centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1622

Procedimiento de empleo seguro
Plataforma TrustCloud

Diciembre 2023

MINISTERIO DE DEFENSA

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

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
Pº de la Castellana 109, 28046 Madrid

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.01.30 10:05:57 +01'00'

NIPO: 083-24-027-3.
Fecha de Edición: diciembre de 2023

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 es un “Orquestador de orquestadores”, cuyos servicios son proporcionados en modelo SaaS (*Software as a Service*).
3. TrustCloud orquesta y blinda las transacciones digitales llevadas a cabo entre los distintos casos de uso que se plantean para los usuarios.
4. Se trata de una plataforma única de orquestación y custodia de todas las evidencias generadas por transacciones digitales, que permite preservar de forma adecuada los activos digitales, garantizando su identidad, integridad e intención de todos los participantes en cualquier parte del mundo, y con ello se consigue que sean seguras.

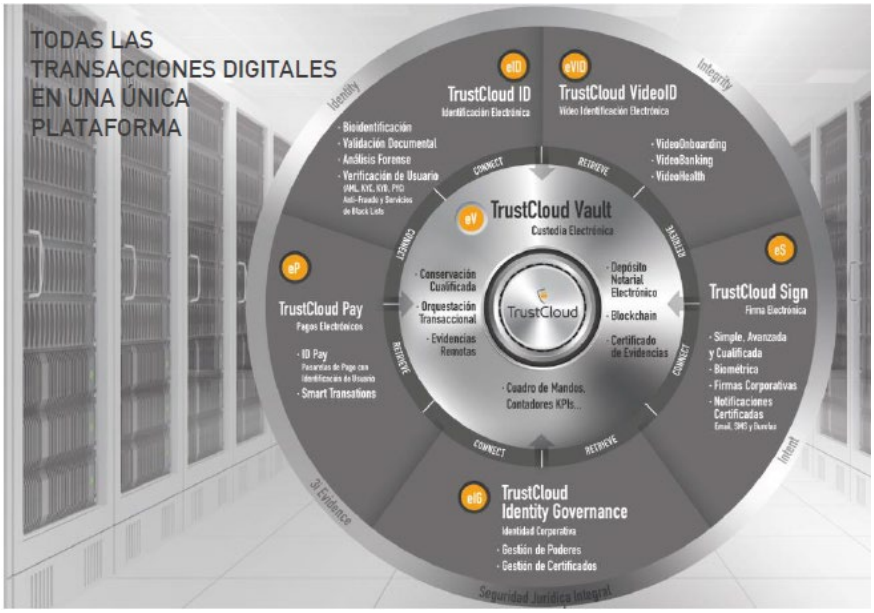

Ilustración 1 – Gráfico de la plataforma Trustcloud

2. OBJETO Y ALCANCE

5. Esta guía es de aplicación para la versión v.4 del servicio TrustCloud alojado en el proveedor de servicios en la nube de Amazon (AWS) [REF1].
6. Se trata de una plataforma a la que se accede mediante API-REST. Mediante el Orquestador, se gestionan los distintos servicios a proporcionar, según el caso de uso correspondiente.
7. El objetivo de este documento es servir como una guía para realizar una instalación, configuración y operación segura del producto TrustCloud v4.

3. ORGANIZACIÓN DEL DOCUMENTO

8. Este documento se compone de los siguientes apartados:

   a) Apartado **4**. En este apartado se recogen aspectos y recomendaciones a considerar en la instalación del producto.

   b) Apartado **5**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

   c) Apartado **6**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

   d) Apartado **7**. Este apartado contiene la documentación a la que se ha hecho referencia a lo largo de este documento.

   e) Apartado **8**. Este apartado contiene las abreviaturas que han sido empleadas a lo largo de este documento.

4. INSTALACIÓN

4.1 ALTA EN EL SERVICIO

9. Al tratarse de un servicio alojado en la nube, el proveedor dará de alta los datos del cliente y le enviará sus datos de acceso de forma segura los accesos pertinentes al producto.
10. Dicho envío se realiza mediante el correo electrónico corporativo support@trustcloud.tech, en un documento cifrado y su contraseña vía SMS.
11. Es posible verificar la autenticidad de dicho correo electrónico empleando la herramienta GpgOL (extensión de firma y cifrado de correos).
12. Los servicios son prestados mediante contratación, por lo que no es necesaria la instalación o configuración de ningún tipo de licencia.

4.2 CONSIDERACIONES PREVIAS

13. El equipo a emplear para acceder al servicio alojado en la nube deberá tener al menos las siguientes características:
    a) Procesador con una potencia de, al menos, dos núcleos a 2.5GHz.
    b) Memoria RAM de, al menos, 4 GB.
    c) Memoria de disco de, al menos, 30 GB.

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

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

15. 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.

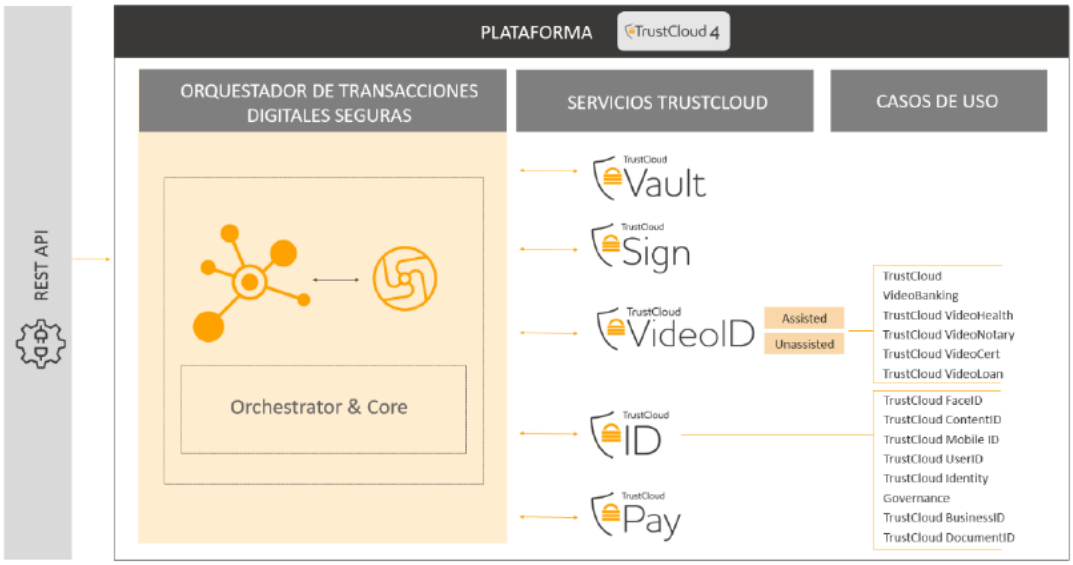

Ilustración 2 – Esquema General Plataforma Trustcloud

16. Al tratarse de un servicio en la nube, no es necesario que el cliente realice ningún tipo de configuración segura.

5.2 AUTENTICACIÓN

17. La identificación, autorización y autenticación de las peticiones API-REST se realiza utilizando *tokens JWT* [REF2]. Para ello, antes de realizar cualquier petición al API del Orquestador de Transacciones, se deberá de pedir un *token* al Servidor de Autorizaciones.

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

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

19. 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. Por defecto, no están habilitados los protocolos inseguros TLS 1.1, TLS 1.0, SSLv2 y SSLv3.

5.3.2 CONFIGURACIÓN DE ADMINISTRADORES

20. **El usuario del servicio debe asegurar que las contraseñas que se generen cumplan con una adecuada política de contraseñas** y se requieran, al menos:
    - Una **longitud mínima de 12 caracteres para la contraseña.** Por defecto, La longitud mínima de la contraseña es de 8 caracteres
    - **Una letra mayúscula** del alfabeto latino (A-Z).
    - **Una letra minúscula** del alfabeto latino (a-z).
    - Un **dígito**.
    - **Un carácter no alfanumérico** (! @ # $ % ^ & * ( ) _ + - = [ ] { } | ').
21. La contraseña caduca en 30 días. Sin embargo, este valor es configurable. No se recomienda establecer un valor superior a 60 días.
22. 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 introducir dos (2) códigos de autenticación de MFA (*Multi-Factor Authentication*) tras tres (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.
23. Asimismo, es posible establecer un cierto número de contraseñas anteriores que no podrán ser repetidas de nuevo. El valor es configurable entre 1 y 24. **Se recomienda establecer un límite de al menos 5.**
24. En el primer inicio de sesión **se deben cambiar esas credenciales en los casos que sean por defecto**, o no tengan credenciales asignadas previamente.
25. 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. Este valor es configurable.
26. 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*.

27. Solo el usuario *Administrador* puede llevar a cabo las siguientes funciones:
    a. Administración del producto de forma remota
    b. Configuración del tiempo de terminación de sesión
    c. Configuración de Casos de Uso
28. 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.

NOTA:
El rol "*Administrador*" es el administrador inicial que se crea. A partir de este rol se creará el resto de usuarios administradores ("*Administradores de Soporte*"). El usuario Administrador se crea a partir de la aplicación web de administración, con una herramienta denominada "*Data Seeder*".

5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

29. 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.

5.5 SINCRONIZACIÓN

30. 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.

5.6 ACTUALIZACIONES

31. 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.

5.7 ALTA DISPONIBILIDAD

32. 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.

5.8 AUDITORÍA

5.8.1 REGISTRO DE EVENTOS

33. El producto registra todas las transacciones, añadiendo un sello de tiempo cualificado según el reglamento europeo EIDAS [REF5], preservando todas las evidencias necesarias de manera segura. 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, y empleando cifrado.

34. Estos registros de auditoría 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 que se manda a sellar.
35. Los eventos de seguridad son gestionados por los servicios AWS CloudWatch [REF12], AWS CloudTrail [REF13], AWS SNS [REF14] y AWS SQS [REF15]. Las acciones que generan eventos son, al menos, las siguientes:
    - *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.

5.8.2 ALMACENAMIENTO LOCAL

36. 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.
37. 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 auditoria a través de su ciclo de vida.

5.9 BACKUP

38. Al ser un servicio en la nube, las copias de seguridad son realizadas por AWS de forma **diaria y semanal**, a través del servicio AWS RDS [REF6].

6. FASE DE OPERACIÓN

39. Dado que se trata de un servicio en la nube, las consideraciones para realizar una operación segura del mismo deben ser tenidas en cuenta por el proveedor del servicio.

40. Sin embargo, el cliente debe analizar periódicamente los registros de auditoría generados por el servicio con el objetivo de detectar cualquier comportamiento anómalo del mismo.

7. REFERENCIAS

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

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

REF3 Remote Dictionary Server
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://www.electronicid.eu/es/blog/post/eidas-nuevo-reglamento-de-firma-electronica-en-europa/es

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/trustcloud-platform/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/sqs/

8. ABREVIATURAS

AMI	*Amazon Machine Image*
API	*Application Programming Interface*
AWS	*Amazon Web Services*
CCN	Centro Criptológico Nacional
ENS	Esquema Nacional de Seguridad
GB	*Gigabytes*
HTTPS	*Hypertext Transfer Protocol Secure*
JWT	*Json Web Token*
NTP	*Network Time Protocol*
RAM	*Random Access Memory*
RDS	*Relational Database*
RSA	*Rivest, Shamir, & Adleman*
SaaS	*Software as a Service*
SHA	*Secure Hash Algorithm*
SMS	*Short Message Service*
STIC	Servicio de Tecnologías de la Información y Telecomunicaciones
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