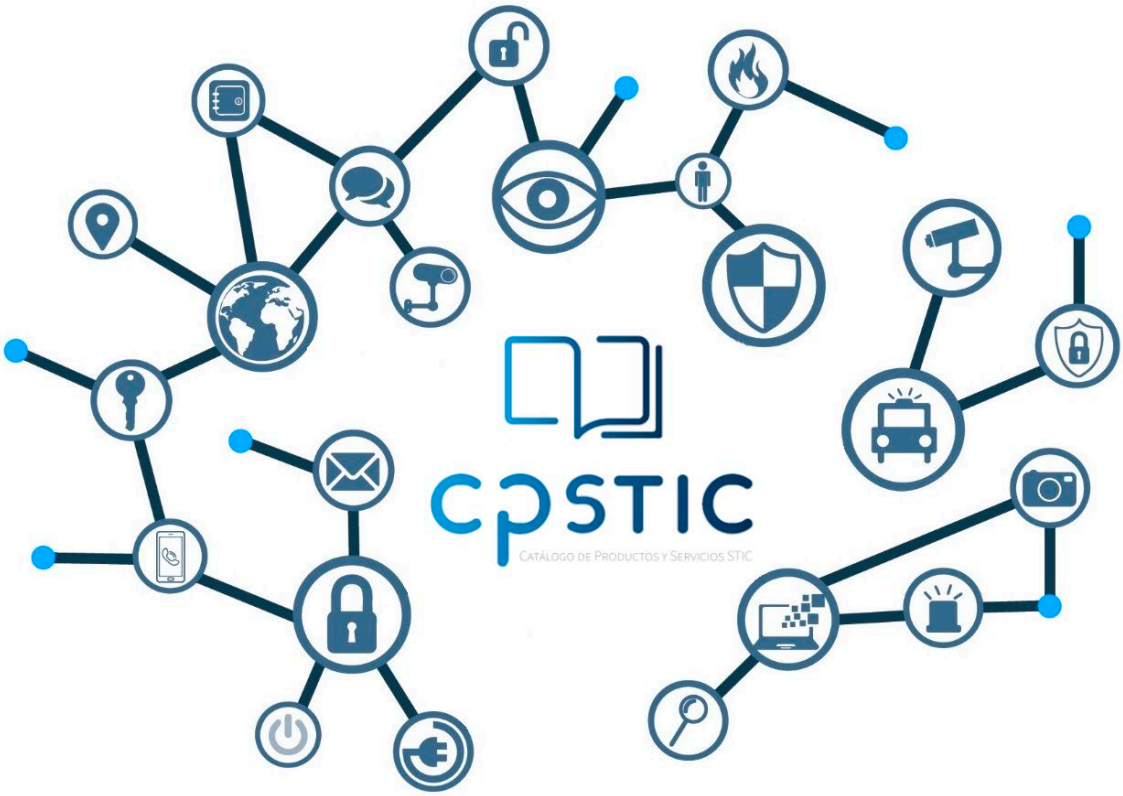
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC-1630

Procedimiento de empleo seguro
Inetum Digital Onboarding Platform



Febrero de 2024

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 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
2024.03.01 11:21:31 +01'00'

NIPO: 083-24-092-9.
Fecha de Edición: febrero de 2024.

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. INETUM ofrece los servicios de su Plataforma de Identidad Digital para ser integrados en los sistemas de los clientes con el objetivo de cubrir distintos casos de uso, entre ellos el Onboarding Digital.
2. La Plataforma de Identidad Digital de INETUM es una colección de microservicios que contempla múltiples opciones de configuración para cubrir las necesidades de los flujos de negocio que el cliente requiera. Dentro de estos flujos, el conjunto de microservicios que constituyen la configuración específica denominada "**Inetum Digital Onboarding 1.0**" son los que han sido cualificados. El modelo de consumo es el de Software como Servicio (*SaaS*) por lo que esto se traduce en un pago por uso de los servicios.
3. La configuración del Onboarding Digital para actuar bajo los Requisitos y Estándares de Calidad de la Guía CCN-STIC 140 ANEXO F11, realiza las siguientes funcionalidades:
    - Verificación del documento capturado y obtención de un *scoring* de evaluación documental a partir del análisis de más de 30 puntos.
    - Clasificador de calidad de imagen. Obtiene un *scoring* de una forma objetiva sobre la calidad de la imagen de un documento.
    - Normalización y enriquecimiento sobre la calidad del dato de las direcciones que se obtienen mediante OCR en los documentos de Identidad.
    - Vídeo-identificación y verificación biométrica multiplataforma, que permite realizar la captura de vídeo en tiempo real (*streaming*).
    - Identificación biométrica y documental de manera guiada automáticamente y desatendida.
    - *Anti-spoofing* (prueba de vida pasiva) en el caso del *selfie*.
    - Análisis de manipulación documental mediante modelos entrenados, que levantan alertas al operador en su posterior revisión.
    - Garantía de canales seguros de captura de evidencias, evitando la inyección de vídeo y los ataques de presentación.
    - Generación de sellado de tiempo a través de prestador cualificado de servicios electrónicos de confianza incluido en la TSL, para el almacenamiento de las evidencias.
    - Custodia y/o almacenamiento de las pruebas documentales y de todas las evidencias utilizadas para la identificación, para poder ser utilizadas ante posibles reclamaciones o litigios.
    - Portal de gestión de transacciones en *backoffice*, que permite que un operador pueda revisar las identificaciones obtenidas y otras funciones.

2. OBJETO Y ALCANCE

4. El objeto del presente documento es detallar cómo se realiza la integración y configuración del servicio Digital Onboarding de la Plataforma de Identidad Digital de Inetum en su versión **cualificada e incluida en el catálogo de productos Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC), siguiendo los Requisitos y los Estándares de Calidad de la guía CCN-STIC 140 ANEXO F11.**

5. El servicio de video identificación está ofrecido como SaaS y está compuesto por los siguientes componentes:

   - **SDK web**: compatible con cualquier tecnología (*javascript, iFrame, webview*…), que se integra en la web del cliente. Es altamente configurable mediante parámetros, y se comporta según dicha configuración (texto, colores, e incluso pasos en la toma de evidencias). El SDK web puede ejecutarse en desktop y en un dispositivo móvil dado que es totalmente responsive.
   - **SDK Android (nativo):** se integra en la App Android del cliente. Es altamente configurable mediante parámetros, y se comporta según dicha configuración (texto, colores, e incluso pasos en la toma de evidencias).
   - **SDK iOS (nativo):** se integra en la App iOS del cliente. Es altamente configurable mediante parámetros, y se comporta según dicha configuración (texto, colores, e incluso pasos en la toma de evidencias).
   - **dobAPIDob-API**: API REST securizada, mediante la cual se controla todo el flujo de cada transacción iniciada. Se comunica con el SDK y con el backend del cliente

3. ORGANIZACIÓN DEL DOCUMENTO

6. Este documento se compone de los siguientes apartados:

   a) **Apartado 4**: Se recogen aspectos y recomendaciones a considerar, antes de proceder a la integración del servicio.

   b) **Apartado 5**: Se describe el proceso de integración del servicio y se recogen recomendaciones a seguir.

   c) **Apartado 6**: Se recogen las recomendaciones de configuración para mantener una configuración segura.

   d) **Apartado 7**: Se describen los mecanismos para conseguir el mejor rendimiento del servicio en fase de operación.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

7. Cuando un cliente muestra su interés en la integración del servicio Digital Onboarding de Inetum se agenda una reunión de presentación en la que se explica el servicio y sus componentes y se informa de los pasos a dar para la integración del Onboarding en su sistema.
8. Con el cliente, se define también qué flujo necesita integrar en su sistema y mediante qué canales. Además, se acuerda el canal de comunicación de *backend* a *backend*, pudiendo ser mediante llamadas SSL con TLS 1.2 o superior, o por VPN.
9. Tras la firma del contrato, Inetum hace entrega al cliente de los siguientes elementos mediante enlace de descarga segura del *Sharepoint* de Inetum o mediante acceso al Portal privado de descargas:
    - Documentación del *dob-API* (REF1).
    - Última versión del SDK web (y/o nativos) y documentación de integración, que incluye un proyecto de integración de ejemplo (REF7, REF8, REF9).
    - *Token* de cliente, necesario para la autenticación, tanto de preproducción como de producción.
    - Certificado digital para las llamadas REST.
    - URLs de acceso al API, tanto de preproducción como de producción.
    - Documentación del BackOffice (REF2).
    - Documentación de la arquitectura y seguridad de la plataforma (REF3).
    - Usuarios de acceso al *BackOffice*, previamente personalizado con los colores y logo del cliente. Se aconseja activar el Factor de Doble Autenticación para el acceso a dicho BackOffice, mediante el uso de OTP disponible.
    - Y finalmente, si el cliente va a optar por su propio BPO para la revisión técnica, se adjunta el procedimiento de revisión (REF4) y la guía de las validaciones técnicas (REF5).
10. El cliente deberá proveer a Inetum de las URLs de *callback* para la notificación automática de los pasos necesarios en el proceso, en el caso de que se quiera automatizar esta respuesta.
11. Además, se ofrecen sesiones de trabajo para la guía en la integración del SDK.

4.2 ENTORNO DE INSTALACIÓN SEGURO

12. El servicio de Digital Onboarding se encuentra desplegado en las instalaciones de KIO Networks, DC TIER IV, ubicado en Murcia. Estas instalaciones cumplen con el Esquema Nacional de seguridad categoría ALTA.
13. KIO también dispone de otras certificaciones de seguridad y capacidad ISO-20000, ISO-27001, ISO 27017, ISO 27018, ISO 22301, PCI-DSS Y RGPD entre otras.
14. **No será necesaria ninguna instalación en el cliente pues se ofrece en modo SaaS (*Software as a Service*)**, facilitando de este modo la integración del servicio con el cliente.

Esta integración se hace a nivel de SDK, siguiendo la tecnología *front* deseada por el cliente, y a nivel de *backend*, mediante llamadas a nuestros servicios REST.

4.3 REGISTRO Y LICENCIAS

15. El Digital Onboarding de Inetum se ofrece como un servicio SaaS por lo que no requiere ningún tipo de licencia, y su modelo de negocio es de pago por uso.

4.4 CONSIDERACIONES PREVIAS

16. La comunicación con el componente dob-API (ver sección 5.2) se realiza a través de dos tipos de comunicación, y en función de la elegida por el cliente se deberán hacer las configuraciones pertinentes:

    - Comunicación segura mediante protocolo https. La versión de TLS admitida es 1.2 o superior, usando solamente los *cipher suites* seguros recomendados por el CCN.
    - Comunicación por VPN. Se deberá establecer el túnel VPN entre el cliente y el entorno de la Plataforma de Identidad Digital, donde se encuentra desplegado el servicio de Digital Onboarding.

17. Además, se deberá habilitar por parte del cliente tantas URLs (junto con sus puertos) como *callbacks* se invoquen en el flujo definido.

18. En lo referente a la integración y uso del producto, las restricciones a la fecha de edición de este documento existen los requisitos mínimos mostrados a continuación.

19. Las versiones mínimas de los navegadores soportados por el SDK web son las siguientes:

Navegadores	Versión mínima
Chrome Desktop	85
Chrome Mobile	90
Firefox Desktop	94
Safari Desktop y Mobile	11
Edge Desktop	95

20. En cuanto a las versiones Android/iOS siempre se actualizan con respecto a los requisitos de las *stores*, a fecha de hoy las versiones mínimas soportadas:

Sistemas Operativos	Versión mínima
iOS	• *XCode 14* • *Swift 5.7* • S.O. iOS 11 (si se usa el flujo de NFC, deberá ser iOS 13)

Sistemas Operativos	Versión mínima
Android	• *Android Studio 2021.3.1* • *Kotlin 1.4.32* (también se puede integrar en una App hecha en java) • *S.O. Android 7*
NOTA: también se da soporte a integraciones en tecnologías híbridas como Cordova o Xamarin.	

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

21. Como se ha indicado ya, el servicio del Digital Onboarding es un servicio SaaS, por lo que no requiere la instalación de ningún componente más allá de la integración del SDK y de las llamadas *backend* a *backend* vía API rest.

5. FASE DE INSTALACIÓN

22. El servicio Digital Onboarding de la Plataforma de Identidad Digital de Inetum se ofrece como un servicio SaaS, por lo que no requiere de ninguna instalación, pero sí requiere integración por parte del cliente, tanto para la parte *front* (SDK) como la parte de *backend*.

5.1 INTEGRACIÓN DE SDK

23. En función de la tecnología decidida por el cliente, existen unas guías de integración de cada una de las tecnologías (web, iOS y Android) y además de la guía, que se puede descargar y/o consultar en el portal privado, En la sección Documentación/[SDK concreto]:

24. El SDK va acompañado de un proyecto de ejemplo para ayudar en la integración.

25. Además de esto, siempre se ofertan sesiones conjuntas para dar soporte a la integración, e incluso se puede solicitar que el equipo técnico de Inetum realice esta integración. En algunos casos si el cliente tiene la necesidad también se ha solicitado el desarrollo de la web o app completa que integra el SDK, servicio que también se puede solicitar.

5.2 INTEGRACIÓN DE BACKEND

26. El cliente controla el flujo del Onboarding desde su backend, por lo que se debe realizar una integración muy sencilla utilizando los servicios REST que brinda el dob-API. La guía de estos servicios también se encuentra en el portal privado, desde donde se puede consultar/descargar.


Home > Documentación SDK's > Backend
Documentación Backend
SDK´s
Web
iOS
Android
Cordova
Backend
Documentación
Versiones
Descargas
Listado de publicaciones
Versión 2.0.0 (07/12/2021)
Versión 1.2.7 (13/06/2022)
Versión 1.2.6 (04/04/2022)
Versión 1.2.5 (14/01/2022)
Versión 1.2.4 (09/07/2021)

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

27. El servicio SaaS de Onboarding Digital se entrega preconfigurado para el cumplimiento de los requisitos definidos en la guía CCN-STIC 140 ANEXO F11, por lo que los clientes no necesitan hacer la configuración. En cualquier caso, en la guía de uso del BackOffice [REF2] se indica la configuración que cumple con los requisitos definidos en la guía CCN-STIC 140 ANEXO F11.
28. La configuración de la plataforma se lleva a cabo mediante varios módulos. Estos módulos, que se explican a continuación, contienen una amplia gama de parámetros de configuración.
29. Entre estos, se incluyen algunos específicos diseñados para satisfacer los requisitos establecidos en la guía CCN-STIC 140 ANEXO F11.
30. Para integrar el SDK correctamente, es necesario realizar ciertas configuraciones específicas, las cuales también se detallarán a continuación y son esenciales para cumplir con los mencionados requisitos.

- **BackOffice**:
  - **Administrador de Inetum**: Esta configuración la hace el personal de INETUM. El administrador puede configurar los servicios que deben activarse o desactivarse para el Onboarding. En este caso, la configuración debe ser:
    - Configuración de flujo de Onboarding, que debe constar de los siguientes pasos:
      - Captura de documento (anverso y reverso)
      - Grabación de vídeo en streaming
      - Captura de selfie
    - Antispoofing pasivo: activo
    - Módulo de detección de manipulación documental: activo
    - Módulo de detección de inyección de vídeo: activo
  - **Supervisor**: el supervisor puede ajustar los umbrales a los distintos componentes. Este perfil es el que suele proporcionarse a los clientes. La configuración está explicada en la guía de uso del BackOffice [REF2].
- **Integración vía API:**
  - **Inicio de transacción** (POST /dob-api/transaction/new). En este end-point se define el flujo que tendrá la transacción que se inicia, que debe coincidir con la que indicará el SDK. Además, se pueden remitir opcionalmente datos de la transacción que se compararán con los capturados para asegurar que la información que provee el usuario y la que se captura es consistente. A partir de esta llamada, se desencadena todo el proceso en el SDK. Ver documento Guía de Referencia del API Rest – Onboarding [REF1].
  - **Resultado de revisión técnica.** Tras la captura de las evidencias y la posterior revisión por un operador experto, el backend del cliente tiene dos formas posibles de implementación para recuperar el resultado:

- **Callback:** se puede configurar un endpoint en las pantallas de configuración del BackOffice (Guía de uso del BackOffice [REF2]) del cliente al que se invocará desde la Plataforma de Identidad para notificar el cambio de estado de la transacción.
- **Pull:** si no se configura un callback, el cliente puede realizar llamadas a modo de pull al endpoint que devuelve el resultado de la revisión:

  GET /dob-api/transaction/${userID}/results

- **Descarga de evidencias.** El cliente podrá descargarse a su entorno las evidencias de las transacciones, pudiendo seleccionar una en concreto o todas, mediante la invocación al servicio:

  GET /dob-api/transaction/${userID}/evidence?e=${evidenceDwld}

6.2 AUTENTICACIÓN

31. El acceso a todos los componentes requiere de autenticación, según lo indicado a continuación:

- **BackOffice:** los usuarios que accederán al Backoffice (https://pro.digitalonboarding.es/dob/dob-backoffice/login#/) necesitarán un usuario y una contraseña (que sigue las políticas de las contraseñas seguras definida en la sección 6.3.2), y en el acceso se solicitará una OTP remitida por correo. Asimismo, el usuario deberá usar un recaptcha para evitar el uso de ataques de fuerza bruta.
- **Backend:** la autorización en las llamadas del cliente a nuestro backend requerirá del uso de un token de autenticación (tipo Bearer) de cliente proporcionado por Inetum y generado por nuestro api manager. La comunicación será mediante TLSv1.2 o superiores con cipher suites seguras y certificado RSA 4096 (siguiendo las recomendaciones del CCN).
- **SDK:** el SDK autentica la comunicación mediante el token de autenticación del cliente, y además se protege mediante comunicación https con TLSv1.2 y superior y RSA 4096. Además, se realiza un cifrado de extremo a extremo entre el SDK y el Backend, que evita la manipulación fraudulenta y la intercepción de la información transmitida.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN REMOTA

32. La única administración del servicio SaaS que un cliente puede hacer se realiza de forma segura mediante comunicación https (con TLSv1.2 y superior y RSA 4096) al Backoffice que ofrecemos, usando un usuario con rol de Supervisor o Administrador. Estos usuarios se dan previamente de alta por el equipo de Inetum.
33. Mientras un usuario con rol de Administrador que puede dar de alta y de baja usuarios en el BackOffice, un usuario con rol Supervisor, podrá ajustar los umbrales de configuración de la plataforma.
34. El control de acceso al BackOffice está descrito en el punto 6.2 AUTENTICACIÓN.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

35. La descripción del funcionamiento del BackOffice se encuentra en el documento Guía de uso del BackOffice.

36. Existen los siguientes **roles**:

    - Administrador global, que es un rol para la administración de los clientes, y sólo tiene acceso personal de INETUM.
    - Administrador de cliente, que se proporciona a los clientes, y que tiene la función principal de administrar los usuarios que puede tener acceso a la plataforma (al entorno del cliente) y sus roles. Accede también a las transacciones.
    - Supervisor, que puede administrar la configuración de umbrales. Accede también a las transacciones.
    - Operador, que puede acceder a las transacciones

37. La **política de contraseñas** es fija para todos los clientes, sus requisitos son los siguientes:

    - Longitud mínima de 8 caracteres.
    - Al menos una letra mayúscula, una letra minúscula, un número y un carácter especial.
    - Que la nueva contraseña no sea igual a las 3 contraseñas anteriores.
    - La contraseña tiene una validez de 360 días.
    - La contraseña se persiste de forma cifrada en base de datos.
    - Cuando se da de alta un usuario o se reactiva desde el BackOffice por un usuario con rol de administrador, (ver Guía de Referencia del Backoffice [REF2]), se remite un correo con una contraseña temporal que debe ser cambiada la primera vez que se accede al sistema, momento en el que se activa el usuario. Una vez generada y enviada dicha contraseña temporal, el usuario dispone de 24 horas para activar el usuario, sino será bloqueado.
    - La contraseña creada tiene un tiempo de validez de 360 días antes de expirar. Si se requiere de un tiempo de expiración menor, será responsabilidad del cliente establecer un procedimiento de cambio de contraseñas para realizar el cambio de forma manual.
    - No está establecido un periodo de tiempo que deba trascurrir tras desde el último cambio de contraseña para que esta pueda ser cambiada de nuevo. Será responsabilidad del cliente establecer un procedimiento para informar a los usuarios que no cambien de contraseña si antes no ha transcurrido 10 días desde la última modificación.
    - En cuanto a la configuración de parámetros de sesión, las políticas son las siguientes:
    - La sesión caduca (se cierra) tras un periodo de inactivad de 30 minutos.
    - El usuario debe facilitar una OTP remitida por correo cada vez que ingrese en el sistema. Esta OTP tiene un periodo de validez de 5 minutos. El usuario puede solicitar un máximo de 2 reenvíos y tiene como máximo 3 intentos de validación antes de ser bloqueado.

- Tras los 3 intentos fallidos, el usuario será bloqueado de forma permanente, y será responsabilidad del cliente (usando un usuario con rol administrador) realizar el desbloqueo desde el BackOffice.
- No se establece un mecanismo que bloquee a usuarios que no hayan hecho login en un periodo establecido de días. Es el cliente el encargado de establecer por política esta funcionalidad.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

38. Como se ha venido indicando, el Digital Onboarding es un servicio que se ofrece en modo SaaS (cloud), y por lo tanto el requisito mínimo para los clientes es una conexión a internet a través de HTTPS, con el protocolo TLS v1.2 o superior y con el uso de cipher suites seguros. La URL de conexión está indicada en la Guía de Referencia del API Rest – Onboarding [REF2]
39. Si además se configura en las pantallas de configuración del BackOffice (Guía de uso del BackOffice [REF2]) el Digital Onboarding para recibir callbacks (eventos que se lanzan desde el BackOffice según se van completando etapas del proceso), se deberán configurar también la IP y el puerto de entrada a su sistema.

6.5 GESTIÓN DE CERTIFICADOS

40. Todas las comunicaciones con el servicio Digital Onboarding de la Plataforma de Identidad Digital cumplen las características siguientes:
    - Certificado digital con clave RSA de 4096 bits de longitud.
    - Comunicación segura https con TLS v1.2 o superior.
    - Las cipher suites de cifrado usadas son las recomendadas en la guía CCN-STIC 807:

    TLSv1.3:

    TLS_AES_128_GCM_SHA256 Curve 25519 DHE 253 (Preferred)

    TLS_AES_256_GCM_SHA384 Curve 25519 DHE 253

    TLS_CHACHA20_POLY1305_SHA256 Curve 25519 DHE 253

    TLSv1.2:

    ECDHE-RSA-AES256-GCM-SHA384 Curve 25519 DHE 253 (Preferred)

    DHE-RSA-AES256-GCM-SHA384 DHE 2048 bits

    ECDHE-RSA-CHACHA20-POLY1305 Curve 25519 DHE 253

    ECDHE-RSA-AES128-GCM-SHA256 Curve 25519 DHE 253

    DHE-RSA-AES128-GCM-SHA256 DHE 2048 bits
41. La configuración de los protocolos se realiza en la infraestructura de la Plataforma de Identidad, por lo que el cliente que contrate el servicio no necesita realizar ninguna configuración adicional.
42. La comunicación de los servicios críticos entre el SDK y el *backend* está cifrada de extremo a extremo con un mecanismo híbrido con AES-256 y RSA 4096.

6.6 SERVIDORES DE AUTENTICACIÓN

43. El Digital Onboarding no utiliza servidores de autenticación.

6.7 SINCRONIZACIÓN

44. La plataforma de Digital Onboarding, ofrecida como servicio SaaS, se encarga de gestionar la sincronización entre los distintos componentes mediante el servicio NTP. De esta manera el cliente puede despreocuparte de este aspecto.

6.8 ACTUALIZACIONES

45. La actualización del servicio de Digital Onboarding se realiza a distintos niveles.

6.8.1 A NIVEL DE INFRAESTRUCTURA

46. La Plataforma de Digital Onboarding está incluida en el programa “Shadowing-IT” de la Oficina Técnica de Seguridad de Inetum, que nos alerta de las nuevas vulnerabilidades que nos puedan afectar en nuestro software de base de la plataforma.
47. Contamos también con antivirus que controlan en todo momento cualquier tipo de posible alteración en el sistema.
48. Nuestro proveedor de infraestructura provee una seguridad perimetral con los estándares más altos de calidad.

6.8.2 A NIVEL DE BACKEND

49. Las actualizaciones son transparentes para el cliente que contrata el servicio. Estas actualizaciones consisten en mejoras tanto funcionales como de rendimiento o seguridad.
50. En el caso de ser funcionales, se comunican a los clientes. Estas actualizaciones no suponen un corte o parada en el servicio por norma general, y siempre son retro-compatibles con los SDKs que estén utilizando los clientes.

6.8.3 A NIVEL DE SDK

51. En el momento en el que se libera una nueva versión del SDK se comunica a los clientes y se recomienda su actualización.
52. Estas versiones siempre incluyen un fichero de gestión de cambios y una guía de instalación.

6.8.4 A NIVEL DE BACKOFFICE

53. Cuando el BackOffice incluye una actualización en el proceso de revisión, se notifica a los clientes que estén utilizando un servicio de BPO ajeno a Inetum para su gestión, y se programa un periodo de formación para los operadores antes del paso a producción.

6.9 AUTO-CHEQUEOS

54. La plataforma de Digital Onboarding dispone de una herramienta de monitorización en tiempo real que lanza alertas en el caso de que se alcance algún indicador de riesgo previo siempre al incidente.

55. Además, se dispone de un conjunto de sondas que auto chequean que los servicios críticos respondan.
56. Estas herramientas se complementan con un equipo de soporte que vela por el buen funcionamiento del servicio 24x7.

6.10 ALTA DISPONIBILIDAD

57. La alta disponibilidad se gestiona en la Plataforma de Identidad Digital y los clientes que contraten el servicio no tienen que configurar nada en su sistema.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

58. Los **eventos de usuario** que se registran en el sistema son los siguientes:
    - *Login.*
    - *Logout.*
    - Revisión técnica.
    - Redictaminación.
    - Cambio de contraseña.
    - Cambio de configuraciones (umbrales entre otros).
59. Por otro lado, el **SDK** envía al BAM (*Business Activity Monitor*) todos los eventos que se capturan en el SDK (además de los que los clientes quieran inyectar desde las aplicaciones que integran los SDKs.
60. Finalmente, todos los servicios generan ficheros de log con información del UID de la transacción y registro de las acciones que se realizan para facilitar la reconstrucción del flujo del servicio.
61. El acceso a los registros de eventos de usuario y a los logs de los servicios están disponibles bajo petición. Los del SDK se pueden consultar en el BackOffice, en la pestaña de trazabilidad de una transacción (Guía de uso del BackOffice [REF2]).

6.11.2 ALMACENAMIENTO LOCAL

62. No existe un almacenamiento local puesto que es un servicio cloud.

6.11.3 ALMACENAMIENTO REMOTO

63. No existe un procedimiento de envío remoto de registro de logs o de eventos.

6.12 BACKUP

64. La política de backup se realiza por parte de Inetum junto con el proveedor de IaaS bajo la política de SGSI. El cliente que contrata el servicio no debe realizar acciones adicionales.

6.13 TRATAMIENTO DE EVIDENCIAS DE VIDEOIDENTIFICACIÓN

65. Las evidencias de videoidentificación, son protegidas en tránsito y comprobadas por mecanismos automáticos y manuales.

66. En las subsecciones siguientes se definen los distintos mecanismos de seguridad relativos al tratamiento de las evidencias de videoidentificación.

67. **Estos mecanismos no requieren de configuración por parte del usuario final y los procesos manuales se llevan a cabo por personal de Inetum.**

6.13.1 PROTECCIÓN DE LAS COMUNICACIONES

68. Las evidencias transmitidas al *backend* son protegidas mediante las siguientes medidas de seguridad a nivel de IaaS:

    - Comunicación segura (protocolo https con TLS 1.2 o superior) y cifrado de extremo a extremo.
    - Firewall que protege de tráfico no deseado.
    - Autenticación por *token* en WSO2.

6.13.2 COMPROBACIONES AUTOMÁTICAS

69. Las funciones automáticas de seguridad incorporadas en el proceso de Digital Onboarding garantizan que los datos y las evidencias proporcionadas por los usuarios han superado ciertas pruebas para poder conseguir un dictamen exitoso.

70. Estas funciones automáticas se entregan configuradas según los estándares definidos en la guía CCN-STIC 140 ANEXO F11 y han superado las pruebas indicadas en la IT.014.

    - Protección frente a ataques de presentación
    - Detección de manipulación de documentos
    - Match facial (verificación biométrica)
    - Prueba de vida pasiva
    - Protección frente a manipulación en el canal de comunicación
    - Chequeos sobre la consistencia de los datos aportados y leídos

6.13.3 COMPROBACIONES MANUALES

71. Finalmente, las evidencias aportadas, así como los *scoring* que las funciones anteriores han arrojado, son presentadas al operador en el BackOffice en el momento de la Revisión Técnica. El equipo de operadores de Inetum está formado en la validación de este tipo de evidencias.

72. El proceso de revisión guía al operador a través de proceso mediante preguntas, alertas y recordatorios, incluso mostrando reglas de negocio que cada cliente pueda incluir en el proceso de revisión.

7. FASE DE OPERACIÓN

73. Durante la fase de operación Inetum pone a disposición de los clientes un Servicio de Gestión liderado por un Delivery Manager que realizará seguimiento, junto con el cliente, del rendimiento del servicio, las métricas, el funnel de conversión y posibles mejoras, orientando el servicio a obtener la mayor cuota de conversión y nivel de seguridad posibles.

74. El cliente que contrate el Digital Onboarding no tendrá que preocuparse de ninguna tarea a nivel de Operación más allá de las integraciones con su sistema y/o recogida de evidencias.

75. El correcto funcionamiento del sistema está garantiza por Inetum mediante las acciones o procedimientos que se han ido indicando en este documento, y otras adicionales que también se indican a continuación:

    - Inclusión en el programa "*Shadowing IT*" de la OTS, que vela por la actualización de SW base en la infraestructura junto con antivirus en la infraestructura.
    - Seguridad perimetral ofrecido por nuestro proveedor *Iaas* KIO.
    - Monitorización del sistema.
    - Sondas de auto-chequeo.
    - Servicio de guardia 24x7.

8. REFERENCIAS

REF1 INETUM-DOB-TI-Guía de Referencia del API Rest - Onboarding

REF2 INETUM-DOB-TI-Guía de Referencia del Backoffice.pdf

REF3 INETUM-DOB-TI-Arquitectura y Seguridad

REF4 INETUM-DOB-Procedimiento de Revisión técnica

REF5 INETUM-DOB-DF-Validaciones Revisión Técnica

REF6 INETUM-DOB-Formación Operadores Backoffice

REF7 Documentación-SDK-Android (según versión)

REF8 Documentación-SDK-iOS (según versión)

REF9 Documentación-SDK-Web (según versión)

9. ABREVIATURAS

API	*Application Programming Interface*
CA	*Certification Authority*
CPD	Centro de Proceso de Datos
ENS	Esquema Nacional de Seguridad.
HTTPS	*HyperText Transfer Protocol Secure*
IaaS	*Infrastructure as a Service*
MRZ	*Machine Readable Zone*
OTP	*One time password*
OTS	*Oficina Técnica de Seguridad*
SaaS	*Software as a Service*
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