PLIEGO DE CLÁUSULAS TÉCNICAS PARTICULARES DE LA FUNDACIÓN CENTRO TECNOLÓXICO DE TELECOMUNICACIÓNS DE GALICIA (GRADIANT) PARA LA CONTRATACIÓN DE SERVICIOS POR PROCEDIMIENTO NEGOCIADO CON PUBLICIDAD

En el marco de la cuarta convocatoria de la Compra Pública Precomercial lanzada por el Instituto Nacional de Ciberseguridad (INCIBE), Gradiant ha sido adjudicataria del proyecto SafeNet UEBA: CENTRO DE OPERACIONES DE SEGURIDAD BASADO EN UEBA EXPLICABLE.

SafeNet UEBA tiene como objetivo el diseño de un sistema para la detección de ciberataques y anomalías en el comportamiento de usuarios y entidades en entornos corporativos mediante técnicas avanzadas de inteligencia artificial y aprendizaje automático. Para mejorar la capacidad de análisis de la plataforma, es fundamental ampliar las fuentes de datos disponibles mediante la integración con servicios de colaboración, almacenamiento en la nube, ERP y CRM, entre otros sistemas SaaS utilizados en entornos corporativos.

El objeto de esta licitación es la contratación de servicios de desarrollo, implementación y validación de conectores de datos que permitan la captura de registros de actividad desde ERPs SaaS. Estos conectores deben ajustarse a la arquitectura tecnológica existente de SafeNet UEBA y cumplir con los requisitos de seguridad, escalabilidad y eficiencia operativa definidos en este documento.

Arquitectura del Sistema y Requisitos de Integración

SafeNet UEBA está basado en una arquitectura modular y distribuida que permite la captura, almacenamiento, procesamiento y análisis de grandes volúmenes de datos en tiempo real. La plataforma se compone de varios módulos interconectados, organizados en distintas capas funcionales, donde se incluyen los módulos de captura y normalización de datos, almacenamiento distribuido, procesamiento y agregación de datos, análisis mediante modelos de aprendizaje automático, interpretabilidad de alertas y visualización en un Centro de Operaciones de Seguridad (SOC), tal y como se detalla en la Figura 1 Arquitectura de datos de la solución SafeNet UEBAFigura 1.

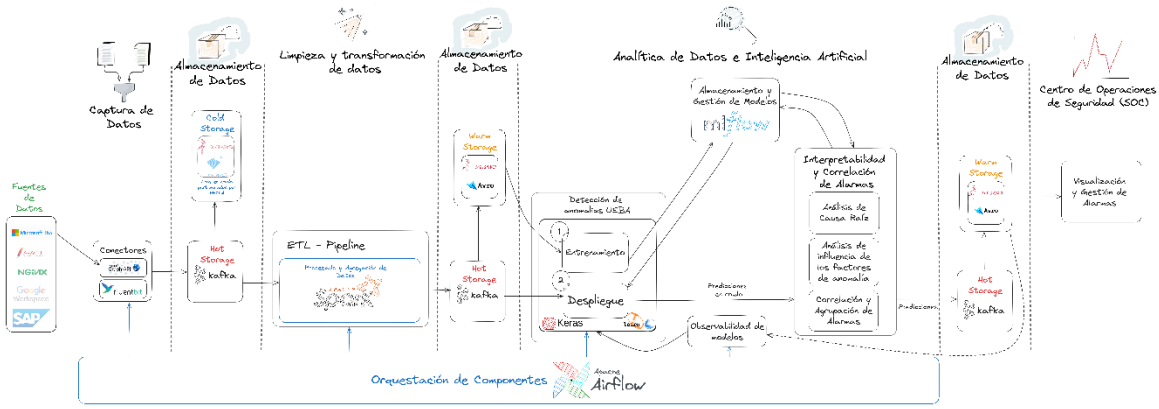

Figura 1 Arquitectura de datos de la solución SafeNet UEBA

La infraestructura de SafeNet UEBA utiliza Apache Kafka como sistema de mensajería para la ingesta de datos en tiempo real y almacenamiento en caliente, mientras que los datos en crudo

se almacenan de forma persistente en MinIO S3. El procesamiento de datos se realiza mediante Apache Spark, con la orquestación de flujos de trabajo a través de Apache Airflow. Los modelos de inteligencia artificial se desarrollan en Keras y scikit-learn, con administración del ciclo de vida en MLFlow. Finalmente, el módulo de interpretabilidad permite enriquecer las alertas mediante técnicas explicativas y generación de informes de seguridad.

El proveedor deberá desarrollar e integrar el nuevo conector en la capa de captura de datos, asegurando su compatibilidad con la infraestructura actual de SafeNet UEBA. Cada conector deberá extraer datos de actividad desde los servicios SaaS especificados, transformarlos en el formato requerido y enviarlos a los sistemas de almacenamiento y procesamiento del SOC. Se espera que la integración de estos conectores se realice utilizando APIs REST o *webhooks* proporcionados por los servicios SaaS, asegurando autenticación segura mediante OAuth2 o credenciales protegidas en un gestor seguro.

Alcance

El proveedor será responsable de analizar la documentación de las APIs de los servicios SaaS seleccionados y desarrollar conectores eficientes para la captura de registros de actividad. Deberá permitirse tanto la extracción de históricos de datos como la captura continua para su análisis en tiempo real. La definición de las plataformas a integrar se definirá junto con el proveedor seleccionado, dependiendo de su experiencia previa y oferta, pero podría incluir:

- SAP EPR
- Salesforce
- Dynamics 365

El desarrollo de cada conector deberá incluir la implementación de procesos de autenticación, la configuración de *endpoints* de extracción de datos, la transformación y normalización de los registros capturados, y su envío a los sistemas de almacenamiento y procesamiento de SafeNet UEBA.

Adicionalmente, el proveedor deberá ofrecer documentación detallada que defina los datos capturados, su tipo, y una descripción de cada uno de los campos capturados, de forma que estos puedan ser explotados correctamente en el módulo de analítica e IA.

El proveedor también será responsable de realizar pruebas de integración y rendimiento, garantizando que los conectores no afecten la estabilidad ni el desempeño de la plataforma. Deberán implementarse mecanismos de monitoreo y *logging* para verificar el correcto funcionamiento de los conectores, con alertas en caso de fallos o desconexiones en la captura de datos.

Para garantizar la compatibilidad con la arquitectura de SafeNet UEBA, el desarrollo de los conectores deberá realizarse en Python. El formato de los datos extraídos deberá ser JSON, Avro o Parquet, y su transmisión deberá realizarse utilizando protocolos seguros como HTTPS con TLS 1.2 o 1.3.

Los registros capturados deberán ser poder ser enviados a Apache Kafka en distintos *topics*, permitiendo su procesamiento en paralelo, así como su almacenamiento persistente en S3.

Desde el punto de vista de la seguridad, los conectores deberán utilizar autenticación OAuth2 cuando la API del proveedor lo permita, asegurando la gestión segura de credenciales en un entorno protegido. Se deberá evitar el almacenamiento de credenciales en código fuente o archivos de configuración accesibles. Además, se exigirá el cifrado de datos en tránsito mediante TLS y el cifrado en reposo mediante AES-256 para los datos sensibles.

Entregables y documentación

Se generarán y entregarán los siguientes entregables:

- E1 – Diseño de la integración: análisis funcional y técnico de las APIs de los sistemas SaaS seleccionados y descripción de los conectores a implementar.
- E2 – Especificación técnica de conectores e implementación *software*: código fuente y documentación, incluyendo la siguiente información por cada conector desarrollado:
    - Campos capturados (nombre, tipo, formato).
    - Frecuencia de extracción.
    - Procedimiento de autenticación.
    - Endpoint utilizados.
    - Esquema de normalización.
    - Protocolo de transmisión.
    - Integración con MinIO S3 y Apache Kafka.
- E3 – Guía de integración y despliegue: documentación detallada con requisitos de entorno, configuración requerida, guía de instalación.