centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1619

Procedimiento de Empleo Seguro
Veridas Identity verification service

Junio 2023

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

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
2023.06.01 11:42:55 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-038-6.
Fecha de Edición: junio 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. El producto **Veridas Identity verification service** es un servicio de verificación de la identidad de manera remota y con medios digitales, utilizando fotos de un documento de identidad, y una foto o un video en el que aparece la cara de la persona a verificar. De forma adicional, se incorpora un vídeo en el que el usuario muestra el anverso y reverso del documento. Está compuesto de varias piezas o productos de *software* que cumplen diferentes funciones dentro de una arquitectura cliente-servidor.
2. El *software* principal es la aplicación *back-end* o servidor, que es la que realiza el procesamiento para la verificación de la identidad a partir del conjunto de evidencias aportadas por el usuario.
3. Adicionalmente, se ofrece una herramienta cuya finalidad es facilitar la descarga y revisión humana de los procesos de validación realizados, y que puede emplearse para realizar una revisión en profundidad de los casos procesados. La persistencia y gestión de los datos que la herramienta de *back-office* genera son propiedad de la organización, ya que todo reside en sus instalaciones.
4. El *back-end* de validación ofrecido como SaaS, permite llevar a cabo los siguientes procesos de verificación:
    a) **Verificación documental**: Esta etapa del proceso de verificación, es obligatoria y consiste en la comprobación de un conjunto de medidas de seguridad extraídas de las fotos de un documento oficial de la persona (documento de identidad, pasaporte, entre otros) que se envían al servicio para su análisis. Igualmente, se revisa y comprueba toda la información recogida en el documento, mediante el empleo de técnicas de OCR. Todo ello permite ofrecer unas puntuaciones o *scorings* relativas a cada uno de los aspectos evaluados, que facilitan el determinar si hay o no intento de fraude, si está en vigor, o si los datos contenidos en el documento son verídicos. El documento de identidad analizado es capturado mediante un componente de captura de documento.
    b) **Verificación de biometría facial**: Esta etapa del proceso de verificación de identidad consiste en la comparación biométrica entre la foto impresa en el documento y la foto *selfie* del usuario. La foto *selfie* es capturada mediante un componente de captura *selfie* que incluye prueba de vida. La prueba de vida del producto se realiza mediante un proceso activo que requiere al usuario la realización de una serie de movimientos de cabeza aleatorios, grabados mediante un vídeo. Este módulo biométrico se denomina **das-Face**.
    c) **Vídeo-identificación**: Esta etapa del proceso de verificación de identidad consiste en la captura de un vídeo *selfie* en el que el usuario graba un vídeo mostrándose en pantalla y enseñando a la cámara el anverso y reverso del documento. El producto analiza que el vídeo grabado sea de la misma persona que capturó las evidencias biométricas en el paso anterior. El vídeo es grabado por un componente de captura.

2. OBJETO Y ALCANCE

5. El objeto del presente documento es facilitar la instalación y configuración segura del servicio **Veridas Identity verification service** compuesto por los siguientes componentes, junto con el aseguramiento del entorno en el que se despliega:

    a) ***vali-Das*:** Este software es ofrecido como un SaaS desplegado en AWS cuyo interfaz es un API REST. Este servicio API, debe ser consumido desde una aplicación cliente que integra los SDKs de captura destinados a guiar el proceso de obtención de los datos y evidencias necesarias para poder realizar los procesos de análisis en el *back-end*.

    b) ***boi-Das***: Esta herramienta se despliega *on-premise* en los servidores de la organización como una solución *docker* configurable que consta de tres partes: la propia aplicación frontal llamada boi-Das, una base de datos *PostgresQL* y un servidor web *NGINX*. Boi-Das se conecta con el *docker* de *PostgreSQL* para la persistencia de datos, que no forma parte del producto, sino que debe ser desplegada, mantenida, protegida y operada por la organización.

    c) ***SDK Document***: Este SDK de captura de plataforma web se encarga de la captura de imágenes de documentos, guiando al usuario en el proceso de captura.

    d) ***SDK Selfie Alive Pro SDK**:* Este SDK de captura de plataforma web se encarga de capturar el rostro de una persona, utilizando algoritmos biométricos avanzados.

    e) ***SDK Video***: Este SDK de captura de plataforma web se encarga de capturar un video *selfie* donde aparece el rostro, anverso y reverso del documento.

6. **El despliegue se debe realizar sobre un dispositivo móvil tipo *Smartphone* que cumpla las siguientes características**:

    a) Sistema operativo Android con versión de Sistema Operativo 4.1 o superior; o iOS con versión de SO 10.0 o superior.

    b) Cámara trasera con capacidad de capturar imágenes en resolución HD (1.280 x 720 píxeles) para la captura del documento de identidad.

    c) Cámara frontal con capacidad para capturar imágenes en resolución HD para la captura de la imagen *selfie*, con prueba de vida, así como del vídeo *selfie* en el que el usuario muestra anverso y reverso del documento.

3. ORGANIZACIÓN DEL DOCUMENTO

7. La estructura de capítulos del documento es la siguiente:
    a) Apartado 1: Descripción del producto.
    b) Apartado 2: Alcance del documento.
    c) Apartado 3: Organización del documento
    d) Apartado 4: Fase de despliegue en instalación.
    e) Apartado 5: Recomendaciones en la fase de configuración y administración.
    f) Apartado 6: Recomendaciones en la fase de operación.
    g) Apartado 7: *Checklist* de las tareas a realizar y el estado de cada una de ellas.
    h) Apartado 8: Referencias (links de consulta) usadas en este documento.
    i) Apartado 9: Abreviaturas usadas en este documento.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

8. La entrega de los componentes del producto se realiza mediante correo electrónico corporativo, confirmado por Veridas y por la organización. El remitente del envío es: Veridas Info<info-noreply@veridas.com>.

9. A este correo electrónico se envía la *API key* de vali-Das y acceso a un *google drive* donde se encontrarán disponibles todos los descargables, imagen *docker* de boi-Das y SDKs. Para comprobar las versiones correctas pueden consultar las versiones Cualificadas en el siguiente enlace:

   https://docs.veridas.com/environments/cloud/v1.0/

10. Dicho correo electrónico, contiene información con las credenciales, *API key* y detalles necesarios. Incluye el documento "*Veridas - Digital Verification of Identity - Integration checks review in Sandbox*", e información sobre el procedimiento de soporte de *Service Desk*.

4.2 ENTORNO DE INSTALACIÓN SEGURO

11. El producto se compone de varios elementos de *software*. El elemento principal es el servicio *backend* de validación que es ofrecido como un API vía SaaS, y constituye el servidor dentro de una arquitectura cliente-servidor. El entorno de ejecución de este servicio es la plataforma nube de servicios web de Amazon, AWS. Se encuentra desplegado sobre un clúster de máquinas con sistema operativo Linux. La distribución sobre la que Veridas valida su *software* es Ubuntu, y actualmente la versión empleada es la 20.04 LTS. Su localización física es Irlanda.

12. Este entorno posee diferentes medidas de seguridad destinadas a garantizar la autenticación y autorización del usuario de las APIs, es decir, que solo utilice y acceda a un recurso quien debe de hacerlo y quién está autorizado a ello. Entre otras medidas, el entorno del SaaS posee un WAF, acceso restringido a conjuntos o rangos de IPs relativas a cada cliente y autenticación por API Key.

13. El único componente del producto que debe instalarse en un Centro de Proceso de Datos (CPD) es **boi-Das**. Esta herramienta se despliega *on-premise* en los servidores de la organización como una solución *docker* configurable que consta de tres partes, cuyo acceso deberá limitarse a un conjunto de personas que posean una autorización expresa.

14. Boi-Das es una solución *docker* configurable que consta de la propia aplicación frontal llamada boi-Das, una base de datos *PostgreSQL* y un servidor web *NGINX*. Boi-Das se conecta con el *docker* de *PostgreSQL* para la persistencia de datos, que no forma parte del producto, sino que debe ser desplegada, mantenida, protegida y operada por la organización. Asimismo, al ser un despliegue *on-premise*, en las instalaciones de la organización, ésta debe definir los volúmenes donde desea almacenar las evidencias

descargadas. La persistencia y gestión de los datos que la herramienta de *back-office* genera son propiedad de la organización, ya que todo reside en sus instalaciones.

4.3 REGISTRO Y LICENCIAS

15. Veridas utiliza sistemas de inventario propio del IaaS contratado. Todo servicio o instancia levantada, queda reflejada en estos sistemas de registro de equipamiento, pudiendo obtener en todo momento un histórico del *hardware* utilizado. Los servicios prestados son mediante contratación y no es necesario la instalación o configuración de ningún tipo de licencia.

4.4 CONSIDERACIONES PREVIAS

16. La instalación del módulo boi-Das dedicado a la revisión humana de procesos de validación debe realizarse en un equipo con las siguientes características:
    a) **Sistema Operativo**: Linux Ubuntu versión 20.04.
    b) **Procesador** con una potencia de, al menos, dos núcleos a 2.5GHz.
    c) **Memoria RAM** de, al menos, 8 GB.
    d) **Memoria de disco** de, al menos, 20 GB.
    e) **Herramientas *Docker* y *Logrotate* instaladas**. Así como PSQL versión 12.6 o un contenedor docker que ofrezca las mismas características.
    f) Un **nombre de dominio** (opcional, pero recomendado).
    g) Un **certificado SSL** asociado al dominio, que es utilizado en el despliegue del contenedor *docker* (opcional para entornos no productivos, altamente recomendado para entornos productivos). Consultar el apartado 5.6 GESTIÓN DE CERTIFICADOS.
    h) **Sistema de *backup*** Ad-hoc (opcional pero altamente recomendado).
17. La parte cliente del proceso de la arquitectura del proceso de validación que ofrece el producto está compuesto por un conjunto de componentes de captura diseñados para ser integrados en una aplicación de software ya existente. Por consiguiente, el entorno de ejecución de estos componentes de captura vendría a ser el entorno de dicha aplicación HTML, que por su naturaleza está concebida para ser ejecutada en un navegador, siendo por tanto su entorno, el host del usuario que ejecute la aplicación y, dependiendo del diseño de la misma, el *backend* correspondiente donde esté implementada la lógica del servidor de la aplicación.

4.5 INSTALACIÓN

18. El único producto a instalar es la herramienta de *backoffice* boi-das. El detalle de los pasos de instalación se puede consultar en la guía *Boi-Das Onpremise Instructions – REF 5*.

19. Los SDKs del producto se construyen como un módulo independiente, para su correcta integración revisar los siguientes documentos:
    a) Descripción y uso del producto (SDK Documento) *SDK Document HTML – REF1*.
    b) Descripción y uso del producto (SDK *Selfie Alive Pro*) *SDK Selfie Alive Pro HTML – REF2*.
    c) Descripción y uso del producto (SDK Video) *SDK Video HTML – REF3*.
20. El elemento principal es el servicio *backend* de validación que es ofrecido como un API vía SaaS, que no requiere instalación alguna.

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

21. El *software* principal es la aplicación *back-end* o servidor llamado vali-Das, que se encarga de la verificación de la identidad de manera remota y con medios digitales, utilizando fotos de un documento de identidad, una foto y un video en el que aparece la cara de la persona a verificar. Este *software* es ofrecido como un SaaS desplegado en AWS cuya interfaz es un API REST.

22. Para asegurar un alto nivel de seguridad en las llamadas a dicha API REST, se debe llevar a cabo la siguiente configuración mediante el uso de las palancas de seguridad. Las palancas son parámetros que permiten modificar el valor máximo del *Score-DocumentGlobal*, donde si no se cumplen sus condiciones se verá penalizada la puntuación global del documento. Las palancas a configurar son las siguientes:

    a) *ScoreRel-PD_BirthDate_FrontNoFlash-PD_BirthDate_MRZ-Tex*t: Esta puntuación asegura que la fecha de nacimiento de la parte visual del anverso es la misma que la fecha de nacimiento leída del MRZ (*Machine Readable Zone*).

    b) *ScoreRel-DD_ExpirationDate_FrontNoFlash-DD_ExpirationDate_MRZ-Text*: Esta puntuación asegura que la fecha de expiración de la parte visual del anverso es la misma que la fecha de expiración leída del MRZ.

    c) *ScoreRel-PD_IdentificationNumber_FrontNoFlash-PD_IdentificationNumber_MRZ-Text*: Esta puntuación asegura que el número de identificación de la parte visual del anverso es la misma que el número de identificación leído del MRZ.

    d) *ScoreGroup-SD_MRZ-MRZDecodificación*: Esta puntuación asegura que todos los checksums de control de MRZ son correctos.

23. Para activar estas palancas es necesario enviar el siguiente JSON en el campo *scoreConfiguration* en el POST */validas/v1/validation/document*. Este POST crea una nueva validación enviando una foto del anverso del documento. Devuelve el ID de validación recién creado. Esta configuración debe enviarse en cada validación.

```
{
   "modifiers": {
       "ScoreRel-PD_BirthDate_FrontNoFlash-PD_BirthDate_MRZ-Text": 1,
       "ScoreRel-DD_ExpirationDate_FrontNoFlash-DD_ExpirationDate_MRZ-Text": 1,
       "ScoreRel-PD_IdentificationNumber_FrontNoFlash-PD_IdentificationNumber_MRZ-
Text": 1,
       "ScoreGroup-SD_MRZ-MRZDecoding": 1
   }
}
```

24. A continuación, se incluye una tabla con los **criterios de validación que se deben emplear para la validación** documental, biométrica y de la prueba de vida respectivamente. Estos valores son devueltos por el API y es el validador quien debe

aprobar o rechazar la validación manualmente basándose en estos valores de referencia.

Principales valoraciones	Validar	Rechazar
Score-DocumentGlobal	> 0.70	<= 0.70
ValidasScoreSelfie	> 0.70	<= 0.70
ValidasScoreLifeProof	> 0.77	<= 0.77

25. Para más información, consultar la guía *Configurations and recommendations for compliant CCN-STIC-140-F11* – REF6.

5.2 AUTENTICACIÓN

26. El producto se divide en dos (2) partes, el servicio *backend* de validación que es ofrecido como un API vía SaaS (vali-Das) y una herramienta cuya finalidad es facilitar la descarga y revisión humana de los procesos de validación (boi-Das). Ambos servicios requieren de procesos de autenticación distintos para el acceso a su configuración y funcionalidades.

27. Las credenciales de autenticación del *backend* vali-Das, el *API key* en este caso, puede ser dada de baja y sustituida por otra nueva únicamente por un usuario autorizado que disponga de credenciales (*API Key*) para hacerlo. De la misma manera, solo este usuario podrá consultar la información relativa a dichas credenciales. Esta rotación de credenciales se hace mediante el uso de *KeyMaker*, un producto interno de rotación de credenciales. El detalle sobre la rotación de claves se puede consultar en la guía *Descripción y manual de rotado de credenciales de servicios backend Veridas – REF8*.

28. Estas credenciales se guardan en una base de datos que se cifra con una clave almacenada y protegida en AWS. Este *API Key* se da de alta también al dar de alta o "aprovisionar" una organización. Las *API Key* son contraseñas generadas aleatoriamente por VeriSaaS, con una longitud mínima de 32 caracteres y que contienen letras mayúsculas, minúsculas y números.

29. Los mecanismos de autenticación empleados por boi-Das son:

    a) Credenciales locales, mediante usuario y contraseña. Estas únicamente podrán ser consultadas y modificadas por los propios usuarios, y por los usuarios administradores. No se almacenan en claro en la base de datos, se almacena únicamente su valor hash (*salted*).

    b) Configuración de doble factor. La herramienta emplea un sistema de doble factor o 2FA utilizando el servicio *Google Authenticator* al realizar el *login* en la aplicación. La configuración de esta funcionalidad se aplica mediante un conjunto de variables de entorno al desplegar el contenedor *docker* que conforma el producto. En concreto, se ha establecido la activación de la funcionalidad y el

tiempo durante el cual no se volverá a pedir 2FA en 24h. Para más detalle referirse al apartado 5.3.2 GESTIÓN DE USUARIOS.

c) Certificados SSL. El servicio permite configurar certificados SSL utilizando un volumen *docker* donde se dejan los certificados propios y confiables del usuario que despliega la herramienta. Estos certificados son utilizados para cifrar las comunicaciones de las diferentes piezas que componen la herramienta. Ver apartado 5.6 GESTIÓN DE CERTIFICADOS.

d) Oauth2. El servicio ofrece un API que requiere autenticación y autorización a través del módulo Oauth2 que tiene instalado. La gestión de los usuarios puede hacerse utilizando dicha API con usuarios que tengan el rol de supervisor o vía el Panel Administración de la aplicación Django.

30. El detalle de configuración de dichos mecanismos se puede consultar en el apartado 5.3 ADMINISTRACIÓN DEL PRODUCTO Para más información referirse al documento *Configurations and recommendations for compliant CCN-STIC-140-F11* – REF6.

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

31. El acceso a la gestión del servicio *backend* de validación vali-Das se realiza únicamente mediante API.

32. La herramienta de *backoffice* boi-das se despliega *on-premise* en los servidores de la organización como una solución *docker* configurable mediante contenedores. **Todas las comunicaciones emplean TLSv1.2 por defecto**. Se dispone de las siguientes interfaces para la administración:

    a) Administración local mediante consola.

    b) Administración remota de tipo GUI.

    c) Administración remota mediante API REST.

5.3.2 GESTIÓN DE USUARIOS

33. Toda la gestión de usuarios de debe de realizar mediante el API de boi-das, consultar la guía *Descripción y manual de uso del producto boi-das – REF7*. La creación de usuarios, así como la asignación de roles se debe hacer mediante la API de boi-das, con el conjunto de llamadas */api/v1/user*. El detalle se puede consultar en la guía *Descripción y definición de API Boidas – REF9*.

34. El producto dispone de distintos roles de usuario predeterminados que se pueden asignar a los usuarios y determinan sus permisos. **No se pueden generar roles adicionales**. Los roles predeterminados son:

    a) Administrador. Acceso completo a las funcionalidades y configuraciones del producto.

    b) Auditor. Acceso y gestión de los registros de auditoría.

c) Supervisor. Acceso completo a las funcionalidades y visualización de una lista con todos los procesos de validación. Puede seleccionar qué validación consultar.

d) Agente. Acceso limitado a las funcionalidades. Su principal uso es visualizar procesos de validación y revisarlos. No puede seleccionar qué validación consultar.

5.3.3 CONFIGURACIÓN DE ADMINISTRADORES

35. Durante la puesta en marcha del contenedor *boidas-service*, se crea un administrador, con el nombre de usuario *admin*, y la contraseña de este usuario se imprime en el registro de pantalla. Por ejemplo:

boidas-servicio | CONTRASEÑA DE SUPERUSUARIO DE BOIDAS: TexQ2N20xh1zQt3RaOwGvob3NKdEdGi0mR4pw3c1

36. **Se debe modificar la contraseña de este usuario en su primer acceso**, creando una que cumpla con la política de contraseñas descrita a continuación.

37. Para acceder al panel de administración, el usuario debe navegar a través de la url https://[BOIDAS_URL]/boidas_admin_configuration.

38. El producto dispone de una política no configurable de contraseñas que:

a) Comprueba la similitud entre la contraseña y un conjunto de atributos del usuario.

b) Exige una longitud mínima de ocho caracteres. **Se deberá exigir una longitud mínima de 12 caracteres de forma procedural**.

c) Evita el uso de palabras comunes como contraseña. Se compara con una lista incluida de 20,000 contraseñas comunes.

d) Previene el uso de contraseñas únicamente numéricas.

39. Adicionalmente el administrador del sistema **deberá exigir a los usuarios la siguiente política de contraseñas de manera procedural**:

a) Exigir una longitud mínima de 12 caracteres.

b) Exigir que se incluya, al menos, una letra minúscula, una mayúscula, un número y un carácter especial.

c) No reutilizar las últimas 5 contraseñas.

d) Cambiar las contraseñas cada 60 días.

e) No permitir un nuevo cambio de contraseñas antes de pasados 7 días.

40. Se debe realizar también la configuración de parámetros de sesión. De forma predeterminada, la autenticación del servicio boi-Das se basa en la verificación de usuario y contraseña. **Se recomienda configurar la funcionalidad de autenticación de "segundo factor"**.

a) ***OTP_ENABLED***=”*yes*": *Google Authenticator 2FA* está activado para la instancia de servicio, lo que requiere que todos los usuarios lo activen y lo usen.

b) ***OTP_PERIOD_ENABLED**="yes":* No se solicitará la 2FA a los usuarios durante un período de tiempo posterior al último inicio de sesión. Este período de tiempo se puede configurar mediante el env. variedad "OTP_PERIOD_HOURS", el valor debe ser 24 horas. **OTP_PERIOD_HOURS**="24"

c) ***GOOGLE_AUTH_ISSUER***: *"Veridas-Boidas"* => Hay dos campos que identifican al proveedor 2FA en el código QR de *Google Authenticator*. Estos campos se denominan "emisor" y "ID de usuario". La aplicación Google Authenticator muestra estos valores justo encima del código OTP de 6 dígitos. Para personalizar el campo "emisor", se puede definir esta variable de entorno. Si no se define esta variable, por defecto será "Veridas-Boidas". El campo "*ID de usuario*" siempre se completará con el nombre de usuario del usuario para el que se creó el código QR.

d) **Bloqueos de acceso**: El servicio tiene por defecto un bloqueo automático de las credenciales de usuario. Tras 3 intentos fallidos de autenticación, el acceso quedará bloqueado por defecto por 600 segundos (Este tiempo puede ser modificado mediante la configuración de la variable de entorno BLOCK LOGIN_TIME).

e) **Bloqueo tras periodo de inactividad**: El servicio tiene por defecto un bloqueo según el cual, tras 10 minutos de inactividad, se hace un logout automático de la herramienta.

41. Para más información sobre cómo configurar estos valores consultar la guía *Boi-Das Onpremise Instructions* – REF5.

5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

42. Boi-das se compone de contenedores *docker*, los cuales ofrecen unos puertos recomendados para exponer sus servicios. La organización deberá elegir qué puertos exponer. Las interfaces, nuevamente, están relacionadas con los servicios de los contenedores *docker*, la organización debe seguir las recomendaciones dictadas por Veridas (ver guía *Boi-Das Onpremise Instructions – REF5*).

43. Por ejemplo:

    a) Deshabilitar los servicios no utilizados en el dispositivo.

    b) Introducir una etiqueta que identifique el uso para el que está destinado cada interfaz.

    c) Asociar a cada interfaz la dirección IP y MAC de la máquina conectada.

44. Veridas ofrece sus servicios con los contenedores *docker* securizados, evitando exponer puertos que no hagan ninguna referencia al servicio. Para más información consultar la guía *Boi-Das Onpremise Instructions – REF5.*

5.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

45. La comunicación con el *back-end* vali-Das emplean siempre HTTPS/TLS, soportando las versiones de TLS v1.2 por defecto. Igualmente, se aplica la misma configuración para todas las conexiones internas entre los diferentes servicios del *back-end* como base de datos, otros microservicios, etc. También se aplica a la herramienta de revisión, boi-Das.

46. El producto emplea las siguientes *ciphersuites*:

    a) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

    b) TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

47. Adicionalmente, se protegen las credenciales durante su almacenamiento haciendo uso de los siguientes mecanismos:

    a) Cifrado AES-256 para proteger el *api-key* de los clientes, que sirve como mecanismo de autenticación para el consumo del API de vali-Das.

    b) Funciones resumen (algoritmo PBKDF2 con SHA256) para almacenar las contraseñas de los usuarios de boi-Das.

5.6 GESTIÓN DE CERTIFICADOS

48. Al conectarse con el servicio de VeriSaaS Cloud, el lado del servidor cifra el tráfico HTTPS mediante un certificado válido emitido y mantenido por AWS ACM. Es importante que **la organización solo confíe en un certificado válido** (el CNAME del certificado debe ser el correspondiente a la URL de VerisaaS Cloud). Para obtener más información sobre los certificados de AWS, consultar: https://aws.amazon.com/certificate-manager/.

49. Se debe tener en cuenta que la fijación de certificados no es una práctica recomendada, pero en caso de ser necesario, considerar fijar todas las CA raíz de AWS publicadas en: https://www.amazontrust.com/repositorio/

50. Adicionalmente se deben configurar los certificados SSL empleados en las comunicaciones entre los usuarios y el GUI en la herramienta boi-das, utilizando un volumen *docker* donde se dejan los certificados propios y confiables del usuario que despliega la herramienta.

51. La configuración se realiza mediante las siguientes variables:

    a) *SERVER_NAME*: *localhost*. Nombre del servidor NGINX empleado para configuración interna.

    b) *NGINX_UPSTREAM*: *Host* de boi-Das (por ejemplo, el nombre de contenedor de boi-Das).

    c) *PORT: 8850* => Puerto empleado por Boidas.

52. Además de estas variables, es necesario un volumen de datos para un uso más conveniente del contenedor NGINX. Algunos de estos contenedores requieren permisos para el usuario de *www-data* (uid=33):

a) */etc/boidas/security/certs/*: Este volumen es necesario para el despliegue de boi-Das utilizando SSL (ENABLE_SSL=TRUE.). El servicio boi-Das incluye certificados predeterminados válidos para fines de prueba y *sandboxing*, estos **se deben modificar por certificados válidos emitidos por una CA de confianza**. Esta carpeta requiere permisos de usuario de *www-data* y debe crearse antes de ejecutar el servicio boi-Das. Se recomienda montar este volumen con permisos de solo lectura. Debe contener las siguientes claves y certificados SSL:

   i. servidor.crt

   ii. servidor.clave

53. Este volumen debe estar correctamente configurado en los scripts de la herramienta de implementación, como se indica en la sección de implementación del panel de boi-Das de la referencia *Boi-Das Onpremise Instructions – REF5*. Para permitir que los contenedores del *docker* del servicio escriban y lean en ellos.

54. **Todos los certificados empleados deberán cumplir las siguientes características**:

    a) Tipo de clave ECDSA, con un tamaño de 256 o 384 bits y algoritmo de firma SHA-384 o SHA-256.

    b) Tipo de clave RSA, con una longitud de clave de 3072 bits o superior.

5.7 SINCRONIZACIÓN HORARIA

55. **Se recomienda que todos los sistemas utilizados por la organización se encuentren sincronizados** para permitir una alta fiabilidad en los sistemas de auditoría y *logging*.

56. En el caso de la nube VeriSaaS, las máquinas están sincronizadas con el servidor de tiempos de AWS (*Amazon Web Services*). Las máquinas llevan un proceso que se ejecuta continuamente para ajustar los tiempos con el servidor de tiempos.

57. Los servicios ejecutándose en la máquina utilizarán la información del reloj de la propia máquina.

5.8 ACTUALIZACIONES

58. Las actualizaciones de los servicios gestionados las lleva a cabo el IaaS. Las actualizaciones de servicios propios se realizan de forma automática sin necesidad de parada del servicio. Las actualizaciones se prueban en entornos previos al de producción.

59. Las actualizaciones del cortafuegos se realizan automáticamente por el proveedor de servicios o IaaS. En cuanto a las configuraciones, cada vez que se despliega o se actualiza un servicio este actualiza la configuración del firewall de forma automática y programática.

60. La actualización de la herramienta boi-Das debe ser llevada a cabo por la organización. Cuando se encuentre disponible una nueva actualización, Veridas hará la entrega del docker de instalación siguiendo el proceso descrito en el apartado 4.1 ENTREGA SEGURA DEL PRODUCTO. Este *docker* debe ser instalado como reemplazo de la versión anterior.

5.9 ALTA DISPONIBILIDAD

61. Veridas ofrece para su producto de *backend*, Vali-Das sus contenedores en HA apuntando siempre a la misma base de datos, de manera que boi-Das tenga alta disponibilidad.

5.10 AUDITORÍA

5.10.1 REGISTRO DE EVENTOS

62. Los registros se encuentran en los volúmenes configurados en tiempo de despliegue para persistir dichos logs. El panel de auditoría muestra una interfaz para la gestión de registros, que permite el acceso y descarga de los diferentes archivos de registro generados en la aplicación panel de auditoría. Solo los usuarios con privilegios de auditor pueden acceder a este panel.
63. Todos los registros muestran el usuario que realiza la acción, la fecha de la acción y el id de validación si corresponde. El detalle de los eventos registrados se puede consultar en la sección *activity tab* de la guía *Descripción y manual de uso del producto boi-das – REF7*.
64. Durante la puesta en marcha del contenedor *boidas-service*, se crea un usuario auditor (con nombre de usuario *auditor*) y la contraseña de este usuario se imprime en el registro de pantalla como el siguiente ejemplo (consultar el apartado 5.3.2 GESTIÓN DE USUARIOS) :

    boidas-servicio | CONTRASEÑA DEL AUDITOR DE BOIDAS:
    TexQ2N20xh1zQt3RaOwGvob3NKdEdGi0mR4pw3c1

65. **Se recomienda modificar la contraseña de este usuario en su primer acceso**, creando una que cumpla con la política de contraseñas descrita en el apartado 5.3.3 CONFIGURACIÓN DE ADMINISTRADORES.
66. Para acceder al Panel de Auditoría, el auditor debe navegar a través de la url *https://[BOIDAS_URL]/boidas_audit* e iniciar sesión con la cuenta de usuario del auditor.
67. Si el inicio de sesión es exitoso, la aplicación mostrará el panel de auditoría con la lista de registros de nombres de archivos de la aplicación como se muestra a continuación:

68. La aplicación descargará el archivo de registro cuando se haga click en cualquier nombre de archivo de registro.
69. Se generan varios archivos de registro como resultado de la operación de boi-Das:
    a) ***boidas.access.log***: registros de acceso de nginx.

b) **boidas.log**: registros de salida del servicio de boi-Das.

c) ***boidasPolling.log***: registros de ejecución de sondeo de boi-Das.

5.10.2 ALMACENAMIENTO LOCAL

70. La gestión del almacenamiento local de registros de auditoría debe ser realizada por la organización, ya que la herramienta boi-das se instala en sus servidores. **Se debe realizar un rotado periódico de los registros**, de tal forma que se asegure siempre espacio de almacenamiento disponible, impidiendo la pérdida de registros.

71. Adicionalmente, para asegurar disponer del histórico de registros, **se recomienda realizar la copia, de forma segura, de los registros en un servidor externo de auditoría**.

5.11 *BACKUP*

72. El producto no dispone de mecanismos propios para la generación de copias de seguridad. **Se recomienda realizar copias de seguridad periódicas** siguiendo las instrucciones incluidas en el apartado *Backup* de la guía *Boi-Das Onpremise Instructions – REF5*.

5.12 SERVICIOS DE SEGURIDAD

73. El *software* principal es la aplicación *back-end* o servidor llamado vali-Das. El cual se encarga de la verificación de la identidad de manera remota y con medios digitales. Este software es ofrecido como un SaaS desplegado en AWS cuya interfaz es un API REST, donde todas las configuraciones de seguridad están aplicadas por defecto. Estas configuraciones son:

    - **Protocolo TLS 1.2:** Todas las comunicaciones con la API de VeriSaaS deben realizarse mediante HTTPS con el protocolo TLS 1.2. No se permiten versiones inferiores del protocolo. Cada comunicación dentro de VeriSaaS Cloud AWS VPC también utiliza TLS 1.2, lo que proporciona una capa de seguridad adicional para el tráfico HTTP dentro de AWS VPC. TLS 1.2 es actualmente el último estándar de seguridad para comunicaciones HTTP seguras. Las ciphersuites que se deben utilizar, siguiendo lo indicado en la guía *CCN-STIC-807 Criptología de empleo en el ENS* son:

        i. TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

        ii. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

    - **Lista de fuentes IP permitidas:** Todas las solicitudes a VeriSaaS Cloud deben originarse en el *middleware* de un cliente. El servicio de atención al cliente de Veridas requiere al menos una dirección IP pública para el aprovisionamiento de una cuenta LIVE, ya que este es un requisito obligatorio para operar el servicio. Una vez entregada la cuenta LIVE para un servicio de VeriSaaS, el cliente podrá administrar la lista de permitidos asociada a esa cuenta de servicio mediante el uso del servicio API de *Keymaker*. La lista de permitidos

también se puede modificar comunicándose con *Veridas Service Desk*. *VeriSaaS Cloud* descarta automáticamente todas las solicitudes que provengan de una IP de origen no registrada.

- **WAF:** Todo el tráfico entrante a VeriSaaS Cloud se analiza primero mediante un filtro de acceso web. WAF es un firewall para aplicaciones web, que filtra ataques comunes, como inyecciones SQL o Path Traversal. Además, WAF incluye una protección DDoS (no solo para la capa 7 sino también para las capas 3 y 4) para prevenir ataques que puedan terminar en una denegación de servicio. Veridas WAF también elimina silenciosamente todas las solicitudes entrantes que no son válidas o que tienen una sintaxis mal formada o que provienen de una red de origen sospechosa. Al hacer esto, se protege el servicio del tráfico no deseado.
- **Autenticación de clave API:** Para que una solicitud de cliente pueda acceder a un servicio, además del cumplimiento de los requisitos anteriores, la solicitud entrante debe ser autenticada incluyendo un archivo de encabezado apikey con la credencial de cliente correspondiente. Se rechazan las solicitudes con el encabezado de clave de API incorrecto. Las APIKEY son contraseñas generadas aleatoriamente por VeriSaaS, con una longitud mínima de 32 caracteres y que contienen letras mayúsculas, minúsculas y números.
- **Datos de cifrado:** El servicio utiliza las capacidades de AWS KMS para cifrar datos tanto en tránsito como en reposo, por ejemplo, en un sistema de archivos de red compartido o en una base de datos. El contenido del sistema de archivos se cifra mediante el algoritmo estándar de cifrado avanzado con modo XTS y una clave de 256 bits (XTS-AES-256). AWS KMS almacena las claves maestras en un almacenamiento altamente duradero en un formato cifrado para ayudar a garantizar que se puedan recuperar cuando sea necesario.

74. El producto previene la descarga de validaciones en caso de detectar el espacio de almacenamiento lleno.

6. FASE DE OPERACIÓN

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

    a) El producto debe contar con las **últimas actualizaciones de seguridad** para preservar al mismo de amenazas y vulnerabilidades conocidas.

    b) Se deben **mantener y analizar periódicamente los registros de auditoría**. Solamente el personal de seguridad autorizado podrá acceder a ellos.

    c) Se deben **gestionar correctamente los certificados empleados**, actualizando los cuando sea necesario, por ejemplo, al expirar.

7. CHECKLIST

76. La *checklist* para la correcta implantación del producto:

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Configuración de las palancas de seguridad	☐	☐	
ADMINISTRACIÓN DEL PRODUCTO			
Configuración de los parámetros de sesión	☐	☐	
GESTIÓN DE CERTIFICADOS			
Configuración de los certificados del producto	☐	☐	
SINCRONIZACIÓN HORARIA			
Configuración de la sincronización de los sistemas	☐	☐	
BACKUP			
Planificación de las copias de seguridad	☐	☐	

8. REFERENCIAS

REF1 Descripción y uso del producto (SDK Documento) SDK Document HTML *https://docs.veridas.com/document-sdk/html/latest/customization/*

REF2 Descripción y uso del producto (SDK Selfie Alive Pro) SDK Selfie Alive Pro HTML *https://docs.veridas.com/sap-sdk/html/latest/customization/*

REF4 Descripción y uso del producto (SDK Video) SDK Video HTML *https://docs.veridas.com/video-sdk/html/latest/customization*

REF5 *Boi-Das Onpremise Instructions*. *https://docs.veridas.com/boi-das/cloud/latest/onpremise_installation/docker-installation/*

REF6 *Configurations and recommendations for compliant CCN-STIC-140-F11.*

REF7 Descripción y manual de uso del producto boi-das. https://docs.veridas.com/boi-das/cloud/latest/annexes/user_guide/.

REF8 Descripción y manual de rotado de credenciales de servicios backend Veridas. *https://docs.veridas.com/keymaker/cloud/latest/main-features/*.

REF9 Descripción y definición de API Boidas. *https://docs.veridas.com/boi-das/cloud/latest/api/api_redoc/*.

9. ABREVIATURAS

2FA	*Two Factor Authentication*
API	*Application Programming Interface*
AWS	*Amazon Web Services*
CA	*Certification Authority*
CPD	Centro de Proceso de Datos
ENS	Esquema Nacional de Seguridad.
HD	*High Definition*
HTML	*HyperText Markup Language*
HTTPS	*HyperText Transfer Protocol Secure*
IaaS	*Infrastructure as a Service*
IP	*Internet Protocol*
MAC	*Media Access Control*
MRZ	*Machine Readable Zone*
SDK	*Software Development Kit*
SSL	*Secure Sockets Layer*
TLS	*Transport Layer Security*

PUBLICACIONES DE DEFENSA

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