centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1234

Procedimiento de Empleo Seguro
Chronicle SIEM and SOAR

Mayo 2025

MINISTERIO DE DEFENSA

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

Edita:

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-25-189-8
Fecha de Edición: mayo de 2025

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 07:28:28 +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. Google Security Operations o Google SecOps es un servicio en la nube, creado como una capa especializada sobre la infraestructura de Google, diseñado para que las empresas retengan, analicen y busquen de forma privada las grandes cantidades de telemetría de seguridad y red que generan. Google Security Operations está formado por los servicios Chronicle SIEM y Chronicle SOAR. Estos servicios se desarrollan a lo largo del presente Procedimiento de Empleo Seguro.
2. Google Security Operations normaliza, indexa, correlaciona y analiza los datos para proporcionar un análisis y contexto instantáneos sobre las actividades riesgosas. Google Security Operations se puede usar para detectar amenazas, investigar su alcance y causa, y proporcionar una solución mediante integraciones precompiladas con plataformas de orquestación, respuesta y flujo de trabajo empresariales.
3. Google Security Operations te permite examinar la información de seguridad agregada de tu empresa desde hace meses o más. Usar Google Security Operations te permite buscar en todos los dominios a los que se accede en tu empresa. Puedes limitar tu búsqueda a cualquier activo, dominio o IP específico para determinar si hubo alguna vulneración.
4. La plataforma de Google Security Operations permite a los analistas de seguridad analizar y mitigar una amenaza de seguridad durante todo su ciclo de vida mediante las siguientes capacidades:
    a) **Recopilación**: Los datos se transfieren a la plataforma con reenvío, analizadores, conectores y webhooks.
    b) **Detección**: Estos datos se agregan, se normalizan con el modelo universal de datos (UDM) y se vinculan a las detecciones y la inteligencia contra amenazas.
    c) **Investigación**: Las amenazas se investigan a través de la administración de casos, la búsqueda, la colaboración y las analíticas centradas en el contexto.
    d) **Respuesta**: Los analistas de seguridad pueden responder rápidamente y proporcionar resoluciones con las guías automatizadas y administración de incidentes.

1.1 DESCRIPCIÓN GENERAL DE SIEM DE GOOGLE SECURITY OPERATIONS

5. **Chronicle SIEM (*Security Information and Event Management*)** es un servicio cloud de las Google Security Operations creado como una capa especializada sobre infraestructura central de Google, diseñada para que las empresas retengan, analicen y busquen en las enormes cantidades de seguridad y telemetría de red que generan. Google Security Operations normaliza, indexa, correlaciona y analiza los datos para proporcionar análisis y contexto instantáneos sobre la actividad riesgosa.
6. Google Security Operations permite examinar la información de seguridad agregada de tu empresa que se remonta a varios meses atrás o más. Se puede limitar la búsqueda a cualquier activo, dominio o dirección IP específicos para determinar si se ha producido algún compromiso.

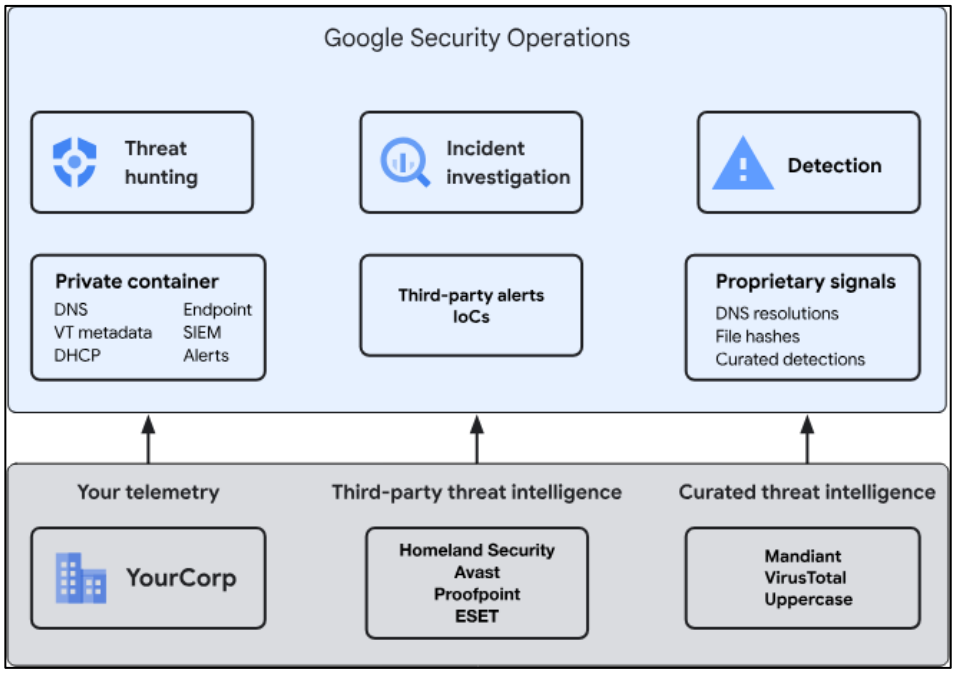

Ilustración 1 – Descripción general de la plataforma de Google Security Operations

1.2 DESCRIPCIÓN GENERAL DE SOAR DE GOOGLE SECURITY OPERATIONS

7. **Chronicle SOAR (*Security Orchestration, Automation and Response*)** es una Plataforma de las Google Security Operations diseñada para ayudar a las organizaciones a detectar, investigar y responder frente a amenazas de seguridad en tiempo real. La plataforma se nutre de la infraestructura de Google Cloud y aprovecha las capacidades de aprendizaje automático de Google para automatizar y agilizar los flujos de trabajo de seguridad.

8. Google Security Operations SOAR recopila datos de diversas fuentes de seguridad, como dispositivos de red, agentes de puntos finales y fuentes de información sobre amenazas. La plataforma utiliza estos datos para identificar posibles incidentes de seguridad e iniciar acciones de respuesta. Chronicle SOAR también se integra con otras herramientas de seguridad como SIEM, plataformas de inteligencia sobre amenazas y escáneres de vulnerabilidades para proporcionar una solución de seguridad integral.

9. La plataforma ofrece una interfaz de usuario intuitiva que permite a los analistas de seguridad investigar incidentes, crear flujos de trabajo y automatizar acciones de respuesta sin necesidad de tener amplios conocimientos de codificación. Google Security Operations SOAR también utiliza el aprendizaje automático para mejorar su precisión y velocidad a la hora de identificar y responder a incidentes de seguridad. Las capacidades de respuesta automatizada de la plataforma ayudan a las organizaciones a reducir el tiempo necesario para detectar y responder a las amenazas de seguridad, reduciendo así el riesgo de filtraciones de datos y otros incidentes de seguridad.

10. Google Security Operations SOAR es una potente plataforma de orquestación, automatización y respuesta de seguridad que ayuda a las organizaciones a mejorar su postura de seguridad mediante la automatización de los flujos de trabajo de seguridad, la reducción de los tiempos de respuesta y la mejora de la precisión de las operaciones de seguridad.

2 OBJETO Y ALCANCE

11. Procedimiento de Empleo Seguro (PES) se desarrolla para los servicios de Google Chronicle SIEM y Chronicle SOAR, los cuales forman parte de las Google Security Operations.

    a) El servicio **Chronicle SIEM** sigue la taxonomía del Anexo B.6 de la guía CCN-STIC-140, correspondiente a los sistemas de información de seguridad y gestión de eventos (SIEM). **No aplica una versión evaluada** específica en este PES dada la naturaleza en nube del servicio.

    b) El servicio **Chronicle SOAR** sigue la taxonomía del Anexo B-9 de la guía CCN-STIC-140, correspondiente a los servicios de *Security Orchestration, Automation and Response* (SOAR). La versión evaluada para este servicio es la **6.3.4.2**.

12. El alcance de este documento cubre las recomendaciones y medidas de seguridad necesarias para el despliegue y configuración segura de ambos servicios en entornos empresariales.

13. El producto Chronicle SIEM ha sido cualificado en el catálogo CPSTIC para categoría ENS ALTA.

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado **4**. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

b) Apartado **5**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

c) 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.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

14. Las Operaciones de seguridad de Google están diseñadas para funcionar exclusivamente con los navegadores Google Chrome o Mozilla Firefox. Google recomienda actualizar el navegador Google Chrome a la versión más reciente.
15. Para poder acceder a los servicios Chronicle SIEM y SOAR es preciso contactar con Google para solicitar acceso a la organización que precise el uso de estos servicios y las funcionalidades de seguridad que ofrecen. El contacto es, generalmente, a través del formulario disponible para ello.
16. Una vez registrado el subdominio de la organización que desea hacer uso de las Google Security Operations, se siguen los siguientes pasos:
    a) Iniciar el navegador Chrome o Firefox.
    b) Tener acceso a la cuenta corporativa.
    c) Para acceder a la aplicación de Google Security Operations, donde ***customer_domain*** es el identificador del dominio del cliente, navega a la siguiente dirección:

       *https://**customer_subdomain**.backstory.chronicle.security*

4.2 ENTORNO DE INSTALACIÓN SEGURO

17. Los servicios de Google Security Operations, SIEM y SOAR, no necesitan ser instalados en ninguna arquitectura o centro de procesado de datos (CPD) en el dominio del cliente usuario de estas soluciones.
18. Estos servicios están protegidos por el entorno de Google, incluyendo su infraestructura y personal, de modo que el acceso a las funcionalidades se proporciona vía navegador a través del subdominio creado para la organización.

4.3 REGISTRO Y LICENCIAS

19. Google Security Operations está disponible en diferentes paquetes basados en la ingestión. Los tipos de paquetes, funcionalidad incluida y precios asociados pueden consultarse en la página web de estos servicios de Google.
20. El paquete que ha sido evaluado para la inclusión en el Catálogo de Productos STIC (CPSTIC) ha sido la versión **Enterprise**. Todas las funcionalidades que proporciona esta versión quedan declaradas en el enlace anteriormente indicado.
21. La licencia de uso de estos servicios viene determinada por las condiciones del contrato de precios tras contactar con el equipo de ventas de Google.

4.4 CONSIDERACIONES PREVIAS

22. Para la configuración relativa a la seguridad, previa a la instalación y configuración de estos servicios de Google, no se precisa de algún aspecto adicional, aparte de las

consideraciones necesarias para el entorno operacional o la propia configuración de los servicios.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

23. Los servicios Chronicle SIEM y Chronicle SOAR, que forman parte de Google Security Operations, requieren de una serie de componentes clave en el entorno de operación para asegurar su correcto funcionamiento y cumplir con los estándares de seguridad. Estos componentes son esenciales para garantizar una gestión segura de los eventos, la orquestación y automatización de respuestas ante incidentes de seguridad.
24. Estos componentes se integran en el entorno de operación de los servicios Chronicle, garantizando una configuración segura y un cumplimiento estricto de las normativas aplicables para la protección de la información sensible.
25. El servicio **Chronicle SIEM** opera con los siguientes componentes en su entorno operacional:
    a) **Fuentes de datos externas** soportadas por Chronicle SIEM para la ingesta de datos. La documentación oficial ofrece un detalle completo sobre las fuentes soportadas.
26. El servicio **Chronicle SOAR** opera con los siguientes componentes en su entorno operacional:
    a) **Integraciones externas con fuentes de datos o sistemas de respuesta** a través de conectores y acciones. Una vez configurados los conectores, la integración ofrece una ingesta de datos hacia SOAR. Respecto a las acciones, una vez configuradas, las integraciones actúan como un sistema de respuesta, proporcionando capacidad de automatizar funcionalidad. La documentación oficial especifica la posible integración con "*Emailv2*", de acuerdo con la configuración evaluada para este servicio.
27. Dado que ambos son servicios parte de Google Security Operations, existen varios componentes del entorno operacional comunes a ambos, listados a continuación:
    a) **Usuarios finales autorizados** a gestionar la funcionalidad de seguridad de Chronicle SIEM/SOAR a través de la interfaz web, denominada *SecOps Console*. Esta consola es accesible a través del navegador usando el enlace de dominio especificado en la sección **4.1 ENTREGA SEGURA DEL PRODUCTO**.
    b) Servicios de la plataforma cloud de Google (GCP), que incluyen:
        i. **Looker (Google Cloud Core)** es una solución de la infraestructura de Google para proporcionar análisis y visualización de los datos a través de dashboards auto generados.
        ii. **Cloud Logging** para gestionar los eventos auditados de las funcionalidades de seguridad.
        iii. **Google Cloud Identity** como servicio de la infraestructura de Google, que ejerce como proveedor de identidad para acceso de usuarios autorizados a la consola *SecOps*. La configuración evaluada se realizó con la integración de la federación de Workforce Identity, según queda especificado en la documentación oficial. Adicionalmente, los usuarios de esta federación deben ser asociados a roles concretos de *Chronicle* para proporcionar control de acceso que ofrece Google IAM (*Identity and Access Management*).

iv. **Google Kubernetes Engine**, como servicio de Google para orquestación donde se despliegan los servicios Chronicle.

v. **Cloud SQL** que actúa como base de datos interna en Google para almacenamiento de auditoría.

vi. **Identity & Access Management (IAM)**. Este servicio, parte de la plataforma de Google Cloud (GCP), permite establecer el control de acceso a los recursos de GCP a través del uso de permisos.

vii. **Cloud Key Management Service (KMS)** para funcionalidades de cifrado de datos a través de claves criptográficas. Este cifrado es utilizado para protección de las bases de datos, como la información almacenada en Cloud SQL.

28. Los servicios Chronicle se ofrecen como una plataforma de software como servicio (SaaS), de forma que los clientes finales no necesitan tener acceso a los componentes del entorno operacional de la plataforma de Google (GCP) para hacer uso de la funcionalidad de SIEM y SOAR a través de la interfaz web de la consola *SecOps*.

5 FASE DE INSTALACIÓN

29. Los servicios Chronicle SIEM y SOAR no requieren instalación en el entorno del cliente usuario, debido a que se tratan de soluciones software como servicio (SaaS).

30. Una vez contactado el soporte de Google, como se indica en el apartado **4.3 REGISTRO Y LICENCIAS**, el equipo de SecOps realizará la integración de la instancia proporcionada a un proyecto de Google Cloud dentro del dominio de la organización usuaria de estos servicios. La **configuración del proyecto de Google** viene definida por la documentación oficial.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

31. Para garantizar que los servicios Chronicle operen de manera segura y conforme a los estándares de seguridad evaluados, es necesario activar configuraciones específicas que aseguren su funcionamiento en un modo de cumplimiento acorde con la cualificación realizada. En este documento se describen los pasos necesarios para configurar ambos servicios de acuerdo con las guías del CCN.

32. Las siguientes **consideraciones** deben tenerse en cuenta a la hora de hacer uso de la funcionalidad de seguridad que proporciona el servicio **Chronicle SIEM**:

    a) Para la configuración y uso de la API de ingesta, un representante de Chronicle proporcionará acceso a los usuarios autorizados. Adicionalmente, para la configuración evaluada no se incluyó la "*Backstory API*" debido a que es una API *legacy*, y su funcionalidad equivale a la Chronicle API evaluada.

    b) Es preciso crear un *feed* de datos de acuerdo con las recomendaciones de la documentación oficial. Estos *feeds* son precisos para recibir los datos de una fuente externa para su posterior procesamiento.

33. Las siguientes **consideraciones** deben tenerse en cuenta a la hora de hacer uso de la funcionalidad de seguridad que proporciona el servicio **Chronicle SOAR**:

    a) Google se encarga de proporcionar el entorno donde los usuarios finales harán uso de las funcionalidades de seguridad de SOAR. Una vez el acceso esté configurado para estos usuarios, es posible que haya usuarios ya creados en la instancia Chronicle del dominio registrado. Se recomienda eliminar estos usuarios y crear nuevos que sean autorizados.

    b) Para proporcionar acceso a la API de Chronicle SOAR, se recomienda a los administradores crear una nueva API key. Adicionalmente, se pueden generar nuevas API keys conforme sea necesario para cumplir estándares de seguridad.

    c) La configuración evaluada contempló el uso de "*Email V2*" como fuente de datos y sistema de respuesta al mismo tiempo, pero haciendo uso de conectores y acciones por defecto. Para realizar esta integración, se han tenido en cuenta las siguientes consideraciones:

        i. Se ha instalado la integración desde el Marketplace.

        ii. La configuración de la integración tuvo en cuenta la activación de los parámetros "*SMTP – Use SSL*", "*IMAP – Use SSL*" and "*SMTP – Use Authentication*" para proporcionar comunicaciones TLS seguras (v1.2 o superior).

        iii. Se configuró el conector para ingesta de datos.

34. La residencia de los datos se garantiza por los términos de servicio de Google Cloud para los servicios Chronicle. La configuración evaluada consideró la **Unión Europea** como localización de estos datos.

6.2 AUTENTICACIÓN

35. Google ofrece servicios como Cloud Identity, Google Workspace o una identidad de terceros (como Okta o Azure AD) para administrar los usuarios, los grupos y la autenticación. No obstante, **Google recomienda hacer uso del proveedor de identidad Cloud Identity** para realizar la autenticación de las principales que accedan a la consola de Chronicle SIEM y SOAR.

36. La configuración de este proveedor de identidad se realiza siguiendo los pasos declarados en la documentación oficial de Google.

37. Para la autenticación de los servicios Chronicle SIEM y SOAR con otras entidades en su entorno operacional, se hace uso de **certificados digitales**. Estos certificados quedan definidos en la sección **6.4 GESTIÓN DE CERTIFICADOS**.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

38. La administración de los servicios Chronicle se puede realizar remotamente a través de su API o mediante la interfaz web accesible por el navegador. Esta segunda vía es la recomendada por Google para que los usuarios puedan administrar las funcionalidades de seguridad de estos servicios. El acceso a esta interfaz web, denominada **consola *SecOps***, viene definido en la sección **4.1 ENTREGA SEGURA DEL PRODUCTO**.

39. Las interfaces de acceso remotas a la consola SecOps para los servicios Chronicle ofrecen comunicaciones seguras a través de los protocolos **QUIC** o **HTTPS**, siempre haciendo uso de **TLS v1.2** o **v1.3**.

40. La conexión a esta consola debe realizarse desde un equipo configurado con un navegador que soporte exclusivamente las **suites de cifrado TLS aceptadas para categoría Alta de ENS**. El navegador utilizado por los usuarios autorizados para este fin que accedan, vía web, a la consola SecOps, debe tener **configurado el uso de suites de cifrado seguras de acuerdo con aquellas permitidas por las guías de criptografía segura CCN-STIC-807**. No se recomienda el uso de cualquier otra suite de cifrado no contemplada en las guías de CCN.

41. No se ofrece administración local dada la naturaleza SaaS de los servicios Chronicle, pertenecientes a las Google Security Operations. Esta administración queda delegada al personal autorizado de la infraestructura de Google.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

42. La documentación oficial de Google define los **roles de los servicios Chronicle como un conjunto de permisos que permite ejercer funcionalidad de seguridad según el alcance del acceso que tenga sobre un recuso determinado**. Estos permisos vienen definidos por los proporcionados en la referencia de IAM.

43. La API de Chronicle sigue el paradigma de diseño orientado a recursos. Este modelo permite el control de acceso a las características de Chronicle haciendo uso de IAM.

44. Los permisos de IAM definen el acceso específico a los métodos de Chronicle, donde cada método representa una acción que se aplica a un determinado recurso.

45. En la documentación oficial de Chronicle se puede acceder a la definición completa de los permisos de IAM, su descripción y roles predefinidos a los que están asociados.

46. La configuración de los roles y permisos se puede realizar desde la consola SecOps de los servicios Chronicle, donde los administradores autorizados pueden crear roles para varios propósitos, tareas y accesos. La descripción completa de cómo **trabajar con roles** viene descrita en la documentación oficial de Google.

47. Al hacer uso de la federación de Workspace de Google para la integración de **Cloud Identity** como proveedor de identidad que gestiona el conjunto de usuarios que pueden acceder a los servicios Chronicle, todos los parámetros de autenticación quedarán delegados en este servicio de Google.

48. Cloud Identity es el servicio encargado de la configuración segura de políticas de contraseñas de los usuarios federados.

49. Los servicios Chronicle SIEM y SOAR, a través de la consola *SecOps*, tienen establecido un **tiempo máximo de sesión de tres horas** en caso de detectar inactividad. Pasado ese tiempo, si las condiciones de inactividad se cumplen; por ejemplo, no realizar ninguna acción administrativa durante ese intervalo, la sesión del usuario se cierra.

6.4 GESTIÓN DE CERTIFICADOS

50. Los usuarios finales que se beneficien del uso de los servicios Chronicle SIEM y SOAR, no precisan de configuración de certificados digitales para autenticación de los canales de comunicación con la consola *SecOps* para funcionalidades de administración o autenticación con otros servicios y componentes del entorno operacional.

51. Existen dos tipos de autenticación a través de los certificados gestionados por Google:

    a) Autenticación con otros servicios dentro del entorno de la plataforma cloud de Google (GCP):

        i. Mediante certificados SSL con longitud de clave de 256 bits y esquema ECDSA.

    b) Autenticación con otras entidades externas del entorno operacional fuera de GCP:

        i. Mediante seguridad de transporte de la capa de la aplicación de Google (ALTS).

52. Los clientes son responsables de notificar a su gestor de cuenta/contacto de ventas de Google los algoritmos criptográficos y certificados por CCN durante el proceso de incorporación del cliente.

53. Los mecanismos de autenticación anteriormente mencionados son los únicos recomendados para un uso seguro de los servicios Chronicle.

6.5 SINCRONIZACIÓN

54. Las marcas de tiempo, o *timestamps*, que utiliza el servicio Chronicle SIEM para los eventos y detecciones vienen dadas por el sistema de marcas de tiempo interno de la infraestructura de Google. Estas marcas de tiempo son confiables y vienen definidas en la documentación oficial.

55. El usuario final que haga uso de este servicio no tiene que configurar ninguna integración con un servicio NTP ya que Google es encargado de gestionar esta configuración con sus sistemas internos.

6.6 ACTUALIZACIONES

56. Los servicios **Chronicle SIEM** y **Chronicle SOAR** de Google Security Operations operan bajo un modelo de servicio cloud, lo que significa que las actualizaciones de software y parches de seguridad no requieren intervención directa por parte del usuario final. **Google** gestiona de manera centralizada todas las actualizaciones, asegurando que los servicios siempre se mantengan en las versiones más recientes y seguras.

57. Google hace uso de estrictos controles de acceso y del servicio *Security Command Center* (SCC) para la gestión segura de las actualizaciones.

58. Aunque Google se encarga de las actualizaciones de estos servicios cloud, el usuario final es responsable de mantener actualizados otros sistemas o componentes que interactúen con Chronicle SIEM y SOAR y estén bajo su dominio, como son los equipos y navegadores desde donde se accede a la consola *SecOps*.

6.7 AUTO-CHEQUEOS

59. Dado que **Chronicle SIEM** y **Chronicle SOAR** de Google Security Operations son servicios SaaS (Software as a Service), los auto-chequeos y el monitoreo de integridad del sistema se gestionan de manera centralizada por Google. Estos servicios están diseñados para funcionar continuamente, con procesos automáticos que garantizan su rendimiento, integridad y disponibilidad sin necesidad de intervención directa por parte del usuario final.

6.8 ALTA DISPONIBILIDAD

60. Los servicios **Chronicle SIEM** y **Chronicle SOAR** de Google Security Operations están diseñados para ofrecer alta disponibilidad mediante la implementación de arquitecturas cloud redundantes, asegurando que los usuarios puedan acceder a los servicios de manera continua, sin interrupciones. La gestión de la alta disponibilidad es una responsabilidad directa de Google, que garantiza la operatividad de los servicios a través de diversas estrategias.

61. La combinación de redundancia geográfica, balanceo de carga y capacidades avanzadas de recuperación ante desastres asegura que los usuarios puedan confiar en que los servicios estarán disponibles en todo momento.

62. En caso de que se produzca una interrupción, Google gestiona el proceso de recuperación, asegurando que el servicio vuelva a estar operativo lo más rápido posible sin intervención del usuario final.

6.9 AUDITORÍA

6.9.1 REGISTRO DE EVENTOS

63. Los servicios **Chronicle SIEM** y **Chronicle SOAR** proporcionan un registro exhaustivo de eventos, que es crucial para la auditoría, la supervisión de seguridad y el cumplimiento normativo. Estos registros capturan todas las acciones relevantes dentro de los sistemas, permitiendo a los administradores y equipos de seguridad llevar un seguimiento detallado de las actividades y potenciales incidentes.

64. Los servicios Chronicle se proporcionan mediante una plataforma SaaS. Los clientes no tienen acceso a los componentes y registros de la infraestructura, solamente a los registros de nivel de plataforma a través de la interfaz de usuario de la consola *SecOps*.

65. Toda la información sobre los registros de auditoría de las Google Security Operations queda definida en la documentación oficial.

6.9.2 ALMACENAMIENTO REMOTO

66. El almacenamiento de auditoría se realiza de forma interna en la infraestructura de Google. Los servicios Chronicle son parte de una plataforma SaaS, por lo que el almacenamiento de los eventos auditados se realiza de forma remota.

67. Los registros de eventos se transmiten a los servidores remotos, dentro de la infraestructura de Google, mediante protocolos cifrados garantizando que los datos no sean interceptados ni alterados durante el proceso de transmisión. La protección de este canal se realiza a través del protocolo TLS 1.2 o superior.

7 REFERENCIAS

[DGSO] Documentación de los servicios Chronicle SIEM y SOAR
Documentación Google Security Operations (Chronicle)

[DGC] Documentación general de todos los servicios de Google Cloud
Documentación de Google Cloud

8 ABREVIATURAS

ALTS	Application Layer Transport Security
API	Application Programming Interface
CCN	Centro Criptológico Nacional
CCN-STIC	Centro Criptológico Nacional - Seguridad de las Tecnologías de la Información y las Comunicaciones
CPD	Centro de Procesamiento de Datos
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación
ECDSA	Elliptic Curve Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad.
GCP	Google Cloud Platform
HTTPS	HTTP over TLS
IAM	Identity & Access Management
IMAP	Internet Message Access Protocol
KMS	Key Management Service
NTP	Network Time Protocol
PES	Procedimiento de Empleo Seguro
QUIC	Quick UDP Internet Connections
SaaS	Software as a Service
SCC	Security Command Center
SecOps	Security Operations
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol
SOAR	Security Orchestration, Automation and Response
SQL	Structured Query Language
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UDM	Unified Data Model

PUBLICACIONES DE DEFENSA

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