centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1634

Procedimiento de empleo seguro
NebulaID Engine

Marzo 2024

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: 083-24-119-0.
Fecha de Edición: marzo 2024.

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
2024.03.06 17:32:22 +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
Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. INTRODUCCIÓN

1. El producto NebulaID Engine 2.0 (de aquí en adelante, NebulaID) es un producto desarrollado por Víntegris que permite la identificación remota mediante vídeo y la evaluación posterior de las evidencias aplicando procesos y mecanismos de comparación y *scoring* biométrico para garantizar la correspondencia y veracidad de la identidad de la persona física involucrada.

2. OBJETO Y ALCANCE

2. El objeto del presente documento es facilitar la instalación y configuración segura de los dispositivos de **NebulaID Engine 2.0 (NebulaID)**, junto con el aseguramiento del entorno en el que se despliega.

3. Incluye la descripción de las acciones a llevar a cabo para el empleo seguro del producto **NebulaID Engine 2.0** (NebulaID), dentro de las especificaciones determinadas por la normativa vigente y los Requisitos establecidos por la guía CCN-STIC aplicable (CCN-STIC 140 – Anexo F11: Herramientas de videoidentificación) **[REF1]**.

3. ORGANIZACIÓN DEL DOCUMENTO

4. Este documento queda organizado según la ordenación mostrada a continuación

   a) Apartado 4. FASE DE DESPLIEGUE E INSTALACIÓN: quedan descritas las acciones fundamentales a tener en cuenta para el despliegue e integración del servicio NebulaID.

   b) Apartado 5. FASE DE CONFIGURACIÓN: quedan descritas las configuraciones del servicio para cumplir con los requisitos establecidos por la Guía de Empleo Seguro de verIDAS y los definidos en la Guía CCN-STIC 140 (ANEXO F11) **[REF1]**.

   c) Apartado 6. CHECKLIST: lista de verificación de las tareas a realizar por el administrador.

   d) Apartado 7. REFERENCIAS: detalle de las referencias documentales recogidas a lo largo del documento.

   e) Apartado 8. ABREVIATURAS: abreviaturas usadas en este documento.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

5. NebulaID opera y es ofrecido en modo SaaS, dentro de la suite de productos *NebulaSUITE* (desarrollada por *Víntegris*), por lo que su uso es licenciado en función de un volumen de operaciones a contratar por parte de la organización.
6. Para la entrega del producto, se otorga acceso a un *tenant* (alojamiento privado) en *NebulaSUITE* desde donde puede obtener el servicio.
7. El acceso a dicho *tenant* se otorga mediante las credenciales de un usuario gestor o manager que se entrega al cliente por correo electrónico indicado por la organización. En dicho correo electrónico, la organización puede establecer las credenciales de acceso al *tenant* de manera privada.

4.2 REGISTRO Y LICENCIAS

8. El licenciamiento se otorga mediante el acceso a un *tenant* (alojamiento privado) en NebulaSUITE de la organización, y a la consumición máxima de un volumen de operaciones de video identificación que se contratan previamente para el servicio NebulaID, por un tiempo máximo establecido, prorrogable mediante contrato.
9. La documentación de licenciamiento se facilita a la organización durante el proceso de adquisición.

4.3 CONSIDERACIONES PREVIAS

10. Además del licenciamiento que permita el uso del servicio NebulaID, la entidad u organización suscriptora que haga uso de este debe considerar:
    - El servicio NebulaID se accede a través de TLS 1.2 o superior, utilizando cifradores contemplados en la Guía CCN-STIC-807 Criptografía de empleo en el ENS **[REF3]**.
    - Para hacer uso de NebulaID, se han de configurar los usuarios correspondientes con capacidad de creación y evaluación de procesos de video identificación remota. Todo ello queda reflejado en el Manual de Operador de NebulaID **[REF4]**.

4.4 INTEGRACIONES

11. Se distinguen dos (2) tipos de integraciones en NebulaID:
    - **Integraciones propias de la plataforma (internas)**: aquellas soluciones o productos con los que el producto NebulaID está integrado por defecto. En este sentido, aparte de las soluciones proporcionadas por el Proveedor de Servicios Cloud (AWS) para el funcionamiento y especificación de requisitos de seguridad de NebulaID, se incluyen:

a) La integración del servicio con *vali-Das* y *boi-Das*, que componen el *Veridas Identity Verification Service* y permiten que las evidencias obtenidas durante el proceso de video identificación remota sean obtenidas y analizadas mediante scoring biométrico.

   i. Dicha integración se realiza siguiendo la Guía de Empleo Seguro de Veridas Identity Verification Service **[REF2]**.

b) La integración del servicio con el Servicio de Verificación de Datos de la Policía Nacional, y que permite la validación de soportes físicos de Documento Nacional de Identidad español.

   i. Esta integración se realiza de cara al cumplimiento de requisitos establecidos por la Orden Ministerial ETD/743/2022 **[REF5]** para la emisión de certificado cualificado mediante video identificación remota.

   ii. Se sigue la documentación de integración servida por la Subdirección General de Tecnologías de la Información y Comunicaciones (Ministerio de Asuntos Económicos y Transformación Digital).

- **Integraciones externas**: aquellas integraciones de soluciones o productos propiedad de clientes suscriptores de NebulaID integrados con la plataforma. De esta manera, NebulaID puede integrarse con diferentes procesos de negocio según las necesidades de las organizaciones.

  a) Esta integración se realiza a través del API ofrecido por NebulaSUITE. Para más información, se refiere al lector la Guía de Usuario de nebulaAPI **[REF6]**.

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

12. NebulaID es un servicio ofrecido en modo SaaS, en el que toda la configuración relacionada con el modo de operación seguro del producto y la configuración relativa a los parámetros que la sustentan queda supeditada a la acción del personal de Víntegris, desarrolladora del producto.
13. Esto, unido a la configuración de la integración con el producto verIDAS siguiendo el Procedimiento de Empleo Seguro **[REF2]**, asegura un empleo seguro del producto.
14. De esta forma, no se permite la definición de modos alternativos de operación al definido en este documento para los ítems de configuración establecidos en este epígrafe.

5.2 AUTENTICACIÓN

15. El modelo de autenticación en NebulaID es el mismo que el ofrecido por NebulaSUITE. Este se gestiona a través del módulo NebulaUSERS **[REF7]**, y que se encarga de gestionar los accesos a los recursos ofrecidos a través de un esquema basado en *tokens* de acceso. Este sistema dispone de dos (2) tipos de *token*:
    - ***Token* simple**: permite el acceso a recursos básicos de consulta o el acceso a la plataforma mediante primer factor de autenticación. Este *token* se obtiene tras la realización del *login* del usuario mediante usuario y contraseña.
    - ***Token* robusto**: permite el acceso a recursos avanzados o para los que se requiere un segundo factor de autenticación. Este *token* se obtiene tras la obtención del *token* simple y la realización de una autenticación basada en un segundo factor dentro de los configurados para el usuario objeto de la autenticación (SMS OTP, Email OTP, tarjeta de coordenadas, TOTP).
16. Los *tokens* de acceso mencionados disponen de una caducidad máxima de 8 horas.
17. Todas las interacciones con el producto (ya sea a través de API o del Portal de Acceso) se basan en este esquema.
18. Los usuarios que tienen entidad en NebulaSUITE pueden sincronizarse con directorios corporativos externos propiedad de la organización. Estos usuarios dispondrán de la validación de credenciales ante el directorio corporativo desde el que se originan. El detalle de configuración de la sincronización con los directorios corportativos de la organización se puede consultar en la guía de Usuario de *NebulaUSERS Synchronizer* **[REF9].**

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

19. La administración de seguridad del producto es llevada a cabo por el equipo de Producción de Víntegris, que dispone de acceso a los servicios y máquinas que forman la infraestructura que da soporte a NebulaSUITE. Todos los protocolos de acceso a dicha infraestructura siguen la Política de Seguridad de Víntegris, incluyendo:
    - Protocolos de acceso seguros:
        - SSHv2 con autenticación mediante clave asimétrica.
        - Frontales y servicios web con:
            - Autenticación multifactor
            - HTTPS con TLS 1.2 o superior y cifradores según la Guía CCN-STIC-807 **[REF3]**
        - En aquellas comunicaciones necesarias, VPN con IKEv2/SHA256 (siguiendo las recomendaciones de la Guía CCN-STIC-807 **[REF3]**).

5.3.2 CONFIGURACIÓN DE ADMINISTRADORES

20. Aunque un *tenant* puede disponer de una política de contraseñas diferente, la política de contraseñas por defecto gestionada por NebulaSUITE se compone de las siguientes restricciones:
    - **Longitud mínima de contraseña:** 12 caracteres
    - **Complejidad de contraseña:** mayúsculas, minúsculas, dígitos y símbolos.
    - **Número máximo de reintentos:** 3
    - **Caducidad de contraseña:** 90 días.
    - **Tiempo máximo de inactividad del usuario:** 180 días
    - **Historial máximo de contraseñas:** 5
21. La modificación de dicha política se llevará a cabo mediante petición expresa a la empresa a través de canales de contacto establecidos tras la contratación del servicio.
22. De manera complementaria, existen grupos predefinidos que definen los roles sobre los que los usuarios pueden interactuar con las diferentes partes de NebulaSUITE, y particularmente, de NebulaID **[REF7]**.
23. Para la creación de usuarios para el empleo de las funcionalidades del producto, consultar la Manual del Operador de NebulaID **[REF4]**.

5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

24. El servicio NebulaID escucha peticiones sobre los puertos estándar HTTPS tanto para el acceso al portal de servicio, como mediante para la integración mediante API para su uso por parte de un suscriptor.
25. Todas las comunicaciones externas e internas de los diferentes módulos que componen el servicio NebulaID utilizan siempre el protocolo HTTPS con TLS 1.2 o superior. Las suites de cifrado empleadas son acordes a las establecidas por la Guía CCN-STIC-807 Criptografía de Empleo en el ENS **[REF3]**.
26. Internamente, el servicio utiliza algoritmos criptográficos seguros para la protección de activos. Entre otros:
    - AES (256 bits) para la protección de datos cifrados en Base de datos.
    - Certificado cualificado de Sello Electrónico emitido por Víntegris como QTSP (https://www.vincasign.net), para la firma electrónica de evidencias que Víntegris custodia de los procesos de video identificación.
    - PBKDF2 con SHA 512 como algoritmo de derivación para el guardado seguro de credenciales.
    - HMAC con SHA256 para firmar el registro de auditoría (NebulaAUDIT).
27. Los protocolos de seguridad relacionados con lo aquí descrito no son configurables por parte de los suscriptores del servicio, siendo el personal de Víntegris (como propietaria de este) los encargados de realizar la configuración de los protocolos.

5.5 GESTIÓN DE CERTIFICADOS

28. NebulaID utiliza como certificado HTTPS público el ofrecido por el portal de NebulaSUITE, de forma que no es ofrecido a través de ningún DNS o nombre alternativo a *.nebulaservice.net.
    - Este certificado está emitido por una CA integrada con los navegadores y sistemas operativos, de tipo OV o EV.
29. El servicio NebulaID no permite ni requiere la configuración de certificados electrónicos para su correcto funcionamiento por parte de un suscriptor del servicio.

5.6 AUDITORÍA

5.6.1 REGISTRO DE EVENTOS

30. A través del módulo NebulaAUDIT (que forma parte de la solución NebulaSUITE), se recogen los eventos de auditoría, que son enviados por los diferentes módulos que conforman NebulaID.
31. Los registros de auditoría (**[REF8]**) pueden ser consultados a través del portal web de NebulaSUITE, o exportados en formato CSV mediante un usuario con los permisos adecuados.
32. Por cada registro de auditoría se guarda la siguiente información: usuario que realiza la acción auditada, operación, objeto afectado y entorno (IP, timestamp, etc.).
33. Para la exportación de registros CSV, un usuario auditor de la organización, dentro del acceso a su *tenant* contratado, desde el propio apartado de auditoría podrá seleccionar la exportación de auditoría en base a unos criterios de búsqueda.

5.6.2 ALMACENAMIENTO LOCAL

34. Los registros de auditoría son almacenados en repositorios que residen en la propia infraestructura en la plataforma que proporciona el Proveedor de Servicios Cloud (AWS), desde donde opera el servicio.

5.6.3 ALMACENAMIENTO REMOTO

35. El producto no dispone de la funcionalidad de reenvío automático de los registros a un servidor externo de auditoría.
36. Sí permite la exportación de dichos registros en CSV (ver apartado 5.6.1 REGISTRO DE EVENTOS) bajo demanda. Tras su descarga, dicho fichero se podrá almacenar de forma segura en la ubicación deseada.

5.7 BACKUP

37. Víntegris, como propietario de la plataforma y desarrollador de la solución, se encarga de las operaciones y responsabilidades de la ejecución de procesos de copia de seguridad o *backup* de evidencias y configuración de los *tenant* de la plataforma.
38. Se genera un *backup* completo de toda la plataforma **diariamente** durante un máximo de 7 días consecutivos, siendo reemplazados a partir del día 8 en un nuevo ciclo de copia de seguridad.
39. Las evidencias generadas de vídeo identificación generadas por el servicio son custodiadas durante 15 años en cumplimiento del Reglamento EU 910/2014, de la Ley 6/2020 de Servicios Electrónicos de Confianza, y de la Orden Ministerial ETD/743/2022 **[REF5]**.

5.8 FASE DE OPERACIÓN

Durante la fase de operación del equipo, el administrador debe llevar a cabo el mantenimiento de los registros de auditoría. Deberán ser almacenados protegidos contra borrado y modificaciones no autorizadas, así como exportados periódicamente.

6. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Establecimiento de credenciales del tenant	☐	☐	
CONFIGURACIÓN			
ADMINISTRACIÓN DEL PRODUCTO			
Creación de usuarios para la operación del producto	☐	☐	
AUDITORÍA			
Exportación de registros de auditoría	☐	☐	

7. REFERENCIAS

40. En este apartado se recopilan los títulos y recursos en los que encontrar la documentación a la que se ha hecho referencia a lo largo del documento.

41. La documentación referente a nebulaSUITE y sus diferentes servicios y productos se encuentra accesible para aquellas entidades suscriptoras por medio del acceso a la plataforma de manera autenticada. Estas son: REF4, REF6, REF7 y REF8.

REF1 Taxonomía de productos STIC. Anexo F.11. Herramientas de Video identificación.
https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/5461-guia-140-anexo-f-11-herramientas-de-videoidentificacion/file.html

REF2 Procedimiento de empleo seguro Veridas Identity Verification Service
https://www.ccn-cert.cni.es/pdf/guias/6894-ccn-stic-1619-procedimiento-de-empleo-seguro-veridas-identity-verification-service/file.html

REF3 Criptología de empleo en el Esquema Nacional de Seguridad
https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html

REF4 Manual del Operador de NebulaID

REF5 Orden Minsterial ETD/743/2022
https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-12934

REF6 Guía de Usuario de NebulaAPI

REF7 Guía de Usuario de NebulaUSERS

REF8 Portal de documentación de NebulaSUITE

REF9 Guía de Usuario de NebulaUSERS Synchronizer

8. ABREVIATURAS

AES	*Advanced Encryption System.*
API	*Application Programming Interface.*
AWS	*Amazon Web Services*
CCN	Centro Criptológico Nacional.
CSV	*Comma Separated Value*
DNS	*Domain Name Service.*
EDR	*End Point Detection and Response*
ENS	Esquema Nacional de Seguridad.
EV	*Extended Validation*
HMAC	*Hash Message Authentication System*
OTP	*One Time Password*
OV	*Organization Validation*
QTSP	*Qualified Trust Service Provider*
RSA	*Rivest Shamir Adleman*
SHA	*Secure Hash Algorithm*
SaaS	*Software as a Service*
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