centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1649

Procedimiento de Empleo Seguro
TrustCloud VideoID

Octubre 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: 083-26-136-7

Fecha de Edición: Octubre de 2025

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.05.05 13:09:31 +02'00'

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. La plataforma Trustcloud es una plataforma que organiza transacciones digitales seguras, también conocida como un “Coreógrafo de Transacciones digitales seguras”.
2. TrustCloud VideoID es una solución SaaS de video identificación segura que permite a las empresas verificar la identidad de sus clientes de forma remota y en tiempo real, a través de llamadas automáticas (video selfie) o asistidas.
3. La tecnología ofrece múltiples capas de autenticación, garantizando seguridad, fluidez y una experiencia de usuario óptima, tanto para el alta de empresa como el de usuario final, poniendo especial atención a aquellos usuarios menos habituados a los procesos digitales.

2 OBJETO Y ALCANCE

4. Esta guía es de aplicación para la versión v.4 del servicio TrustCloud VideoID alojado en el proveedor de servicios en la nube de Amazon (AWS) [REF1].
5. Se trata de una plataforma a la que se accede mediante API-REST, y mediante el Orquestador se gestionan los distintos servicios a proporcionar al Caso de Uso correspondiente.
6. El objetivo de este documento es servir como una guía para realizar una instalación, configuración y operación segura del producto TrustCloud VideoID 4.0.
7. El servicio TrustCloud VideoID ha sido cualificado en el catálogo CPSTIC para categoría ENS ALTA en la familia “Herramientas de videoidentificación”.

3 ORGANIZACIÓN DEL DOCUMENTO

a) Apartado **¡Error! No se encuentra el origen de la referencia.**. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

b) Apartado **¡Error! No se encuentra el origen de la referencia.**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

c) Apartado **¡Error! No se encuentra el origen de la referencia.**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

d) Apartado **¡Error! No se encuentra el origen de la referencia.**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

8. Al tratarse de un servicio alojado en la nube, se dará de alta los datos del cliente y se enviarán de forma segura los accesos pertinentes al producto.
9. La entrega se realiza mediante el correo electrónico corporativo support@trustcloud.tech, en un documento cifrado y su contraseña vía SMS.
10. Es posible verificar la autenticidad de dicho correo electrónico empleando la herramienta GpgOL (extensión de firma y cifrado de correos).

4.2 ENTORNO DE INSTALACIÓN SEGURO

11. Al tratarse de un servicio alojado en la nube, se provisionan recursos y se generan los accesos a la plataforma donde opera el producto, a través de la creación de Casos de Uso.

4.3 REGISTRO Y LICENCIAS

12. Los servicios prestados son mediante contratación, por lo que no es necesaria la instalación o configuración de ningún tipo de licencia. Se dará de alta los datos del cliente y se enviarán de forma segura los accesos pertinentes al producto.

4.4 CONSIDERACIONES PREVIAS

13. Al tratarse de un servicio alojado en la nube, la principal consideración previa es tener conexión a internet y estar dado de alta en el sistema para hacer uso del producto.
14. El equipo a emplear para acceder al servicio alojado en la nube deberá tener al menos las siguientes características:
    - Sistema Operativo: Windows Server 2019.
    - Procesador con una potencia de, al menos, dos núcleos a 2.5GHz.
    - Memoria RAM de, al menos, 4 GB.
    - Memoria de disco de, al menos, 30 GB.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

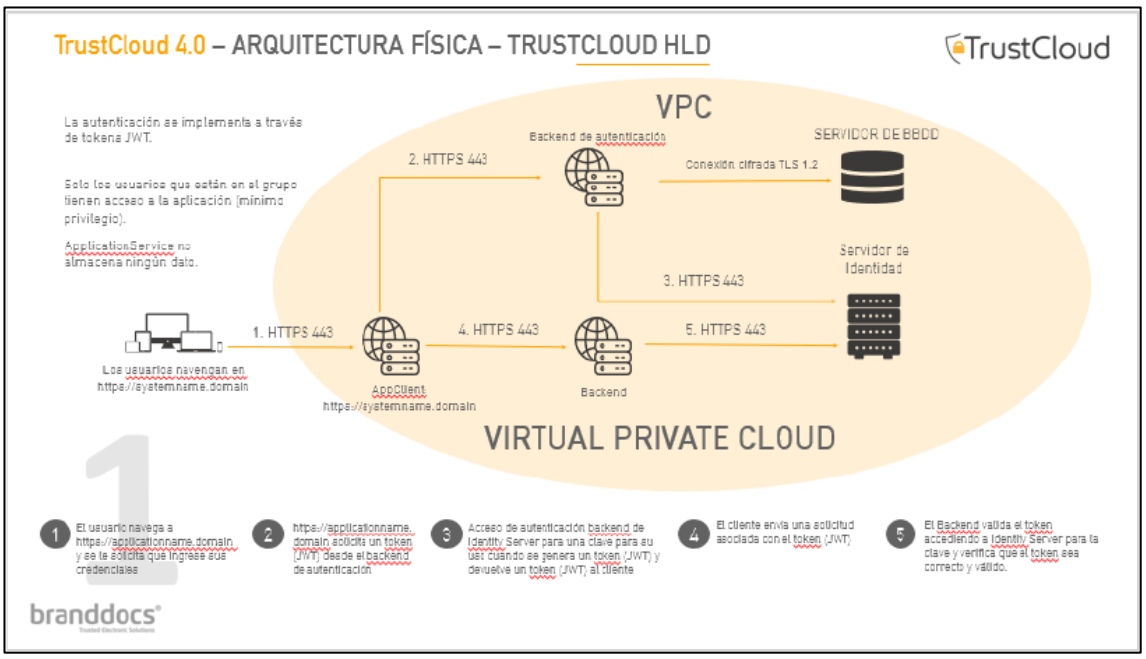

Ilustración 1. Trustcloud High-Level Design

15. El producto es un producto SaaS (*Software as a Service*) que corre en una infraestructura privada en AWS:

    - Las instancias EC2 de AWS corren empleando Sistemas Operativos Amazon LINUX 3. Dichas instancias consisten en servidores ubicados en la nube de AWS, destinados a la ejecución de código.
    - Las bases de datos relacionales AWS RDS (*Amazon Relational Database*, Servicio de bases de datos relacionales) [REF6] se ejecutan en SQL Server 2017.
    - Las bases de datos NoSQL son administradas con DynamoDB [REF7].
    - Las bases de datos para Caché emplean Redis (*Remote Dictionary Server*) [REF3].

5 FASE DE INSTALACIÓN

16. Al tratarse de un servicio en la nube, lo único que se requiere para ser utilizado es que el proveedor del servicio asigne un usuario en el sistema.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

17. Los componentes (servicios) de la Plataforma TrustCloud están disponibles a través de una única interfaz mediante la exposición de un API-REST.

18. A continuación, se muestra el esquema general de la Plataforma TrustCloud 4.0, donde se indica que hay un único punto de entrada a la plataforma (API-REST mencionada) y la existencia de los módulos *Orquestador* y *Core*, que se encargan de realizar las orquestaciones necesarias: en este caso desde el orquestador se invocará al servicio *TrustCloud Sign* [REF8] para realizar la firma de los documentos y a *TrustCloud Vault* [REF9] para custodiar las evidencias generadas durante el proceso.

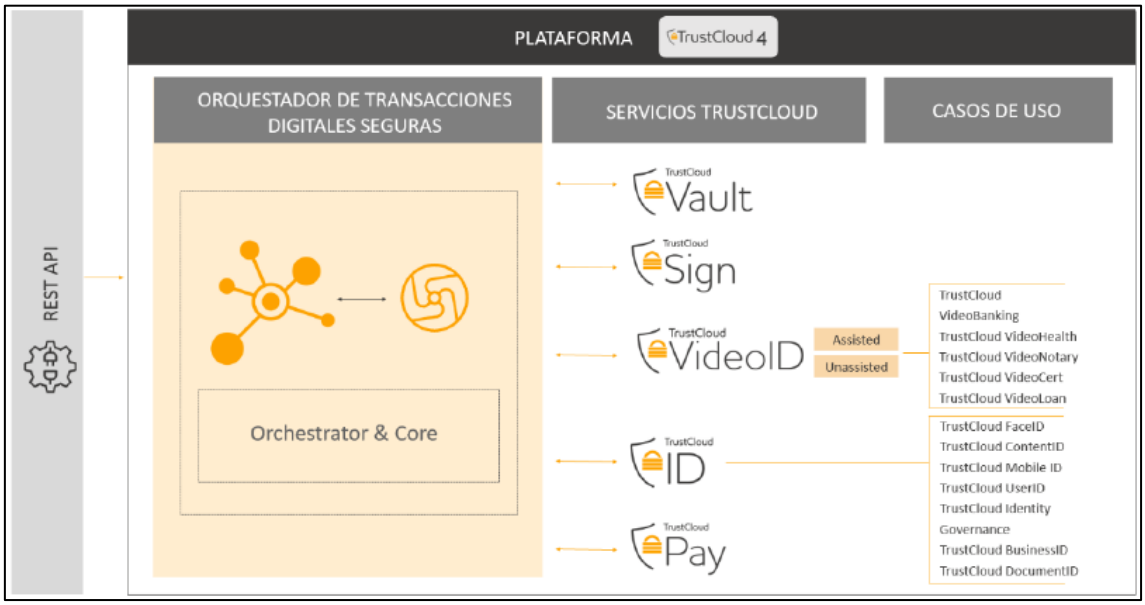

Ilustración 2. Esquema General Plataforma Trustcloud

19. Al tratarse de un servicio en la nube, no existen unos pasos para activar la configuración específica del producto para que este opere en un modo de funcionamiento considerado seguro. Esta configuración ya se adopta por defecto a la hora del alta del servicio en la plataforma.

6.2 AUTENTICACIÓN

20. La identificación, autorización y autenticación de las peticiones API-REST se realizará utilizando *tokens JWT*. Para ello antes de realizar cualquier petición al API del Orquestador de Transacciones, se deberá de pedir un token al Servidor de Autorizaciones.

21. Se identifica y autentica a cada cliente de la API antes de otorgar acceso.

22. Los operadores (***Administrador*** y al ***Administrador de Soporte***) pueden acceder a la aplicación de Administración mediante usuario y contraseña (*Login*) y cookies seguras.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

23. Al tratarse de un servicio en la nube, la administración del producto se realiza de forma remota utilizando el protocolo seguro HTTPS, con TLSv1.2 o superior para crear un canal cifrado para el tráfico de información sensible. Por defecto, no están habilitados los protocolos inseguros en el entorno de producción: TLS 1.1, TLS 1.0, SSLv2 y SSLv3.

24. Las suites de cifrado aceptadas por el producto son:

    - TLS_RSA_WITH_AES_128_CBC_SHA256
    - TLS_RSA_WITH_AES_256_CBC_SHA256
    - TLS_RSA_WITH_AES_128_GCM_SHA256
    - TLS_RSA_WITH_AES_256_GCM_SHA384
    - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
    - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
    - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

25. Está establecida la siguiente política de contraseñas. Dicha política de contraseñas es fija y configurada por el proveedor del servicio:

    - La longitud mínima de la contraseña es de 8 caracteres. Se recomienda establecer una longitud mínima de 12 caracteres para la contraseña.
    - Requerir al menos una letra mayúscula del alfabeto latino (A-Z)
    - Requerir al menos una letra minúscula del alfabeto latino (a-z)
    - Requerir al menos un número
    - Requerir al menos un carácter no alfanumérico (! @ # $ % ^ & * ( ) _ + - = [ ] { } | ')
    - La contraseña caduca en 30 días. Este valor es configurable. Se recomienda establecer un valor de 60 días.
    - Permitir que los usuarios cambien su propia contraseña

26. Es posible establecer un umbral de intentos fallidos de autenticación, a través de lAs políticas de seguridad establecidas en AWS IAM. La política establecida obliga a meter 2 códigos de autenticación de MFA (*Multi-Factor Authentication*) tras 3 intentos de autenticación fallidos. Posteriormente, el usuario deberá volver a introducir correctamente su usuario y contraseña, y un nuevo código de MFA. También es posible establecer el acceso a través de una llave FIDO2.

27. Asimismo, es posible establecer un cierto número de contraseñas anteriores que no podrán ser repetidas de nuevo. La contraseña no se podrá reuitilizar por lo menos en los próximos 5 cambios de contraseña.

28. En el primer inicio de sesión se deben de cambiar esas credenciales en los casos que sean por defecto, o no tengan credenciales asignadas previamente.

29. Para los clientes de la API, el producto garantiza su autorización mediante *cookies*, que garantizarán el inicio de sesión exitoso, y el *token JWT,* generado en la fase de autenticación que garantiza los permisos. El tiempo de uso del token es de 60 minutos.

30. El servidor de Tokens que está dentro de la arquitectura del servicio IDP de la plataforma permite ajustar el tiempo de uso de un token cambiando una propiedad en la configuración de dicho servicio permitiendo valores por minutos. Actualmente está establecido en 60 minutos.
31. Se tiene la capacidad de crear usuarios con permisos de administración. Es el usuario Administrador el que tiene la capacidad de crear otros usuarios Administradores de Soporte.
32. Una vez que un usuario es autenticado y autorizado si su perfil lo permite porque cuenta con el rol de administrador puede crear nuevos usuarios basado en las políticas ACL que gestionan los permisos sobre recursos sobre los que dicho usuario tiene permisos.
33. Esta infraestructura se implementa con base en una arquitectura de lista de control de acceso (LCA). Una LCA es una lista de reglas que especifica qué identidades de usuario tienen acceso a una aplicación o recurso de aplicación en particular. En este caso, un usuario con rol de administrador puede acceder a recursos de administración sobre la aplicación en concreto para acceder a determinados recursos.

    Para poder crear usuarios y gestionar sus permisos el usuario administrador cuenta con una herramienta web que le permite crear, editar, borrar y asignar permisos a usuarios sobre los que tiene privilegios de administración, así como para poder definir acceso a recursos de la plataforma a dichos usuarios.
34. Solo el usuario administrador puede llevar a cabo las siguientes funciones:
    - Administración del producto de forma remota
    - Configuración del Caso de Uso
35. Para los operadores (***Administrador*** y al ***Administrador de Soporte***) la sesión web de la aplicación de Administración se cierra a los 60 minutos. La aplicación de Administración es solo para usuarios administradores, que son los que se ven afectados por el cierre de sesión de UI.
36. El rol "***Administrador***" es el administrador inicial que se crea. A partir de este rol se creará el resto de los usuarios administradores ("***Administradores de Soporte***"). El usuario Administrador se crea a partir de la aplicación web de administración, con una herramienta denominada "*Data Seeder*".

6.3.2.1 GESTIÓN DE USUARIOS

37. El usuario con rol Administrador a través de la herramienta web de administración una vez es autenticado y autorizado accede a la sección de gestión de usuarios:

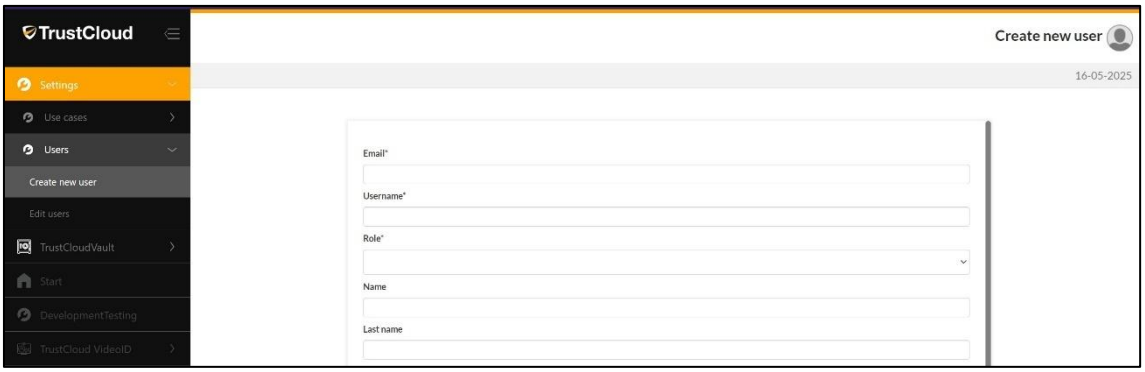

Ilustración 3. Gestión de usuarios (añadir usuario)

38. Puede cumplimentar los datos del perfil del usuario que desea crear y el rol de dicho usuario:

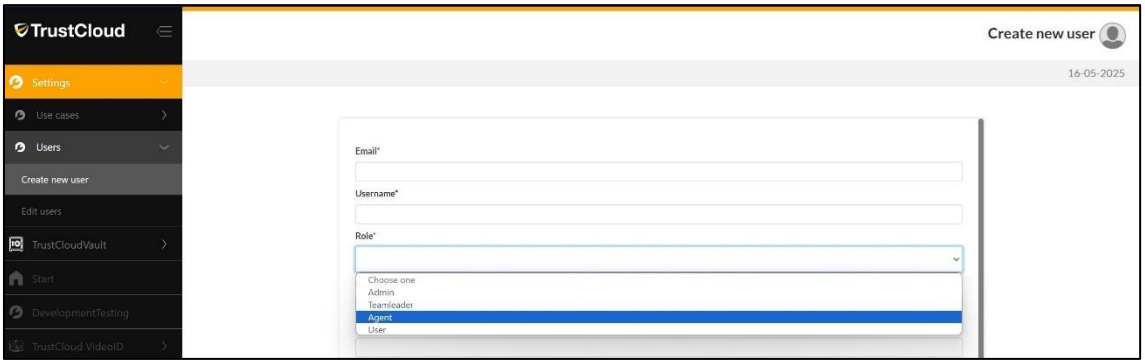

Ilustración 4. Selección de rol de usuario

39. Una vez los datos son cumplimentados el usuario recibirá una invitación vía email para poder verificar su cuenta y establecer la contraseña. A partir de ese momento el nuevo usuario tendrá acceso a los recursos que se hayan definido en su perfil de usuario como por ejemplo ser un video agente.

40. El usuario administrador puede editar otros usuarios sobre los que tiene privilegios para controlar sus permisos o gestionar su perfil:

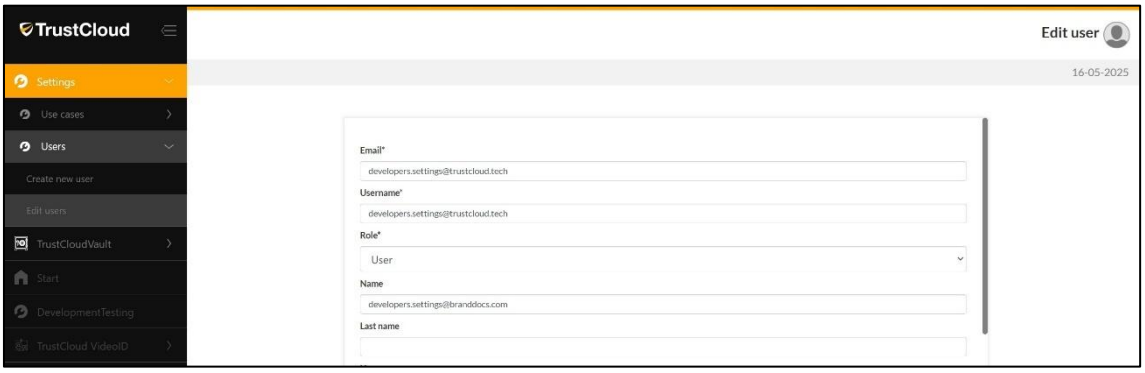

Ilustración 5. Modificación de usuario

41. Se puede otorgar permisos a recursos:

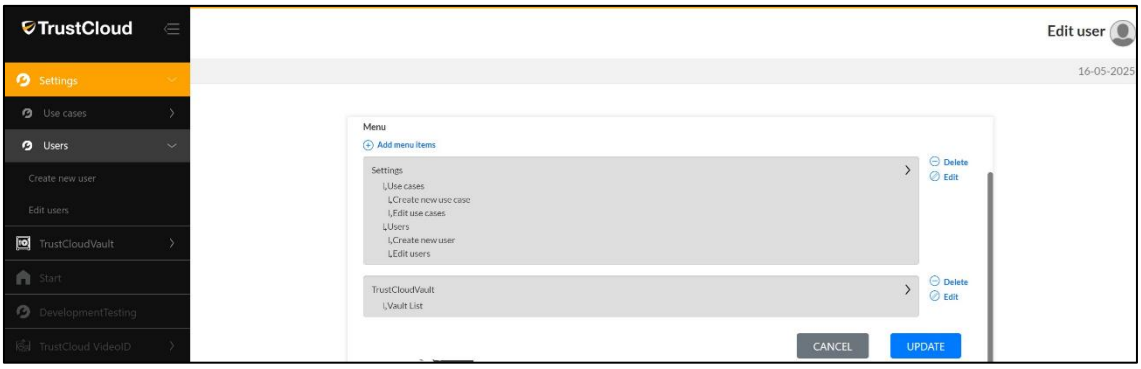

Ilustración 6. Modificación de permisos de usuario

42. De esta manera un usuario administrador puede controlar la parte IAM de un usuario dentro de la plataforma.

6.3.2.2 TIEMPO DE EXPIRACIÓN DE SESIONES

43. El usuario no tiene capacidad de controlar el tiempo de expiracion de la sesión. Esta sesión se controla del lado backend o desarrollo y atiende a criterios de seguridad.

44. Al autenticar la identidad de un usuario, el sistema crea una sesión donde la identidad raíz (UserId) se vincula a un ticket de autorización (AuthTicketId). Esto permite al usuario solicitar autorización para acceder a los diferentes recursos y funcionalidades de la Plataforma TrustCloud. La vinculación entre UserId y AuthTicketId se almacena en cookies seguras vinculadas al dominio de TrustCloud, que pueden almacenarse en el navegador web del usuario para mantener la sesión en las aplicaciones web de la Plataforma TrustCloud. Sin embargo, los tickets de autorización se almacenan en el servidor. Esto permite al sistema invalidar los tickets de autorización, deshabilitando cualquier cookie relacionada y, por lo tanto, cerrando cualquier sesión vinculada.

45. El ticket de autorización permite establecer un tiempo de vida del mismo que es usado para controlar el tiempo de duración de la sesión del usuario y que es configurable a través de los settings del servicio IDP estableciendo mediante propiedades la duración en minutos de dicho tiempo.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

46. Al tratarse de un servicio en la nube, todo acceso al producto ya sea mediante cliente API o web, se realiza mediante el uso del puerto 443 (HTTPS). Los demás puertos están cerrados.

6.5 GESTIÓN DE CERTIFICADOS

47. El servicio usa algoritmos asimétricos RSA (RS256) [REF10] para firmar los *tokens JWT* y funciones hash SHA256.

48. La configuración se realiza mediante *Internet Information Server*.

49. El certificado se instala en IIS y se gestiona en el almacén de Windows.

50. IdentityServer lo usa (a través de la configuración .AddSigningCredential) para firmar tokens JWT con su clave privada.

51. Esto asegura la integridad y autenticidad del token, permitiendo verificarlo con la clave pública.

6.6 SERVIDORES DE AUTENTICACIÓN

52. Toda la autenticación se realiza dentro del entorno virtual donde se aloja el servicio. Las comunicaciones están protegidas empleando el protocolo TLSv1.2.

6.7 SINCRONIZACIÓN

53. Al tratarse de un servicio en la nube, los servidores donde está alojado el servicio se sincronizan mediante el uso de NTP con el proveedor de servicios en la nube.

6.8 ACTUALIZACIONES

54. El software será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
55. El proveedor de servicios en la nube actualiza el software en sus servicios administrados, y se encarga de mantener sus sistemas actualizados sin la intervención del usuario.
56. Al tratarse de un servicio en la nube, se suben los binarios a través de un usuario con permisos de *Deployment* (acceso a la instancia EC2 de AWS y subida de código).
57. El proceso de actualización se lleva a cabo mediante RDP (*Remote Desktop Protocol*) [REF4], con usuario y contraseña e IPs restringidas para acceder. Este proceso de actualización es llevado a cabo por usuarios no administradores, pero que tienen permisos de despliegue. Los usuarios administradores son los encargados de crear y eliminar usuarios con permisos de despliegue en función de las necesidades.
58. Para más información al respecto, consultar el apartado **¡Error! No se encuentra el origen de la referencia. ¡Error! No se encuentra el origen de la referencia.**.

6.9 AUTO-CHEQUEOS

59. El proceso de chequeo es el que se realiza en entornos previos, ya que el mismo código es desplegado en el entorno de preproducción como medida previa para verificar su correcto funcionamiento. Asimismo, el proceso indicado a continuación es el proceso a seguir cuando se lleve a cabo el proceso de actualización de una AMI (Imagen de Máquina de Amazon).
60. Se usa un checklist para la correcta implantación del producto:
    - Actualización del equipo BASE con el nuevo código que se quiere añadir.
    - Generación de la AMI (Imagen de Máquina de Amazon) [REF11] de este equipo BASE.
    - Generación de una nueva versión del "*Launch Template*" con la AMI generada.
    - Aumentar la capacidad deseada en el "*Autoscaling*" provocando el despliegue de una nueva instancia actualizada.
    - Actualizar la capacidad deseada a los valores previos provocando la eliminación de la instancia con la versión anterior.

6.10 ALTA DISPONIBILIDAD

61. Al tratarse de un servicio en la nube, el proveedor de servicios en la nube brinda el servicio de alta disponibilidad sobre los servidores donde se aloja el servicio y las conexiones para el acceso al mismo.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

62. El producto registra todas las transacciones, añadiendo un sello de tiempo cualificado según el reglamento europeo EIDAS [REF5], preservando todas las evidencias necesarias para revertir la carga de la prueba. Las evidencias de las transacciones serán almacenadas en el servicio ***Trustcloud Vault***, que podrá ser invocado desde el Orquestador. Este servicio cuenta con funciones de gestión documental, búsqueda y descarga de documentos. Los documentos generados por los procesos de Trustcloud son enviados a Vault de manera automática.

63. Estos registros de auditoria contienen la siguiente información:

    - Id: identificador único de la transacción
    - ResponseId: identificador único de la transacción en el proveedor de sello de tiempo cualificado
    - ResponseContext: formato de devolución del sello de tiempo cualificado del proveedor
    - RequestContext: formato de llamada del sello de tiempo cualificado hacia el proveedor
    - RestampFrequency: tiempo de frecuencia en días para hacer el resellado
    - Date: fecha del registro del sello de tiempo cualificado
    - LTAName: nombre del proveedor de sello de tiempo cualificado
    - LTADate: fecha del sello de tiempo cualificado
    - CertificateExpiration: fecha de expiración del certificado
    - HASH: SHA256 HASH que se manda a sellar

64. Se genera información de auditoría al comienzo y finalización de las funciones de auditoría y cuando se produce alguno de los siguientes eventos. Estos eventos son gestionados por los servicios AWS CloudWatch [REF12], AWS CloudTrail [REF13], AWS SNS [REF14] y AWS SQS [REF15]:

    - Login y logout de personal autorizado.
    - Cambio en las credenciales de clientes y usuarios.
    - Cambios en la configuración del producto: creación y modificación de casos de uso
    - Eventos relativos a la funcionalidad del producto: creación, modificación y cierre de expedientes, y registro completo de las transacciones.

65. Los registros de auditoría contienen la siguiente información. Estos registros de auditoría son mantenidos por los servicios AWS CloudWatch y AWS CloudTrail.

    - fecha y hora del evento
    - tipo de evento identificado
    - resultado del evento
    - cliente/usuario que produce el evento

66. A los registros de auditoría se le aplica la siguiente política de acceso. Dicha política de accesos es configurable mediante el servicio AWS IAM [REF16]:
    - Lectura: usuarios autorizados.
    - Modificación: ningún usuario.
    - Borrado: administradores, y solo bajo petición por causa justificada

6.11.2 ALMACENAMIENTO LOCAL

67. Al tratarse de un servicio en la nube, el almacenamiento es proporcionado por el proveedor de servicios en la nube, guardándose de forma cifrada. El almacenamiento en reposo de la información se lleva a cabo mediante AWS S3, empleando para ello AES-256 bits.
68. El producto es capaz de gestionar los registros de auditoría y eliminarlos o sobrescribirlos cuando se requiera o por requerimiento legal, a través del establecimiento de períodos de retención configurables. El producto usa los servicios del proveedor de servicios en la nube que gestionan los registros de auditoría a través de su ciclo de vida.

6.11.3 ALMACENAMIENTO REMOTO

69. No hay almacenamiento remoto, todo se realiza de forma local en los servidores alojados en el proveedor de servicios en la nube.

6.12 BACKUP

70. Al ser un servicio en la nube, las copias de seguridad se realizan **diariamente** por el proveedor de servicios en la nube, a través del servicio AWS RDS [REF6].
71. Las copias de seguridad son llevadas a cabo por el proveedor de AWS, de forma semanal.

7 FASE DE OPERACIÓN

72. El correcto funcionamiento del producto requiere de unas características que deben estar presentes en el entorno operacional:

    - Se deben mantener y analizar periódicamente los registros de auditoría. Solamente el personal de seguridad autorizado podrá acceder a ellos.
    - Se deben gestionar correctamente los certificados empleados, actualizándolos cuando sea necesario, por ejemplo, al expirar.

8 REFERENCIAS

[REF1] Amazon Web Services
https://aws.amazon.com/es/

[REF2] JSON Web Tokens
https://auth0.com/docs/secure/tokens/json-web-tokens

[REF3] Amazon Web Services Elastic cache
https://aws.amazon.com/es/redis/#:~:text=Redis%2C%20que%20significa%20Remote%20Dictionary,de%20su%20empresa%20emergente%20italiana.

[REF4] Descripción del Protocolo de Escritorio Remoto (RDP)
https://learn.microsoft.com/es-es/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol

[REF5] Eidas: Reglamento Europeo de Identificación Digital
https://digital-strategy.ec.europa.eu/es/policies/discover-eidas

[REF6] AWS – RDS
https://aws.amazon.com/es/rds/

[REF7] DynamoDB
https://aws.amazon.com/es/dynamodb/#:~:text=Amazon%20DynamoDB%20is%20a%20fully,data%20import%20and%20export%20tools

[REF8] TrustCloud Sign
https://trustcloud.tech/trustcloud-platform/sign/

[REF9] TrustCloud Vault
https://trustcloud.tech/es/onboarding-tradicional/quantum-vault

[REF10] RSA (RS256)
https://auth0.com/blog/rs256-vs-hs256-whats-the-difference/

[REF11] AMI - Imagen de Máquina de Amazon
https://docs.aws.amazon.com/es_es/AWSEC2/latest/UserGuide/AMIs.html

[REF12] AWS – CloudWatch
https://aws.amazon.com/es/cloudwatch/

[REF13] AWS – CloudTrail
https://aws.amazon.com/es/cloudtrail/

[REF14] AWS – SNS (Simple Notification Service)
https://aws.amazon.com/es/sns/

[REF15] AWS – SQS (Simple Queue Service)
https://aws.amazon.com/es/sqs/

[REF16] AWS – IAM (Identity and Access Management)
https://aws.amazon.com/es/iam/

9 ABREVIATURAS

AES-256	Advanced Encryption Standard 256-bit
AMI	Amazon Machine Image
ACL	Access Control List
API	Application Programming Interface
API-REST	Application Programming Interface - Representational State Transfer
AWS	Amazon Web Services
AWS CloudTrail	Amazon Web Services CloudTrail
AWS CloudWatch	Amazon Web Services CloudWatch
AWS S3	Amazon Simple Storage Service
AWS SNS	Amazon Simple Notification Service
AWS SQS	Amazon Simple Queue Service
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos y Servicios de las TIC
EC2	Elastic Compute Cloud
eIDAS	Electronic Identification, Authentication and Trust Services
ENS	Esquema Nacional de Seguridad.
FIDO2	Fast Identity Online 2
GB	Gigabytes
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
IDP	Identity Provider
IIS	Internet Information Server
IP	Internet Protocol
JWT	Json Web Token
LCA	Lista de Control de Acceso
MFA	Multi-Factor Authentication
NoSQL	Not Only SQL
NTP	Network Time Protocol
RAM	Random Access Memory
RDP	Remote Desktop Protocol
RDS	Relational Database
Redis	Remote Dictionary Server

RSA	Rivest, Shamir, & Adleman
SaaS	Software as a Service
SHA	Secure Hash Algorithm
SMS	Short Message Service
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UI	User Interface

PUBLICACIONES DE DEFENSA

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