centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1231

Procedimiento de empleo seguro
Aiuken Security Intelligence Platform

Mayo 2025

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-25-187-7
Fecha de Edición: Mayo de 2025

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2026.01.16 07:22:36 +01'00'

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

1. ASIP (Aiuken Security Intelligence Platform) es una plataforma cloud *multi-tenant* de gestión de SOC (*Security Operations Center*) que provee todas las herramientas que un SOC necesita para la gestión del ciclo de vida completo de la gestión de incidentes de seguridad, desde el procesado de los eventos de actividad de las infraestructuras protegidas, pasando por la detección, envío de informes a los actores involucrados, investigación y mitigación final.
2. A continuación, se detallen los componentes que forman la solución:
    - **Data Lake**. Base de datos donde se indexa toda la actividad generada por los dispositivos, aplicaciones y servicios de las infraestructuras protegidas. La información se normaliza y también se mantiene *en bruto*, para poder aplicar procesos de investigación y relación de la información basados en técnicas de *big data*.
    - **Threat Intelligence**. Sistema de agregación de actividad maliciosa que ocurre en Internet a través de fuentes de inteligencia, que indexa toda la actividad registrada en el *data lake* en tiempo real y de forma continua. La información obtenida por la *Threat Intelligence* es comprobada en tiempo real contra todos los eventos que se integran en la plataforma de forma autónoma y completamente desatendida, con el fin de identificar actividades que ocurren en las infraestructuras protegidas.
    - **Generador de dashboards**. Herramienta que permite convertir en información visual la actividad proveniente de las fuentes integradas. Permite generar fácilmente cuadros de mando que describen el comportamiento de los activos integrados, como se relacionan entre ellos y entre recursos externos a la compañía, uso de protocolos, aplicaciones, comportamiento de personas, etc.
    - **Motores de detección.** Permiten la identificación de riesgos en las infraestructuras protegidas mediante a la búsqueda de criterios conocidos y de la obtención de patrones de comportamiento. El sistema cuenta con tres motores diferentes para dar la mayor cobertura a las posibles técnicas de detección atendiendo al contexto de los eventos:
        - **Motor de detección sin contexto.** Analiza en tiempo real todos los eventos que se procesan por la plataforma, teniendo como contexto de análisis la propia información del evento y la de la *Threat Intelligence*, sin contar con información de otros eventos u otras fuentes.
        - **Motor de detección correlada.** Analiza los eventos en *batches* una vez se indexan en el *data lake*, añadiendo contextos de otras fuentes integradas y de la *Threat Intellligence*. Añade también la variable temporal, lo que permite la aplicación de casos de uso de detección que tienen en cuenta actividad del pasado en el contexto de múltiples fuentes.

  - **Motor de Inteligencia Artificial.** Implementa casos de uso de detección basados en la obtención de perfiles de comportamiento para resolver problemas que no pueden ser solucionados con correlación.

- **Framework de integración.** Conjunto de componentes que permiten la recolección de eventos desde cualquier tipo de fuente atendiendo a la infraestructura donde se generan, como elementos *on-premises* o *public cloud providers*, así como el procesado e integración de cualquier tipo de eventos independientemente de su formato, ya sean generados por dispositivos IT, OT, aplicaciones propietarias o servicios cloud.
- **Generador de informes.** Sistema de elaboración autónoma de informes que garantiza la generación de reportes. El motor de generación de informes está basado en plantillas.
- **Módulo de enriquecimiento.** Integrado con las APIs de NIST, MITRE y CAPEC para mantener diariamente actualizada una representación local de estos frameworks.
- **Portal de servicio.** Interfaz para que analistas del SOC y clientes finales interactúen en un punto único, permitiendo así prestar servicios de ciberseguridad transparentes donde los usuarios reciben en tiempo real toda la información de la plataforma, así como la interacción de ambas partes (analistas y usuarios finales) el mismo sistema donde se reciben y procesan los eventos, se investigan los casos y donde se integran todos los componentes de la plataforma, sirviendo como canal de *delivery* en tiempo real de los resultados a clientes y resto de actores involucrados en los servicios de ciberseguridad.
- **Ticketing.** Sistema para la documentación de los incidentes gestionados y reporte a los actores involucrados.
- **CMDB**. Sistema para el inventariado de todos los activos de cada infraestructura protegida, donde se clasifican por su tipología, criticidad, y se añade toda la información necesaria para los motores de detección y generador de informes.
- **API de integración.** La plataforma cuenta con un conjunto de endpoints que permiten la integración de herramientas externas como sistemas *SOAR* o cualquier otro sistema IT (ej. ticketings) con el objetivo de integrar el sistema en un ecosistema y alimentar a este de la información que necesite.

3. La plataforma ASIP opera en un modelo (Platform as a Service) desde la nube pública de Google GCP (*Google Cloud Platform*) [REF1]. Está basada en tecnología *cloud* nativa *Kubernetes* [REF2], lo que permite aplicar todas las capacidades de escalabilidad y alta disponibilidad de GCP distribuyendo sus componentes en diferentes regiones geográficas.
4. A continuación, se detallan los módulos principales que componen el sistema:

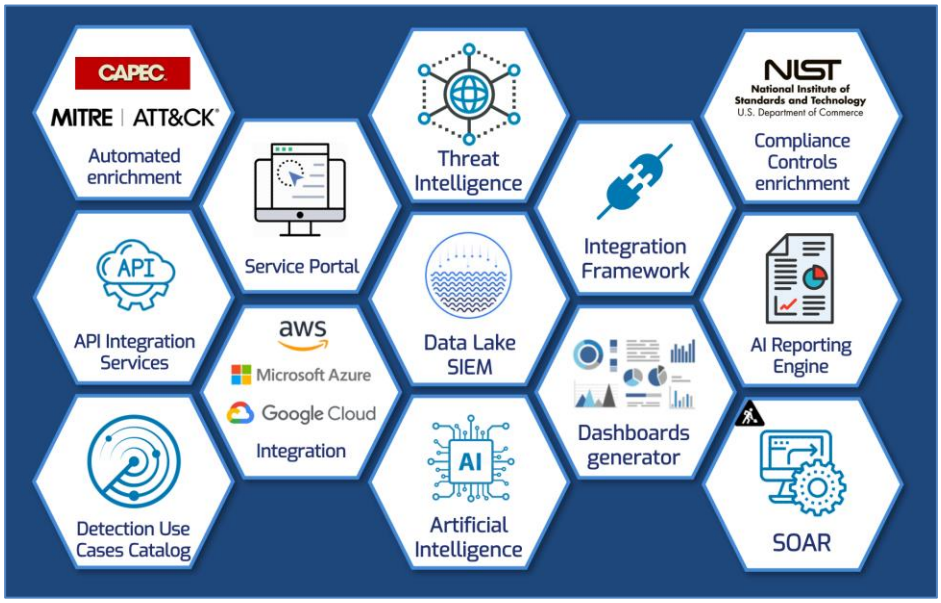

Ilustración 1. Módulos que componen la plataforma ASIP

2. OBJETO Y ALCANCE

5. Este documento muestra el procedimiento de despliegue y configuración segura de los componentes que han de ser instalados en la infraestructura de los clientes para recoger los eventos seguridad.
6. Dado que la plataforma es *cloud*, no es necesario instalar la plataforma en el lado de los clientes, ya que se les ofrece como servicio a través de una interfaz web. Los clientes finales utilizan la plataforma desde la nube, y despliegan en su infraestructura el componente *Forwarder* encargado de recoger los logs en sus infraestructuras, y enviarlos a los colectores que están en la nube. Este componente consiste en un colector local encargado de recolectar los logs en la red del cliente.

3. ORGANIZACIÓN DEL DOCUMENTO

7. Este documento se compone de los siguientes apartados:

    - Apartado **4**. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.
    - Apartado **5**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.
    - Apartado **6**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
    - Apartado **7**. En este apartado se recogen las referencias empleadas a lo largo del documento.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

8. Puesto que ASIP se ofrece en un modelo PaaS (*Platform as a Service*), su entrega se realiza en forma de portal de servicio accesible a través de Internet, por lo que no existe riesgo de que el cliente final pueda manipular ninguno de sus componentes.
9. A continuación, se listan los componentes que son instalados en el lado del cliente para recoger los logs localmente:
    - Forwarder (colector local encargado de recolectar los logs en la red del cliente)
10. El siguiente diagrama muestra la arquitectura de ingestión de eventos de la plataforma.

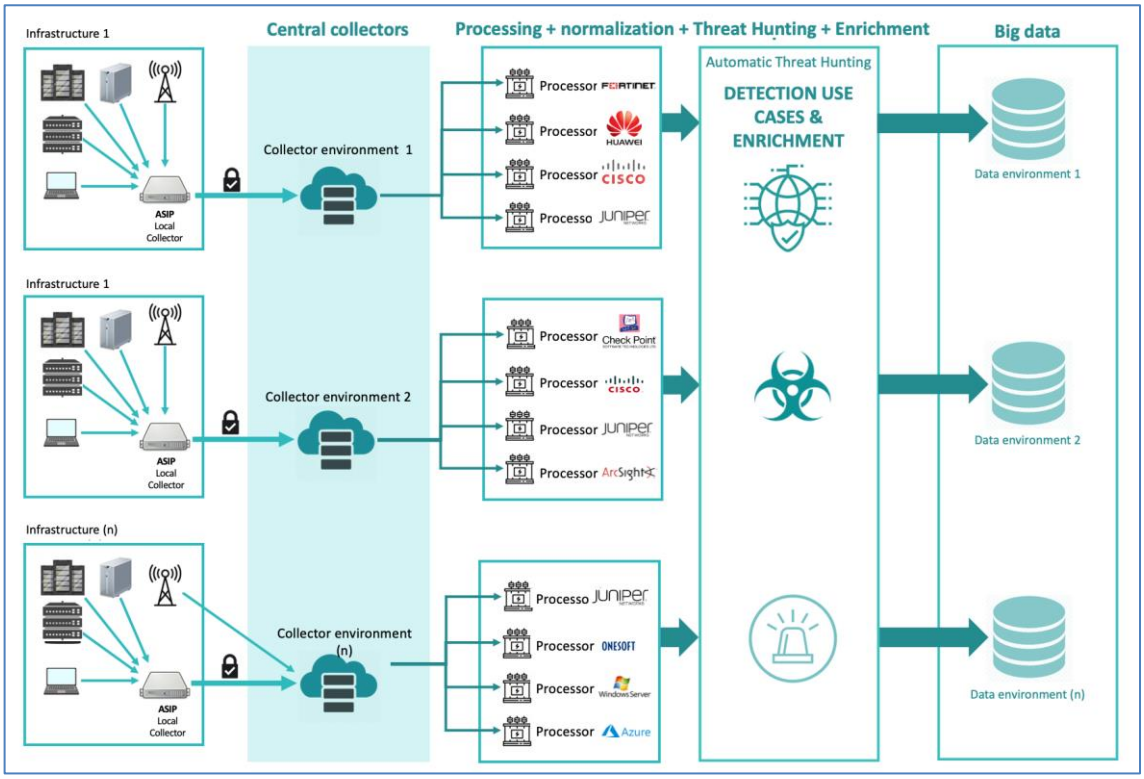

Ilustración 2. Diagrama de capas de envío de logs desde las fuentes a la plataforma ASIP

11. La primera capa -*Infraestructure (n)*- es donde se generan los logs de los dispositivos *on-premises* de los clientes, y donde se instala el colector local Forwarder (*ASIP local collector)*.
12. Las capas "*Central collectors, Processing + normalization + Threat Hunting + Enrichment y Big Data"* están físicamente en la nube de Aiuken. Forman parte de la plataforma PaaS, por lo que se ofrecen como servicio desde la nube y no requieren instalación en los clientes.

4.2 ENTORNO DE INSTALACIÓN SEGURO

13. Los diferentes servicios que ofrece el producto están ubicados en la nube del fabricante.

4.3 REGISTRO Y LICENCIAS

14. En el apartado 5.3 Gestión de claves de licencia se trata en detalle la gestión y comprobación de las licencias del producto.

4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN

15. Los diferentes servicios que ofrece el producto están ubicados en la nube del fabricante.

5. FASE DE INSTALACIÓN

5.1 INSTALACIÓN DE COLECTOR LOCAL FORWARDER

16. En un correo electrónico dirigido al cliente, se enviará la URL de descarga, el valor Hash asociado al fichero .iso, y un nombre de usuario. Posteriormente, y por un canal diferente, se entregará la contraseña al cliente, para que pueda realizar la descarga del fichero.
17. Una vez descargada la imagen .iso, proceder a la verificación de su integridad antes de continuar con el siguiente paso. Para ello, se recomienda emplear una herramienta externa que permita calcular el hash de dicha imagen.
18. Para la instalación, crear y configurar la máquina virtual para arrancar utilizando el archivo .iso descargado en el paso anterior.
19. Una vez arrancada la máquina virtual, creada empleando la imagen .iso descargada en los pasos anteriores, se iniciará automáticamente el asistente de instalación y se seguirán los siguientes pasos:
    - En el menú, seleccionar **Install Forwarder** (primera opción)
    - Cuando se muestre la *Licencia de usuario final*, seleccionar **Aceptar**
    - Cuando se pregunte por la configuración IP introducir los siguientes datos:
        - Seleccionar la interfaz de red que será configurada para recibir los eventos
        - Dirección IP
        - Máscara de red
        - Gateway
        - Servidor de nombres
    - Seleccionar **Aceptar**
    - En el siguiente menú se muestra un resumen de la configuración introducida. Revisar que todo es correcto y seleccionar **Aceptar**
    - La instalación se inicia tras este paso y una vez terminada, el servicio de recolección de logs se inicia automáticamente.
20. Para más información al respecto, se recomienda consultar la Guía de Instalación del producto [REF5]. Dicho documento es proporcionado por el fabricante durante el proceso de compra del producto.

5.2 USUARIOS DE ACCESO AL FORWARDER

21. La imagen instalada contiene toda la configuración de usuarios necesaria, así como sus certificados, para realizar la instalación en remoto. Estos usuarios son únicamente utilizados para la ejecución de los servicios del Forwarder, y para el

acceso a la utilidad de configuración de red TCP/IP que figura en la Guía de Instalación. Dichos usuarios empleados para estos procesos no tienen relación con los usuarios que se emplean para acceder a la plataforma a través de la interfaz web.

22. No es necesaria la creación de usuarios adicionales ni configuración manual. De esta forma el Forwarder se convierte en una *caja negra* que no puede ser manipulada por el cliente final, garantizando así la integridad del sistema.

5.3 GESTIÓN DE CLAVES DE LICENCIA

23. Durante el proceso de instalación del Forwarder en el cliente, se genera la licencia para el cliente y un identificador único para el Forwarder, siguiendo el siguiente proceso automático:
    - Tras la instalación de la imagen base .iso y despliegue del software, se inician los servicios del Forwarder.
    - El servicio del Forwarder conecta con el API de ASIP en la nube, se identifica mediante certificado de clave asimétrica y en caso de estar autorizado, recibe los datos de licencia. Dicho certificado ya viene incluido en la imagen de instalación del producto.
    - Este proceso se repite automáticamente cada 5 minutos para controlar el estado de la licencia.
24. Por lo tanto, no es necesaria ninguna acción manual en el lado del cliente para instalar la licencia. Todo se realiza en la nube de ASIP.

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

25. El producto funciona por defecto con una configuración considerada segura, proporcionada por el fabricante, y está contenido en una caja negra a la que no hay acceso.

6.1.1 DESPLIEGUE DE CAMBIOS EN LA CONFIGURACIÓN

26. Dado que ASIP es una plataforma PaaS que se ofrece como servicio, los cambios en la plataforma se realizan en la nube de ASIP sin requerir en el lado del cliente ninguna acción manual.
27. Los Forwarders de los clientes conectan cada 5 minutos con la plataforma en la nube para buscar cambios en la configuración pendientes de aplicar. En caso de haber un cambio pendiente, el Forwarder descarga la configuración y la aplica automáticamente sin intervención manual.

6.2 AUTENTICACIÓN

28. La autenticación requiere de usuarios dados de alta previamente en la plataforma en la nube. **Los usuarios solo pueden ser creados, modificados y eliminados por los administradores de Aiuken. Si el cliente desea dar de alta, modificar o eliminar usuarios, será necesario solicitarlo a dichos administradores.**
29. La autenticación de los usuarios se realiza mediante usuario, contraseña y código OTP, que es generado por el usuario en el momento del login.

Ilustración 3. Formulario de login

Ilustración 4. Formulario de entra de código OTP

30. El proceso para entregar la semilla para la generación del código OTP a los usuarios es el siguiente:
    - El administrador de la plataforma registra un nuevo usuario en el cloud de la plataforma.
    - Durante el proceso de creación del usuario, se definen detalles como nombre y apellidos, dirección de correo electrónico, sus permisos de acceso y su nivel de privilegios.
    - Al registrar el usuario, la plataforma genera automáticamente la semilla para la generación del código OTP del usuario, y le envía automáticamente un email con las instrucciones de acceso y de uso del OTP a la dirección de correo electrónico especificada durante la creación del usuario.
31. Una vez registrado el usuario, es posible revocar su semilla para el OTP o dar de alta nuevas semillas en el caso de que el usuario necesite diferentes dispositivos para la generación de los códigos.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

32. La administración de ASIP se lleva a cabo en su nube, de forma centralizada para todos los clientes que la utilizan.
33. La plataforma cuenta con una sección específica de administración donde se pueden configurar todos sus componentes, gestión de clientes y gestión de usuarios finales.
34. Para acceder a la administración de la plataforma es necesario lo siguiente:
    - Acceder a la interfaz web de la plataforma en la URL https://soc.aiuken.com [REF4]
    - Tras introducir unas credenciales válidas, generar e introducir el código OTP.
    - El usuario con el que se accede debe tener el rol *SOC Administrator*. En caso de no contar con este rol, el sistema no le mostrará el acceso el acceso a la

sección de administración, y también limitará su acceso en caso de que trate de acceder directamente indicando la URL en el navegador.

- Hacer clic en el icono que lleva a la administración.
- En este momento el sistema vuelve a requerir un nuevo código OTP al usuario.

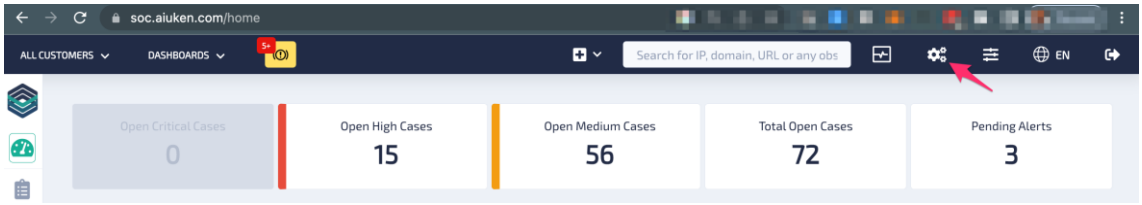

Ilustración 5. Sección de casos pendientes en el dashboard principal

35. A continuación, la plataforma da acceso a la sección de administración del sistema, desde la que es posible configurar clientes, usuarios, reglas de detección, informes, y el resto de parametrizaciones para los distintos módulos de la plataforma. **Este menú solo es accesible y visible para los administradores de la plataforma (los administradores de Aiuken)**.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

36. ASIP cuenta con un sistema de roles y permisos que permiten limitar el nivel de acceso de los usuarios, qué información pueden visualizar y de qué clientes, y a qué herramientas tendrán acceso.
37. Además del sistema de roles, la plataforma cuenta con dos niveles de administración:
    - **Usuario cliente final**. Tiene acceso únicamente a la información de los clientes que se asocien a su usuario. No tiene acceso a las herramientas de analista.
    - **Usuario administrador**. Puede realizar cambios sobre cualquier elemento de la plataforma, así como sobre todos los usuarios, excepto sobre los *superadministradores*.
    - **Usuario superadministrador**. Puede realizar cambios sobre cualquier elemento de la plataforma y también sobre los *administradores* (ej. crear nuevos *administradores*, borrarlos o modificarlos).
38. Los privilegios de los usuarios se deben definir obligatoriamente durante el proceso de creación, ya que el sistema no permite crear usuarios sin tener todos sus permisos definidos.

6.3.3 CUENTAS Y ROLES DE USUARIOS

39. La administración de la plataforma permite la gestión de los usuarios y sus permisos de acceso, los cuales pueden ser modificados en cualquier momento por parte de los administradores.

40. Para configurar los permisos y roles de los usuarios es necesario acceder al panel de administración, tal como se detalla en el apartado 6.1 de este documento, y acceder a la sección *Authentication and authorization > Users*

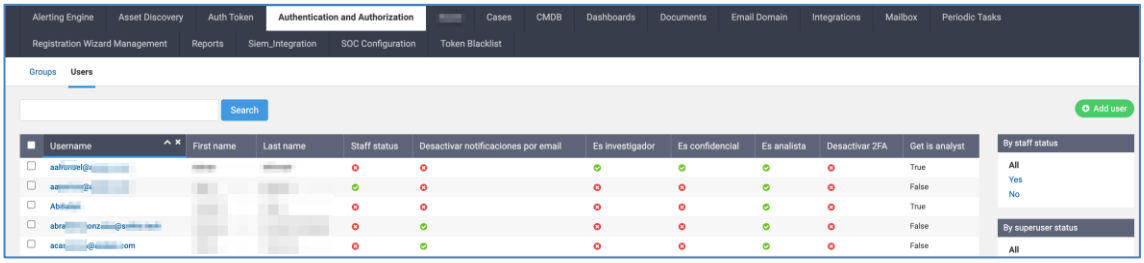

Ilustración 6. Interfaz de gestión usuarios

41. A continuación, se detallan los parámetros del sistema de privilegios de los usuarios:

- **Administrador**. Indica si tiene permiso de gestión sobre todos los elementos de la plataforma y sobre el resto de los usuarios, a excepción de los *superadministradores*.
- **Superadministador**. Indica si tiene permiso de gestión sobre todos los elementos de la plataforma y sobre el resto de los usuarios, incluyendo a los *administradores*.
- **Active**. Indica si el usuario puede acceder o no a la plataforma. Los usuarios sin este rol seguirán dados de alta en la plataforma, pero no tendrán permiso para hacer login.
- **Grupos**. Especifica a la información de qué clientes tendrá acceso el usuario. Es posible tener usuarios con acceso a la información de un solo cliente, o de varios, dando la posibilidad de segmentar el acceso a la información en grandes clientes que segmenten su información mediante una estructura de unidades organizativas.
- **SOC Analyst**. Especifica si el usuario es un analista del SOC o no. En caso de serlo, el usuario tendrá acceso a todas las herramientas de SOC y a la información de todos los clientes.
- **Notifications**. Especifica si el usuario recibirá notificaciones automáticas por las acciones que se realicen en la plataforma relacionadas con los grupos a los que esté asociado, tales como alertas, gestión de casos, generación de informes, etc.
- **Analyst**. Especifica si el usuario tendrá acceso a las herramientas de analista.
- **Investigator**. Especifica si el usuario tendrá acceso a las herramientas de investigador.
- **Threat Intelligence**. Especifica si el usuario tendrá acceso a la Threat Intelligence.
- **Two factor authentication**. Especifica si el usuario podrá acceder a la

plataforma sin introducir el código OTP. Esta opción solo afecta a clientes finales que no son administradores ni analistas de SOC. Los administradores, superadministradores y analistas de SOC están obligados siempre a generar e introducir código OTP en la plataforma. Los clientes finales también para acceder a su información, pero podría deshabilitarse en caso de que lo soliciten.

- **Business services.** Especifica a qué unidades organizativas de los grupos asociados al cliente tendrá acceso el usuario. Esto permite segmentar la información de los clientes aumentando la granularidad de los permisos de acceso y para las capacidades de reporting.
- **TOPT.** Permite gestionar las semillas de los generadores OTP de los clientes.

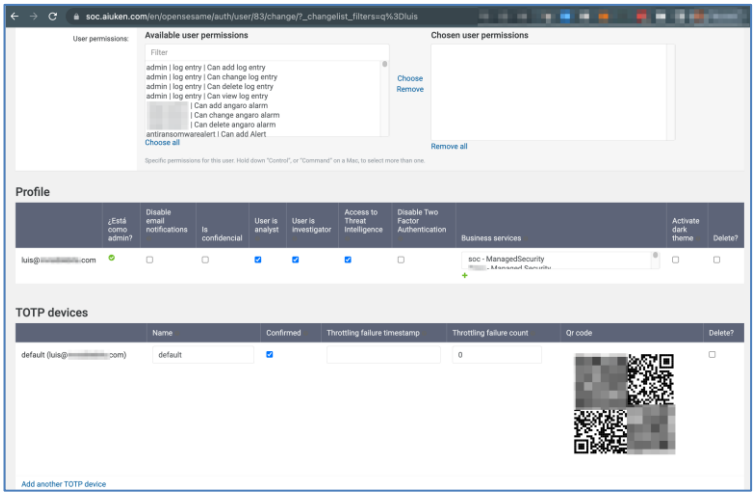

Ilustración 7. Edición de parámetros y permisos de un usuario

42. **NOTA**: es necesario indicar que solo administradores (*Administrator*) y superadministradores (*Superadministrator*) pueden modificar los privilegios de los usuarios finales (clientes). Los usuarios finales no pueden modificar sus propios permisos, y no tienen acceso a la herramienta de administración.

6.3.4 PARÁMETROS DEL SISTEMA

43. Los usuarios no pueden modificar la parametrización del sistema en cuanto a políticas de seguridad de contraseñas, sistemas de cifrado o tiempo de inactividad de las sesiones, ya que estas configuraciones se aplican de forma centralizada para todos los clientes por igual por parte de los administradores del lado de la plataforma.
44. Las contraseñas deben cumplir la política de seguridad de contraseñas. En caso contrario no serán aceptadas por el sistema, proponiendo al usuario especificar una nueva contraseña hasta que esta cumpla con la siguiente política de contraseñas:
    - Debe tener un mínimo de 8 caracteres y un máximo de 16. Se recomienda una longitud mínima de 12 caracteres.

- Debe estar formada por caracteres alfanuméricos, incluyendo al menos una letra mayúscula, una letra minúscula, un número y un símbolo especial.
- No puede ser igual que las últimas 5 contraseñas.
- La contraseña tendrá un tiempo de validez de 6 meses, momento tras el cual el sistema solicitará su cambio, cumpliendo con los puntos anteriores. **El tiempo de validez de la contraseña no es configurable.**

45. Una vez realizada autenticación en la plataforma, y la introducción de un código OTP válido, se creará una sesión para dicho usuario. La sesión expirará tras 5 minutos de inactividad por parte del usuario, debiendo volver a autenticarse e introducir un nuevo código OTP.
46. El tiempo de validez de la sesión no es configurable por el usuario. Es un valor fijo establecido para todos los usuarios de la plataforma. Dicho valor es de 60 segundos. Adicionalmente, todas las peticiones enviadas al interfaz de la plataforma son autenticadas mediante *JSON Web Tokens*, que se refrescan cada 10 segundos.
47. La cuenta de un usuario será deshabilitada tras realizar 5 intentos de autenticación fallidos seguidos. El número de intentos fallidos seguidos es un valor fijo para todos los usuarios de la plataforma, que no puede ser modificado por los usuarios.
48. Para reestablecer una cuenta deshabilitada, es necesario realizar una solicitud por email al equipo de soporte de la plataforma.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

49. El acceso a la plataforma por parte de los usuarios finales se realiza mediante HTTPS/TLSv1.2.
50. Las comunicaciones entre los Forwarders y la plataforma en la nube se realizan también mediante HTTPS/TLSv1.2, con autenticación de certificado en ambos extremos.
51. El envío de logs desde los Forwarders a los colectores cloud se realiza mediante TLS/v1.2 con autenticación de certificado en ambos extremos.
52. Tanto el acceso a la interfaz web como al API que da servicio a los Forwarders, como los colectores que reciben los logs, solo utilizan suites de cifrado basadas en AES y SHA256.

6.5 GESTIÓN DE CERTIFICADOS

53. Los procesos de autenticación de usuarios finales en la interfaz web, y de los Forwarders en el API de servicio y en los colectores cloud donde envían los logs, se realizan mediante HTTPS.
54. La gestión de los certificados la realizan los administradores de la plataforma de Aiuken, por lo que los usuarios finales no tienen la capacidad de gestionar los certificados utilizados para proteger las comunicaciones con la nube de ASIP.

55. Los certificados se crean empleando los siguientes algoritmos y funciones criptográficas:
    - ECDHE-ECDSA-AES-256-GCM-SHA384
    - ECDHE-RSA-AES-256-GCM-SHA384
    - ECDHE-ECDSA-CHACHA20-POLY1305
    - ECDHE-ECDSA-AES-128-GCM-SHA256
    - ECDHE-RSA-AES-128-GCM-SHA256

6.6 ACTUALIZACIONES

56. Al tratarse de una plataforma PaaS, ASIP se actualiza continuamente cumpliendo con los tiempos de sus ciclos de desarrollo y evolutivos.
57. ASIP está construido sobre Kubernetes e integrado con sus mecanismos, cumpliendo con los principios *cloud native* para todo lo relacionado con la alta disponibilidad y auto-escalado de microservicios.
58. Las actualizaciones de la plataforma se realizan utilizando pipelines CI/CD (*Continuous Delivery*) que garantizan que no hay impacto en la disponibilidad de los servicios de la plataforma durante los procesos de actualización en producción, ya que durante las pipelines CD se despliegan automáticamente contenedores en paralelo a los que actualmente están en producción y que van a ser sustituidos, y una vez que pasan todos los tests, el tráfico es redirigido automáticamente los nuevos contenedores que tienen la versión actualizada del componente y se elimina automáticamente la versión antigua, garantizando un 100% de disponibilidad del servicio.

6.7 ALTA DISPONIBILIDAD

59. Al tratarse de una plataforma PaaS construida sobre tecnología *cloud native* Kubernetes, los componentes de la plataforma son distribuidos en diferentes centros de datos para garantizar que, en caso de caídas de uno de los centros de datos, los servicios de la plataforma seguirán dando servicio y que no se pierde la información almacenada, ya que está replicada y distribuida en diferentes regiones geográficas.
60. Al ser una plataforma PaaS, los usuarios finales no necesitan hacer ninguna configuración para conseguir alta disponibilidad de la plataforma, ya que esta es gestionada por el equipo SRE (*Site Reliable Engineering*) de la plataforma.

6.8 AUDITORÍA

6.8.1 REGISTRO DE EVENTOS

61. Los eventos de auditoría (los logs de la propia plataforma) son almacenados en la misma nube donde se generan y distribuidos mediante los mecanismos que

provee Kubernetes al resto de regiones geográficas (tal y como se indica en el Apartado 6.7), indexadas en el propio Data Lake y disponibles para su explotación desde un sistema externo basado en *Graphana Loki* [REF3], para garantizar que en caso de cualquier contingencia los logs podrán ser analizados sin contar con la propia plataforma.

62. Los eventos de auditoría que se registran incluyen:
    - Actividad de login (tanto logins OK como NOK).
    - Actividad de logout.
    - Cambios de contraseñas.
    - Creación, borrado y modificación de grupos.
    - Creación, borrado y modificación de usuarios.
    - Creación, borrado y modificación de códigos QR para la generación de OTPs.
    - Creación y modificación de alertas.
    - Creación y modificación de casos.
63. Los eventos de auditoría se registran en texto plano.
64. Los eventos de auditoría se guardan permanentemente y para siempre, no estando afectados por las políticas de archivado que procesan los eventos de los dispositivos integrados de los clientes.
65. Los eventos de auditoría no pueden ser enviados a sistemas externos, sino que son almacenados en el Data Lake de la propia plataforma, al tratarse esta precisamente de un sistema distribuido de recepción y gestión de eventos de seguridad. Existe la posibilidad de exportar los eventos de auditoría para enviarlos a un sistema externo, pero esta funcionalidad se realiza bajo petición por parte de un cliente del servicio. Los eventos de auditoría solo pueden ser consultados mediante API privada, accesible únicamente desde dentro de la plataforma, previa autenticación y mediante canal seguro TLS. Tras recibir una solicitud específica para extraer eventos de auditoría, el procedimiento sería el siguiente:
    - Acceso con usuario con rol de administración a los sistemas internos de la plataforma donde corren el Data Lake.
    - Petición autenticada mediante protocolo HTTPS al API del Data Lake, realizando la consulta adecuada para extraer los eventos de auditoría deseados, que son transferidos por un canal con encriptación TLS para su extracción y envío al colector/receptor del sistema externo al que enviar dichos eventos. El túnel hacia sistemas externos se establecerá utilizando únicamente una de las siguientes combinaciones algoritmo/longitud de clave:
        - ECDHE-ECDSA-AES-256-GCM-SHA384
        - ECDHE-RSA-AES-256-GCM-SHA384

- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-ECDSA-AES-128-GCM-SHA256
- ECDHE-RSA-AES-128-GCM-SHA256

6.8.2 INTEGRIDAD DE LOS DATOS

66. ASIP utiliza un Data Lake como almacén para la indexación de todos los eventos recogidos y procesados. El Data Lake solo permite operaciones de escritura, en ningún caso de modificación de los datos indexados, garantizando así que no es posible modificar la información almacenada ya que no existen mecanismos que permitan su modificación.
67. Cada capa de almacenamiento del Data Lake está formada por varios nodos de *storage*, y es duplicada y distribuida por los nodos para garantizar que no se perderá información en caso de una contingencia relacionada con un problema de infraestructura.

6.8.3 RETENCIÓN DE DATOS

68. Las capas de almacenamiento del Data Lake donde se almacenan los eventos procesados, permiten definir políticas de retención distintas para cada cliente. Esta funcionalidad garantiza el cumplimiento de marcos regulatorios que afecten a cada cliente.
69. Por defecto se aplica la siguiente configuración para todos los clientes:
70. El Data Lake está distribuido en cuatro capas atendiendo al tiempo de retención de la información:

- **Capa hot**. La información es indexada por los nodos de esta capa y retenida durante 24 horas. La información es accesible para su consulta e investigación.
- **Capa warm**. La información pasa a esta capa a las 24 horas de ser indexada. Permanece en esta capa durante el tiempo de retención configurado para cada cliente. La información es accesible para su consulta e investigación.
- **Capa cold**. La información pasa a esta capa tras el tiempo de retención configurado para cada cliente. Permanece en esta capa antes de ser enviada a la capa de archivado. La información es accesible para su consulta e investigación.
- **Capa frozen**. Capa de archivado. La información pasa a esta capa tras el tiempo de retención configurado para cada cliente. Pasado el tiempo configurado, la información es eliminada automáticamente. La información no es accesible, pero en caso de requerir su acceso es posible restaurarla a la capa frozen para realizar una investigación sobre datos del pasado.

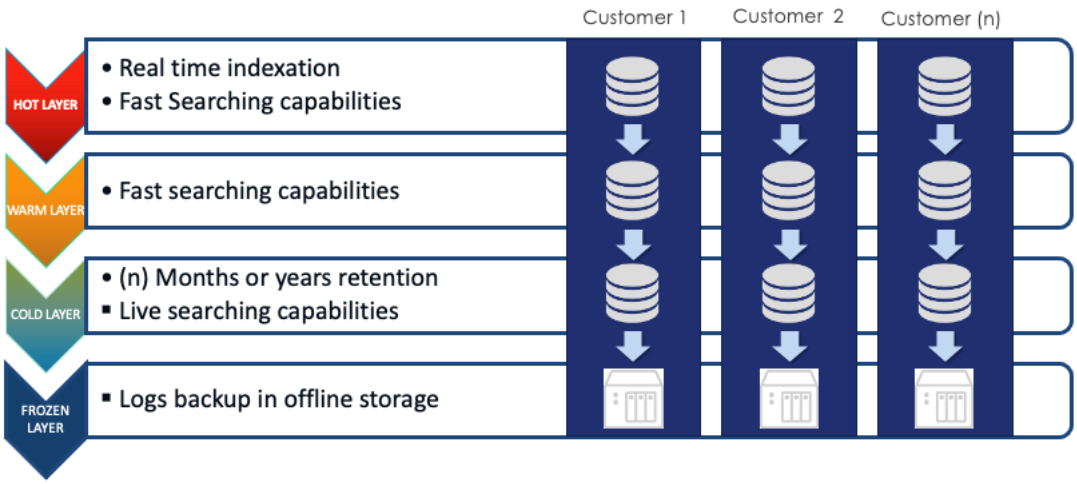

Ilustración 8. Capas de almacenamiento que componen el Data Lake

6.8.4 ENVÍO DE DATOS A SISTEMAS EXTERNOS

71. ASIP permite el envío de los eventos recibidos a sistemas externos: tanto los eventos normalizados y enriquecidos, como los eventos en bruto recibidos desde las fuentes originales.
72. Para ello el cliente solicita al servicio del SOC las características del colector donde hay que enviar los datos, indicando si quieren reenviar todos los datos o si solo quieren reenviar los eventos de un grupo concreto de fuentes.
73. Una vez recibida la solicitud, los administradores de la plataforma configuran los *adapters* de las fuentes seleccionadas para que además de indexar los eventos en el Data Lake de ASIP, se envíen también al colector especificado por el cliente.
74. La plataforma permite reenviar la información que procesa a tantas fuentes como requiera el cliente.
75. Los envíos a sistemas externos se realizan empleando el servicio de recolección y reenvío de eventos (el Forwarder). Este componente permite el envío de eventos a sistemas externos siempre estableciendo antes un túnel TLS basado únicamente en una de las siguientes combinaciones algoritmo/longitud de clave:
    - ECDHE-ECDSA-AES-256-GCM-SHA384
    - ECDHE-RSA-AES-256-GCM-SHA384
    - ECDHE-ECDSA-CHACHA20-POLY1305
    - ECDHE-ECDSA-AES-128-GCM-SHA256
    - ECDHE-RSA-AES-128-GCM-SHA256

7. REFERENCIAS

76. A continuación, se introducen las referencias empleadas a lo largo del documento.

REF1	Google Cloud Platform https://cloud.google.com/
REF2	¿Qué es Kubernetes? https://kubernetes.io/es/docs/concepts/overview/what-is-kubernetes/
REF3	Grafana Loki https://grafana.com/oss/loki/
REF4	Interfaz web de la plataforma https://soc.aiuken.com
REF5	Guía de Instalación ASIP Forwarder – Installation Guide

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL