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.4 Security management (FMT)

FMT_MOF.1 Management of security functions behaviour

- FMT_MOF.1.1 The TSF shall restrict, **on the Front End Servers subsystem,** the ability to [determine the behaviour of, modify the behaviour of] the functions [*security policies about password restrictions and unsuccessful authentication attempts*] to [*super root and user defined roles*].

Application note: Specifically user defined roles with admin/security access section.

FMT_MTD.1 Management of TSF data

- FMT_MTD.1.1 The TSF shall restrict, **on the Front End Servers subsystem,** the ability to [query, modify, delete, [*create*]] the [*queues to control access to security events, log queries and log file patterns to control access to log lines and actions to be performed on security events or log lines*] to [*super root and user defined roles*].

  Application note: Specifically user defined roles with admin/cep and admin/loghost access sections.

FMT_SMF.1 Specification of Management Functions

- FMT_SMF.1.1 The TSF shall be capable of performing, **on the Front End Servers subsystem,** the following management functions: [*management of: front end users, roles, syslog entry configurations, correlation rules, response/notification upon correlation rules triggering; assignment of – access sections, file patterns, queries, queues and actions – to roles and front end users to roles*].

FMT_SMR.1 (1) Security roles

- FMT_SMR.1.1 (1) The TSF shall maintain, **on the Real time streaming and processing bus subsystem,** the roles *[information sender]*.

  Application note: The Real time streaming and processing bus subsystem has a single role to transmit information, which is defined as information sender.

- FMT_SMR.1.2 (1) The TSF shall be able to associate users with roles **on the Real time streaming and processing bus subsystem**.

FMT_SMR.1 (2) Security roles

- FMT_SMR.1.1 (2) The TSF shall maintain, **on the Front End Servers subsystem,** the roles [*super root and user defined roles*].

- FMT_SMR.1.2 (2) The TSF shall be able to associate users with roles **on the Front End Servers subsystem**.

5.1.5 Access of the TSF (FTA)

FTA_SSL.3 TSF-initiated termination

- FTA_SSL.3.1 The TSF shall terminate an interactive session after a [*time interval of user session inactivity, configurable parameter*].

FTA_SSL.4 User-initiated termination

- FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

5.1.6 Trusted path (FTP)

FTP_TRP.1 Trusted path

- FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

- FTP_TRP.1.2 The TSF shall permit [remote users] to initiate communication via the trusted path.

- FTP_TRP.1.3 The TSF shall require the use of the trusted path for [initial user authentication, [*all remote actions]*].

5.2 Security assurance requirements

Los requisitos de garantía de seguridad descritos en la presente sección de la Declaración de Seguridad, se ajustan al Paquete de requisitos de Garantía EAL2 especificado en la Parte 3 de la norma CC v3.1r5.

Se ha elegido este conjunto de requisitos de garantía porque supone un primer paso, necesario para evolucionar a niveles de certificación superiores y que permite conocer el impacto sobre la empresa y el producto.

En la siguiente tabla están incluidos los requisitos de garantía de seguridad citados:

CLASE	NOMBRE	COMPONENTE	NOMBRE
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	Operational user guidance
		AGD_PRE.1	Preparative procedures
ALC	Life-Cycle support	ALC_CMC.2	Use of a CM system
		ALC_CMS.2	Parts of the TOE CM coverage
		ALC_DEL.1	Delivery procedures
ASE	Security Target Evaluation	ASE_CCL.1	Conformance claims
		ASE_ECD.1	Extended components definition
		ASE_INT.1	ST introduction
		ASE_OBJ.2	Security objectives
		ASE_REQ.2	Derived security requirements
		ASE_SPD.1	Security 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 – sample
AVA	Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

TABLA 6: SECURITY ASSURANCE REQUIREMENTS

5.2.1 Development (ADV)

ADV_ARC.1 – Security architecture description

- ADV_ARC.1.1D – The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.
- ADV_ARC.1.2D – The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

- ADV_ARC.1.3D – The developer shall provide a security architecture description of the TSF.
- ADV_ARC.1.1C – The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.
- ADV_ARC.1.2C – The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.
- ADV_ARC.1.3C – The security architecture description shall describe how the TSF implementation process is secure.
- ADV_ARC.1.4C – The security architecture description shall demonstrate that the TSF protects itself from tampering.
- ADV_ARC.1.5C – The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.
- ADV_ARC.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2 – Security-enforcing functional specification

- ADV_FSP.2.1D – The developer shall provide a functional specification.
- ADV_FSP.2.2D – The developer shall provide a tracing from the functional specification to the SFRs.
- ADV_FSP.2.1C – The functional specification shall completely represent the TSF.
- ADV_FSP.2.2C – The functional specification shall describe the purpose and method of use for all TSFI.
- ADV_FSP.2.3C – The functional specification shall identify and describe all parameters associated with each TSFI.
- ADV_FSP.2.4C – For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.
- ADV_FSP.2.5C – For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.
- ADV_FSP.2.6C – The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
- ADV_FSP.2.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- ADV_FSP.2.2E – The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

ADV_TDS.1 – Basic design

- ADV_TDS.1.1D – The developer shall provide the design of the TOE.
- ADV_TDS.1.2D – The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.
- ADV_TDS.1.1C – The design shall describe the structure of the TOE in terms of subsystems.
- ADV_TDS.1.2C – The design shall identify all subsystems of the TSF.
- ADV_TDS.1.3C – The design shall provide the behaviour summary of each SFR-supporting or SFR-non-interfering TSF subsystem.

- ADV_TDS.1.4C – The design shall summarise the SFR-enforcing behaviour of the SFR-enforcing subsystems.
- ADV_TDS.1.5C – The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.
- ADV_TDS.1.6C – The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.
- ADV_TDS.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- ADV_TDS.1.2E – The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.2.2 Guidance documents (AGD)

AGD_OPE.1 – Operational user guidance

- AGD_OPE.1.1D – The developer shall provide operational user guidance.
- AGD_OPE.1.1C – The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
- AGD_OPE.1.2C – The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
- AGD_OPE.1.3C – The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
- AGD_OPE.1.4C – The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
- AGD_OPE.1.5C – The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
- AGD_OPE.1.6C – The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.
- AGD_OPE.1.7C – The operational user guidance shall be clear and reasonable.
- AGD_OPE.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1 – Preparative procedures

- AGD_PRE.1.1D – The developer shall provide the TOE including its preparative procedures.
- AGD_PRE.1.1C – The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.
- AGD_PRE.1.2C – The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

- AGD_PRE.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- AGD_PRE.1.2E – The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-Cycle support (ALC)

ALC_CMC.2 – Use of a CM system

- ALC_CMC.2.1D – The developer shall provide the TOE and a reference for the TOE.
- ALC_CMC.2.2D – The developer shall provide the CM documentation.
- ALC_CMC.2.3D – The developer shall use a CM system.
- ALC_CMC.2.1C – The TOE shall be labelled with its unique reference.
- ALC_CMC.2.2C – The CM documentation shall describe the method used to uniquely identify the configuration items.
- ALC_CMC.2.3C – The CM system shall uniquely identify all configuration items.
- ALC_CMC.2.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_CMS.2 – Parts of the TOE CM coverage

- ALC_CMS.2.1D – The developer shall provide a configuration list for the TOE.
- ALC_CMS.2.1C – The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.
- ALC_CMS.2.2C – The configuration list shall uniquely identify the configuration items.
- ALC_CMS.2.3C – For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.
- ALC_CMS.2.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DEL.1 – Delivery procedures

- ALC_DEL.1.1D – The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.
- ALC_DEL.1.2D – The developer shall use the delivery procedures.
- ALC_DEL.1.1C – The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.
- ALC_DEL.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Security Target Evaluation (ASE)

ASE_CCL.1 – Conformance claims

- ASE_CCL.1.1D – The developer shall provide a conformance claim.
- ASE_CCL.1.2D – The developer shall provide a conformance claim rationale.
- ASE_CCL.1.1C – The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.
- ASE_CCL.1.2C – The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

- ASE_CCL.1.3C – The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.
- ASE_CCL.1.4C – The CC conformance claim shall be consistent with the extended components definition.
- ASE_CCL.1.5C – The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.
- ASE_CCL.1.6C – The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.
- ASE_CCL.1.7C – The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.
- ASE_CCL.1.8C – The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.
- ASE_CCL.1.9C – The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.
- ASE_CCL.1.10C – The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.
- ASE_CCL.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1 – Extended components definition

- ASE_ECD.1.1D – The developer shall provide a statement of security requirements.
- ASE_ECD.1.2D – The developer shall provide an extended components definition.
- ASE_ECD.1.1C – The statement of security requirements shall identify all extended security requirements.
- ASE_ECD.1.2C – The extended components definition shall define an extended component for each extended security requirement.
- ASE_ECD.1.3C – The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.
- ASE_ECD.1.4C – The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.
- ASE_ECD.1.5C – The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.
- ASE_ECD.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- ASE_ECD.1.2E – The evaluator shall confirm that no extended component can be clearly expressed using existing components.

ASE_INT.1 – ST introduction

- ASE_INT.1.1D – The developer shall provide an ST introduction.
- ASE_INT.1.1C – The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

- ASE_INT.1.2C – The ST reference shall uniquely identify the ST.
- ASE_INT.1.3C – The TOE reference shall uniquely identify the TOE.
- ASE_INT.1.4C – The TOE overview shall summarise the usage and major security features of the TOE.
- ASE_INT.1.5C – The TOE overview shall identify the TOE type.
- ASE_INT.1.6C – The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.
- ASE_INT.1.7C – The TOE description shall describe the physical scope of the TOE.
- ASE_INT.1.8C – The TOE description shall describe the logical scope of the TOE.
- ASE_INT.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- ASE_INT.1.2E – The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_OBJ.2 – Security objectives

- ASE_OBJ.2.1D – The developer shall provide a statement of security objectives.
- ASE_OBJ.2.2D – The developer shall provide a security objectives rationale.
- ASE_OBJ.2.1C – The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.
- ASE_OBJ.2.2C – The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.
- ASE_OBJ.2.3C – The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.
- ASE_OBJ.2.4C – The security objectives rationale shall demonstrate that the security objectives counter all threats.
- ASE_OBJ.2.5C – The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.
- ASE_OBJ.2.6C – The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.
- ASE_OBJ.2.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_REQ.2 – Derived security requirements

- ASE_REQ.2.1D – The developer shall provide a statement of security requirements.
- ASE_REQ.2.2D – The developer shall provide a security requirements rationale.
- ASE_REQ.2.1C – The statement of security requirements shall describe the SFRs and the SARs.
- ASE_REQ.2.2C – All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.
- ASE_REQ.2.3C – The statement of security requirements shall identify all operations on the security requirements.
- ASE_REQ.2.4C – All operations shall be performed correctly.

- ASE_REQ.2.5C – Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.
- ASE_REQ.2.6C – The security requirements rationale shall trace each SFR back to the security objectives for the TOE.
- ASE_REQ.2.7C – The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.
- ASE_REQ.2.8C – The security requirements rationale shall explain why the SARs were chosen.
- ASE_REQ.2.9C – The statement of security requirements shall be internally consistent.
- ASE_REQ.2.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_SPD.1 – Security problem definition

- ASE_SPD.1.1D – The developer shall provide a security problem definition.
- ASE_SPD.1.1C – The security problem definition shall describe the threats.
- ASE_SPD.1.2C – All threats shall be described in terms of a threat agent, an asset, and an adverse action.
- ASE_SPD.1.3C – The security problem definition shall describe the OSPs.
- ASE_SPD.1.4C – The security problem definition shall describe the assumptions about the operational environment of the TOE.
- ASE_SPD.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1 – TOE Summary specification

- ASE_TSS.1.1D – The developer shall provide a TOE summary specification.
- ASE_TSS.1.1C – The TOE summary specification shall describe how the TOE meets each SFR.
- ASE_TSS.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- ASE_TSS.1.2E – The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

5.2.5 Test (ATE)

ATE_COV.1 – Evidence of coverage

- ATE_COV.1.1D – The developer shall provide evidence of the test coverage.
- ATE_COV.1.1C – The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.
- ATE_COV.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 – Functional testing

- ATE_FUN.1.1D – The developer shall test the TSF and document the results.
- ATE_FUN.1.2D – The developer shall provide test documentation.

- ATE_FUN.1.1C – The test documentation shall consist of test plans, expected test results and actual test results.
- ATE_FUN.1.2C – The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.
- ATE_FUN.1.3C – The expected test results shall show the anticipated outputs from a successful execution of the tests.
- ATE_FUN.1.4C – The actual test results shall be consistent with the expected test results.
- ATE_FUN.1.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 – Independent testing

- ATE_IND.2.1D – The developer shall provide the TOE for testing.
- ATE_IND.2.1C – The TOE shall be suitable for testing.
- ATE_IND.2.2C – The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
- ATE_IND.2.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.6 Vulnerability Assessment (AVA)

AVA_VAN.2 – Vulnerability analysis

- AVA_VAN.2.1D – The developer shall provide the TOE for testing.
- AVA_VAN.2.1C – The TOE shall be suitable for testing.
- AVA_VAN.2.1E – The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- AVA_VAN.2.2E – The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
- AVA_VAN.2.3E – The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.
- AVA_VAN.2.4E – The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

5.3 Security requirements rationale

5.3.1 Security functional requirement rationale

Esta sección relaciona todos los requisitos funcionales de seguridad identificados y su relación con cada objetivo de seguridad que se pretende cumplir.

SECURITY FUNCTIONAL REQUIREMENTS RATIONALE	SECURITY OBJECTIVES											
	O.LOG	O.LOG_REVIEW	O.LOG_STORAGE	O.LOGIN_ATTEMPTS	O.IDENTIFY_AUTHENTICITY	O.PASSWORD_POLICY	O.PASSWORD_PROTECT	O.ROLE	O.SECURECOM	O.SESSION_LOGOUT	O.SIEM_COLLECT	O.SIEM_ALERT
FAU_ARP.1												X
FAU_SAA.1												X
FAU_GEN.1 (1)	X										X	
FAU_GEN.1 (2)	X											
FAU_SAR.1 (1) FAU_SAR.1 (2)		X										
FAU_SAR.2 (1) FAU_SAR.2 (2)		X										
FAU_SAR.3 (1) FAU_SAR.3 (2)		X										
FAU_STG.2 (1) FAU_STG.2 (2)			X									
FAU_STG.3			X									
FAU_STG.4			X									
FCS_CKM.1									X			
FCS_CKM.4									X			
FCS_COP.1 (1)							X		X			
FCS_COP.1 (2)							X					
FIA_AFL.1				X								
FIA_ATD.1 (1) FIA_ATD.1 (2) FIA_ATD.1 (3)					X							
FIA_SOS.1 (1) FIA_SOS.1 (2)						X						
FIA_UAU.1					X							
FIA_UAU.6 (1) FIA_UAU.6 (2)					X							
FIA_UID.1					X							
FMT_MOF.1								X				
FMT_MTD.1								X				
FMT_SMF.1								X			X	X
FMT_SMR.1 (1) FMT_SMR.1 (2)								X				
FTA_SSL.3										X		
FTA_SSL.4										X		
FTP_TRP.1									X			

TABLA 7: SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

Security functional requirements rationale justifica que los requerimientos de seguridad, satisfacen todos los objetivos de seguridad del TOE.

O.LOG

El TOE debe proporcionar auditoría de actividad, por medio de la generación de registros de auditoría, de todos los accesos que se realizan en él, del resultado de los mismos, y de la actividad de componentes que lo constituyen, para que los usuarios administradores del TOE revisen los registros de auditoría generados.

Este objetivo se satisface por los siguientes requisitos de seguridad:

- FAU_GEN.1 (1) FAU_GEN.1 (2) – los registros de auditoría se generan para los tipos de eventos auditables relacionados con la actividad de accesos contra el TOE e 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 o fallido.

O.LOG_REVIEW
El TOE debe proporcionar un mecanismo de consulta de registros de auditoría a los usuarios administradores del TOE.

El objetivo se satisface por los siguientes requisitos de seguridad:

- FAU_SAR.1(1) FAU_SAR.1(2) - el TOE proporciona a los usuarios administradores del TOE la capacidad de leer la información de los registros de auditoría. Los registros de auditoría se muestran de manera adecuada para que el usuario autorizado interprete la información.
- FAU_SAR.2(1) FAU_SAR.2(2) - el TOE prohíbe a todos los usuarios del TOE el acceso de lectura a los registros de auditoría, excepto aquellos usuarios administradores del TOE a los que se les ha otorgado acceso de lectura explícito.
- FAU_SAR.3(1) FAU_SAR.3(2) - el TOE proporciona capacidades de seleccionar datos de auditoría para revisar según rangos de fecha y hora, y opcionalmente según la identidad del sujeto y el resultado, exitoso o fallido, del evento, y para ordenar los datos de auditoría seleccionados según la fecha y la hora, la identidad del sujeto o el tipo de evento.

O.LOG_STORAGE
El TOE debe proteger los registros de auditoría almacenados de modificaciones o eliminaciones no autorizadas.

Este objetivo se satisface por los siguientes requisitos de seguridad:

- FAU_STG.2 (1) FAU_STG.2 (2) - el TOE protege los registros de auditoría almacenados de modificaciones y eliminaciones no autorizadas, mientras que no se alcance el límite máximo establecido de almacenamiento.
- FAU_STG.3 – el TOE genera eventos de seguridad si se aproxima o supera los umbrales definidos con respecto al límite definido de registros de auditoría.
- FAU_STG.4 – el TOE sobrescribe los registros más antiguos de auditoría si se supera el umbral máximo de registros de auditoria.

O.LOGIN_ATTEMPTS
El TOE limitará el número de intentos de autenticación sin éxito consecutivos.

Este objetivo se satisface por los siguientes requisitos de seguridad:

- FIA_AFL.1 - el TOE es capaz de detectar cuándo se produce un número, configurable por un usuario administrador del TOE, de intentos fallidos de autenticación del usuario remoto. Cuando se ha alcanzado el número definido de intentos de autenticación sin éxito, el TOE bloquea la cuenta de usuario remoto temporalmente, tiempo también configurable por un usuario administrador del

TOE. Por defecto 3 intentos en un rango de 1 a 5 y un tiempo de bloqueo de tres minutos.

O.IDENTIFY_AUTHENTICITY
El TOE debe requerir que todos los usuarios remotos estén identificados y autenticados antes de obtener acceso a los servicios del TOE.

Este objetivo se satisface por los siguientes requisitos de seguridad:

- FIA_ATD.1 (1) FIA_ATD.1 (2) FIA_ATD.1 (3) - el TOE mantiene los siguientes atributos de seguridad asociados con cada usuario remoto: identidad del usuario, datos de autenticación, y adicionalmente, roles asignados, dirección de correo electrónico.
- FIA_UAU.1 - el TOE requiere que cada usuario remoto se autentique con éxito antes de permitir cualquier otra acción mediada por el TSF en nombre de ese usuario, excepto con los servicios públicos de front end.
- FIA_UAU.6 (1) FIA_UAU.6 (2) - el TOE requiere que el usuario remoto vuelva a autenticarse antes de permitir que el usuario cambie su propia contraseña o su sesión expire por inactividad.
- FIA_UID.1 - el TOE requiere que cada usuario remoto se identifique con éxito antes de permitir cualquier otra acción mediada por el TOE en nombre de ese usuario, excepto con los servicios públicos de front end.

O.PASSWORD_POLICY
El TOE debe proporcionar un mecanismo para reducir la probabilidad de que los usuarios remotos elijan contraseñas débiles.

Este objetivo se satisface por los siguientes requisitos de seguridad:

- FIA_SOS.1 (1) FIA_SOS.1 (2) - el TOE aplica políticas de contraseña que garantizan que todos los secretos asociados con las cuentas de usuario remoto se cumplen.

O.PASSWORD_PROTECT
El TOE debe proporcionar un mecanismo para proteger las contraseñas almacenadas.

Este objetivo se satisface por los siguientes requisitos de seguridad:

- FCS_COP.1 (1) FCS_COP.1 (2) - el TOE proporciona operaciones de encriptación y hash para el almacenado de contraseñas. La clave para operaciones de encriptación es accesible únicamente por los usuarios del sistema operativo.

O.ROLE
El TOE debe realizar control de acceso a recursos y objetos del propio TOE basándose en los atributos de los usuarios remotos: identificador, contraseña y roles que permitan segregar las funciones a las cuales tenga acceso cada usuario remoto.

Este objetivo se satisface por los siguientes requisitos de seguridad:

- FMT_MOF.1 - el TOE restringe la habilidad de determinar el comportamiento o, modificar el comportamiento de las funciones basadas en políticas de seguridad.

- FMT_MTD.1 - el TOE permite restringir la administración de los datos de TSF a los usuarios administradores del TOE que tienen asignados roles con secciones de autorización, que permiten la gestión de colas, patrones/consultas y acciones.
- FMT_SMF.1 - el TSF es capaz de ejecutar las siguientes funciones de gestión: roles, asignación de roles a – secciones de control, colas, consultas de líneas de logs, patrones de ficheros de líneas de logs y acciones -, usuarios de front end, asignación de roles a usuarios de front end, gestión de la configuración de syslog, asignación de colas a eventos de seguridad, activación de reglas de correlación, activación de respuestas - y notificaciones por correo electrónico -, debido a las respuestas de correlación.
- FMT_SMR.1 (1) – los usuarios del bus poseen un único rol para transmitir información.
- FMT_SMR.1 (2) - inicialmente usuario de front end administrador del TOE, super root, con capacidad de crear roles y usuarios de front end. Los roles son asignados a usuarios de front end.

O.SECURECOM
El TOE debe proteger las comunicaciones entre los usuarios remotos y el TOE.

Este objetivo se satisface por los siguientes requisitos de seguridad:
- FCS_CKM.1 – el TOE proporciona algoritmos de generación de claves soportados por TLS 1.2.
- FCS_CKM.4 – el TOE proporciona algoritmos de destrucción de claves soportados por TLS 1.2.
- FCS_COP.1 (1) - el TOE proporciona operaciones de encriptación durante el establecimiento de la sesión TLS 1.2.
- FTP_TRP.1 - el TOE proporciona una ruta de confianza para que los usuarios remotos se comuniquen con el TOE, la comunicación se encuentra protegida ante modificación y exposición. Toda acción frente al TOE requiere el empleo de una ruta de confianza.

O.SESSION_LOGOUT
El TOE debe proporcionar mecanismos para finalizar una sesión de usuario remoto después de un período de inactividad o a petición del usuario remoto.

Este objetivo se satisface por los siguientes requisitos de seguridad:
- FTA_SSL.3 - el TOE finaliza una sesión interactiva después de un intervalo de tiempo de inactividad.
- FTA_SSL.4 - el TOE permite al usuario remoto la terminación de su propia sesión interactiva.

O.SIEM_COLLECT
El TOE debe proporcionar mecanismos de captura de datos SIEM desde los sistemas cedentes y de la actividad del propio TOE.

Este objetivo se satisface por los siguientes requisitos de seguridad:
- FAU_GEN.1 (1) – los registros de auditoría se generan para todos los eventos relevantes relacionados con la seguridad e 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 o fallido.

- FMT_SMF.1 - el TSF es capaz de ejecutar las siguientes funciones de gestión: roles, asignación de roles a – secciones de control, colas, consultas de líneas de logs, patrones de ficheros de líneas de logs y acciones -, usuarios de front end, asignación de roles a usuarios de front end, gestión de la configuración de syslog, asignación de colas a eventos de seguridad, activación de reglas de correlación, activación de respuestas - y notificaciones por correo electrónico -, debido a las respuestas de correlación.

O.SIEM_ALERT
El TOE debe proporcionar mecanismos de generación de alertas ante potenciales amenazas de seguridad basadas en la correlación de los eventos de seguridad recibidos.

Este objetivo se satisface por los siguientes requisitos de seguridad:

- FAU_ARP.1 - ante potenciales riesgos de seguridad el TOE notifica mediante el envío de un correo electrónico a destinatarios previamente configurados.
- FAU_SAA.1 - el TOE aplica reglas de correlación en la monitorización de los registros de auditoría de datos SIEM, concretamente en los eventos de seguridad, para indicar una potencial violación en la seguridad en la aplicación de los requisitos de seguridad, SFRs.
- FMT_SMF.1 - el TSF es capaz de ejecutar las siguientes funciones de gestión: roles, asignación de roles a – secciones de control, colas, consultas de líneas de logs, patrones de ficheros de líneas de logs y acciones -, usuarios de front end, asignación de roles a usuarios de front end, gestión de la configuración de syslog, asignación de colas a eventos de seguridad, activación de reglas de correlación, activación de respuestas - y notificaciones por correo electrónico -, debido a las respuestas de correlación.

5.3.2 Functional requirement dependency rationale

La siguiente tabla identifica los SFRs requeridos en la ST, sus dependencias según se establece en Parte 2 Security functional components de CC, y cómo se satisface la dependencia en la ST. Todas las dependencias se han satisfecho mediante la inclusión en la ST de los SFRs dependientes.

REQUISITO	DEPENDENCIAS	SATISFECHO CON	NOTAS
FAU_ARP.1 Security alarms	FAU_SAA.1 Potential violation analysis	FAU_SAA.1 Potential violation analysis	
FAU_SAA.1 Potential violation analysis	FAU_GEN.1 Audit data generation	FAU_GEN.1 Audit data generation	
FAU_GEN.1 Audit data generation	FPT_STM.1 Reliable time stamps	OE.TIME	Esta dependencia no se cumple con un requisito functional de seguridad porque existe un objetivo de entorno operacional que se satisfice con la hipótesis de entorno A.TIME. Este objetivo de entorno operacional, OE.TIME, cumple lo requerido con la dependencia.

REQUISITO	DEPENDENCIAS	SATISFECHO CON	NOTAS
FAU_SAR.1 Audit review	FAU_GEN.1 Audit data generation	FAU_GEN.1 Audit data generation	
FAU_SAR.2 Restricted audit review	FAU_SAR.1 Audit review	FAU_SAR.1 Audit review	
FAU_SAR.3 Selectable audit review	FAU_SAR.1 Audit review	FAU_SAR.1 Audit review	
FAU_STG.2 Guarantees of audit data availability	FAU_GEN.1 Audit data generation	FAU_GEN.1 Audit data generation	
FAU_STG.3 Action in case of possible audit data loss	FAU_STG.1 Protected audit trail storage	FAU_STG.2 Guarantees of audit data availability	
FAU_STG.4 Prevention of audit data loss	FAU_STG.1 Protected audit trail storage	FAU_STG.2 Guarantees of audit data availability	
FCS_CKM.1 Cryptographic key generation	FCS_CKM.4 Cryptographic key destruction FCS_COP.1 Cryptographic operation	FCS_CKM.4 Cryptographic key destruction FCS_COP.1 Cryptographic operation	
FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1 Cryptographic key generation	FCS_CKM.1 Cryptographic key generation	
FCS_COP.1 Cryptographic operation	FCS_CKM.1 Cryptographic key generation FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1 Cryptographic key generation FCS_CKM.4 Cryptographic key destruction	En el algoritmo de clave asimétrica el TSF no está involucrado en la generación y la destrucción de la clave por lo que FCS_CKM.1 y FCS_CKM.4 no están incluidos. Las claves asimétricas son generadas por el fabricante del TOE, son distribuidas con el TOE, y no se destruyen, sino que expiran y deben ser actualizadas por el fabricante del TOE. La clave simétrica para el cifrado de contraseñas es generada por el fabricante, distribuida con el TOE, la clave no se destruye, por lo que para este tipo de operación no se ha indicado FCS_CKM.1 y FCS_CKM.4. El algoritmo de hash no requiere claves criptográficas, por lo que para este tipo de operación no se ha indicado FCS_CKM.1 y FCS_CKM.4
FIA_AFL.1 Authentication failure handling	FIA_UAU.1 Timing of authentication	FIA_UAU.1 Timing of authentication	
FIA_ATD.1 User attribute definition	NINGUNA	NINGUNA	
FIA_SOS.1 Verification of secrets	NINGUNA	NINGUNA	
FIA_UAU.1 Timing of authentication	FIA_UID.1 Timing of identification	FIA_UID.1 Timing of identification	
FIA_UAU.6 Re-authenticating	NINGUNA	NINGUNA	
FIA_UID.1 Timing of identification	NINGUNA	NINGUNA	
FMT_MOF.1 Management of security functions behaviour	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	
FMT_MTD.1 Management of TSF data	FMT_SMR.1 Security roles FMT_SMF.1 Specification of	FMT_SMR.1 Security roles FMT_SMF.1 Specification of	

REQUISITO	DEPENDENCIAS	SATISFECHO CON	NOTAS
	Management Functions	Management Functions	
FMT_SMF.1 Specification of Management Functions	NINGUNA	NINGUNA	
FMT_SMR.1 Security roles	FIA_UID.1 Timing of identification	FIA_UID.1 Timing of identification	
FTA_SSL.3 TSF-initiated termination	NINGUNA	NINGUNA	
FTA_SSL.4 User-initiated termination	NINGUNA	NINGUNA	
FTP_TRP.1 Trusted path	NINGUNA	NINGUNA	

TABLA 8: REQUIREMENT DEPENDENCY RATIONALE

5.3.3 Security assurance requirements rationale

Se ha seleccionado EAL 2 como el nivel de aseguramiento para el TOE al tratarse de producto comercial basado en solución software con requisitos de aseguramiento independiente de la seguridad con un nivel moderado, y el TOE ha sido diseñado para funcionamiento en un entorno físico de confianza.

REQUISITO	DEPENDENCIAS	SATISFECHO CON
ADV_ARC.1 Security architecture description	ADV_FSP.1 Basic functional specification ADV_TDS.1 Basic design	ADV_FSP.2 Security-enforcing functional specification ADV_TDS.1 Basic design
ADV_FSP.2 Security-enforcing functional specification	ADV_TDS.1 Basic design	ADV_TDS.1 Basic design
ADV_TDS.1 Basic design	ADV_FSP.2 Security-enforcing functional specification	ADV_FSP.2 Security-enforcing functional specification
AGD_OPE.1 Operational user guidance	ADV_FSP.1 Basic functional specification	ADV_FSP.2 Security-enforcing functional specification
AGD_PRE.1 Preparative procedures	NINGUNA	NINGUNA
ALC_CMC.2 Use of a CM system	ALC_CMS.1 TOE CM coverage	ALC_CMS.2 Parts of the TOE CM coverage
ALC_CMS.2 Parts of the TOE CM coverage	No dependencies	No dependencies
ALC_DEL.1 Delivery procedures	No dependencies	No dependencies
ASE_CCL.1 Conformance claims	ASE_INT.1 ST introduction ASE_ECD.1 Extended components definition ASE_REQ.1 Stated security requirements	ASE_INT.1 ST introduction ASE_ECD.1 Extended components definition ASE_REQ.2 Derived security requirements
ASE_ECD.1 Extended components definition	NINGUNA	NINGUNA
ASE_INT.1 ST introduction	NINGUNA	NINGUNA
ASE_OBJ.2 Security objectives	ASE_SPD.1 Security problem definition	ASE_SPD.1 Security problem definition
ASE_REQ.2 Derived security requirements	ASE_OBJ.2 Security objectives ASE_ECD.1 Extended components definition	ASE_OBJ.2 Security objectives ASE_ECD.1 Extended components definition
ASE_SPD.1 Security problem definition	NINGUNA	NINGUNA
ASE_TSS.1 TOE summary specification	ASE_INT.1 ST introduction ASE_REQ.1 Stated security requirements ADV_FSP.1 Basic functional specification	ASE_INT.1 ST introduction ASE_REQ.2 Derived security requirements ADV_FSP.2 Security-enforcing functional specification
ATE_COV.1 Evidence of coverage	ADV_FSP.2 Security-enforcing functional specification	ADV_FSP.2 Security-enforcing functional specification

REQUISITO	DEPENDENCIAS	SATISFECHO CON
	ATE_FUN.1 Functional testing	ATE_FUN.1 Functional testing
ATE_FUN.1 Functional testing	ATE_COV.1 Evidence of coverage	ATE_COV.1 Evidence of coverage
ATE_IND.2 Independent testing – sample	ADV_FSP.2 Security-enforcing functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures ATE_COV.1 Evidence of coverage ATE_FUN.1 Functional testing	ADV_FSP.2 Security-enforcing functional specification AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures ATE_COV.1 Evidence of coverage ATE_FUN.1 Functional testing
AVA_VAN.2 Vulnerability analysis	ADV_ARC.1 Security architecture description ADV_FSP.1 Basic functional specification ADV_TDS.1 Basic design AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures	ADV_ARC.1 Security architecture description ADV_FSP.2 Security-enforcing functional specification ADV_TDS.1 Basic design AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures

TABLA 9: SECURITY ASSURANCE REQUIREMENTS RATIONALE

6. TOE Summary specification

Esta sección describe las siguientes funciones de seguridad implementadas por el TOE, para satisfacer los SFR establecidos en el apartado 5.1

- Registros de auditoría
- Claves criptográficas
- Identificación y autenticación
- Gestión de la seguridad
- Protección del TSF
- Acceso al TOE
- Rutas de confianza

6.1 Registros de auditoría

Las funciones de auditoría satisfacen los siguientes requisitos funcionales de seguridad:

- FAU_ARP.1 - ante potenciales riesgos de seguridad el TOE genera alarmas (eventos de seguridad) y notifica mediante el envío de un correo electrónico a destinatarios previamente configurados, informando de la alarma generada.
- FAU_SAA.1 - el TOE aplica reglas de correlación en la monitorización de los registros de auditoría de datos SIEM, concretamente en los eventos de seguridad, para indicar una potencial violación en la seguridad en la aplicación de los requisitos de seguridad, SFRs.
- FAU_GEN.1 (1) FAU_GEN.1 (2) - los registros de auditoría se generan para todos los eventos relevantes relacionados con la seguridad e 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 o fallido.
- FAU_SAR.1 (1) - el TOE proporciona a los usuarios de front end administradores del TOE la capacidad de leer la información de los registros de auditoría de los datos SIEM del subsistema del bus de streaming y procesado en tiempo real. Los registros

de auditoría se muestran de manera adecuada para que el usuario de front end administrador del TOE interprete la información. El resto de registros de auditoría del subsistema del bus de streaming y procesado en tiempo real son accesibles por usuarios del sistema operativo.

- FAU_SAR.1 (2) - el TOE proporciona a los usuarios de front end administradores del TOE la capacidad de leer la información de los registros de auditoría del subsistema de servidores de front end. Los registros de auditoría se muestran de manera adecuada para que el usuario de front end administrador del TOE interprete la información.
- FAU_SAR.2 (1) - el TOE prohíbe a todos los usuarios de front end el acceso de lectura a los registros de auditoría de datos SIEM del subsistema del bus de streaming y procesado en tiempo real, excepto aquellos usuarios de front end administradores del TOE a los que se les ha otorgado acceso de lectura explícito. Usuarios de front end adminstradores del TOE con roles asignados que tengan las secciones de acceso admin/cep (o view/admin) y admin/loghost (o view/loghost). Además, el TOE requiere que el rol tenga autorización a acceder a la cola de clasificación, en el caso de eventos de seguridad, y la consulta/patrón de búsqueda, en el caso de líneas de log.
- FAU_SAR.2 (2) - el TOE prohíbe a todos los usuarios de front end el acceso de lectura a los registros de auditoría del subsistema de servidores de front end, excepto aquellos usuarios de front end administradores del TOE a los que se les ha otorgado acceso de lectura explícito. Usuarios de front end administradores del TOE que dispongan de un rol con la sección de acceso view/audit.
- FAU_SAR.3 (1) FAU_SAR.3 (2) - el TOE proporciona capacidades de seleccionar datos de auditoría para revisar según rangos de fecha y hora, y opcionalmente según la identidad del sujeto y el resultado, exitoso o fallido, del evento, y para ordenar los datos de auditoría seleccionados según la fecha y la hora, la identidad del sujeto o el tipo de evento, tanto para los registros de auditoría de datos SIEM del subsistema del bus de streaming y procesado en tiempo real como los registros de auditoría del subsistema de servidores de front end.
- FAU_STG.2 (1) FAU_STG.2 (1) - el TOE protege los registros de auditoría almacenados de modificaciones y eliminaciones no autorizadas, mientras que no se alcance el límite máximo establecido de almacenamiento.
- FAU_STG.3 - el TOE genera registros de auditoría si se aproxima o supera los umbrales definidos con respecto al límite definido de registros de auditoría.
- FAU_STG.4 - el TOE sobrescribe los registros más antiguos de auditoría si se supera el umbral máximo de registros de auditoria.

6.2 Claves criptográficas

Las funciones de criptografía satisfacen los siguientes requisitos funcionales de seguridad:

- FCS_CKM.1 – el TOE proporciona métodos de generación de clave AES 128/256 soportados por TLS 1.2.
- FCS_CKM.4 – el TOE proporciona métodos de destrucción de clave AES 128/256 soportados por TLS 1.2.

- FCS_COP.1 (1) FCS_COP.1 (2) - el TOE proporciona operaciones de cifrado, para almacenar contraseñas y establecer sesión TLS 1.2, y hash, para almacenar contraseñas.

6.3 Identificación y autenticación

Las funciones de identificación y autenticación satisfacen los siguientes requisitos funcionales de seguridad:

- FIA_AFL.1 - el TOE es capaz de detectar cuándo se produce un número, configurable por un usuario administrador del TOE, de intentos fallidos de autenticación del usuario remoto. Cuando se ha alcanzado el número definido de intentos de autenticación sin éxito, el TOE bloquea la cuenta de usuario remoto temporalmente, tiempo también configurable por un usuario administrador del TOE. Por defecto 3 intentos en un rango de 3 a 5 y un tiempo de bloqueo de tres minutos.
- FIA_ATD.1 (1) FIA_ATD.1 (2) FIA_ATD.1 (3) - el TOE mantiene los siguientes atributos de seguridad asociados con cada usuario remoto: identificación del usuario, datos de autenticación, y adicionalmente, roles asignados y dirección de correo electrónico.
- FIA_SOS.1 (1) FIA_SOS.1 (2) - el TOE aplica políticas de contraseña que garantiza que todos los secretos asociados con las cuentas de usuario remoto se cumplen.
- FIA_UAU.1 - el TOE requiere que cada usuario remoto se autentique con éxito antes de permitir cualquier otra acción mediada por el TSF en nombre de ese usuario, excepto con los servicios públicos de front end.
- FIA_UAU.6 (1) FIA_UAU.6 (2) - el TOE requiere que el usuario remoto vuelva a autenticarse antes de permitir que el usuario cambie su propia contraseña o su sesión expire por inactividad.
- FIA_UID.1 - el TOE requiere que cada usuario remoto se identifique con éxito antes de permitir cualquier otra acción mediada por el TOE en nombre de ese usuario, excepto con los servicios públicos de front end.

6.4 Gestión de la seguridad

Las funciones de la gestión de la seguridad satisfacen los siguientes requisitos funcionales de seguridad:

- FMT_MOF.1 - el TOE restringe la habilidad de determinar el comportamiento o, modificar el comportamiento de las funciones basadas en políticas de seguridad.
- FMT_MTD.1 - el TOE permite restringir la administración de los datos de TSF a los usuarios de front end administradores del TOE que tienen asignados roles con secciones de autorización, que permiten la gestión de colas, patrones/consultas y acciones.
- FMT_SMF.1 - el TSF es capaz de ejecutar las siguientes funciones de gestión: roles, asignación de roles a – secciones de control, colas, consultas de líneas de logs, patrones de ficheros de líneas de logs y acciones -, usuarios de front end, asignación de roles a usuarios de front end, gestión de la configuración de syslog, asignación de colas a eventos de seguridad, activación de reglas de correlación,

activación de respuestas - y notificaciones por correo electrónico -, debidas a correlación.
- FMT_SMR.1 (1) - un único rol, el rol es asignado a usuarios del bus.
- FMT_SMR.1 (2) - inicialmente usuario de front end administrador del TOE, super root, con capacidad de crear roles y usuarios de front end. Los roles son asignados a usuarios de front end.

6.5 Acceso

Las funciones de acceso al TOE satisfacen los siguientes requisitos funcionales de seguridad:

- FTA_SSL.3 - el TOE finaliza una sesión interactiva después de un intervalo de tiempo de inactividad.
- FTA_SSL.4 - el TOE permite al usuario remoto la terminación de su propia sesión interactiva.

6.6 Rutas de confianza

Las rutas de confianza satisfacen los siguientes requisitos funcionales de seguridad:

- FTP_TRP.1 - el TOE proporciona una ruta de confianza para que los usuarios remotos se comuniquen con el TOE, la comunicación se encuentra protegida ante modificación y exposición. Toda acción frente al TOE requiere el empleo de una ruta de confianza.

6.7 TOE Summary specification rationale

En esta sección, se muestra la trazabilidad de los requisitos funcionales de seguridad con las funciones de seguridad del TOE a los que dan cumplimiento. Para ello, se muestra en formato tabular cada instancia de cada requisito cruzado con las diferentes funciones de seguridad del TOE.

REQUIREMENT	SECURITY FUNCTION					
	REGISTROS DE AUDITORÍA	CLAVES CRIPTOGRÁFICAS	IDENTIFICACIÓN Y AUTENTICACIÓN	GESTIÓN DE LA SEGURIDAD	ACCESO	RUTAS DE CONFIANZA
FAU_ARP.1 Security alarms	X					
FAU_SAA.1 Potential violation analysis	X					
FAU_GEN.1 Audit data generation	X					
FAU_SAR.1 Audit review	X					
FAU_SAR.2 Restricted audit review	X					
FAU_SAR.3 Selectable audit review	X					
FAU_STG.2 Guarantees of audit data availability	X					
FAU_STG.3 Action in case of possible audit data loss	X					
FAU_STG.4 Prevention of audit data loss	X					
FCS_CKM.1 Cryptographic key generation		X				

REQUIREMENT	SECURITY FUNCTION					
	REGISTROS DE AUDITORÍA	CLAVES CRIPTOGRÁFICAS	IDENTIFICACIÓN Y AUTENTICACIÓN	GESTIÓN DE LA SEGURIDAD	ACCESO	RUTAS DE CONFIANZA
FCS_CKM.4 Cryptographic key destruction		X				
FCS_COP.1 Cryptographic operation		X				
FIA_AFL.1 Authentication failure handling			X			
FIA_ATD.1 User attribute definition			X			
FIA_SOS.1 Verification of secrets			X			
FIA_UAU.1 Timing of authentication			X			
FIA_UAU.6 Re-authenticating			X			
FIA_UID.1 Timing of identification			X			
FMT_MOF.1 Management of security functions behaviour				X		
FMT_MTD.1 Management of TSF data				X		
FMT_SMF.1 Specification of Management Functions				X		
FMT_SMR.1 Security roles				X		
FTA_SSL.3 TSF-initiated termination					X	
FTA_SSL.4 User-initiated termination					X	
FTP_TRP.1 Trusted path						X

TABLA 10: SUMMARY SPECIFICATION RATIONALE