centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1626

Procedimiento de empleo seguro
Alice Biometrics

Agosto de 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

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-029-4.
Fecha de Edición: agosto de 2023

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
2024.01.30 10:03:26 +01'00'

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

1. Alice Onboarding es un sistema de verificación de identidad remota no asistido y multiplataforma para un caso de uso desatendido, en el que el usuario interactúa directamente con el sistema sin necesidad de establecer una videoconferencia con un operador. Esto se consigue mediante la captura guiada y procesado automático de *selfie* y documento de identidad, que son analizados con tecnología de inteligencia artificial desarrollada por Alice Biometrics. También se proporciona un *dashboard* de supervisión en el que un operador dispone de toda la información necesaria para la revisión del proceso y sus evidencias.
2. Todas las tecnologías involucradas han sido desarrolladas por Alice Biometrics, entre ellas: extracción del perfil biométrico facial para cotejar la identidad contra las fotografías del documento; análisis PAD pasivo y activo (*Presentation Attack Detection* o *Liveness*) para detectar ataques de suplantación de identidad; lectura automática del anverso y el reverso del documento; y análisis automático de seguridad documental.
3. Alice cumple con todas las regulaciones vigentes en términos de privacidad (GDPR), seguridad (ISO27.001) y los más altos estándares de seguridad biométrica avalados por evaluaciones internacionales independientes (NIST).

2. OBJETO Y ALCANCE

4. La finalidad de este documento es la de explicar y guiar durante el proceso de instalación y configuración segura del servicio Alice Onboarding y de todos los componentes que lo conforman. En concreto, se cubrirán los siguientes módulos:
   a) Alice API: eje central del producto Alice Onboarding en forma de API REST. Este API es la que consumen, usan y con la que comunican el resto de módulos del producto para poder llevar a cabo la realización de un proceso de *Onboarding*: recepción, procesado y generación del resultado de las evidencias del selfie y el documento del usuario.
   b) Alice *Dashboard*: herramienta web que permite al cliente visualizar todos los registros y transacciones realizadas en el producto Alice Onboarding, desde los *onboardings* realizados por los usuarios hasta las operaciones llevadas a cabo por el propio cliente en relación a los mismos.
   c) Alice Android SDK: módulo SDK que permite facilitar la integración de Alice Onboarding y gestionar la captura y envío automático de documentos y vídeo selfie del usuario en tiempo real desde la cámara de su dispositivo a la API de Alice (Alice API) en aplicaciones Android.
   d) Alice iOS SDK: módulo SDK que permite facilitar la integración de Alice Onboarding y gestionar la captura y envío automático de documentos y vídeo selfie del usuario en tiempo real desde la cámara de su dispositivo a la API de Alice (Alice API) en aplicaciones iOS.
   e) Alice Web SDK: módulo SDK que permite facilitar la integración de Alice Onboarding y gestionar la captura y envío automático de documentos y vídeo selfie del usuario

en tiempo real desde la cámara de su dispositivo a la API de Alice (Alice API) en aplicaciones web.

5. Los siguientes entornos de operación son soportados:

   a) **Web**: Entorno *desktop* con navegador compatible (ver listado a continuación). También se puede ejecutar desde un dispositivo móvil Android y/o iOS. Los navegadores compatibles con Alice Onboarding son:

      - Desktop: Chrome, Safari, Firefox, Opera, Edge
      - Mobile: Chrome, Safari, Firefox, Opera, Samsung.

   b) **Móvil**: Entorno de dispositivo móvil Android y/o iOS. El producto Alice Onboarding soporta las siguientes versiones:

      - Versión mínima Android: Android 5.0 (sdk 21) o superior.
      - Versión mínima iOS: iOS 11.0 (Swift 5.0) o superior.

3. ORGANIZACIÓN DEL DOCUMENTO

6. A continuación, se muestra la estructura del documento en los distintos capítulos que lo conforman:

   a) Apartado **1**, Introducción: descripción de Alice Biometrics, su producto Alice Onboarding y las tecnologías empleadas por el mismo.

   b) Apartado **2**, Objeto y alcance: detalle de los distintos módulos que conforman el producto Alice Onboarding, así como sus versiones y características.

   c) Apartado **3**, Organización del documento: resumen de las distintas secciones y apartados que conforman este documento.

   d) Apartado **4**, Fase de despliegue e instalación: pasos necesarios para la correcta instalación de Alice Onboarding.

   e) Apartado **5**, Fase de configuración: pasos necesarios para la correcta configuración de Alice Onboarding.

   f) Apartado **6**, Fase de operación: pasos necesarios para el correcto uso de Alice Onboarding.

   g) Apartado **7**, *Checklist*: lista de comprobaciones a realizar para garantizar la correcta puesta en marcha del producto Alice Onboarding.

   h) Apartado **8**, Referencias: enlaces de interés a otros documentos citados y referenciados en este documento.

   i) Apartado **9**, Abreviaturas: definición sobre las distintas abreviaturas presentes a lo largo del documento.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

7. Las empresas interesadas en utilizar el producto Alice Onboarding deben ponerse en contacto con Alice Biometrics a través de la sección contacto de su página web https://alicebiometrics.com/contacto/. Rellenando este formulario se concreta una reunión entre representantes de ambas empresas, pudiendo así acompañar el acceso a la plataforma y garantizar que se le concede a entidades reales que lo necesiten.
8. En concreto, el acceso que se recibe es el del componente Alice Dashboard, dentro del cual se encuentra toda la información y recursos necesarios para instalar, configurar y usar el producto de Alice. De esta forma se evita enviar datos sensibles como el api key.
9. La empresa designará un administrador de la cuenta, que será quien recibirá el acceso, siendo él el responsable de invitar al resto del equipo. El acceso a la plataforma se recibe vía mail bajo el remitente noreply@alicebiometrics.com. En el primer acceso se solicita al administrador establecer una contraseña segura.
10. Adicionalmente, es recomendable, que una vez el administrador disponga de acceso completo al Alice Dashboard, active el mecanismo de segundo factor de autenticación (2FA), para proteger y securizar los posteriores accesos a la plataforma.

4.2 ENTORNO DE INSTALACIÓN SEGURO

11. La mayor parte de componentes que conforman el producto Alice Onboarding no necesitan ningún tipo de despliegue o instalación por parte del cliente, al tratarse de una solución *cloud*, como es el caso de Alice API o Alice Dashboard. Dichos elementos están disponibles en el entorno Cloud de Google Cloud Platform desplegado en servidores dentro de la región de Europa y es gestionado únicamente por Alice Biometrics.
12. Aunque no es necesario, por tanto, la instalación módulos al uso, sí es cierto que el cliente deberá importar e integrar tanto los módulos SDKs, como es el caso de Alice Android, Alice iOS o Alice Web, como las llamadas a Alice API dentro de su producto. En la sección **4.5 INSTALACIÓN** se explica y detalla cómo debe realizarse dicho proceso.

4.3 REGISTRO Y LICENCIAS

13. Al tratarse de una solución Cloud/SaaS, no es necesario ningún tipo de licencia de instalación. No así para su uso, donde sí son necesarias unas credenciales que autentiquen y garanticen el acceso al cliente en cuestión.
14. Para ello, junto a la creación de una cuenta en Alice Onboarding se hace entrega de dos credenciales. Una cuenta de desarrollo (-dev) diseñada para testing y uso en entornos previos, y otra de producción (-prod) para su uso en entornos productivos. El acceso a ambas credenciales se realiza a través de Alice Dashboard y se entrega al administrador de la cuenta designado por la empresa siguiendo los pasos descritos en el apartado **4.1 ENTREGA SEGURA DEL PRODUCTO**.

4.4 CONSIDERACIONES PREVIAS

15. Existen una serie de requisitos mínimos que el cliente debe tener en cuenta en términos de compatibilidad con el producto de Alice Onboarding, entre las que destacan:

    a) Peticiones seguras a través del protocolo HTTPS con versión TLSv1.2 o superior.

    b) Navegadores web soportados por Alice Web:

        - Desktop: Chrome, Safari, Firefox, Opera, Edge.
        - Mobile: Chrome, Safari, Firefox, Opera, Samsung.

    c) SO mínimos soportados por Alice Android y Android iOS:

        - Versión mínima Android: Android 5.0 (sdk 21) o superior.
        - Versión mínima iOS: iOS 11.0 (Swift 5.0) o superior.

4.5 INSTALACIÓN

16. Como se comenta en **4.2 ENTORNO DE INSTALACIÓN SEGURO**, aunque gran parte del producto Alice Onboarding no requiere instalación por parte del cliente al ser ofrecido como un SaaS Cloud, sí se requiere que se realice una integración software mínima tanto en la capa del *backend* como en la de *frontend* del producto del cliente.

17. Por el lado del *frontend*, el cliente debe importar los módulos Alice Android, Alice iOS y/o Alice Web en sus aplicaciones móviles y/o páginas web. En la sección de configuración de SDKs de la documentación técnica oficial de Alice Biometrics [REF1] se puede ver cómo se realizan dichas acciones necesarias, tales como: importar el SDK, gestionar los permisos de la cámara del dispositivo o configurar el flujo de onboarding deseado.

18. En lo relativo a la capa de backend, es necesario realizar una serie de llamadas mínimas a Alice API tales como el proceso de autenticación [REF2] y obtener el resultado del proceso de *onboarding* [REF3]

19. Durante dicho proceso de integración, el cliente dispondrá de soporte personal y dedicado por parte del equipo de Alice Biometrics.

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

20. Tanto Alice Dashboard como Alice API están configurados por defecto para cumplir con los requisitos y criterios definidos en la guía CCN-STIC 140.F11 [REF4], por lo que no es necesario que el cliente realice ningún ajuste en esta capa.
21. Por su parte, en la capa de *frontend* y los SDKs sí es necesario que se realice una configuración mínima. Es en esta capa, donde debe elegirse cuál es el flujo de *onboarding* deseado, es decir, cuales son aquellos pasos y evidencias que los usuarios tendrán que completar para realizar un *onboarding*.
22. Según lo definido por la guía CCN-STIC, dicho *onboarding* debe ser conformado por la subida y procesamiento de un *selfie* y de un documento de identidad. Por tanto, el cliente indicará al SDK en cuestión que debe solicitar dichas evidencias al usuario.
23. La manera correcta para realizar dicha invocación para Alice Android, Alice iOS y Alice Web se puede consultar en la propia documentación de Alice Onboarding, que estará disponible y accesible desde Alice Dashboard. A continuación se indican los enlaces:
    a) Android [REF5]
    b) iOS [REF6]
    c) Web [REF7]
24. Cabe destacar que para cumplir con los requisitos definidos en la guía CCN-STIC 140.F11, los pasos a seleccionar son: 1) "*Selfie with Challenge*" para la parte del selfie e 2) "IDCARD" para la parte de documento.
25. Una vez configurados los SDKs correctamente, las propias SDKs se encargarán de capturar y enviar esta información directamente a Alice API para su análisis y posterior visualización en Alice Dashboard.
26. En la Sección **5.15 SERVICIOS DE SEGURIDAD** de este documento se explica en detalle cómo interpretar el resultado de un proceso de *onboarding* en el Alice Dashboard para determinar si es exitoso o no.

5.2 AUTENTICACIÓN

27. Dentro de la *suite* que conforma el producto Alice Onboarding se diferencian principalmente 3 capas de autenticación:
    a) Autenticación de *Backend* del cliente ante Alice API → junto a la creación de una cuenta de Alice Onboarding se ofrece al cliente un api key correspondiente para que este pueda autenticar las conexiones que realiza desde su *backend* hacia Alice API. Esta API key solamente está accesible a través de Alice Dashboard por parte del administrador. Aunque la mayor parte de comunicaciones necesarias son realizadas directamente desde las propias SDKs de Alice, existen una serie de operaciones que el cliente deberá realizar desde su propio *backend* como: la gestión de usuarios

(creación, eliminación, etc.) u obtener el resultado del proceso de *onboarding* en formato *raw* (en caso de ser necesario). Para estas operaciones, el *backend* del cliente utilizará un procedimiento de obtención de *tokens* temporales tal y como se describe en la sección de Autenticación de la documentación [REF2] de la API.

b) Autenticación de SDK (Alice Android, Alice iOS, Alice Web) ante Alice API → las SDKs se Alice se encargan tanto de la captura de las evidencias requeridas como de su envío al Alice API para su posterior procesado. Este envío y comunicación está preconfigurado y securizado en las SDKs mediante el uso de certificados SSL de acuerdo a los requisitos de la guía CCN-STIC 140.F11. Para establecer la comunicación será necesario un *token* temporal (*USER_TOKEN*) que el *backend* de cliente debe obtener y enviar a la SDK siguiendo el procedimiento descrito en la sección Autenticación de la documentación de Alice Onboarding [REF2] accesible a través de Alice Dashboard.

c) Autenticación de usuarios de Alice Dashboard → para poder acceder al Alice Dashboard, desde el cual se pueden consultar el resultado de todos los procesos de onboarding o de los registros de auditoría, el cliente debe autenticarse ante el sistema mediante el uso de un usuario y contraseña. Así mismo, es recomendable activar adicionalmente el proceso 2FA, por lo que también será necesario introducir el código OTP correspondiente cada vez que se accede al Alice Dashboard.

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

28. La única capa de administración que se pueda realizar sobre el producto Alice Onboarding se realiza a través del Alice Dashboard, el cual se encuentra desplegado en un dominio securizado bajo el protocolo HTTPS, y para el cual el usuario debe autenticarse como se indica en la sección 5.2 AUTENTICACIÓN de este mismo documento.
29. A continuación, se detalla los distintos elementos de Alice Onboarding que un administrador puede gestionar:

    a) Conceder y retirar el acceso de usuarios al Alice Dashboard, así como seleccionar el rol adecuado para cada uno de ellos.

    b) Habilitar y deshabilitar la vista de registro de logs de auditoría a aquellos usuarios que deban disponer de la misma.

    c) Configurar la propia cuenta individual. Tareas como: Activar el 2FA, cambiar contraseña, etc.

5.3.2 CONFIGURACIÓN DE ADMINISTRADORES

30. La solución de Alice Onboarding soporta 3 tipos distintos de roles que se pueden asignar a los usuarios:

a) Visor → puede ver información general pero no puede realizar ninguna acción. Secciones del Dashboard ocultas para los visores: Equipo y Credenciales.

b) Editor → puede ver información general y realizar determinadas acciones. Secciones del Dashboard ocultas para los editores: Equipo y Credenciales.

c) Administrador → puede ver y realizar todas las acciones disponibles en el sistema.

31. Se recomienda conceder siempre el rol con los permisos mínimos necesarios para la función a desempeñar.

32. Adicionalmente, existe un permiso llamado "Auditor", el cual puede ser habilitado para cualquier tipo de usuario por parte de un administrador. Los usuarios con este permiso activo tendrán acceso a una nueva sección del Dashboard llamada "Logs de auditoría" desde la cual podrán ver todas las acciones llevadas a cabo por cualquier miembro del equipo.

33. Solo un usuario con rol de administrador puede encargarse de invitar y conceder acceso a nuevos usuarios, así como de asignar o cambiar el rol adecuado a cada uno. Dichas operaciones se realizan desde la sección "Equipo" del Alice Dashboard.

34. Una vez que el usuario recibe la invitación debe definir cuál será su contraseña de acceso, la cual debe cumplir con una serie de requisitos mínimos. En concreto:

    a) Longitud mínima de 12 caracteres.

    b) No existen caracteres excluidos, todos están permitidos.

    c) La contraseña elegida debe seguir las siguientes reglas (la propia herramienta dará feedback al usuario si alguna de ellas falla):

        - No hacer uso de palabras comunes
        - Más de una única palabra
        - No repetir palabras o caracteres
        - No usar secuencias
        - No utilizar fechas

35. Actualmente, el producto Alice Onboarding no dispone de ningún mecanismo para la renovación periódica de las contraseñas de acceso. El definir la validez de estas contraseñas y definir un proceso de actualización periódica es algo que recae en el lado del cliente. Se recomienda que los usuarios de Alice Dashboard actualicen su contraseña de acceso de forma periódica y frecuente.

36. Comentar además, que la solución de Alice dispone de un tiempo de sesión activa de 60 minutos. A partir de ese tiempo, un nuevo inicio de sesión es necesario para poder seguir utilizando la plataforma.

5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

37. Al tratarse de una solución Cloud toda la gestión recae en Alice Biometrics y por tanto no es necesario que el cliente se encargue de configurar y gestionar interfaces, puertos o servicios. Solo es necesario que disponga de conexión a internet a través de HTTPS.

5.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

38. Todas las comunicaciones del servicio Alice Onboarding solo funcionan con conexiones seguras vía HTTPS con TLSv1.2 o superior.

39. Por otra parte, en lo relativo a las suites de cifrado, se soportan únicamente las están admitidas y consideradas en la guía CCN-STIC 807 como recomendadas. En concreto:

    a) TLS 1.3 (*server has no preference*)

    - *TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS 128*
    - *TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS 256*
    - *TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS 256*

    b) TLS 1.2 (*server has no preference*)

    - *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp521r1 (eq. 15360 bits RSA) FS 128*
    - *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp521r1 (eq. 15360 bits RSA) FS 256*
    - *TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH secp521r1 (eq. 15360 bits RSA) FS 256*

40. Al tratarse de una solución *cloud* toda la gestión recae en Alice Biometrics y por tanto no es necesario que el cliente se encargue de configurar y gestionar nada relativo a estos protocolos.

5.6 GESTIÓN DE CERTIFICADOS

41. Al tratarse de una solución *cloud* toda la gestión recae en Alice Biometrics y por tanto no es necesario que el cliente se encargue de configurar y gestionar certificados en el servicio.

5.7 SERVIDORES DE AUTENTICACIÓN

42. Al tratarse de una solución *cloud* toda la gestión recae en Alice Biometrics y por tanto no es necesario que el cliente se encargue de configurar y gestionar servidores de autenticación.

5.8 SINCRONIZACIÓN HORARIA

43. Al tratarse de una solución *cloud* toda la gestión recae en Alice Biometrics y por tanto no es necesario que el cliente se encargue de configurar y gestionar la sincronización horaria, pues ya lo proporciona Google Cloud Platform.

5.9 ACTUALIZACIONES

44. Al tratarse de una solución *cloud* toda la gestión recae en Alice Biometrics y por tanto las actualizaciones de mejora y correcciones para las capas de Alice API y Alice Dashboard se realizan de forma automática, continúa y transparente para los clientes, informando convenientemente a los clientes en aquellas que precisen realizar algún cambio o ajuste por su parte.
45. En lo relativo a las SDKs, las actualizaciones van acompañadas de unas *release notes* indicando las novedades incluídas para que el cliente pueda decidir realizar la actualización de su producto.

5.10 AUTO-CHEQUEOS

46. Alice Biometrics dispone de mecanismos que están comprobando frecuentemente el correcto funcionamiento de todo el producto Alice Onboarding de forma automática. Así mismo, el propio equipo técnico dispone de una suite de herramientas de monitorización y alertas para estar enterados en tiempo real de todo lo que ocurre en la plataforma.
47. Por otra parte, cabe destacar que al tratarse de una solución *cloud* toda la gestión recae en Alice Biometrics y por tanto no es necesario que el cliente se encargue de configurar y gestionar nada relativo a auto-chequeos.

5.11 SNMP

48. Al tratarse de una solución Cloud toda la gestión recae en Alice Biometrics y por tanto no es necesario que el cliente se encargue de configurar y gestionar lo relativo a SNMP.

5.12 ALTA DISPONIBILIDAD

49. Al tratarse de una solución Cloud toda la gestión recae en Alice Biometrics y por tanto esta se encarga de que el servicio sea replicado en varias instancias simultáneas para garantizar su disponibilidad.

5.13 AUDITORÍA

5.13.1 REGISTRO DE EVENTOS

50. Todas las acciones realizadas en el Alice Dashboard quedan registradas en el sistema de logs de auditoría, con el fin de que un usuario con permiso de auditor pueda consultarlos (a través de la sección “Logs de auditoría” del Alice Dashboard).

51. Los eventos registrados constan de los siguientes campos o información:
    a) Dashboard user → que usuario ha realizado la acción.
    b) Date → cuando se ha realizado la acción.
    c) Action → qué acción se ha realizado.
    d) Affected user → sobre qué usuario se ha realizado la acción.
52. Las acciones que se registran son:
    a) DashboardUserLoggedIn
    b) DashboardUserLoggedOut
    c) DashboardCertificateDownloaded
    d) DashboardUserOnboardingRemoved
    e) DashboardUserOnboardingSeen
    f) DashboardUserOnboardingAuthorized
    g) DashboardUserOnboardingDeauthorized
    h) DashboardUserOnboardingAmlScreened
    i) DashboardUserOnboardingDocumentVoided
    j) DashboardUserOnboardingOtdVoided
    k) DashboardUserOnboardingSelfieVoided
    l) DashboardUserOnboardingDocumentDeleted
    m) DashboardUserOnboardingSelfieDeleted
    n) DashboardUserRemoved
    o) DashboardUserRoleUpdated
    p) DashboardUserPermissionsUpdated
    q) DashboardUserInvited
    r) DashboardUserPasswordUpdated
    s) DashboardUserSettingsSaved

5.13.2 ALMACENAMIENTO LOCAL

53. Al tratarse de una solución *cloud* toda la gestión recae en Alice Biometrics y por tanto esta se encarga de almacenar dicho registro.

5.13.3 ALMACENAMIENTO REMOTO

54. Los registros se almacenan en la infraestructura de Alice Biometrics y solo son consultables a través del Alice Dashboard.

55. Actualmente, el producto Alice Onboarding no permite enviar los registros de auditoría a ningún servidor o plataforma externa.

5.14 BACKUP

56. Al tratarse de una solución *cloud* toda la gestión recae en Alice Biometrics y por tanto es esta quien se encarga de realizar los procesos de *backup* del servicio. Alice Biometrics realiza *backups* de acuerdo con lo definido en su política de SGSI.

5.15 SERVICIOS DE SEGURIDAD

57. Alice Onboarding cuenta con una serie de servicios de seguridad que se encuentran preconfigurados por defecto en cumplimiento de los requisitos indicados en la guía "Taxonomía de productos STIC. Anexo F.11. Herramientas de Video identificación" [REF4], por lo que no es necesario que la empresa cliente aplique ninguna configuración de seguridad adicional.
58. Los principales controles de seguridad son implementados por Alice Onboarding son:
    a) Prueba de vida del *selfie* que combina análisis de video pasivo con presentación de retos aleatorios.
    b) *Matching* facial de *selfie* y documento.
    c) Comprobación de que solo hay una cara presente en el proceso de *selfie.*
    d) Comprobación de número de sesiones, dispositivos, IPs, etc. intervinientes en el proceso de *onboarding*.
    e) Verificaciones de seguridad del documento de identidad, entre otras:
        - El documento mostrado es el esperado.
        - Validación de coherencia de fechas.
        - Contraste entre los campos leídos en la zona de inspección visual (VIZ) y el MRZ.
        - Checks de seguridad del MRZ.
        - Coherencia entre la parte frontal y trasera del documento.
        - Comprobación de que el documento no es mostrado en una pantalla.
        - Comprobación de que el documento no está impreso.
        - Comprobación de que no existen manipulaciones.
    f) *Timeline* descriptivo con todas las interacciones del usuario con el proceso.
59. Para facilitar el proceso de revisión, todos los *checks* de seguridad se agrupan en una vista de resultado del proceso, que consta de cuatro *checks* principales: seguridad del *selfie*, seguridad documental, lectura documental y seguridad del proceso.

a) Seguridad del *selfie* → Indica si el selfie pertenece a una persona real y además coincide con la identidad mostrada en el documento.

b) Seguridad documental → Indica si el documento mostrado es legítimo o por la contra contiene rasgos fraudulentos.

c) Lectura documental → Indica si el documento se ha podido leer correctamente.

d) Seguridad del proceso → Indica si el proceso ha sido realizado correctamente o si por la contra muestra algún indicio o rasgos fraudulentos como cambio de IP, cambio de dispositivo, realización del proceso en varios actos secuenciales, etc.

60. Estos cuatro parámetros permiten tener la decisión global sobre el proceso videoidentificación. Para que un usuario sea aceptado, debe de obtener un resultado positivo en los cuatro (*check* en verde).

61. Además, Alice Dashboard implementa los siguientes elementos de seguridad:

    a) Sistema de roles y usuarios.

    b) Sistema de logs de auditoría.

    c) Usuarios separados para administración y auditoría.

    d) 2FA.

    e) Posibilidad de lectura de NFC de los documentos y verificación de la información interna.

62. Finalmente, el servicio Alice Onboarding, desplegado en Google Cloud Platform y accesible a través de API REST (Alice API) cuenta con los siguientes elementos de seguridad:

    a) Todas las comunicaciones son cifradas con protocolo TLS.1.2 o superior, en cumplimiento de lo indicado en la guía CCN-STIC- 807 Criptología de empleo en el ENS.

    b) Cifrado en reposo de todos los datos con AES 256 (AES-GCM 256 bits).

    c) Autenticación con la API de Alice Onboarding mediante un procedimiento de *tokens* temporales que debe ser implementado siguiendo las instrucciones de la documentación de Alice Onboarding accesible desde Alice Dashboard.

6. FASE DE OPERACIÓN

63. En lo relativo a la operación del servicio, el cliente no necesita tener en cuenta operaciones de mantenimiento, backups, actualizaciones, etc. ya que son gestionadas por Alice Biometrics en el servicio.
64. Para la revisión de los procesos de alta de usuarios y toma de decisión de si son válidos o no, el cliente debe seguir los parámetros y criterios de decisión preconfigurados en el dashboard y explicados en la sección **5.15 SERVICIOS DE SEGURIDAD**.
65. Durante la fase de operación, la empresa deberá gestionar los usuarios y roles de Alice Dashboard, retirando el acceso a aquellos usuarios que ya no lo necesiten y manteniendo el rol y nivel de permisos adecuado para las labores a realizar por parte de cada usuario. Asimismo, deberá encargarse de asignar los permisos de auditoría solamente al personal autorizado y retirarlos una vez dejen de ser necesarios.
66. Se recomienda al cliente de Alice Onboarding estar al día de las nuevas actualizaciones que Alice Biometrics irá publicando regularmente de la capa de las SDKs para decidir su actualización.
67. Como cliente de Alice Biometrics, la empresa dispondrá de acceso a un portal de soporte a través del cual podrá resolver cualquier problema o duda que surja durante la operación y uso del servicio.

7. CHECKLIST

68. Incluir una *checklist* que contenga todas las recomendaciones sobre la configuración de cada apartado. Como ejemplo:

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Reunión *kickoff* con equipo Alice	☐	☐	
Recepción email acceso Alice *Dashboard*	☐	☐	
Aceptar invitación y configurar contraseña Alice *Dashboard*	☐	☐	
Visualización de dos cuentas: -dev y prod	☐	☐	
Importación de la SDK de Alice deseada en la web/app como dependencia	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
El SDK de Alice deseado ha sido configurado con las opciones *Selfie with Challenge* y IDCARD	☐	☐	
El *backend* del cliente hace uso del api key para comunicarse con Alice API	☐	☐	
Los usuarios con acceso a Alice *Dashboard* han activado el 2FA	☐	☐	
El administrador de la cuenta ha invitado al resto de integrantes de su equipo con el rol asociado	☐	☐	
El administrador ha concedido permisos de auditor al menos a un usuario	☐	☐	

8. REFERENCIAS

69. Documentación complementaria que se ha referenciado a lo largo del presente procedimiento de empleo seguro:

REF1 Configuración de SDK Alice Onboarding:
https://docs.alicebiometrics.com/onboarding/sections/alice_integration/sdks_setup/

REF2 Autenticación y gestión de *tokens* de Alice Onboarding:
https://docs.alicebiometrics.com/onboarding/sections/alice_integration/authentication/

REF3 Alice Onboarding *report*:
https://docs.alicebiometrics.com/onboarding/sections/report/report/

REF4 Taxonomía de productos STIC. Anexo F.11. Herramientas de Video identificación (CCN-STIC 140.F11)
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

REF5 Configuración SDK Android:
https://docs.alicebiometrics.com/onboarding/sections/mobile_client_side_sdks/android/#4-stages-configuration

REF6 Configuración SDK iOS:
https://docs.alicebiometrics.com/onboarding/sections/mobile_client_side_sdks/ios/#4-stages-configuration

REF7 Configuración SDK Web:
https://docs.alicebiometrics.com/onboarding/sections/web_client_side_sdks/html_js/#3-onboarding-flow

9. ABREVIATURAS

2FA	*Two Factor Authentication*
API	*Application Programming Interface*
ENS	Esquema Nacional de Seguridad
OTP	*One Time Password*
PAD	*Presentation Attack Detection*
SaaS	*Software as a Service*
SDK	*Software Development Kit*
SO	Sistema Operativo
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